

# Systemwalker Desktop Keeper V14g



## User's Guide for Administrator

Windows

B1WD-2774-05ENZ0(00)  
March 2012

# Preface

---

## Purpose of This Guide

This guide describes how to use the following product:

- Systemwalker Desktop Keeper V14g (14.2.0)

The target readers of this manual are the users of Windows.

## Intended Readers

This guide is for readers who construct/apply information protection systems using Systemwalker Desktop Keeper.

This guide assumes readers have the following knowledge:

- General knowledge of PCs
- General knowledge of Microsoft® Windows
- General knowledge of the Internet
- General knowledge of VMware View™ (when installing client (CT) in the VMware View™ environment)
- General knowledge of Citrix XenDesktop™ (when installing client (CT) in the VMware View™ environment)
- General knowledge of Citrix XenApp™ (when using the monitoring function of the Citrix XenApp)

## Structure of This Guide

This guide consists of chapters 1-8 and Appendix A.

### [Chapter 1 Before Operation](#)

### [Chapter 2 Prepare Operating Environment](#)

This chapter describes the methods for policy setting and preparation of operating environment.

### [Chapter 3 Set Policy in Management Console](#)

### [Chapter 4 Check Trend of Client \(CT\) Operation](#)

### [Chapter 5 Audit Operations on Client \(CT\) via Log Viewer](#)

### [Chapter 6 Create Auditing Material](#)

This chapter describes the methods for creating auditing files.

### [Chapter 7 Change Operating Environment](#)

This chapter describes the methods for changing the operating environment.

### [Chapter 8 Policies That Can be Set](#)

This chapter describes the policies that can be set by Systemwalker Desktop Keeper.

### [Appendix A List of Aggregation Objectives](#)

This chapter describes the purposes for statistics set in the log viewer.

## Location of This Guide

The location of this guide in Systemwalker Desktop Keeper manuals is as follows.

Manual Name	Content
Systemwalker Desktop Keeper User's Guide	This guide describes the summary and the operating environment of Systemwalker Desktop Keeper.
Systemwalker Desktop Keeper Installation Guide	This guide describes the installation settings, as well as maintenance and management measures of Systemwalker Desktop Keeper.
Systemwalker Desktop Keeper User's Guide: for Administrator (This Guide)	This guide describes how to use Systemwalker Desktop Keeper.
Systemwalker Desktop Keeper User's Guide: for Client (Note)	This guide describes the function summary and operation methods of Export Utility of Systemwalker Desktop Keeper.
Systemwalker Desktop Keeper Reference Manual	This manual describes the commands, files, messages and port numbers used in Systemwalker Desktop Keeper.
Systemwalker Desktop Keeper Troubleshooting Guide	This guide describes the causes and processing methods for assumed exceptions in Systemwalker Desktop Keeper.

Note: "Systemwalker Desktop Keeper User's Guide for Client" can also be viewed from the "Help" of Systemwalker Desktop Keeper Export Utility.

## Notations

For the convenience of description, this guide uses the following names, symbols and abbreviations.

### Symbols Used in Commands

This subsection describes the symbols used in examples of commands.

#### Meaning of symbol

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

### Icons

The following icons are used in manuals.



Note

The above symbol applies to items requiring special attention.



Point

The above symbol applies to skills required for more efficient use of this software.

### Abbreviations

The manual uses abbreviations of the following products:

Product Name	Abbreviation
Systemwalker Desktop Keeper Base Edition V12.0L10	BEV12.0L10

Product Name	Abbreviation
Systemwalker Desktop Keeper Base Edition V12.0L20	BEV12.0L20
Systemwalker Desktop Keeper Base Edition V13.0.0	BEV13.0.0
Systemwalker Desktop Keeper Base Edition V13.2.0	BEV13.2.0
Systemwalker Desktop Keeper Base Edition V13.3.0	BEV13.3.0
Systemwalker Desktop Keeper Standard Edition V12.0L20	SEV12.0L20
Systemwalker Desktop Keeper Standard Edition V13.0.0	SEV13.0.0
Systemwalker Desktop Keeper Standard Edition V13.2.0 Systemwalker Desktop Keeper Standard Edition V13.2.1	SEV13.2.0
Systemwalker Desktop Keeper Standard Edition V13.3.0	SEV13.3.0
Systemwalker Desktop Keeper V14g (14.0.0)	V14.0.0
Systemwalker Desktop Keeper V14g (14.0.1)	V14.0.1
Systemwalker Desktop Keeper V14g (14.1.0)	V14.1.0
Systemwalker Desktop Keeper V14g (14.2.0)	V14.2.0
Microsoft® Internet Explorer® 6.0 Windows® Internet Explorer® 7 Windows® Internet Explorer® 8 Windows® Internet Explorer® 9	Internet Explorer®

The manual uses abbreviations of the following operation systems:

OS	Abbreviation
Microsoft® Windows Server® 2008 Foundation Microsoft® Windows Server® 2008 Standard Microsoft® Windows Server® 2008 Enterprise Microsoft® Windows Server® 2008 Standard without Hyper-V™ Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ Microsoft® Windows Server® 2008 R2 Foundation Microsoft® Windows Server® 2008 R2 Standard Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® Small Business Server 2011 Essentials	Windows Server® 2008(※)
Microsoft® Windows Server® 2003, Standard Edition Microsoft® Windows Server® 2003, Enterprise Edition Microsoft® Windows Server® 2003 R2, Standard Edition Microsoft® Windows Server® 2003 R2, Enterprise Edition Microsoft® Windows Server® 2003, Standard 64-bit Edition Microsoft® Windows Server® 2003, Enterprise 64-bit Edition Microsoft® Windows Server® 2003 R2, Standard 64-bit Edition Microsoft® Windows Server® 2003 R2, Enterprise 64-bit Edition	Windows Server® 2003(※)
Microsoft® Windows® 2000 Professional operating system Microsoft® Windows® 2000 Server operating system Microsoft® Windows® 2000 Advanced Server operating system	Windows® 2000
Microsoft® Windows® XP Professional Microsoft® Windows® XP Home Edition	Windows® XP(※)
Windows Vista® Home Basic Windows Vista® Home Premium Windows Vista® Business Windows Vista® Enterprise Windows Vista® Ultimate	Windows Vista®(※)



OS	Abbreviation
Windows® 7 Ultimate Windows® 7 Enterprise Windows® 7 Professional Windows® 7 Home Premium	Windows® 7(※)
Microsoft® Windows® Millennium Edition	Windows® ME
Microsoft® Windows® 98 Second Edition	Windows® 98
Microsoft® Windows® 95 operating system	Windows® 95
Microsoft® Windows Server® 2008 Foundation Microsoft® Windows Server® 2008 Standard Microsoft® Windows Server® 2008 Enterprise Microsoft® Windows Server® 2008 Standard without Hyper-V™ Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ Microsoft® Windows Server® 2008 R2 Foundation Microsoft® Windows Server® 2008 R2 Standard Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® 2003, Standard Edition Microsoft® Windows Server® 2003, Enterprise Edition Microsoft® Windows Server® 2003 R2, Standard Edition Microsoft® Windows Server® 2003 R2, Enterprise Edition Microsoft® Windows Server® 2003, Standard 64-bit Edition Microsoft® Windows Server® 2003, Enterprise 64-bit Edition Microsoft® Windows Server® 2003 R2, Standard 64-bit Edition Microsoft® Windows Server® 2003 R2, Enterprise 64-bit Edition Microsoft® Windows® 2000 Professional operating system Microsoft® Windows® 2000 Server operating system Microsoft® Windows® 2000 Advanced Server operating system Microsoft® Windows® XP Professional Microsoft® Windows® XP Home Edition Windows Vista® Home Basic Windows Vista® Home Premium Windows Vista® Business Windows Vista® Enterprise Windows Vista® Ultimate Windows® 7 Ultimate Windows® 7 Enterprise Windows® 7 Professional Windows® 7 Home Premium Microsoft® Windows® Millennium Edition Microsoft® Windows® 98 Second Edition	Windows

\*) For commands and file saving locations, especially when they are differentially noted under 64 bit edition, the abbreviations are as follows.

- Windows Server® 2008 64-bit Edition
- Windows Server® 2008 R2
- Windows Server® 2003 64-bit Edition
- Windows Server® 2003 R2 64-bit Edition
- Windows® XP 64-bit Edition
- Windows Vista® 64-bit Edition n
- Windows® 7 64-bit Edition

## Specific Operations of Operation System

For specific operations of the operating system (such as LAN connection), this manual takes Windows Server® 2003 as an example for description.

For operations apart from Windows Server® 2003, please refer to the operation methods of the respective operating systems.

## Export Restriction

Our documentation may contain certain technologies subject to regulation by the Foreign Exchange and Foreign Trade Control Law. Export of any documents that contains such technologies and supply of such documents to any nonresident require an appropriate export license under the above law.

## General Restriction

The following functions are recorded in this manual but cannot be used.

(These functions can be used in the Japanese version, but are not available in English and Chinese versions.)

- Prohibition Function
  - Encryption Function in File Export
  - Encryption Function in E-mail Attachment
  - Logon Prohibition Function
  - E-mail Attachment Prohibition Function
  - E-mail Recipient Address Confirmation Function
  - USB Device Individual Identification Function
- Record Function
  - Command Prompt Operation
  - Citrix XenApp Monitoring Function
- Others
  - Notification to Client
  - All-in-one Machine Linkage Report

In addition, for the specification of characters recorded in this manual, please pay attention to the following points:

- For character code, please replace Shift-JIS with local character code (character code that corresponds to the code page on OS).
- Please replace "Japanese" or "Double-byte" with multi-byte character.
- For number of characters that can be used, multi-byte characters such as double-byte in this manual are calculated as 2 bytes, but when actually saving to database, one character may occupy 2~6 bytes, please pay attention.

The following versions do not exist, please ignore relevant record.

Systemwalker Desktop Keeper Base Edition V12.0L10

Systemwalker Desktop Keeper Base Edition V12.0L20

Systemwalker Desktop Keeper Base Edition V13.0.0

Systemwalker Desktop Keeper Base Edition V13.2.0

Systemwalker Desktop Keeper Base Edition V13.3.0

Systemwalker Desktop Keeper Standard Edition V13.2.1

Systemwalker Desktop Keeper Standard Edition V13.3.0

Systemwalker Desktop Keeper V14g (14.0.0)

Systemwalker Desktop Keeper V14g (14.0.1)

Systemwalker Desktop Keeper V14g (14.1.0)

For example, when it is described as “V13.3.0 or later”, since V13.3.0 does not exist, please replace it with “V14.2.0 or later. In addition, when it is described as ”V14.0.0 or earlier”, please replace it with “V13.2.0 or earlier” for the same reason.

## Trademarks

Microsoft, Windows, Windows Vista and Windows Server or other Microsoft product names are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

Citrix, Xen, Citrix XenApp, Citrix XenServer, Citrix XenDesktop and Citrix Presentation Server are trademarks or registered trademarks Citrix Systems, Inc in the United States and other countries.

Vmware is registered trademark or trademark of VMware, Inc. in the United States and other countries.

Other product names are trademarks or registered trademarks of their respective holders.

Screenshots are used according to the guidelines of Microsoft Corporation

March 2012

Revision History
March 2012, First Edition

Copyright 2005 - 2012 FUJITSU LIMITED

# Contents

---

Chapter 1 Before Operation.....	1
1.1 Flow of Operation.....	1
1.2 Notes Relating to Functions .....	2
1.2.1 General Functions .....	2
1.2.2 About Collective Management of User Policy .....	4
1.2.3 About Installation of Client (CT) of Management (Master Management) Server .....	4
1.2.4 About Windows Vista® 64-Bit Edition, Windows® 7 64-Bit Edition, Windows Server® 2008 64-Bit Edition, and Windows Server® 2008 R2 Edition.....	5
1.2.5 Export Utility .....	5
1.2.6 About Automatically Adding Encrypted Files to E-mail Software .....	8
1.2.7 About USB Device Individual Identification Function.....	10
1.2.8 File Export Prohibition .....	10
1.2.9 Printing Prohibition .....	12
1.2.10 Logon prohibition.....	12
1.2.11 Application Startup Prohibition .....	12
1.2.12 URL Access Prohibition .....	13
1.2.13 FTP Server Connection Prohibition .....	13
1.2.14 Web Upload and Download Operation Prohibition .....	13
1.2.15 Clipboard Operation Prohibition.....	14
1.2.16 All Logs .....	15
1.2.17 File Export Log .....	15
1.2.18 Printing Operation Log .....	15
1.2.19 Window Title Obtaining Log .....	17
1.2.20 E-mail Sending Log .....	18
1.2.21 Command Operation Log .....	19
1.2.22 Device Configuration Change Log .....	20
1.2.23 PrintScreen Key Operation Log .....	20
1.2.24 Web Operation Log .....	20
1.2.25 FTP Operation Log .....	21
1.2.26 Clipboard Operation Log.....	21
1.2.27 File Operation Log .....	22
1.2.28 Logon/Logoff Log .....	25
1.2.29 Screen Capture .....	25
1.2.30 About Collection of Logs for Investigation of Client (CT) .....	25
1.2.31 About File Trace Function of Log Viewer .....	25
1.2.32 About Viewing Operation Logs of the Remote Connection Source and Target in Log Viewer.....	26
Chapter 2 Prepare Operating Environment.....	27
2.1 Considerations for Preparing Operating Environment.....	27
2.1.1 What is Policy.....	27
2.1.2 How to Apply Policy.....	38
2.2 Flow of Preparing Operating Environment.....	46
2.3 Start Management Console.....	49
2.4 Set Initial Value of Policy.....	60
2.4.1 Perform Terminal Initial Settings.....	60
2.4.1.1 Settings of [Log Switches] Tab.....	61
2.4.1.2 Settings of [File Export Prohibition] Tab.....	64
2.4.1.3 Settings of [Printing Prohibition] Tab.....	75
2.4.1.4 Settings of [Logon Prohibition] Tab.....	77
2.4.1.5 Settings of [Application Startup prohibition] Tab.....	79
2.4.1.6 Settings of [File operational process] Tab.....	81
2.4.1.7 Settings of [File operation extension] Tab.....	85
2.4.1.8 Settings of [E-mail Sending] Tab.....	87
2.4.1.9 Settings of [Log Filtering Condition] Tab.....	90
2.4.1.10 Settings of [Screen Capture Condition] Tab.....	92

2.4.1.11 Settings of [Eco monitoring settings] Tab.....	94
2.4.1.12 Settings of [Virtual Environment setup] Tab.....	95
2.4.1.13 Settings of [URL Access Prohibition] Tab.....	96
2.4.1.14 Settings of [FTP Server Connection Prohibition] Tab.....	98
2.4.1.15 Settings of [Web Upload and Download Prohibition] Tab.....	99
2.4.1.16 Settings of [Other Settings] Tab.....	100
2.4.2 Perform Terminal Operation Settings.....	102
2.5 Create Configuration Information Tree.....	108
2.5.1 Import Information from Active Directory.....	108
2.5.2 Import Information from Systemwalker Desktop Patrol.....	114
2.5.3 Create through Management Console.....	124
2.6 Allocate Department Administrator.....	131
2.6.1 Export Department Administrator Information through Management Console.....	139
2.7 Preparations for Log Aggregation.....	141
2.7.1 Prepare for Using Status Window.....	141
2.7.2 Prepare for Using Log Analyzer.....	150
2.7.2.1 Schedule Log Transmission.....	150
2.7.2.1.1 Set Log Obtaining Period on Management Server.....	150
2.7.2.1.2 Set Transmission Schedule on Management Server.....	152
2.7.2.1.3 Save Logs to the Database of Log Analyzer Server.....	163
2.7.2.2 Set Conditions for Aggregation /Report Output.....	175
2.7.2.2.1 Set Ranking Display Number.....	178
2.7.2.2.2 Set Screening Condition.....	179
2.7.2.2.3 Set Items Excluded From Aggregation Target.....	182
2.7.2.2.4 Set Other Conditions.....	184
2.7.2.2.5 Select Log Analyzer Server.....	187
<b>Chapter 3 Set Policy in Management Console.....</b>	<b>189</b>
3.1 Search CT Information/User Information.....	189
3.2 Modify Group Policy.....	196
3.2.1 Modify CT Group Policy.....	196
3.2.2 Modify User Group Policy.....	202
3.3 Allocate CT/User to Group.....	207
3.3.1 Add/Move/Delete CT.....	208
3.3.2 Register a User.....	210
3.3.3 Update/Move/Delete User.....	214
3.4 Modify CT Policy/User Policy.....	216
3.4.1 Modify CT Policy.....	216
3.4.2 Modify User Policy.....	222
3.5 Export CT information/User information.....	224
3.6 Control Client (CT).....	229
3.6.1 Control Services of Client (CT).....	230
3.6.2 Control the Processes of Client (CT).....	233
<b>Chapter 4 Check Trend of Client (CT) Operation.....</b>	<b>238</b>
4.1 Check the Trend in Status Window.....	239
4.1.1 Display Status Window.....	239
4.1.2 Confirm Result of Log Aggregation.....	242
4.2 Check the Trend in Log Analyzer.....	246
4.2.1 Start Log Analyzer.....	247
4.2.2 Diagnose Risk of Information Disclosure.....	251
4.2.2.1 Display the Result of aggregation by Operation.....	252
4.2.2.2 Display the Worst Ranking of Violations.....	256
4.2.2.3 Specify a Past Date to Display Aggregation Result.....	256
4.2.3 Aggregate by Objectives.....	256
<b>Chapter 5 Audit Operations on Client (CT) via Log Viewer.....</b>	<b>263</b>
5.1 Start Log Viewer.....	263

5.2 View Logs.....	275
5.2.1 View Logs in [CT Operation Log] Window .....	279
5.2.2 View in [Configuration Change Log] .....	294
5.3 Trace File Operation .....	299
5.4 Search CT Information in Log Viewer .....	308
<b>Chapter 6 Create Auditing Material.....</b>	<b>312</b>
6.1 How to Make Flexible Use of Report Output Tool.....	312
6.2 Start Report Output Tool.....	314
6.3 Information Disclosure Analysis Report.....	315
6.3.1 Output Information Disclosure Analysis Report.....	316
6.3.2 Content of Information Disclosure Analysis Report.....	321
6.4 Terminal Usage Analysis Report.....	327
6.4.1 Output Terminal Usage Analysis Report.....	328
6.4.2 Content of Terminal Usage Analysis Report.....	331
6.5 Violation Analysis Report.....	331
6.5.1 Output Violation Analysis Report.....	332
6.5.2 Contents of Analysis Report of Violation Operation.....	336
6.6 Comprehensive Analysis Report.....	336
6.6.1 Output Comprehensive Analysis Report.....	337
6.6.2 Content of Comprehensive Analysis Report.....	340
6.7 Printing Volume Auditing Report.....	343
6.7.1 Output Printing Volume Auditing Report.....	344
6.7.2 Content of Printing Volume Auditing Report.....	347
6.8 Set Report Output Schedule.....	356
<b>Chapter 7 Change Operating Environment.....</b>	<b>362</b>
7.1 Change Import Method of Configuration Information.....	362
7.2 Change Management Method of User Information.....	364
7.3 Change System Structure from 2-level to 3-level.....	366
7.4 Add/Delete Management Server in 3-level System Structure.....	372
7.5 Export Files to Specified USB Device Only.....	377
7.6 Modify Period to Save Logs.....	395
7.7 Change CT Environment.....	396
7.7.1 Change Management Server/Master Management Server To Be Connected.....	396
7.7.2 Change Operation Settings of Client (CT).....	401
7.7.3 Replace Client (CT).....	406
7.8 Change Management Console Environment.....	407
7.9 Change Management Server Environment.....	409
7.9.1 Start Server Settings Tool.....	409
7.9.2 Change Password of Initial Administrator.....	412
7.9.3 Modify Administrator Notification.....	412
7.9.4 Change System Environment with the Change of IP Address/Computer Name of Management Server/Master Management Server.....	413
7.9.5 Modify Communication Information of Management Server.....	437
7.9.6 Change Saving Target Folder.....	439
7.9.7 Transfer Management Server/Master Management Server.....	439
7.9.8 Transfer Log Analyzer Settings with Transfer of Management Server/Master Management Server.....	441
7.10 Reconstruct Database of Management Server.....	442
7.11 Create Log Viewing Database.....	451
7.12 Change Log Analyzer Server Environment.....	451
7.12.1 Transfer Log Analyzer Server.....	451
7.12.2 Modify IP Address/Port Number of Log Analyzer Server.....	452
<b>Chapter 8 Policies That Can be Set.....</b>	<b>454</b>
8.1 Set the Policies of Prohibition Function.....	454
8.1.1 File Export Prohibition.....	454
8.1.2 File Reading Prohibition.....	457

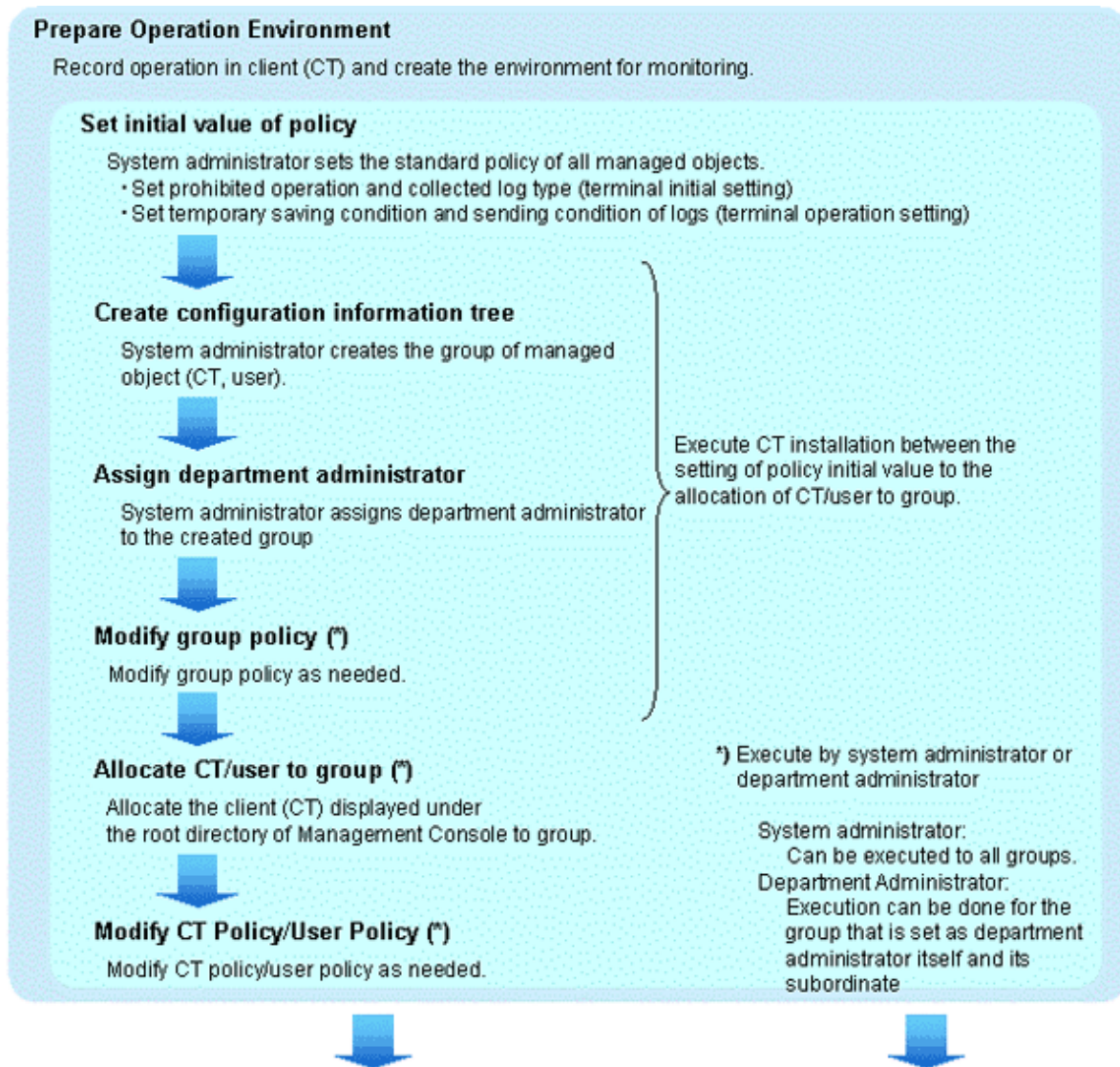
8.1.3 Printing Prohibition.....	458
8.1.4 Logon Prohibition.....	460
8.1.5 Application Startup Prohibition.....	462
8.1.6 E-mail Attachment Prohibition.....	464
8.1.7 PrintScreen Key Prohibition.....	466
8.1.8 URL Access Prohibition.....	468
8.1.9 FTP Server Connection Prohibition.....	470
8.1.10 Web Upload and Download Prohibition.....	472
8.1.11 Clipboard Operation Prohibition.....	474
8.2 Policy Settings of Record Function.....	475
8.2.1 Application Startup Log.....	479
8.2.2 Application Termination Log.....	480
8.2.3 Application Startup Prohibition Log.....	481
8.2.4 Window Title Obtaining Log.....	482
8.2.5 E-mail Sending Log.....	484
8.2.6 E-mail Sending Suspension Log.....	485
8.2.7 Device Configuration Change Log.....	486
8.2.8 Printing Operation Log.....	489
8.2.9 Printing Prohibition Log.....	490
8.2.10 Logon Prohibition Log.....	490
8.2.11 File Export Log.....	491
8.2.12 PrintScreen Key Operation Log.....	494
8.2.13 PrintScreen Key Prohibition Log.....	494
8.2.14 Web Operation Log.....	495
8.2.15 Web Operation Prohibition Log.....	496
8.2.16 FTP Operation Log.....	498
8.2.17 FTP Operation Prohibition Log.....	499
8.2.18 Clipboard Operation Log.....	500
8.2.19 Clipboard Operation Prohibition Log.....	502
8.2.20 File Operation Log.....	503
8.2.21 Logon/Logoff Log.....	507
8.2.22 Linkage Application Log.....	512
8.2.23 Configuration Change Log.....	513
Appendix A List of Aggregation Objectives .....	515
Appendix B Appendix B Visualize Information through Linking with All-in-one PC/Printer.....	519
B.1 Design.....	519
B.1.1 Application pattern.....	519
B.1.2 Determine user information of all-in-one PC/printer.....	520
B.1.3 Aggregation mechanism for usage status of each all-in-one PC/printer.....	520
B.1.4 Aggregation mechanism for usage status of all-in-one PC/printer of each user.....	520
B.1.5 Determine the method for relating printing information with Systemwalker Desktop Keeper information .....	521
B.2 Operating Environment .....	521
B.3 Restrictions and Considerations.....	522
B.4 Installation .....	522
B.4.1 Confirm the log analyzer server has been constructed.....	522
B.4.2 Confirm the environment of report output tool has been constructed.....	523
B.4.3 Construct the environment of all-in-one/printer management server.....	523
B.4.4 Register log analyzer server information on the management server of 3-level system .....	523
B.4.5 Set import time.....	523
B.4.6 Relate printing information with Systemwalker Desktop Keeper information.....	524
B.4.7 Set user details (name and target).....	525
Index.....	526

# Chapter 1 Before Operation

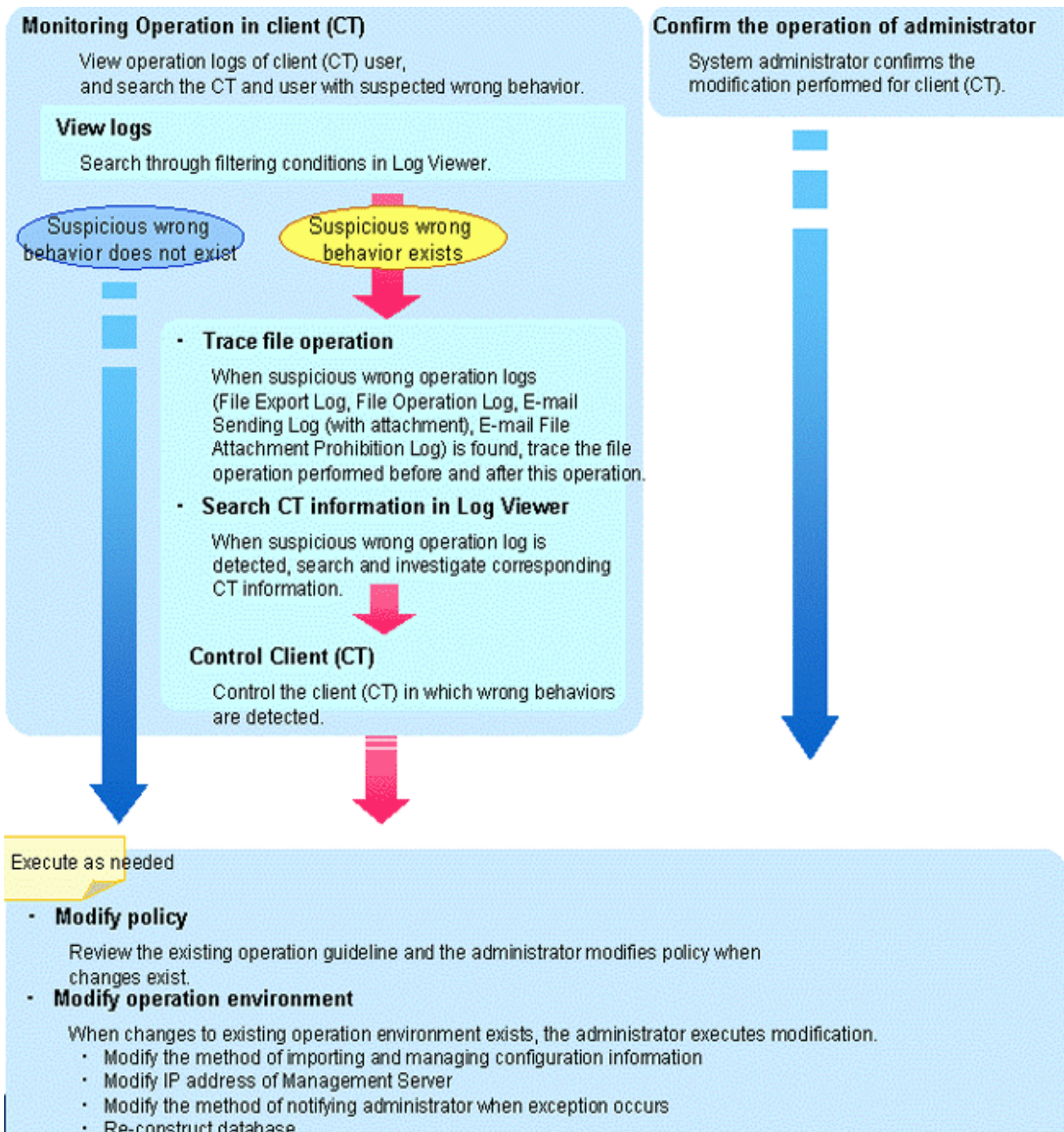
This chapter outlines the operations for system administrators, department administrators and client users according to the operation flow of Systemwalker Desktop Keeper.

## 1.1 Flow of Operation

The entire operation flow is shown below.







## 1.2 Notes Relating to Functions

### 1.2.1 General Functions

- For a built-in disk identified as a removable drive by the OS, logs will be collected and prohibition will be performed by considering the disk as a removable drive instead of a local drive.
- When multiple logon is enabled on a Windows Server® 2008, the E-mail recipient confirmation window or the E-mail attachment prohibition window will not be displayed during the E-mail sending. The Systemwalker Desktop Keeper performs the following operations during the E-mail sending:
  - For the E-mail of which the recipient address is only the address of an exclusion domain, the information will not be displayed while the E-mail is sent, so there is no change.

- For E-mails of which the recipient address contains addresses apart from the exclusion domain, execute judgment for the E-mail attachment prohibition. Perform the following operations according to the judgment result of the E-mail attachment prohibition:
  - When the prohibited file has been added, the E-mail sending will be terminated without showing the E-mail attachment prohibition window.
  - When the prohibited file is not added, the E-mail will be sent without showing the recipient prohibition window.
- The policy status when multiple users are logged on at the same time is shown in the table below.

Function		Valid Policy
Log (recording function)	Application startup/ termination	Operate according to user policy.
	Window title obtaining log	Operate according to user policy.
	E-mail sending	Operate according to CT policy.
	E-mail sending interruption	Operate according to CT policy.
	Command operation	Operate according to user policy.
	Device configuration change	Operate according to user policy.
	Printing operation	Operate according to user policy.
	File export	Operate according to user policy.
	PrintScreen key operation	Operate according to user policy.
	Web operation	Operate according to user policy.
	FTP operation	Operate according to user policy.
	File operation	Operate according to CT policy.
	Logon/Logoff	Operate according to CT policy.
	Clipboard operation	Operate according to user policy.
	External application	Operate according to user policy.
Prohibition function	Application startup prohibition	Operate according to user policy.
	Printing prohibition	Operate according to user policy.
	PrintScreen key prohibition	Operate according to user policy.
	Logon prohibition	Operate according to CT policy.
	E-mail attachment prohibition	Operate according to CT policy.
	File export prohibition	Operate according to CT policy.
	File reading prohibition	Operate according to CT policy.
	URL access prohibition	Operate according to user policy.
	FTP server connection prohibition	Operate according to user policy.
	Web upload and download operation prohibition	Operate according to user policy.
	Clipboard operation prohibition	Operate according to user policy.

When the OS of the client (CT) is Windows Vista®, Windows Server® 2008, or Windows® 7 OS, and the command prompt and file export utility are run by an administrator user, the message “Requested resource is in use” will be output sometimes and the application cannot be started. In this case, wait a moment and restart the application.

- When using the Web console, please do not click the [Back] button on the browser. If this button is used, errors may occur and it may not display properly.
- Please do not allow multiple users to log on the Windows OS at the same time using the same user ID. Otherwise, the logs cannot be differentiated.

## About character code that can be processed in Systemwalker Desktop Keeper

There are following two types of character code that can be processed in Systemwalker Desktop Keeper. Other character code will be converted to "?".

- Local Character Code

It will be displayed correctly.

- UNICODE

It may be able to be displayed correctly or converted to "?".

## 1.2.2 About Collective Management of User Policy

---


When communication between the master management server and management server is disabled due to network problems, even if the Management console is connected to the management server and various settings have been performed, once the communication between the master management server and management server is recovered the settings in the management server will be overwritten by the settings in the master management server.

The management users of the collective management console are also managed collectively by the master management server.

## 1.2.3 About Installation of Client (CT) of Management (Master Management) Server

---

- In the export prohibition setting, even if export prohibition policy has been set for the hard disk of [Fixed] drive type, export still cannot be prohibited. This can prevent the wrong setting of export prohibition for the fixed hard disk of the management (master management) server, which may cause abnormal operation of the management (master management) server.
- The setting for Logon prohibition is invalid. This can prevent the wrong setting of Logon prohibition for the management (master management) server, which may cause abnormal operation of the management (master management) server.
- When the client (CT) is installed on the management (master management) server, the MAC address, IP address, and subnet mask of the client (CT) will be displayed as 00-00-00-00-00-00, IP address is 127.0.0.1, and 255.0.0.0 in the Management Console.

Name	Computer name	MAC address	IP address	Subnet mask
 FNST123-1PVJ811	FNST	00-00-00-00-00-00	127.0.0.1	255.0.0.0

- Though the following messages will be displayed during the input of maintenance command, it is not an exception
  - "NBT Remote Cache Name Table has been deleted normally and accessed in advanced"
  - "Successful purge and preload of the NBT Remote Cache Name Table."

## 1.2.4 About Windows Vista® 64-Bit Edition, Windows® 7 64-Bit Edition, Windows Server® 2008 64-Bit Edition, and Windows Server® 2008 R2 Edition

- In the [Get/Control Process List] function of the Management Console, when the client (CT) is Windows Vista® 64-bit edition, Windows® 7 64-bit edition, Windows Server® 2008 64-bit edition, or Windows Server® 2008 R2 edition, the process list of 64-bit application cannot be viewed. Also, the processes cannot be terminated.

## 1.2.5 Export Utility

Encryption Function is not available.

### About File Export

- When exporting files by using the file export utility, ensure that the drive (the system disk) storing the system temporary files must have the available capacity described in the following table.

Export Destination Drive		When original file is not original file backup		When backing up original file (Note 1)	
		During normal (plain text) Export	During encrypted export	During normal (plain text) Export	During encrypted export
DVD/CD		More than 1.5 times of the capacity of files that are actually exported	More than 3 times of the capacity of files that are actually exported	More than 2.5 times of the capacity of files that are actually exported	More than 4 times of the capacity of files that are actually exported
Except DVD/CD	When it is not system drive (Note 2)	Not required	More than 1.5 times of the capacity of files that are actually exported	Same capacity as that of files that are actually exported	More than 2.5 times of the capacity of files that are actually exported
	When it is system drive	Same capacity as that of files that are actually exported	More than 2.5 times of the capacity of files that are actually exported	More than 2 times of the capacity of files that are actually exported	More than 3.5 times of the capacity of files that are actually exported

Note 1: When backing up the original file, the log folder of the client (CT) must have the capacity that is equivalent to the size of the original file in addition to the capacity described in the above table.

Note 2: Specify the drive that satisfies all the following conditions:

- Except DVD/CD drive
- Except Windows system drive (usually the C drive)
- When exporting files using the export utility, the available capacity of the startup drive is recommended to be larger than 1 GB in normal (plain text) export mode and larger than 2 GB in encrypted export mode.
- When encrypted export is performed for empty folder using the export utility, the empty folder will not be decrypted during decryption.
- When exporting a write-protected folder in the OS later than Windows Vista® using the export utility, it is actually configured to “%LOCALAPPDATA%\VirtualStore” instead of writing to the folder.

Example: C:\Users\*user name*\AppData\Local\VirtualStore

When the writing into OS is restricted because the security policy “User Account Control: Virtualize the error of writing of file and registry to each user location” is “Enabled”, the following folders will be restricted:

- %ProgramFiles%  
Example: C:\Program Files
- %Windir%  
Example: C:\Windows
- %Windir%  
Example: C:\Windows

#### About File Export to CD-R/RW or DVD-R/RW Media

- If a user logs on with a user name that contains UNICODE specific characters (characters that cannot be converted to local character code), encrypted export to CD or DVD media cannot be performed.
- The OS that allows the use of the export utility for exporting files to CD-R/RW or DVD-R/RW is shown as follows. However, it is limited to the OS that support the CD-R/RW or DVD-R/RW drive being used.

##### **[Export Files to CD-R/RW]**

- Windows® 7 Ultimate
- Windows® 7 Enterprise
- Windows® 7 Professional
- Windows® 7 Home Premium
- Microsoft® Windows® XP Professional (Service Pack 2 or later)
- Microsoft® Windows® XP Home Edition (Service Pack 2 or later)
- Windows Vista® Home Basic
- Windows Vista® Home Premium
- Windows Vista® Business
- Windows Vista® Enterprise
- Windows Vista® Ultimate

In case of the safe mode started under Windows® XP, files cannot be exported to CD media and files in CD media cannot be erased.

##### **[Export Files to DVD-R/RW]**

- Windows® 7 Ultimate
  - Windows® 7 Enterprise
  - Windows® 7 Professional
  - Windows® 7 Home Premium
  - Windows Vista® Home Basic
  - Windows Vista® Home Premium
  - Windows Vista® Business
  - Windows Vista® Enterprise
  - Windows Vista® Ultimate
- Before the function of exporting files to CD-R/RW or DVD-R/RW media is used, use a PC and a CD-R/RW or DVD-R/RW drive, as well as media to verify the ability to do so.

- If burning software or packet-writing software is installed, the DVD/CD writing function of the export utility may fail to run normally. When exporting files to CD-R/RW or DVD-R/RW using the export utility, please uninstall the burning software and packet-writing software.
- Since the power saving function is not supported when writing data to a DVD/CD using the export utility, please ensure the power is always on. When the system is on standby, sleeping or suspended status, problems such as failure when using media may occur. In addition, under suspension status, the message of completed writing will be displayed, but in fact, the writing to the media may not complete normally.
- When a DVD/CD device connects to the PC for the first time, if files need to be exported to CD-R/RW or DVD-R/RW media through this DVD/CD device, the system must be restarted. Otherwise, the function of writing into CD-R/RW or DVD-R/RW media may not run properly.
- When burning a new CD using the export utility, the stream-writing mode (the session-at-once function in CDFS (Joliet mode)) can be used.

**[Written Files]**

- File name: Maximum 64 characters (1 character for both SBC and DBC) (including extension).
- Directory name: Maximum 64 character (1 character for both SBC and DBC) (including extension).
- Full path length: Maximum 240 bytes (the delimiter of folder is counted as 1 byte, and one character of a file/folder name is counted as two bytes. One character of drive letter is counted as two bytes (Example: **C:** is counted as four bytes)).
- The DVD/CD export function of the export utility regards only the empty media that does not record any information including volume labels as the target.

**[Definition of Empty Media]**

- CD-R, CD-RW, DVD-R, or DVD-RW media that is not formatted after purchase.
- CD-RW or DVD-RW media in which CD-RW/DVD-RW erasing has not been performed using the export utility
- Files cannot be exported to the following media.
  - When disks are formatted to UDF format for packet writing (including the case without files in it)
  - When disks are formatted to CDFS format for stream writing (including the case without files in it)
- The drive types, connection methods, and media types supported by the DVD/CD export function of the export utility are as follows.
  - Drive connection methods  
ATAPI, USB 1.1/2.0, and IEEE1394
  - Media types  
CD-R/RW (Maximum 700 MB is supported) and DVD-R/RW (Maximum 4.7 GB is supported)

The following table shows whether each type of media supports the export utility and export prohibition function.

Operation/Function of the File Export Utility		CD-R	CD-RW	DVD-R	DVD-RW	DVD-R DL (Note 1)	DVD+R	DVD+RW	DVD+R DL (Note 2)	DVD+RAM (Note 3)
Write	<b>Windows® XP (Note 4)</b>	○	○	×	×	×	×	×	×	×
	<b>Windows Vista®</b>	○	○	○	○	×	×	×	×	×
	<b>Windows® 7</b>	○	○	○	○	×	×	×	×	×
Erase	<b>Windows® XP (Note 4)</b>	×	○	×	×	×	×	×	×	×
	<b>Windows Vista®</b>	×	○	×	○	×	×	×	×	×
	<b>Windows® 7</b>	×	○	×	○	×	×	×	×	×
<b>Export prohibition</b>		○	○	○	○	○	○	○	○	○

○: Supported

×: Not supported

Note 1: It refers to DVD-R Dual Layer

Note 2: It refers to DVD+R Dual Layer

Note 3: Except when it is identified as a removable disk

Note 4: Windows® XP 64-bit edition is not supported

- Blu-ray and HD DVD are not supported.
- Under Windows® XP, in order to use the CD export function, the IMAPI service (IMAP CD-Burning COM Service) must be installed in the system and the status of server cannot be "Disabled".
- A volume label can be specified for the media when writing files. Letters from A to Z, numbers from 0 to 9, and underscores (\_) can be used in the volume label, and a maximum 16 characters can be specified.
- The CD export function of the export utility is not closed (but it will be closed in the case of DVD-R). The Windows explorer or burning software can be used to add data to the PC without DVD/CD writing prohibition. However, since the file export utility supports only the writing to empty media, data cannot be added. In addition, since it is in unclosed status, the unit that only processes the closed media cannot be accessed.
- When the total size of source files to be exported is larger than the media capacity of export destination, the DVD/CD export function of the export utility cannot perform writing (multi-volume writing is not supported).
- The size of the data that can be written varies with the writing media, number of files and structure of folder.
- When multiple files are being written, the file size that can be written may not reach to the maximum capacity that is allowed to be written because information such as folder structure and file name must be saved.
- When performing DVD/CD export through the export utility, work files should be written to the temporary directory of user. Therefore, please do not change the temporary directory from the startup drive to another drive.
- When the burning software is used to write files, media errors may occur if policies have been changed (writing to DVD/CD is not allowed).
- The erase mode includes quick erase and complete erase. In quick erase mode, only the PMA (Program Memory Area) and TOC (Table of Contents) will be erased. In complete erase mode, all areas will be erased.
- The file operation logs cannot be obtained from the export utility.
- For some burning software, during writing prohibition, the burning may appear to have finished normally (but data are not really written into the media).
- During the installation of the client (CT), if the OS is Windows® XP and the startup mode of IMAPI service (IMAPI CD-Burning COM Service) is not [Disabled], the installation program will automatically change it to [Manual] (but the setting of IMAPI service (IMAPI CD-Burning COM Service) will not be changed during when the client (CT) is uninstalled.
- When performing DVD/CD writing by using the DVD/CD export function of the export utility, please use the DVD/CD drive and media that are supported by the PC in use.
- When exporting large number of files using the export utility, it takes certain amount of time to output the export logs (Normally, it requires 10 minutes when exporting 10,000 files).
- The writing speed is the lower speed supported by the drive unit and media.
- Fingerprints, dirt, dust, or scratches on the recording surface of the CD-R/RW media may result in abnormal data writing or erasing.
- The media that can be closed during the burning process will be displayed as CD-ROM when the media type is a CD, and it will be displayed as DVD-ROM in the case of a DVD.
- In the case of the media that cannot be erased and have been written, the disk total capacity displayed on the media erase window will be incorrect.

## **1.2.6 About Automatically Adding Encrypted Files to E-mail Software**

---

**This function is not available.**

- This function automates the operation of “Create self-decrypting files using export utility and attach to E-mail”. The format of the encrypted file that is added automatically is the same as the format of the self-decrypting file created by the export utility.
- The notes for creating and decrypting encrypted files are the same as those for encrypted files of the “Export Utility”.
- Encrypted files are located in the folder generated at each encryption process under the temporary folder of a logon user. Since the folder generated during the encryption process is managed separately, even if encrypted files with same name exist, they will not be overwritten.

C:\Documents and Settings\\Local Settings (or\AppData\Local)\Temp\fs01ej8\

- If the environment variables TMP, TEMP, and USERPROFILE do not exist or the folders specified by TMP, TEMP, and USERPROFILE are system folders, this function cannot be used.
- The encrypted files will be deleted when the logon user logs on again. Therefore, E-mails should be sent during the logon period after encryption.
- This function requires that the E-mail software must support the MAPI (Messaging Application Program Interface).
- The E-mail software that automatically adds encrypted files is the standard E-mail software. This function cannot be used in the PC without setting of standard E-mail software.
- The OS that can automatically add encrypted files are shown as follows.  
Windows Vista® 64-bit edition, Windows Server® 2008 64-bit edition, Windows Server® 2008 R2 edition, Windows® 7 64-bit edition, and compatibility mode of 32-bit editions
  - Microsoft® Windows® XP Professional (Service Pack 2 or later)
  - Microsoft® Windows® XP Home Edition (Service Pack 2 or later)
  - Microsoft® Windows Server® 2003, Standard Edition
  - Microsoft® Windows Server® 2003 R2, Standard Edition
  - Microsoft® Windows Server® 2003, Enterprise Edition
  - Microsoft® Windows Server® 2003 R2, Enterprise Edition
  - Windows Vista® Home Basic
  - Windows Vista® Home Premium
  - Windows Vista® Business
  - Windows Vista® Enterprise
  - Windows Vista® Ultimate
  - Windows® 7 Ultimate
  - Windows® 7 Enterprise
  - Windows® 7 Professional
  - Windows® 7 Home Premium
  - Microsoft® Windows Server® 2008 Standard
  - Microsoft® Windows Server® 2008 Enterprise
  - Microsoft® Windows Server® 2008 Standard without Hyper-V (TM)
  - Microsoft® Windows Server® 2008 Enterprise without Hyper-V (TM)
  - Microsoft® Windows Server® 2008 R2 Standard
  - Microsoft® Windows Server® 2008 R2 Enterprise



## 1.2.7 About USB Device Individual Identification Function

---

**This function is not available.**

- Before using the USB device individual identification function, perform an execution test using a USB device that has been used before.
- When using the USB device individual identification function, the built-in floppy disk drive connected by USB must be registered as well. In addition, the floppy disk drive that is not connected by USB cannot be identified and thus cannot be registered.
- If reading prohibition and export prohibition functions are not configured in the [File Export Prohibition] tab, the USB device individual identification function for Explorer will not be run.

Specifically, even if [Read only], [Read and Write by file export utility only] or [Write by file export utility only] has been set in [Access settings] of the USB device registered in [List of available USB devices] in the [File export prohibition-Individual USB device identification function-Detailed setting] window, reading and exporting through Explorer cannot be prohibited. The file export utility will run according to the settings.

- When the individual identification function is used for a USB device with the lock function, please register by using the information of the USB device in the unlocked state.
- Please selected multiple USB devices with same [Device name] and [Internal serial number] but different [Identification methods] in the [File export prohibition-Detailed setting of individual USB device identification function-Select USB device] window of the Management Console. The USB device identification function may run abnormally.

## 1.2.8 File Export Prohibition

---

### Common Notes for All Media Types

- When the log saving folder that is set during the installation of the client (CT) is not in the C drive, please do not set export prohibition for the drive where the folder for the saving logs is located.
- The target device of export prohibition can be a fixed hard disk, floppy disk, MO, memory storage, DVD/CD, removable hard disk (connecting through USB, IEEE1394, or PCMCIA), network folders, or devices identified as removable drives by the OS.
- The target facilities of the reading prohibition can be floppy disks, MO, flash memories, DVDs/CDs, removable hard disks (connected through USB, IEEE1394, or PCMCIA), network folder, or device identified as removable drive by the OS.
- The drive for which the export prohibition has been set is read only.
- When a folder is copied from a drive under export prohibition, only the folder will be copied but the files in the folder will not be copied.
- A drive under export prohibition cannot be formatted through Explorer (but can be formatted using export utility).
- When the file on is shared on a network and the folder is accessed through UNC path, the network access prohibition will be effective and the access will be disabled.
- Though network access prohibition can be set in the [File Export Prohibition] tab of Management Console, the drive letter of the drive under writing prohibition cannot be set. Therefore, when setting the writing prohibition function, please make sure to select the [Network] in the drive type.
- If a folder is set to be an excluded folder and its upper-level folder is allocated as a network drive, access to the excluded folder may be disabled or files cannot be copied from or created in the excluded folder, even though this excluded folder can be displayed under the network drive. In this case, please access the excluded folder through the UNC path.
- A maximum of 50 excluded folders or 500-byte full paths of excluded folders can be registered. However, after a large number of excluded folders have been registered, terminal performance will be reduced. Therefore, it is recommended to reduce the number of registered excluded folders if possible.
- In the structure of shared folders as follows, the shared folder B will not be excluded when the shared folder A is set as an excluded folder.  
Example: If a shared folder exists under the shared folder A.  
When excluding the shared folder B, please set both shared folder A and B to excluded folders.

- If export prohibition is enabled for the drive of the recycle bin, files cannot be deleted to the recycle bin. In this case, please disable the export prohibition for the drive or press Shift+Delete to permanently delete files.

Example: the recycle bin is in D drive and is under export prohibition.

- When the PEINT command in the Command Prompt window is used to print via the network printer, access prohibition may occur. In this case, print after registering the network printer to an excluded folder.

Example of specifying an excluded folder: \\192.168.1.1\printer01

## Notes on DVD/CD/BD Media Types

- Since this product has the driver that is similar to that of burning software installed on the client (CT), when other burning software or packet writing software are installed at the same time, they may run abnormally. If these burning software or packet writing software are used frequently, it is recommended to verify whether the software can run normally in advance.
- Sometimes, export prohibition may fail due to the burning software.
  - For the burning software (Example: Drag'on Drop) that writes to the drive of direct path (IDE/USB) Please perform startup prohibition for the burning software by registering the program name of the burning software in the application startup prohibition.  
(Example: Specify to DragDrop in the case of Drag'on Drop)
- The drive types, connection methods, media types, and burning software that support CD/DVD export prohibition are as follows:
  - Drive connection methods
    - ATAPI
    - USB 1.1/2.0
    - IEEE1394
  - Media
    - CD-R/RW
    - DVD-R/RW
    - DVD-R Dual Layer
    - DVD+R/RW
    - DVD+R Dual Layer
    - DVD-RAM (unless it is identified as a removable disk)
    - BD-R
    - BD-RE
  - Burning software
    - B's Recorder GOLD 9
    - Win CDR 9
    - Record Now! Version 7
    - Easy Media Creator 8
    - Nero 7
    - Burning a CD by using the explorer
- DVD-RAM media is likely to be identified as a removable disk by the OS. At this time, it must be prohibited as a removable disk.
- HD DVD is not supported. (When writing to an HD-DVD drive under writing prohibition, the written media may be damaged.)
- Set [Access to CD-ROM is restricted to local logon user only] of Windows security policy to [Disable]. If [Access to CD-ROM is restricted to local logon user only] is set to [Enable], Systemwalker Desktop Keeper will not be able to control the DVD/CD drive. Therefore, even if export prohibition has been set for DVD/CD, burning software can be used for writing.
- During DVD/CD/BD writing or reading prohibition, the information of media device cannot be obtained with other software.
- During DVD/CD/BD writing or reading prohibition, files in the media cannot be deleted.
- During DVD/CD/BD writing or reading prohibition, the DVD/CD/BD media cannot be ejected. In this case, please eject again after canceling the DVD/CD/BD writing or reading prohibition.

- During DVD/CD/BD writing or reading prohibition, the DVD/CD/BD device cannot be deleted. In this case, please delete again after canceling DVD/CD/BD writing or reading prohibition.

## **About Export to a USB Device with Locking Function**

If export prohibition and reading prohibition have been set for a USB device with locking function, locking, unlocking, or ejection of the USB device may fail. In this case, please lock, unlock, or eject again.

In addition, when reading prohibition has been set, since the following USB device with locking function cannot be unlocked, it cannot be used as well (neither can it be used through the export utility).

- It is identified as two removable drives: one allows read-only access and the other is the device ejected before authentication (※).

## **1.2.9 Printing Prohibition**

---

- The Systemwalker Desktop Keeper monitors the running processes. After the Windows API "StartDocA()" and "StartDocW()" have been released, functions cannot be replaced and printing is disabled. Printing prohibition cannot be performed for products that cannot be monitored through workbooks or do not use "StartDocA()" or "StartDocW()".
- When printing prohibition policy has been set, the [Print] on the right-click menu of the explorer is disabled. In this case, please use an application to perform printing.
- Printing prohibition cannot be implemented under the following conditions:
  - Printing that uses ActiveX or COM interface.
  - Similar to label printer, data is output directly from the printing drive to the COM or printer port (printing is not performed through Windows APIs or spooling).
  - The Windows printing protocol is not used (For example, part of free software).
- When Microsoft® Word is under printing prohibition, two same logs will be collected at one printing operation.
- When UAC (user account control) of Windows Vista®, Windows Server® 2008, or Windows® 7 is disabled, printing prohibition cannot be performed. The [Print] on the right-click menu of the Explorer is grayed out.
- The prohibition operation will take effect about one minute after the number of printed pages reaches to the preset value of printing prohibition. At this time, printing can still be performed by bypassing the setting.

## **1.2.10 Logon prohibition**

---

**This function is not available.**

- When the user of logon prohibition that specifies shutdown has logged on, if other logon users exist, they will log out without shutdown. It will also be recorded as a logout in the Logon prohibition log.

## **1.2.11 Application Startup Prohibition**

---

- Application startup prohibition can be performed under the following condition:
  - With Windows Application interface
- To prohibit command prompt on a client (CT), the following applications must be registered:
  - cmd.exe
  - fsw41ej1.exe

## 1.2.12 URL Access Prohibition

---

- This function cannot be run in a Web browser that is not Internet Explorer®.
- This function must be run in Windows® Internet Explorer® 7 or higher.
- Running the prohibition function will activate the Internet Explorer® window.
- Even if the prohibited URL is accessed, the web page during access will not be captured.
- When the URL access prohibition policy is applied, in the case of access to a prohibited URL, Internet Explorer will be forced to close.
- If there is only one Web page tab, in the case of access to a prohibited URL, Internet Explorer® will be forced to close. If there are multiple Web page tabs, only the tab that accesses to the prohibited URL will be forced to close.
- This function will not be performed when a prohibited site is contained in the frame of Web page being displayed.
- If the prohibited site is accessed while collecting Window title obtaining log, the URL will not be recorded in the Remarks column of the Window title obtaining log.

## 1.2.13 FTP Server Connection Prohibition

---

- FTP.EXE connections cannot be prohibited in the 64-bit OS.
- When prohibiting the FTP connection that uses Internet Explorer®, please execute the URL access prohibition function.
- Only the FTP communication when the communication port to which the FTP client is connected is set to “21” can be prohibited.
- When the FTP client is started through the Command Prompt window, this function can only prohibit Windows FTP.EXE.
- This function will not prohibit the secure FTP (FTP protocols for encrypted communication such as FTPS or SFTP).
- When FTP server connection prohibition policy is applied, if the FTP server has been connected, server connection will be cut off forcibly.
- Under the following conditions, FTP server prohibition function will be run when operations are continued after the secure content has been displayed, when moving between folders and file transfer have been started and when connecting FTP server.
  - When the FTP folder browser is effective and FTP connection prohibition is applied for the Windows Explorer.
  - When the previous connection has been saved in the cache.

## 1.2.14 Web Upload and Download Operation Prohibition

---

- This function must be run in Windows® Internet Explorer® 7 or higher.
- File downloading through ActiveX and plug-in cannot be prohibited.
- When a file is opened and run directly in Internet Explorer®, the Web upload and download prohibition function will run.
- When the Web page component displayed in Internet Explorer® is saved as image, the Web upload and download prohibition function will not be run.
- When the entire Web page displayed in Internet Explorer® is saved as a file, the Web upload and download prohibition function will not be run.
- The policy at startup of the Web browser is effective. When the policy has been changed but the Web browser has been started, the function will be run according to the policy before the change.

- During Web upload and download prohibition when Windows® Internet Explorer® 9 is used, the blank page (about: blank) will be displayed under the following conditions. When the blank page is displayed, please click the [Back] button to go back to the page displayed before downloading.
  - When the protection mode performs download from wrong sites.  
The protection mode can be set in [Internet Options] - [Security] tab of Windows® Internet Explorer® 9.
- In an OS later than Windows Vista®, when a user without administrator authority executes the web upload prohibition as the administrator, the related prohibition logs will be collected but the prohibition message will not be displayed.

## 1.2.15 Clipboard Operation Prohibition

---

- Information delivery from the virtual environment to the physical environment or from the physical environment to the virtual environment via the clipboard will be prohibited, while the delivery from the virtual environment to the virtual environment or from the physical environment to the physical environment will not be prohibited.
- When information is extracted from the clipboard through pasting, the operation of saving information to clipboard (copy, paste) will not be prohibited or recorded.
- During clipboard operation of text data, the maximum size of the original file that can be saved is 2048 byte. For the operation of cutting or copying text data, an original file of a maximum of 2048 byte can be original file backup. If the size is larger than 2048 byte, the excessive part will be truncated.
- When continuing with a clipboard operation after copying, the prohibition log after the second clipboard operation will not be sent in the copy source.
- When the remote desktop or Citrix Online Plugin is used, a prohibition log will be output when the right-click context menu of explorer at the copy destination is displayed. If the copy sources are in the same environment, no prohibition log will be output.
- Multiple prohibition logs will be sent for one paste operation.
- The application name in the copy source log is blank.
- When an image is pasted to Microsoft® EXCEL, the original file will not be original file backup.
- When a virtual environment client other than remote desktop is used, the name of PC at the copy destination in the copy source log is blank.
- The PC name of copy destination cannot be obtained in the environment in which remote desktop is used and IPV6 is effective.
- When a file is being copied, the original backup file name of the copy source is the file name with path, while the file name of the copy destination is the file name only.
- When Microsoft® WORD or Microsoft® Excel is used in the virtual or physical environment, clipboard operations can be performed within the Microsoft® WORD or Microsoft® Excel after the window has been activated. Therefore, the relevant prohibition log will be recorded.
- When logging off the Citrix Online Plugin, the relevant clipboard prohibition log will be recorded.
- When VMWare View Client/VMWare vSphere Client is used, data can be obtained from the clipboard when switching between the window of physical environment and virtual environment. Therefore, the relevant prohibition log will be recorded. In addition, the prohibition logs at the copy source and destination are different.
- When text data is copied and pasted within an application, the line feeds in the [Content] column will be replaced with “??”.
- When the Citrix Online Plugin is used, the PC name of the physical environment is blank in the log of virtual environment.
- When VMWare View Client/VMWare vSphere Client is used, the PC name of the physical environment in the virtual environment is blank and the PC name of the virtual environment in the physical environment is blank.
- If remote desktop is used, the path name of cache data will be recorded in the [Content] column in the physical environment log after a file has been copied from the virtual environment to the physical environment according to the following operations.  
[Operation]

After performing the paste operation before the clipboard operation prohibition policy has been set, set clipboard operation prohibition on the client (CT). Then, copy the file from the virtual environment to the physical environment.

## 1.2.16 All Logs

---

- In the operation log obtained when no one logs on, the user name will be recorded as "SYSTEM", while the domain name will be recorded as "This computer name".
- When the user name in the logs is recorded as [SYSTEM], the domain name will surely be recorded as "This computer name".
- If the logon user performs operations within seconds after logon, the user name of log will be recorded as [SYSTEM].
- In startup, shutdown, sleep, and return logs of PC, the user name will be recorded as [SYSTEM] and the domain name will be recorded as "This computer name".
- If multiple log-on users exist in Windows Vista®, Windows Server® 2008, or Windows® 7, the user names will surely be recorded as [SYSTEM] and the domain names will be recorded as "This computer name" in E-mail sending log and E-mail attachment prohibition log.
- Under Windows Vista®, Windows Server® 2008, or Windows® 7, the user name of file operation log will be recorded as [SYSTEM] and the domain name will be recorded as [NT AUTHORITY].
- When the log information recording was stopped due to a compulsory shutdown of the power of the client (CT), the log information will not be recorded.

## 1.2.17 File Export Log

---

- File export logs are obtained only when the "Export Utility" is used. File export logs cannot be recorded when files are exported using a tool such as Windows Explorer, which is not "Export Utility".

### About Original File Backup

- When the export data is folder, only the file not the folder structure will be original file backup as original file.
- The original file will not inherit the properties of exported file.
- If the backup original file has been specified, the files encrypted using the encrypting file system (EFS) of Windows cannot be exported.
- Only the user with the [System] authority is permitted to access to the folder that saves the backup original data on the management server. Since the data of backup original file itself is not encrypted, it is necessary to pay attention to the change of access authority and data management after backup.

## 1.2.18 Printing Operation Log

---

- When a shared printer connects to the server defined as a Windows printing server in Windows Vista®, Windows Server® 2008, or Windows® 7 for printing, the name resolution of Windows Vista®, Windows Server® 2008, or Windows® 7 must be set to use complete DNS name for domain name resolution. If it fails to use the complete DNS name for name resolution, the printing operation logs cannot be obtained.
- When a shared printer connects to the server defined as Windows printing server in Windows Vista®, Windows Server® 2008, or Windows® 7 for printing, two identical logs will be recorded at one printing operation when the [Render printing jobs on client computers] is active in network printer properties defined in Windows Vista®, Windows Server® 2008, or Windows® 7. One of the two logs records the name of the PC that performs printing operation changes to the name of the printing server.
- If the printing server is Windows® 95, Windows® 98, or Windows ME (client (CT) of V12), the printing operation log of the client (CT) that records printing performed via the print server cannot be collected.

- When [Set printing monitoring mode] is set to [Monitoring the printing of local printer only], the printing operation log cannot be collected in the following conditions:
  - Pattern 1
    - When printing via the printer server without the client (CT) installed.
  - Pattern 2
 

When all the following conditions are satisfied:

    - When printing is performed via the printer server with the client (CT) installed
    - The printer server and the client (CT) are not in the same subnet
  - Pattern 3
 

When all the following conditions are satisfied:

    - When printing is performed via the printer server with the client (CT) installed
    - When multiple NICs are used by the client (CT)
    - The machine information sent from the printer to the client (CT) is not in the same network segment as the management server of the client (CT).
  - Pattern 4
 

When all the following conditions are satisfied:

    - When printing is performed via the printer server with the client (CT) installed
    - When both the machine information sent from the printer to the client (CT) and the client (CT) are IPV6 IP address.
- In order to collect printing operation log, Port 139 must be opened. When a personal firewall is used, please confirm that the Port 139 is open during the installation of the client (CT). In addition, when installing or change the configuration of a personal firewall during the operation, please confirm that port 139 is open at all times. When the client (CT) is being installed in the following OS, port 139 will be opened automatically for Windows firewall:
  - Windows® 7
  - Windows Vista®
  - Windows® XP
  - Windows Server® 2003
  - Windows Server® 2008
- To collect the printing operation log that records the printing through a network printer, the [File and Printer Sharing for Microsoft Network] checkbox must be selected in the network connection properties of the Control Panel. When the computer has multiple LAN cards, please check all the LAN cards that perform printing via network.
- Please pay attention to the following when [Monitor the printing of local printers only] is selected during the installation of the client (CT).
  - It is necessary to log on to the OS first in the client (CT) that acts as the printer server. Without logon to the operating system, the printing requests from other clients (CTs) cannot be detected and thus the printing operation logs cannot be collected.
  - If the log viewer is used to view the printing operation logs, the name of the computer that performs printing will be displayed in the [Domain Name] column.
- If a printer is heavy-loaded and the shutdown or logoff operation is executed on the client (CT) after the printing has finished, the following log may be collected sometimes.
  - The printed file name is [Local Down Level Documents].
  - The total number of printed pages is [Unknown] or is inconsistent with the total number of actual printed pages.
- If the client (CT) is powered-off or a blue screen occurs immediately after the printing has finished, logs cannot be collected.

- When network printer is used for printing, sometimes the total number of printed pages is [Unknown] or is inconsistent with the actual number of printed pages in printing operation log.
- If a printed file has many pages, the log may be collected as multiple printing operation logs sometimes. At this time, the file names will be the same, but the pages will be divided.  
For example, when "File A 100 pages" log is collected, it may be divided into three logs for collection sometimes, which include "file A 4 pages", "file A 90 pages", and "file A 6 pages".
- If a large number of files are printed in a short period (for example, multiple copies or files are printed), printing operation logs may not be collected by files, or the number of pages of the collected log may be incorrect sometimes.
- The number of pages displayed in the log viewer may be less than the actual number of pages. This occurs because the printing operation log collects the information reported by the Printer Spool, when printing a file with many pages, the number of pages reported by Printer Spool may be less than the actual number of pages.
- For some applications, the name of a printed file displayed in the log viewer may be blank.  
This occurs because the printing operation log collects the information reported by the Printer Spool. But due to different applications, the printed file names are not reported to the Printer Spool sometimes.
- For some applications, in the case of printing with multiple copies, only one printing operation log will be displayed in the log viewer.  
This occurs because the printing operation log collects the information reported by the Printer Spool. But due to different applications, the Printer Spool may report the printing of multiple copies as the printing of a single copy sometimes.
- If [Monitor printing of all printers in this terminal (recommended)] is selected during the installation of the client (CT), when printing is performed from the client (CT) via network printer, if the printer server does not use a server edition OS, the maximum connection limit may be reached. If the limit has been reached, printing cannot be performed from machines other than the client (CT). The limit varies with OS editions and is determined according to the number of sessions.
- If the same printer is defined repeatedly during the registration of printer, two printing operation logs will be collected at one printing operation.
  - The two normal logs with same contents.
  - One normal log, and one log in which the printed file name is [Remote Down Level Document] and the number of pages is [Unknown].
- If [Monitor the printing of local printers only] is selected during the installation of the client (CT) on the printer server, the user name used by the client (CT) that performs printing via this printer server must be registered on the printer server in advance. Otherwise, the user name of the print log may be recorded as follows:
  - If the user name used by the client (CT) has general user authority only, the "User name" of log will sometimes be recorded as [Guest].
  - When the print server requires logon as Administrator before printing, the "User name" of log will sometimes be recorded as "Administrator".
- The operation of document writer (Microsoft Office Document Image Write and Adobe PDF) that does not print on paper will be recorded as print log.
- The number of pages displayed in log viewer may be [Unknown]. This is because the printer driver reports two printing jobs to the Printer Spool at one printing operation, and one of them is reported to the Printer Spool as [Unknown].

## 1.2.19 Window Title Obtaining Log

---

- If "Window title of application" and "URL information displayed in address bar" is the same as that at last log collection, this item of Window Title Obtaining Log cannot be collected.
  - For Internet Explorer® or Windows Explorer, if the window title or URL information displayed in the address bar is the same as that at last log collection, this item of window title log cannot be collected.
  - For other applications, if the window title is the same as that of the last log collection, this item of window title log cannot be collected.



- The repeated window title log filter can manage a maximum of 100 repeated window title logs. When the number of window title log exceeds 100, the filter will delete the earliest window title logs.
- After the power of PC is re-connected, check for repeated log filtering should be performed all over again.

## 1.2.20 E-mail Sending Log

---

- When E-mail sending logs are recorded, Systemwalker Desktop Keeper monitors the SMTP port (the port number specified during the installation of client (CT)). In other words, the E-mail software that uses SMTP communication protocol during E-mail sending will be monitored. When multiple E-mail software is being used, please set each SMTP port number to the same one.
- The Web mail and groupware that do not use SMTP communication protocol cannot be monitored.
- When the type of server that uses Outlook E-mail account is “Microsoft Exchange Server”, since it is not SMTP protocol, E-mail sending logs cannot be collected.
- If the port number specified during installation has been disabled by personal firewall, E-mail sending logs cannot be collected.
- The E-mails to be sent must be encoded with JIS:ISO-2022-JP, UTF-7, UTF-8, or US-ASCII. The E-mails not encoded with JIS:ISO-2022-JP, UTF-7, UTF-8, or US-ASCII will not be sent. Even the policy of collecting E-mail sending log has been set, the logs will not be collected.
- When Microsoft® Outlook® 2003 or Microsoft® Outlook® 2007 is used to send an E-mail that contains UNICODE characters and [Auto select encoding for E-mail sending] has been set, even the characters are set to Japanese (JIS), they will be replaced with Simplified Chinese (GB2312) before sending the E-mail. Therefore, please do not set [Auto select encoding for E-mail sending] in Microsoft® Outlook® 2003 or Microsoft® Outlook® 2007.
- If the E-mail software does not comply with the “RFC2183” standard, the logs cannot be collected properly sometimes. (For example: attachment name cannot be recorded)
- The maximum size of all information collected in E-mail sending log is 2048 bytes. If it exceeds 2048 bytes, delete information according to the following sequence until it is lower than 2048 bytes.  
Therefore, when part of the E-mail sending log has been deleted, file related to the e-sending log may not be traced in the log viewer.
  1. The sender address will be truncated to 100 bytes. If the 100th byte is the first byte of double-byte character, the maximum of 99 bytes will be reserved.
  2. The recipient address (Bcc) will be truncated to 500 bytes. If the 500th byte is the first byte of double-byte character, the maximum of 499 bytes will be reserved.
  3. The recipient address (Cc) will be truncated to 500 bytes. If the 500th byte is the first byte of double-byte character, the maximum of 499 bytes will be reserved.
  4. The recipient address (To) will be truncated to 500 bytes. If the 500th byte is the first byte of double-byte character, the maximum of 499 bytes will be reserved.
  5. The E-mail topic will be truncated to 100 bytes. If the 100th byte is the first byte of double-byte character, the maximum of 99 bytes will be reserved.
  6. The attachment name will be truncated to 300 bytes. If the 300th byte is the first byte of double-byte character, the maximum of 299 bytes will be reserved.
- For the recipient address (Bcc), only the address part will be recorded as log. The names attached to the E-mail software will not be collected.
- During the installation of a new network device and a LAN driver, the E-mail sending logs will be collected only after the client (CT) has been restarted.
- When the recipient addresses (To, Cc, or Bcc) contains “,” and “;”, based on the difference of E-mail software, addresses are separated at “,” and “;” sometimes before logs are collected.
- If the recipient addresses in the [To] and [Bcc] fields are the same and the recipient addresses in the [cc] and [Bcc] are the same, the recipient addresses in the [Bcc] field are not logged.

## About Viewing E-mail Content

- After MIME encoding, the E-mail contents (including body text and attachment) will be saved on the server as a file for viewing. Therefore, the file size is the size of the MIME-encoded file. If the file of E-mail content exceeds 50 MB, the contents cannot be saved (E-mail sending log can be collected).  
Since the backup tool will not back up the file of E-mail content, it is recommended to back up the file periodically.
- Similar to other backup original files, the file saved on management server for viewing E-mail content cannot be original file backup by the backup tool or command.

## About Confirmation of Recipient Address

### **This function is not available.**

- The addresses are confirmed during an E-mail sending refer to all the recipient addresses (To, CC and BCC). FROM does not need to be confirmed.
- When the user sends an E-mail to an address that does not belong to the excluded domain through E-mail software, even if the sending is terminated, the E-mail software will still complete the E-mail sending process. Therefore, the E-mail will be considered as sent.
- When this function is used on the mail server, messages will be displayed when sending the forwarded E-mail. Since the E-mail sending process will not be completed when the message is displayed, the E-mail will probably be suspended Please do not use this function on the mail server.
- When the warning message is being displayed, E-mail cannot be sent. If the state of message display lasts for a long time, E-mail sending may fail.
- If this function is run in the client (CT) installed in the computer of management server, the address may be confirmed and warning messages may be displayed when the administrator notifies E-Mail sending. Since E-mail sending process will not be completed during the period when message is being displayed, please set the recipient address of administrator notification E-mail to the address in of excluded domain.
- This function will confirm the E-mail that is automatically sent by system and display warning message. Since E-mail sending process will not be completed during the period when message is being displayed, please set the recipient address of administrator notification E-mail to the address in of excluded domain.

## 1.2.21 Command Operation Log

---

- The command prompt is collected only when it is started from [Start]-[All Programs]-[Accessories]-[Command Prompt]. When “cmd.exe” or “command.com” is run directly, the command log will not be collected.  
Also, the IME (Input Method Editor) in the command operation only supports IME provided by Microsoft.  
However, under the following conditions, the command prompt will not be collected even the command operation is started through the [Start] menu.
  - Processing in batch files.
  - Operation of the “start” command
  - Output result of applications output by independent console (example: “telnet, ”doskey”, “debug” .etc)
- If a command with many output results is executed, when confirming the collected command prompt in the Log Viewer, the log will be displayed in shift sometimes.
- If one command has more than 300 lines of output results, only 300 lines of the log will be collected.
- After the Command Prompt window is closed through the “exit” command or the “×” button, the command prompt will be collected to the master management server/management server. Therefore, when the user of the client (CT) does not close the Command Prompt window, the command prompt cannot be collected.

- If the properties of the command prompt (size of window buffer and the size of window) are modified (including the time of modifying properties through command), the following states may occur:
  - The modified settings are invalid.
  - The window is displayed in chaos.
  - Part of log is not collected.

In addition, the modified properties will take effect at next startup of the client (CT).

- When the command prompt is being collected, date and time will be inserted after the input command. Therefore, the date and time that do not exist in command prompt will be displayed in the Log Viewer.  
However, when the next command is input before terminating the command output, data and time will not be inserted after the input command sometimes due to the timing of input. When there are many output results, the date and time will sometimes be inserted in midway.

#### Example of display in Command Prompt

```
C:\Documents and Settings\Administrator>dir

The volume label of Drive C does not exist.

Volume serial number is EC12-57D0
```

#### Example of display in Log Viewer

```
C:\Documents and Settings\Administrator>dir

                                --[2005/05/27 13:40:19]--

The volume label of Drive C does not exist.

Volume serial number is EC12-57D0
```

- If the command for displaying the window again is input, logs will be collected twice at one output. (Example: “append” command)

## 1.2.22 Device Configuration Change Log

---

When UAC is enabled in Windows Vista®, Windows Server® 2008, or Windows® 7, the device configuration change log will not be collected when a general user upgrades to the administrator and connects to the network drive.

The device to be recorded will be allocated as a drive (A-Z drive) in Windows.

In the virtual environment, the device configuration change log when a DVD/CD is mounted as the local device will not be collected.

## 1.2.23 PrintScreen Key Operation Log

---

When the software that collects the hardcopy of window through the PrintScreen key is installed, PrintScreen key operation log will be collected.

## 1.2.24 Web Operation Log

---

- This function must be run in Windows® Internet Explorer® 7 or higher.
- The log of file upload and download using HTTP protocol will be collected.
- When files are downloading through Active X or plug-in, log cannot be collected.

- If files are opened and run directly in Internet Explorer®, the Web upload and download operation log cannot be collected.
- If the Web page components (such as button and LOGO) displayed in Internet Explorer are saved as images, the Web upload and download operation log cannot be collected.
- If the entire Web page displayed in Internet Explorer® is saved as a file, the Web upload and download operation log cannot be collected.
- The policy at the start of Web browser is enabled. When the policy is changed while the Web browser has been started, the Web browser being started will run according to the policy before change.
- The web operation log is the log collected during web upload and download operations. Therefore, even if exception occurs during download and the processing is cancelled by user, log will still be collected.
- The download operation performed when connecting to FTP sites through Internet Explorer® will be obtained as a Web operation log.
- Web upload operation logs will only be collected when the sent HTTP header conforms to the Content-Disposition field and filename parameter specified in RFC1806. Otherwise, logs cannot be collected.

## 1.2.25 FTP Operation Log

---

- Only the FTP communication log when the communication port of server to which the FTP client is collected is set to “21” will be recorded.
- The log of FTP.EXE on 64-bit OS cannot be obtained.
- When an FTP client is started from Command Prompt, only the Windows FTP.EXE will be recorded by this function.
- This function will not record FTP transfer performed by secure FTP (FTP protocol such as FTPS and SFTP for encrypted communication), Web browser plug-in, or ActiveX.
- The file names obtained in the FTP operation log are the file names on the FTP server. The file paths will not be obtained.
- When an FTP download operation is performed in Windows Explorer, the file name may be encoded with URL. In this case, the log will be recorded as URL encoded string.
- A FTP operation log is collected during FTP upload and download operations. Therefore, even if exception occurs during the process of file transfer and the transfer is cancelled by user, log will still be recorded.
- The FTP transfer using Internet Explorer® will be obtained as Web operation log.
- When policy is changed during the startup process of the FTP client, the FTP client being started will run according to the policy before change.
- When using Windows Explorer, the following operations may occur through enabling/disabling FTP folder view:
  - When FTP folder view is enabled  
The upload and download operation log will be obtained, but the file path will not be obtained. Only the file name will be obtained.
  - When FTP folder view is disabled  
The upload operation cannot be performed. The download operation log will be obtained. The file path will not be obtained. Only the file name will be obtained.

## 1.2.26 Clipboard Operation Log

---

- The operation log during information delivery from virtual environment to physical environment and from physical environment to virtual environment is obtained. The operation log during delivery from the virtual environment to the virtual environment or from the physical environment to the physical environment will not be obtained.
- When extracting information from clipboard (paste), the operation log for saving the information to clipboard (copy and paste) will not be recorded.

- When performing a clipboard operation of text data, the maximum size of the original file that can be original file backup is 2048 byte. If the size is exceeded, the excessive data will be truncated before the file is saved.
- When continuing with the paste operation after the copy operation, the operation log after the second operation will not be sent in the copy source.
- If the remote desktop or Citrix Online Plugin is used, operation log will be output when the right-click context menu of Explorer is displayed at the copy destination. If the copy source and destination are under the same environment, no operation log will be output.
- Multiple operation logs will be sent at one paste operation.
- The application name in the log of copy source is blank.
- When an image is pasted to Microsoft® EXCEL, the original file will not be original file backup.
- When the virtual environment client other than the remote desktop is being used, the PC name of copy destination will be blank in the log of copy source.
- In the environment in which remote desktop is used and IPV6 is effective, the PC name of copy destination will not be obtained.
- When a file is copied, the name of the backup original file at the copy source contains the file path, whereas the file at the copy destination contains the file name only.
- When Microsoft® WORD or Microsoft® Excel is used in the virtual or physical environment, the clipboard operation can be performed within Microsoft® WORD or Microsoft® Excel when the window is activated. Therefore, the operation log will be recorded.
- When logging off from Citrix Online Plugin, the operation log will be recorded.
- When VMWare View Client/VMWare vSphere Client is used, data can be obtained from the clipboard when switching between the physical environment window and virtual environment window. Therefore, the operation log will be recorded. In addition, the operation logs at the copy source and copy destination are different.
- When text data is copied and pasted within an application, the line feeding code in the Content column will be replaced with “??”.
- When Citrix Online Plugin is used, the PC name of the physical environment will be blank in the log of virtual environment.
- When VMWare View Client/VMWare vSphere Client is used, the PC name of the physical environment is blank in the virtual environment, and the PC name of the virtual environment is blank in the physical environment.

## 1.2.27 File Operation Log

---

- The file tracing function cannot be used according to the compression and decompression log of the compression software (such as the ZIP, LZH, and compression tools provided by Microsoft).
- The application operation log of adding functions on Internet Explorer® or Windows Explorer will not be collected.
- When the OS is Windows Vista®, Windows Server® 2008, or Windows® 7, if authority upgrade is allowed through UAC and operation is continued, the program name in the collected log is displayed in [Content] of [Log List] of Log Viewer).
- When the file displayed in the [Open File] dialog box exists, even if the file is not opened, the viewing log will be collected.
- When a large file is copied, a large number of file operation logs will be collected.
- Under the following conditions, the file size may not be obtained normally.
  - When a file is moved and renamed repeatedly or the device that stores the processed file is added, deleted, and ejected within 30 seconds.
  - When file operations are performed before logoff or shutdown.

When the actual operation is different from the collected operation log

- When the following software or command is used, the file operation log will be collected as described in “[8.2.20 File Operation Log](#)”.
  - Windows Explorer

- Notepad
- Wordpad
- Microsoft® Word (2000, 2002, 2003, 2007 and 2010)
- Microsoft® Excel (2000, 2002, 2003, 2007 and 2010)
- Microsoft® PowerPoint® (2000, 2002, 2003, 2007 and 2010)
- Commands in the Command Prompt window (COPY, XCOPY, MOVE, DEL, ERASE, RD, REN and MD)

However, please pay attention to the following items.

- The [Update] operations (such as Save As and Replace) of Microsoft® Word are collected as the log of [Create] operation.
- Same as Explorer and XCOPY, for a process registered in the [File Operation Process] tab, if the scope of file operation log of this process is set to [Get operations excluding viewing], the [View] logs of the process will not be collected.
- The excessive logs that are not listed in “[8.2.20 File Operation Log](#)” may be collected sometimes even when the software or command mentioned above is used.
- When the software or command apart from the above is used, the operation log that does not conform to the actual operation may be collected sometimes (For example, [Copy] or [Move] logs cannot be collected, but they will be collected as [View], [Create], [Delete], or [Rename] operation.
- When the Redirect command (> or >>) or MD command is run in Command Prompt, logs cannot be collected.
- When the data in the local drive is written to a DVD/CD by using the burning software, this operation can only be collected as a [View] operation instead of [Copy] because information of access to DVD/CD cannot be collected.
- For output to a tape device, communication through cross cable such as RS-232C, or operation via IrDA (Infrared device), since the information of target drive cannot be obtained, only the information of local drive will be collected during log collection.
- When moving a large file (it takes more than 30 seconds to move one file), the log may be divided into two pieces sometimes, which are [Copy] and [Delete].
- When the Move command is used to move a file by overwriting in the same drive, if the overwriting operation is performed after the prompt for confirmation of overwriting is displayed for more than 30 seconds, the log will be [Rename] instead of [Move]. When other commands are used, if the conformation prompt is displayed, the collected log may be different from the actual one sometimes.
- If the COPY or XCOPY command such as COPY A.TXT+B.TXT C.TXT or COPY \*.TXT C.TXT is executed in Command Prompt, it will be collected as the [Create] log of C.TXT.
- A maximum of 259 bytes can be collected as the information of [File Name], [Target File Name], or [Source File Name] in a collected log.
- When a path that does not exist is specified in the file operation of command prompt, the operation will fail, but the log will still be collected.
- When the operation of displaying the confirmation window is performed, even if the operation is cancelled, the file operation log will still be collected.
- In Windows Vista®, Windows Server® 2008, or Windows® 7, when the operation of displaying the confirmation window (Copy by overwriting, move by overwriting), the log type will not be recorded as [Copy] or [Move]. (The update log of the target file for copying or moving and the log of deleting the source of moving will be collected.)
- Under virtual environment, the file name of physical drive of drive mapping may contain extra information sometime [\\Device\Ntfs\{PicaDriveRedirector}\].  
Example: [\\Client\F\$\Customer\CustomerInformation.xls] will be obtained as [\\Device\Ntfs\{PicaDriveRedirector}\Client\F\$\Customer\CustomerInformation.xls].
- Under virtual environment, the full path may not be obtained for the file name of physical drive of drive mapping.  
Example: [\\Client\F\$\Customer\CustomerInformation.xls] will be obtained as [\\CustomerInformation.xls] or [\\Customer\CustomerInformation.xls]

#### When a large number of [View] logs are collected

- When collecting operation logs, register the process that requires the file operation log to be recorded in the [File Operation Process] tab. At the time, If the [Select according to Extension] option is set to [Get all extensions], information about all files accessed by the process (application) will be collected Apart from data file, these files also contains execution modules and temporary files such as files with “exe”, “dll”, “ini”, “tmp”, “lnk” or “inf” extensions. All these operation logs will be collected.

#### When logs cannot be collected

- The operation log of playing music CDs cannot be collected.

#### File Operation Logs Relating to the Network Drive

- The file operation log relating to network drive to be collected is the file and folder operation performed for computers in the network from the client (CT) of Systemwalker Desktop Keep.
- The file operation log relating to network drive is displayed in UNC format or the UNC format in which part of the computer name is IP address. However, in the following conditions, the [Target File Name] information of log will be displayed with the absolute path of file name or folder name.
  - Allocate a drive letter for the network drive and perform rename operation in the drive letter
  - Allocate a drive letter for the network drive and perform move operation in the drive letter.
  - For the drive letter that is allocated as a network drive, perform the move operation from the folder that directly accessed to the network drive with the same drive letter as the allocated one.
- For moving operations between the drive letter that is allocated to a network drive and the folder that directly accessed to the network drive with the same drive letter as the allocated one, the logs listed in “[8.2.20 File Operation Log](#)” will be collected, but the following information in the collected logs, however, may be different.
  - In [File operation]-[About log of files under the folder]-[In same drive], logs of [Rename] instead of [x] will be collected.
  - In [File operation]-[About log of folder]-[In same drive], logs of [Create], [Delete], and [(Delete)] instead of [Rename], [(Rename)], and [(Delete)] will be collected.

#### [Set excluded folder for file operation Log obtaining]

- Based on the setting of the excluded folder for obtaining the file operation log, even for built-in disk, when the OS identifies it as a removable drive, the disk will not be excluded.
- Even if the excluded folder is enabled, the operation logs related to the folders that are not excluded will be obtained.
- All the folders, subfolders, and files under an excluded folder are targets to be excluded.
- When modifying the configuration value of system environment variable TEMP and TMP, the value after modification will take effect after the next startup of OS. The configuration value prior to modification will be used before the OS is restarted.
- When modifying the configuration value of user environment variable TEMP and TMP, the value after modification will take effect upon the next user logon. The configuration value prior to modification will be used before the next logon.
- When only symbols such as “\” and “\\” have been set in the configuration value of TEMP and TMP of system environment variable and user environment variable, the setting will be invalid.  
“\” indicates that the root directory of current drive while the program is running, but it will not be excluded because it cannot be fixed.  
In addition, “\\” indicates the beginning of network path in UNC format, but it is meaningless when it contains only “\\”, and it will not be excluded at this time.
- When the folders of system environment variable TEMP and TMP and the temporary Internet files are specified to target for exclusion if the file name is a path of more than 260 bytes, the exclusion setting will be invalid and the file operation log will be collected.  
However, if the path is 260 bytes and the 260th byte is “\”, the setting will be valid.

- If the path of an excluded target contains dedicated UNICODE characters, these characters will be replaced with “?” before comparison, Therefore, the file operation logs that contain UNICODE characters at the same place will also be excluded. For example, when Windows user name contains dedicated UNICODE characters, access to the TEMP or TMP folders of other users that also contain dedicated UNICODE characters will also be excluded.
- When the path of excluded target in Windows Vista®, Windows Server® 2008, or Windows® 7 contains dedicated UNICODE characters, it will not become the target for exclusion.

## **1.2.28 Logon/Logoff Log**

---

- The logon logs, PC shutdown logs, PC suspension logs will not be sent to the server immediately. They are saved on the local disk first and then sent to the Management Server. It may take some time before the logs can be searched on the log viewer.
- If the power of a PC is cut off by force, the logoff log and PC shutdown log will be created at next start of the client (CT). Therefore, it may take some time before the logs can be searched on the log viewer.
- If the power of a PC is cut off by force at the moment of logoff, two logoff logs for the user may be created sometimes.
- Under Windows Vista® or Windows® 7, the logoff logs of all logon users at the time when power of a PC is cut off by force will be recorded.

## **1.2.29 Screen Capture**

---

- When the available capacity of the drive in which the folder that saves log files is located is smaller than 50 MB in the client (CT), screen capture cannot be performed.
- For the game interface and video editing software that run on a special graphic board, when the direct interfaces are displayed or edited through hardware, screen capture cannot be performed.

## **1.2.30 About Collection of Logs for Investigation of Client (CT)**

---

When the logs for investigation (trace logs) of the client (CT) are collected, a large number of file operation logs of tracing will be collected after the policy of obtaining the file operation log is set.

## **1.2.31 About File Trace Function of Log Viewer**

---

- A maximum of 1000 records can be searched through [Back Trace] or [Forward Trace]. If the number of search results exceeds 1000, the searching will stop at that time and only 1000 records will be displayed.
- When [Save As] is performed for a file, it will be recorded as “Create” in the file operation log and the relationship with the file at source for saving cannot be output in logs. Therefore, at the time, the file trace function cannot be performed.
- When the file operation logs are obtained from the [File Export Utility], the file export logs and file operation logs will be displayed repeatedly in the trace window.
- File names containing spaces cannot be specified. Since space is used as the separator between keywords, the search condition must contain at least one keyword.
- Window title logs cannot be the search target of file trace.
- The process name of each log (for example, “Explorer.exe” when the file operation log is obtained by Explorer) cannot be the search target of file trace.
- When the setting of File Operation Process is not set to [Get All], the file trace may not be performed properly through the file trace function.



## 1.2.32 About Viewing Operation Logs of the Remote Connection Source and Target in Log Viewer

---

### Link of logs between terminals based on the information of inter-terminal connection

- To link the logs between two terminals, the client (CT) must be installed on both the connection source and target terminals. If only one of them is installed with the client (CT), only the information of connection, disconnection and the log of terminal with the client (CT) installed can be collected.
- When [Collect information of connection between terminals] has been set in the system settings of the server settings tool, the following logs will definitely be collected. "Do not collect" cannot be set as a policy.
  - Logon log
  - Logoff log
  - PC startup log
  - PC shutdown log
  - PC sleep log
  - PC recovery log
  - PC connection log
  - PC disconnection log

If the above logs are no need to be collected, set [Do not collect information of connection between terminals] in the system settings of the server settings tool. But in this case, the logs of the connection source and target terminals cannot be linked.

- When the same user is allowed to log on a terminal for multiple times regardless of physical environment or virtual environment, even if one user logs in at separate times, it will be considered as the operation of a single user and operations at each logon will be bound and displayed in time sequence.
- The logs of the connection source and target terminals can be searched by specifying the same. If the time on the terminals is different, a series of operation logs cannot be searched. Therefore, please synchronize the time on the source and target terminals.
- Since the terminal that performs log search and the connection source and target terminals are registered on different Management Servers, in the environment with a 3-level structure, the log searching terminal must be connected to the master management server before searching logs. When log searching is performed after connecting to a lower-level management server, log search for connection source and target terminals cannot be executed.
- For the virtual OS on Hyper-V, when connection is performed through the Hyper-V manager, the connection will be regarded as a local connection rather than an inter-terminal connection. When remote desktop connection is performed for a virtual OS, the connection will be regarded as an inter-terminal connection and the logs can be collected.

# Chapter 2 Prepare Operating Environment

This chapter describes how to use Systemwalker Desktop Keeper.

It describes how the system administrator and department administrator should prepare the operating environment, search the collected logs and modify settings in order to audit the operations of the user of the client (CT).

It also introduces the environment prepared for recording and auditing the client (CT) operations.

## 2.1 Considerations for Preparing Operating Environment

When preparing the environment that enables viewing of the logs in the mean time of prohibiting the operations of the client (CT) and collecting logs, the following three operation policies must be determined and the determined contents should be set in Systemwalker Desktop Keeper.

Determine the allowed operations, unallowed (prohibited) operations and log collection operations when the PC is being used.

The determined contents will be set as “Terminal Initial Settings” in the GUI.

Determine how to send the saved logs to the server.

The determined contents will be set as “Terminal Operation Settings” in the GUI.

Determine how to manage PC and PC users (Users) in the Group.

The managed group will be set as configuration information tree.

### 2.1.1 What is Policy

#### What is policy

Policy is the rules determined according to the guidelines for using the system.

It regulates the allowed operations, unallowed (prohibited) operations as well as information about which operation logs will be collected when the PC is being used.

#### Contents can be set in policy.

Policies of “Prohibited Operation” and “Log Collection Operation” can be set in Systemwalker Desktop Keeper.

#### Set Prohibited Operations

The following are types of prohibited operations, which are set by the administrator or department administrator in the Management Console.

- File Export Prohibition

#### **Encryption Function is not available.**

By setting the file export prohibition policy, file and folder export in drive, network drive, removable drive or DVD/CD of the PC with the client (CT) installed can be prohibited conditionally.

According to the set condition, “File Export Utility” can be used to export files and folders from the prohibited drive. Also, encryption can be performed while exporting.

Please refer to “Systemwalker Desktop Keeper User’s Guide: for Client” for “File Export Utility”.

- Reading Prohibition

By setting the reading prohibition policy, reading of data on the removable drive, network drive or DVD/CD in the PC with the client (CT) installed can be prohibited.

- Printing Prohibition

By setting the printing prohibition policy, printing by non-specified applications can be prohibited in the PC with the client (CT) installed.

- PrintScreen Key Prohibition

By setting the PrintScreen key prohibition policy, the use of PrintScreen key for collecting the hard copy of screen in the PC with the client (CT) installed can be prohibited. In this case, the type of screen hard copy to be collected becomes clear, and screen capture can be collected.

- Logon Prohibition

**This function is not available.**

By setting the logon prohibition policy, logon with the user name that belongs to a set group when logon from the PC with the client (CT) installed can be prohibited. The groups that can be prohibited are as follows:

- Administrators
- Backup Operators
- Debugger Users
- Power Users
- Guests
- Replicator
- Users
- Domain Admins
- Domain Guests
- Domain Users
- Enterprise Admins
- Group Policy Creator Owners

- Application Startup Prohibition

By setting the application startup prohibition policy, startup of the specified applications in the PC with the client (CT) installed can be prohibited.

- E-mail Attachment Prohibition

**This function is not available.**

By setting the E-mail file attachment policy, sending or saving the E-mail with the prohibited file attachment from the PC with the client (CT) installed can be prohibited.

However, saving cannot be prohibited when porting auditing mode is used (the E-mail software uses SMTP to send attachment).

The files that can be specified as prohibited targets are unencrypted files or the files with specified extensions.

In addition, as long as there is one prohibited file in the attachment, the E-mail (E-mail text and all attachments) cannot be sent.

- URL Access Prohibition

By setting the URL access prohibition policy, access to the unauthorized URL in the PC with the client (CT) installed can be prohibited.

- FTP Server Connection Prohibition

By setting the FTP server connection prohibition policy, connection to the non-specified FTP server can be prohibited in the PC with the client (CT) installed.

- Web Upload and Download Prohibition

By setting the Web upload and download prohibition policy, upload and download on the non-specified Web site in the PC with the client (CT) installed can be prohibited.

- Clipboard Operation Prohibition

By setting the clipboard operation prohibition policy, information transfer from the virtual environment to the physical environment or from the physical environment to the virtual environment via clipboard can be prohibited.

### Set Log Collection Operation

This is a policy that sets the type of operation log to be collected. The operation logs that can be collected are as follows. Policies are set by the system administrator or department administrator in the Management Console.

- Application startup log
- Application termination log
- Application startup prohibition log
- Window title obtaining log
- E-mail sending log
- E-mail sending interruption log
- This function is not available.
- E-mail attachment prohibition log
- This function is not available.
- Command log
- This function is not available.
- Device configuration change log
- Printing operation log
- Printing prohibition log
- Logon prohibition log
- This function is not available.
- File export log
- PrintScreen key operation log
- PrintScreen key prohibition log
- Web operation log
- Web operation prohibition log
- FTP operation log
- FTP operation prohibition log
- Clipboard operation log
- Clipboard operation prohibition log
- File operation log
- Logon/Logoff log
- Linkage log
- Screen capture

### Policy Settings Targets

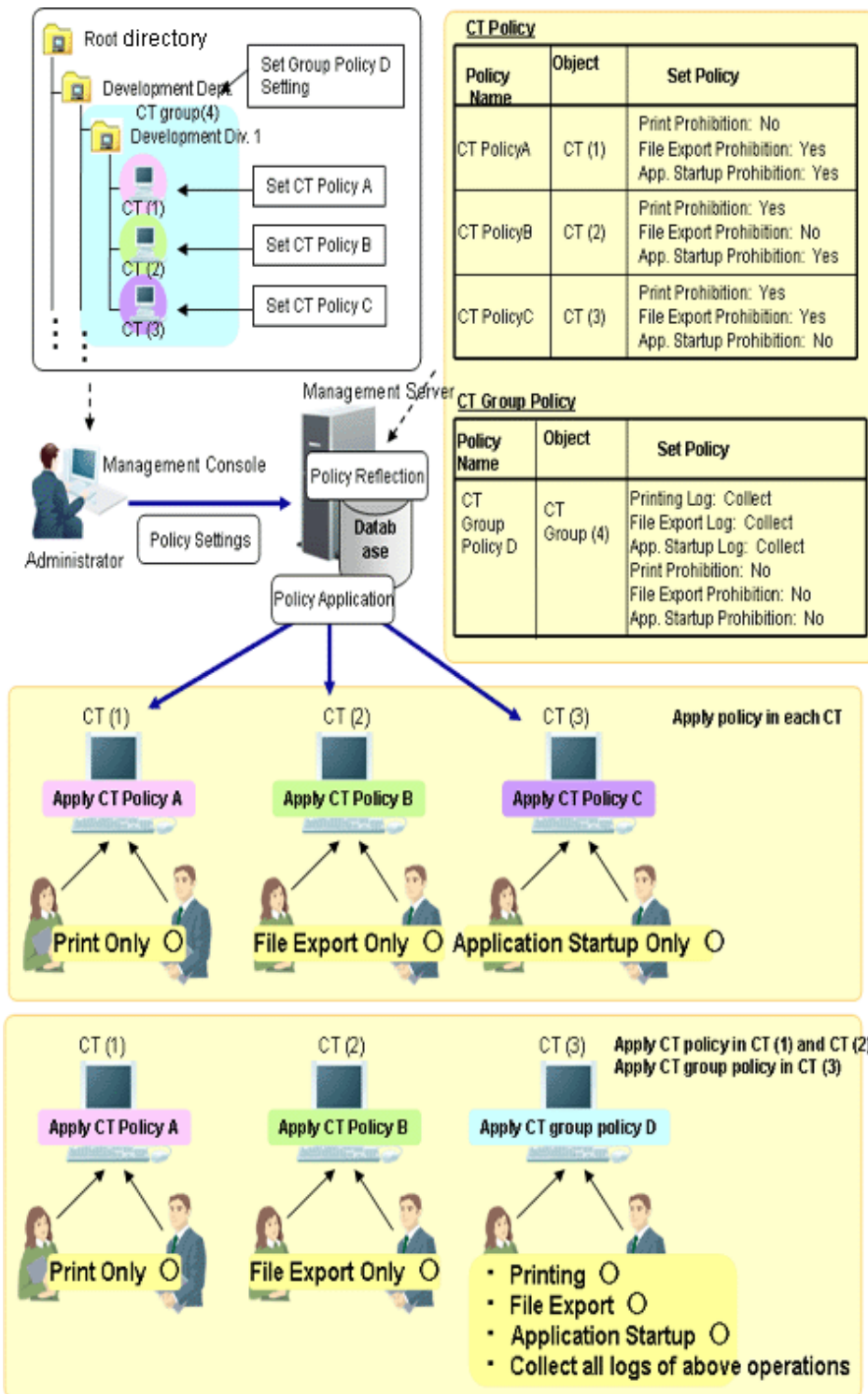
The name of policy varies according to the settings of the defined policy.

When setting policy for the “Client (CT)”, it is called “CT Policy”.  
When setting policy for the “User”, it is called “User Policy”.

#### Settings for Client (CT)

The policy set for the “Client (CT)” is called “CT Policy”. During the client (CT) operation, when the CT policy is valid, the prohibition and log collection will be implemented according to the policies set in the client (CT), no matter which user performs operation. Different policies can be set for each client (CT).

In addition, the clients (CTs) can be grouped by department, and after the clients (CTs) with same purpose of operation is divided into one group, the policy set for this group is called CT group policy. Different policies can be set for each group.



In the above image, the following settings can be performed for the client (CT) and CT group through the Management Console.

The following policies can set for each the client (CT):

- CT (1) Printing only.  
 Printing prohibition: No  
 File export prohibition: Yes  
 Application startup prohibition: Yes

- CT (2) File export only.  
 Printing prohibition: Yes  
 File export prohibition: No  
 Application startup prohibition: Yes
- CT (3) Application startup only.  
 Printing prohibition: Yes  
 File export prohibition: Yes  
 Application startup prohibition: No

Group the clients (CTs) and set the group policy can be to “Allow Printing, File Export and Application Startup” and “Collect All Logs”.

CT policy will be applied to each client immediately or at the next startup. After policy has been applied, the client (CT) will run according to the applied policy.

**[When CT policy is applied in the each CT]**

- CT (1) No matter who operates, only printing is allowed.
- CT (2) No matter who operates, only file export is allowed.
- CT (3) No matter who operates, only application startup is allowed.

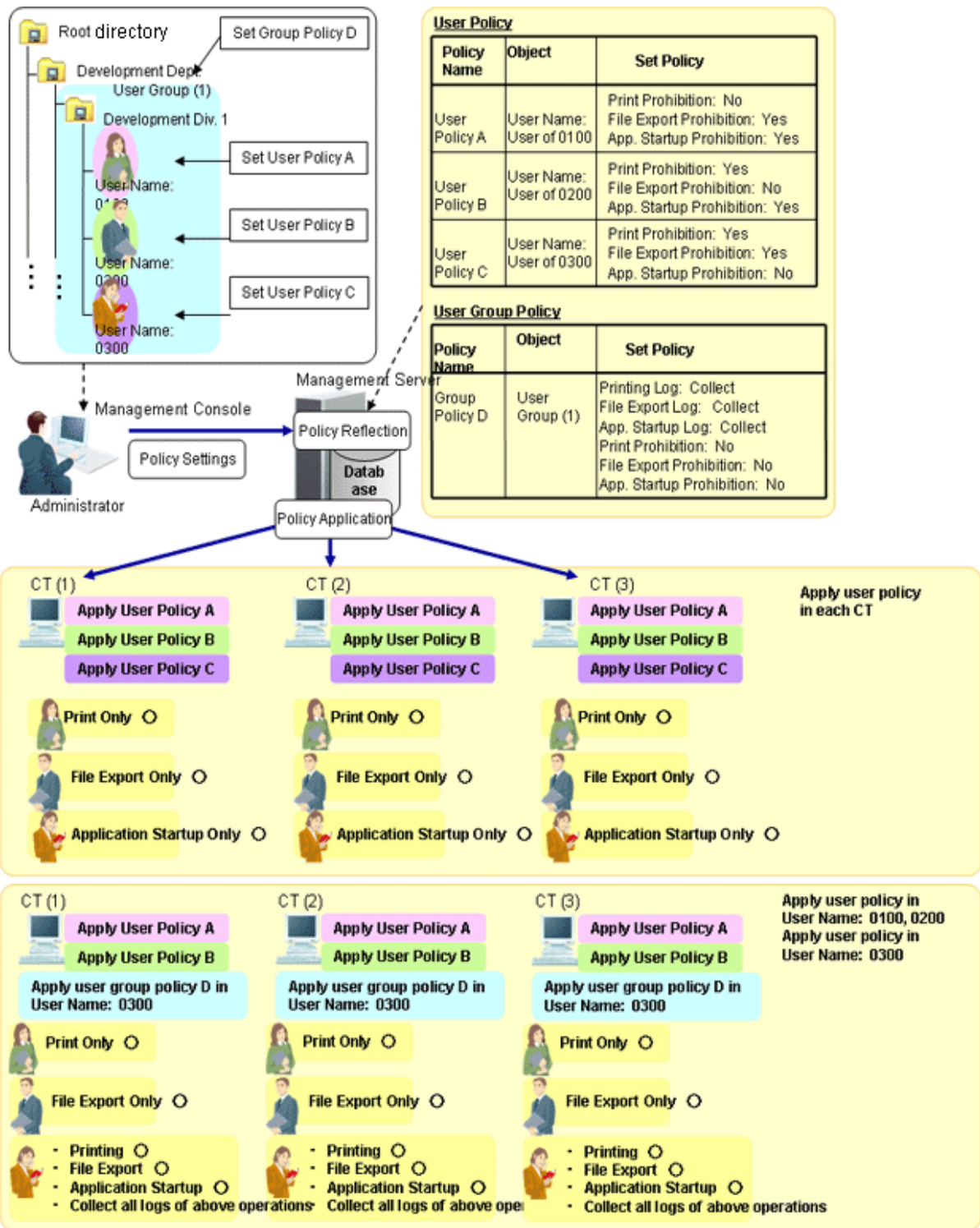
**[When CT policy is applied in CT (1) and CT (2) while group policy is applied in CT (3)]**

- CT (1) No matter who operates, only printing is allowed .
- CT (2) No matter who operates, only file export is allowed.
- CT (3) No matter who operates, printing, file export, application startup can be performed, and the logs of each operation will be collected.

**Settings for User**

The policy set for the user name that is input during logon to Windows in the PC with the client (CT) installed is called User Policy. During the client (CT) operation, when the user policy is valid, the prohibition and log collection can be implemented according to the policies set for the logon user name regardless of the PC on which the operation is performed. Different policies can be set for each user.

In addition, the users can be grouped by department, and after the clients (CTs) with same operation content can be divided into one group, and the policy set for this group is called user group policy. Different policies can be set for each group.



In the above image, the following settings can be performed for the user and user group through the Management Console.

The following policies can be set for each user name:

- User name: 0100 user can only print.
- Printing prohibition: No
- File export prohibition: Yes
- Application startup prohibition: Yes



- User name: 0200 user can only export files.

Printing prohibition: Yes  
 File export prohibition: No  
 Application startup prohibition: Yes

- User name: 0300 user can only start applications.

Printing prohibition: Yes  
 File export prohibition: Yes  
 Application startup prohibition: No

Group the users and set the group policy to “Allow Printing, File Export and Application Startup” and “Collect All Logs”.

After logon to Windows by each user name, correspondent user policy can be applied. After the policy is applied, it has nothing to do with the CT policy of the client (CT). Instead, operation will be performed according to user policy only.

**[When user policy is applied in each CT]**

- Regardless of the client (CT) on which logon occurs, all operations that can be performed by the user have been determined.

User name: 0100 user can only print.  
 User name: 0200 user can only export files.  
 User name: 0300 user can only start applications.

**[When user policy is applied to User Name: 0100 and User Name: 0200 while user group policy is applied to User Name: 0300]**

- Regardless of the client (CT) on which logon occurs, all operations that can be performed by the user have been determined.

User name: 0100 user can only print.  
 User name: 0200 user can only export the file.  
 User name: 0300 user can print, export files and start applications, and logs of each operation will be collected.

**CT Policy/User Policy and Items can be Set**

The items that can be set in the CT policy are different from those can be set in user policy. The items that can be set are as follows:

	Settings Items	CT Policy	User Policy
Prohibition Function	File export prohibition	<input type="radio"/>	<input type="radio"/>
	Reading prohibition	<input type="radio"/>	<input type="radio"/>
	Printing prohibition	<input type="radio"/>	<input type="radio"/>
	PrintScreen key prohibition	<input type="radio"/>	<input type="radio"/>
	Logon prohibition	<input type="radio"/>	— (Note)
	Application startup prohibition	<input type="radio"/>	<input type="radio"/>
	E-mail attachment prohibition	<input type="radio"/>	<input type="radio"/>
	URL access prohibition	<input type="radio"/>	<input type="radio"/>
	FTP server connection prohibition	<input type="radio"/>	<input type="radio"/>
	Web upload and download prohibition	<input type="radio"/>	<input type="radio"/>
	Clipboard operation prohibition	<input type="radio"/>	<input type="radio"/>
Record Function	Application startup log	<input type="radio"/>	<input type="radio"/>
	Application termination log	<input type="radio"/>	<input type="radio"/>
	Application startup prohibition log	<input type="radio"/>	<input type="radio"/>
	Window title obtaining log	<input type="radio"/>	<input type="radio"/>
	E-mail sending log	<input type="radio"/>	<input type="radio"/>

Settings Items	CT Policy	User Policy
E-mail sending interruption log	○	○
E-mail attachment prohibition log	○	○
Command log	○	○
Device configuration change log	○	○
Printing operation log	○	○
Printing prohibition log	○	○
Logon prohibition log	○	— (Note)
File export log	○	○
PrintScreen key operation log	○	○
PrintScreen key prohibition log	○	○
Web operation log	○	○
Web operation prohibition log	○	○
FTP operation log	○	○
FTP operation prohibition log	○	○
Clipboard operation	○	○
Clipboard operation prohibition log	○	○
File operation log	○	— (Note)
Logon/Logoff log	○	— (Note)
Linkage log	○	— (Note)
Screen capture	○	○

○: can be set

—: cannot be set

Note: During the client (CT) operation, when the user policy is valid, for the items that cannot be set as user policy, the configuration value of CT policy in the operated the client (CT) is valid.

## Form of Operation and Valid Prohibition/Log Collection

### Citrix XenApp is not available.

After the CT policy and user policy have been set and updated to the client (CT), though operation prohibition and log collection can be performed in the client (CT), the valid prohibition is different from the collected logs according to the form of operation.

The valid items are shown as follows:

In addition, functions may be restricted due to the operating environment. Please refer to “[1.2 Notes Relating to Functions](#)” for details.

Form of operation		When recording the operations of the client (CT) of Systemwalker Desktop Keeper			When recording the operations on Citrix XenApp Server (Note 1)
OS Startup Mode		At normal startup (Logon to Windows after OS has started)	When starting in safe mode or the safe mode with network (Note 3) (Note 5)		At normal startup (Logon to Windows after OS has started)
			Windows Vista® Windows® 7 Windows Server® 2008	Windows® XP Windows Server® 2003	
Prohibition Function	File export prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	Printing prohibition	<input type="radio"/>	—	—	—
	PrintScreen key prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	Logon prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	Application startup prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	E-mail attachment prohibition	<input type="radio"/>	—	<input type="radio"/>	—
	URL access prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	FTP server connection prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	Web upload and download prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	Clipboard prohibition	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
Record Function	Application startup log	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Application termination log	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Application startup prohibition log	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	Window title obtaining log	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Window title obtaining log (with URL)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	E-mail sending log	<input type="radio"/>	—	<input type="radio"/>	—
	E-mail sending interruption log	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	—
	E-mail attachment prohibition log	<input type="radio"/>	—	<input type="radio"/>	—
	Command log	<input type="radio"/> (Note 4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Form of operation		When recording the operations of the client (CT) of Systemwalker Desktop Keeper			When recording the operations on Citrix XenApp Server (Note 1)
OS Startup Mode		At normal startup (Logon to Windows after OS has started)	When starting in safe mode or the safe mode with network (Note 3) (Note 5)		At normal startup (Logon to Windows after OS has started)
			Windows Vista® Windows® 7 Windows Server® 2008	Windows® XP Windows Server® 2003	
	Device configuration change log	○	○	○	—
	Printing operation log	○	—	—	○
	Printing prohibition log	○	—	—	—
	Logon prohibition log	○	○	○	—
	File export log	○	○	○	—
	PrintScreen key operation log	○	○	○	○
	PrintScreen key prohibition log	○	○	○	—
	Web operation log	○	○	○	○
	Web operation prohibition log	○	○	○	—
	FTP operation log	○	○	○	○
	FTP operation prohibition log	○	○	○	—
	Clipboard operation log	○	○	○	○
	Clipboard operation prohibition log	○	○	○	—
	File operation log	○	○	○	○
	Logon/Logoff log	○	○ (Note 2)	○ (Note 2)	○ (Note 2)
	Linkage log	○	○	○	—
	Screen capture	○	○	○	—

○: Valid

—: Invalid.

Note 1: The policy set for Citrix XenApp monitoring is CT policy. The user policy is not set.

Note 2: PC sleep logs and PC restoration logs are not collected.

Note 3: When starting in safe mode or if the network is in safe mode, only the CT policy will be running while the user policy will not be applied.

Note 4: In the Windows Server® 2008 64 bit Edition, Windows Server® 2008 R2, prohibition operations and log collection cannot be performed.

Note 5: When starting in safe mode or safe mode with network, sometimes the operation logs will not be sent to the Management Server before the next normal startup.

## 2.1.2 How to Apply Policy

---

### Timing for Policy Update

The timing for policy updates is as follows:

- CT Policy
  - When the client (CT) is connected to the Master Management Server or Management Server.
  - When CT policy is updated in the Management Console and the [Update Immediately] button is selected.
  - When [Create Policy Application Tool] is used.
  - When the automatic policy acquisition function is running.
- User Policy
  - When logging on as the user that has been registered in the Master Management Server or Management Server.
  - When the [Update] button in the [User Policy Settings] window of the Management Console is selected and logging on with the user that has been registered in the Master Management Server or Management Server
  - When the [Update] button in the [User Policy Settings] window of the Management Console is selected to update CT policy immediately.
    - \* This is only valid for the logged on users.
  - When the automatic policy acquisition function is running.
    - \*This is only valid for the user that is logging on.



.....  
The Automatic Policy Acquisition function is to obtain policy once every day when the client (CT) is installed on a PC that is always running (Example: file server). CT policy and user policy are obtained between 00:30 and 01:30 everyday.  
.....

### Policy Change

The kind of operation will be performed by the system administrator (department administrator) and the client (CT) user and which policy will be valid varies in different cases.

This Department describes the relationship between operation content and valid policy.

To confirm the set policies, please start the Management Console.

After the CT group to which the client (CT) expected to be confirmed belongs has been selected in the CT group tree, if a the client (CT) is selected from the CT list, the CT policy will be displayed in the policy list.

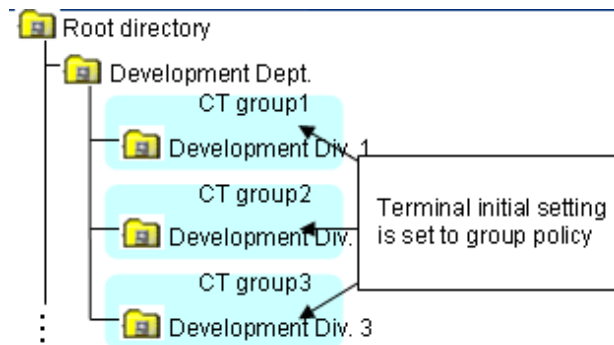
Select the [User Policy Settings] from the [User Settings] menu. After the user group to which the user expected to be confirmed belongs has been selected from in the displayed window, if a user is selected from the user list, the user policy will be displayed in the policy list.

### Relationship between CT Group Policy and CT Policy

1. Create a group.

The value of terminal initial settings is set as the group policy.

But in case of a three-level structure, when creating a CT group in the subordinate Management Server under the Master Management Server by connecting to the Master Management Server, the policy that has been set in the Master Management Server will be set for this CT group.

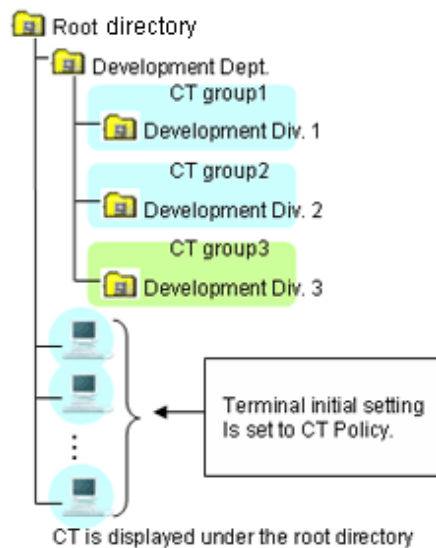


2. Modify the group policy as needed.

The group policy will be modified as follows:

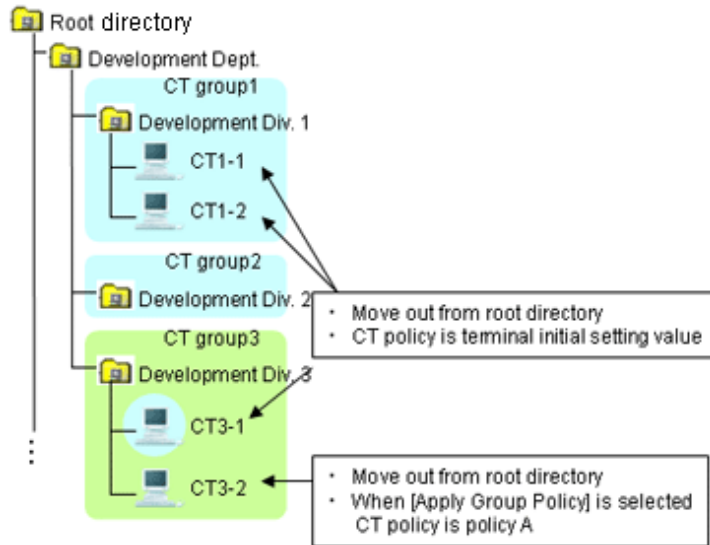
- Modify the group policy of "CT Group 3" from "Terminal Initial Settings Value" to "Policy A".

3. After the CT is installed and the client (CT) has communicated with the Management Server, the terminal initial settings value will be set as CT policy.



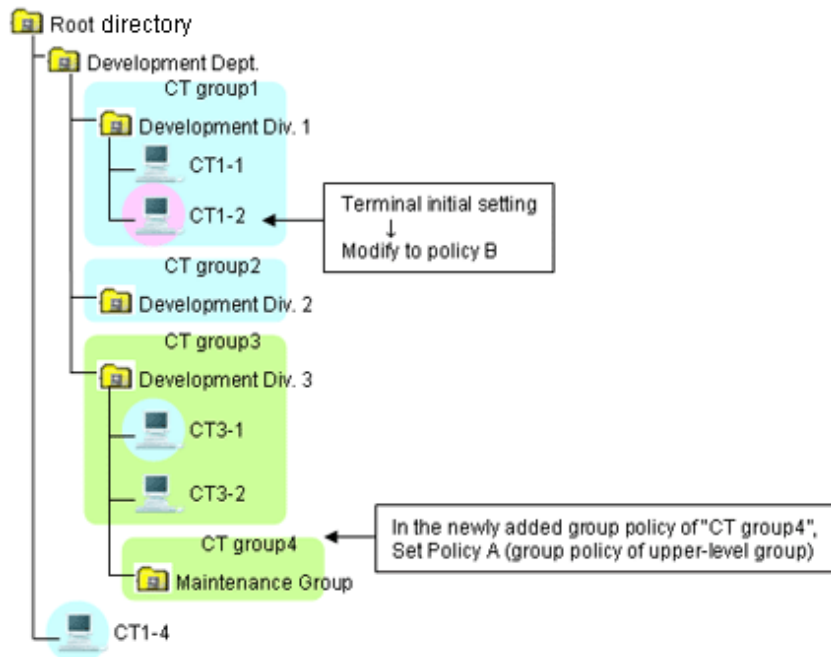
4. Move the client (CT) to each group.

In the CT policy of the client (CT) that is directly moved out from the Root directory, the value of terminal initial settings is set. In the policy of the client (CT) for which "Apply Group Policy" checkbox is selected, the group policy of moving destination will be set.

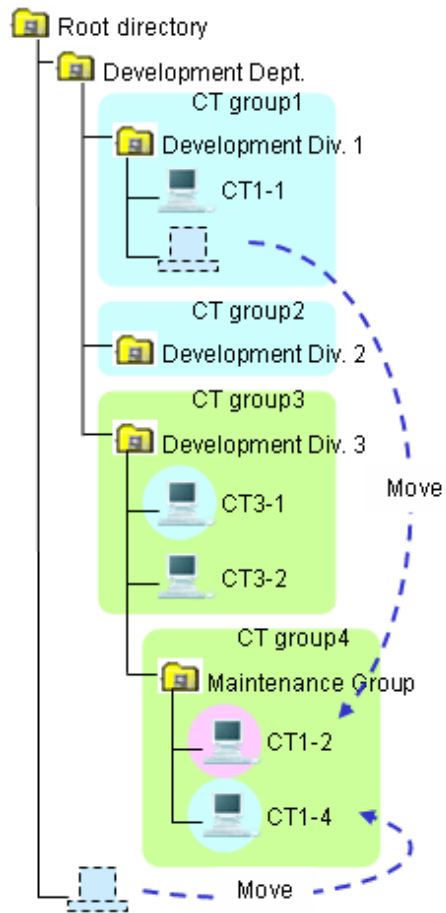


5. Create a sub-group.

In the group policy of the created sub-group, the group policy of the upper class group will be set. In addition, the modified CT policy of "CT1-2" from "Terminal Initial Settings Value" to "Policy B".



6. Move a CT.

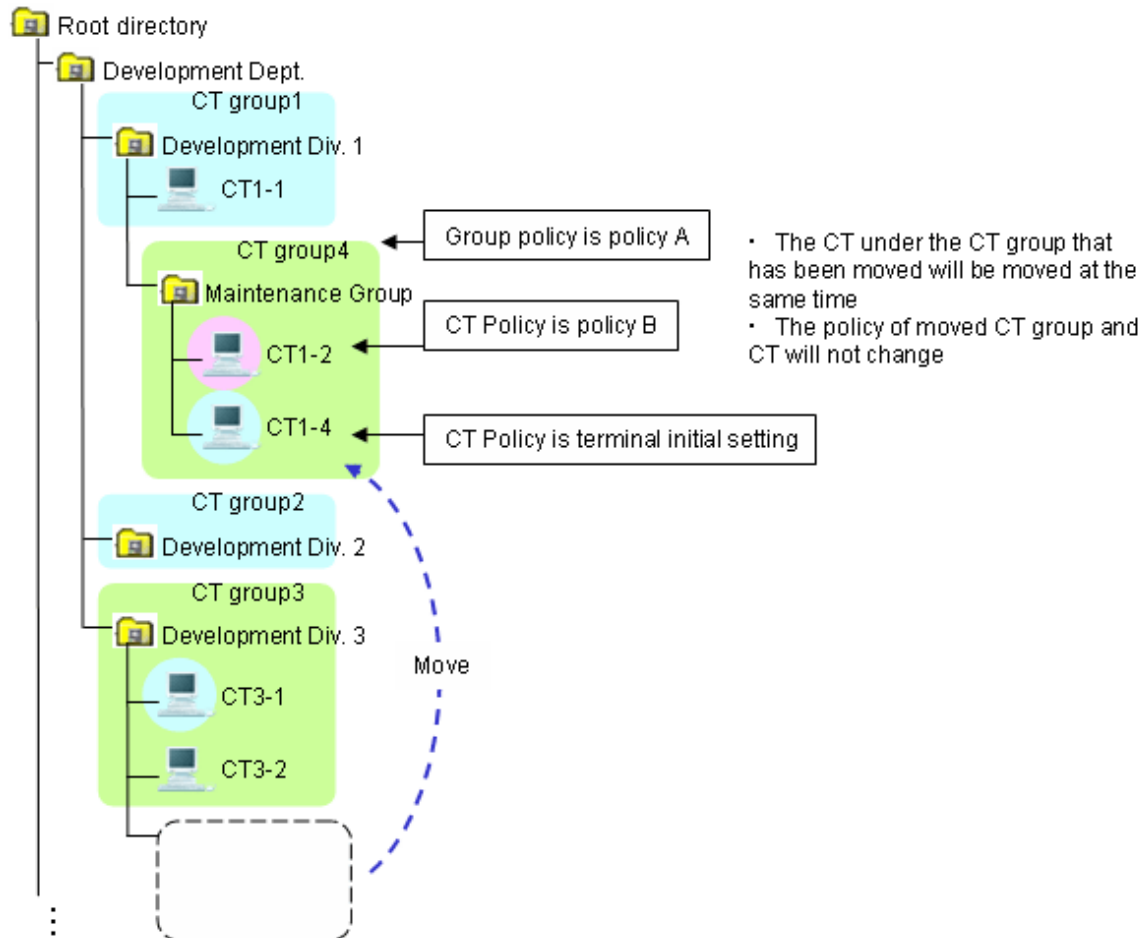




## 7. Move a CT group.

After a CT group is moved, the subordinate CTs will be moved at the same time.

The moved CT group and CT policy will not be modified (it is still the policy before moving).



8. After the “Apply Group Policy” checkbox has been selected, even if the policy of the CT exists under the Root directly is updated immediately, CT policy will still be applied. The settings of “Apply Group Policy” will be invalid.

## Relationship between User Group Policy and User Policy

The relationship between user group policy and user policy is the same as the change of policy described in “Relationship between CT Group Policy and CT Policy”.

## Client (CT) Operation and Valid Policy

This Department describes the policy that become valid during the client (CT) operation when CT policy and user policy are used at the same time.

The application of user policy is judged by the result of confirming whether the user information (user name) has been registered in the Master Management Server or Management Server, based on the user name that is input when logging on to Windows.

In this case, it has nothing to do with domain authentication status and confirmation is performed only according to the user name that is input when logging on to Windows. Therefore, even for the user name without domain authentication, if it is in accordance with the user information (user name) registered in the Master Management Server or Management Server, the user policy of this user information (user name) will be applied.

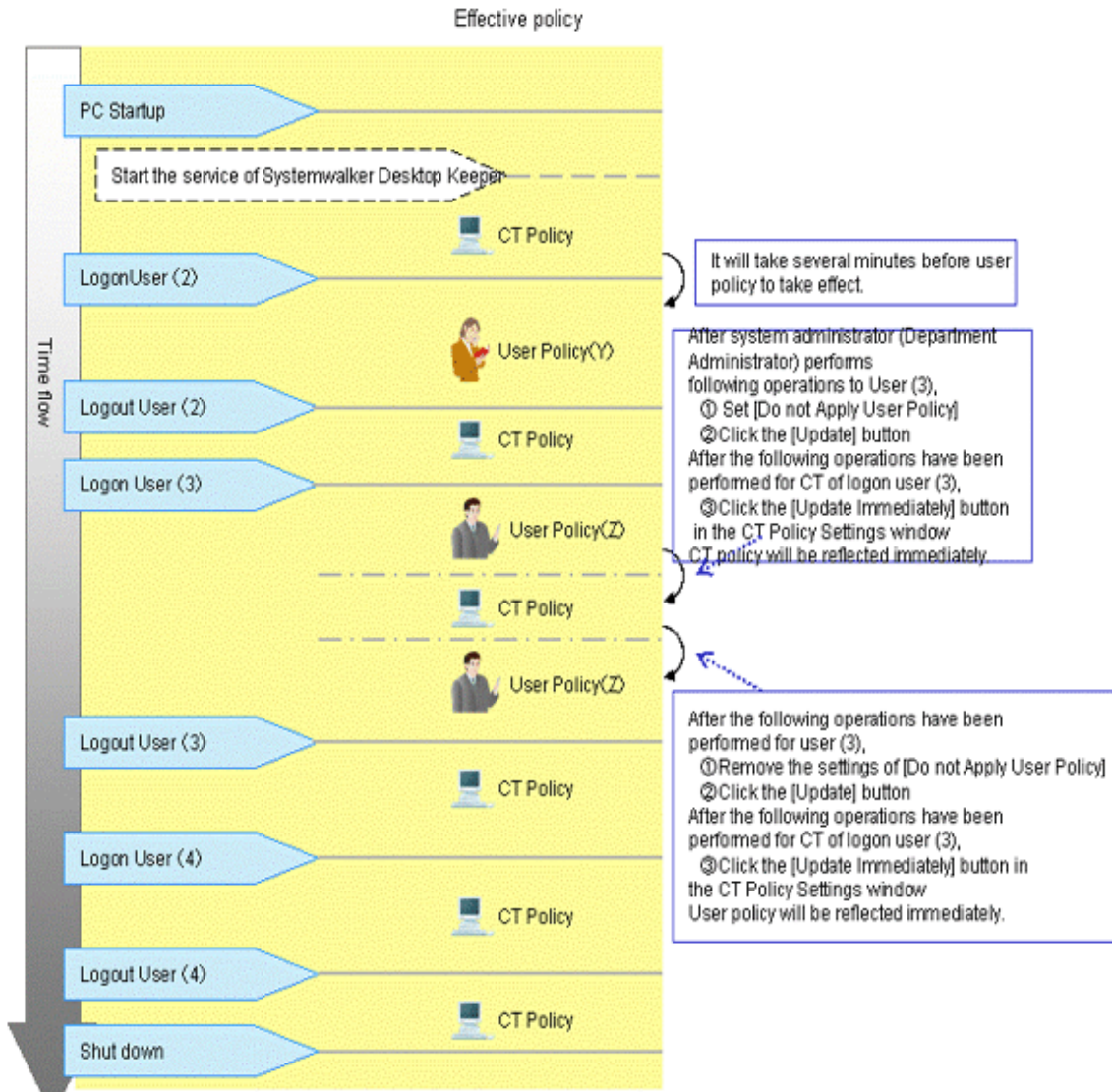
Select three users out of the five from “User (1) to User (5)” to register to the Management Server.

After the user is registered, set the user policy of “User (1)” to “User (3)” as follows:

User Name	User Policy
User (1)	Policy X
User (2)	Policy Y
User (3)	Policy Z

User (4) and User (5) are not registered.

When the client (CT) and Management Server are always online



1. Start the client (CT).

After starting the service of Systemwalker Desktop Keeper, CT policy will take effect. (For the interval from PC startup to the startup of Systemwalker Desktop Keeper service, the settings of CT policy will become invalid.)

2. User (2) logs on to the client (CT).

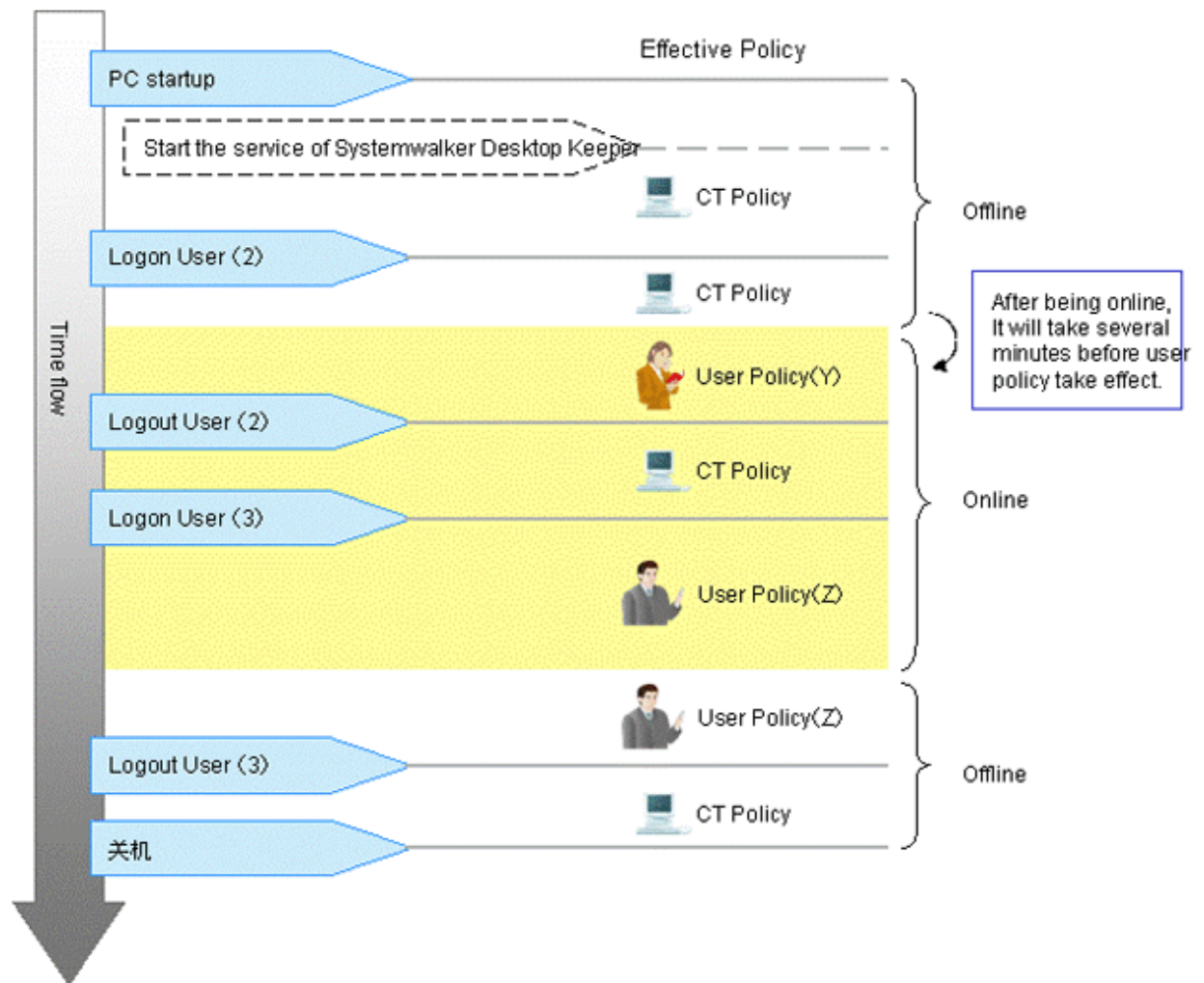
3. User policy (Policy Y) takes effect.

It will take 2 to 3 minutes from the logon to Windows until the user policy is applied. CT policy will be valid before the user policy is applied. User (2) will be logged off.

CT policy will take effect.

4. User (3) logs on to the client (CT).  
User policy (Policy Z) will take effect.
  - a) In the [User Policy Settings] window, after setting [Not Using User Policy] for User (3), the system administrator (department administrator) will click the [Update] button.
  - b) Then for the client (CT) to which the User (3) logs on, click [Update Immediately] in the CT policy settings window after the Management Console has been started.  
→CT policy is updated immediately.
  - c) In the [User Policy Settings] window, after canceling the settings of [Do not Apply User Policy] for User (3), the system administrator (department administrator) will click the [Update] button.
  - d) Then for the client (CT) to which the User (3) logs on, click [Update Immediately] in the CT policy settings window after the Management Console has been started.  
→User policy (Policy Z) is updated immediately.
5. User (3) will logoff.
6. CT policy will take effect.
7. User (4) logs on to the client (CT).
8. CT policy will be valid.  
When the user that has not been registered has logged on, operate with CT policy.
9. User (4) will logoff.  
CT policy will be valid.

When the client (CT) and Management Server are not always online



1. Start the client (CT) when it is offline.

After the service of Systemwalker Desktop Keeper has been started, CT policy will take effect. (For the interval from PC startup to the startup of Systemwalker Desktop Keeper service, the settings of CT policy will become invalid.)

2. User (2) logs on to the client (CT).

As the client (CT) cannot get user information from Management Server when it is offline, CT policy will take effect.

When it becomes online during the logon process, user policy (Policy Y) will take effect. It will be 2 to 3 minutes from offline till the user policy is applied.

3. User (2) will logoff.

CT policy will take effect.

4. User (3) logons to the client (CT).

User policy (Policy Z) will take effect.

When it becomes offline during the logon process, the user policy will still be valid.

5. User (3) will logoff.

CT policy will take effect.

## 2.2 Flow of Preparing Operating Environment

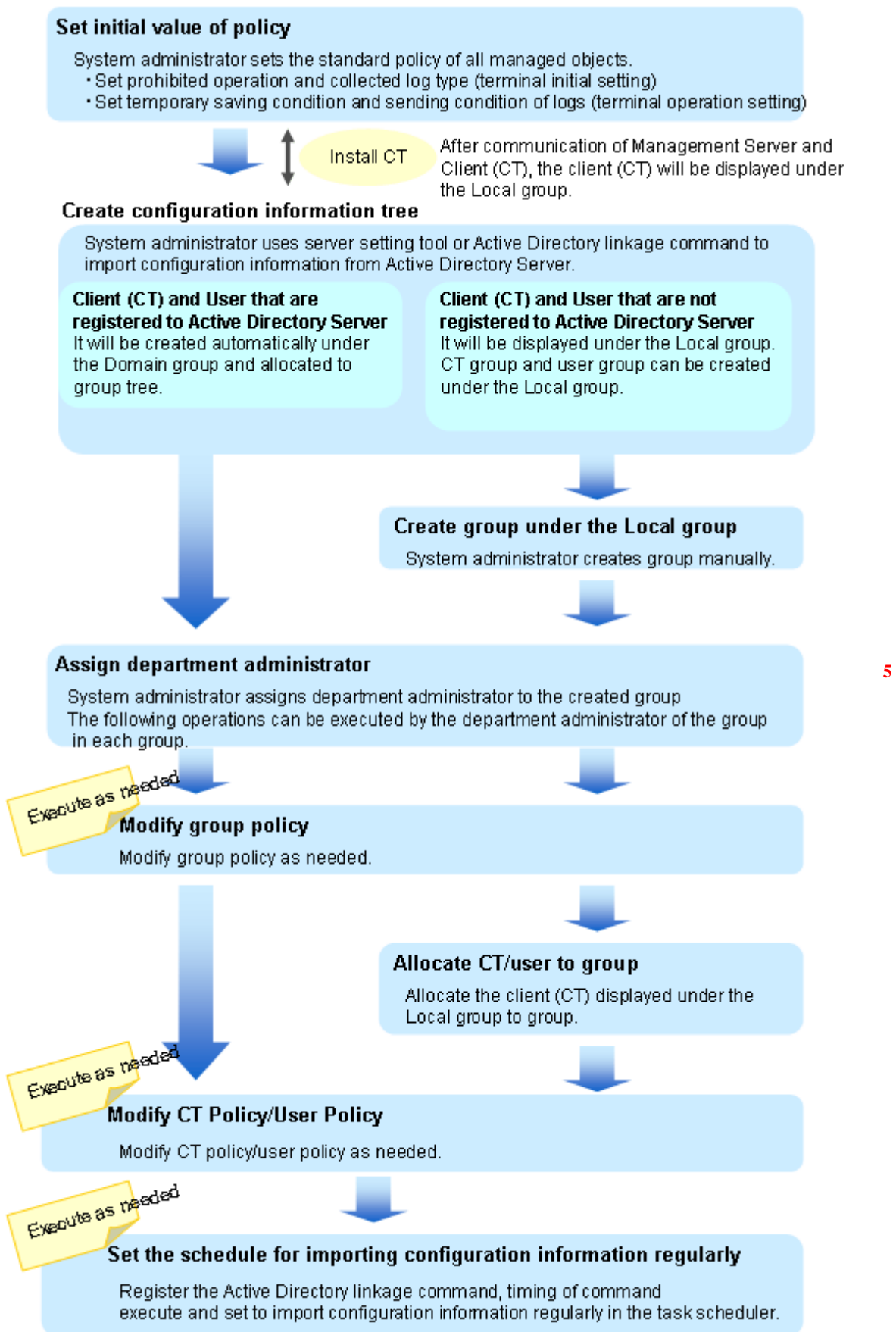
---

The operation flow from completing the installation of Systemwalker Desktop Keeper until the client (CT) operations can be audited is shown as follows:

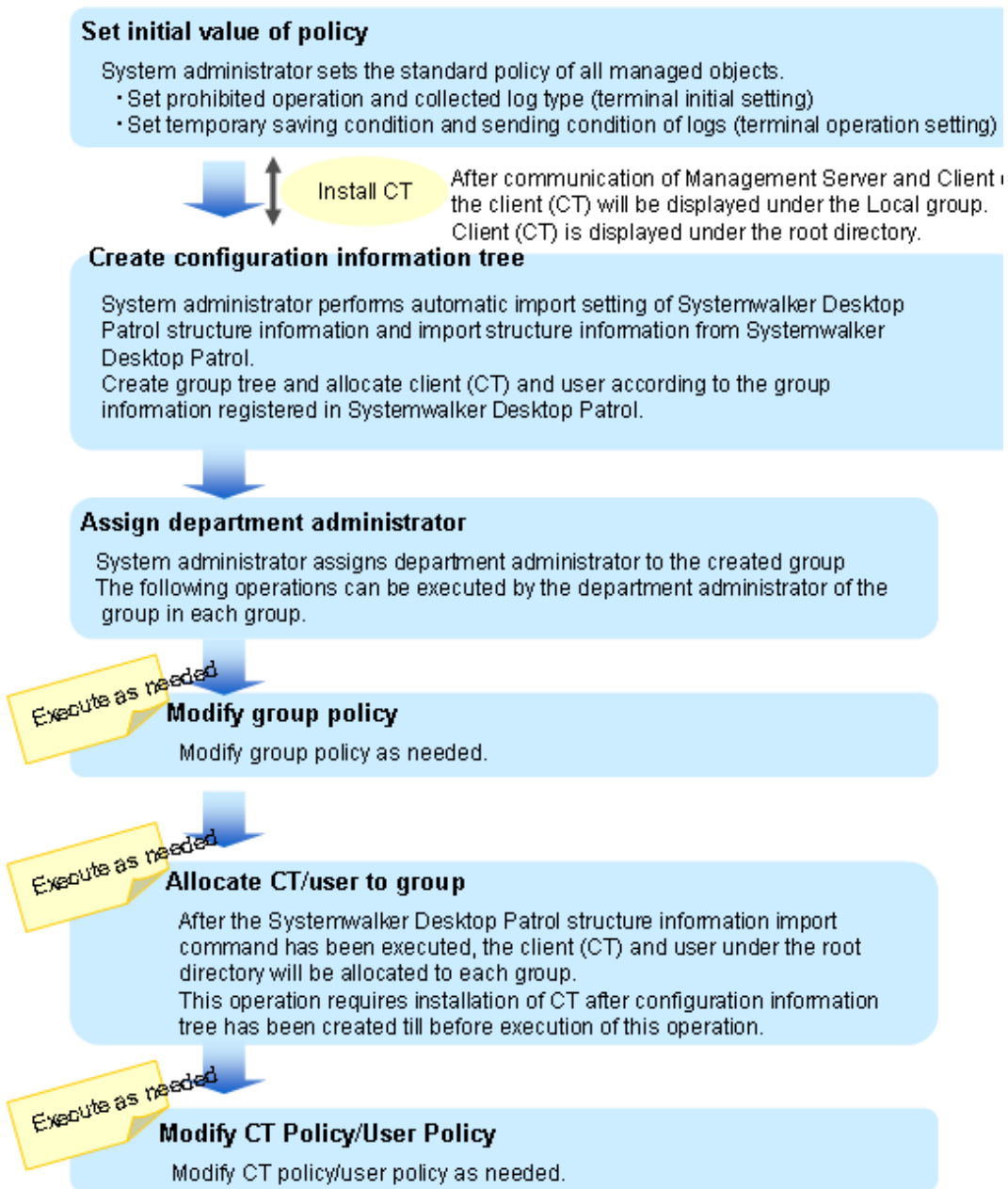
The flow varies upon the method of creating configuration information tree.

- [When importing configuration information from active directory](#)
- [When importing configuration information from Systemwalker Desktop Patrol](#)
- [When creating configuration information with Management Console](#)

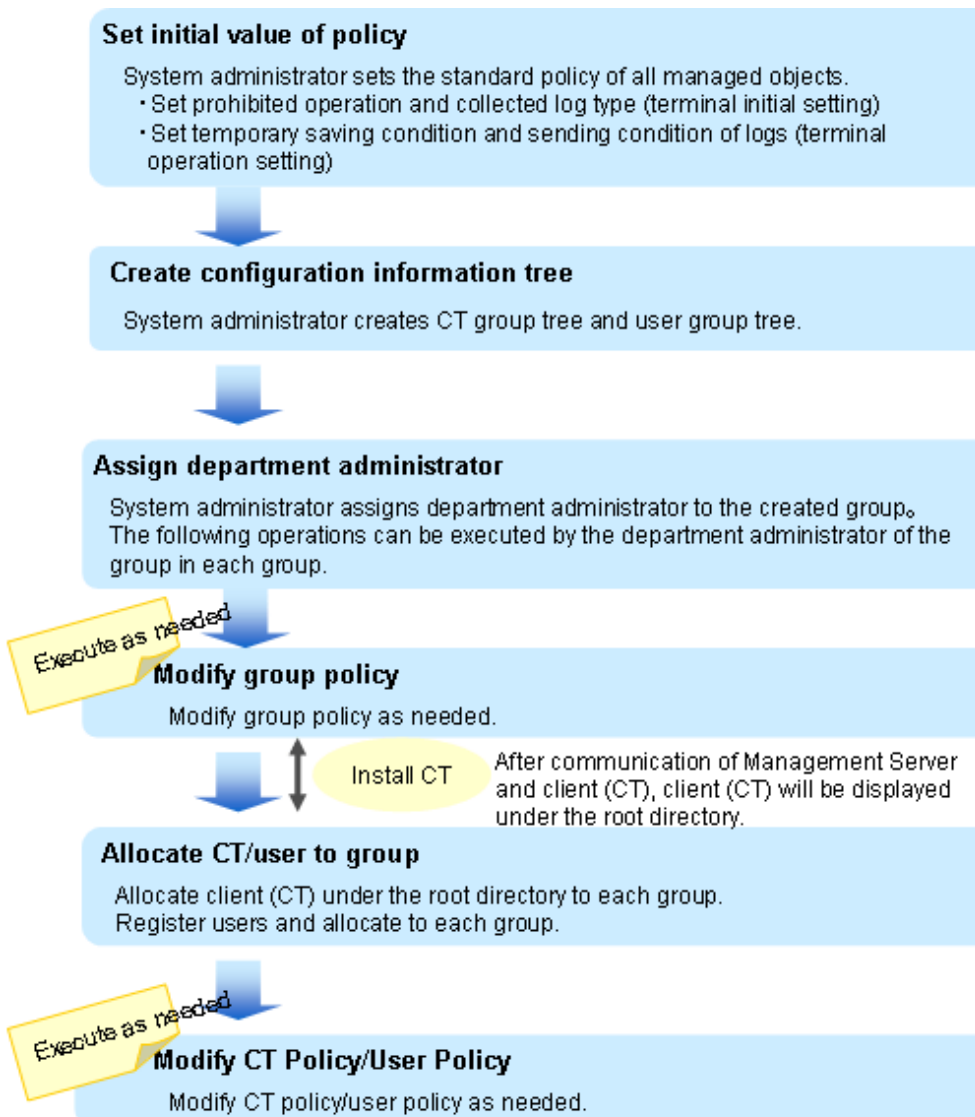
## When importing configuration information from active directory



## When importing configuration information from Systemwalker Desktop Patrol



## When creating configuration information with Management Console



## 2.3 Start Management Console

### Start Management Console



Note

#### For preventing incorrect modification of policy

When leaving the PC installed with the Management Console after starting the Management Console, please close the Management Console to prevent the incorrect modification of policy settings.

#### For reducing the startup time of Management Console



When there are many CT number of sets to be managed (about more than 2000), the startup time of the Management Console will be delayed. By setting [Get Latest Information at Startup] of the Management Console to [Get from Master Management Server], delay can be avoided.

These settings will become valid when the Management Console is connected to the Master Management Console.

---

1. Select [Programs] - [Systemwalker Desktop Keeper] - [Management Console] - [Management Console] from the [Start] menu of the PC with the Management Console installed.

→ The [Systemwalker Desktop Keeper - Management Console] window is displayed.



2. Enter the following information and click the [OK] button.

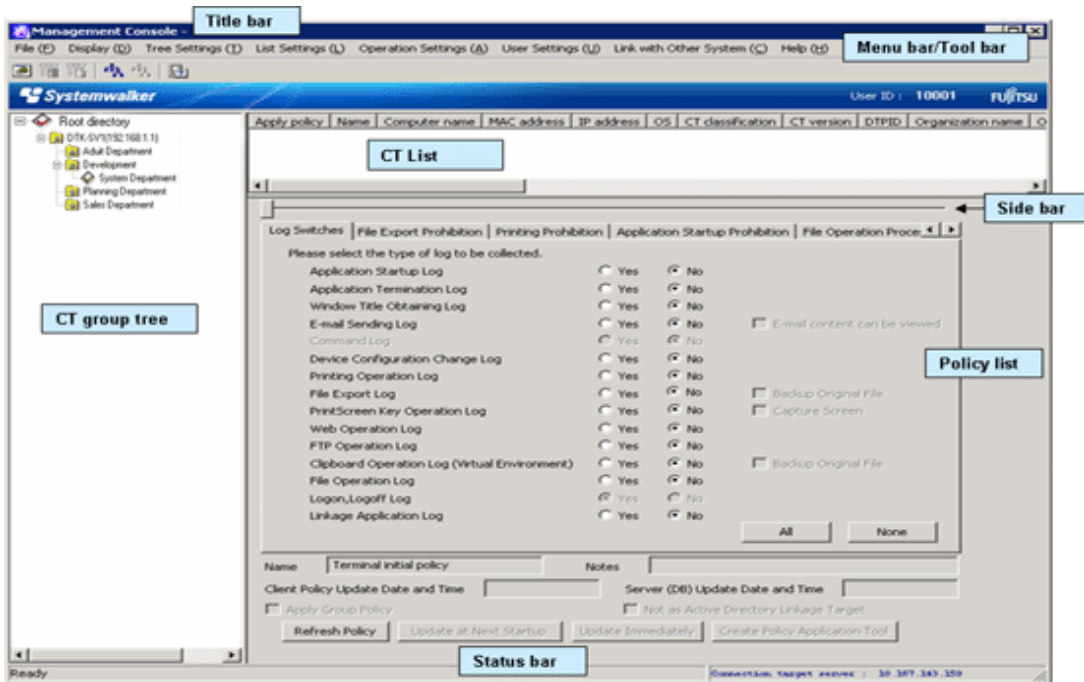
The login method of the system administrator is the same as that of a department administrator.

- [Connection Target Server Name]: Select the IP address or computer name of the Management (Master Management) Server to be connected
- [User ID]: It is the [User ID] set in the [Administrator Information Settings] window of the Server Settings Tool.
- [Password]: it is the [Password] set in the [Administrator Information Settings] window of the Server Settings Tool.

It is recommended to modify password regularly. Please refer to “[Modify Password at Startup of Management Console](#)” for how to do so.

→ The [Management Console] window is displayed.

The information displayed in the window and menu bar varies upon the logon status of the system administrator and department administrator.



## Displayed Content of Window

This Department describes the name of each part of the [Management Console] window.

## CT Group Tree

The CT group information imported by Active Directory Linkage and the created CT group are displayed.

When confirming the latest information of CT group tree, select [Refresh Tree (All Servers)] from the [Tree Settings] menu.

When [Unfold All Trees] is selected from the [Tree Settings] menu, all CT groups will be displayed.

When [Fold All Trees] is selected from the [Tree Settings] menu, only the CT groups under the Root directory (only the CT groups under server is displayed when server is displayed and only the CT group under domain is displayed when domain is displayed) will be displayed.



When a CT group is selected, the latest CT policy set by CT group will be displayed.












The server name displayed in the CT group tree is the value that has been set in [Computer Name] of the [Server Information Settings] window of the Server Settings Tool.

## Icons relating to CT group tree

The icons displayed in the CT group tree vary depending upon the person who logs on to the Management Console and the execution status of Active Directory Linkage.

The following describes the conditions for displaying each icon.

Personnel Logon to Management Console	Active Directory Linkage Status	Displaying Symbol	Meaning of Icons
System Administrator	When Active Directory Linkage is performed		Indicates the group for which the department administrator has been set.
			Indicates the group for which the department administrator has been set.

Personnel Logon to Management Console	Active Directory Linkage Status	Displaying Symbol	Meaning of Icons
	When Active Directory Linkage is not performed or in case of the local group during Active Directory Linkage		Indicates the group for which the department administrator has been set.
			Indicates the group for which the department administrator has not been set.
	—		Indicates the “Deleted” group.
	—		Indicates the “Not Configured” group.
department administrator	When Active Directory Linkage is performed		Indicates the group which has been set as the department administrator.
			Indicates the group which is not set as the department administrator.
			Indicates CT group which has been set so the department administrator exists in the sub-group under that group.
	When Active Directory Linkage is not performed or in case of the local group during Active Directory Linkage		Indicates the group which has been set as the department administrator.
			Indicates the group which is not set as the department administrator.
			Indicates CT group which has been set so the department administrator exists in the sub-group under that group.
	—		Indicates the “Not Configured” group.

#### CT list

The PC on which the CT is installed is displayed. The items displayed in the CT list are as follows:

Item Name	Description
[Apply Policy]	The policy applied to the client (CT) is displayed. - [CT]: indicates the CT policy has been set. - [Group]: indicates the CT group policy has been set.
[Name]	This refers to a name that can be given to the client (CT) and the initial value is computer name. Please refer to “ <a href="#">Modify CT Policy</a> ” during modification and it is executed in the CT policy settings window after Management Console is started. After the client (CT) has been installed, even the computer name of the client (CT) is modified, the name will remain unchanged.
[Computer name]	This refers to the computer name of the client (CT).
[MAC address]	This refers to the MAC address of the client (CT).
[IP address]	This refers to the IP address of the client (CT).
[OS]	Operating system name of the client (CT).
[CT classification]	This is displayed as [SE] when the client (CT) is in Standard Edition.

Item Name	Description
[CT version]	This refers to the version of installed Systemwalker Desktop Keeper client (CT). In addition, please refer to “CT Version” of “Systemwalker Desktop Keeper Reference Manual” for correspondence of Version/Edition of product.
[DTPID]	This refers to “User ID (+) PC Name” of Systemwalker Desktop Patrol client (CT).  It indicates the client (CT) of Systemwalker Desktop Keeper and the client (CT) of Systemwalker Desktop Patrol are installed in the same computer.
[Organization name]	This refers to the organization name set in the OS of the client (CT).
[Owner name]	This refers to the owner name set in the OS of the client (CT).
[Subnet mask]	This refers to the subnet mask set in the OS of the client (CT).
[Link with Active Directory]	Whether the client (CT) imports information by linking with Active Directory can be displayed.  <ul style="list-style-type: none"> <li>- When the client (CT) imports information by linking with Active Directory: (Blank)</li> <li>- When the client (CT) imports information by other methods apart from linking with Active Directory: [Non-target] is displayed</li> </ul>
[Network participation status]	The network participation status of the client (CT) is displayed.  <ul style="list-style-type: none"> <li>- [Domain]: It is displayed when it belongs to a domain.</li> <li>- [Group]: It is displayed when it does not belong to domain.</li> </ul>
[Affiliated domain name]	The affiliated domain of the client (CT) can be displayed. When [Network Participation Status] is [Group], the group name will be displayed.
[Last logon date and time]	When the client (CT) is started, it communicates with the Master Management Server or Management Server. This refers to the deadline for the server to execute the following operations in the client (CT) during the communication.  <ul style="list-style-type: none"> <li>- Send CT policy</li> <li>- Send user policy</li> </ul>
[Date and time of client policy update]	This refers to the final date and Time when the Management Server or Master Management Server sends CT Policy to the client (CT). it will be displayed or updated in following cases:  <ul style="list-style-type: none"> <li>- When the client (CT) added to the CT list is restarted and starts to communicate with the Master Management Server or Management Server.</li> <li>- When the CT policy is reflected in the client (CT) after clicking [Update Immediately] button of the Management Server.</li> </ul>
[Date and time of server (DB) update]	This refers to the final date and Time when the Management Server or Master Management Server updates the policy of the client (CT) and reflects to the database (including immediate update).
[Notes]	This refers to the information entered when the policy of the client (CT) is reflected.  Please refer to “ <a href="#">Modify CT Policy</a> ” during modification.
[Trace conditions]	This refers to the settings that are traced and collected in the client (CT).  <ul style="list-style-type: none"> <li>- [Summary]: Collect the summary of content traced by the client (CT).</li> </ul>

Item Name	Description
	<ul style="list-style-type: none"> <li>- [Details]: The details traced by the client (CT) are collected by levels.</li> <li>- Blank: When the trace content is not collected or the client (CT) is V12.0.</li> </ul>
[DTP version]	This is the version of Systemwalker Desktop Patrol CT installed in PC.
[Virtual PC]	<p>When installing the client (CT) in the virtual environment, it is displayed as follows:</p> <ul style="list-style-type: none"> <li>- [- (Main)]: When it is the master image of the virtual PC.</li> <li>- [-]: When it is the virtual PC.</li> </ul>

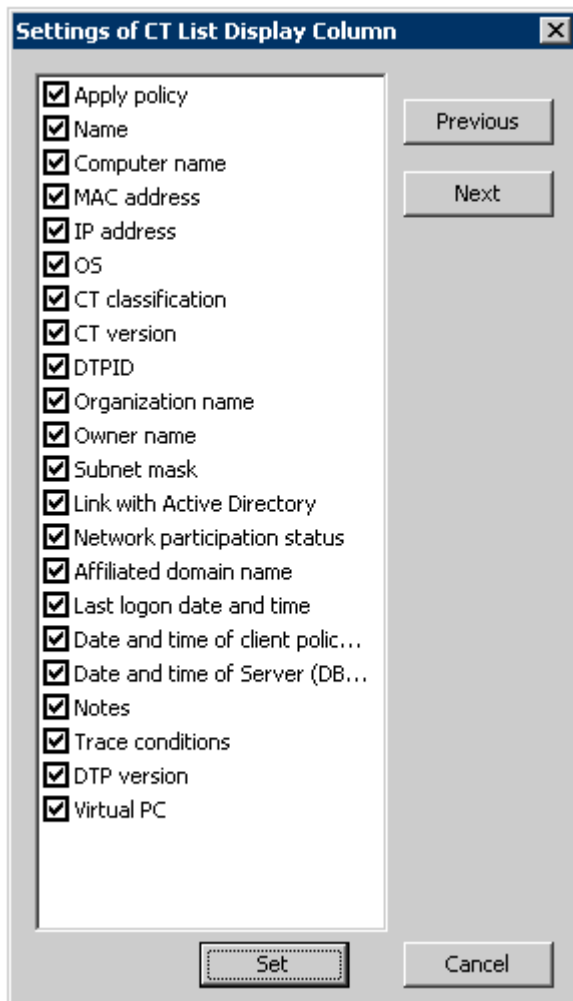
When it is required to confirm the information in the latest CT list, perform the following operations:

- When confirmation is performed by the CT,  
Select a CT from the CT list. At the moment, the CT policy will be updated.
- When updating information for all CTs,  
Select [Refresh Tree (All Servers)] from the [Tree Settings] menu.
- When updating information of all subordinate CTs in the selected Management Server,  
Select [Refresh Tree (Selected Servers)] from the [Tree Settings] menu.

The items displayed in the CT list and sequence of display can be modified. The procedure is as follows.

When modifying the displayed items and sequence

1. Start the [Management Console] window.
2. Select [Setting of CT List Display Column] from the [List Settings] menu.  
→ The [Settings of CT List Display Column] window is displayed.



3. Select the checkbox displayed in the CT list.
4. Select the item that requires modification of display sequence by clicking the [Up] or [Down] button.
5. After all operations have been completed, click the [Set] button.

→The visible columns in the CT list are updated.

#### When modifying the display sequence temporarily

The items in the CT list can be moved by drag-and-drop operation. When the Management Console is started at the next time, it will still return to the display sequence before moving.

#### Slide bar

This is the window for switching each tab of the policy list.

By dragging the slide bar, each window can be switched in sequence. After stopping the drag and drop, the window of neighbor tabs will be displayed.

By clicking the slide bar, each window can be switched in order.

#### Policy List

This displays the policies that have been set.

Please refer to “[2.4.1 Perform Terminal Initial Settings](#)” for details of how to set the policy list.

### Status bar




This displays the name of specified target server when the Management Console is started.



### Title bar

This displays the group name and level of the selected CT or CT group.


### Menu bar/Tool bar

This describes the menu bar and toolbar of [Management Console] window.

	Menu Bar	Toolbar	Function Summary
File	[Search CT/CT Group]	-	Display the client (CT)/CT group search window .
	[Create CT Group]	-	Display the CT group creation window.
	[Delete CT Group]	-	Display the CT group deletion window. When the selected CT group does not exist in the client (CT) or CT group, the menu cannot be selected.
	[Set Department Administrator of CT Group]	-	Display the administrator registration window. When the department administrator logs on, the menu cannot be selected.
	[Export CT Information in CSV Format]	-	Display the [Specify a CSV File to Export CT Information] window.
	[Export CT Group Information in CSV Format]	-	Display the [Specify a CSV File to Export CT Group Information] window.
	[Import Department Administrator of CT Group in CSV Format]	-	Display the [Specify a CSV File to Import department administrator Information of CT Group] window.
	[Export Department Administrator of CT Group in CSV Format]	-	Display the [Specify a CSV File to Export department administrator Information of CT Group] window.
	[Collect Remote Material]	-	Collect the data used for trouble investigation of the selected client (CT).
	[CT Debugging Trace]	-	Set the collection conditions of trace logs in the selected client (CT).
	[Output IP Address of Subordinate CT]	-	Output the file that records the IP address of subordinate clients (CTs) (including the subordinate unit of group) under the selected CT group.
	[Change Password]	-	Modify password at the startup of the Management Console.
[Exit]	-	Close the Management Console.	
[Display]	[View/Set Terminal Information]		Display the View/Set Policy window.
	[Get/Control Service List]		Display the Get/Control Service List window.
	[Get/Control Process List]		Display the Get/Control Process List window.

Menu Bar		Toolbar	Function Summary	
[Policy Settings]	[Refresh Tree (All Servers)]		Refresh the level status of CT group tree for all subordinate servers of Master Management Server.	
	[Refresh Tree (Selected Servers)]	-	Refresh the level status of CT group tree for the selected server in the CT group tree of the Management Console connected to the Master Management Server. Only one set of server can be selected.	
	[Unfold All Trees]	-	Display all CT groups.	
	[Fold All Trees]	-	Display only the CT group under the Root directory (display only the CT group under server when server is displayed and only the CT group under domain when domain is displayed).	
	[Do not Display Empty Group]	-	Do not display the CT group under which no client (CT) or CT group is registered.	
	[Reflect CT Group Structure]		Save the level status of CT group tree.	
	[Display Server]	-	Display the connected Management Server in the tree. As the server is always displayed when Active Directory Linkage is performed, the selection of the [Display Server] checkbox cannot be cancelled.	
	[Display "Deleted CT" Group]	-	Display the "Deleted CT" group in configuration information tree. The "Deleted CT" group is displayed when the [Display Server] checkbox is selected. When Active Directory Linkage is performed, the "Deleted CT" group will be displayed as the last group under the Local group. When Active Directory Linkage is not performed, the "Deleted CT" group will be displayed as the last group under the server.	
[List Settings]	[Setting of CT List Display Column]	-	Display the window for the settings of CT list display column.	
[Operation Settings]	[Terminal Initial Settings]	-	Display the Terminal Initial Settings window.	
	[Terminal Operation Settings]	-	Display the Terminal Operation Settings window.	
	[USB Device Registration]	-	Display the USB Device Registration window. In a 3-level structure system, the menu cannot be selected in the Management Console of a Management Server that is not connected to the Master Management Server.	
	[Get Latest Information at Startup]	[Get from Lower Level Management Server]	-	When the Management Console connected to the Master Management Server is started, the latest configuration information will be obtained through the lower level Management Server and the information will be displayed in the window.
		[Get from Master]	-	When the Management Console connected to the Master Management Server is started, data inquiry and data synchronization will be performed for the lower level Management



Menu Bar		Toolbar	Function Summary	
	Management Server]		Server. The information that is currently saved by the Master Management Server will be displayed in the window.	
	[Debugging Trace]	[No]	-	Close the trace of server service/level control service/administrator E-mail notification function.
		[Summary]	-	Set the trace mode of server service/level control service/administrator E-mail notification function to [Summary].
		[Details]	-	Set the trace mode of server service/level control service/administrator E-mail notification function to [Detail].
	[Management Console Trace]	[No]	-	Close the trace of the Management Console.
		[Summary]	-	Set the trace mode of the Management Console to [Summary].
		[Details]	-	Set the trace mode of the Management Console to [Detail].
[User Settings]	[User Policy Settings]	-	Display the [User Policy Settings] window.	
[Link with Other System]	[Link with Systemwalker Desktop Patrol]	[Import Structure Information]	-	Display the configuration information Import window. When the department administrator logs on or Active Directory Linkage is performed, it cannot be selected.
		[Export Structure Information]	-	Display the Configuration Information Export window. When the department administrator logs on or Active Directory Linkage is performed, it cannot be selected.
[Help]	[Online Help]			Display the online manual.
	[Version information]	-		Display the copyright information and version information.

### Display server

After the “Display Server” checkbox of “Tree Settings” is selected in the Management Console connected to Master Management Server, the computer name and IP address of the connected Master Management Server and Management Server will be displayed, and the CT group will be displayed on each server.

As the server is always displayed during Active Directory Linkage, the selection of [Display Server] checkbox cannot be cancelled.

**[When [Display Server] is not selected (when Active Directory Linkage is not performed)]**



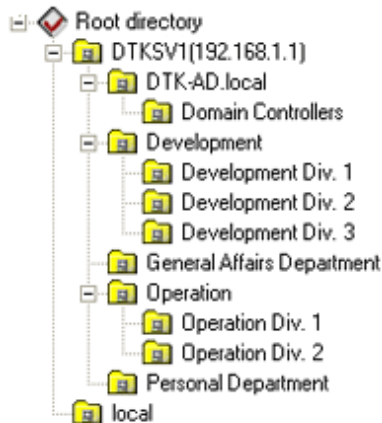
**[When [Display Server] is selected (when Active Directory Linkage is not performed)]**



### Display domain

When Active Directory Linkage, the server name and domain name will be displayed at all times, and they cannot be hidden.

#### [Example of domain display when linking with Active Directory]



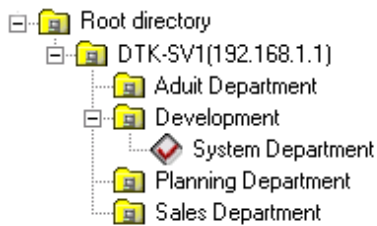
### Display “Deleted CT” group

After [Tree Settings]-[Display Server] of the Management Console is selected, the “Deleted CT” group (when the [Display Server] checkbox is not selected, the [Display “Deleted” Group] checkbox cannot be selected.) will be displayed when [Display “Deleted” Group] of [Tree Settings] is selected.

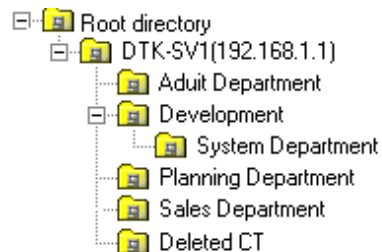
The following is an example when Active Directory Linkage is not performed.

When Active Directory Linkage is performed, the “Deleted CT” group will be displayed under the Local group.

#### [Display “Deleted CT” group is not selected]



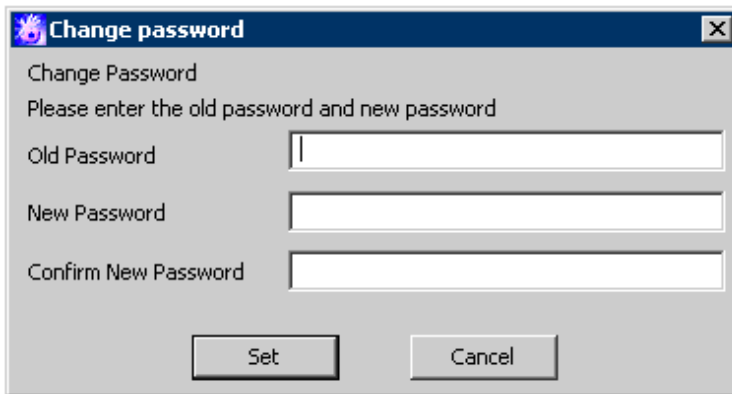
#### [Display “Deleted CT” group is selected]



## Modify Password at Startup of Management Console

1. Start the Management Console.

2. Select [Change Password] from the [File] menu.  
→ The [Change Password] window is displayed.



3. Enter the following information and click the [Set] button.
  - [Old Password]: Enter the password previous used.
  - [New Password]: Enter the new password with 1-32 characters of single-byte alphanumeric characters or single-byte symbols. But "&", "\", ":", "?", ":", "~", "^", "'", "<", ">", "|" and space cannot be used. In addition, it is case-sensitive.
  - [Confirm New Password]: Re-enter the new password .
4. Click the [Set] button in the displayed confirmation window.  
→ Password change is completed.

## 2.4 Set Initial Value of Policy

---

The standard policy in line with the system operation policy of all managed targets will be set as the initial value.

### 2.4.1 Perform Terminal Initial Settings

---

Set the conditions of prohibiting client (CT) operation and collected logs in the terminal initial settings.

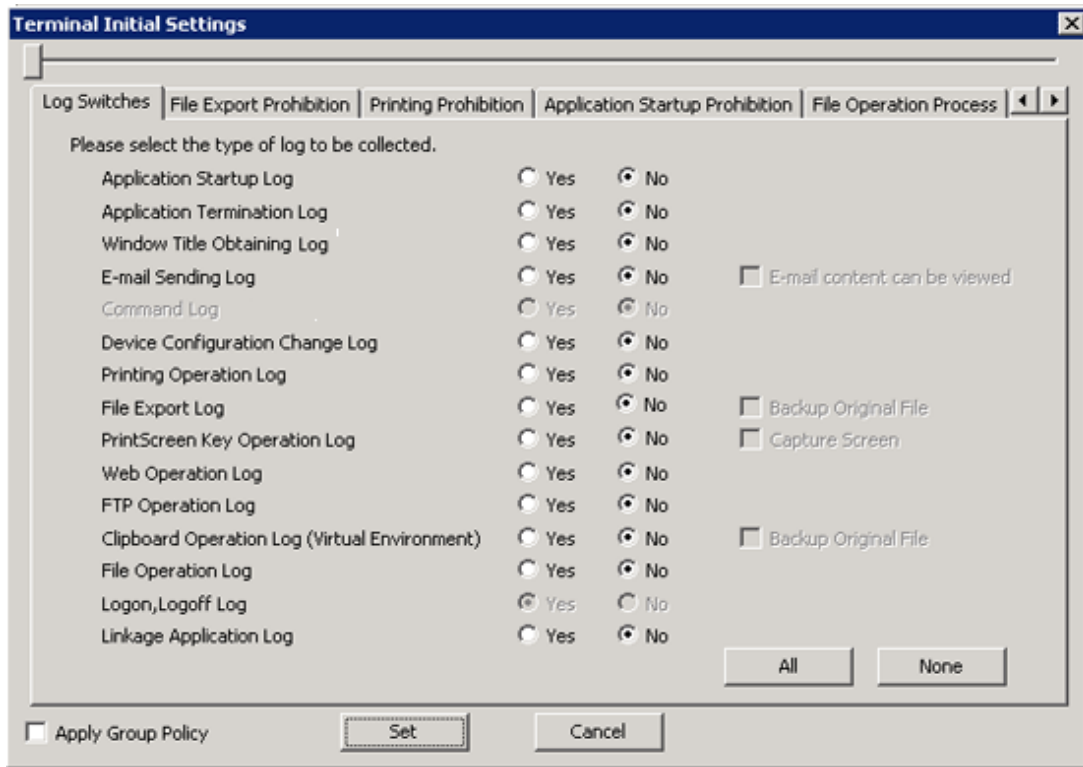
In a 3-level system structure, please perform terminal initial settings in each the Management Server (even if the terminal initial settings is performed in the Master Management Server, it cannot be reflected to a Management Server).

The procedure is as follows:

1. Start [Management Console]

2. Select [Terminal Initial Settings] from the [Operation Settings] menu.

→The [Terminal Initial Settings] window is displayed.



Item Name	Description
[Apply Group Policy]	<p>When registering a new CT or creating a user, set whether to apply the policy of the group to which it belongs as its CT policy or user policy .</p> <p>When it is selected: The group policy of the group to which it belongs will be applied . .</p> <p>When it is not selected: <b>(Initial Value)</b> The group policy of the group to which it belongs will not be applied.</p> <p>For the CT or user under the Root directory, the settings are invalid.</p>

3. After setting policy for each tab, click the [Set] button.

When modifying the set terminal initial settings value (when setting the policy item added because of version upgrade/edition upgrade, or modifying the terminal initial settings value in the operation process), the policy should be updated for the CT after clicking the [Set] button.

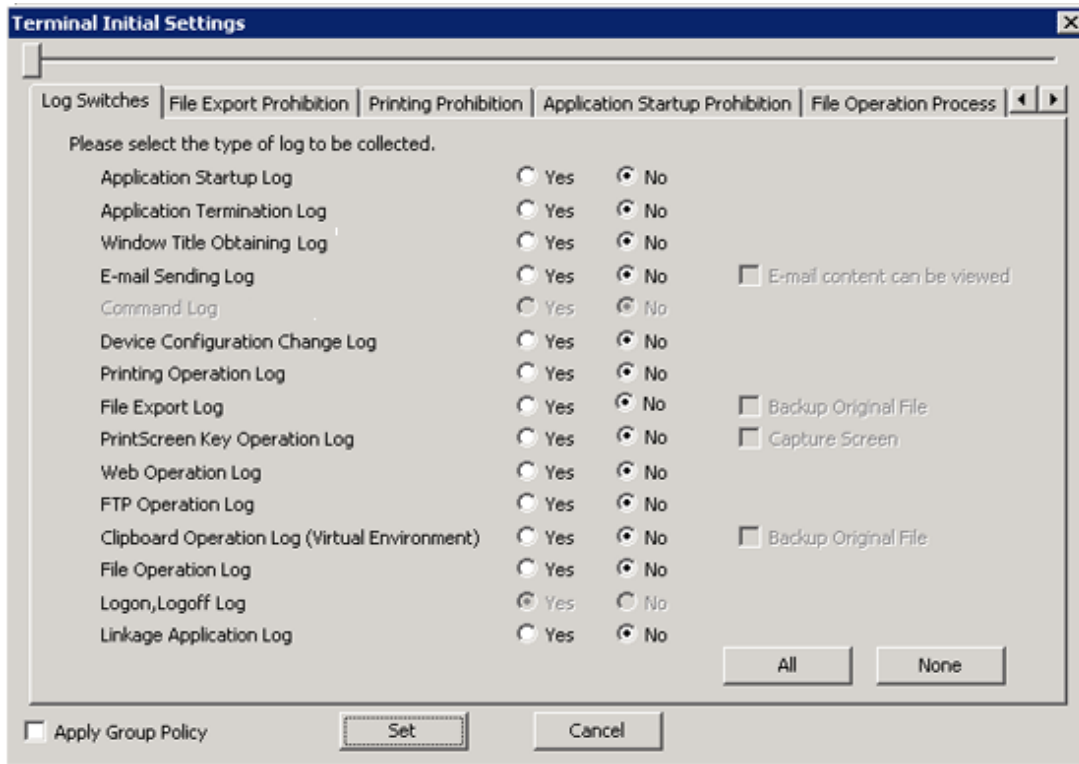
Please refer to “[Modify CT Policy](#)” or “[3.4.2 Modify User Policy](#)” for the policy reflection operation.

The following Department describes the settings in each tab.

### 2.4.1.1 Settings of [Log Switches] Tab

Whether to collect various logs can be set in the [Log Switches] tab. When it is set to “Yes”, the operation logs in the client (CT) will be collected.

The settings in [Log Switches] tab are described.



Item Name	Description
[Application Startup Log]	Application startup logs will be collected. <b>Initial Value:</b> [No] is selected.
[Application Termination Log]	Application termination logs will be collected. <b>Initial Value:</b> [No] is selected.
[Window Title Obtaining Log]	Window title logs at startup of window application will be collected. <b>Initial Value:</b> [No] is selected.
[E-mail Sending Log]	E-mail sending logs will be collected. <b>Initial Value:</b> [No] is selected.
[E-mail content can be viewed]	This can be set when [E-mail Sending Log] is "Yes".  When it is selected: When the E-mail sending log or E-mail sending interruption log is collected, the sent E-mail content and attachment will be saved. The authorized administrator can view the content of the sent E-mail and attachment.  When it is not selected: <b>(Initial Value)</b> The content of the sent E-mail content and attachment will not be saved, so the contents of sent E-mail and attachment cannot be viewed.
[Command Log] <b>(This function is not available)</b>	The logs of command and command result input in the command prompt will be collected. <b>Initial Value:</b> [No] is selected.
[Device Configuration Change Log]	Device configuration change logs will be collected. <b>Initial Value:</b> [No] is selected.
[Printing Operation Log]	Printing logs will be collected. <b>Initial Value:</b> [No] is selected.  When "Yes" is selected, input can be performed in the following tab:  - [Eco Monitoring Settings] Tab

Item Name	Description
[File Export Log]	Logs during file export with File Export Utility will be collected. <b>Initial Value:</b> [No] is selected.
[Backup Original File]	This can be set when the [File Export Utility] option is "Yes".  When it is selected: The original file of the file exported by File Export Utility will be backed up.  When it is not selected: <b>(Initial Value)</b> The original file of the file exported by File Export Utility will not be backed up.
[PrintScreen Key Operation Log]	PrintScreen key operation logs will be collected. This can be set when the [Disabling PrintScreen Key] of [Printing Prohibition] tab is "No". <b>Initial Value:</b> [No] is selected.
[Screen Capture]	This can be set when [PrintScreen Key Operation Log] is "Yes".  When it is selected: The screen capture at the time point when PrintScreen key operation logs are collected will be recorded.  When it is not selected: <b>(Initial Value)</b> The screen capture at the time point when PrintScreen key operation logs are collected will not be recorded.
[Web Operation Log]	The following log will be collected:  - Web download log  <b>Initial Value:</b> [No] is selected.
[FTP Operation Log]	The following logs will be collected:  - FTP upload log - FTP download log  <b>Initial Value:</b> [No] is selected.
[Clipboard Operation Log(Virtual Environment)]	Clipboard operation logs will be collected.  - <b>Initial Value:</b> [No] is selected.
[Backup Original File]	This can be set when the [Clipboard Operation Log (Virtual Environment)] is set to "Yes".  When it is selected: The information (text, image, file path) copied via clipboard can be backed up as original file.  When it is not selected: <b>(Initial Value)</b> The information (text, image, file path) copied via clipboard will not be backed up as original file.
[File Operation Log]	File operation logs will be collected. <b>Initial Value:</b> [No] is selected.  When "Yes" is selected, input can be performed in the following tabs:  - [File Operation Process] tab - [File Operation Extension] tab
[Logon,Logoff Log]	The following logs will be collected:  - Logon log - Logoff log

Item Name	Description
	<ul style="list-style-type: none"> <li>- PC startup log</li> <li>- PC shutdown log</li> <li>- PC sleep log</li> <li>- PC restoration log</li> <li>- PC connection log</li> <li>- PC disconnection log</li> </ul> <p><b>Initial Value:</b> “Yes” is selected, and it cannot be modified.</p> <p>In the Server Settings Tool, when [Not Manage] is selected in the [Connection information between Terminals] of [System Settings], the item can be Modified to [Yes] or [No].</p>
[Linkage Application Log]	<p>External application logs will be collected.</p> <p><b>Initial Value:</b> [No] is selected.</p>
[All]	Select to collect all logs.
[None]	Select not to collect all logs.



#### Note

#### About settings of [Printing Operation Log]

During the installation of the client (CT), when [Monitoring the printing of local printer only] is selected, it is assumed that the printing operation of the client (CT) is performed via the printer servers that are registered to the same Master Management Server or Management Server. (The client (CT) should also be installed on the printer sever.)

At the moment, printing logs will be collected from the printer server. Therefore, in the client (CT) that is not the printer server, even if the [Printing Operation Log] is set to [Yes], the printing log will not be collected. However, if [Printing Operation log] in the print sever is set to [Yes], the printing operation log can be collected.

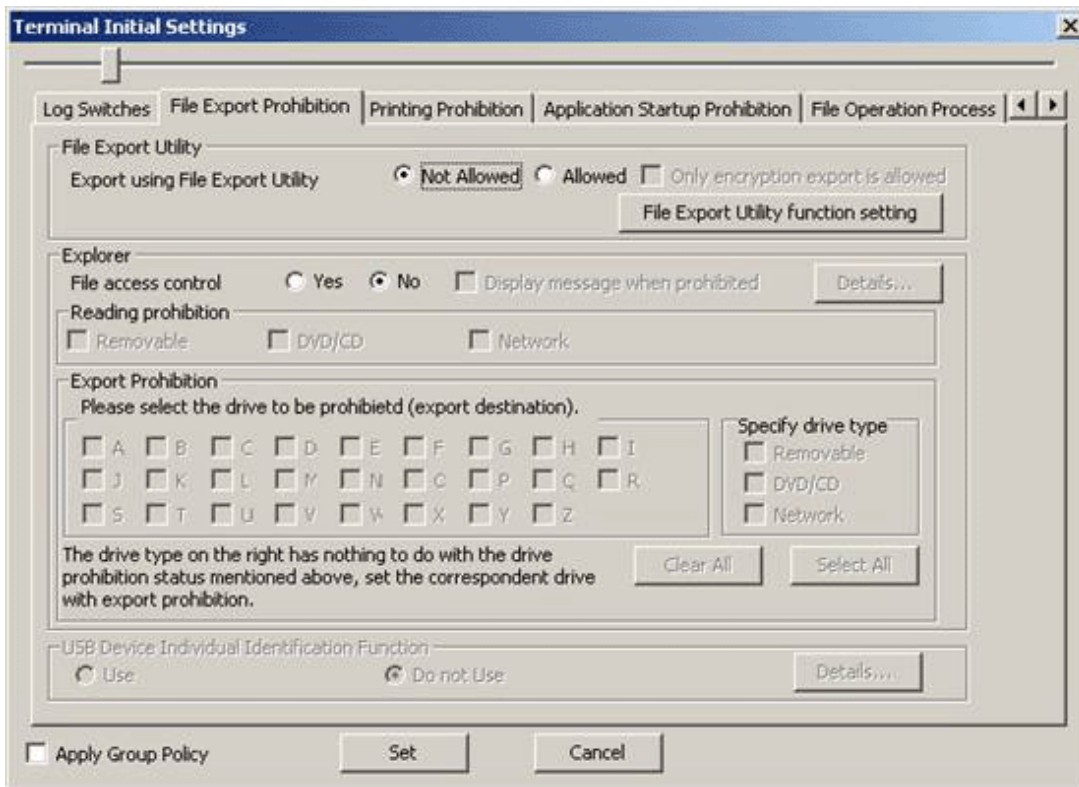
### 2.4.1.2 Settings of [File Export Prohibition] Tab

In the [File Export Prohibition] tab, the conditions of prohibiting the export and reading of files or folders from disk drive, removable device, DVD/CD drive or network drive of the client (CT) PC will be set.

Though the reading prohibition is effective when the Explorer is used, it will become invalid while the File Export Utility is being used.

In addition, the limiting conditions for export to the allowed USB device will be set by the administrator.

The following section describes the settings of the [File Export Prohibition] tab.



[File Export Utility]

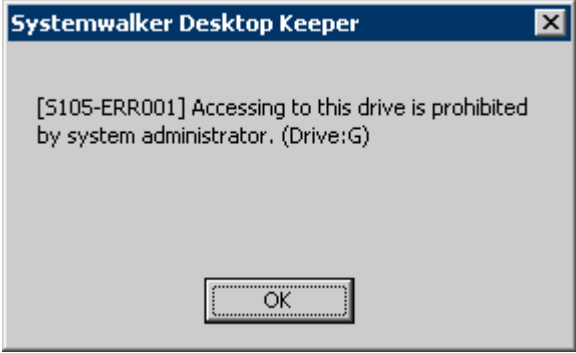
Item Name		Description
[Export using File Export Utility]	[Not Allowed] <b>(Initial Value)</b>	The File Export Utility cannot be used.
	[Allowed]	The File Export Utility can be used. Even for the drive with export prohibition, the File Export Utility can be used.
	[Only encryption export is allowed]	<b>This function is not available.</b> When it is selected: The export is allowed only when the file is encrypted by the File Export Utility. When it is not selected: No matter whether the file is encrypted or not, the File Export Utility can always be used for export.
[File Export Utility function setting]		The [Setting of File Export Utility function] is displayed. (Set the conditions when File Export Utility is used)


[Explorer]

Set the control when operation is performed via Explorer .etc.

Item Name		Description
[File access control]	[Yes]	[Reading Prohibition] and [Export Prohibition] can be set. The [Display message when prohibition] checkbox can be selected when this item is selected. After it is selected, messages will be displayed when the prohibition operation is performed.



Item Name		Description
	[No] <b>Initial Value</b>	Reading of removable drive and export of files can be performed freely (files can be accessed in the same way as if Systemwalker Desktop Keeper is not installed). When this item is selected, [Reading Prohibition] and [Export Prohibition] cannot be set.
[Display message when prohibited]		After setting this item, the following message will be displayed when inserting the prohibited device into the client (CT).  The above message will be displayed when "Violation" of device configuration change log occurs. <b>Initial Value:</b> Not selected Please refer to "8.2.7 Device Configuration Change Log" for "Violation" of device configuration change log.
Detailed Settings		Settings can be performed when the [File Access Control] is "Yes". The [File access control - Detailed Settings] window will be displayed. (Set the conditions of folders excluded from network drive access prohibition)
[Reading Prohibition]		Set the targets for reading prohibition.
	[Removable]	Reading of the following devices that are identified as drive letter are prohibited. <b>Initial Value:</b> Not selected - Floppy disk - External hard disk (removable hard disks such as USB, IEEE1394, PCMCIA connection) - MO - USB memory Compact flash memory
	[DVD/CD]	Reading of DVD/CD is prohibited. <b>Initial Value:</b> Not selected
	[Network]	Reading of network drive is prohibited. <b>Initial Value:</b> Not selected
[Export Prohibition]		Set the targets for exporting prohibition.
	Please select the drive to be prohibited(export destination).	Select the drive that is the target for export prohibition. <b>Initial Value:</b> All are not selected The drive that becomes the prohibited target by specifying the drive letter should satisfy all the following conditions.

Item Name		Description
		<p>The prohibited targets do not include the drive or C drive apart from the following conditions (infrared connection):</p> <ul style="list-style-type: none"> <li>- Drive identified as a drive letter in the PC.</li> <li>- Drive apart from the network drive.</li> </ul> <p>When F drive is a removable drive, even if the [Removable] (not regarded as the prohibited target) is not selected, when [F] (regarded as prohibited target) is selected, F drive will also be prohibited.</p> <p> <b>Note</b></p> <hr style="border-top: 1px dotted orange;"/> <p><b>About network drive</b></p> <p>The network drive cannot be prohibited by specifying the drive letter. Please prohibit it by selecting the [Network] checkbox.</p> <hr style="border-top: 1px dotted orange;"/>
[Specify drive type]	[Removable]	<p>Export to the following devices that are identified as drive letter is prohibited. <b>Initial Value:</b> Not selected</p> <ul style="list-style-type: none"> <li>- Floppy disk</li> <li>- External hard disk (removable hard disks connected by such as USB, IEEE1394, PCMCIA connection)</li> <li>- MO</li> <li>- USB memory</li> <li>- Compact flash memory</li> </ul>
	[DVD/CD]	<p>Export to DVD/CD is prohibited. <b>Initial Value:</b> Not selected</p>
	[Network]	<p>Export to network drive is prohibited. <b>Initial Value:</b> Not selected</p>
[Clear All]		<p>Clear all the selections for the settings of the prohibited drive (export destination) and [Specify drive type].</p>
[Select All]		<p>Select all for the settings of the prohibited drive (export destination) and [Specify drive type].</p>

 **Note**

Please do not set the target drive for saving log files.

If the target drive for saving log files set during the installation of the client (CT) is regarded as the prohibited target, logs cannot be collected from the client (CT).

[USB Device Individual Identification Function]

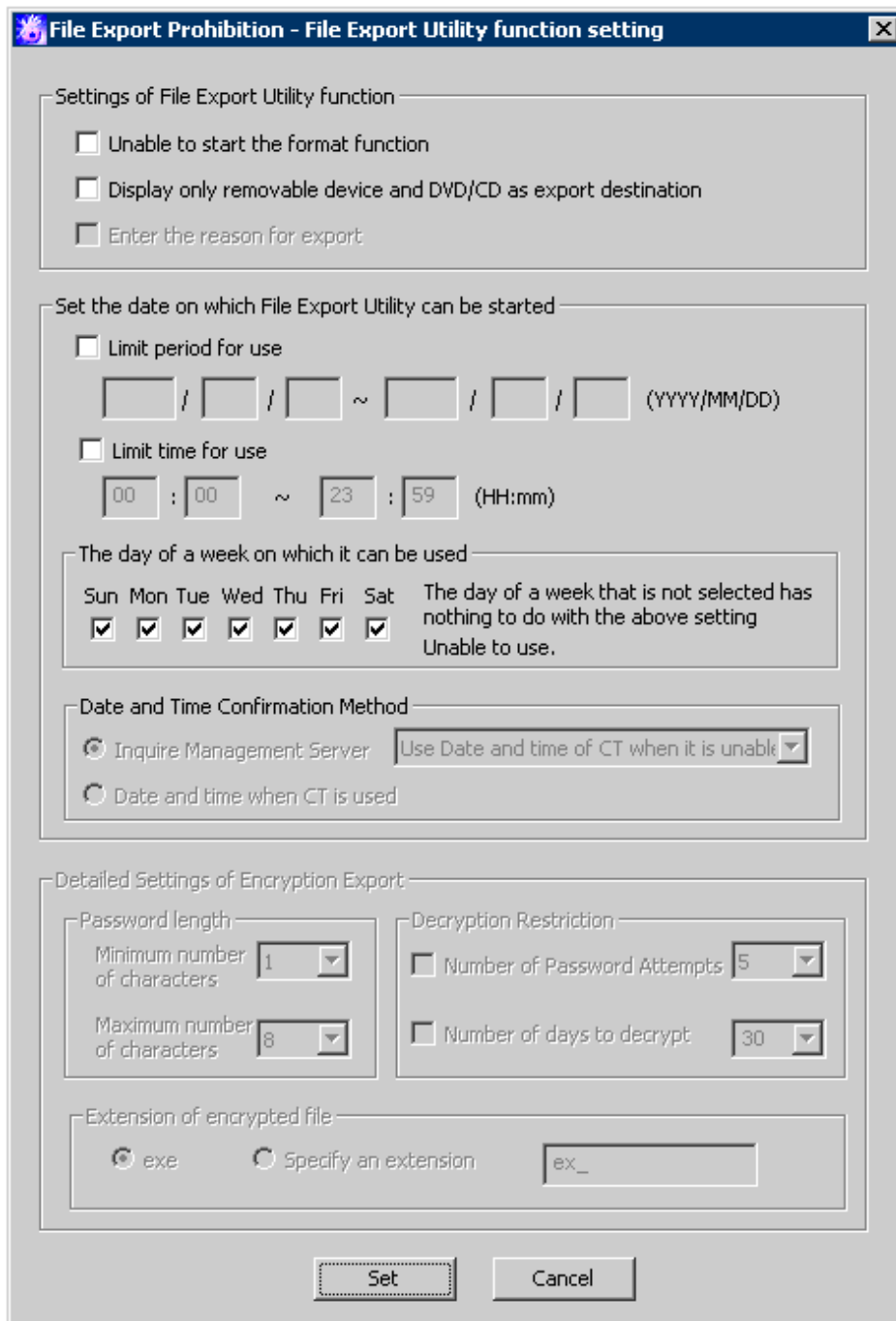
**This function is not available.**

Item Name	Description
[Use]	<p>When exporting files and folders using File Export Utility, they can only be exported to the USB device specified by the administrator among the USB devices registered in the [USB Device Registration] window of the Management Control.</p> <p>In addition, when the writing and reading with Explorer, etc. (Not File Export Utility) is prohibited, files and folders can only be exported to the USB device specified by the administrator among the</p>

Item Name	Description
	USB devices registered in the [USB Device Registration] window of the Management Control. Please refer to “ <a href="#">Register USB device</a> ” of “ <a href="#">7.5 Export Files to Specified USB Device Only</a> ” for the method of adding USB devices.
[Do not Use] <b>Initial Value</b>	When exporting files and folders using File Export Utility, follow the policies set in <a href="#">[File Export Utility]</a> . In addition, the writing and reading with Explorer, etc. should follow the policies set in <a href="#">[Explorer]</a> .
[Detailed Settings]	The <a href="#">[File Export Prohibition - Individual Identification Function of USB Device - Detailed Settings] window</a> will be displayed. (Set the access condition for the administrator to use the allowed USB device, as well as adding and deleting the allowed USB device.)

### **[File Export Utility function setting] window**

The conditions of using File Export Utility can be set.



[Setting of File Export Utility function]

Item Name	Description
[Unable to start the format function]	<p>When this is selected:            The following content will not be displayed when selecting the [File] menu. The data in the drive and CD-RW/DVD-RW cannot be deleted.</p> <ul style="list-style-type: none"> <li>- [Format Drive]</li> <li>- [Erase CD-RW/DVD-RW]</li> </ul> <p>When it is not selected: <b>(Initial Value)</b>            The data in the drive and CD-RW/DVD-RW can be deleted.</p>

Item Name	Description
[Display only removable device and DVD/CD as export destination]	<p>When this is selected: During file export, only removable device and DVD/CD will be displayed as export destinations.</p> <p>When it is not selected: <b>(Initial Value)</b> During file export, all export destinations will be displayed.</p>
[I]Enter the reason for export]	<p>When this is selected: The input field for entering the reason for export will be displayed in the [File Export Utility] window. The reason for export must be input during file export. Up to 10 reasons can be saved by each CT/client. At the next export, the information input previously can be selected from the pull-down menu.</p> <p>When it is not selected: <b>(Initial Value)</b> The input field for entering the reason for export will not be displayed in the [File Export Utility] window.</p>

[Set the date on which File Export Utility can be started]

Item Name	Description
[Limit period for use]	<p>When this is selected: The period in which the startup is allowed will be set. The File Export Utility can be used in the set period only. The scope of input value is as follows: - 1<sup>st</sup>, January, 2000 ~ 31<sup>st</sup>, December, 2037</p> <p>When it is not selected: <b>(Initial Value)</b>: The File Export Utility can be used all the time.</p>
[Limit time for use]	<p>When this is selected: The hours in which the startup is allowed will be set. The File Export Utility can be used in the set period only</p> <p>When it is not selected: <b>(Initial Value)</b>: The File Export Utility can be used 24 hours.</p>
[The day of a week on which it can be used]	<p>The day in a week when the startup is allowed will be set. <b>(Initial Value)</b>: All are selected.</p>
[Date and Time Confirmation Method]	<p>[Inquire Management Server] <b>(Initial Value)</b>:</p> <p>The date and time when the File Export Utility can be started is based on the date and time of the Management Server.</p> <p>In addition, set the operations when the client is offline or the Management Server gives no response.</p> <ul style="list-style-type: none"> <li>- [Use Date and time of CT when it is unable to obtain]: The date and time of CT will be used as the date and time when the File Export Utility can be started.</li> <li>- [Unable to start when it is unable to obtain] <b>(Initial Value)</b>: The File Export Utility cannot be started.</li> </ul>
	<p>[Date and Time when CT is used] The date and time when the File Export Utility can be started is based on the date and time of the CT.</p>

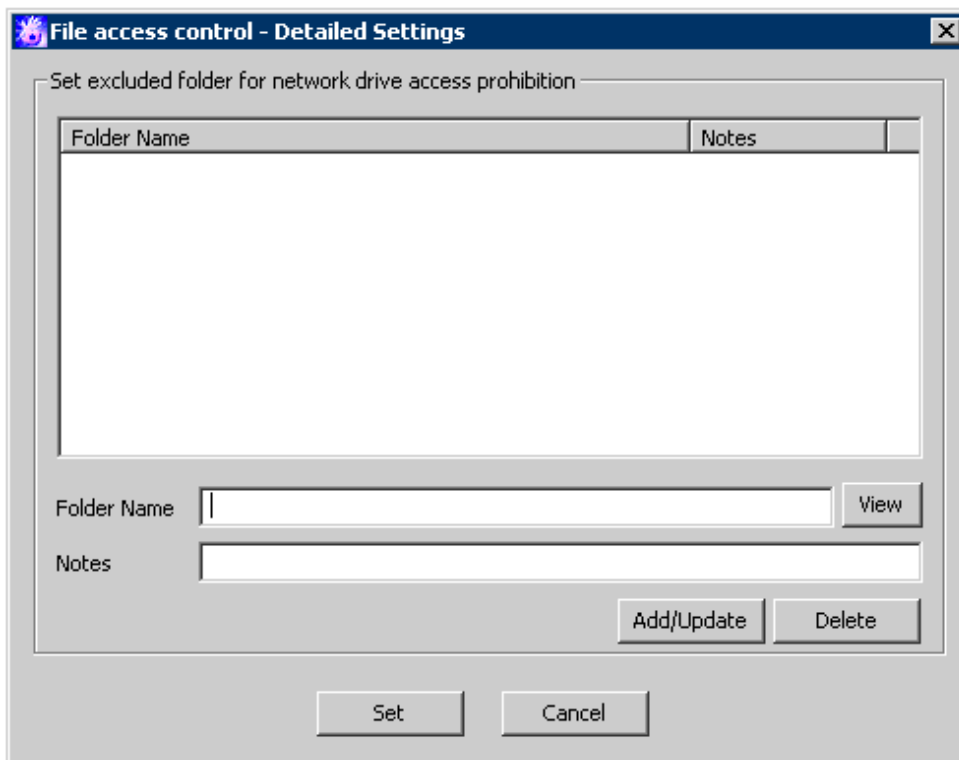
[Detailed Settings of Encryption Export]

**This function is not available.**

Item Name		Instruction
[Password Length]	[Minimum number of characters]	This is the minimum number of characters for a password when the encrypted file export is set. 1-128 can be set. <b>Initial Value:</b> 1
	[Maximum number of characters]	This is the maximum number of characters for a password when the encrypted file export is set. 1-128 can be set. <b>Initial Value:</b> 8
[Decryption Restriction]	[Number of Password Attempts ]	When this is selected: The number of password attempts can be set. The range of 1-5 times can be set. (5 times will be displayed at the beginning.) If the times of password input exceeds the set value, the encrypted files will be deleted. However, if an encrypted file is exported to the following media, the encrypted file will not be deleted: <ul style="list-style-type: none"><li>- DVD/CD</li><li>- Write-protected floppy disk and USB memory</li></ul> When it is not selected ( <b>Initial Value</b> ): There is no limit for the number password attempts, and the encrypted files will not be deleted.
	[Nubmer of day to decrypt]	When this is selected: The time (number of days) when the encrypted file can be decrypted can be set. The days include the day of encryption. 1-999 days can be set. (30 days will be displayed initially.) If the decryption operation is still performed after the set days has passed, the encrypted files will be deleted. However, if the encrypted files are exported to the following media, the encrypted files will not be deleted: <ul style="list-style-type: none"><li>- DVD/CD</li><li>- Write-protected floppy disk and USB memory</li></ul> When it is not selected: ( <b>Initial Value</b> ): There is no limit for the number of password attempts, and the encrypted files will not be deleted.
[Extension of encrypted file]	[exe] ( <b>Initial Value</b> )	The “exe” will be automatically added as the extension of encrypted files. The relationship between the [Encrypted File Name] of the [Settings of Encrypted Files] window and the file name after encryption is shown as follows: <ul style="list-style-type: none"><li>- Specify “Encryption” in the encrypted file name→ The created file name is “Encryption.exe”</li><li>- Specify “Encryption.txt” in the encrypted file name→The created file name is “Encryption.exe”</li><li>- Specify “Encryption.exe” in the encrypted file name→The created Create file name is “Encryption.exe.exe”</li><li>- Specify “Encryption.ex_” in the encrypted file name→The created Create file name is “Encryption.ex_.exe”</li></ul> The encrypted file can be presented by the private icon for an encrypted file of File Export Utility.
	[Specify an extension]	The extension of encrypted file can be set. 16 digits of single-byte alpha-numeric characters symbols (except “.”) can be used. But the following characters are not allowed: “.”, “\”, “/”, “:”, “*”, “?”, ““”, “<”, “>”, “ ”

Item Name		Instruction
		<p>Even if the extensions of compressed files such as “zip”, “lzh”, etc. have been set, they will not be compressed.</p> <p><b>Initial Value:</b> “ex_”</p> <p>The relationship between the [Encrypted File Name] of the [Settings of Encrypted Files] window and the file name after encryption is shown as follows:</p> <p>The specified extension is “ex_”.</p> <ul style="list-style-type: none"> <li>- Specify “Encryption” in the encrypted file name→The created file name is “Encryption.ex_”</li> <li>- Specify “Encryption.txt” in the encrypted file name→The created file name is “Encryption.txt.ex_”</li> <li>- Specify “Encryption.exe” in the encrypted file name→The created file name is “Encryption.exe.ex_”</li> <li>- Specify “Encryption.ex_” in the encrypted file name→The created file name is “Encryption.ex_”</li> </ul> <p>When the extension relating to the file has been specified for the encrypted file, it will be displayed with the icon of the related file.</p>
[Set]		Confirm the input contents and return to the “File Export” tab.
[Cancel]		Do not save the settings and close the window.

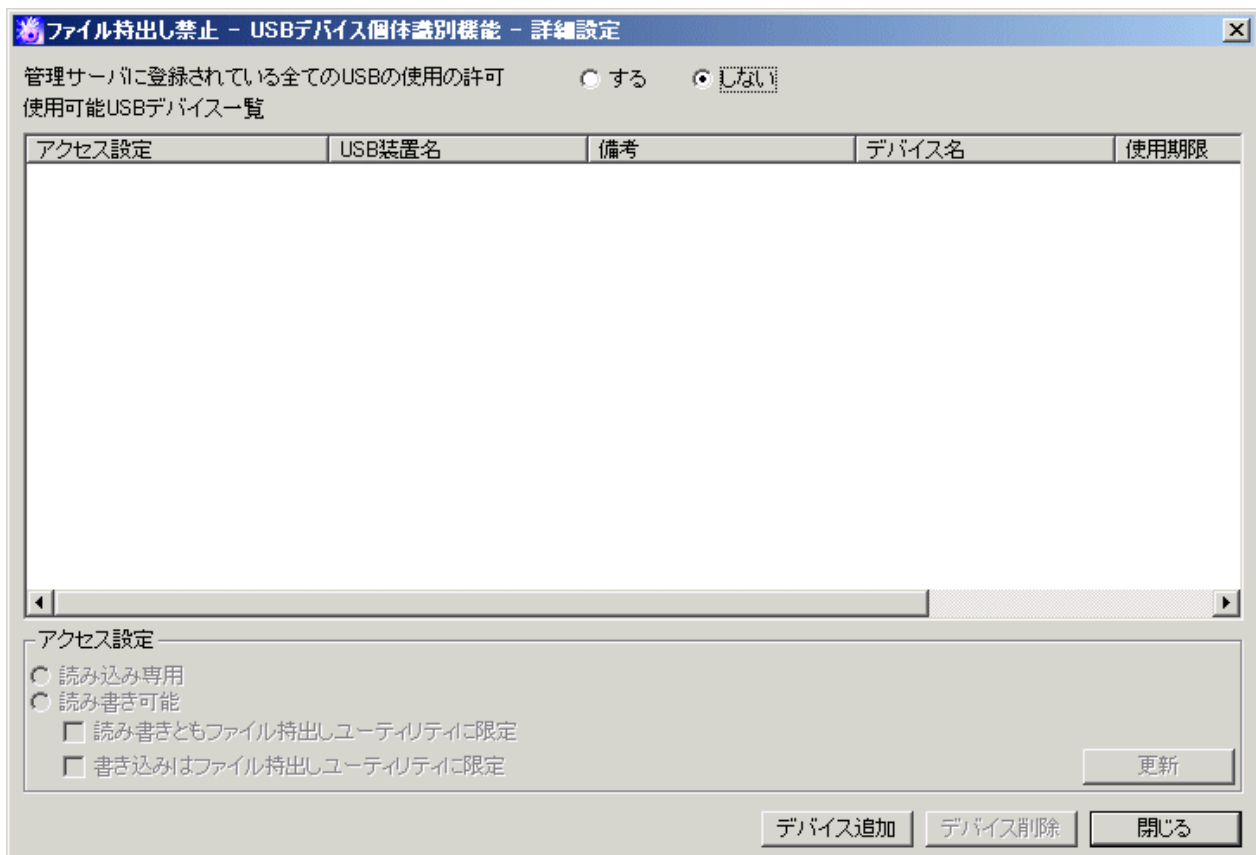
**[File access control - Detailed Settings] window**



Item Name	Description
[Set excluded folder for network drive access prohibition]	The folder excluded from network drive access prohibition can be set.

Item Name	Description
[Folder Name]	The folder excluded from network drive access prohibition can be set. The folder name can only be specified to "Path described by UNC". (Example: \\192.168.0.1\shared, \\nas-server\public) The drive which is allocated with a network drive cannot be specified. (Example: Z:) The following characters cannot be specified: "/", ":", "*", "?", " ", "<", ">", " " In addition, "\" cannot be specified at the end of path. <b>Initial Value:</b> No specification
[View]	The dialog for selecting the excluded folder can be displayed.
[Notes]	Enter the information such as memo. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> No specification
[Add/Update]	Add an excluded folder. Up to 50 cases can be added. In addition, all folder paths cannot exceed 500 bytes altogether. After modifying the selected [Notes] in the folder list, the information will be updated ([Folder Name] cannot be updated).
[Delete]	Delete the selected lines in the folder list.
[Set]	Confirm the input contents and return to the "File Export" tab.
[Cancel]	Do not save the settings and close the window.

**[File Export Prohibition - Individual Identification Function of USB Device - Detailed Settings] window**





Item Name	Description
[Allow to Use All USB Devices Registered in Management Server]	Select whether the used of all USB devices registered in the Management Server is allowed.  Yes: All USB devices registered in the Management Server can be used. Whether each USB device can be used or not cannot be set.  No: <b>(Initial Value)</b> Whether each USB device can be used or not can be set.  When Management Server cannot communicate with the client (CT), the USB device used before can be used.
[List of Available USB Devices]	The USB device that is allowed to be used by the administrator will be displayed. When setting and modifying the access condition and canceling the usage permission, select the line corresponding to the USB device.
[Access Settings]	Set the conditions for accessing to the USB device allowed to be used.
[Read Only] (Initial Value)	The selected USB device in [List of Available USB Devices] can be read only.
[Read and Write]	The selected USB device in [List of Available USB Devices] can be read and written.  Only one can be selected among the [Read and Write by File Export Utility Only] checkbox and the [Write by File Export Utility Only] checkbox. When neither is selected, the registered USB devices can be read and written using File Export Utility and Explorer, etc. (Not File Export Utility).
[Read and Write by File Export Utility Only]	When it is selected: Only File Export Utility can be used to read and write (file export). Explorer, etc. (Not File Export Utility) cannot be used to read and write.
[Write by File Export Utility Only]	When it is selected: Only File Export Utility can be used to read (file export). Any tool can be used to read.
[Update]	The settings can be displayed in [List of Available USB Devices].
[Add Device]	The <a href="#">[File Export Prohibition - Detailed Settings of USB Device Individual Identification Function - Select a USB Device]</a> window can be displayed and the available USB devices can be added. Up to 100 cases can be added.
[Delete Device]	The usage permission of the selected USB device can be canceled in [List of Available USB Devices] and the USB device can be deleted from [List of Available USB Devices].
[Close]	Shutdown the window.

#### When setting (modifying) the access conditions of available USB devices

1. Select the line corresponding to the USB device in [List of Available USB Devices].
2. Set conditions in [Access Settings].
3. Click the [Update] button.

#### When canceling the usage permission of USB devices

1. Select the line corresponding to the USB device in [List of Available USB Devices].
2. Click the [Delete Device] button.

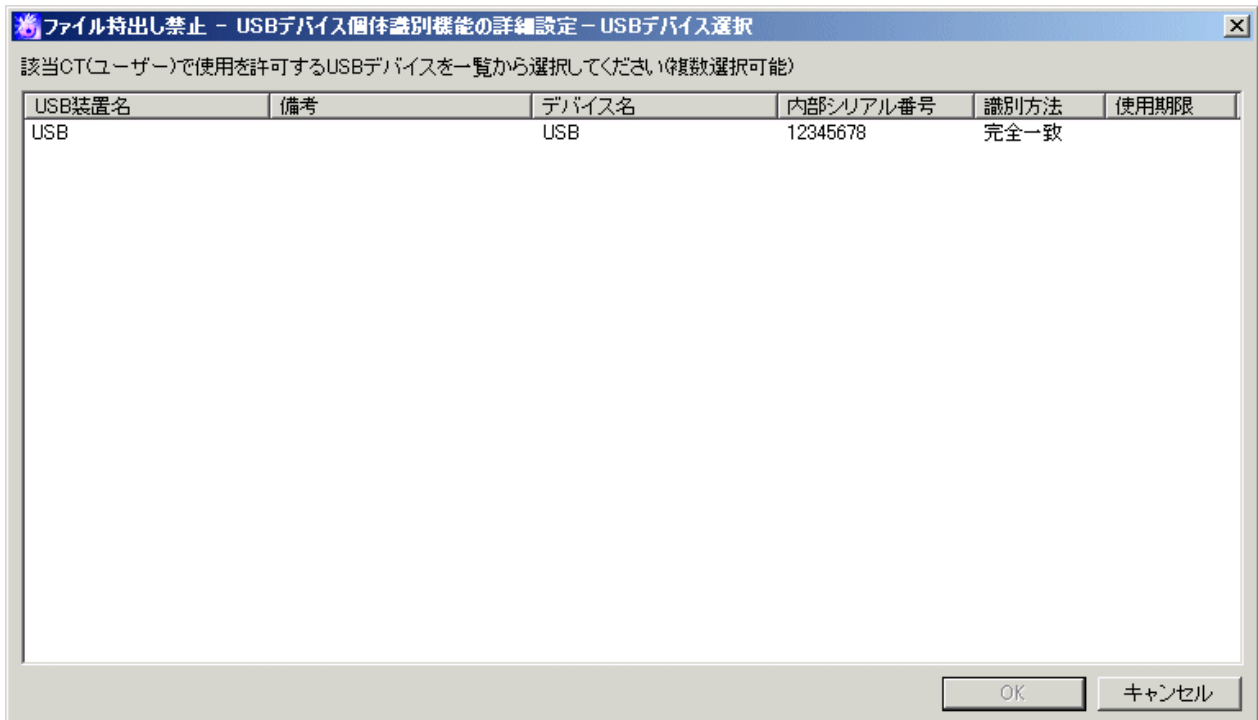
When adding an available USB device

Click the [Add Device] button.

### [File Export Prohibition - Detailed Settings of USB Device Individual Identification Function - Select a USB Device] window

The content registered in the [USB Device Registration] window of the Management Console can be displayed.

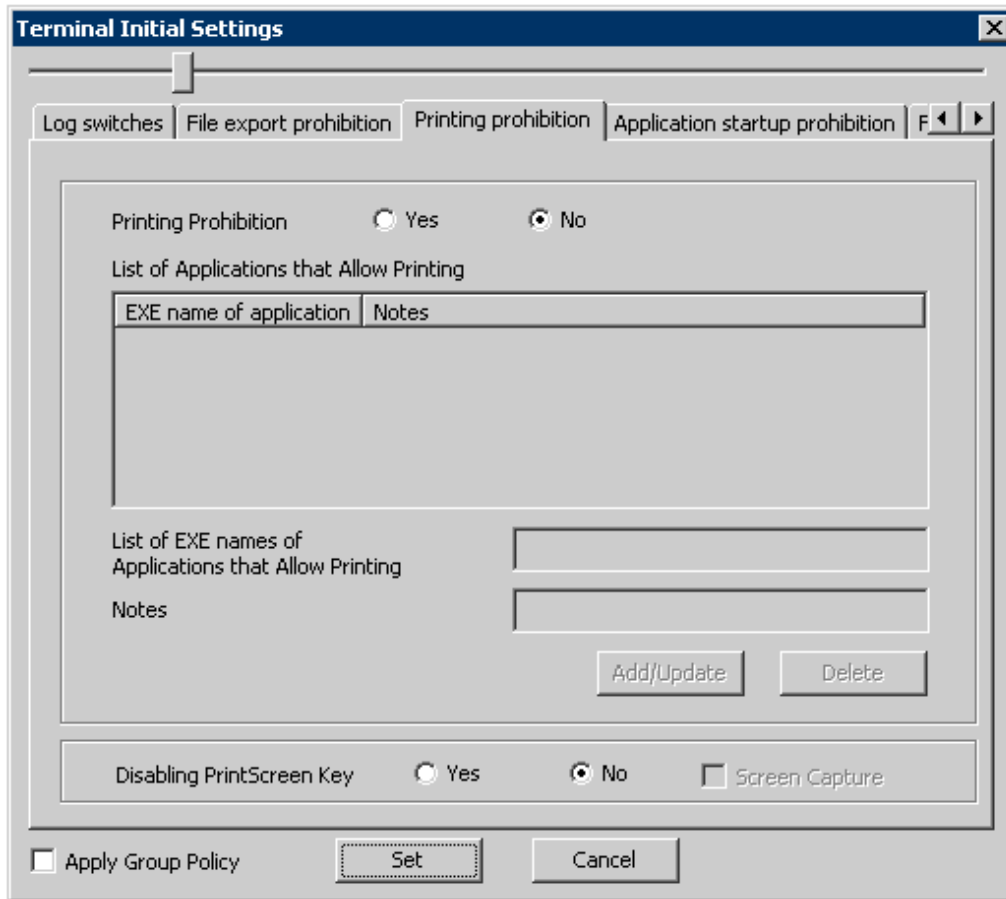
The line of the available USB device can be selected. After clicking the [OK] button, the corresponding USB Device will be added to the [List of Available USB Devices] in the [File Export Prohibition - Individual Identification Function of USB Device - Detailed Settings] window window.



### 2.4.1.3 Settings of [Printing Prohibition] Tab

The conditions for prohibiting printing on the PC with the client (CT) installed (specify the application allowed to print) and the prohibition of using PrintScreen key to collect screen hard copy can be set in the [Printing Prohibition] tab.

The following section describes the settings of the [Printing Prohibition] tab.



[Printing Prohibition]

Item Name		Description
[Printing Prohibition]	[Yes]	Printing that uses applications apart from the [EXE Name of application] displayed in the [List of Applications that Allow Printing] is prohibited.
	[No] <b>(Initial Value)</b>	Printing is not prohibited.
[List of Applications that Allow Printing]		The set [EXE Name of Application that Allow Printing] will be displayed. <b>Initial Value:</b> No specification will be made.
[List of EXE names of Applications that Allow Printing ]		Enter the EXE names including the extensions of Applications allowed to print. (For example: Enter EXCEL.EXE in case of Microsoft® Excel)  Up to 254 single-byte characters (127 double-byte characters) can be entered. (For alphabets, it is case-sensitive.) However, if the following symbols are used, error will occur. “\” “/” “.” “:” “;” “?” “!” “” “<” “>” “ ”  <b>Initial Value:</b> No specification will be made.
[Notes]		Enter the application name and memo information. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> No specification will be made.
[Add/Update]		Add the EXE name of application allowed to print. Up to 100 cases can be added.  After modifying the [Notes] of selected lines in the [List of Applications Allowed to Print], the information will be updated (The [EXE Name of Application that Allow Printing] cannot be updated.).

Item Name	Description
[Delete]	The selected lines in the [List of Applications that Allow Printing] can be deleted.

[PrintScreen Key Prohibition]

Item Name	Description
[Disabling PrintScreen Key]	When the [PrintScreen Key Operation Log] option in the [Log Switches] tab is [No], settings can be performed.
[Yes]	The use of PrintScreen key is prohibited. Even if the PrintScreen key is pressed, the hard copy of screen cannot be collected.
[No] (Initial Value)	The use of PrintScreen key is not prohibited.
[Capture Screen]	When the option of [PrintScreen Key Prohibition] is “Yes”, settings can be performed When it is selected: When the use of PrintScreen key is prohibited, the screen capture when PrintScreen key is pressed can be recorded. When the [Prohibiting PrintScreen Key] option is “No”, it will be changed to not selected automatically. When it is not selected: When the use of PrintScreen key is prohibited, even if the PrintScreen key is pressed, the screen capture will not be recorded.

[When adding the EXE name of applications that Allow Printing ]

Enter the above settings items and click the [Add/Update] button.

Up to 100 cases can be added.

[When updating the existing information]

Select the lines to be updated from the [List of Applications that Allow Printing], modify the [Notes] information and click the [Add/Update] button.

The [EXE Name of Application that Allow Printing] cannot be updated.

[When deleting information]

Select the lines to be deleted from the [List of Applications that Allow Printing], and click the [Delete] button.

#### 2.4.1.4 Settings of [Logon Prohibition] Tab

**This function is not available.**

The group prohibited from logon can be set in the [Logon Prohibition] tab. After setting the [Logon Prohibition], logon with the user name that belongs to the set group can be prohibited when logging on to the PC with the client (CT) installed.

The groups for which logon prohibition can be set are as follows:

- Administrators
- Backup Operators
- Debugger Users
- Power Users
- Guests
- Replicator
- Users
- Domain Admins
- Domain Guests

- Domain Users
- Enterprise Admins
- Group Policy Creator Owners

In addition, when one user name belongs to multiple groups, it will become a target of logon prohibition when it satisfies all the following conditions:

- The user name entered during logon to the Windows PC belongs to multiple groups.
- Logon prohibition is set for any one group in the multiple groups to which the user name belongs.



## Note

### About the creation of system administrator user under the Windows® XP system

Under Microsoft® Windows® XP Home Edition, the user names belong to the Administrators group and the Users group will be created automatically when the system administrator user is created. If either the Administrators group or the Users group is prohibited, the policy set in Systemwalker Desktop Keeper will be prohibited logon.

The set contents will be operated as CT policy.

When only one person logs on to the PC, prohibition can be performed through the settings in the [Logon Prohibition] tab.

When 2 or more users log on to the same PC, it will have nothing to do with the settings in the [Logon Prohibition] tab and it will be logged off.

The following section describes the settings of the [Log Filtering Condition] tab.

The screenshot shows the 'Terminal Initial Settings' dialog box with the 'Log Filtering Condition' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'File operation process', 'File operation extension', 'Log Filtering Condition', and 'Screen Capture Control'. The 'Log Filtering Condition' tab is active and contains the following elements:

- A note: '\* This tab can be set when "Window Title Log" of the "Log Switches" tab is "Yes".'
- 'Repeated Log Filter Setting' section with a checkbox: 'When same window title logs exist in the same process, only the log of first time will be obtained.' (unchecked).
- 'Keyword filtering' section with the instruction 'Please set the filtering condition of window title logs.' and three radio buttons: 'Filtering conditions are not set' (selected), 'Obtain matched logs only', and 'Exclude matched log'.
- 'Filtering Condition' section with a table:

Process EXE Name	Keyword

Below the table are two input fields: 'Process EXE Name' and 'Keyword'. At the bottom of the table area are three buttons: 'Add', 'Update', and 'Delete'. At the very bottom of the dialog are a checkbox 'Apply Group Policy' (unchecked), and 'Set' and 'Cancel' buttons.

Item Name	Description
[List of Logon Prohibition Groups]	The set logon prohibition group will be displayed. <b>Initial Value:</b> Not specified.
[Logon Prohibition Group]	Select the logon prohibition group from the pull-down menu. Please refer to Windows manual for the details of each group. <b>Initial Value:</b> Not specified.
[Set]	<p>When prohibiting the target group from logon, the processing in the client (CT) can be specified.</p> <ul style="list-style-type: none"> <li>- [Logoff] Logoff by force. Under Windows Server® 2008, Windows Server® 2003 or Windows® 2000 Server, please set [Logoff] when users with User authority are not expected to use.</li> <li>- [Shutdown] (Initial Value) Shutdown by force. However, under Windows Server® 2008 or Windows Server® 2003, the User authority cannot shut down the computer.</li> </ul> <p>The time from logon prohibition being detected from the client (CT) to logoff or shutdown can be set in the “Terminal Operation Settings”. Please refer to “<a href="#">2.4.2 Perform Terminal Operation Settings</a>” for “Terminal Operation Settings”.</p>
[Add/Update]	<p>The name of group that is prohibited from logon and the processing during logon will be added.</p> <p>After modifying the [Set] of selected lines in the [List of Logon Prohibition Groups], the information will be updated (The [Logon Prohibition Group] cannot be updated.).</p>
[Delete]	The selected lines in the [List of Logon Prohibition Groups] will be deleted.

**[When adding a logon prohibition group]**

After entering the above set items, click the [Add/Update] button.

**[When updating the existing information]**

Select the lines to be updated from the [List of Logon Prohibition Groups], modify the [Settings] information and click the [Add/Update] button.

The [Group Name] cannot be updated.

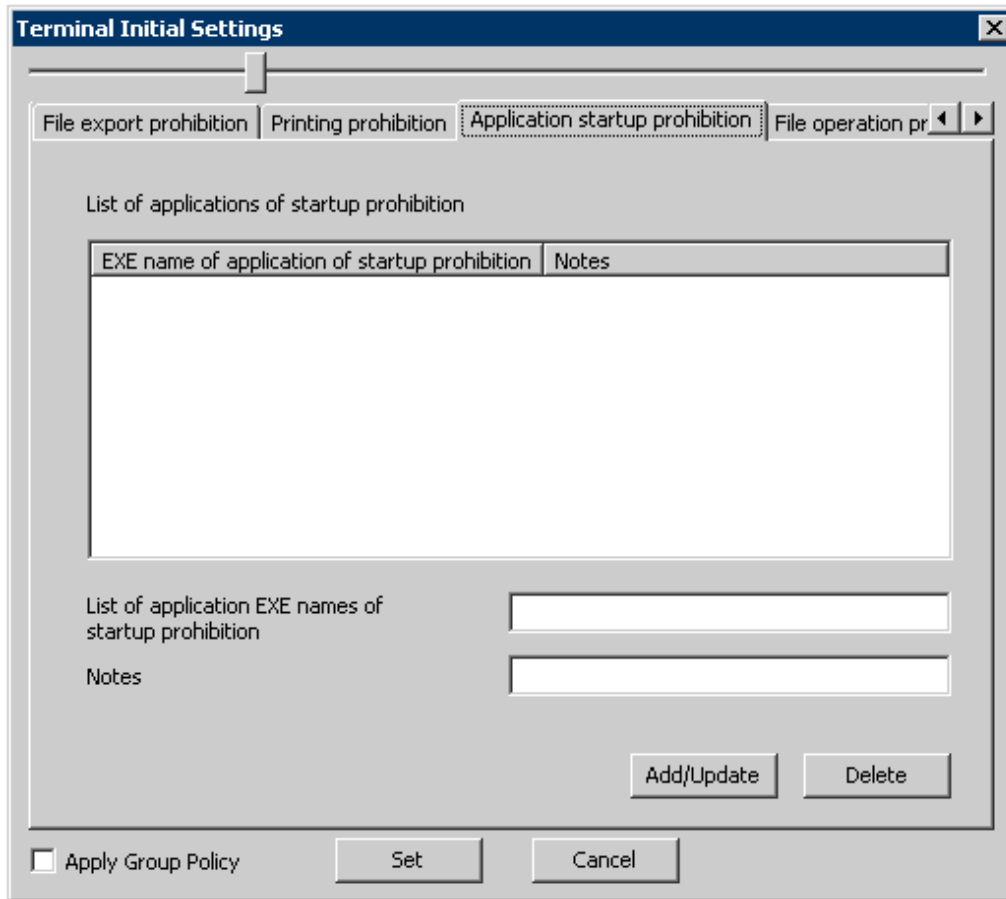
**[When deleting information]**

Select the lines to be deleted from the [List of Logon Prohibition Groups] and click the [Delete] button.

### 2.4.1.5 Settings of [Application Startup prohibition] Tab

In the [Application Startup Prohibition] tab, the name of the application that is prohibited from startup in the PC with the client (CT) installed can be set.

The following section describes the settings of the [Application Startup Prohibition] tab.



Item Name	Description
[List of Applications of startup prohibition]	The set EXE name of the application prohibited from startup will be displayed. <b>Initial Value:</b> Not specified.
[EXE name of application of startup prohibition]	Enter the EXE name including extension of the application prohibited from startup. (For example: Enter EXCEL.EXE in case of Microsoft® Excel)  Up to 254 single-byte characters (127 double-byte characters) can be entered. (Alphabets are not case-sensitive)  However, error will occur if the following symbols are used. “\” “/” “:” “*” “?” “ ” “<” “>” “ ”  <b>Initial Value:</b> Not specified.
[Notes]	Enter the application name and memo information. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> No specified.
[Add/Update]	The EXE name of the application prohibited from startup will be added. Up to 100 cases can be added.  After modifying the [Notes] of the selected lines in the [List of Applications Prohibited from Startup], the information will be updated (The [EXE Name of Application Prohibited from Startup] cannot be updated.).
[Delete]	The lines selected in the [List of applications of startup prohibited] will be deleted.

**[When adding an EXE name of the application prohibited from startup]**

Enter the above set items and click the [Add/Update] button.

Up to 100 cases can be added.

**[When updating the existing information]**

Select the lines to be updated from the [List of applications of startup prohibited], modify the [Notes] information and click the [Add/Update] button.

The [EXE Name of application of startup prohibited] cannot be updated.

**[When deleting information]**

Select the lines to be deleted from the [List of applications of startup prohibited ], and click the [Delete] button.

### 2.4.1.6 Settings of [File operational process] Tab

The screening conditions for obtaining file operation logs can be set in the [File Operation Process] tab. Set the file location for log collection during access, and the process of log collection during startup. As the file operation logs can be selected and collected according to objectives, the search efficiency after collection can be improved.

When the [File Operation Log] option in the [Log Switches] tab is [Yes], the set items of the [File Operation Process] tab can be set.

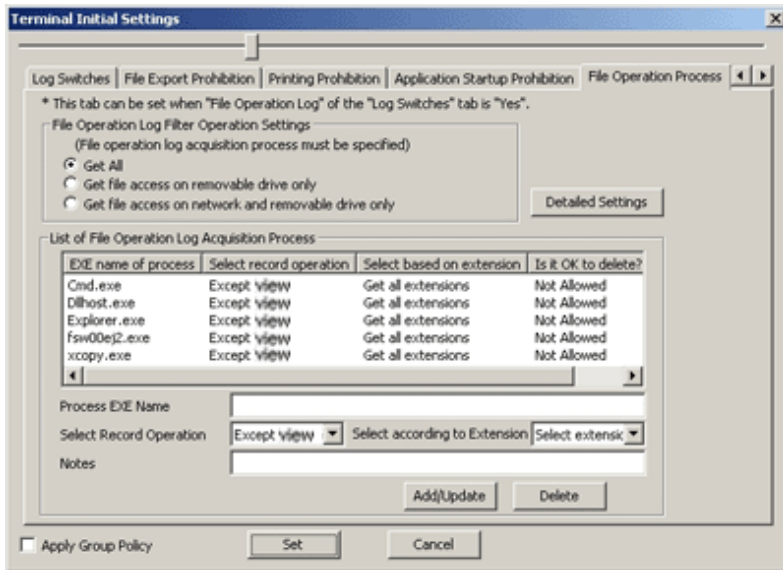


Note

**Please do not register the software with many disk accesses.**

Since the output of a large amount of logs will cause insufficient database capacity, please do not register software that has significant access to disks such as antivirus software, disk check and repair software, etc.

In addition, as the software related to the OS may also output too many logs, please register after confirming the performance and OS operation state on the test machine.



Initial Value Displayed in [File Operation Process]

EXE Name of Process	Select Record Operation	Select based on extension	Is it OK to delete?	Notes
[Cmd.exe]	[Except view]	[Get all extensions]	[Not Allowed]	[Command Prompt]
[Explorer.exe]	[Except view]	[Get all extensions]	[Not Allowed]	[Explorer]



EXE Name of Process	Select Record Operation	Select based on extension	Is it OK to delete?	Notes
[fsw00ej2.exe]	[Except view]	[Get all extensions]	[Not Allowed]	[Command Prompt (DTK)]
[xcopy.exe]	[Except view]	[Get all extensions]	[Not Allowed]	[Copy Command]
[dllhost.exe]	[Except view]	[Get all extensions]	[Not Allowed]	[Explorer]

[File Operation Log Filter Operation Settings]

Item Name	Description
[File Operation Log Filter Operation Settings]	Select the drive type as the targets for collection of file and folder operation logs can be selected.
[Get All] <b>(Initial Value)</b>	Record the operations of all drives.
[Get file access on removable drives only.]	Record the operation for the drive, the drive type of which is removable disk.
[Get file access on network and removable drive only]	Record the operation for the drive, the drive type of which is network and removable disk.
[Detailed Settings]	The <a href="#">[File Operation Process - Detailed Settings] window</a> will be displayed. Set the folder in which the file operation logs are not collected. (When [No] is selected in [File Operation Log] of the [Log Switches] tab, it cannot be selected.)

[List of File Operation Log Obtaining Process]

Item Name	Description
[List of File Operation Log Obtaining Process]	The processes and conditions during the obtaining of file operation logs are displayed in lists. <b>Initial Value:</b> <a href="#">“Initial Value Displayed in [File Operation Process]”</a> will be displayed.
[Process EXE Name]	Enter the EXE name of a process regarded as the target for the collection of file and folder operation logs.  Up to 254 single-byte characters can be entered. (Alphabets are not case-sensitive)  In addition, [.com] or [.exe] can be entered in the extension of a process. However, if double-byte characters or the following symbols are used, error will occur. “\”“/”“:”“*”“?”“”“<”“>”“ ”  <b>Initial Value:</b> Not Specified.
[Select Record Operation]	Select the operation that is recorded as a log.  - [Get all] The operations of all files and folders will be recorded.  - [Except view] <b>(Initial Value)</b> The operations of files and folders apart from viewing will be recorded.  - [Do not get] Operations of all files and folders will not be recorded.
[Select according to Extension]	Select the extension of the file name that is recorded as a log.

Item Name	Description
	<p>- [Get all extensions] Select when collecting the file operation logs of all files (extensions) accessed by the process (application). In these files, in addition to data files, execution modules and temporary files indicated by the following extensions are also included:</p> <ul style="list-style-type: none"> <li>- exe</li> <li>- dll</li> <li>- ini</li> <li>- tmp</li> <li>- lnk</li> <li>- inf</li> </ul> <p>- [Select extension] (Initial Value) This is selected when collecting only the necessary file operation log. The operations of entering extensions in the [File Operation Extension] tab will be recorded.</p> <p>* When operating the process (application of files or folders in the similar way as Explorer and [Get all extensions] is selected, a large amount of [View] logs will be collected. Therefore, it is recommended to select [Select extension] when collecting only the necessary operation logs, such as data files.</p>
[Notes]	<p>Enter the memo information of process name. Maximum 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> Not Specified.</p>
[Add/Update]	<p>Add the entered information to the list. Up to 30 cases of information can be registered including the number of processes that are preset in the system.  In addition, the changed information shall also be set.</p>
[Delete]	<p>Delete the selected information of [List of File Operation Log Obtaining Processes].</p>

**[When adding a process]**

Enter the above set items and click the [Add/Update] button.

Up to 30 cases of information can be registered including the number of processes that are preset in the system.

**[When updating the existing information]**

Select the lines to be updated from the [List of File Operation Log Obtaining Processes], modify the following information and click the [Add/Update] button.

The [EXE Name of Process] cannot be updated. If the [Can be Deleted or Not] of a certain line is set to [No], the [Select Record Operation] cannot be set to [Get All].

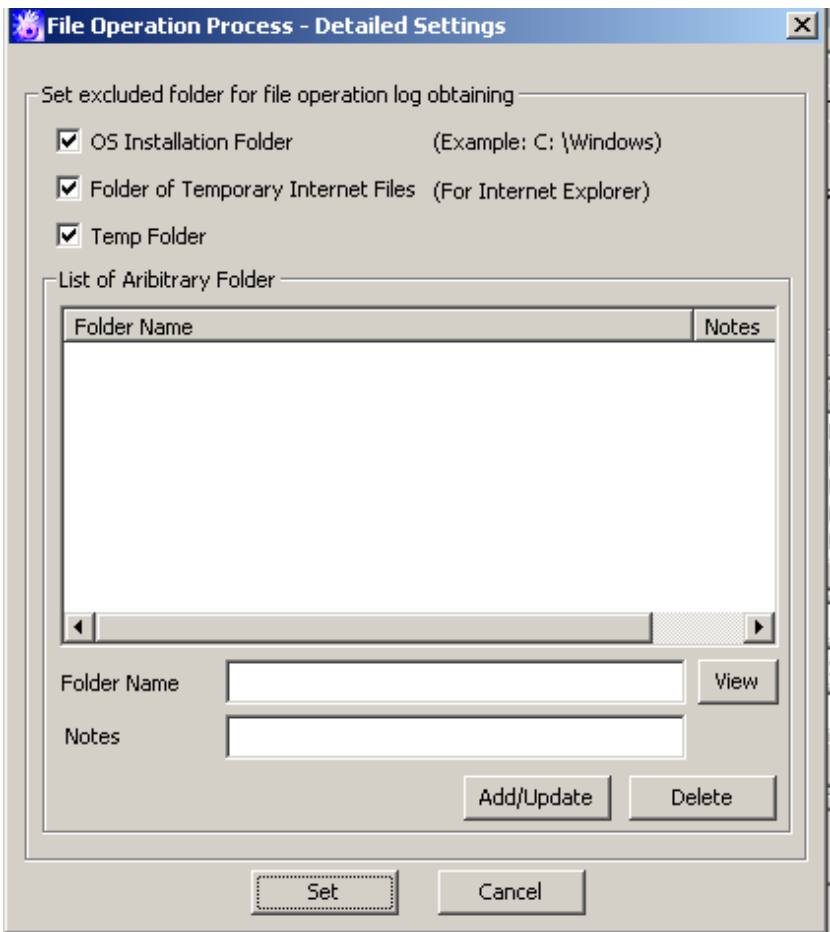
- [Select Record Operation]
- [Select according to Extension]
- [Notes]

**[When deleting information]**

Select the lines to be deleted from the [List of File Operation Log Obtaining Processes], and click the [Delete] button.

But If the [Is it OK to delete?] of a certain line is set to [No], the line cannot be deleted.

**[File Operation Process - Detailed Settings] window**



[Set excluded folder for file operation log obtaining]

Item Name	Description
[OS Installation Folder]	Select this checkbox when accessing the files on the OS installation folder but when the file operation logs are not to be obtained. When it is selected, the file operation logs of folders and subfolders under the OS installation folder will become excluded targets. <b>(Initial Value):</b> Selected (*)
[Folder of Temporary Internet Files]	Select this checkbox when accessing the files on the folder of Temporary Internet Files, but when the file operation logs are not to be obtained. <b>(Initial Value):</b> Selected (*)
[Temp Folder]	Select this checkbox when accessing to the files on the following folders, but the file operation logs are not to be collected. <ul style="list-style-type: none"> <li>- The folder specified according to the user environment variable TEMP and TMP.</li> <li>- The folder a specified according to the system environment variable TEMP and TMP.</li> </ul> <b>(Initial Value):</b> Selected (*)
[List of Arbitrary Folder]	The fixed disk folder excluded from the acquisition of file operation logs can be set and deleted.
[Folder Name]	Specify the fixed disk folder excluded from the acquisition of file operation logs with full path. Up to 254 bytes can be specified. It is not case-sensitive. A maximum of 100 folder names can be registered.

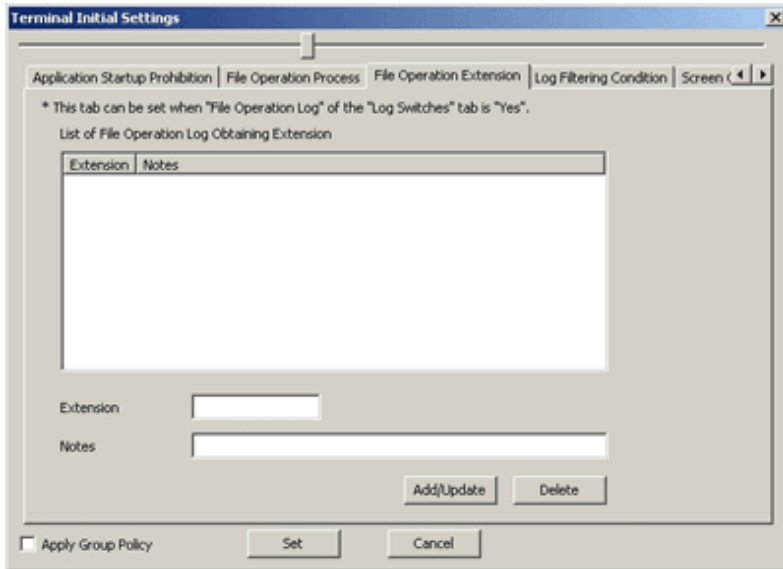
Item Name	Description
	<p>Specify the folder by adding “\” or “/” after the drive’s name + colon (:), Specifying the drive name only is also allowed (“D” .etc). When only the drive’s name is specified, the file operation log under the D drive cannot be obtained.</p> <p>When the drive specified in this window is the network drive or removable drive in the client (CT), it cannot become an excluded folder for obtaining file operation log.</p> <p>[Example] When the “D:\temp” in the window is specified as the excluded folder,</p> <ul style="list-style-type: none"> <li>- When the D drive of “Client (CT) A” is the fixed disk, it will become an excluded folder. Even if the files in the D:\temp folder is deleted, the file operation logs will not be obtained.</li> <li>- When the D drive of “Client (CT) B” is the removable drive that can use the USB memory, it will not become an excluded folder. After deleting the files in the D:\temp folder, the file operation logs can be obtained.</li> </ul> <p>The same folder name cannot be registered more than once (“D:\aaa” and “D:\aaa\bbb” can be registered at the same time.).</p> <p>The folder with an extension should be distinguished from the folder without extension. (When “d:\data” is specified as the excluded folder, “d:\data.tmp” will not become the excluded folder.) To make “d:\data.tmp” into the excluded folder, please register “d:\data.tmp”.</p> <p><b>Initial Value:</b> Not Specified.</p>
[Notes]	<p>Enter the memo information, etc. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> Not Specified.</p>
[View]	<p>The folder structure of the PC with the Management Console installed can be viewed. When the excluded folder is set in the client (CT) with a different folder structure from that of the PC with the Management Console installed, please enter the full path in [Folder Name].</p>
[Add/Update]	<p>Add the folder excluding the acquisition of file operation log to the list. In addition, update the notes of the registered folder (The folder name cannot be updated.).</p>
[Delete]	<p>Delete the folder excluding the acquisition of the file operation log from the list. Select the correspondent lines in the [List of Aribitray Folder], and click the [Delete] button.</p>
[Set]	<p>Confirm the input content and return to the “File Operation Process” tab.</p>
[Cancel]	<p>Do not save the set information and close the window.</p>

\*)When it is upgraded from the version earlier than Systemwalker Desktop Keeper V13.2.0, all the items are unselected.

### 2.4.1.7 Settings of [File operation extension] Tab

For the file (extension) accessed by the process set in the [File Operation Process] tab, when the file operation log is collected, the extension can be set in the [File Operation Extension] tab.

When [File Operation Log] in the [Log Switches] tab is [Yes], the set items in the [File Operation Extension] tab can be set.



Item Name	Description
[List of File Operation Log Obtaining Extension]	<p>Display the extension of the registered and obtained file operation log.</p> <p>When the number of registered extensions is 0, even if the [Select Extension] has been set in [Select According to Extension] of the registered process in the [File Operation Process] tab, the log of that process will not be collected.</p> <p><b>Initial Value:</b> Not Specified.</p>
[Extension]	<p>Enter the extension as the target for the collection of file and folder operation logs. The "." of extension is not required. (It cannot be entered.)</p> <p>Up to 16 single-byte characters (Alphabets are not case-sensitive) can be entered.</p> <p>Error will occur if the following symbols are used.            “\” “/” “:” “*” “?” “ ” “&lt;” “&gt;” “ ”</p> <p>If the wildcard (*) is used, "*" should be put at the beginning or at the end of the extension.</p> <ul style="list-style-type: none"> <li>- When forward matching is specified. Enter "Extension". [Example] x1*</li> <li>- When backward matching is specified Enter "Extension". [Example] *ls</li> </ul> <p>The wildcard "*" cannot be entered in other locations.            In addition, the wildcard "*" cannot be entered alone Please enter it in combination with characters.</p> <p><b>Initial Value:</b> Not Specified.</p>
[Notes]	<p>Enter the extension and memo information.</p> <p>Up to 128 single-byte characters (64 double-byte characters) can be entered.</p> <p><b>Initial Value:</b> Not Specified.</p>
[Add/Update]	<p>Add the entered information to the list.</p> <p>Up to 20 cases can be registered.</p> <p>In addition, the modified information should be set.</p>
[Delete]	<p>Delete the information selected in the [List of File Operation Log Obtaining Processes].</p>

**[When adding an extension]**

Enter the above set items and click the [Add/Update] button.

Up to 20 cases can be registered.

**[When updating the existing information]**

Select the lines to be updated from [List of File Operation Log Obtaining Extension], modify the [Notes] information and click the [Add/Update] button.

The [Extension] cannot be updated.

**[When deleting information]**

Select the lines to be deleted from [List of File Operation Log Obtaining Extension], and click the [Delete] button.

### 2.4.1.8 Settings of [E-mail Sending] Tab

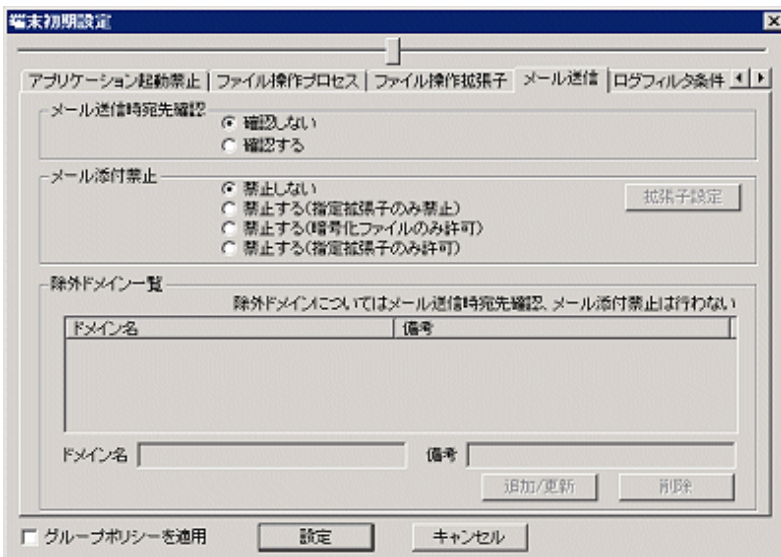
**This function is not available.**

The following settings can be performed in the [E-mail Sending] tab:

- Allow or prohibit to add E-mail file attachment
- Whether or not to confirm the recipient address for E-mail sending.
- Settings of the exclusion domain of file attachment prohibition and recipient address confirmation.

According to the set conditions, the message for confirming the recipient address will be displayed when an E-mail is being sent. Attaching permitted or prohibited files to an E-mail for sending can be permitted or prohibited.

The following section describes the settings of the [E-mail Sending] tab.



**[Recipient Address Confirmation during E-mail Sending]**

This item has nothing to do with the acquisition policy of [E-mail Sending Log] in the [Log Switches] tab.

Item Name	Description
[Unconfirmed] <b>(Initial Value)</b>	It has nothing to do with the recipient address at E-mail sending and the warning message will not be displayed.
[Confirmed]	When the user is sending an E-mail to the domain apart from the domains set in the [List Exclusion Domains], the warning message will be displayed. The user will confirm whether the E-mail address of the warning domain is correct or not in the warning message window, and the E-mail can be sent only after the checkbox is selected.

**[E-mail Attachment Prohibition]**

This item has nothing to do with the acquisition policy of [E-mail Sending Log] in the [Log Switches] tab.

In addition, even if there is only one prohibited file in the attachment, the E-mail (E-mail text and all file attachments) cannot be sent.

Item Name	Description
[Do not Prohibit] (Initial Value)	Sending or saving the E-mail after adding the file attachment is prohibited.
[Prohibit (Prohibit the specified extension only)]	<p>Sending or saving the E-mail after adding the file with the specified extension is prohibited.</p> <p>The following describes the E-mail software:</p> <ul style="list-style-type: none"> <li>- In the case of port monitoring mode: the E-mail software that uses SMTP protocol will be used.</li> <li>- In the case of V12.0L20-V13.0.0 compatible mode: the following E-mail software will be used: <ul style="list-style-type: none"> <li>- Microsoft® Outlook® Express 5.5</li> <li>- Microsoft® Outlook® Express 6.0</li> <li>- Microsoft® Outlook® 2000</li> <li>- Microsoft® Outlook® 2002</li> <li>- Microsoft® Outlook® 2003</li> </ul> </li> </ul>
[Prohibit (Permit the encrypted files only)]	<p>Only the files encrypted by the following software can be added to E-mail for sending and saving:</p> <ul style="list-style-type: none"> <li>- The files encrypted by all versions of Systemwalker Desktop Keeper</li> <li>- The files encrypted by Systemwalker Desktop Encryption V12.0L10/L20, V13.0.0</li> <li>- The self-decrypting files of SecureBOX V2.0</li> <li>- The files encrypted by FENCE-PRO V5/V6</li> </ul>
[Prohibit (Permit the specified extension only)]	<p>Sending or saving the E-mail after adding the file with the specified extension is permitted.</p> <p>The settings are valid when all the following conditions are satisfied:</p> <ul style="list-style-type: none"> <li>- When setting policy for the client (CT) is V14.2.0 or later;</li> <li>- When the [Settings of E-mail Control Mode] is set to [Port Monitoring Mode];</li> </ul> <p>When the version of the client (CT) is V13.0.0 or later, or [12.0L20-V13.0.0 Compatible Mode], the specified extension that is permitted to be added will become invalid and any file can be added as the E-mail attachment.</p>
[Extension Settings]	<p>The <a href="#">[E-mail Sending - Set E-mail Attachment Prohibition Extension] window</a> window will be displayed.</p> <p>(Set the extension name of file that is permitted or prohibited in an E-mail attachment.)</p>

[List of Exclusion Domains]

Item Name	Description
[List of Exclusion Domains]	It is not necessary to confirm the recipient address when sending an E-mail to the domain displayed in the list, and file attachment will not be prohibited.
[Domain]	<p>Enter the domain that allows E-mail sending.</p> <p>Up to 254 single-byte characters (Alphabets are not case-sensitive) can be entered.</p> <p>Error will occur if the following symbols are used.</p> <p>“~”, “!”, “@”, “#”, “\$”, “^”, “&amp;”, “*”, “(”, “)” “=”, “+”, “[”, “]”, “{”, “}”, “\”, “ ”, “;”, “:”, “,”, “.”, “&lt;”, “&gt;”, “/”, “?”, “%”</p> <p><b>Initial Value:</b> Not Specified.</p>
[Notes]	<p>Enter the memo information related to the domain.</p> <p>Up to 128 single-byte characters (64 double-byte characters) can be entered.</p> <p><b>Initial Value:</b> Not Specified.</p>
[Add/Update]	<p>Add the domain that allows E-mail sending.</p> <p>Up to 100 domains can be added.</p>

Item Name	Description
	After modifying the [Notes] of selected lines in [List of Exclusion Domains], the information will be updated (The domain name cannot be updated).
[Delete]	The selected lines in [List of Exclusion Domains], will be deleted.

### [E-mail Sending - Set E-mail Attachment Prohibition Extension] window

Set the file extension permitted or prohibited to be added.



[List of Extensions]

Item Name	Description
[List of Extensions]	The extension name of the file that is permitted or prohibited in E-mail file attachment will be displayed in a list. <b>Initial Value:</b> Not Specified.
[Extension]	Enter the extension name of the file that is permitted or prohibited in E-mail file attachment. The “.” of extension is not required. (It cannot be entered)  A maximum of 16 single-byte characters (Alphabets are not case-sensitive) can be entered. Error will occur if the following symbols are used. “\” “/” “:” “*” “?” “ ” “<” “>” “ ” <b>Initial Value:</b> Not Specified.
[Notes]	Enter the extension and memo information. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> Not Specified.
[Add/Update]	Add the permitted or prohibited extension of E-mail file attachment. Up to 100 cases can be added.  After modifying the [Notes] of selected lines in the [List of Extensions], the information will be updated (The [Extension] cannot be updated).
[Delete]	Delete the lines selected in the [List of Extensions].
[OK]	Confirm the input content and return to the [E-mail Sending] tab.
[Cancel]	Do not save the set information and close the window.



## 2.4.1.9 Settings of [Log Filtering Condition] Tab

The conditions for collecting the window title obtaining log can be set in the [Log Filtering Condition] tab.

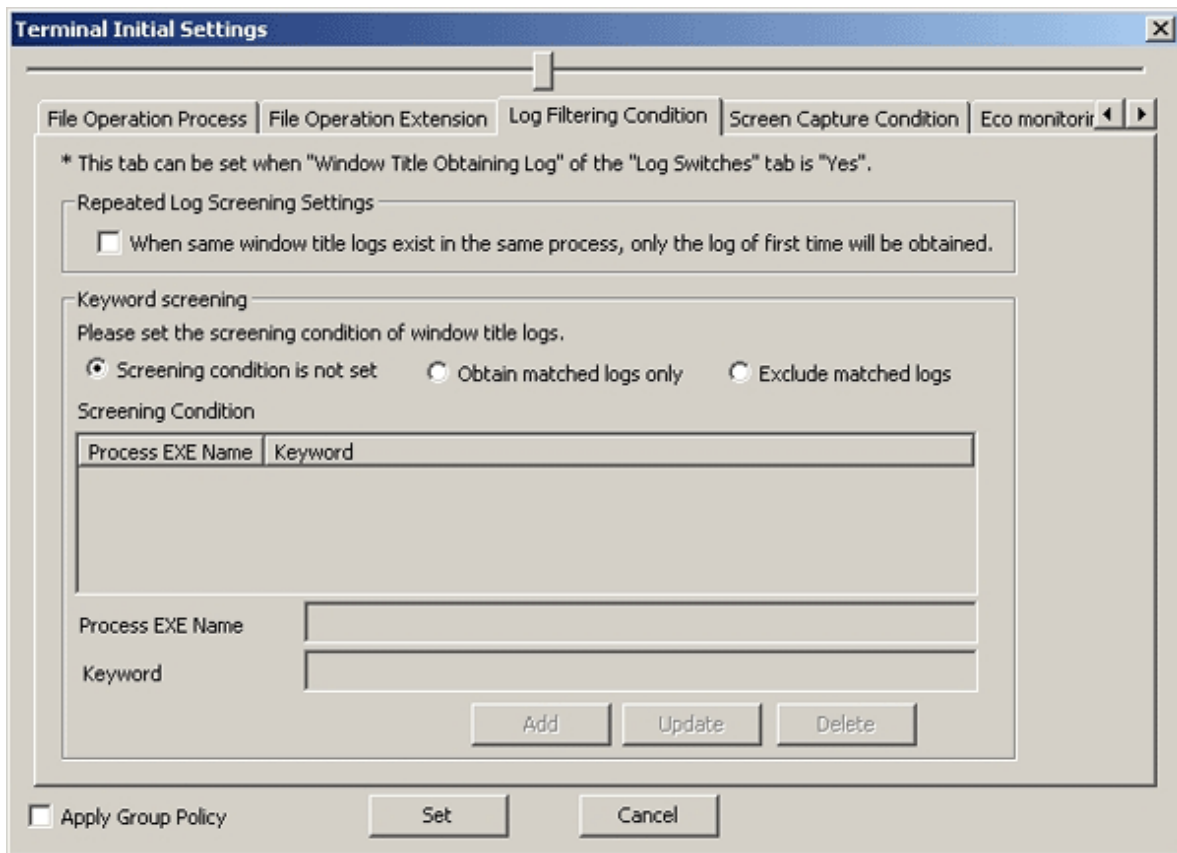
Though a large number of window title obtaining logs can be collected in order to record all operations on the PC, there will be many repeated logs. Therefore, to avoid collecting the repeated logs, the filtering condition should be set.

The log filtering condition involves two aspects, and two conditions can be specified at the same time.

- Settings of Repeated Log Screening:  
Only the first log will be collected for the same process and same window title.
- Keyword Screening:  
By specifying the process names and keywords, the window title logs including the specified process names and keywords can be collected or excluded.

When [Yes] is selected in [Window Title Obtaining Log] of the [Log Switches] tab, the [Log Filtering Condition] tab can be set.

The following describes the settings in the [Log Filtering Condition] tab.



[Repeated Log Filter Setting]

Item Name	Description
[Repeated Log Screening Settings]	<p>Select the method of obtaining repeated logs.</p> <ul style="list-style-type: none"> <li>- When it is selected: The first log will be collected for the same process and same window title.</li> <li>- When it is not selected (<b>Initial Value</b>): All window title obtaining logs will be collected.</li> </ul>

[Keyword Screening]

Item Name	Description
[Screening condition is not set] <b>(Initial Value)</b>	The window title logs will not be screened according to process name and keyword.
[Obtain matched logs only]	Only the logs belong to the specified process name and the window title log partially matches with the keyword specified in screening conditions will be collected.
[Exclude matched Logs]	The logs belong to the specified process name, and the window title log that partially matches with the keyword specified in screening conditions will not be collected.
[Screening Condition]	Display the set conditions in a list. <b>Initial Value:</b> Not Specified.
[Process EXE Name]	Enter the EXE name of process that collects window title logs. When the [Exclude matched Logs] is selected in the Window Title Obtaining Log Screening Condition, specify the name of process that does not collect window title obtaining logs.  Up to 254 single-byte characters (127 double-byte characters) can be entered. (Alphabets are not case-sensitive) [.com] or [.exe] can be entered in the extension of process. Error will occur if the following symbols are used. “\” “/” “:” “*” “?” “ ” “<” “>” “[”  When it is not specified, logs of all processes will be collected (or excluded). <b>Initial Value:</b> Not Specified.
[Keyword]	Enter the keyword for collecting window title obtaining logs. (When the window title includes (partially match) / does not include (partially match) the keyword specified here, window title logs will be collected.) When the Window Title Log Screening Condition is set to [Exclude matched Logs], specify the keyword for not to collect window title obtaining logs. [Example] <ul style="list-style-type: none"><li>- Save as</li><li>- Print</li></ul> Up to 254 single-byte characters (127 double-byte characters) can be entered. (Alphabets are not case-sensitive)  When [Keyword] is not specified, all window title obtaining logs of processes specified in [Process EXE Name] will be collected (will not be collected). <b>Initial Value:</b> Not Specified.
[Add]	Add conditions in [Screening Conditions]. Up to 30 cases can be added.
[Update]	After modifying the information of lines selected in the [Screening Condition], the information will be updated.
[Delete]	Delete the lines selected in the [Screening Condition].

In [Filtering Condition], when [Process EXE Name] and [Keyword] are specified at the same time, the AND condition is used. When [Process EXE Name] and [Keyword] are specified separately in lines, the OR condition is used.

#### **[When adding a condition]**

Enter the above set items and click the [Add] button.

Up to 30 cases can be registered.

#### **[When updating the existing information]**

Select the lines to be updated from the [Screening Condition], modify the information and click the [Update] button.

**[When deleting information]**

Select the lines to be deleted from the [Screening Condition], and click the [Delete] button.

### 2.4.1.10 Settings of [Screen Capture Condition] Tab

The condition of collecting the screen capture can be set in the [Screen Capture Condition] tab. Set the conditions for collecting the window title obtaining logs in the [Screen Capture Condition] tab.

When [Yes] is selected in [Window Title Obtaining Log] of the [Log Switches] tab, the [Screen Capture Condition] tab can be set.

The settings related to screen capture can be performed in the [Terminal Operation Settings] window (Settings item: [Attached data condition settings]). Please refer to “[2.4.2 Perform Terminal Operation Settings](#)” for details.

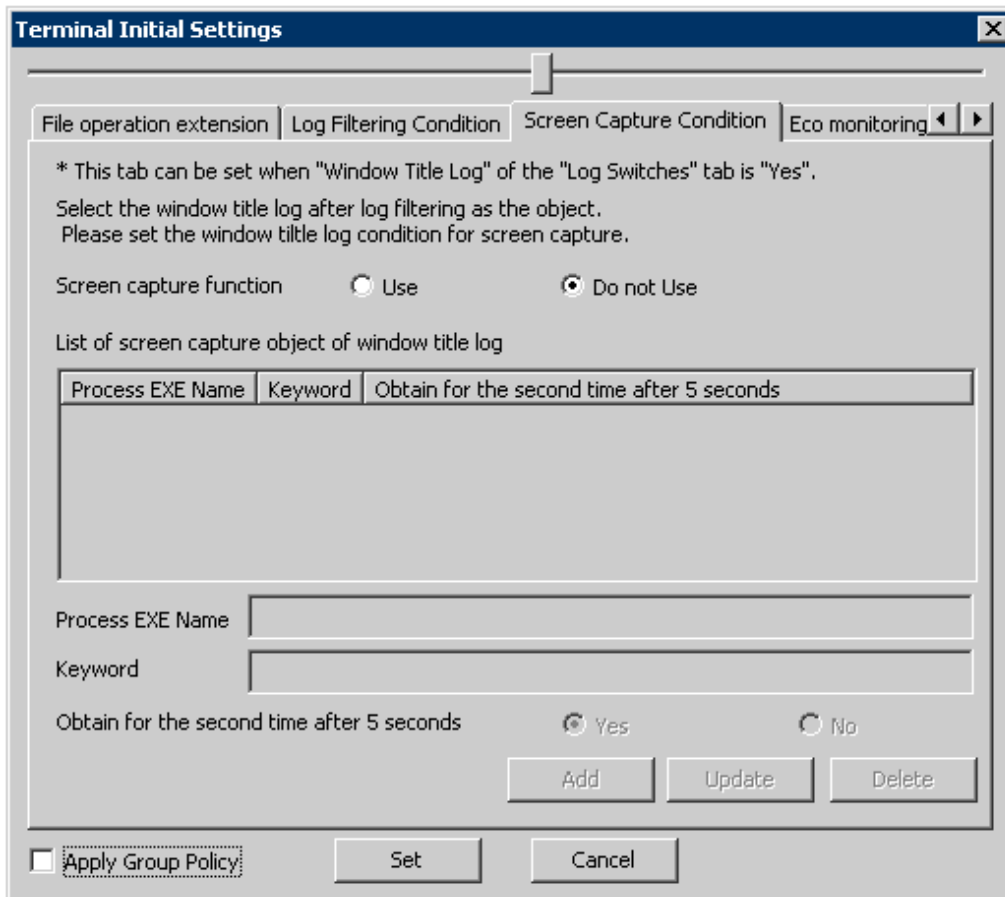


**Note**

**Please backup or delete the screen capture data regularly.**

According to the screen capture condition, storing a large amount of screen capture data on the server (the client (CT) according to terminal operation settings) will cause insufficient disk capacity. Therefore, please regularly confirm the capacity and backup and delete.

The following describes the settings in the [Screen Capture Condition].



Item Name	Description
[Screen capture function]	Select whether to obtain screen capture.

Item Name	Description
	<ul style="list-style-type: none"> <li>- [Use] Obtain screen capture.</li> <li>- [Do not Use] (<b>Initial Value</b>) Do not obtain screen capture.</li> </ul>
[List of screen capture object of window title log]	<p>The conditions for obtaining screen capture are displayed in a list.</p> <p><b>Initial Value:</b> Not Specified.</p>
[Process EXE Name]	<p>Enter the EXE name of screen capture.</p> <p>Up to 254 single-byte characters (127 double-byte characters) can be entered. (Alphabets are not case-sensitive)</p> <p>[.com] or [.exe] can be input in the process extension. Error will occur if the following symbols are used. “\”“/”“:”“*”“?”“”“&lt;”“&gt;”“ ”</p> <p>When the EXE name of process is set to blank, logs of all process will be collected (excluded).</p> <p><b>Initial Value:</b> Not Specified.</p>
[Keyword]	<p>Enter the keyword for collecting screen capture. (When the window title includes (partially match)/does not include ((partially match) the keyword specified here, screen capture can be obtained.)</p> <p>[Example]</p> <ul style="list-style-type: none"> <li>- Save as</li> <li>- Print</li> </ul> <p>Up to 254 single-byte characters (127 double-byte characters) can be entered. (Alphabets are not case-sensitive)</p> <p>When the EXE name of process is entered in the [EXE Name of Process], please make sure to input in [Keyword].</p> <p><b>Initial Value:</b> Not Specified.</p>
[Obtain for second time after 5 seconds]	<p>Set the second acquisition 5 seconds later after the screen capture has been obtained. When it is expected to obtain screen capture continuously to get further knowledge of operation status, please select [Yes].</p> <ul style="list-style-type: none"> <li>- [Yes] Obtain screen capture for the second time after 5 seconds.</li> <li>- [No] Obtain screen capture once only.</li> </ul> <p>When selecting [Yes], the screen capture will be collected for the second time after 5 seconds. However, in the 5 seconds from the first collection to the second collection, even if a new window that satisfies the condition of screen capture collection exists, that screen capture will not be collected. As it is the second screen capture of the initial window, “2” which indicates two screen capture collections will be displayed in the [Additional] in the log list of Log Viewer.</p>
[Add]	<p>After selecting [Use] in the [Screen Capture Function], the condition of screen capture collection will be added to the list.</p> <p>Up to 10 cases can be registered.</p>
[Update]	<p>After modifying the information of lines selected in the [List of screen capture object of window title Log], the information will be updated.</p>
[Delete]	<p>Delete the lines selected in the [List of screen capture object of window title].</p>

In [List of screen capture object of window title], when [Process EXE Name] and [Keyword] are specified at the same time, it is the AND condition.

When [Process EXE Name] and [Keyword] are specified separately in lines, the OR condition is used.

The settings in the [Screen Capture Condition] tab and [Log Filtering Condition] tab are set using the AND condition. Therefore, even if the policy of obtaining screen capture is set, the log screening condition will be considered as not set when screen capture cannot be obtained.

**[When adding a condition]**

Enter the above settings items and click the [Add] button.

Maximum 10 cases can be registered.

**[When updating the existing information]**

Select the lines to be updated from the [List of screen capture object of window title], modify the information and click the [Update] button.

**[When deleting information]**

Select the lines to be deleted from the [List of screen capture object of window title], and click the [Delete] button.

### 2.4.1.11 Settings of [Eco monitoring settings] Tab

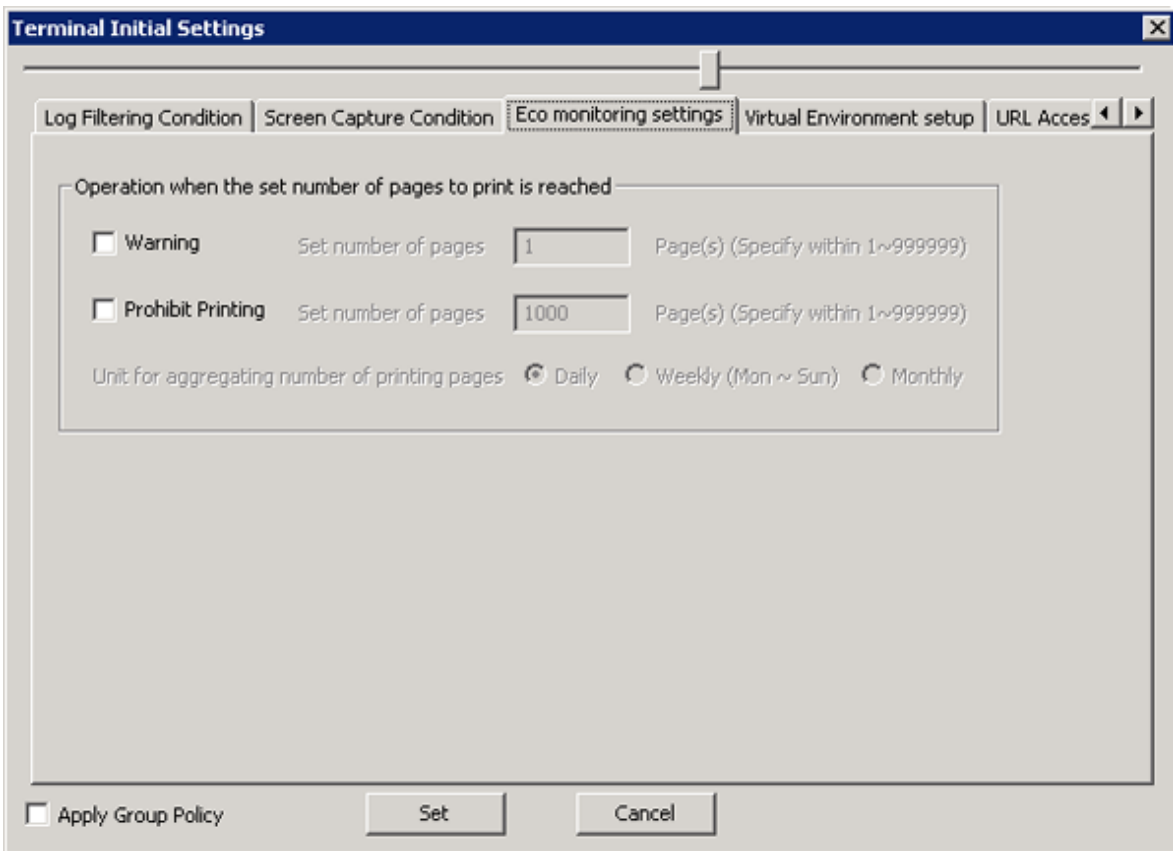
By monitoring the printed pages, the conditions can be set in the [Eco Monitoring Settings] tab to reduce unnecessary printing.

In the [Settings of Printing Monitoring Mode] during the installation of CT, this function is effective when [Monitor the printing of all printers set in the terminal (Recommended)] is selected.

When [Yes] is selected in [Printing Operation log] of the [Log Switches] tab, the monitoring condition can be set.

When the set number of pages is reached and the printing is prohibited, a warning message will be displayed to the user of the client (CT), and the printing can be prohibited. At the same time, it will be recorded as a violation to the printing prohibition log.

The settings of the [Eco Monitoring Settings] tab will be processed as CT policy.



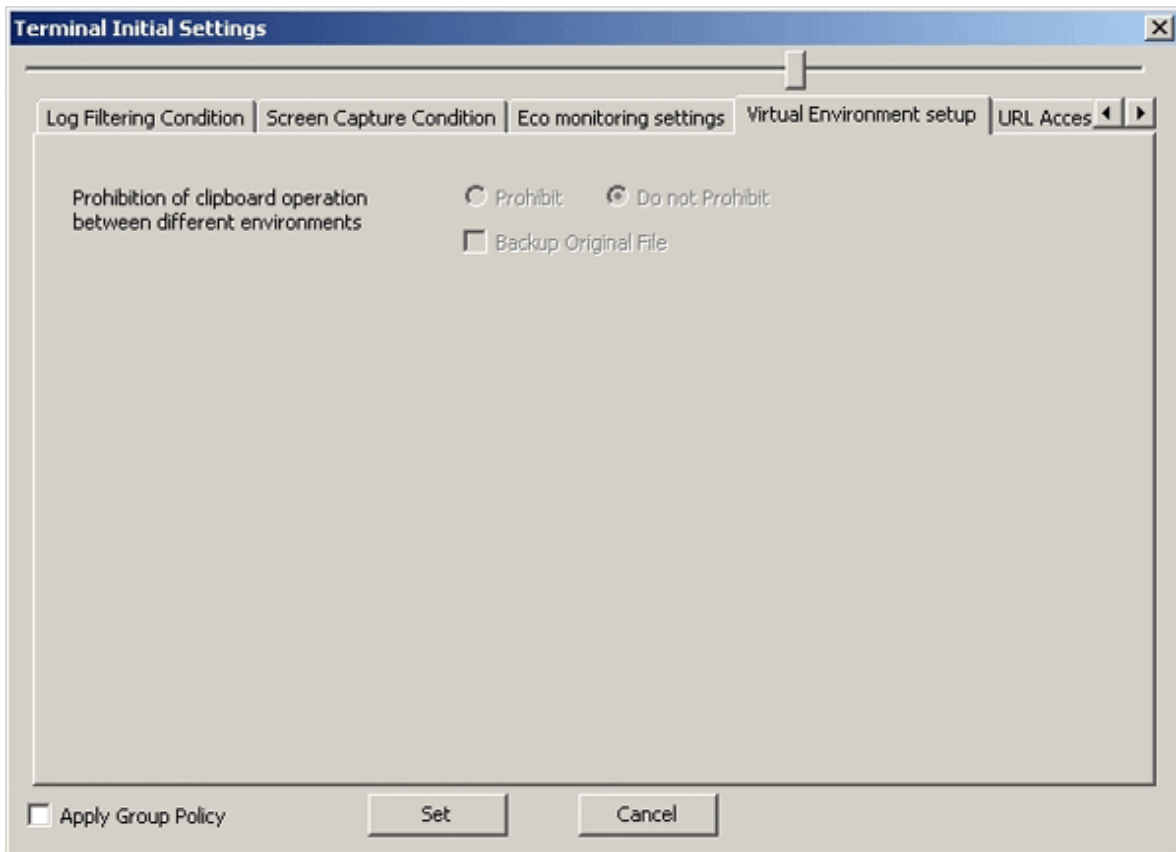
[Operations when the set number of pages to print is reached]

Item Name		Instruction
[Warning] (*)		<ul style="list-style-type: none"> <li>- When this is selected: When the set number of printed pages is reached, the warning message will be displayed. It will be recorded as a printing operation log. The actions of a document writer (Microsoft Office Document Image Writer, Adobe PDF, etc.) that does not print on paper will be counted as printed pages.</li> <li>- [Set number of pages]: the set scope of the number of pages that triggers the display of message is 1-999999. The initial value is 1.</li> <li>- When this is not selected (Initial Value): Though the printing pages can be counted, the messages cannot be displayed.</li> </ul>
[Prohibit Printing](*)		<ul style="list-style-type: none"> <li>- When this is selected: When the set number of printed pages is reached, the printing will be prohibited. The application that allows printing specified in the [Printing Prohibition] tab cannot print. The printing for a document writer (Microsoft Office Document Image Writer, Adobe PDF, etc) cannot be performed either. It will be recorded as a violation to printing prohibition log. When this item is selected, the [Warning] will be selected automatically. When the number of printed pages reaches the value of prohibition at the beginning of printing, the printing cannot be performed (The message of printing prohibition will be displayed.). When the prohibited number of pages is reached in the process of printing, the printing will be interrupted. The following printing will be prohibited. When the administrator notification settings are performed, the administrator will be notified by E-mail. In addition, an event log will be recorded.</li> <li>- [Set number of pages]: the set scope of the number of pages that triggers printing prohibition is 1-999999. The initial value is 1000.</li> <li>- When this is not selected: (Initial Value) Though the printing pages will be counted, the printing will not be prohibited.</li> </ul>
[Unit for aggregating number of printed pages]	[Daily] <b>(Initial Value)</b>	Monitor the number of printed pages in 24 hours. If the "Date" of PC time is changed, the number of printed pages will be reset to 0.
	[Weekly(Mon~Sun)]	Monitor the number of printed pages in a week. If the PC time is "12am of Monday", the number of printed pages will be reset to 0.
	[Month]	Monitor the number of printed pages in a month If the "Month" of PC time is changed, the number of printed pages will be reset to 0.

\*) When both [Warning] and [Prohibit Printing] are selected, please input the set number of pages in [Warning]  $\leq$  the set number of pages in [Prohibit Printing].

## 2.4.1.12 Settings of [Virtual Environment setup] Tab

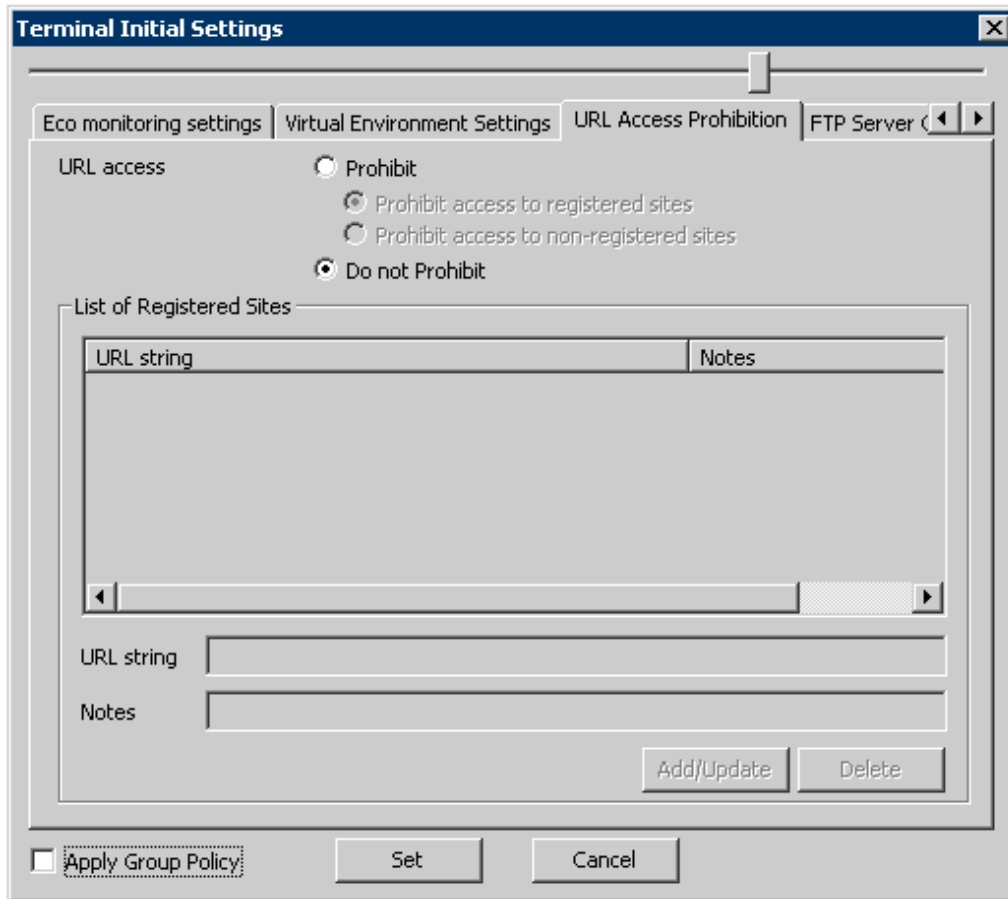
The clipboard operation prohibition can be set in the [Virtual Environment setup] tab.



Item Name	Description
[Prohibition of clipboard operation between different environments]	When the [Clipboard Operation Log (Virtual Environment)] option in the [Log Switches] tab is [No], settings can be performed.
[Prohibit]	The clipboard operation is prohibited.
[Do not Prohibit] (Initial Value)	The clipboard can be used to copy from the virtual environment to the physical environment or from the physical environment to the virtual environment.
[Backup Original File]	When the option of [Prohibition of clipboard operation between different environments] is [Prohibit], the item can be set. When this is selected: The information (text, image) copied from the clipboard will be backed up as the original file. When this is not selected: <b>(Initial Value)</b> The information (text, image) copied from the clipboard will not be backed up as the original file.

### 2.4.1.13 Settings of [URL Access Prohibition] Tab

The URL prohibited from being accessed can be set in the [URL Access Prohibition] tab.



Item Name		Description
[URL access]	[Prohibit]	Access to URL is prohibited.
	[Prohibit access to registered sites]	Access to the URL specified in [List of Registered Sites] is prohibited.
	[Prohibit access to non-registered sites]	Access to the URL other than the one specified in the [List of Registered Sites] is prohibited.
	[Do not Prohibit] <b>(Initial Value)</b>	Any URL can be accessed.
[List of Registered Sites]		The URL that is prohibited or allowed to be accessed and the memo related to the URL will be displayed. <b>Initial Value:</b> Not Displayed.
[URL string]		Enter the character string that contains part of the domain name of the prohibited or allowed to be accessed URL. [Example] When fujitsu.com is set in the [URL string], the following address will be prohibited or allowed. http://www.fujitsu.com/global/ Up to 254 single-byte alphanumeric characters and symbols (*) (127 double-byte characters) can be entered (Alphabets are not case-sensitive) *) The valid characters of URL are as follows: “.” “_” “*” “(” “)” “_” “:” “%” “+” A multi-byte character domain name cannot be used. Up to 100 cases can be registered. <b>Initial Value:</b> Not Specified.

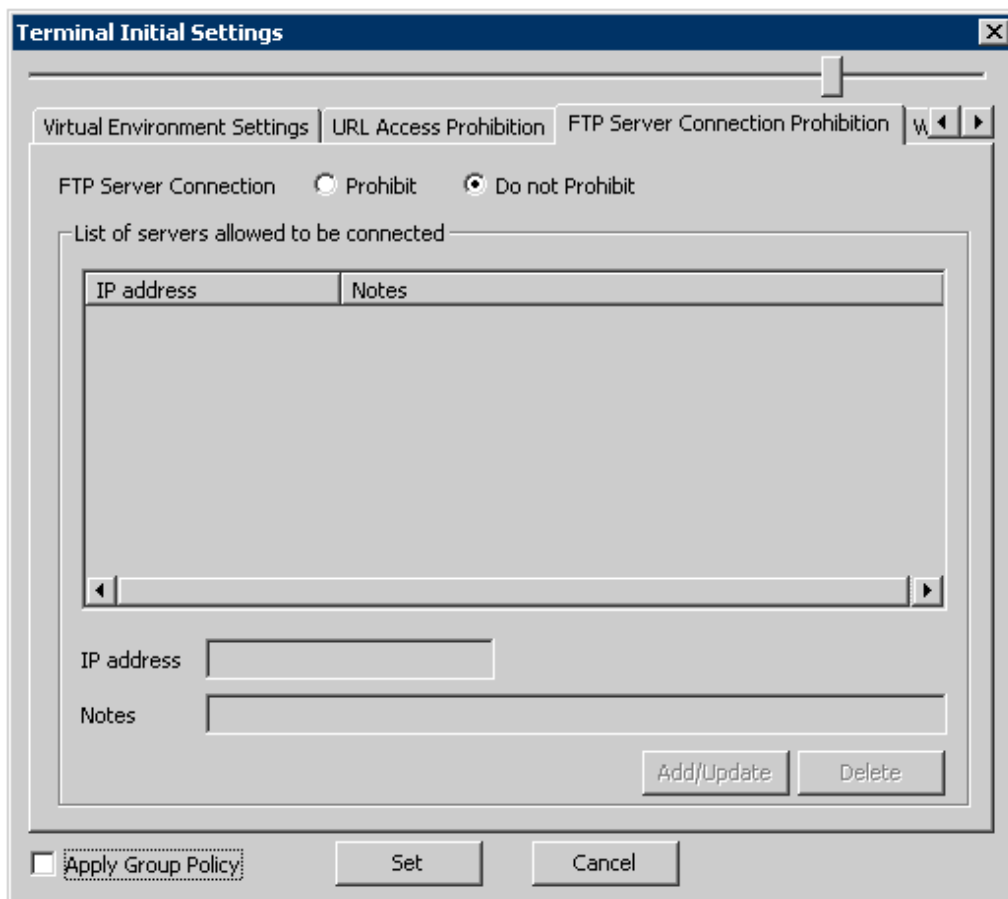


Item Name	Description
[Notes]	Enter the information such as the memo of URL. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> Not Specified.
[Add/Update]	URL will be added. Up to 100 cases can be added.  After modifying [Notes] the lines selected in [List of Registered Sites], the information can be updated (The [URL string] cannot be updated.)
[Delete]	The lines selected in [List of Registered Sites] will be deleted.

#### 2.4.1.14 Settings of [FTP Server Connection Prohibition] Tab

Prohibition of the connection to the FTP server which is not permitted by the administrator can be set in the [FTP Server Connection Prohibition] tab.

To prohibit the connection to FTP server from Internet Explorer®, please set in the [URL Access Prohibition] tab.

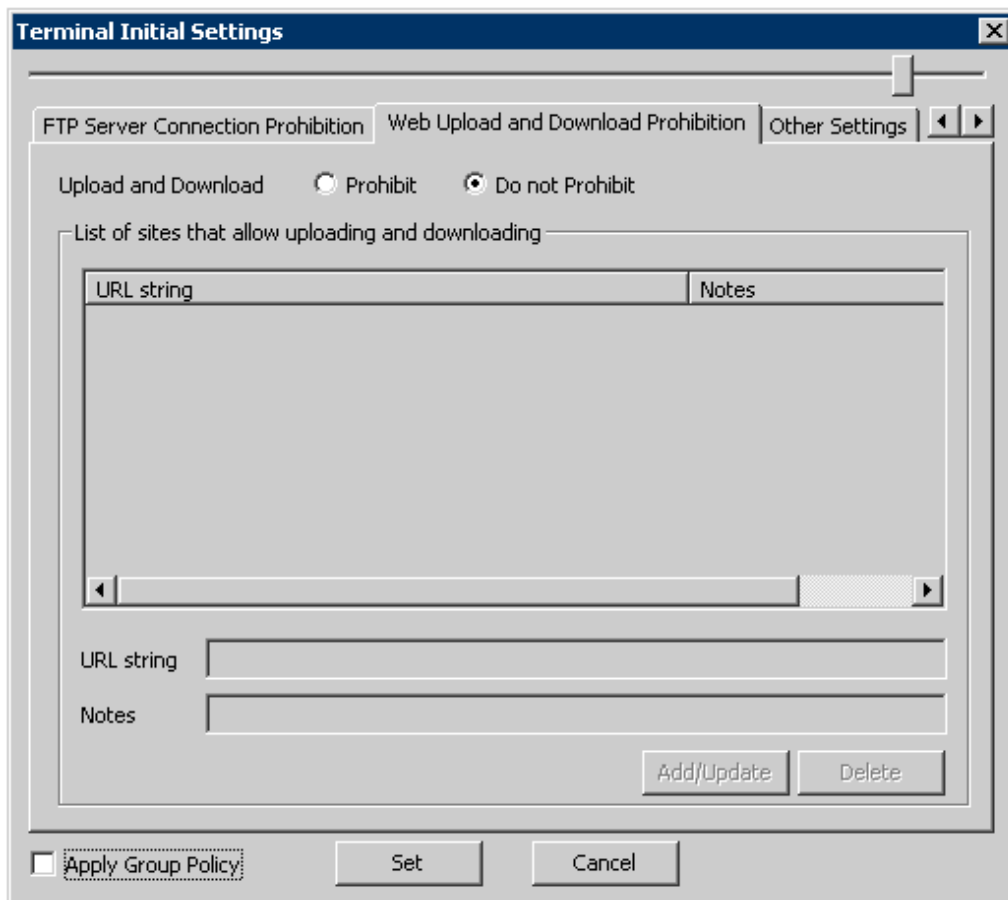


Item Name	Description
[FTP Server Connection]	[Prohibit]
	[Do not Prohibit] ( <b>Initial Value</b> )
	Prohibit the access to the servers that is not specified in the [List of servers allowed be connected].
	Any FTP server can be connected.

Item Name	Description
[List of servers allowed to be connected]	The IP address of FTP server allowed to be connected and the memo related to the server to be connected are displayed. <b>Initial Value:</b> Not Displayed.
[IP address]	Enter the IP address (IPV4 format) of the server to be connected. Up to 100 cases can be registered. <b>Initial Value:</b> Not Displayed.
[Notes]	Enter the memo information of the server allowed to be connected .etc. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> Not Specified.
[Add/Update]	The server allowed to be connected will be added. Up to 100 cases can be added.  After modifying the [Notes] of lines selected in the [List of servers allowed to be connected ], the information will be updated (The [IP Address] and [Connecting Target port] cannot be updated.)
[Delete]	The lines selected in [List of servers allowed to be connected] will be deleted.

### 2.4.1.15 Settings of [Web Upload and Download Prohibition] Tab

The Web upload and download operations permitted by the administrator can be set in the [Web Upload and Download Prohibition] tab.



Item Name		Description
[Upload and Download]	[Prohibit]	The Web upload and download operations that are not in the [List of Sites Allow Upload and Download] tab will be prohibited.
	[Do not Prohibit] <b>(Initial Value)</b>	The upload and download operations can be performed on any website.
[List of sites allow uploading and downloading]		The URL of a Web site that allows upload and download, as well as the memo information related to the URL will be displayed. <b>Initial Value:</b> Not Displayed.
[URL string]		Enter the URL of the Web site that allows upload and download. The site that includes the entered character string will allow all the upload and download. [Example] When fujitsu.com is set in the [URL string], all the following addresses are permitted. http://www.fujitsu.com/global/  Up to 254 single-byte alphanumeric characters and symbols (*) (127 double-byte characters) can be entered. (Alphabets are not case-sensitive) *) The valid characters of URL are as follows: “.” “_” “(” “)” “:” “/” “+”  A multi-byte character domain name cannot be used.  Up to 100 cases can be registered. <b>Initial Value:</b> Not Specified.
[Notes]		Enter the memo information of the URL that allows upload and download. Up to 128 single-byte characters (64 double-byte characters) can be entered. <b>Initial Value:</b> Not Specified.
[Add/Update]		The URL of the Web site that allows upload and download will be added. Up to 100 cases can be added.  After modifying the [Notes] information of lines selected in the [List of sites allow uploading and downloading], the information can be updated (The [URL Character String] cannot be updated.).
[Delete]		The lines selected in the [List of sites allow uploading and downloading] will be deleted.

### 2.4.1.16 Settings of [Other Settings] Tab

The method of sending operation logs from the client (CT) to the Management Server can be set in the [Other Settings] tab. The sent logs are operation logs, prohibition logs and attached data.



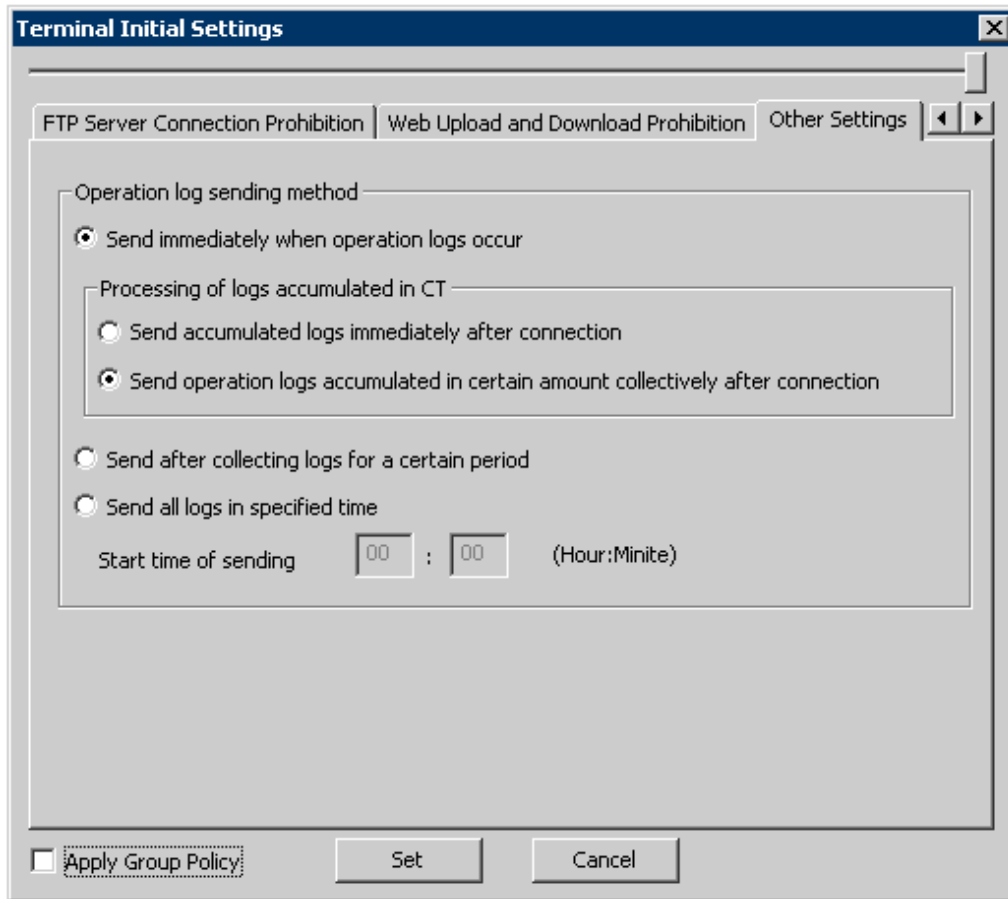
#### Note

#### About sending command operation log to the server

Command logs are always sent immediately after collection (not affected by this setting).

The method of sending can be set according to the following cases:

- When the client (CT) is always connected to the server and network
- When connecting to the server, the logs accumulated in the client (CT) due to the reasons such as a mobile application will be sent immediately.



Operation log sending method

Item Name		Description
[Send immediately when operation logs occur] <b>(Initial Value)</b>		Logs will be sent to the server immediately when they are generated.
	[Processing of logs accumulated in CT]	Set the method of sending the logs accumulated in the client (CT) due to reasons such as a mobile application immediately when the network connects to the server.
	[Send accumulated logs immediately after connection]	When changing from the network disconnection environment to the network connection environment (when the communication with the Management Server and Master Management Server is started), the accumulated logs will be sent to the server immediately from the client (CT).
	[Send operation logs accumulated in certain amount collectively after connection]	When changing from the network disconnection environment to the connection environment (when the communication with the Management Server and Master Management Server is started), the accumulated logs will be sent collectively to the Management Server after reaching to certain amount.  The amount of logs to be sent at one time and the interval for sending are set in the [Terminal Operation Settings] window. Please refer to <a href="#">“2.4.2 Perform Terminal Operation Settings”</a> for details.
[Send after collecting logs for a certain period]		The logs accumulated in a period of time will be sent to the server.  The number of logs to be sent at one time and the interval for sending are set in the [Terminal Operation Settings] window. Please refer to <a href="#">“2.4.2 Perform Terminal Operation Settings”</a> for details.

Item Name	Description
[Send all logs in specified time]	<p>Send logs to server in the specified time.  [Start time of sending] of logs must be set.  [About the Time Required for Completing Log Sending]</p> <p>The standards are as follows. The number of clients (CT number of sets) and amount of logs are basically in proportion to the time required for log sending.</p> <p>Example 1</p> <ul style="list-style-type: none"> <li>- The number of clients (CT number of sets): 1000</li> <li>- Number of daily logs: 1000</li> <li>- Time required for log sending: About 15 minutes at most</li> </ul> <p>Example 2</p> <ul style="list-style-type: none"> <li>- The number of clients (CT number of sets): 2000</li> <li>- Number of daily logs: 1000</li> <li>- Time required for log sending: About 30 minutes at most</li> </ul> <p>The number of logs to be sent at one time and the interval for sending are set in the [Terminal Operation Settings] window. Please refer to “<a href="#">2.4.2 Perform Terminal Operation Settings</a>” for details.</p>

## 2.4.2 Perform Terminal Operation Settings

Perform operation settings of the client (CT) (settings of conditions relating to attached data and method of log sending). Only the system administrator can perform the settings.

The operation settings of the client (CT) is performed in the unit of the Management Server and Master Management Server. The configuration value is obtained from the Management Server and Master Management Server when the client (CT) is started. In addition, when the CT policy is updated immediately, the value of operation settings of the client (CT) will also be updated.

In a 3-level structure, when the initial configuration value of terminal operation settings is changed, it has nothing to do with the Active Directory Linkage and the collective management of user policy, and the value must be reset in all Management Servers (when the client (CT) is connected to the Master Management Server, the Master Management Server should be the same.)



### Note

#### The timing for operation settings to be reflected to the client (CT)

The timing for operation settings to be reflected to the client (CT) is as follows:

- When the client (CT) operation settings are performed and the CT policy is updated immediately in the client (CT), it will be reflected after the next startup of the client (CT).
- When the client (CT) operation settings are performed and the CT policy is not updated immediately in the client (CT) it will be reflected after the next startup of the client (CT).

The set procedure is as follows:

1. Start [Management Console].

2. Select [Terminal Operation Settings] from the [Operation Settings] menu.

→The [Terminal Operation Settings] window is displayed.

3. Enter the following information and click the [Set] button.

[Attached data condition settings]

Item Name	Description
[Attached data accumulation settings]	Specify the location for saving the attached data (screen capture, original file backup in file export). <ul style="list-style-type: none"> <li>- [Server (recommended)] Save the attached data in the Management Server.</li> <li>- [CT] Save the attached data to the client (CT). The data will not be sent to the Management Server. It will be saved to the Save folder under the folder for saving log files in the client (CT).</li> </ul>

Item Name	Description
	<p>The function of managing the saved attached data does not exist. Therefore, the system administrator needs to regularly confirm the saved data. The location for saving attached data is protected by the SYSTEM authority. During confirmation, please add the user of viewing data in the security settings of save folder.</p> <p>For screen capture data, the file name is “CAP-(CTID of 36 characters)-YYYYMMDDHHMMSS-04-02-00-AAAAAA-B.png”, AAAAAA is random digit. B is 1 or 2, 1 is the screen capture obtained at first while 2 is the screen capture obtained after 5 seconds.</p> <p>For the original file backup being exported, the file name is “CAB-(CTID of 36 characters)-YYYYMMDDHHMMSS-11-00-00-AAAAAA-1.(extension of the original file)”, AAAAAA is random digit.</p> <p>The initial value is [Server (Recommended)].</p>
[Invalid interval of screen capture]	<p>To prevent the high load of the client (CT), specify the interval between two screen captures. The initial value (recommended value) is “60”. The minimum value is “1”, and the maximum value is “999”.</p> <p>Within the configuration value, even if the conditions of next screen capture are satisfied, the screen capture cannot be performed. (In window title log, the action of screen capture will be collected. When collecting the screen capture during PrintScreen key operation and PrintScreen key prohibition, even if the settings take effect, collection can be continued.)</p>
[Maximum number of images can be saved in CT]	<p>The number of maximum screen captures saved in the client (CT) can be specified. The initial value (recommended value) is “100”. The minimum value is “10”, and the maximum value is “999”.</p> <p>It is the settings that are valid for both the screen capture collection in window title logs, and screen capture collection during PrintScreen key operation and PrintScreen key prohibition.</p> <p>When the screen capture data saved in the client (CT) exceeds the value specified in [Maximum number of images can be saved in CT], the older images will be deleted. When more screen capture data can be saved in the client (CT), please modify [Maximum number of images can be saved in CT] as needed.</p>

[Terminal Operation Settings]

Item Name	Description
[Start time of logon prohibition]	<p>Select the interval from the detection of logon prohibition to logoff or shutdown in the client (CT).</p> <ul style="list-style-type: none"> <li>- [Prohibition after 30 seconds] Logoff or shutdown 30 seconds after the logon prohibition is detected.</li> <li>- [Prohibit immediately] Logoff or shutdown immediately after the logon prohibition is detected.</li> </ul> <p>Initial value is [Prohibition after 30 seconds].</p>
[Printer increasing/decreasing monitor interval]	<p>Specify monitoring interval (seconds) of printer increase/decrease in the client (CT).</p> <p>The initial value (recommended value) is “15”. The minimum value is “15”, and the maximum value is “9999”.</p> <p>Although the monitoring interval of the printer increase/decrease can be prolonged, and the load of imposed on the client (CT) and network can be reduced by increasing this value, it is possible that neither the newly installed printer nor the printing log during printing on this printer will be recorded. Please set to the recommended value if there is no particular problem.</p>
[Number of times of printing jobs monitoring]	<p>Specify the monitor times for printing jobs performed by the client (CT) after printing. The initial value is (recommended value) is “4”. The minimum value is “3”, and the maximum value is “9”. (Monitoring interval is 10 seconds.)</p>

Item Name	Description	
	Please increase this value when file names and total number of pages are incorrect in the collected log.	
[Printing Monitor Mode]	<p>Select the mode of printing in the client (CT).</p> <ul style="list-style-type: none"> <li>- [Manage printing monitor mode in Management server] is not selected Changes for settings of printing methods on the Management Server and Master Management Server are invalid.</li> <li>- [Manage printing monitor mode in Management server] is selected Changes for the settings of printing methods on the Management Server and Master Management Server are valid. <ul style="list-style-type: none"> <li>- [Monitor printing of all printers set in CT (recommended)] The printing mode becomes [Monitor printing of all printers on this CT (recommended)]</li> <li>- [Monitor printing of local printers only] The printing mode becomes "Monitor the printing of local printers only".</li> </ul> </li> </ul> <p>The initial value is that [Manage printing monitor mode in Management server] is not selected</p>	
[Settings of Collective Log Sending]	[Interval of Log Sending]	<p>Specify the interval (seconds) of sending logs when collective log sending. The initial value (recommended value) is "300". The minimum value is "60", and the maximum value is "9999".</p> <p>The [Interval of Log Sending] will be valid when any of the following options in the [Other Settings] tab of CT policy is set.</p> <ul style="list-style-type: none"> <li>- When [Send immediately when operation logs occur] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> <li>- When [Send after collecting logs for a certain period] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> </ul>
	[Interval during continuous sending]	<p>Specify the interval (seconds) between two times of log sending when collective log are sent. The initial value is (recommended value) is "60". The minimum value is "30", and the maximum value is "9999".</p> <p>The [Interval of Continuous Sending] will be valid when any of the following options in the [Other Settings] tab of CT policy is set.</p> <ul style="list-style-type: none"> <li>- When [Send immediately when operation logs occur] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> <li>- When [Send after collecting logs for a certain period] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> </ul>
	[Maximum number of logs can be sent at one time]	<p>Specify the maximum number of logs that can be sent at one time when collective log are sent. The initial value is (recommended value) is "1000". The minimum value is "100", and the maximum value is "5000".</p> <p>The [Maximum Number of Logs Sending for One Time] will be valid when any of the following options in the [Other Settings] tab of CT policy is set.</p> <ul style="list-style-type: none"> <li>- When [Send immediately when operation logs occur] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> <li>- When [Send after collecting logs for a certain period] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> </ul>



Item Name		Description
	[Communication Timeout]	<p>Specify the timeout value (seconds) of connection between the CT and server when logs are sent collectively.</p> <p>The initial value is (recommended value) is “150”. The minimum value is “30”, and the maximum value is “300”.</p> <p>When communication cannot be performed within the configuration value, logs will be re-sent during the next log sending.</p> <p>The [Communicate Timeout] will be valid when any of the following options in the [Other Settings] tab of CT policy is set.</p> <ul style="list-style-type: none"> <li>- When [Send immediately when operation logs occur] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> <li>- When [Send after collecting logs for a certain period] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> </ul>
[Settings of offline log sending]	[Interval of log sending each item of log]	<p>Specify the interval (ms) of sending each log when logs are sent immediately.</p> <p>The initial value is (recommended value) is “50”. The minimum value is “50”, and the maximum value is “5000”.</p> <p>The [Sending Interval of Each Log] will be valid when any of the following options in the [Other Settings] tab of CT policy is set.</p> <ul style="list-style-type: none"> <li>- When [Send immediately when operation logs occur] and [Send accumulated logs immediately after connection] are selected.</li> <li>- When [Send immediately when operation logs occur] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> </ul>
	[Interval of monitoring server connection]	<p>Specify the communication confirmation interval (seconds) of the server when logs are sent immediately.</p> <p>The initial value is (recommended value) is “60”. The minimum value is “30”, and the maximum value is “900”.</p> <p>The [Monitoring Interval of Server Connection] will be valid when any of the following options in the [Other Settings] tab of CT policy is set.</p> <ul style="list-style-type: none"> <li>- When [Send immediately when operation logs occur] and [Send accumulated logs immediately after connection] are selected.</li> <li>- When [Send immediately when operation logs occur] and [Send operation logs accumulated in certain collectively after connection] are selected.</li> </ul>

### Note

#### About sending command operation log to server

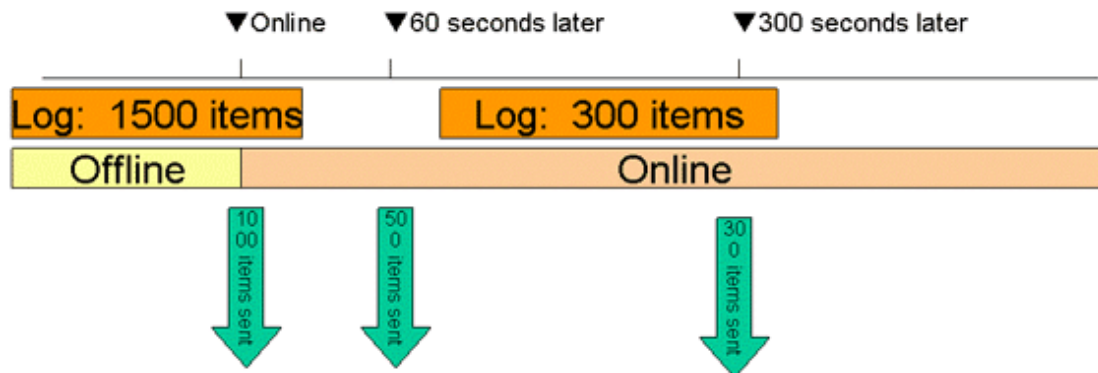
Command logs are always sent immediately after collection (not affected by these settings).

The following describes the settings of collective log sending .

**Setting of collective log sending**

- Log Sending Interval: 300 seconds
- Interval of continuous sending: 60 seconds
- Maximum number of items can be set at once: 1000 items

Log sending action when changing into online status after 1500 logs have been accumulated under offline status (300 logs have been accumulated after being online)



When shifting from offline to online, 1000 logs in the 1500 accumulated logs will be sent first and the remaining 500 logs will be sent 60 seconds later (the interval of continuous sending).

After being online, new logs will continue to be accumulated. When the number reaches 300, after 500 logs are sent, these logs that continue to be accumulated will be sent 300s later.

[Setting of Original File Backup Condition]

Item Name	Descriptions
[Maximum total size of Original of File Export]	Specify the maximum value of total original files backup in file export that can be saved in the client (CT). The original file backup that exceeds this configuration value cannot be saved. The initial value is the maximum value. The minimum value is "1" (MB) and the maximum value is "700" (MB).
[Maximum Size of a single File]	Specify the maximum of one file when original file is backed up. The original file backup that exceeds this configuration value cannot be saved. The initial value is the maximum value. The minimum value is "1" (MB) and the maximum value is "50" (MB).

**Logs Collected in Safe Mode or Safe Mode with Network**

Logs collected in safe mode or safe mode with the network will be sent to the Management Server when starting in normal mode next time.

## 2.5 Create Configuration Information Tree

---

After setting the standard policy of all managed targets, create a group tree (configuration information tree) that is used for managing clients (CTs) and users in groups.

The following are three types of methods for creating configuration information tree:

- Import information from Active Directory
- Import information from Systemwalker Desktop Patrol
- Create through Management Console

### 2.5.1 Import Information from Active Directory

---

This section describes how to import configuration information (CT group information, CT information, user group information and user information) from the Active Directory Server and create a configuration information tree of Systemwalker Desktop Keeper.

Only when the built environment of Active Directory in Windows® 2000 Server, Windows Server® 2003 and Windows Server® 2008 is Native Mode, Systemwalker Desktop Keeper can import configuration information from Active Directory. (The so-called “native mode” is the standard operation mode of Active Directory built in the environment of Windows® 2000 Server or later.) The NT compatible mode built in Windows NT® Server is not supported.

Active Directory Server for importing configuration information is only one server (one domain). Even if a domain trust relationship has been set in Active Directory, the information cannot be imported, but only the data of server that directly links with Systemwalker Desktop Keeper is imported.

To import configuration information from Active Directory, the CT of Systemwalker Desktop Keeper must be installed on the client of link target. Also, the following information must be set in the Server Settings Tool:

- System settings  
Set the conditions when data link with Active Directory Server is performed.
- Settings of Active Directory Linkage  
Set the computer name and domain name of Active Directory Server.
- Server information settings  
Set the information of Master Management Server or Management Server.

According to use, the following are two types of methods for importing configuration information:

- Using server setting utility  
When configuration information changes, import and update are performed by the system administrator.
- Using Active Directory link commands  
Register commands in task scheduler and perform import and update regularly.



---

#### **When importing information containing UNICODE specific characters through Active Directory link command**

If OU name and user name (UserPrincipalName) contain UNICODE specific characters, take different measures according to the version of Systemwalker Desktop Keeper.

- V13.2.0  
After changing the correspondent character to “?”, import it as the group and user information of Systemwalker Desktop Keeper.
- V13.3.0 or later  
Do not import correspondent OU name and user name (UserPrincipalName).

Thus, if V13.2.0 is converted to V14.2.0 or later, the OU name and user name (containing “?”) containing UNICODE specific characters that has been imported initially through Active Directory command will be deleted from Systemwalker Desktop Keeper.

However, even if in user information of Active Directory, the “User Name (Japanese .etc)”, “Employee Number”, “Title”, “Organization” and “Organization Code” containing contain UNICODE specific characters that are imported to Systemwalker Desktop Keeper will also be replaced by symbol “?”.

---

Because the group will be created automatically under the domain group according to the organization information of the Active Directory Server, there is no need to create a CT group tree and user group tree in the Management Console.

However, a group can be created under the Local group even if Active Directory Linkage is performed. Because the Local group does not link with Active Directory, even if Active Directory Linkage is performed, the subordinate information of Local group will not be changed. The following content can be registered in the Local group:

- CT which has not been registered in Active Directory.
- User (the user that has been registered in Active Directory Server can also be registered.)

When importing configuration information from Active Directory Server, after deleting OU, user and computer from Active Directory, the correspondent group (CT group/user group) and user information in Systemwalker Desktop Keeper will be deleted unconditionally after the link, and the CT will be placed in the Local group under the Root directory.

In addition, after disabling the user account in Active Directory, the user information (user policy) in Systemwalker Desktop Keeper will be deleted when Active Directory Linkage is executed.

In a 3-level system structure, when executing Active Directory Linkage on the Master Management Server, a link with Active Directory will be also executed on the Management Server.

Also, in a 3-level system structure, the method of managing user policy for Active Directory Linkage is to collective management in the Master Management Server.

## Point

---

### To search operation logs in Citrix XenApp client more efficiently

When linking with Citrix XenApp Server(TM) for an application, if logon through Citrix XenApp client in the environment where multiple Citrix XenApp Servers have been set, the Citrix XenApp client will be used to perform load distribution. As a result, it may be confusing which Citrix XenApp Server has been connected. Therefore, when viewing and searching operation logs, logs collected in all Citrix XenApp Servers must be viewed.

To search more effectively, it is recommended to allocate multiple Citrix XenApp Servers to one CT group and search that group only. Therefore, please register Citrix XenApp Server to Active Directory as organization unit (OU) information.

---

## Use Server Settings Tool

The following describes the procedure of import using the Server Settings Tool.

If the user information imported from Active Directory Server contains the following information, the user information will not be imported.

- When the string followed by @ in “User Logon Name (UserPrincipalName)” is 0 byte or over 41 bytes.

1. Select [Execute Active Directory Linkage] in the [Set] menu.  
→ The confirmation window for executing the link is displayed.

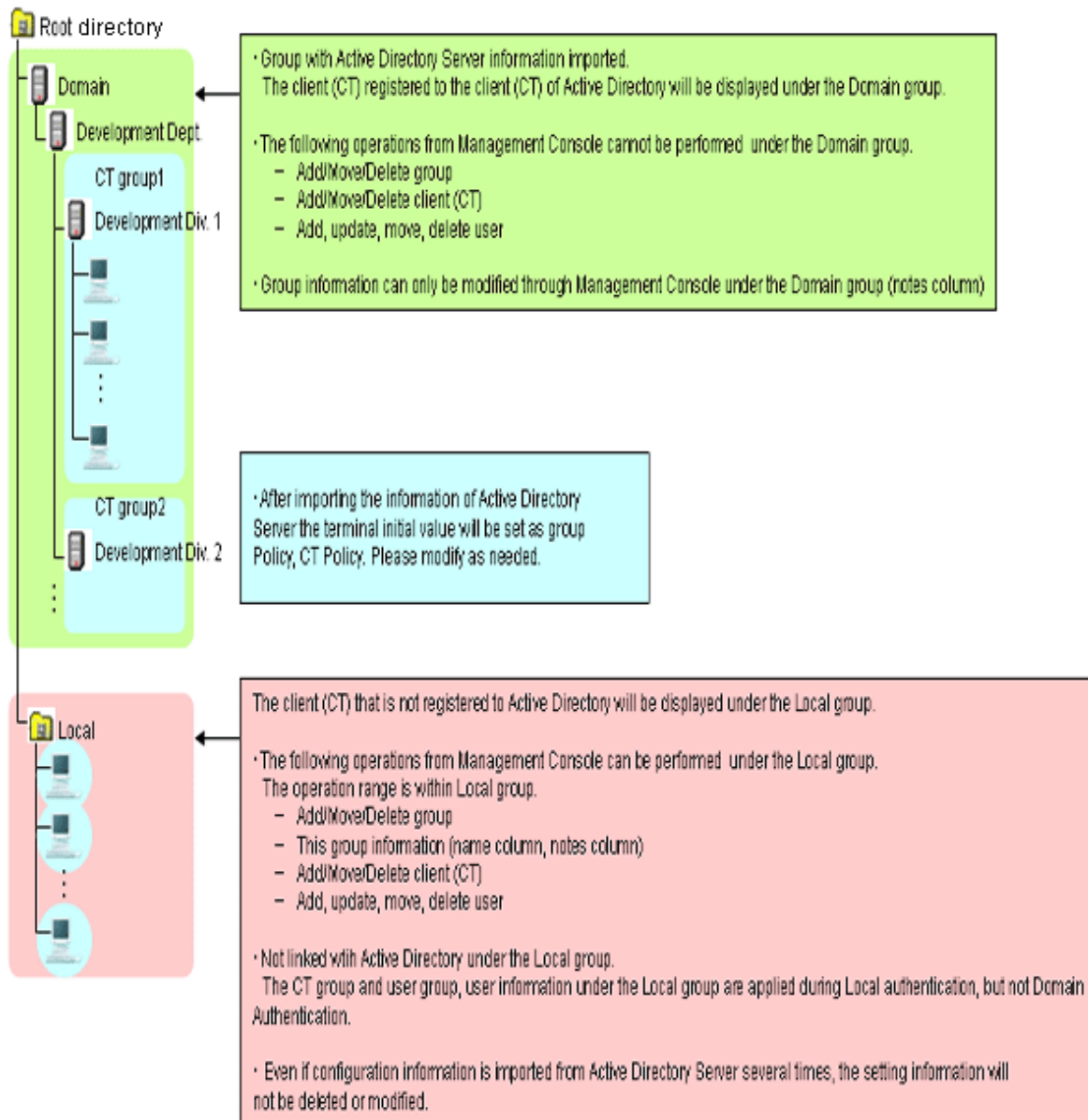
```
[STSY-SEL014] Strat to communicate with Active Directory.
Get from Active Directory user information, computer information,level composition information
and update the database..
The process will take some time. Start to communicatie?

                [Yes]                [No]
```

2. If performing Active Directory, click the [Yes] button.
  - The information indicating that the data is being imported from Active Directory is displayed.
  - After the data is imported, the information indicating completed is displayed.
3. Click the [OK] button.

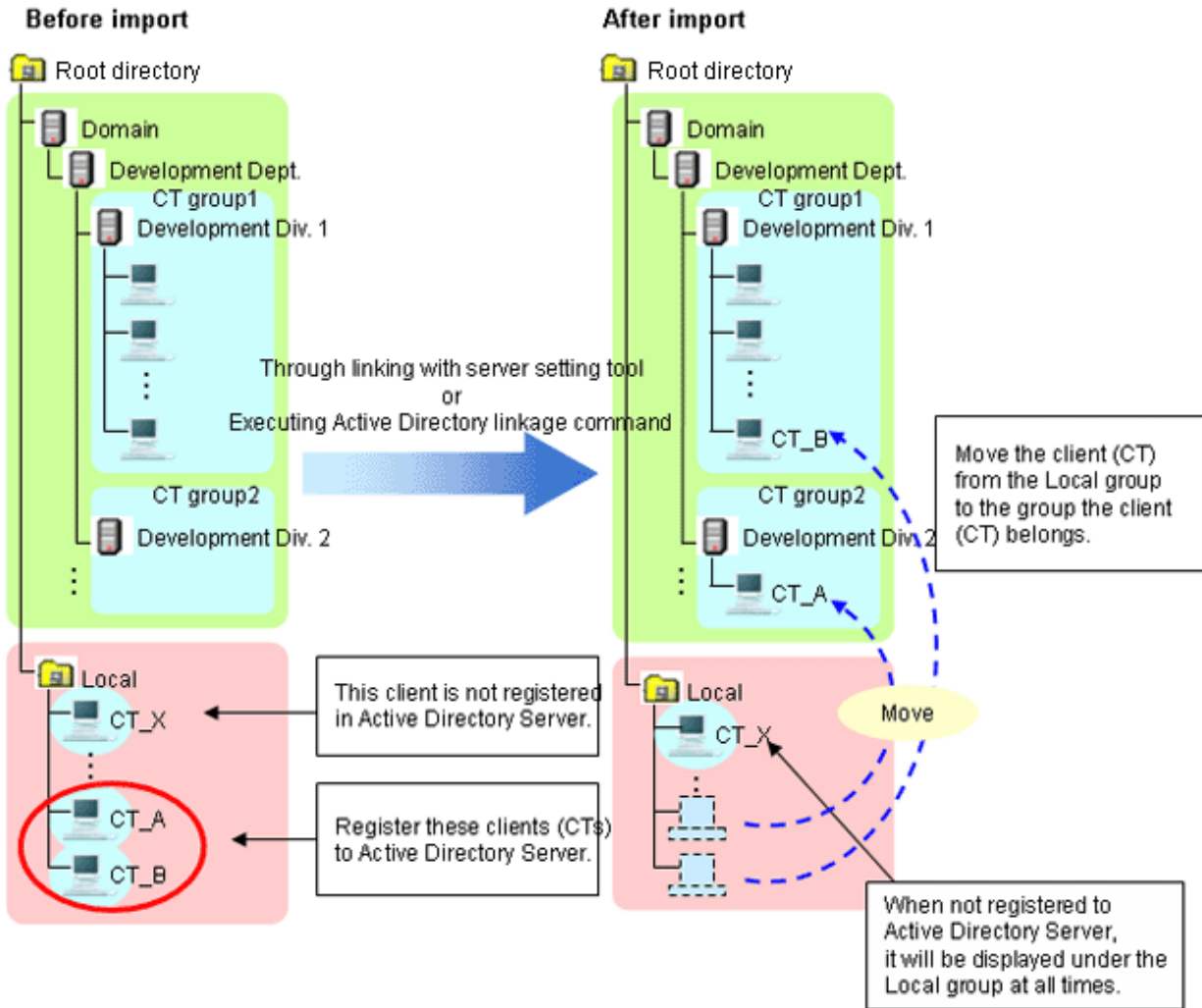
### Display Configuration Information Tree

Start the Management Console immediately after configuration information has been imported, and the configuration information tree will be displayed as follows.



After registering the client (CT) displayed in Local group the Active Directory Server, the registered client (CT) will be moved to the group after Active Directory Linkage has been performed in Systemwalker Desktop Keeper.

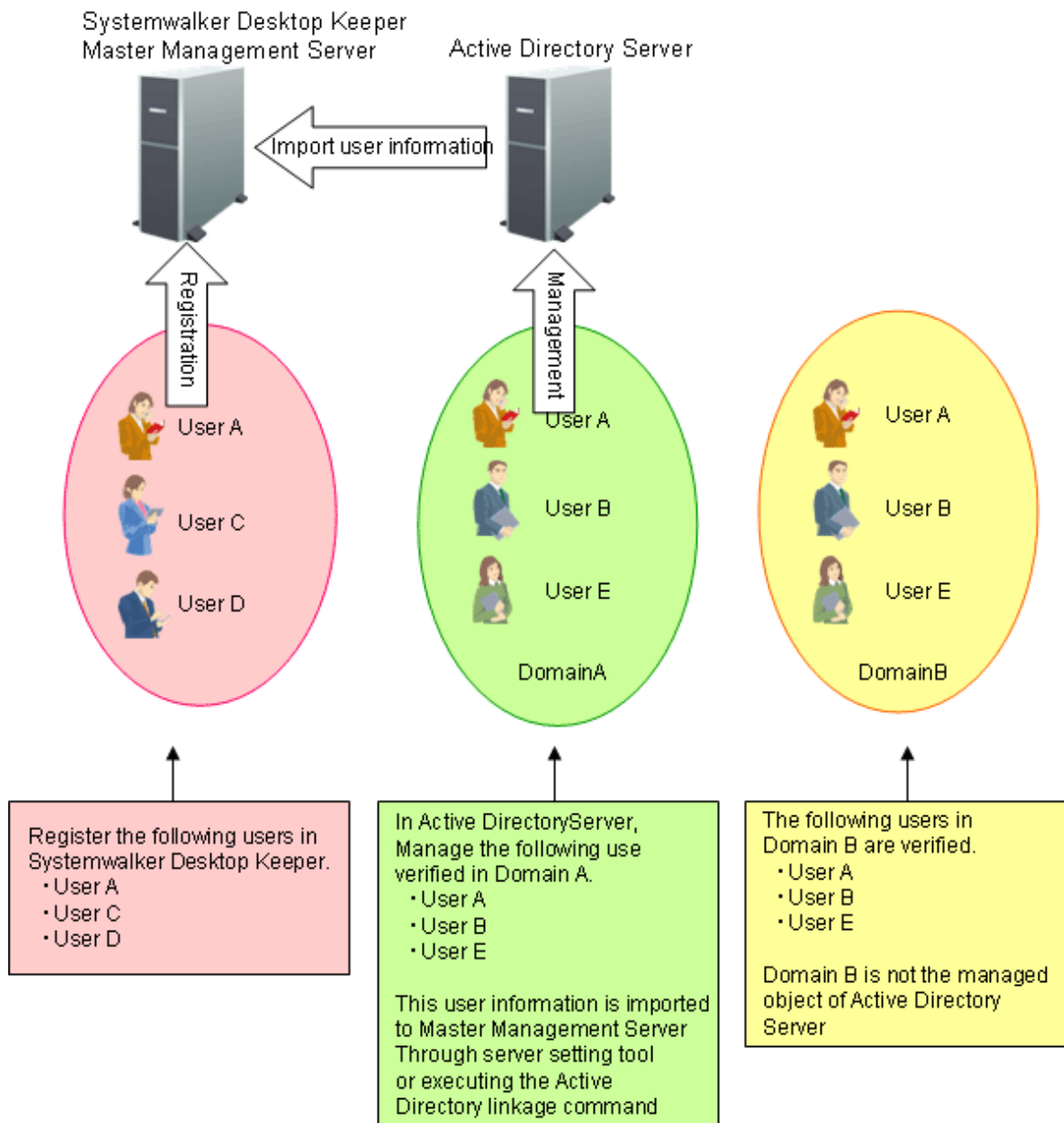
In addition, when performing Active Directory Linkage and deleting the client (CT) managed in the domain group through the Management Console, please select the client (CT) to be deleted in the window after Management Console is started (CT policy settings window) and perform Active Directory Linkage after setting to [Not as Target to be Linked with Active Directory]. As the client (CT) will be moved to the Local group, please delete CT information manually.



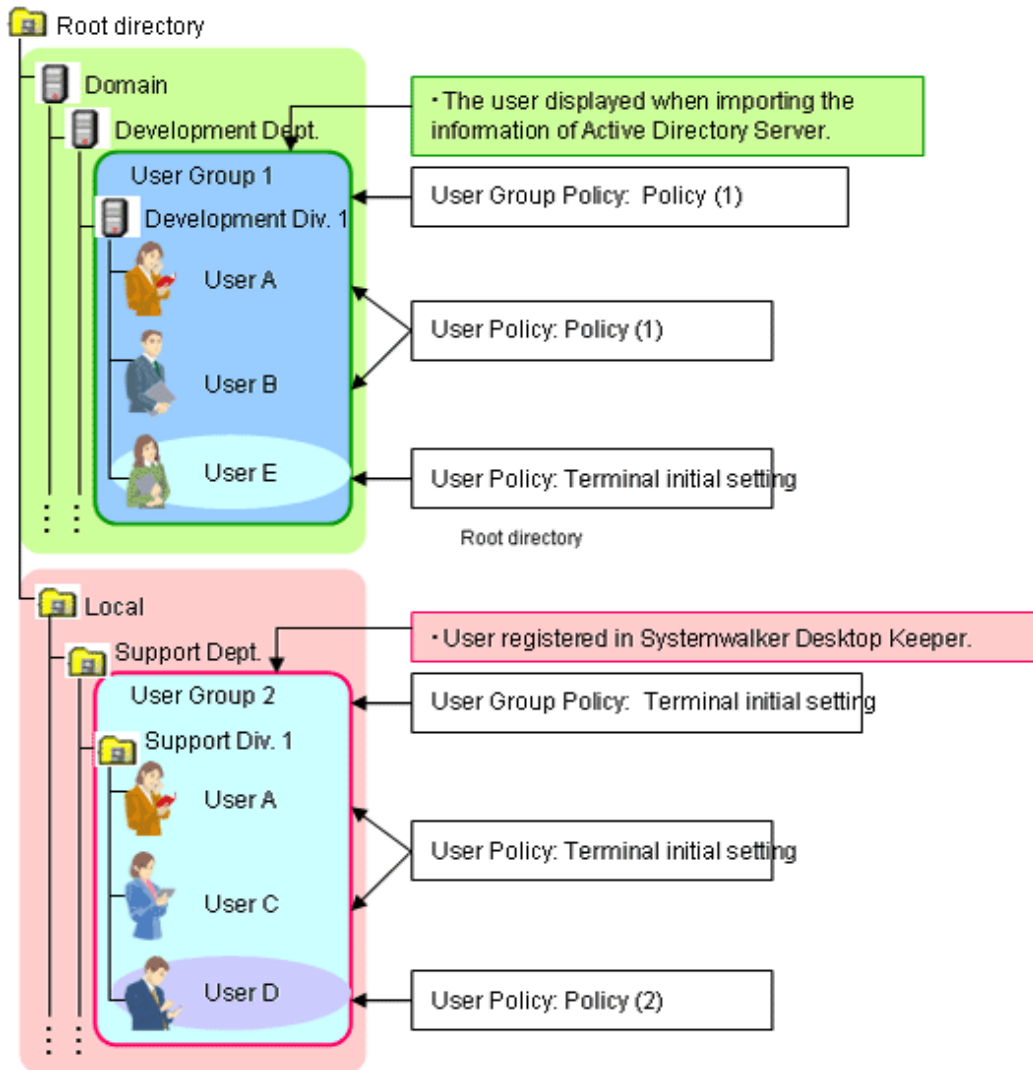
When a new client (CT) is added, it will be displayed in the Local group first. After this client has been registered to the Active Directory Server, it will be moved to the group to which the client (CT) belongs from the Local group after the link with Active Directory is performed in Systemwalker Desktop Keeper.

**Login Destination and Applied Policy in Client (CT)**

As a user will be created automatically when importing configuration information from the Active Directory Server, user policy should be used as well.  
 After linking with Active Directory for the first time, set the value of terminal initial settings in user policy of the created user. User policy can be modified as needed.  
 After the second and later Active Directory Linkage has completed, set the group policy of correspondent user group (OU) in the user policy of newly added user.  
 The applied policy varies depending on whether logged in to local or to the linked domain from the client (CT). The login destination and applied policy in the client (CT) are described.  
 Operate in the following environment.



After Active Directory Linkage is performed, the Management Console of Systemwalker Desktop Keeper is displayed as follows.



- When logging on to the domain specified in Active Directory Linkage  
→ User policy of domain is applied.

In the above example, user A, B and E can operate according to the user policy of the following domains:

- User A: Policy (1)
- User B: Policy (1)
- User E: Terminal initial settings

- When logging on to the local computer (if users with the same name exist in Local)  
→ The local user policy is applied.

In the above example, user A can operate according to user policy of terminal initial settings.

- When logging in to the local computer (if no user with the same name exists in Local)  
→CT policy is applied.

In the above example, user B and E can operate according to CT policy.

- When logging in to a domain that is not specified in Active Directory Linkage (if users with the same name exist in Local)  
→ The local user policy is applied.

In the above example, when user A logs in to domain B, user A can operate according to user policy of terminal initial settings.



- When logging in to a domain that is not specified in Active Directory Linkage (if users with the same name exist in Local) →CT policy is applied.

In the above example, when user B and E log in to domain B, they can operate according to CT policy.

## Use Active Directory Link command

The following describes the procedure of importing using the Active Directory link command.

“List of Active Directory Link Organization Unit Targets” can be set before executing the command. Import after limiting the organizations as link targets. The list is stored in the specified location (no need to specify in the command option.).

For details of the Active Directory link command, please refer to “DTKADCON.EXE (Active Directory Linkage)” in “Systemwalker Desktop Patrol Reference Manual”.

1. Logon to the Management Server with the user name that belongs to the Administrator or Domain Admins group of the local PC.
2. Start task scheduler and register the following content:
  - Active Directory link command
  - Timing (date, time frame etc.) for command execution

Specify the time frame in which the backup tool, restoration tool and backup command will not be started.

In addition, specify the time frame in which there are fewer users of the Management Console and Log Viewer.

3. Check whether task program is started normally.

After executing the command, the change of configuration information tree in the Management Console is the same as “[Display Configuration Information Tree](#)” of “Use Server Settings Tool”.

## 2.5.2 Import Information from Systemwalker Desktop Patrol

This section describes how to import configuration information of Systemwalker Desktop Patrol and create configuration information tree of Systemwalker Desktop Keeper.

When linking with Systemwalker Desktop Patrol, please refer to the configuration information managed in Systemwalker Desktop Patrol. Import information from Systemwalker Desktop Patrol first, and update the inherent information of Systemwalker Desktop Keeper to the tree for management.

After the environment of Systemwalker Desktop Patrol has been built completely, install Systemwalker Desktop Keeper, and import configuration information from Systemwalker Desktop Patrol after CT has been installed.

### Automatically Import Configuration Information of Systemwalker Desktop Patrol

When [Link with Other systems] of the Server Settings Tool has been set, the configuration information of Systemwalker Desktop Patrol will be imported automatically.

For how to do so, please refer to “Set the Link with Other Systems” of “Systemwalker Desktop Keeper Installation Guide”.

### Use Server Settings Tool

The following describes the procedure of import using the Server Settings Tool.

1. Select [Execute Systemwalker Desktop Patrol Linkage] in [Settings] menu.  
→The confirmation window for executing the link is displayed.

```
[STSY-SEL017] Execute Systemwalker Desktop Patrol configuration information import command.
Get configuration information from Systemwalker Desktop Patrol, and update the database.
The processing will take some time. Start to link?
```

[ Yes ]

[ No ]

2. To execute the link with Systemwalker Desktop Patrol, click the [Yes] button.
  - The information indicating data is being imported from Systemwalker Desktop Patrol is displayed.
  - After the data import has completed, the completion message will be displayed.
3. Click the [OK] button.

## Use Systemwalker Desktop Patrol Configuration Information Import Command

This section describes how to import configuration information using the Systemwalker Desktop Patrol configuration information import command.

When importing configuration information for the first time, create a new group and import all configuration information.

When importing for the second time and later, import the information that is different from the last time.

During the execution of the Systemwalker Desktop Patrol configuration information import command, do not operate in the Management Console and Log Viewer.

The start and end information of configuration information import will be output to event logs.

When importing configuration information for the first time, the following methods can be selected:

- Import through executing the command manually as the administrator.
- Register the command in the task scheduler and execute it when there is no user of the Management Console and Log Viewer.

When importing configuration information for the second time and later, the following methods can be selected:

- Import information only when system configuration changes.
- Register the command in task scheduler and update it regularly.

### Procedure of Import

#### 1. Output configuration information in Systemwalker Desktop Patrol

Prepare the configuration information file (CSV file) that records import information in Systemwalker Desktop Patrol.

CT group information and CT location information are recorded in the configuration information file.

For how to output configuration information, please refer to the manual of Systemwalker Desktop Patrol.

\* Please do not edit the created configuration information file.

#### 2. Copy configuration information file

Copy the configuration information file created in Systemwalker Desktop Patrol to Management Server of Systemwalker Desktop Keeper.

In a 3-level system structure, when the managed client (CT) exists under the Master Management Server, the configuration information file should be copied to the Master Management Server as well.

#### 3. Execute Systemwalker Desktop Patrol configuration information import command

##### [Execution Location of Command]

Execute the command on the server that has copied the configuration information file.

However, as for the order of execution, in a 3-level system structure, when copying configuration information file to Master Management Server, please execute the command on the Master Management Server again after executing it on Master Management Server.

##### [When executing the command manually]

1. Logon to the server on which the command is executed with the user name that belongs to the Administrator or Domain Admins group of the local PC.

2. Confirm the following are not in operation:
  - Backup tool
  - Backup command
  - Restoration tool
  - Command of Active Directory Linkage
3. Start the command prompt.
4. Execute the Systemwalker Desktop Patrol configuration information import command.  
 It is not necessary to pay attention to the directory during command execution.  
 When viewing all execution result information of command, specify result log file in command option.  
 For examples of executing the Systemwalker Desktop Keeper configuration information import command, please refer to “DTKIMPDP.EXE (Import Systemwalker Desktop Patrol Configuration Information)” in “Systemwalker Desktop Patrol Reference Manual”.
5. Confirm the execution result in the window.  
 In addition, confirm again after obtaining the value of environment variable %ERRORLEVEL%.  
 The value of %ERRORLEVEL% is the return value of Systemwalker Desktop Patrol configuration information import command. For the value and its definition, please refer to “DTKIMPDP.EXE (Import Systemwalker Desktop Patrol Configuration Information)” in “Systemwalker Desktop Keeper Reference Manual”.

**When executing after the command is registered in task scheduler.**

1. Logon to the server on which the command is executed with the user name that belongs to the Administrator or Domain Admins group of the local PC.
2. Start the task scheduler and register the following content.
  - Systemwalker Desktop Patrol configuration information import command
 Specify the result log file in command option.  
 In the case of a 3-level Management Server, set retry times in command option (also for confirming data consistency with the Master Management Server).  
 The waiting time for each retry is 60 seconds. The number of retry times is specified to 10 (with a maximum waiting time of 10 min).  
 For details on how to specify the option, please refer to “Systemwalker Desktop Patrol Configuration Information Import Command” in “Systemwalker Desktop Keeper Reference Manual”.
  - Timing (date, time frame, etc.) for command execution
 Specify the time frame in which backup tool, restoration tool and backup command are not started.  
 In addition, specify the time frame in which there are fewer users of the Management Console and Log Viewer.
3. Confirm the job execution result displayed in task scheduler.
4. After the command execution has finished, view result log file and confirm the command has ended normally (operation log will be added).

**[Status after command execution]**

- When a group is created
  - After creating a group under the Root directory, the value of terminal initial settings will be set as the user policy.
  - After creating a group in an existing group, group policy of the parent group will be set.
- When a group is updated
  - Even if the update of group name and moving of group level location exist, the registration information of group policy and department administrator will still be inherited.
- When a group is deleted
  - The information of group policy and department administrator of deleted group will be deleted at the same time.
  - When the group and the client (CT) created in Systemwalker Desktop Keeper after the import of configuration information exist under the deleted group, this content will be moved to the Root directory.

- When no client (CT) exists under the group

Only the group is displayed. Please select [Do not display empty group] from the [Tool Settings] menu of the Management Console if it is not needed.

- About moving of CT

After importing configuration information, the CT will move according to configuration information file.

The CT will not move if there is no data in configuration information (displayed under the Root directory always).

If the CTs of Systemwalker Desktop Patrol and Systemwalker Desktop Keeper installed in the PC are 13.0.0 or later, the clients (CTs) can be moved according to configuration information file.

#### 4. Modify configuration information tree as needed

Create, rename, move and delete a group in the Management Console according to the management information in Systemwalker Desktop Keeper.

The system administrator and department administrators can update, move and delete a user name, set group policy and department administrator (only system administrator is allowed) for the imported group. For the allocation of the department administrator, please refer to “[2.6 Allocate Department Administrator](#)”.

The updating, moving and deleting of group name performed in the Management Console of Systemwalker Desktop Keeper will be invalid after next import of configuration information and will be corrected in the re-imported configuration information.

Registration information of group policy and department administrator will be inherited after it is imported again.

When deleting a group, the correspondent group will be imported again through the next import of configuration information, but since the information of group policy and department administrator has been deleted, the group must be reset.

In addition, system administrator and department administrator can create a new group, update and delete a group in the imported group.

When there is no upper level group at next import of configuration information, the group created in the imported group will be moved to the Root directory.

The same operation as group can be conducted to the client (CT).

When continuing when continuing to import configuration information by linking with Systemwalker Desktop Patrol after the second time and the folders of Systemwalker Desktop Patrol and Systemwalker Desktop Keeper are used at the same time, please perform the following operations.

For the group used in Systemwalker Desktop Keeper only, no need to perform the following operations.

1. Update the change information of the Management Console to Systemwalker Desktop Patrol

Because the updating, moving and deleting of group name performed in Management Console will be invalid after the next import of configuration information, changes performed in “[4. Modify configuration information tree as needed](#)” will be updated to Systemwalker Desktop Patrol manually.

2. Delete the group created in the Management Console of Systemwalker Desktop Keeper. For details on how to delete, please refer to “[Delete](#)”.

3. Output configuration information in Systemwalker Desktop Patrol and import Systemwalker Desktop Keeper.

To use the configuration information file with changes in Systemwalker Desktop Keeper updated, repeat the steps from “[1. Output configuration information in Systemwalker Desktop Patrol](#)” to “[4. Modify configuration information tree as needed](#)” before using it.

### Information

[Use Systemwalker Desktop Patrol configuration information to import correspondent file]

This is the file required for creating user group tree when importing information from Systemwalker Desktop Patrol.

The correspondent information of PC (computer name) and user name is specified in this file

For details how to create correspondent files of Systemwalker Desktop Keeper configuration information import, please refer to

“Correspondent Files of Systemwalker Desktop Keeper Configuration Information Import” in “Systemwalker Desktop Keeper Reference Manual”.

The relationship between files in use and the server that saves the files is as follows:

- In a 2-level system structure  
Save the correspondent files and configuration information files on Management Server.
- In a 3-level system structure
  - When managing user information collectively  
Correspondent file: It is saved in the Master Management Server (this is for importing user information on Master Management Server).  
Configuration information file: it is saved in the Master Management Server and Management Server (even if there is no the client (CT) under the Master Management Server, it should still be saved in the Master Management Server).
  - When managing user information on each the Management Server  
Correspondent file: it is saved in the Management Server (this is for importing user information on each Management Server).  
Configuration information file: it is saved in Management Server. However, the client (CT) exists under the Master Management Server, so it should still be saved in the Master Management Server.

Please add /U and /F options before executing the Systemwalker Desktop Patrol configuration information import command. For details, please refer to “DTKIMPDP.EXE (Systemwalker Desktop Patrol Configuration Information Import)” in “Systemwalker Desktop Keeper Reference Manual”.

#### [To use information file of discarded folder]

This is the file required for updating the information of a discarded PC in Systemwalker Desktop Patrol to configuration information tree when importing information from Systemwalker Desktop Patrol.

For details on how to create information file of discarded folder, please refer to “Information File of Discarded Folder” in “Systemwalker Desktop Keeper Reference Manual”.

The following tasks must be completed before executing the Systemwalker Desktop Patrol configuration information import command.

- Create a group for deleted CT  
In order to display the PC deleted in Systemwalker Desktop Patrol in groups in the configuration information tree of Systemwalker Desktop Keeper, a special group for deleted PCs must be created in the configuration information tree of Systemwalker Desktop Keeper.  
The group name must be unique.  
After specifying a name for the created group in the option of Systemwalker Desktop Patrol configuration information import command, the deleted PC will be displayed in the group of configuration information tree of Systemwalker Desktop Keeper.
- Create information file of discarded folder  
During differential import of the discarded PC information in Systemwalker Desktop Patrol, the file will be created when it is displayed in configuration information tree of Systemwalker Desktop Keeper.  
Set the discarded PC and the group to which it belongs in Systemwalker Desktop Patrol.  
For details how to create information file of discarded folder, please refer to “Information File of Discarded Folder” in “Systemwalker Desktop Keeper Reference Manual”.  
Information File of Discarded Folder is saved in the Management Server. However, it should also be saved in the Master Management Server if the managed the client (CT) exists under the Master Management Server.

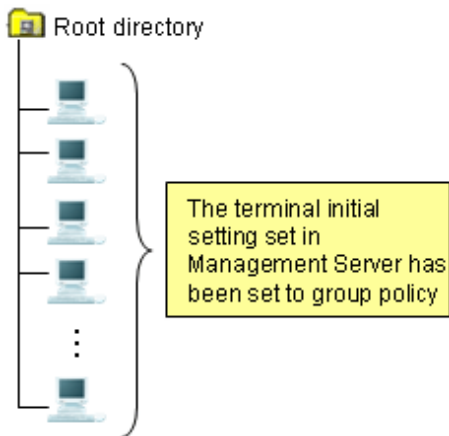
Please add the /E option before executing the Systemwalker Desktop Patrol configuration information import command. For details, please refer to “DTKIMPDP.EXE (Systemwalker Desktop Patrol Configuration information Import)” in “Systemwalker Desktop Keeper Reference Manual”.



## Display in Configuration Information Tree

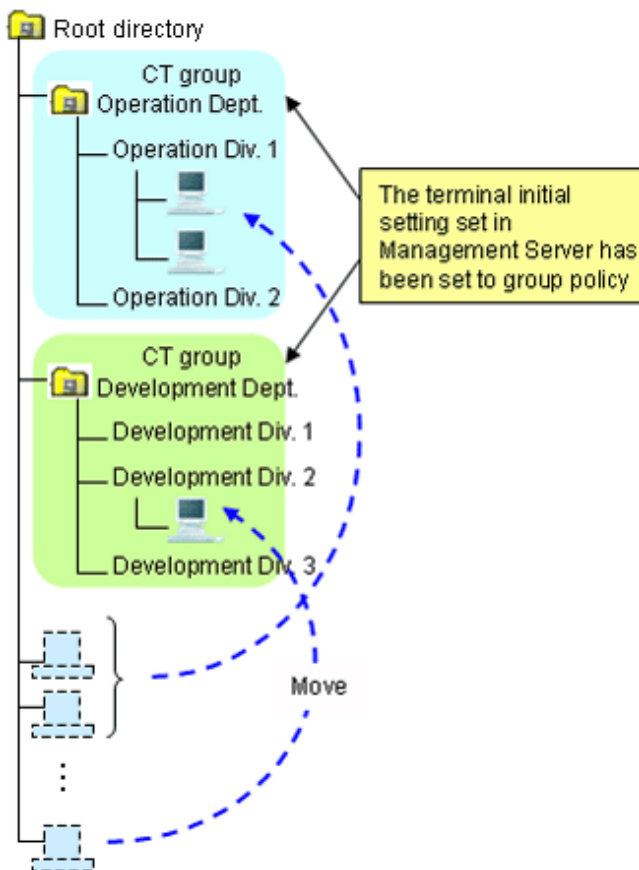
1. Install the CT of Systemwalker Desktop Keeper.

→ When the Management Server communicates with the client (CT), the client (CT) will be displayed under the Root directory. At this time, the value of terminal initial settings will be set as CT policy in the client (CT).

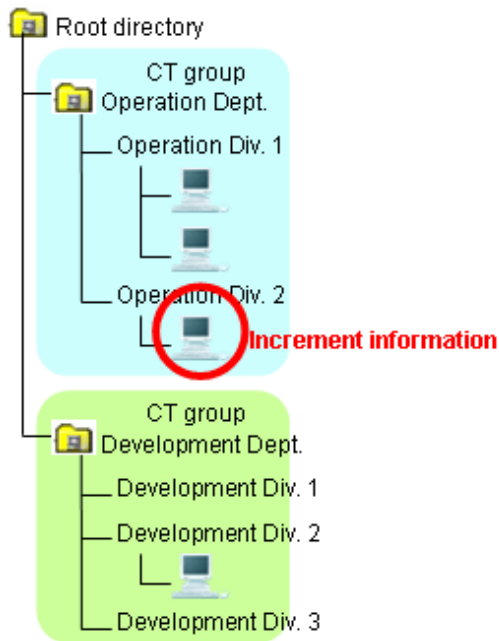


2. Execute the Systemwalker Desktop Patrol configuration information import command (for the first time).

→ The client (CT) is allocated to the tree.



- Execute the Systemwalker Desktop Patrol configuration information import command (for the second time and later).  
→ Only the differential information is imported.



## Use [Link with Other Systems] of Management Console

This section describes how to import configuration information through the menu of the Management Console.



### Note

**The method of importing configuration information by using [Link with Other Systems] will be limited.**

[Available conditions are limited]

When importing new configuration information, [Link with Other Systems] of the Management Server can be used for the first import only.

[Do not use it in combination with Systemwalker Desktop Patrol configuration information import command]

After creating configuration information by using [Link with Other Systems] of the Management Console, the configuration information imported through [Link with Other Systems] will be reserved and the configuration information will be imported again and the group will be created when the Systemwalker Desktop Patrol configuration information import command is used.

This will cause repeated information and difficulties in management; therefore, please do not use them in combination.

[The original management information imported through [Link with Other Systems] will be deleted]

After importing configuration information by using [Link with Other Systems] of the Management Console for the second time and later, all the original management information (group information, policy, department administrator, etc.) imported through [Link with Other Systems] will be deleted and re-built in the information of Systemwalker Desktop Patrol.

Therefore, group policy and department administrator must be reset after import.

In the case of a 3-level system structure, please import configuration information by connecting the Management Console of the Master Management Server. At this time, the Master Management Server and lower level servers will have the same group structure.

When importing configuration information, the client (CT) that satisfies any of the following conditions will be displayed under the Root directory. Other clients (CTs) will be displayed under each group according to configuration information.

- The CT version of Systemwalker Desktop Keeper is V12.

- Systemwalker Desktop Patrol is not installed in the client (CT).

After importing configuration information, the value of terminal initial settings will be set as group policy. In the case of a 3-level system structure, set the value of terminal initial settings of the Management Server in CT group policy under each Management Server.

In order to match the imported CT group information and CT information, information must be displayed in [DTPID] of the PC as import target in CT list on the Management Console window of Systemwalker Desktop Keeper. (Install Systemwalker Desktop Keeper and Systemwalker Desktop Patrol in the target PC and the information will be imported to [DTPID] after next startup of Windows.)

When there is no information displayed in [DTPID] of the PC as import target, CT group information will not be imported during the import of configuration information of Systemwalker Desktop Patrol. The client (CT) will be registered to the Root directory.

CT group that does not have 1 client (CT) registered will not be imported.

The client (CT) that belong to the “deleted CT” group will not become the link target.

If the group name in Systemwalker Desktop Patrol contains over 40 single-byte characters, the first 40 single-byte characters will be made as the group name to import to Systemwalker Desktop Keeper.

The following describes procedure of import.

1. Output configuration information in Systemwalker Desktop Patrol.

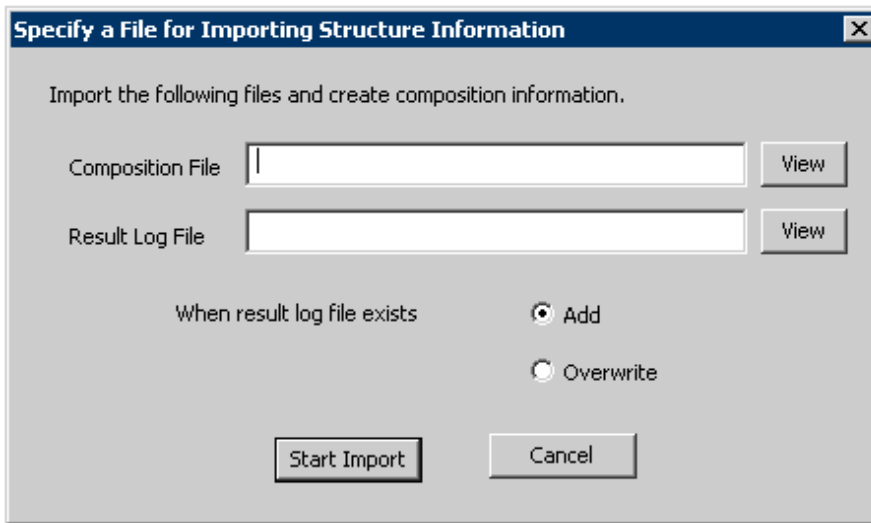
For the method of output, please refer to the manual of Systemwalker Desktop Patrol.

\*Please do not edit the created configuration information file.

2. Start the [Management Console] window.

3. Select [Link with Systemwalker Desktop Patrol] - [Import Configuration Information] from the [Link with Other Systems] menu.

→ The [Specify the File to Importing Structure Information] window is displayed.



4. Click the [Start Import] button after entering the following information.

Item Name	Description
[Composition File]	<p>Specify the imported file using the following method.</p> <ul style="list-style-type: none"> <li>- Enter the file name with full path. Enter the path until the path of imported file with full path.</li> <li>- Select the [View] button. The [Specify an Import File] window is displayed. Select the imported file and click the [Open] button.</li> </ul> <p>The maximum length of full path that can be entered is 218 characters. However, the following symbols are not allowed in a file name:            \, /, :, *, ?, ", &lt;, &gt;,  .</p>



Item Name	Description
[Result Log File]	<p>Specify the file for outputting import operation result. As the extension will not be added automatically, please specify an extension that can be determined easily, such as “KEKKA.TXT” through the following method.</p> <ul style="list-style-type: none"> <li>- Enter the file name with full path. Enter with full path in the input field until the path of the output result log file.</li> <li>- Input through the [View] button. The [Specify result log file] window is displayed. Select the location of the configuration information file to be output and click the [Open] button after entering the file name.</li> </ul> <p>The maximum length of full path that can be entered is 218 characters. However, the following symbols are not allowed in a file name: \\, /, :, *, ?, “, &lt;, &gt;,  .</p>
[When result log file exists]	<p>Select the processing when result log file exists in the specified location in [Result Log File].</p> <ul style="list-style-type: none"> <li>- [Add] Add after the result log of last time.</li> <li>- [Overwrite] Overwrite the result log of last time.</li> </ul>

Configuration information can also be output to Systemwalker Desktop Patrol.

[Output Conditions]

Configuration information of Systemwalker Desktop Keeper can be output to configuration information file if it satisfies all the following conditions:

- When the client (CT) version of Systemwalker Desktop Keeper is V13.0.0 or later
- When there is information in [DTPID] in the CT list of Management Console

The client (CT) that belongs to the “deleted CT” group will not become a link target.

The following describes the procedure of outputting information.

1. Start the [Management Console] window.

2. Select [Link with Systemwalker Desktop Patrol] - [Export Configuration Information] from the [Link with Other Systems] menu.

→ The [Specify a File for Exporting Structure Information] window is displayed.

3. Click the [Start Output] button after entering the following information.

Item Name	Description
[Composition File]	<p>Specify the target for saving the file for outputting configuration information. Output cannot be performed if a file with the same name as output target of configuration information exists.</p> <p>As the extension will not be added automatically, please specify an extension that can be determined easily such as "FILEA.CVS" through the following method.</p> <ul style="list-style-type: none"> <li>- Enter the file name with hhe full path. Enter with the full path in the input field until the path of the output configuration information file.</li> <li>- Select the [View] button. The [Specify Output File] is displayed. Select the location of the output configuration information file and click the [Open] button after entering the file name.</li> </ul> <p>The maximum length of full path that can be entered is 218 characters. However, the following symbols cannot be contained in a file name. Symbols cannot be used: \, /, :, *, ?, ", &lt;, &gt; and  .</p>
[Result Log File]	<p>Specify the file for outputting import operation result. As the extension will not be added automatically, please specify an extension that can be determined easily such as "KEKKA.LOG", through the following method.</p> <ul style="list-style-type: none"> <li>- Enter the file name with the full path. Enter with the full path in the input field until the path of the output result log file.</li> <li>- Input through the [View] button. The [Specify Output File] window is displayed. Select the location of the configuration information file to be output and click the [Open] button after entering the file name.</li> </ul> <p>The maximum length of full path that can be entered is 218 characters. However, the following symbols are not allowed in a file name: \, /, :, *, ?, ", &lt;, &gt;,  .</p>

Item Name	Description
[When result log file exists]	Select the processing when result log file exists in the specified location in [Result Log File]. <ul style="list-style-type: none"> <li>- [Add] Add after the result log of last time.</li> <li>- [Overwrite] Overwrite the result log of last time.</li> </ul>

4. Import configuration information in Systemwalker Desktop Patrol.

For the method of import, please refer to the manual of Systemwalker Desktop Patrol.

## 2.5.3 Create through Management Console

In the case of a 3-level system structure, when creating configuration information tree manually through the Management Console, please execute in each Management Server.

### Create a CT group



Point

#### To search operation logs in Citrix XenApp client more efficiently

When linking with Citrix XenApp Server(TM) for application, if logon through the Citrix XenApp client in the environment where multiple Citrix XenApp Servers have been set, the Citrix XenApp client will be used to perform load distribution. As a result, it may be confusing which Citrix XenApp Server is connected. Thus, when viewing and searching operation logs, logs collected in all Citrix XenApp Servers must be viewed.

To search more effectively, it is recommended to allocate multiple Citrix XenApp Servers to one CT group and search that group only. Therefore, please set the Citrix XenApp Server as a CT group in the Management Console.

The following describes the construction of a CT group displayed in the CT group tree.

#### Create

The CT group tree is displayed in grey. If a group cannot be created, set in [Do not display empty group] of the [Tree Settings] menu. Please cancel the settings.

After a CT group is created, CT policy can be set collectively for CTs in the CT group.

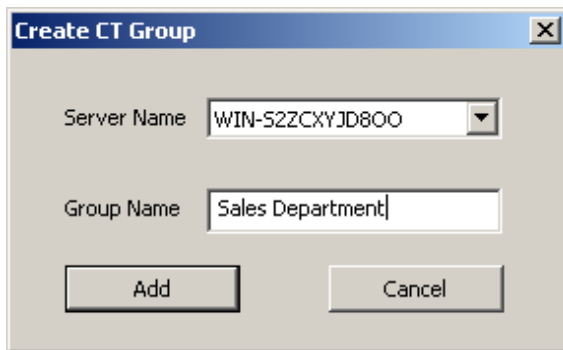
CT group names are displayed in ascending order of character code.

The procedure for creating a CT group is as follows.

1. Start the [Management Console] window.
2. Select the upper level group of the group to be created from the CT group tree.

3. Select [Create CT Group] from the [File] menu.

→ The [Create CT Group] window is displayed.



4. Enter the following information and click the [Add] button:

- [Server Name]
- [Group Name]

Up to 40 single-byte characters (20 double-byte characters) of alphanumeric characters and Chinese characters can be entered.

→ The group added in CT group tree is displayed.

5. Select [Reflect CT Group Structure] from the [Tree Settings] menu.

→ The created CT group is updated to the database.

If [Reflect CT Group Structure] is not performed, [Refresh Policy], [Update at Next Startup] and [Update Immediately] buttons will be grayed out and a message prompting [Reflect CT Group Structure] will be displayed.

After the created CT is updated to the database, CT group policy must be set as follows. Please modify the policy as needed. For details regarding the modification of policy, please refer to “[3.2.1 Modify CT Group Policy](#)”.

- When creating a CT group under the Root directory

On the Master Management Server or Management Server where a CT group is created, policy set in the [Terminal Initial Settings] window will be updated.

- When creating a CT group under other groups

Policy set in the upper level group of the created CT group will be updated.

## Move

The CT group created in the CT group tree can be moved to other CT groups under the same server, or directly under the server.

Even if the group has moved, CT group policy will not change. Besides, though the CT registered in the group will be moved when the CT group is moved, the policy set for CT will not change.

When a department administrator has been set in the CT group, it will be moved if the CT group is moved.

The procedure for moving a CT group is as follows.

1. Start [Management Console].
2. Select the group to be moved from the CT group tree.  
→ The selected CT group is highlighted.
3. Move the CT group to be moved to the target CT group under the same server by dragging and dropping.  
→ The CT group is moved.
4. Select [Reflect CT Group Structure] from the [Tree Settings] menu.  
→ The moved CT group is updated to the database.

If [Reflect CT Group Structure] is not performed, [Refresh Policy], [Update at Next Startup] and [Update Immediately] buttons will be grayed out and a message prompting [Reflect CT Group Structure] will be displayed.

## Delete

A CT group cannot be deleted if other CT groups or CTs exist in it. Please delete the CT groups or CTs under it first. For detail on how to delete a CT, please refer to “[Delete CT](#)”.

The procedures for deleting a CT group is as follows.

1. Start the [Management Console] window.
2. Select the group to be deleted from the CT group tree.
3. Select [Delete CT group] from the [File] menu.  
→ The deletion confirmation window is displayed.
4. Click the [OK] button.  
→ The selected CT group is deleted.
5. Select [Reflect CT Group Structure] from the [Tree Settings] menu.  
→ The “deleted” CT group is updated to the database.

If [Reflect CT Group Structure] is not performed, [Refresh Policy], [Update at Next Startup] and [Update Immediately] buttons will be grayed out and a message prompting [Reflect CT Group Structure] will be displayed.

## Modify group information

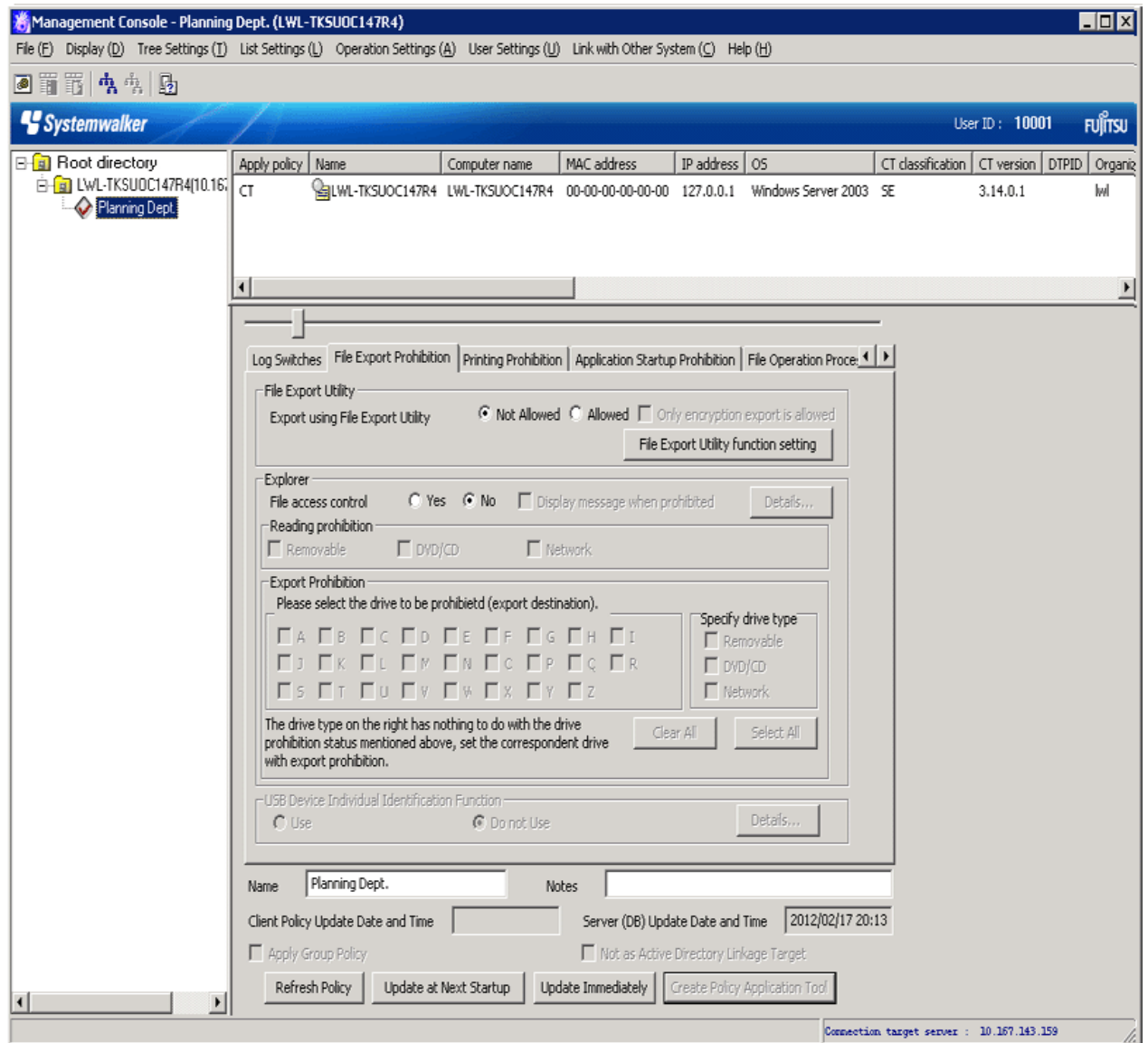
This section describes how to modify the name or notes of a CT group created in the CT group tree.

The procedure is as follows.

1. Start the [Management Console] window.

2. Select the CT group to be modified from the CT group tree.

→ The selected CT group is highlighted.



3. Enter the following information and click the [Update at Next Startup] or [Update Immediately] button:

- [Name]: Enter the modified CT group name.

Up to 40 single-byte characters (20 double-byte characters) of alphanumeric characters and Chinese characters can be entered.

- [Notes]: Enter the notes relating to CT group.

Up to 128 single-byte characters (63 double-byte characters) of alphanumeric characters and Chinese characters can be entered.

4. Select [Refresh Tree] from the [Tree Settings].

→ Name of the selected CT group is modified.

If [Refresh Tree] in the [Tree Settings] menu is grayed out, structure might not be updated after a CT group has been created, moved or deleted. At this time, please select [Reflect CT Group Structure] from the [Tree Settings] menu to update the structure.

## Create automatic distribution file during CT registration

After CT installation, the client (CT) will be registered to the Management Server once the client (CT) communicates with the Management Server. At this time, all the clients (CTs) are placed under the Root directory.

When automatic distribution file is used during CT registration, the client (CT) will be automatically distributed to each group after the client (CT) communicates with the Management Server.

The procedure is as follows.

1. Export CT group information.  
For details, please refer to “[Export CT Group Information](#)”.
2. Rename the CSV file to export CT group information as “DTKCTEntry.csv”.
3. The automatic distribution file (DTKCTEntry.csv) is created and saved to Management Server during CT registration.  
For details of automatic distribution file during CT registration, please refer to “Automatic Distribution File During CT Registration” of “Systemwalker Desktop Keeper Reference Manual”.

Location for saving

Environment excluding Windows Server® 2008

```
[OS installation drive] \Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper
```

Windows Server® 2008 environment

```
[OS installation drive] \ProgramData\Fujitsu\Systemwalker Desktop Keeper
```

→ After CT installation, once the client (CT) communicates with the Management Server, the client (CT) will be distributed to a CT group according to the specification of automatic distribution file during CT registration.

If the content of automatic distribution file during CT registration contains error, all the clients (CTs) will be placed under the Root directory.

## Create a user group

This section describes the construction of user group displayed in user group tree.



**Please operate collective management of user policy through Master Management Server.**

To manage user policy collectively, please create, move and delete a user on the Master Management Server.

### Create

The User group tree is displayed in grey. If a group cannot be created, set in [Do not display empty group] of the [Tree Settings] menu. Please cancel the settings.

Create user group one by one. Multiple users cannot be created using an CSV file.

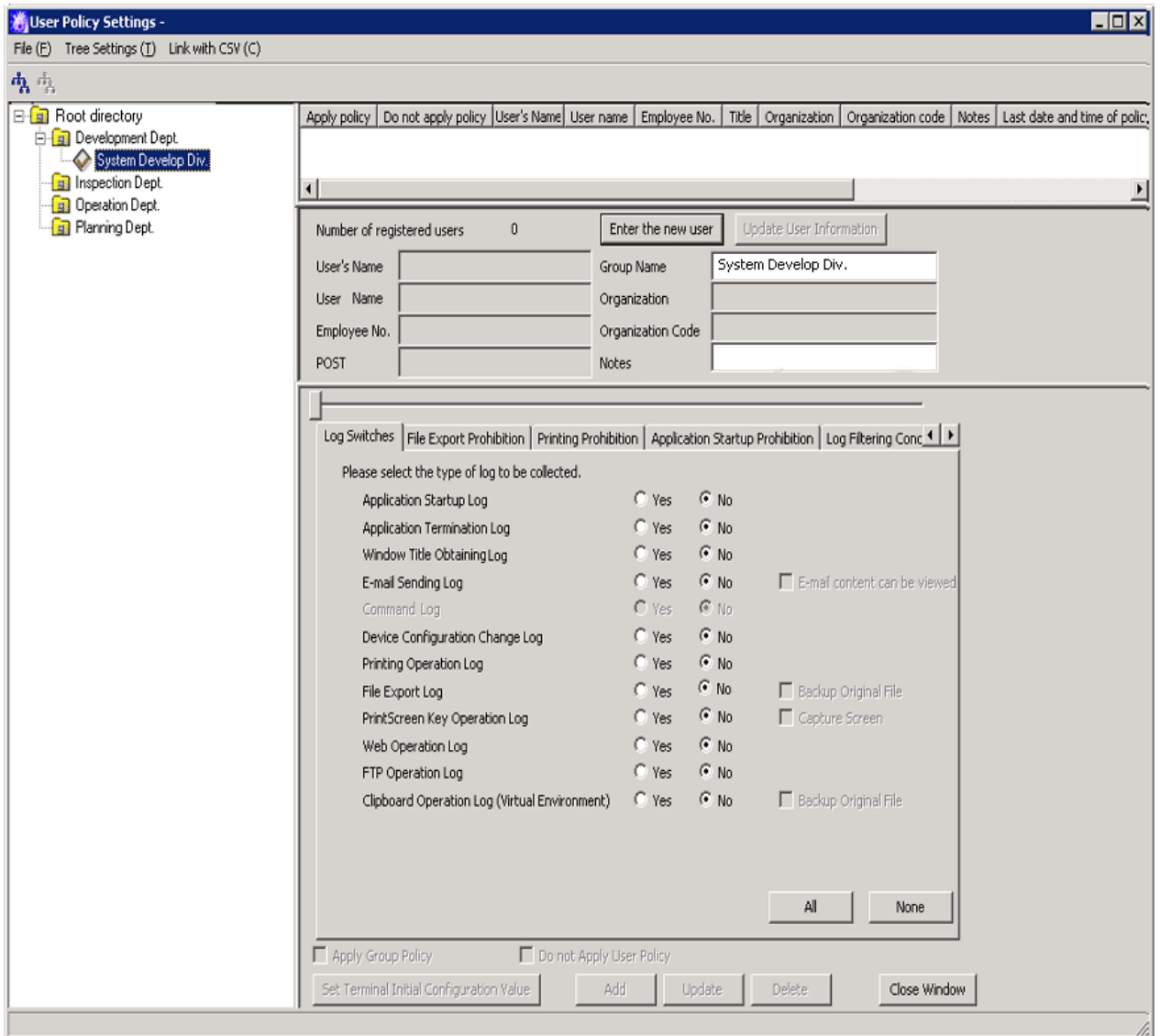
After a user group has been created, user policy can be set collectively for users in the user group.

The procedure for creating a user group is as follows.

1. Start [Management Console].

2. Select [User Policy Settings] from the [User Settings] menu.

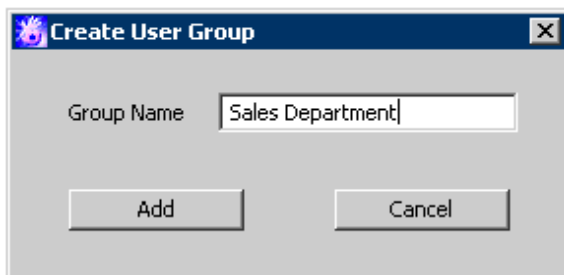
→ The [User Policy Settings] window is displayed.



3. Select the upper level group of the group to be created from user group tree.

4. Select [Create User Group] from the [File] menu.

→ The [Create User Group] window is displayed.



1. Enter the following information and click the [Add] button.

[Group Name]: Up to 40 single-byte characters (20 double-byte characters) of alphanumeric characters and Chinese characters can be entered.



→ The message that prompts structure update is output.

2. Click the [OK] button.

→ The group added in user group tree is displayed.

3. Select [Reflect CT Group Structure] from the [Tree Settings] menu.

→ The created user group is updated to the database.

If [Reflect CT Group Structure] is not performed, the message prompting [Reflect CT Group Structure] will be displayed when closing the [User Policy Settings] window.

After the created user has been updated to the database, the user group policy must be set as follows. Please modify the policy as needed. For details regarding policy modification, please refer to "[3.2.2 Modify User Group Policy](#)"

- When creating a user group under the Root directory

On the Master Management Server or Management Server where the user group has been created, policy set in the [Terminal Initial Settings] window will be updated.

- When creating a user group under other groups

Policy set in the upper level group of the created user group will be updated.

## Move

This section describes how to move the created user group in the user group tree to other user groups on the same server.

Even if the group is moved, the user group policy will not change. Though the user registered in the group will be moved if the user group is moved, user policy will not change (same as the condition before moving).

When a department administrator has been set in the user group, it will be moved if the user group is moved.

The procedure for moving a user group is as follows.

1. Start the [User Policy Settings] window.

2. Select the user group to be moved from the user group tree.

→ The selected user CT group is highlighted.

3. Move the user group to be moved to the target user group on the same server by dragging and dropping.

→ The message that prompts structure update is output.

4. Click the [OK] button.

→ The user group is moved.

5. Select [Reflect CT Group Structure] from the [Tree Settings] menu.

→ The moved user group is updated to the database.

If [Reflect CT Group Structure] is not performed, the message prompting [Reflect CT Group Structure] will be displayed when closing the [User Policy Settings] window.

## Delete

This section describes how to delete a user group created in the user group tree.

A user group cannot be deleted if any CT group or CT exists under it. Please delete the user group or user under it first. For details on how to delete a user, please refer to "[Delete a User](#)"

The procedure for deleting a user is as follows.

1. Start the [User Policy Settings] window.

2. Select the user group to be deleted from the user group tree.

3. Select [Delete User Group] from the [File] menu.  
→ The deletion confirmation window is displayed.
4. Click the [OK] button.  
→ The selected user group is deleted.
5. Select [Reflect CT Group Structure] from the [Tree Settings] menu.  
→ The “deleted” user group is updated to the database.  
If [Reflect CT Group Structure] is not performed, the message prompting [Reflect CT Group Structure] will be displayed when closing the [User Policy Settings] window.

### Modify group information

This section describes how to modify the name or notes of the user group created in the user group tree.

The procedure is as follows.

1. Start the [User Policy Settings] window.
2. Select the user group for information modification from the user group tree.  
→ The selected user CT group is highlighted.
3. Enter the following information and click the [Update] button.
  - [Group Name]: Enter the modified user group name.  
Up to 40 single-byte characters (20 double-byte characters) of alphanumeric characters and Chinese characters can be entered.
  - [Notes]: Enter the notes relating to the user group.  
Up to 40 single-byte characters (20 double-byte characters) of alphanumeric characters and Chinese characters can be entered.
4. Select [Refresh Tree] from the [Tree Settings] menu.  
→ The name of the selected user group is modified.  
If [Refresh Tree] in the [Tree Settings] menu is grayed out, structure may not be updated after creating, moving or deleting a user group. At this time, please select [Reflect CT Group Structure] from the [Tree Settings] menu to updating configuration.

## 2.6 Allocate Department Administrator

---

When allocating a department administrator, the department administrator should be allocated to a group after the configuration information tree has been created. (If the list of department administrators has been registered through the Server Settings Tool during the installation of Systemwalker Desktop Keeper.)

After the application has started, the department administrator can be registered again and allocated by using the Server Settings Tool. For the registration method please refer to the “Set Administrator’ Information” of “Systemwalker Desktop Keeper Installation Guide”.

Only the system administrator can allocate a department administrator.

Even if any subgroup exists under the CT group (user group) in which the department administrator has been set, the same department administrator will be set automatically.

Though the department administrator can be confirmed in the group where it has been set, it cannot be displayed in the subgroup even if it is expected to be confirmed.

The department administrator can create groups, set policies and register users for the CT/user of the group and its subgroup in which it is set as the department administrator. For operations that can be performed by the department administrator and the scope of operation, please refer to “Function Available for Each Type of Administrator” of “Systemwalker Desktop Keeper Installation Guide”.

When the department administrator is set for user group only, but not for CT group, the department administrator cannot view logs. When the group tree displayed in Log Viewer is CT group tree, the logs in each CT can be viewed. Therefore, please set the department administrator in CT group in order to view logs.

As to the client (CT) displayed in the following locations of the configuration information tree, the department administrator cannot be set (if a group is created in the following locations, the department administrator can be set for this group). Therefore, only the system administrator can move and delete the client (CT) displayed in the following locations.

- Directly under the Root directory
- Directly under domain group
- Directly under Local group

In a 3-level system structure, set department administrator in which the server is determined by the settings in the [System Settings] window of [Server Settings Tool].

When linking with Active Directory	When Active Directory Linkage is not performed	
	To manage user information collectively in Master Management Server	To manage user information on each Management Server (Compatible with V13.0 or earlier)
Set in Master Management Server. (Notes)	Set in Master Management Server. (Notes)	Set in each Management Server. The information of Master Management Server will be updated to each Management Server.

Notes: If it cannot be used due to troubles in the Master Management Server, settings can be performed in the Management Server. However, the settings in the Management Server will be overwritten by the latest information in the Master Management Server in the following cases:

- When restarting SWLevelControlService/SWServerService
- When performing Active Directory Linkage
- When updating [Administrator Information Settings] in Server Settings Tool
- When setting in the Management Console connected with the Master Management Server (but only the department which has been set can be updated)



**To search the operation logs in Citrix XenApp client more efficiently**

If the administrator of the Citrix XenApp Server has been set, the department administrator of the Citrix XenApp Server group can audit all the operations on the Citrix XenApp Server.

In addition, when the Citrix XenApp Server group and CT group exist in this department, both the department administrators of the two groups can know the operations on the Citrix XenApp client and the client (CT).

The following are two methods for allocating a department administrator.

- Allocate using GUI
- Allocate collectively using CSV files

During operation, the Management Console must be authorized with [Import CSV files]. Authority can be set in [Detailed Authority] in the [Administrator Information Settings] window of the Server Settings Tool.

CSV files of allocated department administrator must be created in advance.

At first, the department administrator information is exported in CSV format in the Management Console to get the format of the CSV file. Add the added department administrator to the file.

When allocating multiple department administrators to the same CT group (user group), please copy the records of target groups and record the logon ID of department administrator.

[Examples of Creation]

The boldface part after the second line (the fifth item is “Logon ID of Department Administrator”) is the newly added information in CSV file.

```

"Depth", "Group ID", "Group Name", "Processing Flag", "Logon ID of Department Administrator",
"User Name of Department Administrator", "Access Authority", "Detailed Authority - Management
Console 1", "Detailed Authority - Management Console 2", "Detailed Authority - Management Console
3", "Detailed Authority - Management Console 4", "Detailed Authority - Management Console 5", "
Detailed Authority - Management Console 6", " Detailed Authority - Management Console 7", "
Detailed Authority - Management Console 8", "Detailed Authority - Log Viewer 1", "Detailed
Authority - Log Viewer 2", "Detailed Authority - Log Viewer 3", "Detailed Authority - Log Viewer
4", "Detailed Authority - Log Viewer 5", "Detailed Authority - Log Viewer 6", "Detailed Authority
- Log Viewer 7", "Detailed Authority - Log Viewer 8", "Notes"
"1", "8F10E643-2E93-4c5d-820E-D4A3322130A7", "Planning Department", " ", "Moriyama", " ", " ",
" ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " "
"2", "7F9CB48C-DA30-45d7-9E86-08E95994AF1C", "Planning Department", " ", "Lin", " ", " ", " ", " ",
" ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " "
"2", "7F9CB48C-DA30-45d7-9E86-08E95994AF1D", "Planning Department", " ", " ", " ", " ", " ", " ",
" ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " ", " "

```

For details of CSV files, please refer to “File Reference” of “Systemwalker Desktop Keeper Reference Manual”. Also, the authority of the department administrator must be set for the department administrator that logs on to CSV files. Authority is set in the [Administrator Information Settings] window of Server Settings Tool. For details, please refer to “Set Administrator’ Information” of “Systemwalker Desktop Keeper Installation Guide”.

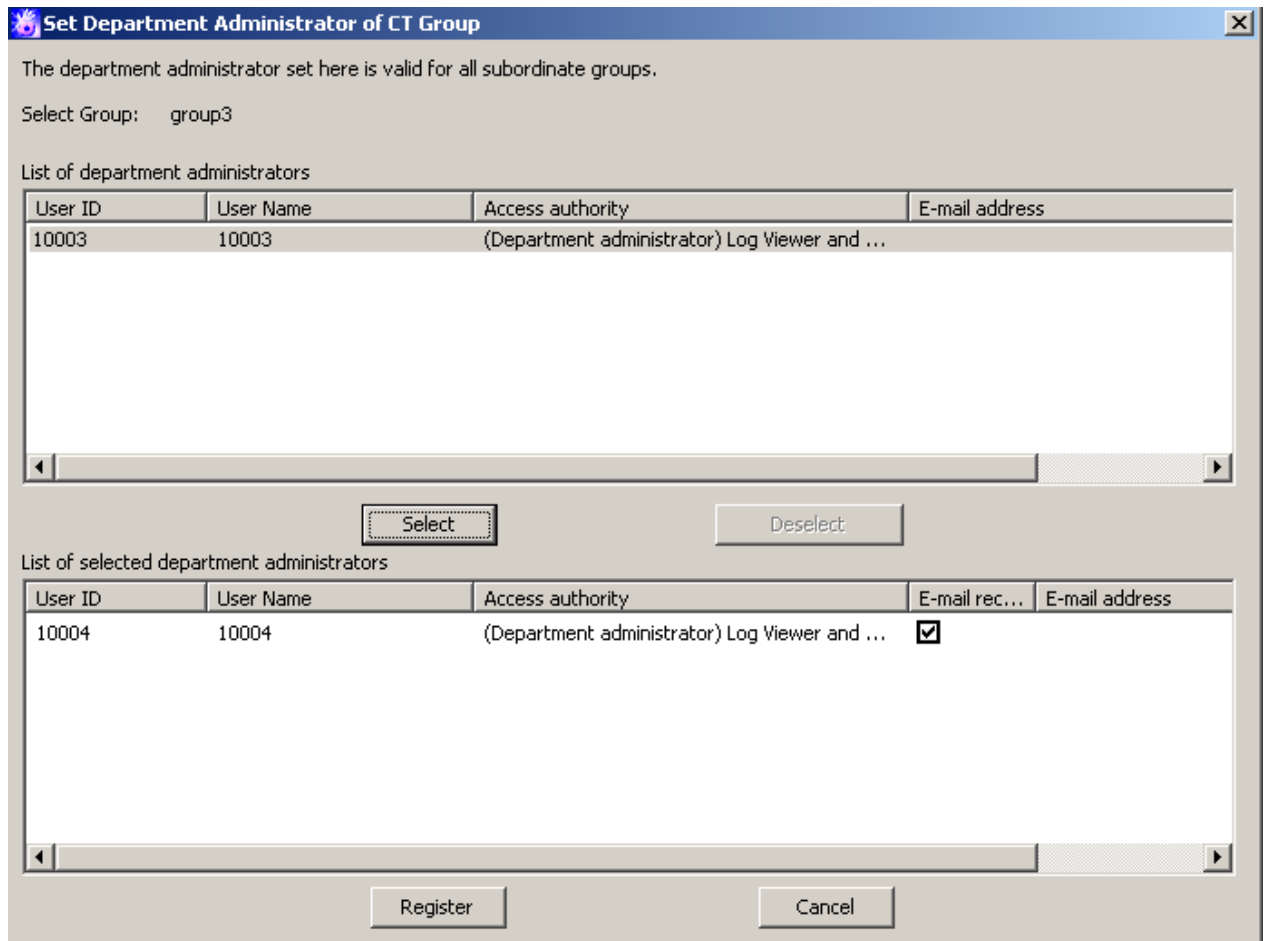
**Allocate using GUI**

This section describes how to allocate department administrator using GUI.

Allocate department administrator to CT group

1. Start [Management Console].  
Use the user ID and password of administrator to logon.
2. Select a CT group to set department administrator from the CT group tree.

3. Select [Set Department Administrator of CT Group] from the [File] menu.  
→ The [Set Department Administrator of CT Group] window is displayed.

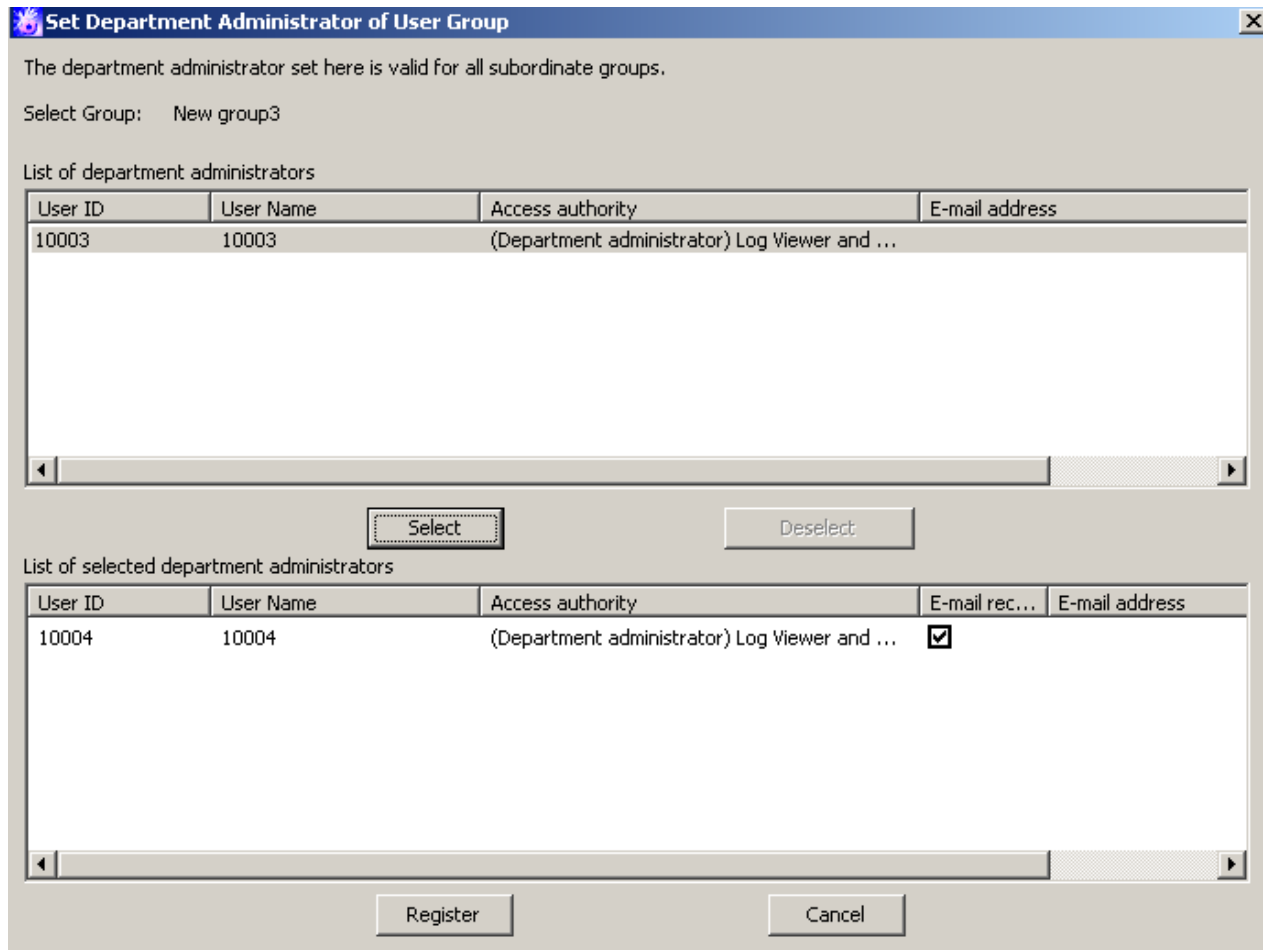


4. Select the department administrator to be set from [List of department administrators] and click the [Select] button.  
→ The selected department administrator is displayed in [List of Selected department administrators].
5. Please set [E-mail receiving].  
If selected (initial value): an administrator notification E-mail will sent to the registered department administrator.  
If not selected: an administrator notification E-mail will not be sent.  
If [Administrator Notification Settings] has not been set in the Server Settings Tool, the E-mail will not be sent even if it is selected.
6. Click the [Register] button.  
→ The confirmation window is displayed.
7. Click the [OK] button.

#### Allocate department administrator to user group

1. Start [Management Console].  
User the user ID and password of the system administrator to logon.
2. Select [User Policy Settings] from the [User Settings] menu.  
→ The [User Policy Settings] window is displayed.
3. Select a user group to set the department administrator from the user group tree.

4. Select [Set Department Administrator of User Group] from the [File] menu.  
→ The [Set Department Administrator of User Group] is displayed.



5. Select the department administrator to be set from [List of department administrator] and click the [Select] button.  
→ The selected department administrator is displayed in [List of Selected department administrator].
6. Please set [E-mail receiving].  
If selected (initial value): an administrator notification E-mail will be sent to the registered department administrator.  
If not selected: an administrator notification E-mail will not be sent.  
If [Administrator Notification Settings] has not been set in the Server Settings Tool, the E-mail will not be sent even if it is selected.
7. Click the [Register] button.  
→ The confirmation window is displayed.
8. Click the [OK] button.

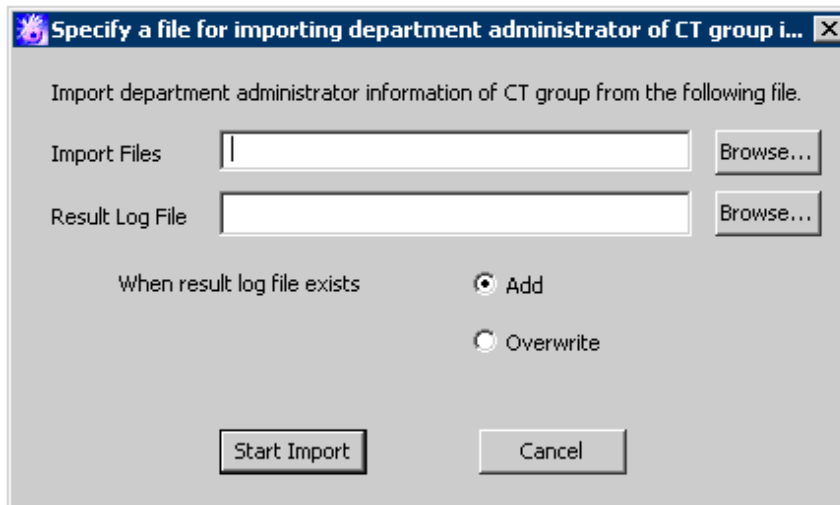
### Allocate collectively using CSV files

This section describes how to allocate department administrators collectively using CSV files.

#### Allocate department administrator to CT group

1. Start [Management Console].  
Use the user ID and password of the system administrator to logon.

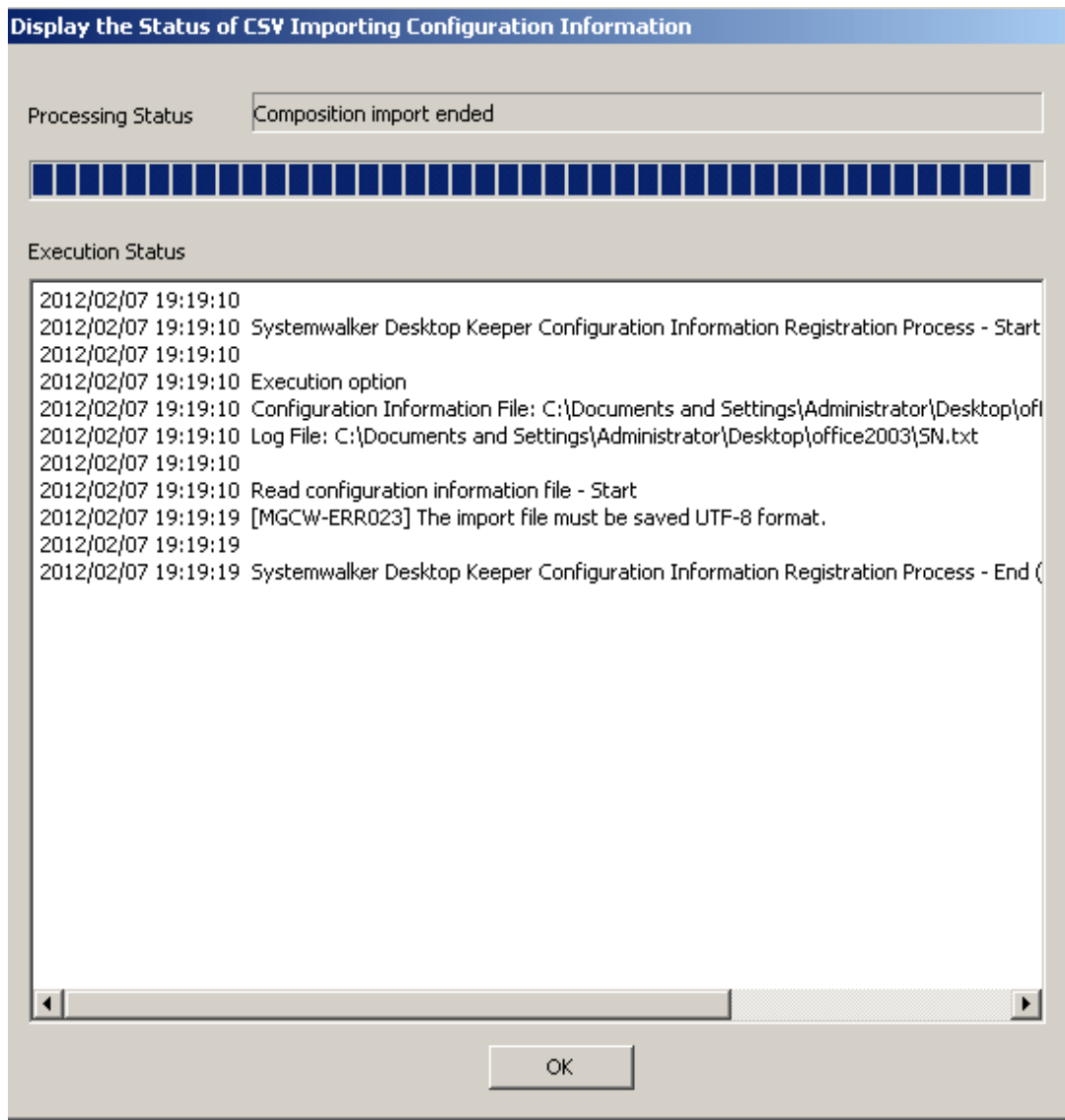
2. Select [Import Department Administrator of CT Group in CSV Format] from the [File] menu.  
→ The [Specify a file for importing department administrator of CT group] window is displayed.



- **[Import File]** (required): Specify the CVS file with defined department administrator information with the full path.
- **[Result Log file]** (required): Specify the file for saving operation result with full path.
- **[When result log file exists]**: When a current result log file exists, please make sure to set it.  
**[Add]**: Select it to add a record to the existing result log file.  
**[Overwrite]**: Select it to overwrite the existing result log file.

3. Set the above information and click the [Start Import] button.

→ The [Display the Status of CSV Importing Configuration Information] window is displayed.



4. After department administrator information has been registered to the database, [Registering] will change to [Registration completed]. Click the [OK] button.

#### Allocate department administrator to user group

1. Start [Management Console].

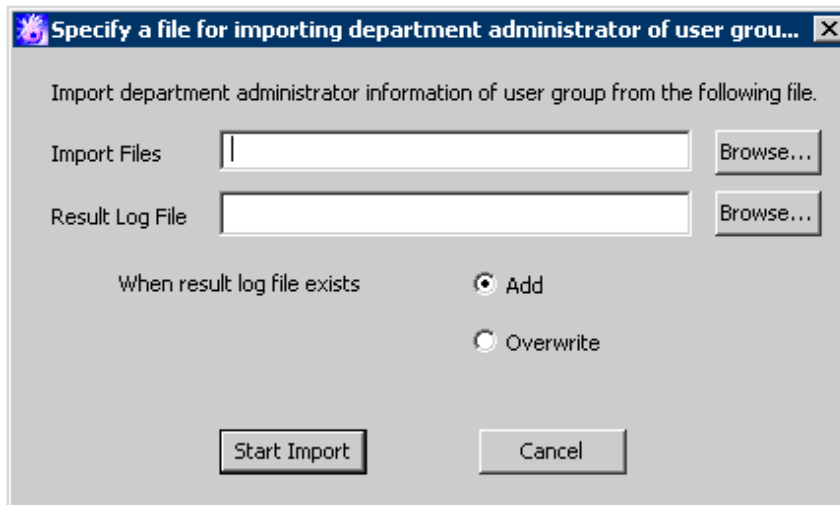
Use the user ID and password of the system administrator to logon.

2. Select [User Policy Settings] from the [User settings] menu.

→ The [User Policy Settings] window is displayed.

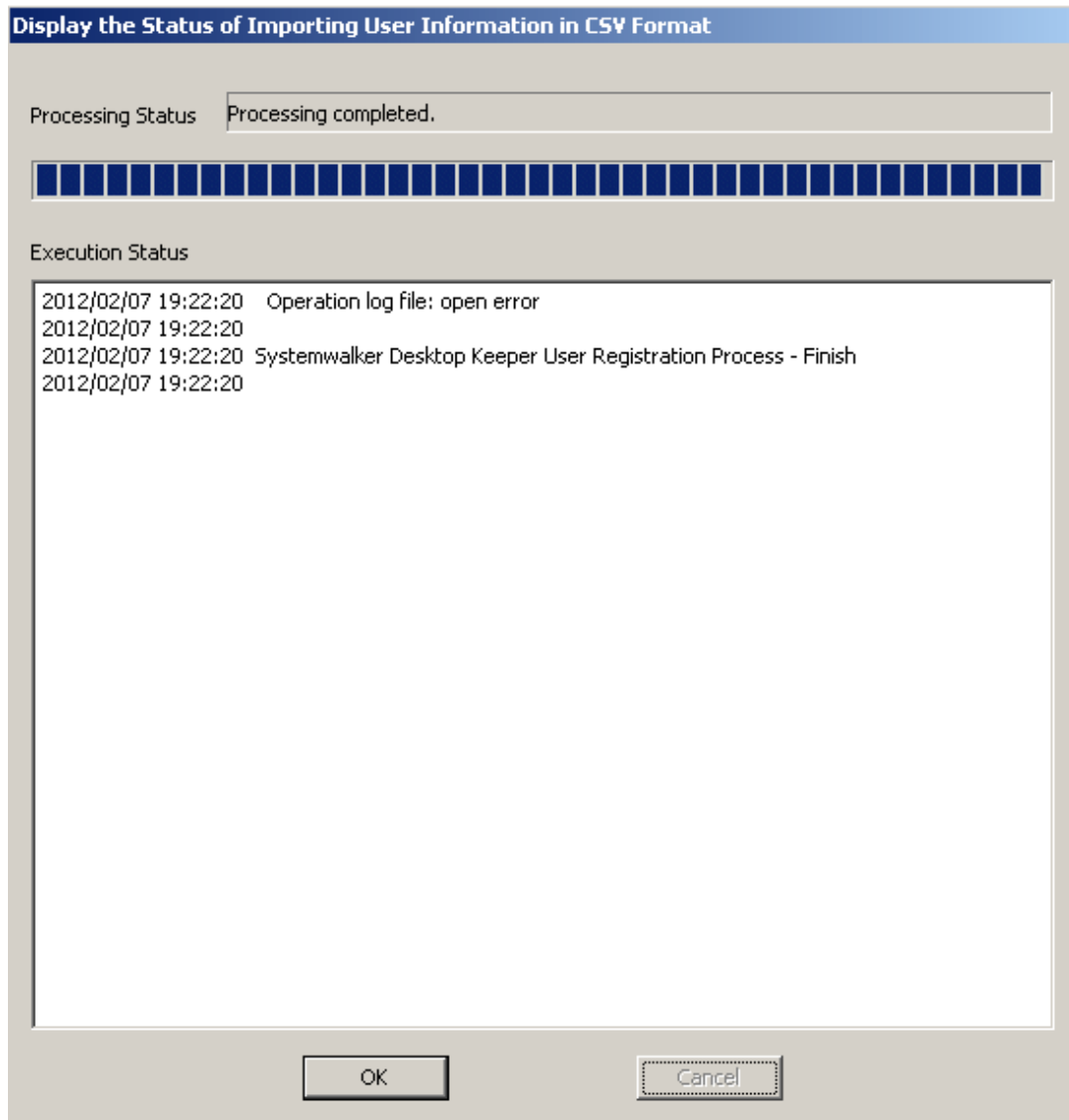


3. Select [Import Department Administrator Information of User Group in CSV Format] from the [File] menu.  
→ The [Specify a file for importing department administrator of user group] window is displayed.



- **[Import File]** (required): Specify the CVS file with defined department administrator information with the full path.
- **[Result Log File]** (required): Specify the file for saving operation result with full path.
- **[When result log file exists]**: When a current result log file exists, please make sure to set it.  
**[Add]**: Select it to add a record to the existing result log file.  
**[Overwrite]**: Select it to overwrite the existing result log file.

4. Set the above information and click the [Start Import] button.  
→ The [Display the Status of Importing User Information in CSV Format] window is displayed.



5. After department administrator information has been registered to the database, [Registering] will change to [Registration completed]. Click the [OK] button.

## 2.6.1 Export Department Administrator Information through Management Console

---

This section describes how to export department administrator information to CSV files.

### Executer

The system administrator and department administrator can export department administrator information to CSV files.

[Import CSV file] authority must be granted to the Management Console before execution. The system administrator can set the authority in [Detail authority] in the [Administrator Information Settings] window of the Server Settings Tool.

### Scope of Export

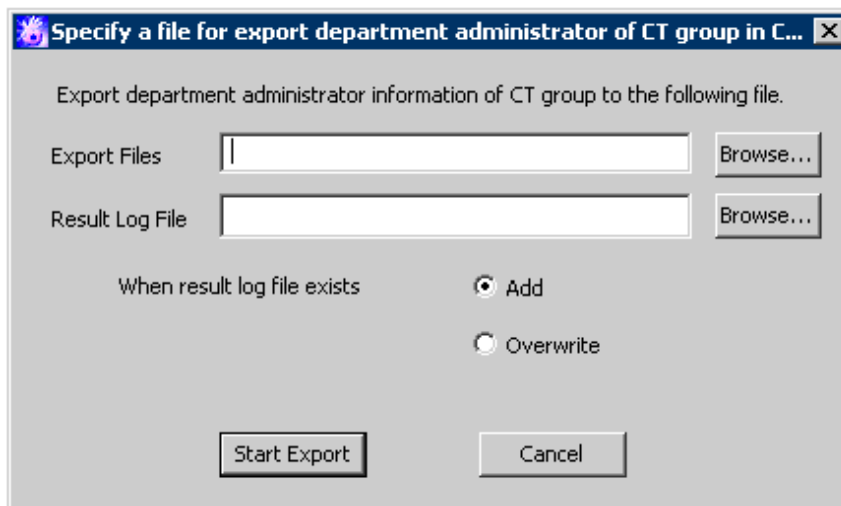
When the system administrator performs the export, department administrator information of all groups on the Management Server can be exported. For groups without a department administrator, [Group ID] and [Group Name] will be exported.

When the department administrator performs the export, all information of the department group and its subordinate groups can be exported. For groups that do not belong to a department, only [Group ID] and [Group Name] will be exported.

For details about exported content, please refer to “Department Administrator Information” in “File Reference” of “Systemwalker Desktop Keeper Reference Manual”.

## Export department administrator information of CT group

1. Start [Management Console].
2. Select [Export Department Administrator of CT Group in CSV Format] from the [File] menu.  
→ The [Specify a file for export department Administrator of CT Group in CSV Format] window is displayed.

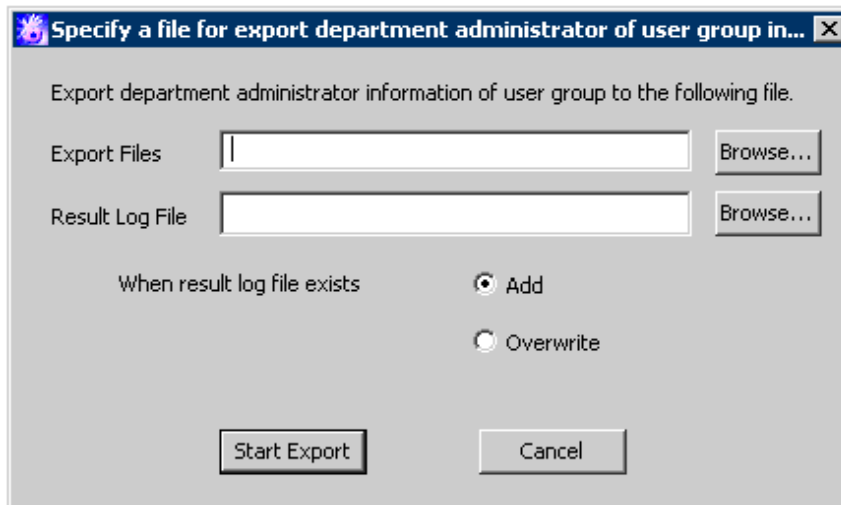


- **[Export Files]** (required): Specify the CSV file to export department administrator information with the full path.  
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in a file name:  
“\” “/” “:” “\*” “?” “” “<” “>” “|”.
  - **[Result Log File]** (required): Specify the file for saving operation result with the full path.  
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in a file name:  
“\” “/” “:” “\*” “?” “” “<” “>” “|”.
  - **[When result log file exists]**: When the current result log file exists, please make sure to set it.  
**[Add]**: Select it to add a new record to the existing result log file.  
**[Overwrite]**: Select it to overwrite the existing result log file.
3. To set the information above, click the [Start to Export] button.
  4. A message appears after the operation. Click the [OK] button.

## Export department administrator information of user group

1. Start [Management Console].
2. Select [User Policy Settings] from the [User settings] menu.  
→ The [User Policy Settings] window is displayed.

3. Select [Export Department Administrator of User Group in CSV Format] from the [File] menu.  
→ The [Specify a file for export department administrator of user group in CSV Format] window is displayed.



- **[Export Files]** (required): Specify the CSV file to export department administrator information with the full path. Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in a file name: “\” “/” “:” “\*” “?” “|” “<” “>” “|”.
  - **[Result Log File]** (required): To specify files saving operation result by using the full path. Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in a file name. “\” “/” “:” “\*” “?” “|” “<” “>” “|”.
  - **[When result log file exists]**: When the current result log file exists, please make sure to set it.  
**[Add]**: Select it to add new record to the existing result log file.  
**[Overwrite]**: Select it to overwrite the existing result log file.
4. Set the above information and click the [Start Export] button.
  5. A message will be displayed after the operation has completed. Click the [OK] button.

## 2.7 Preparations for Log Aggregation

---

When using the status window or Log Analyzer to confirm the log aggregation result, visible columns and threshold value must be defined in advance.



### Note

#### Notes relating to the start of Web Console

Please do not start multiple Web Consoles on one PC.

### 2.7.1 Prepare for Using Status Window

---

This section describes how to set aggregation conditions.

Only the system administrator can set aggregation conditions.

When modifying the aggregation conditions in use, the modified condition will be updated at next aggregation. Therefore, the number of PC number of sets detected according to the old conditions and detailed graph will be displayed in the window before the next aggregation.

In a 3-level system structure, to know the overall system state, please set aggregation conditions in the Master Management Server. To know the state of the subordinate Management Server, please set aggregation conditions in each Management Server.

1. Start Web Console with any of the following methods.

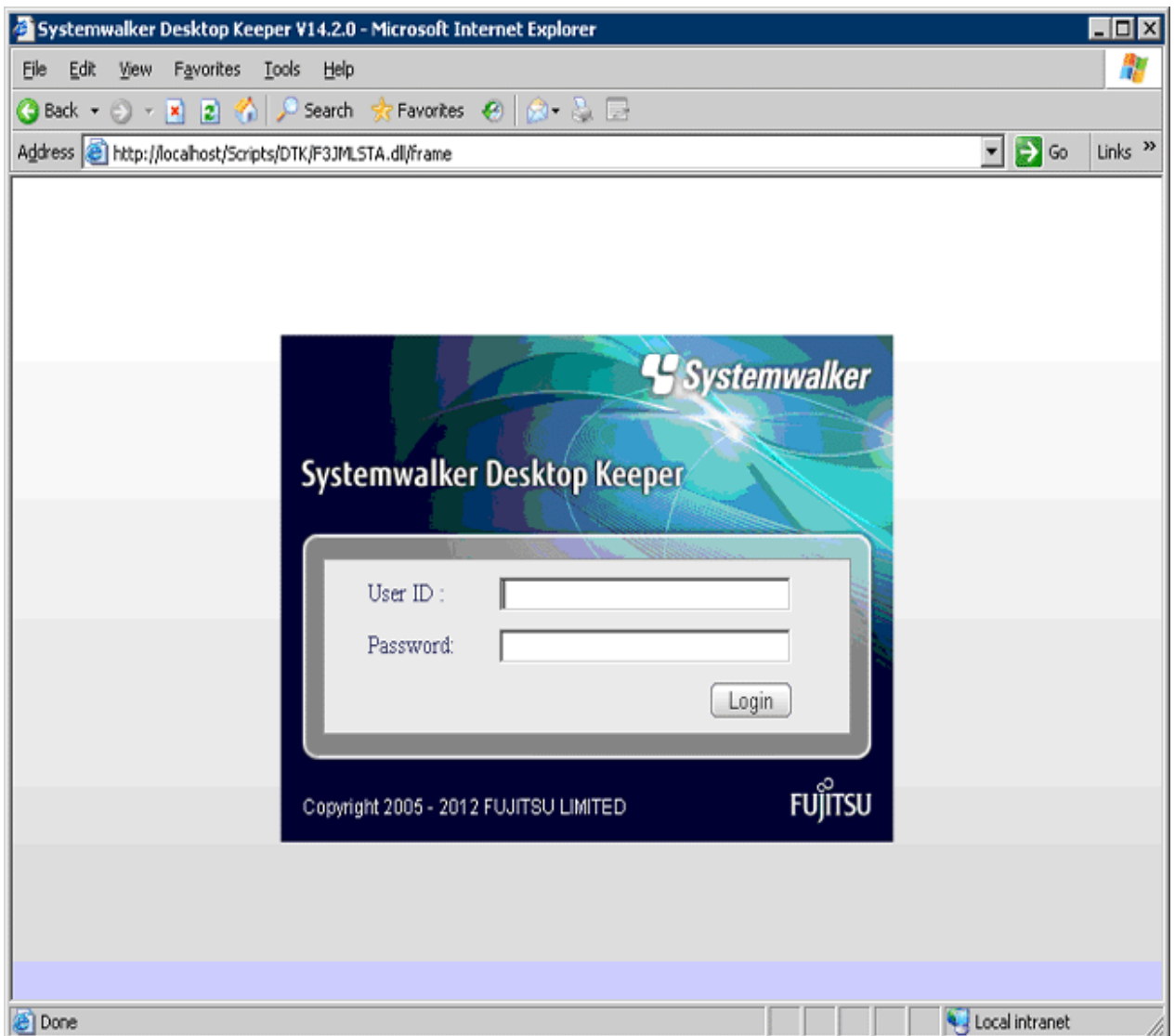
In a 2-level system structure, please connect to the Management Server.

- Select [All Programs]-[Systemwalker Desktop Keeper]-[Server]-[Desktop Keeper Main Menu] from the [Start] menu on Management Server.
- Specify “http://host name of Management Server or IP address/DTK/index.html” in the address bar of browser.  
When the port number of IIS is modified, specify as follows.  
http://IP address: port number/DTK/index.html

In a 3-level system structure, please connect to (Master) Management Server respectively.

- Select [All Programs]-[Systemwalker Desktop Keeper]-[Server]-[Desktop Keeper Main Menu]] from the [Start] menu on (Master) Management Server.
- Specify “http://host name of (Master) Management Server or IP address/DTK/index.html” in the address bar of browser.  
When the port number of IIS is modified, specify as follows.  
http://IP address: port number/DTK/index.html

→ The [Login] window is displayed.



2. Enter the following information and click the [Login] button.

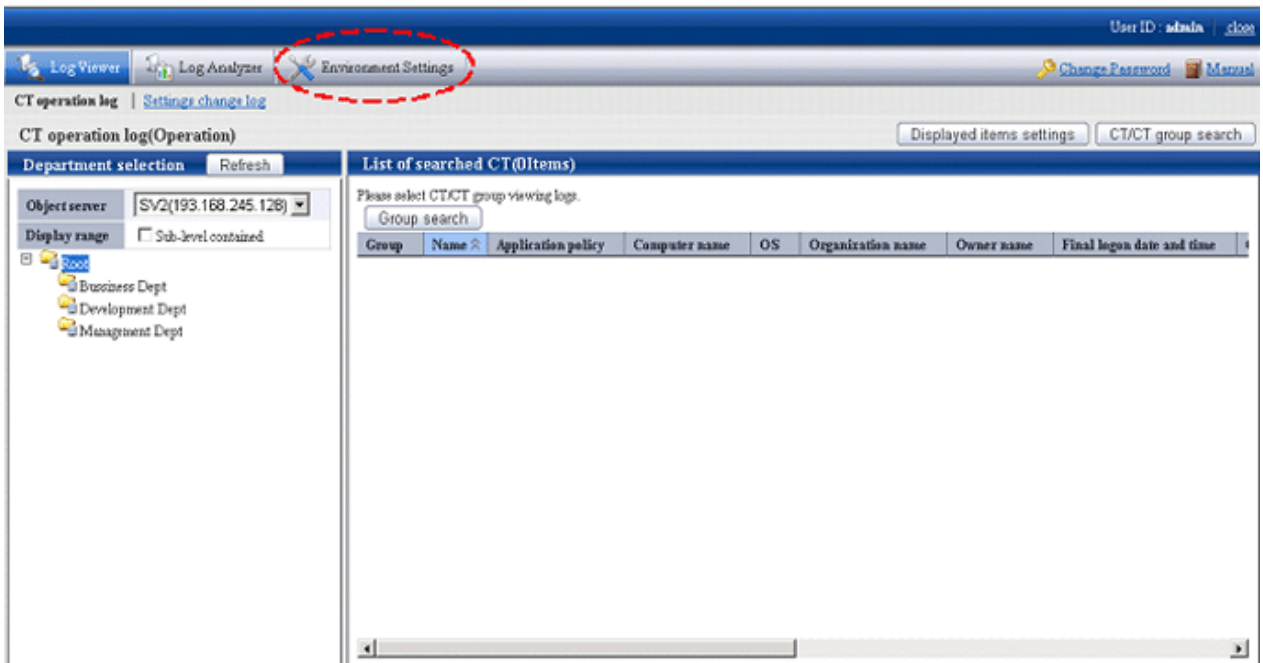
- [User ID]: The [User ID] set in the [Administrator Information Settings] window of Server Settings Tool.
- [Password]: The [Password] set in the [Administrator Information Settings] window of Server Settings Tool.  
It is recommended to Modify password regularly. For how to Modify password, please refer to "[Change password](#)".

→ The status window is displayed.

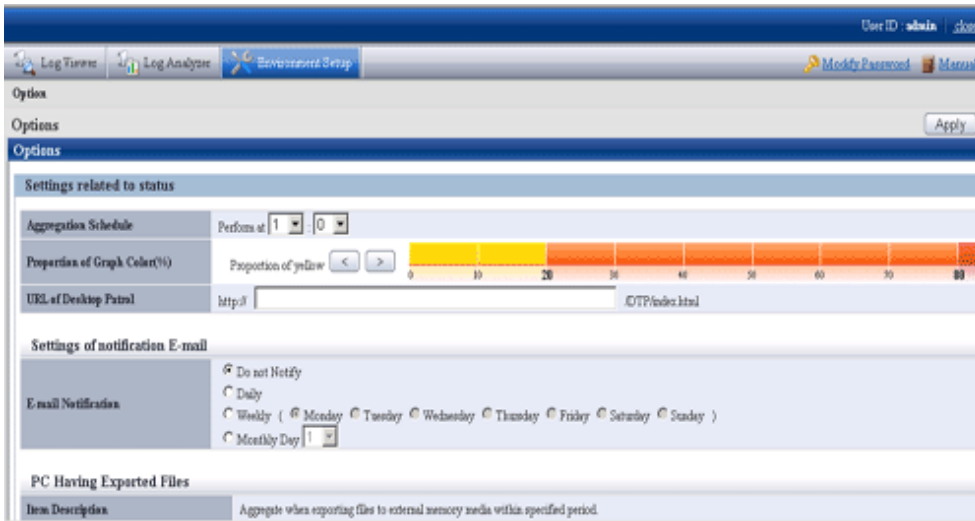


3. Click [Log Management] of Global Navigation.

→Log Viewer is started and the [CT Operation Log] window is displayed.



- Click [Environment Setup] of Global Navigation.  
→ The [Options] window is displayed.



- Enter the following information and click the [Apply] button.

#### About the processing time required for aggregation

The processing time required for aggregation is affected by the following factors:

- Hardware specification (CPU, memory, disk performance, etc.)
- Operating environment (network status, operation conditions of other applications, etc.)
- Number of Management Servers (Master Management Server in a 3-level structure)
- Aggregation conditions (number of audited items and auditing period (\*))
- CT number of sets
- Amount of logs saved in the database

Even if the above operating environments are the same, the aggregation result will still be affected by the following factors, which will result in a different processing time:

- CT number of sets satisfying the aggregation conditions (\*)
- Number of logs satisfying the aggregation conditions (\*)

Items marked by (\*) are the main reasons and have significant influence.

The following is an example of processing time. (As a reference value, it is greatly affected by hardware and data.)


In fact, the processing time affected by environment and data conditions is from several minutes to hours.

When both of the hardware are CPU:Core2Duo 2.4GHz with 3GB memory.


- Number of CTs is 100 (all meeting the aggregation conditions), number of logs is 630,000 (among which 210,000 satisfies the aggregation conditions), the auditing period is 31 days, and the processing time is about 150 seconds.
- Number of CTs is 500 (all meeting the aggregation conditions), number of logs is 630,000 (among which 210,000 satisfies the aggregation conditions), the auditing period is 31 days, and the processing time is about 430 seconds.


Item Name	Description
[Aggregation Schedule]	Set the time to start aggregation. <ul style="list-style-type: none"> <li>- Hour: Select by hour within the range of 0-23</li> <li>- Minute: Select by minute within the range of 0-59</li> </ul> <b>Initial value:</b> 1 hour 0 minute



Item Name	Description
	 <b>Note</b> ..... <b>Please take the following points into consideration in the settings of an aggregation schedule:</b> <ul style="list-style-type: none"> <li>- The aggregation process will cause a heavy load. Please perform in the time frame with lower business load (at midnight, etc.).</li> <li>- Please do not modify configuration information and environment setup during aggregation. The aggregation result may be displayed incorrectly.</li> <li>- Level Control Service must be started during the aggregation process. Please do not overlap with the operation of stopping Level Control Service (backup, restoration, data transmission, etc.).</li> </ul> .....
[Proportion of Graph Color(%)]	Set and modify the threshold value of histogram colors in the status window. Select and modify the proportion of yellow and red through the button. Modify it by 10%. Initial value: the threshold value of the yellow histogram is within 20% the threshold value of the red histogram is above 80%
[URL of Desktop Patrol]	Set it when assets management information of Systemwalker Desktop Patrol is displayed. Single-byte alphanumeric characters, "." and ":" can be specified. Initial value: not displayed
Settings of Notification E-mail	
E-mail Notification	Set to notify the department administrator about the aggregation result by E-mail. <ul style="list-style-type: none"> <li>- Do not notify: Do not notify by E-mail.</li> <li>- Daily: notify by E-mail every day.</li> <li>- Weekly: Specify the day to notify by E-mail once a week. Please set which day and whether to notify the aggregation result by E-mail on that day weekly.</li> <li>- Monthly: Specify which day to notify by E-mail once a month. Select one day from the first day to the 28th day in a month to notify the aggregation result by E-mail.</li> </ul> <b>Initial value:</b> [Do Not notify] The following aggregation items are not notified by E-mail. <ul style="list-style-type: none"> <li>- [PC having blocked the use of prohibited USB memory]</li> <li>- [PC having blocked the use of prohibited account group]</li> <li>- [PC having blocked the use of prohibited application]</li> <li>- [PC having blocked prohibited printin]</li> <li>- [PC having blocked the sending of E-mail with prohibited attachment]</li> </ul> E-mail notification will be sent to the department administrator of the group to which the error PC belongs (when no department administrator is set in the group, notification will be sent to department administrator of the upper level group). E-mail is not sent in following cases: <ul style="list-style-type: none"> <li>- When there is no department administrator in the upper level group</li> <li>- When the recipient address of the department administrator is not set though department administrator has been set</li> </ul>

Item Name	Description
	<ul style="list-style-type: none"> <li>- When there is no error PC in the department managed by the department administrator</li> <li>- When [Manage on each Management Server] has been set in [System Information Settings]-[Manage User Information] of server settings tool At this time, the result aggregated in the Master Management Server will not be sent to the department administrator set in the Management Server. Please set an E-mail notification on each Management Server.</li> <li>- When aggregation process stops abnormally</li> <li>- When Level Control Service stops At this time, if aggregation process ends normally, E-mail notification will be performed after Level Control Service starts.</li> </ul> <p>Also, please set the recipient address of the E-mail server and department administrator in [Server Settings Tool].</p>
E-mail Title	<p>Set the subject of E-mail.</p> <p>Please specify characters to be no greater than 128 bytes. The E-mail will be sent without any subject if the subject is omitted.</p> <p><b>Initial value:</b> (blank)</p>
E-mail Text	<p>Set the body text of E-mail.</p> <p>Please specify characters no greater than 512 bytes in size.</p> <p><b>Initial value:</b> (blank)</p> <p>The body text of notification is shown as follows.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> The specified content in [E-mail Body Text]  [Overview] Aggregation target department:  [Counting information] (*1) PC having exported files: PC pattern 1 that is is used out of working time PC pattern 2 that is is used out of working time PC having performed suspicious access: PC not connected for a long time:  [Attachment information] (*2) ----- PC having exported files 1: terminal name    :    : ----- PC pattern 1 that is used out of working time: 1: terminal name    :    : -----       :       :       (omitted) -- http://IP address DTK/index.html </pre> </div> <p>*1: if over one correspondent terminal exists in items to be aggregated, they will be recorded.</p>

Item Name	Description
	<p>*2: when [Attach] is selected in [List of Problem PCs], the correspondent terminal name will be displayed in each aggregation target item.</p> <p> <b>Note</b></p> <hr style="border-top: 1px dotted orange;"/> <p><b>About content recorded in E-mail body text</b></p> <p>The content notified by using the E-mail notification function is the aggregation result during the E-mail notification. After the next aggregation (once a day), the result may be inconsistent with that in the status window.</p> <hr style="border-top: 1px dotted orange;"/>
List of Fault PCs	<p>Set whether to record the list of aggregated PCs in the E-mail body text.</p> <ul style="list-style-type: none"> <li>- Not attach: Not to record the list of problem PCs.</li> <li>- Attach: Record the list of problem PCs. (Up to 1000 error PCs can be recorded.)</li> </ul> <p><b>Initial value:</b> not attach</p>
[PC Having Exported Files] (all conditions are aggregated as AND conditions)	
[Item Description]	Description of the aggregated items.
[Aggregation of Items]	<p>Set whether to display the aggregation result in the status window or not.</p> <p><b>Initial value:</b> [Yes]</p>
[Settings of Aggregation Period]	<p>Set the aggregation time for error PCs (from the day before X to the day of aggregation).</p> <p>Select by 1 day within 1-31 days.</p> <p><b>Initial value:</b> 7 days</p>
[Type of Operation]	<p>Select from file export, file operation (move, copy and rename) as the type of operation log of counting target.</p> <p>Multiple selection can be made. At least one must be selected.</p> <p><b>Initial value:</b> [File export]</p>
[Settings of External Memory Media Type]	<p>Select from Removable, CD/DVD and Network as the drive type of external memory media.</p> <p>Multiple can be selected. At least one must be selected.</p> <p><b>Initial value:</b> [Removable]</p>
[Filtering Settings]	<p>Set keyword contained in the file path of export source.</p> <p>By specifying the path of the shared folder as a keyword, aggregation can be performed when exporting files of specific shared server only.</p> <p>To specify multiple keywords, enter a single-byte space between each of them. Up to 10 keywords can be specified.</p> <p>As single-byte space is used as a separator, it cannot be used as a keyword. Up to 128 byte including the separator can be set.</p> <p>The alphabets are case-insensitive.</p> <p>When specifying shared folder, please specify as follows.</p> <p>\\server name\folder name          \\IP address\folder name</p> <p><b>Initial value:</b> (blank)</p>
[PC Used out of Working Time] (all conditions are aggregated as AND conditions)	
[Item Descriptions]	Description of the aggregated items.
[Aggregation of Items]	<p>Set whether to aggregate or not.</p> <p>When selecting not to count, the status window will not be displayed.</p> <p><b>Initial value:</b> [Yes]</p>

Item Name	Description
[Settings of Aggregation Period]	Set the aggregation time for error PCs (from the day before X to the day of counting). Select by 1 day within 1-31 days. <b>Initial value:</b> 7 days
[Settings of Non-working Time]	Define the time frame as “Non-working Time”. <ul style="list-style-type: none"> <li>- Day of a week: select which day to be set as non-working time. At least one must be selected.</li> <li>- Time: select the time to be set as non-working time. Specify by 1 hour within 0-23. When n the time is not specified, set to “-”.</li> </ul> <b>Initial value:</b> <ul style="list-style-type: none"> <li>- Pattern 1 (supposed from Monday to Friday)               <ul style="list-style-type: none"> <li>- Day of the week: Monday, Tuesday, Wednesday, Thursday, Friday</li> <li>- Time: from 00:00 to 08:59 and 17:00 to 23:59</li> </ul> </li> <li>- Pattern 2 (supposed on weekend supposed)               <ul style="list-style-type: none"> <li>- Day of the week: Saturday, Sunday</li> <li>- Time: Not specified</li> </ul> </li> </ul>  <b>Example</b> ..... <b>Specification Example 1</b> When aggregating PCs used at weekends <ul style="list-style-type: none"> <li>•Time: not specified</li> <li>•Day of the week: Saturday and Sunday are selected</li> </ul> <b>Specification Example 2</b> When aggregating PCs used during non-working time from Monday to Friday <ul style="list-style-type: none"> <li>•Time: 00:00 to 08:59 or 17:00 to 23:59</li> <li>•Day of the week: Monday, Tuesday, Wednesday, Thursday, Friday selected</li> </ul> ..... When the same period is set, it will not be aggregated repeatedly. [Example] Set to from 00:00 to 06:59 or 00:00 to 06:59 and only one PC is used in the above period, there will be only one aggregation result.
[PC Having Performed Suspicious Access] (all conditions are aggregated as AND conditions)	
[Item Descriptions]	Description of the aggregated items.
[Aggregation of Items]	Set whether to aggregate or not. When selecting not to count, the status window will not be displayed. <b>Initial value:</b> [Yes]
[Settings of Aggregation Period]	Set the aggregation time for error PCs (from the day before X to the day of aggregation). Select by 1 day within 1-31 days. <b>Initial value:</b> 7 days
[Settings of Access Type]	Set access type. <ul style="list-style-type: none"> <li>- Start in safe mode: it is aggregated when the PC is started in safety mode.</li> </ul>

Item Name	Description
	<ul style="list-style-type: none"> <li>- Login with local user: in the environment where the domain is used, it is aggregated when logging in as local user.</li> <li>- Login with administrator authority: it is aggregated when logging in with administrator authority.</li> </ul> <p><b>Initial value:</b> [Start in safe mode]</p>
[PC Not Connected for a Long Time] (all conditions are aggregated as AND conditions)	
[Item Descriptions]	Description of the aggregated items.
[Aggregation of Items]	Set whether to aggregated or not. When selecting not to count, the status window will not be displayed. <b>Initial value:</b> [Yes]
[Settings of Disconnection Period]	Set the disconnection period. Select by 1 day within 1-366. <b>Initial value:</b> 30 days
[PC Having Blocked the Use of Prohibited USB Memory] [PC Having Blocked the Use of Prohibited Account Group] [PC Having Blocked the Use of Prohibited Application] [PC Having Blocked Prohibited Printing] [PC Having Blocked the Sending of E-mail with Prohibited Attachment]	
(All conditions are aggregated as AND conditions)	
[Item Descriptions]	Description of the aggregated items.
[Aggregation of Items]	Set whether to display the aggregation result in the status window or not. <b>Initial value:</b> [No]
[Settings of Aggregation Period]	Set the aggregation time for error PCs (from the day before X to the day of aggregation). Select by 1 day within 1-31 days. <b>Initial value:</b> 7 days

## 2.7.2 Prepare for Using Log Analyzer

---

### 2.7.2.1 Schedule Log Transmission

Log transmission from the Management Server to the Log Analyzer Server should be performed during the time frame when there are less users on the clients (CTs), such as midnight. Regular transmission can be performed if the task function of the OS is used.

#### 2.7.2.1.1 Set Log Obtaining Period on Management Server

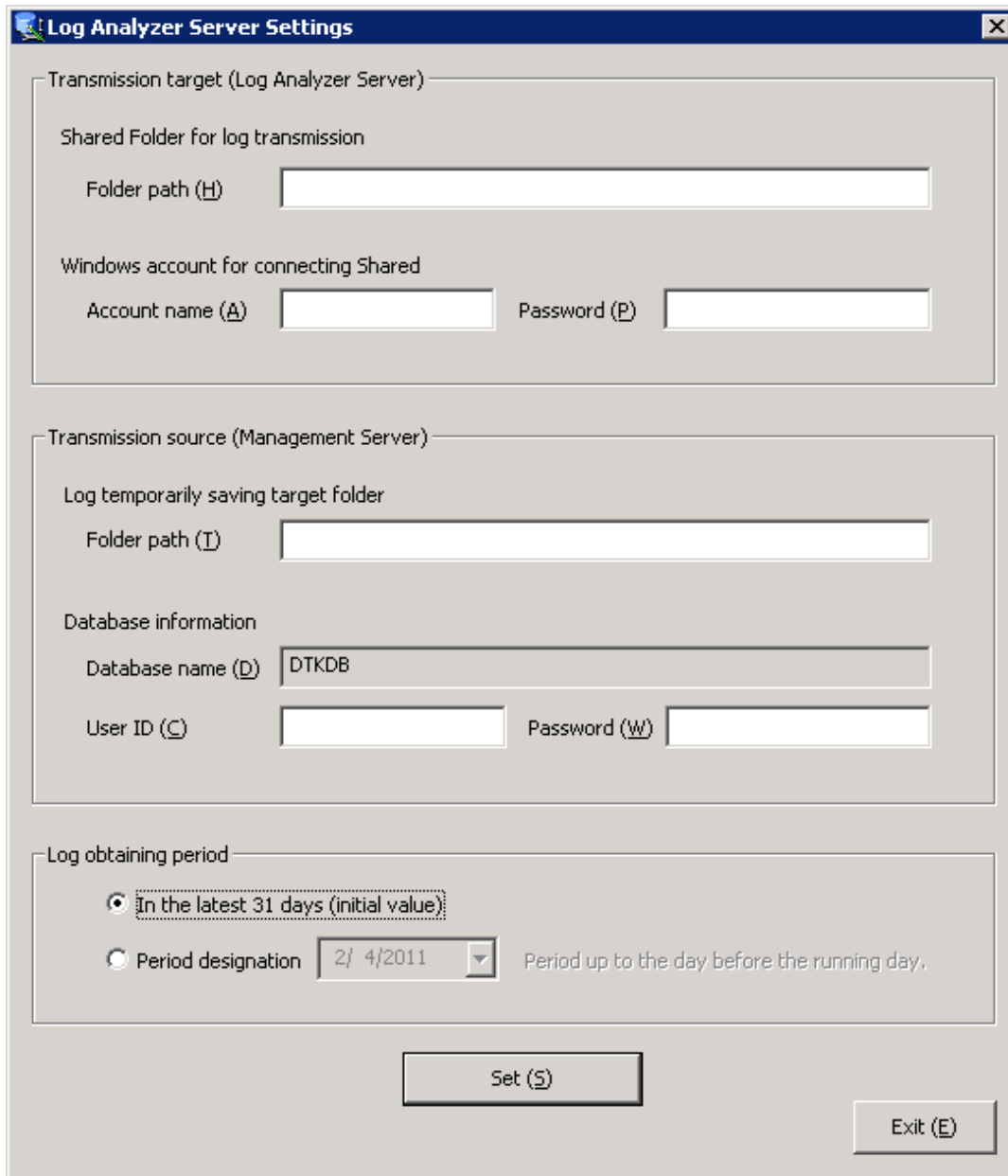
When transferring logs from the Management Server to the Log Analyzer Server, the following three items must be set:

- Transmission target (Log Analyzer Server)
- Transmission source (Management Server)
- Log obtaining period

When the transmission target and transmission source are being installed, set for transferring administrator information. For settings items, please refer to “Set Log Analyzer Server Environment on Management Server/Master Management Server” in “Systemwalker Desktop Keeper Installation Guide”.

The following describes how to set the log obtaining period.

1. Select [All Programs]-[Systemwalker Desktop Keeper]-[Server]-[Log Analyzer Settings] from the [Start] menu and start the [Log Analyzer Server Settings] window.



2. Set the start date for log obtaining in [Log obtaining period].

#### Relationship between configuration value of log obtaining period and transferred logs

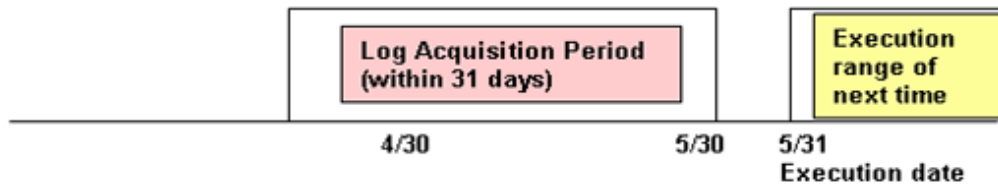
Log transmission considers logs of the days before the task operation day (the day of executing data transmission command) as its target. The log obtaining period, as the target date, is the date on which logs are registered to the Management Server, rather than the time when operation logs are generated in the client (CT).

The following describes the configuration value of the log obtaining period and the range of transferred logs:

- When the log obtaining period is [In the latest 31 days (initial value)]

Log data from the day 1 to 31 days before the execution day of transmission task (day of executing data transmission command) will be transferred.

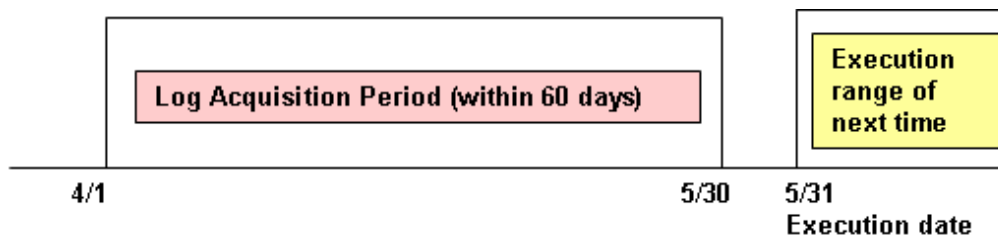
The following is the example of executing a task on May 31st.



- When the log obtaining period is [Period designation]

Transfer log data from the day before the execution date of task to the specified date in the log obtaining period.

The following is the example of specifying April 1st, 2007 in the log obtaining period and executing the task on May 31st.



The log obtaining period is to specify the start time of transferring logs on the Management Server/Master Management Server to the Log Analyzer Server. Therefore, there is no need to reset the log obtaining period after the application is started..

## 2.7.2.1.2 Set Transmission Schedule on Management Server

Transfer logs and user information from the Management Server to the Log Analyzer Server.

Register TRANS.bat (move data to Log Analyzer Server) command in the task function of the OS of the Management Server and set it to regular transmission. It is recommended to execute transmission processing everyday. The following example for settings describes the supposed daily transmission.

When transferring logs using TRANS.bat (transfer data to Log Analyzer Server) command, there must be no user accessing the shared folder.

When other users access the shared folder, the network must be disconnected or logoff is required.

It takes about 25 minutes for transferring about 5 million logs (but processing time is only for reference. It might change based on PC performance and network status).



### Note

#### Please perform data transmission when there are less users of the client (CT)

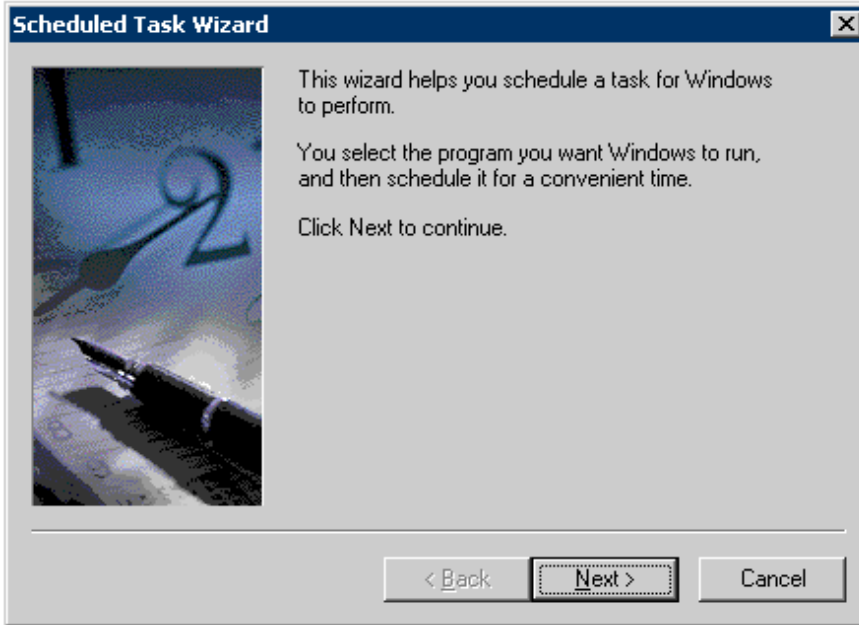
When TRANS.bat is executed, the following services of the Management Server will be stopped during the period of saving and sending log data. Therefore, please perform data transmission when there are less users of the client (CT).

- SWLevelControlService
- SWServerService
- In addition, after starting SWServerService or during date change (12am), confirmation of available database capacity will be performed. In the 15 minutes till the confirmation operation has completed, service may not be able to be stopped.
- Therefore, please do not transfer at the above time frame.

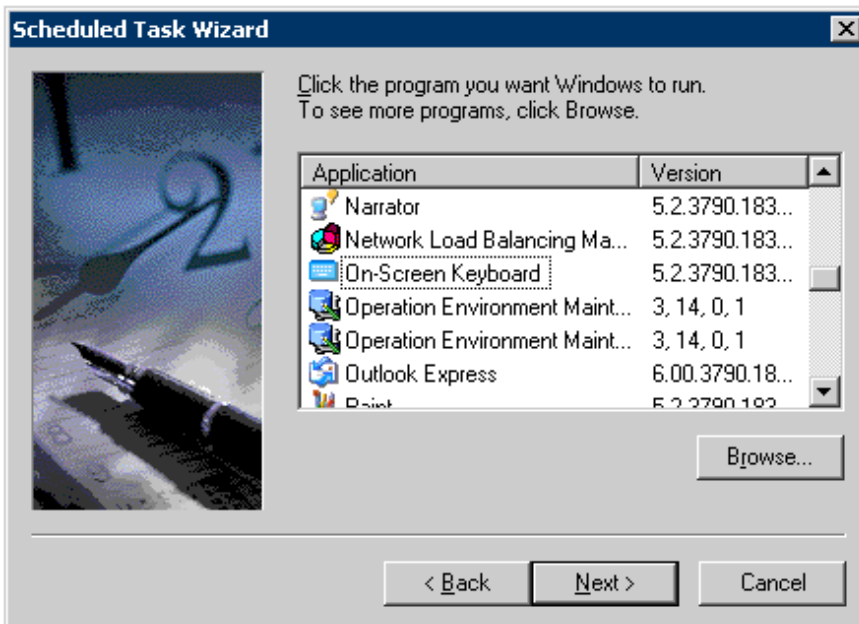
The following describes the settings procedures.

### Registration method in editions excluding Windows Server® 2008

1. Select [Settings]-[Control Panel]-[Scheduled Tasks] from the [Start] menu and double-click [Add Scheduled Task].  
→ The following window is displayed. Please click the [Next] button.



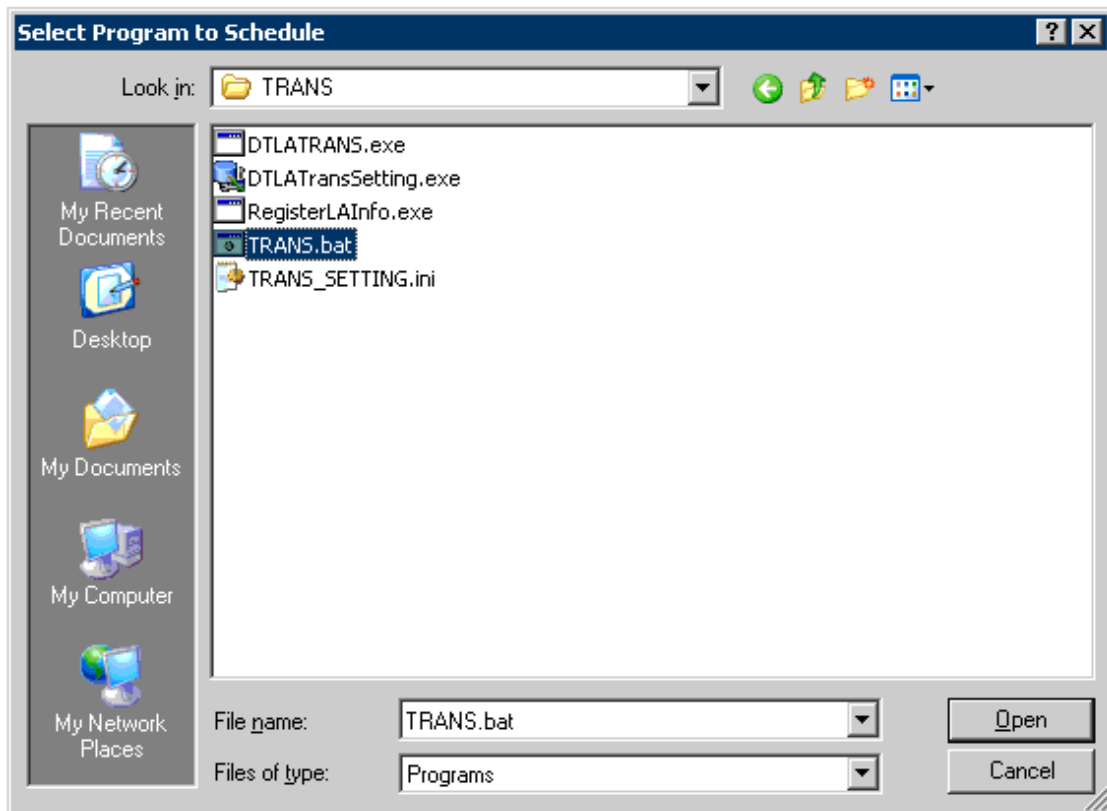
2. Click the [Browse] button in the running programs selection window of the task wizard.



3. Select batch command “TRANS.bat” saved in the following location.

```
[Installation Folder of Systemwalker Desktop Keeper]\LogAnalyzer\TRANS\TRANS.bat
```

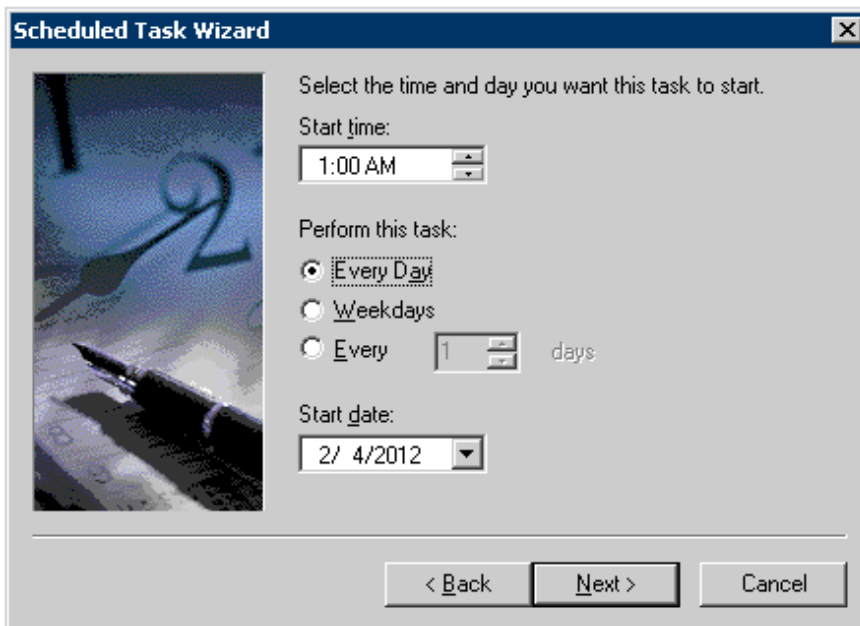




4. Enter the task name and select [Daily] in the execution of task.



5. Set the start time, execution interval and start date of task. The start time is specified to the time frame in which there are less users of the client (CT) such as midnight, etc. Select [Every Day] as the execution interval.



**Scheduled Task Wizard**

Select the time and day you want this task to start.

Start time: 1:00 AM

Perform this task:

Every Day

Weekdays

Every 1 days

Start date: 2/ 4/2012

< Back Next > Cancel

6. Register the user ID and password during the execution.  
Please specify a user name and password that has Administrator authority.



**Scheduled Task Wizard**

Enter the name and password of a user. The task will run as if it were started by that user.

Enter the user name: ADMIN\Administrator

Enter the password: .....

Confirm password: .....

If a password is not entered, scheduled tasks might not run.

< Back Next > Cancel

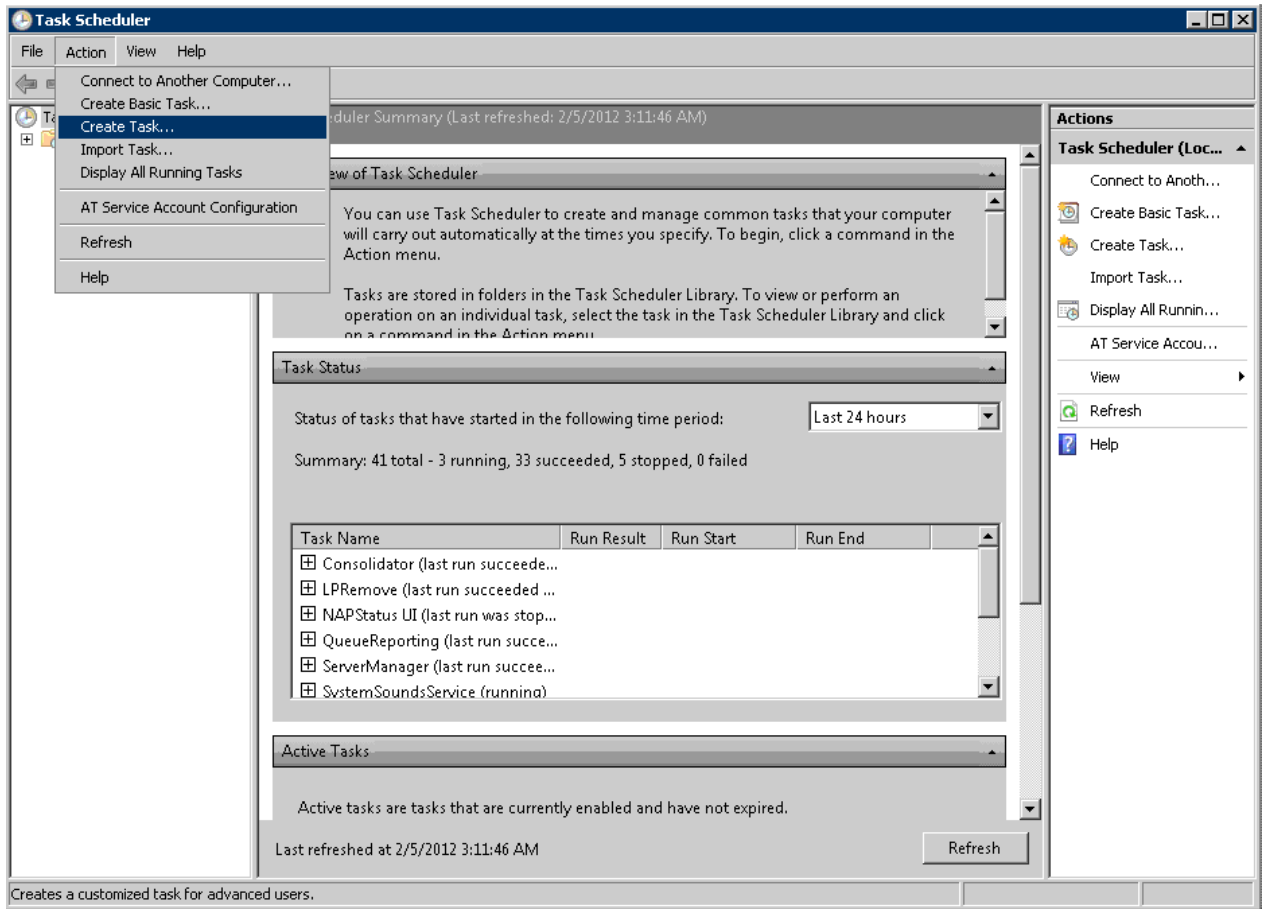
7. Click the [Finish] button.



### Registration method in Windows Server® 2008

1. Select [All Programs]-[Accessories]-[System Tools]-[Task Scheduler] from the [Start] menu.  
→ The [Task Scheduler] window is displayed.

2. Select [Create Task] from the [Action] menu.



→ The [Create Task] window is displayed.

**Create Task**

General | Triggers | Actions | Conditions | Settings

Name: datatransfer

Author: WIN-CNO5W8OSTDK\Administrator

Description:

Security options

When running the task, use the following user account:  
WIN-CNO5W8OSTDK\Administrator

Change User or Group...

Run only when user is logged on

Run whether user is logged on or not

Do not store password. The task will only have access to local computer resources.

Run with highest privileges

Hidden

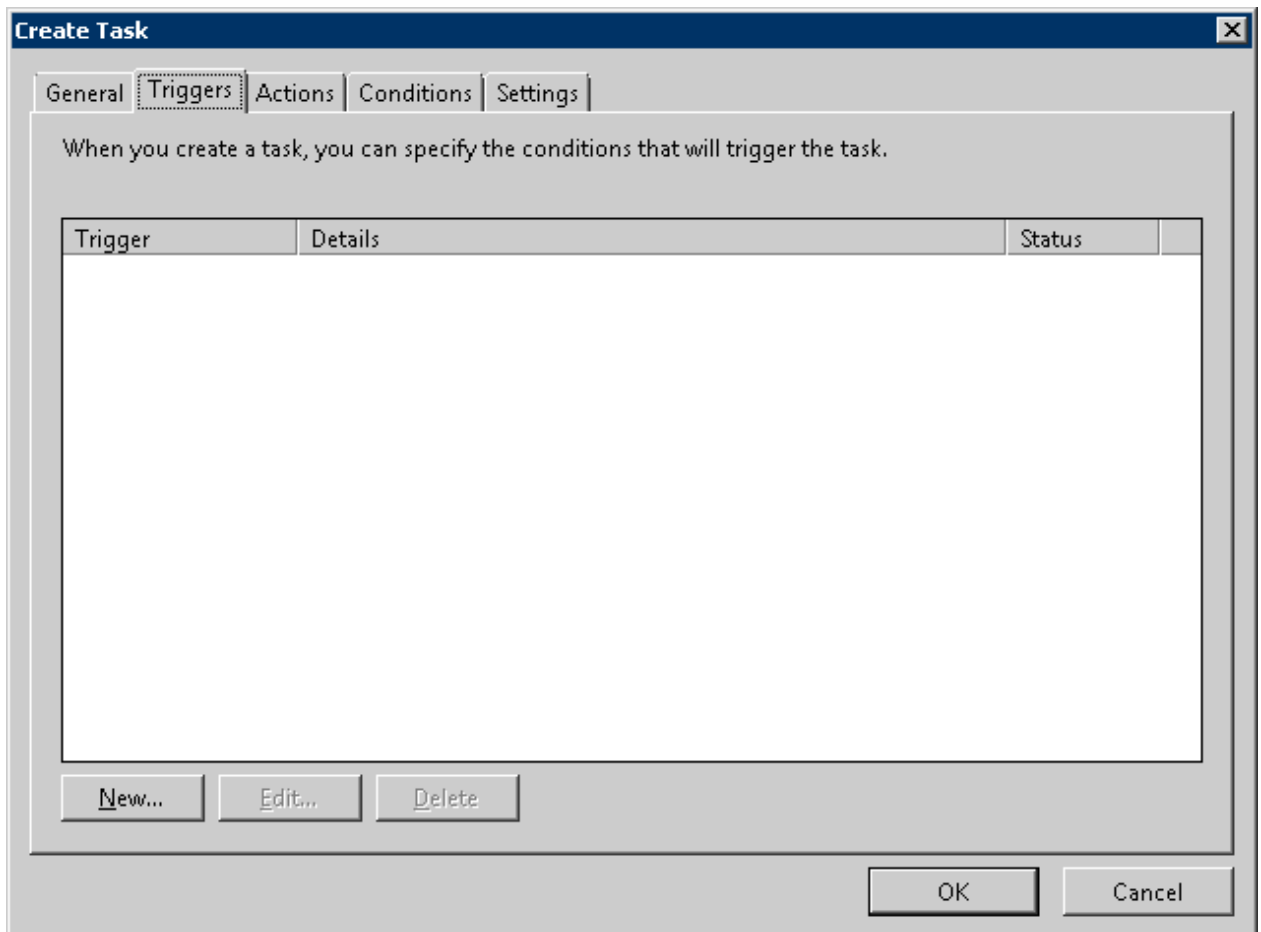
Configure for: Windows Vista™ or Windows Server™ 2008

OK Cancel

3. Select the [General] tab, set the following information and click the [OK] button.

- Set the registered task name in [Name].
- Set a user that has Administrator authority in [When Running the Task ,Use the Following User Account]. Click the [Change User or Group] button to set.
- Select [Run Whether User is Logged on or Not].
- Select [Run with Highest Privileges].

4. Select the [Triggers] tab and click the [New] button.



→ The [New Trigger] window is displayed.

**New Trigger**

Begin the task: On a schedule

**Settings**

One time

Daily

Weekly

Monthly

Start: 8/ 6/2009 1:00:00 AM  Synchronize across time zones

Recur every: 1 days

**Advanced settings**

Delay task for up to (random delay): 1 hour

Repeat task every: 1 hour for a duration of: 1 day

Stop all running tasks at end of repetition duration

Stop task if it runs longer than: 3 days

Expire: 2/ 5/2013 8:27:03 AM  Synchronize across time zones

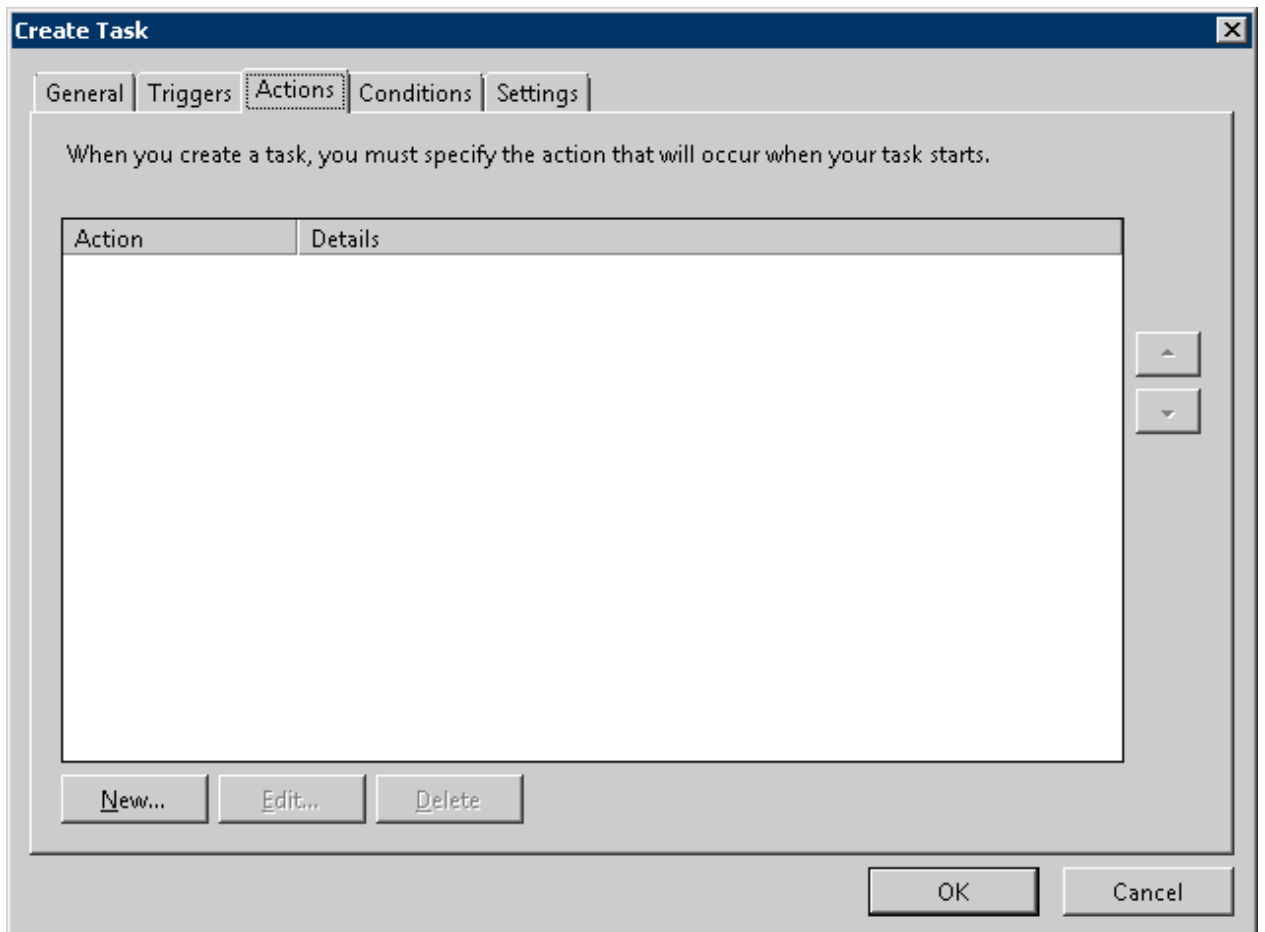
Enabled

OK Cancel

5. Set the following information in [Settings] and click the [OK] button:

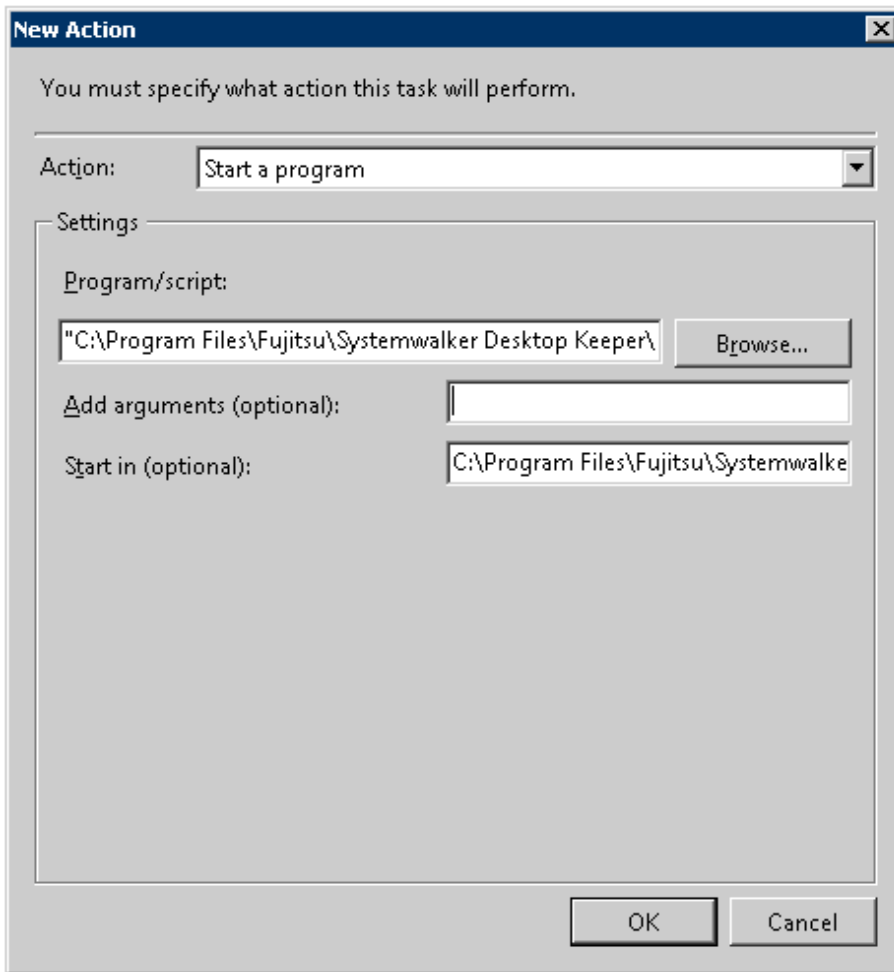
- Select [Daily].
- Set the start date and time in [Start]. The start time is specified to be a time frame in which there are less users of the client (CT) such as midnight, etc.
- Set 1 day in [Recur every].

6. Select the [Actions] tab and click the [New] button.





→ The [New Action] window is displayed.



7. Set the following information in [Settings] and click the [OK] button.

- [Program/Script]: Specify the batch command “TRANS.bat” saved in the following location with full path. Enclose the path with double quotes.

```
"[Installation Folder of Systemwalker Desktop Keeper]\LogAnalyzer\TRANS\TRANS.bat"
```

- [Start in (optional)]: Specify the full path of the folder in which the “TRANS.bat” specified in [Program/Script] is located. Do not enclose the path with double quotes.

8. Click the [OK] button in the [Create Task] window.

## Information

### Log transmission can also be performed manually

1. Execute the following command in the command prompt to enter the "TRANS" folder in which the product has been installed.

```
cd [Installation Folder of Systemwalker Desktop Keeper]\LogAnalyzer\TRANS [Enter]
```

2. Execute the following batch command, save the log data transferred to the Log Analyzer Server as a CSV file and send it.

```
TRANS.bat [Enter]
```

After executing in the command prompt, the command prompt window will be closed automatically when the processing finishes. Please execute the following command when it is expected to keep the command prompt window.

```
cmd /c TRANS.bat [Enter]
```

### 2.7.2.1.3 Save Logs to the Database of Log Analyzer Server

Save logs and user information from the Management Server to the database of the Log Analyzer Server.

At this time, when registering DTTOOLEX.EXE (move data to the Log Analyzer Server or delete from it) command in the task function of OS of the Log Analyzer Server, it can be set to save to the database regularly. It is recommended to save logs to the database everyday. The following example for settings describes the supposed daily saving.

After executing the DTTOOLEX.EXE command, logs moved in will be aggregated while the log data is being moved in, and the aggregation result will be updated.

At this time, the difference between the aggregation result before and after the execution of DTTOOLEX.EXE will be output as logs.

- [Output Target of Logs]

[Installation Folder of Log Analyzer Server]\bin\batchnavi\update0.log

When the folder size is larger than 10MB, update0.log will change to update1.log, and update0.log will be generated (up to update4.log can be generated at most in sequence). The latest information is always recorded in update0.log.

- [Output Content of Logs]

-----  
The updated information of counting implementation date 2008/04/21 01:00:00 is output

Start

20080421 operation happening day 20080408 information disclosure (0, 0, 0, 0, 0) terminal use (0, 0, 20) violation operation (0, 0, 0, 0, 0) printing volume auditing (0)

20080421 operation happening day 20080409 information disclosure (0, 0, 0, 0, 0) terminal use (0, 0, 31) violation operation (1, 0, 1, 0, 0) printing volume auditing (2)

End  
-----

The above is the aggregation result of data moved in on April 21st, 2008, indicating the number of the updated operation logs on April 8 and 9, and the different number being updated is displayed in ().

The number in () is the different number of each of the following logs (\*).

- Information disclosure (file export, file operation, times of printing operation, number of pages of printing operation and E-mail sending by recipient address)
- Terminal usage (window title obtaining with URL, E-mail sending by recipient address and application startup)
- Violation operation (application startup prohibition, printing prohibition, logon prohibition, PrintScreen key prohibition and E-mail attachment prohibition)
- Printing volume auditing (times of printing operation)

\*) logs displayed in the report output by the Report Output Tool (Only information disclosure is also displayed in the information disclosure prevention diagnosis window of the Web Console.)

It will take about 80 minutes to move about 10 million logs (but the processing time is only for reference. It might change because of CPU, memory, disk performance, operation status of other applications, etc., of the PC).



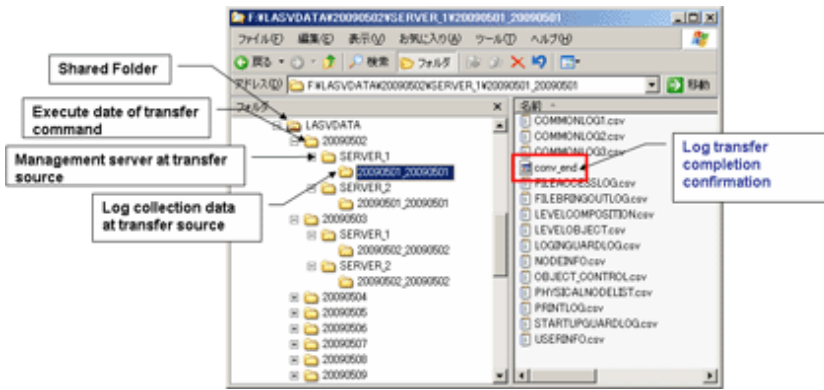
#### Note

**To ensure disk capacity, please save the CSV files of log data that are not needed to external media regularly**

As for the CSV files of log data transferred from the Management Server to the Log Analyzer Server, even if they are saved to the database on the Log Analyzer Server, they will still remain on the disk of the Log Analyzer Server.

When the capacity of the Shared Folder is exhausted, logs cannot be transferred from the Management Server/Master Management Server. Therefore, please confirm the capacity of the shared folder and delete the analyzed and aggregated logs after saving them.

The structure of shared folder of the Log Analyzer Server is shown as follows.



Logs that have not finished analyzing and aggregating on the Log Analyzer Server cannot be saved or deleted.

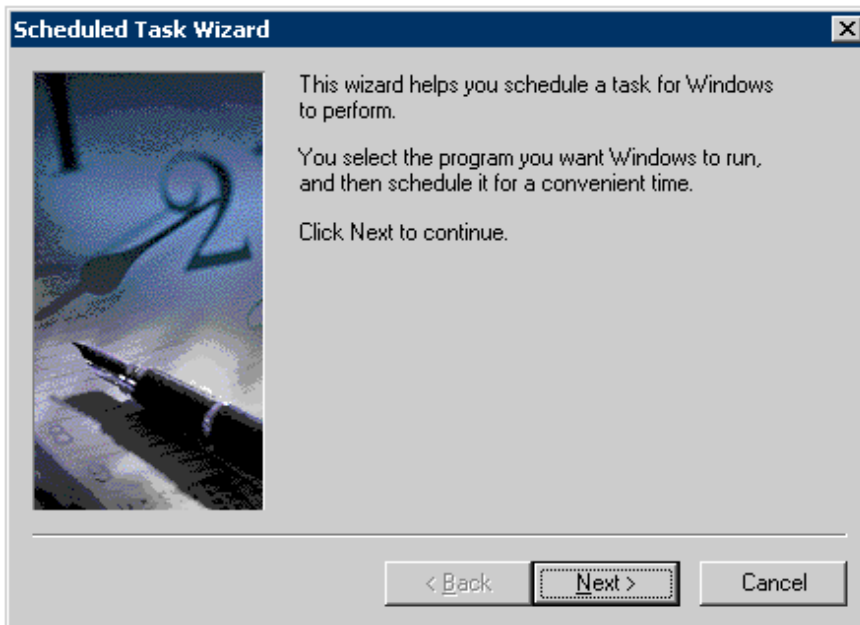
Under the folder of the transmission source log collection day, the created folder of “File for confirming the completion of log transmission (conv\_end)” has finished log analyzing and aggregating, and has been saved to the database on the Log Analyzer Server.

When “File for confirming the completion of log transmission (conv\_end)” has been created in all “Folder of transmission source log collection day” in the “Transmission source Management Server name” folder under the “Transmission command execution day” folder in the above image, saving and deletion can be performed. Please save and delete logs according to the “Transmission command execution day” folder unit.

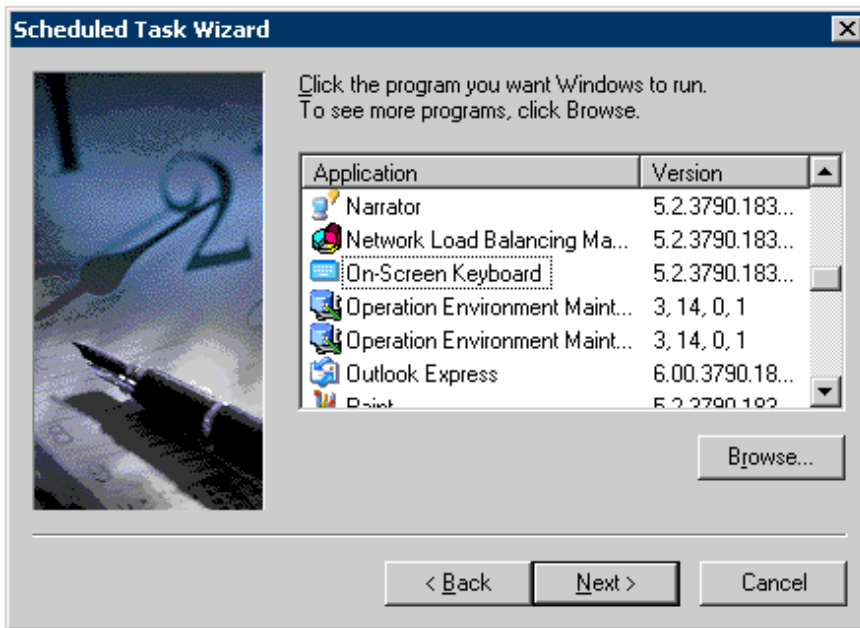
The following describes the settings procedure.

### Registration method in editions excluding Windows Server® 2008

1. Open [Start]-[Settings]-[Control Panel]-[Scheduled Task] and double-click [Add Scheduled task].  
→ The following window is displayed. Click the [Next] button.

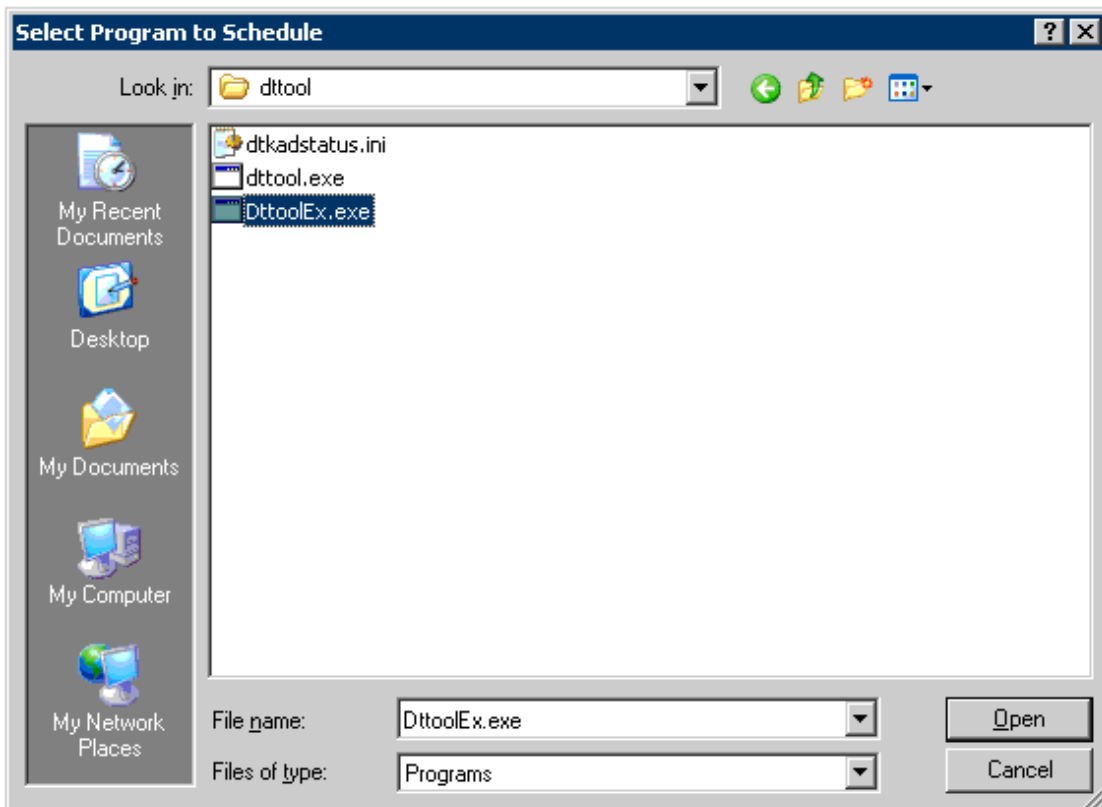


2. Click the [Browse] button in the running program selection window of the task wizard.



3. Select the “DTTOOLEX.EXE” command saved in the following location.

[Installation Folder of Log Analyzer Server]\bin\dttool\DttoolEx.exe



4. Enter the task name and select [Daily] in the execution of the task.



5. Set the start time, perform this task and start date of task. Set the start time to one later than the start time of the task of the data transmission command. Execute the task after the execution of data transmission command has finished. Select [Every Day] as the perform this task.



6. Register the user name and password during the execution.  
Please specify the user name and password of the Log Analyzer Server.



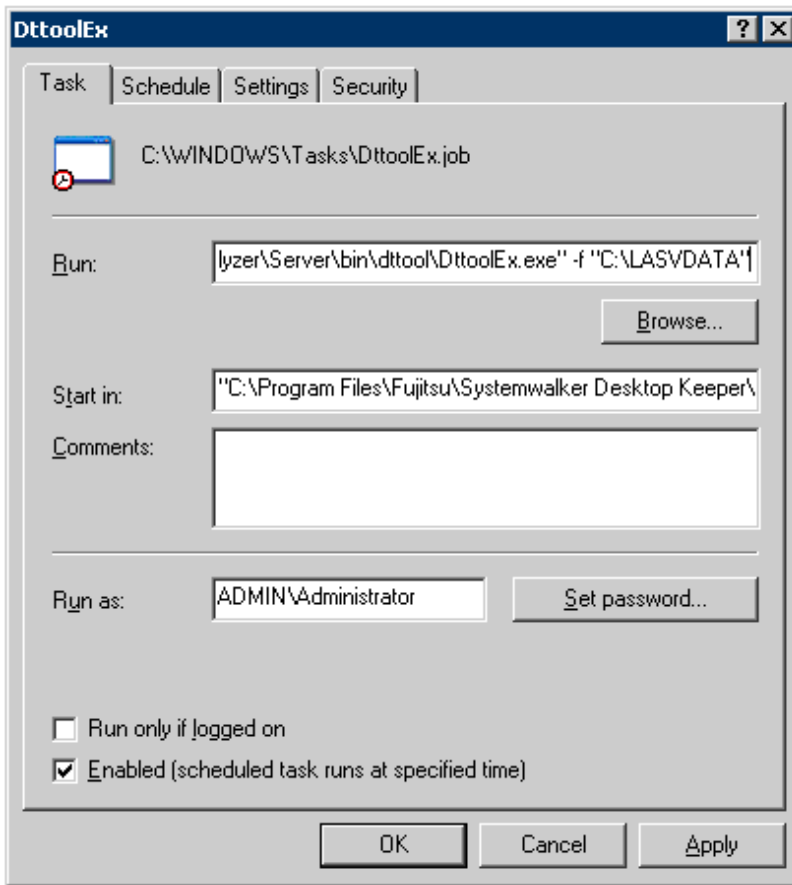
7. Select [Open advanced properties for this task when I click Finish]] and then click the [Finish] button.



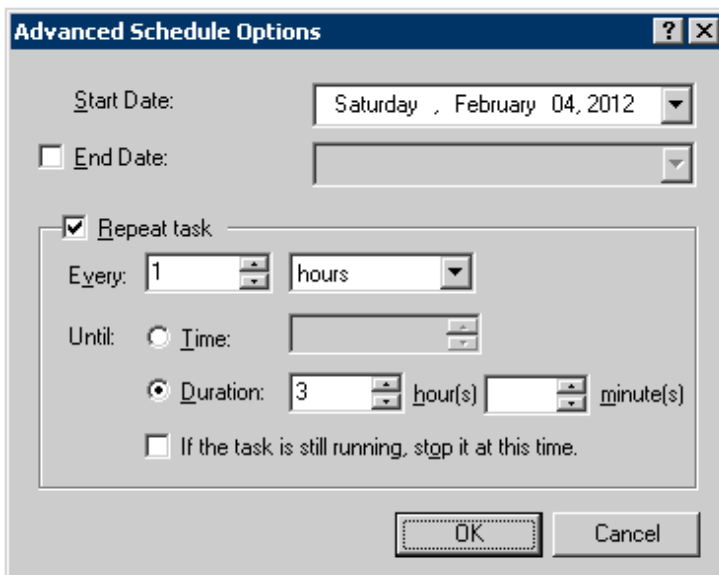
8. Specify the following options after the path set in [Run] in the [Task] tab.

```
-f [Path of shared folder of log transmitting target]
```

\*[Path of shared folder of log transmitting target] is specified with the format of the local path instead of theUNC. Please make sure to enclose it with double quotes.

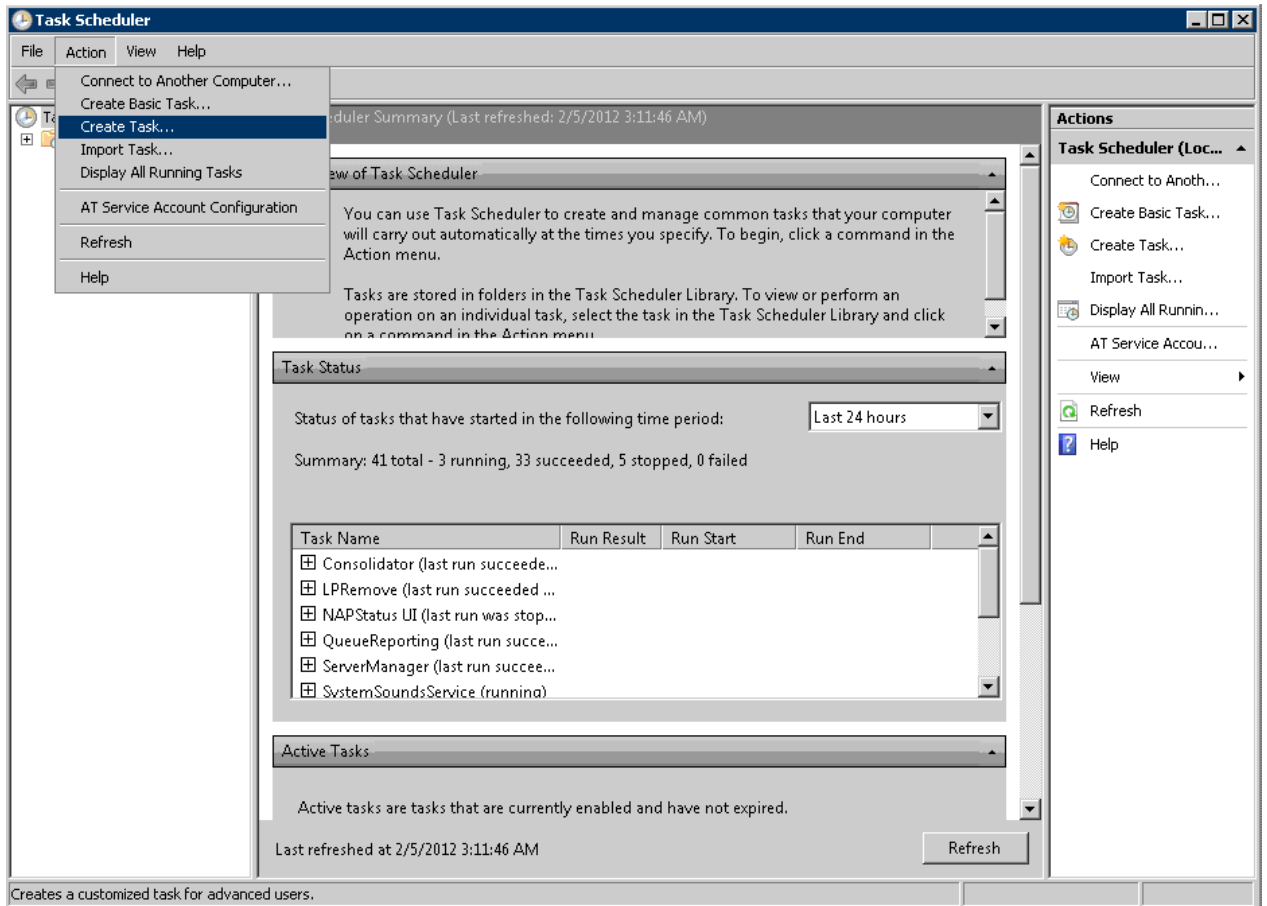


9. Click the [Schedule] tab, and then click the [Advanced] button.
10. Select [Repeat Task] and set [Every] and [Duration].



## Registration method in Windows Server® 2008

1. Select [All Programs]-[Accessories]-[System Tools]-[Task Scheduler].  
→ The [Task Scheduler] window is displayed.
2. Select [Create Task] from the [Action] menu.





→ The [Create Task] window is displayed.

**Create Task**

General | Triggers | Actions | Conditions | Settings

Name: datainput

Author: WIN-CNO5W8OSTDK\Administrator

Description:

Security options

When running the task, use the following user account:  
WIN-CNO5W8OSTDK\Administrator

Change User or Group...

Run only when user is logged on

Run whether user is logged on or not

Do not store password. The task will only have access to local computer resources.

Run with highest privileges

Hidden

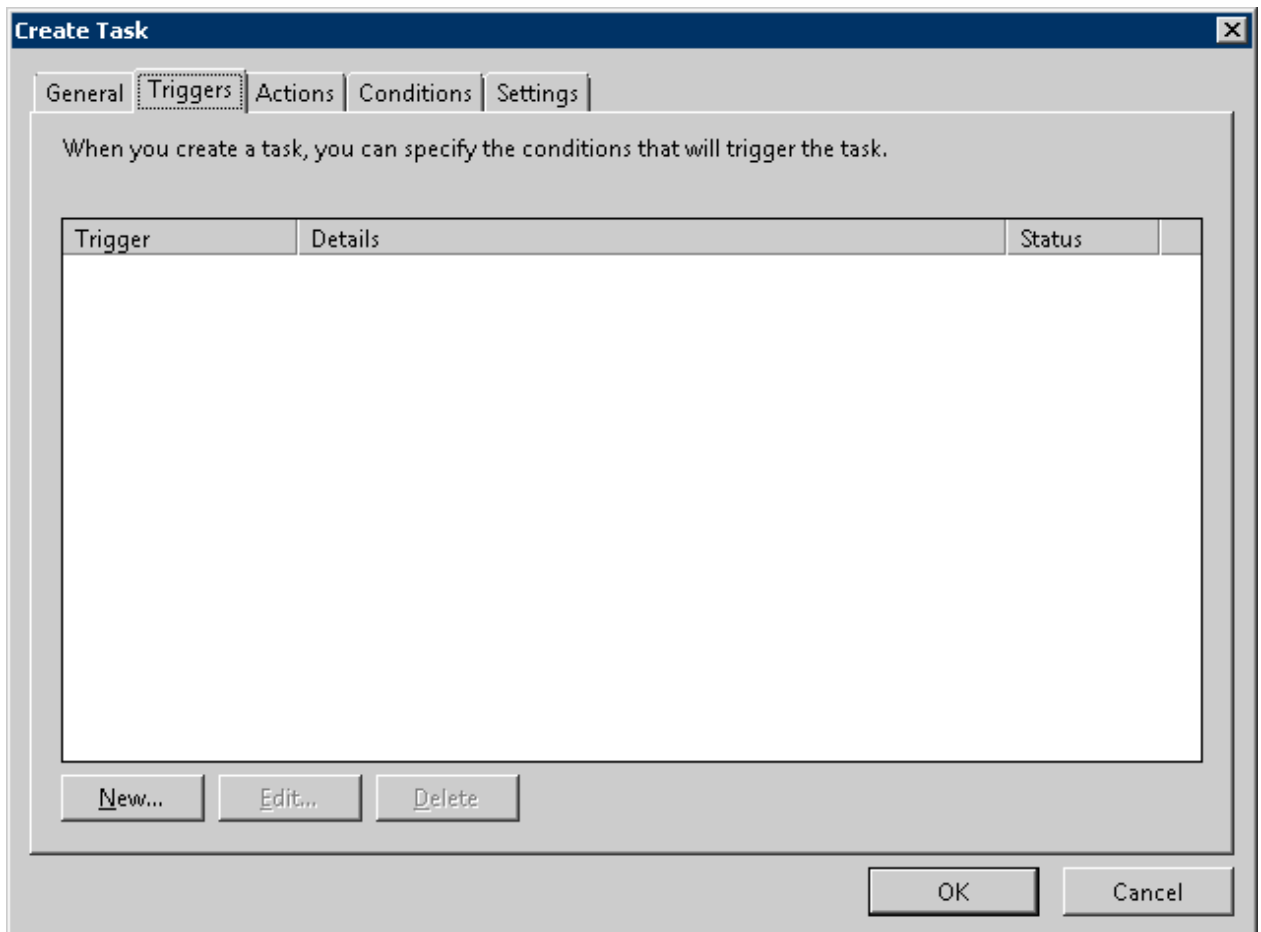
Configure for: Windows Vista™ or Windows Server™ 2008

OK Cancel

3. Select the [General] tab, set the following information and click the [OK] button.

- Set the registered task name in [Name].
- Set the user of Log Analyzer in [When Running the Task ,Use the Following User Account]. Click the [Change User or Group] button to set.
- Select [Run Whether User is Logged on or Not].
- Select [Run with Highest Privileges].

4. Select the [Triggers] tab and click the [New] button.



→ The [New Trigger] window is displayed.

**New Trigger**

Begin the task: On a schedule

Settings

One time

Daily

Weekly

Monthly

Start: 8/ 6/2009 1:00:00 AM  Synchronize across time zones

Repeat every: 1 days

Advanced settings

Delay task for up to (random delay): 1 hour

Repeat task every: 30 minutes for a duration of: 1 hour

Stop all running tasks at end of repetition duration

Stop task if it runs longer than: 3 days

Expire: 2/ 5/2013 8:27:03 AM  Synchronize across time zones

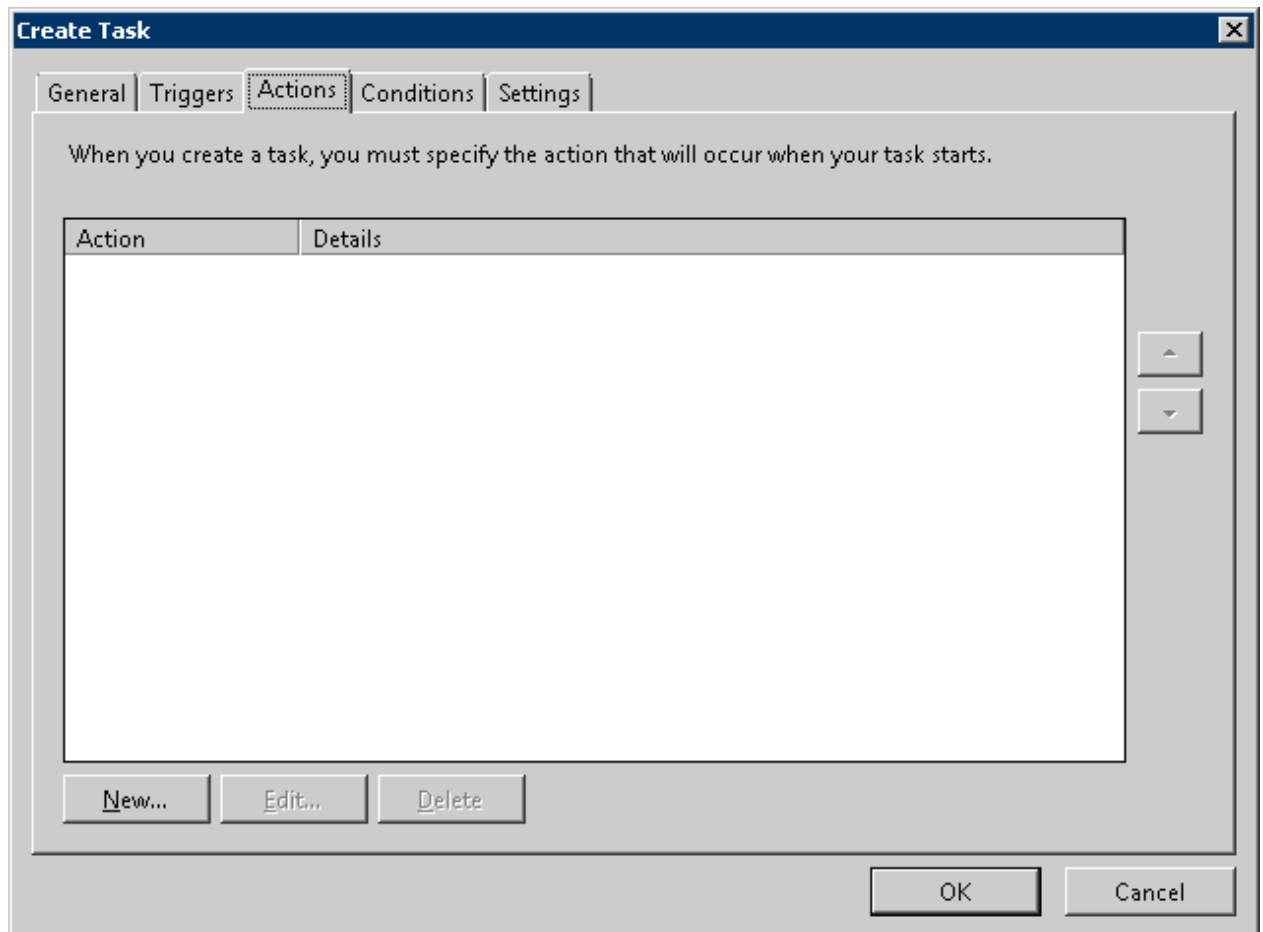
Enabled

OK Cancel

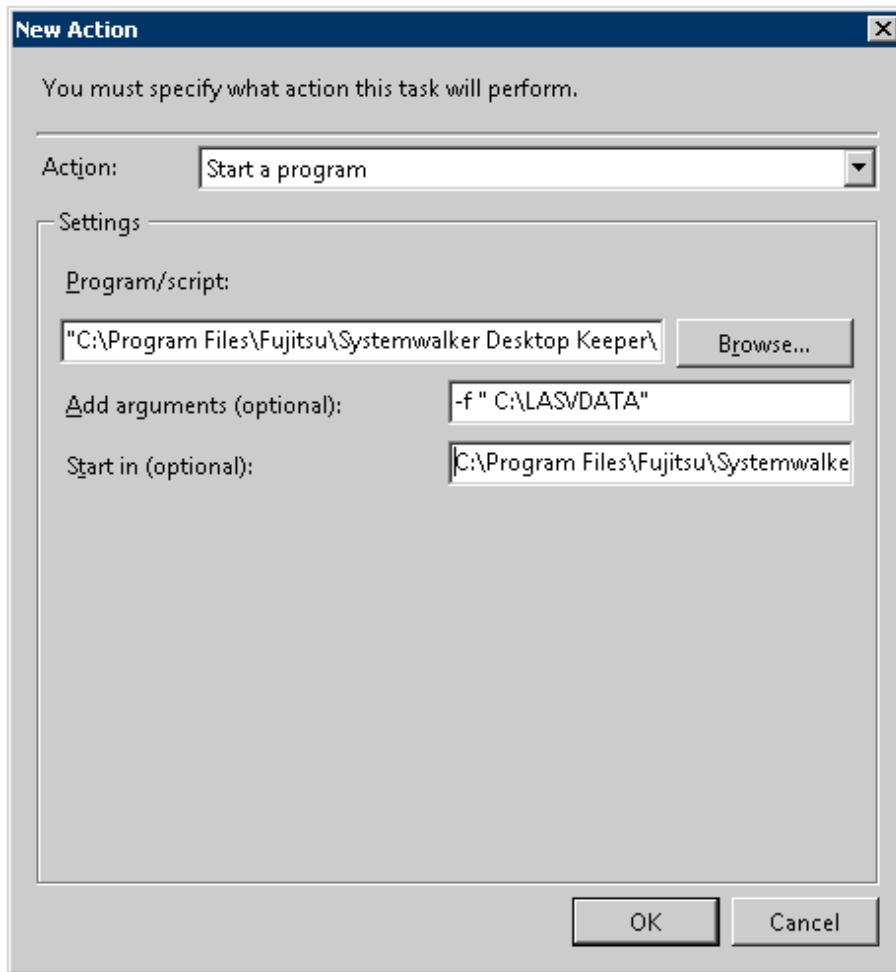
5. Set the following information in [Settings] and click the [OK] button.

- Select [Daily].
- Set the date and time in [Start]. Set the start time to the one later than the start time of the task of the data transmission command and execute the task after the execution of the data transmission command has finished.
- Select [Repeat task every] and set [Interval] and [for a duration of].

6. Select the [Actions] tab and click the [New] button.



→ The [New Action] window is displayed.



7. Set the following information in [Settings] and click the [OK] button.

- [Program/Script]: Specify the “DttoolEx.exe” command saved in the following location with a full path. The path is enclosed with double quotes.

```
[Installation Folder of Log Analyzer Server]\bin\dttool\DttoolEx.exe
```

- [Add arguments(optional)]: Set “-f [Path of Shared folder of log transmission target]”. Specify [Path of shared folder of log transmission target] with the format of the local path instead of UNC. Please make sure to enclose it with double quotes.
- [Start in (optional)]: Specify the full path of the folder in which “DttoolEx.exe” specified in [Program/Script] is located. Do not enclose the path with double quotes.

8. Click the [OK] button in the [Create Task] window.

## Information

### Logs can also be saved to database manually

1. Execute the following command in the command prompt of the Log Analyzer Server to access to the folder for saving tools in the installation folder of the Log Analyzer Server.

```
cd [Installation Folder of Log Analyzer Server]\bin\dttool [Enter]
```

2. Execute the following command to add data to the database of the Log Analyzer Server.

```
DttoolEx.exe -f [Path of shared folder of log transmitting target] [Enter]
```

## 2.7.2.2 Set Conditions for Aggregation /Report Output

Start Log Analyzer Server and set the conditions for aggregation and report output.

As conditions can be set according to the operating environment of PC and business status, the aggregation result can be acquired by functions.

### Start Log Analyzer Server

1. Start the main menu with any of the following methods.



#### About Web Server connecting to Log Analyzer (Web Console)

When starting Log Analyzer, only one Web Server can be connected. In a 3-level structure, though the Log Viewer window can also be displayed even if the Management Server is connected, the Log Analyzer window cannot be displayed.

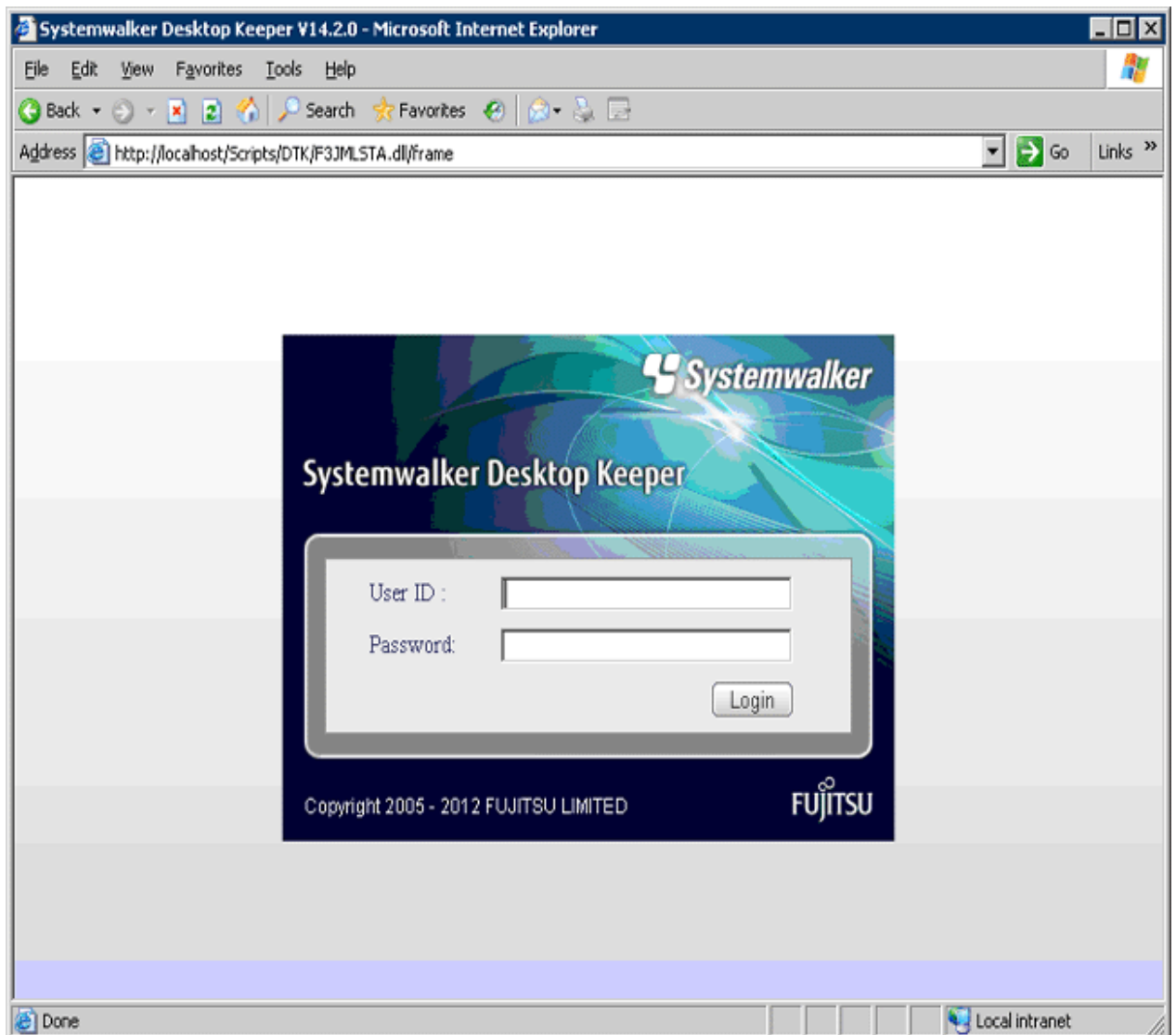
**In a 2-level system structure:** Please connect to the Management Server.

- Select [All Programs]-[Systemwalker Desktop Keeper]-[Server]-[Desktop Keeper Main menu] from the [Start] menu of the Management Server.
- Specify “http://host name or IP address of Management Server/DTK/index.html” in the address bar of the Browser.  
When the port number of IIS is changed, specify as follows:  
http://IP address: port number/DTK/index.html

**In a 3-level system structure:** Please connect to the Master Management Server.

- Select [All Programs]-[Systemwalker Desktop Keeper]-[Server]-[Desktop Keeper Main menu] from the [Start] menu of the Master Management Server.
- Specify “http://host name or IP address of Master Management Server/DTK/index.html” in the address bar of the Browser.  
When the port number of IIS is changed, specify as follows:  
http://IP address: port number/DTK/index.html

→ The [Login] window is displayed.



2. Enter the following information and click the [Login] button.

The following information is [User ID] and [Password] set using the Server Settings Tool.

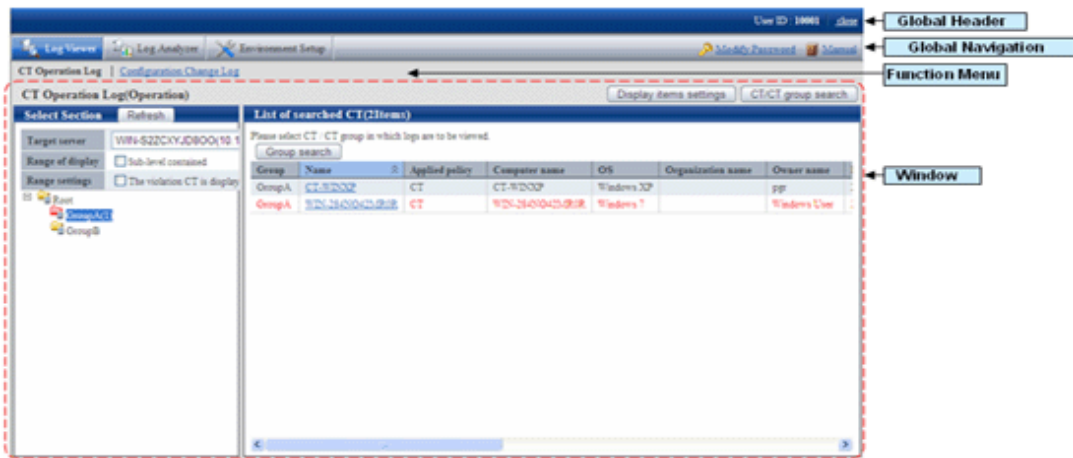
When using Log Analyzer, the system administrator with “Log Viewer” authority must be specified.

- [User ID]
- [Password]

It is recommended that the password be changed regularly. For details on how to do so, please refer to “[Change password](#)”.

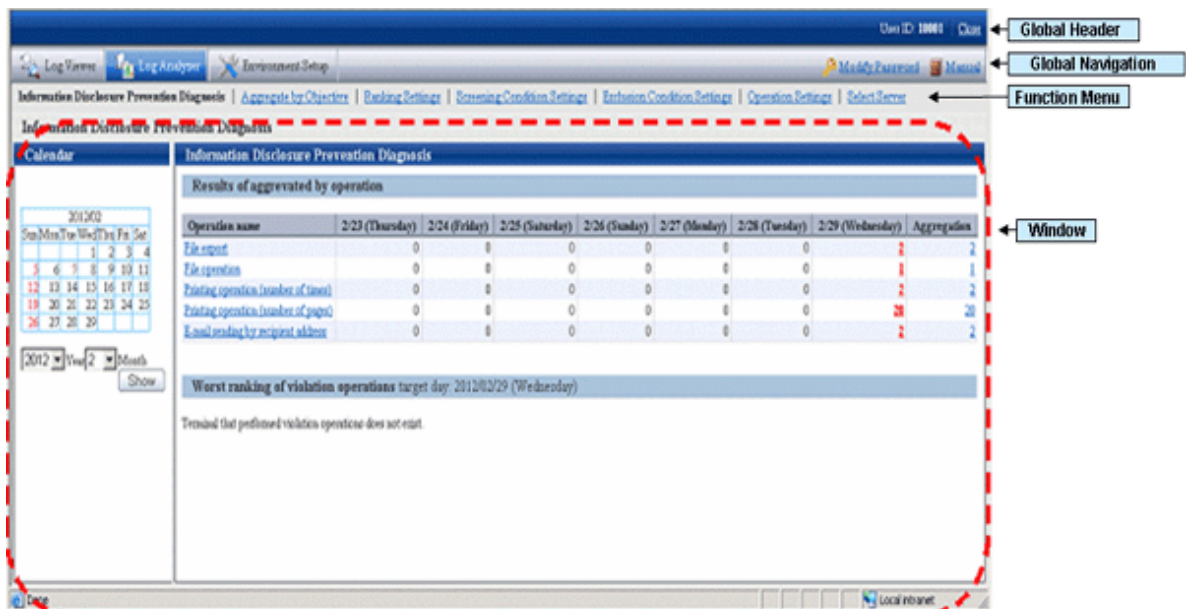
3. Click [Log Management] of Global Navigation in the displayed status window.

→ Start Log Viewer and the [CT Operation Log] window is displayed.



4. Click [Log Analyzer] of Global Navigation.

→ The [Information Disclosure Prevention Diagnosis] window is displayed.



Displayed content of window

#### Global Header

- User ID: The login user ID is displayed.
- Logout: To log off.

#### Global Navigation

- Log Viewer: The Log Viewer window is displayed.
- Log Analyzer: The Log Analyzer window is displayed.
- Modify password: Used to Modify password when starting the Web window. For details on how to do so, please refer to “[Change password](#)”
- Manual: The manual is displayed.

#### Function menu



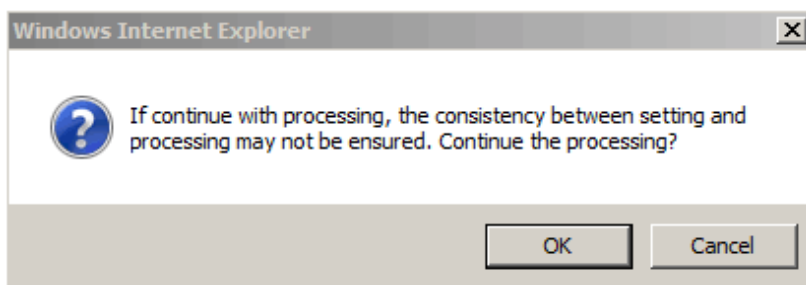
- Information disclosure prevention diagnosis: The [Information Disclosure Prevention Diagnosis] window is displayed.
- Aggregate by objective: Display the aggregate by objective window.
- Ranking settings: Set “Display/Hide” and the displayed number of various rankings by group, user and terminal+user.
- Screening condition settings: Set keywords, domains, URLs or applications during log aggregation as screening conditions.
- Exclusion condition settings: Set terminal as non-aggregation target during log aggregation.
- Operation settings: Set ranking display of information disclosure prevention diagnosis and set the day of a week to start weekly report and eco auditing in the report output.
- Select server: Display the select server window. Click to change the currently selected Log Analyzer Server.  
This window will be automatically displayed when the following conditions are satisfied.
  - When there are multiple Log Analyzer Servers in the system structure
  - When login through the main menu and Log Analyzer is used for the first time

### Note

**Please make sure to use [Logout] to close the settings window**

When the screening condition settings window, the exclusion condition settings window and operation settings window are used. If closing them through “×” of the Brower, the following message will appear even if there is no other user of these windows. At this time, the new user cannot use the settings window without receiving a warning message until 24 hours later (Selecting “No” will shift it to the information disclosure prevention diagnosis window).

Please make sure to use [Logout] when closing the settings windows.



### 2.7.2.2.1 Set Ranking Display Number

Set the displayed number of tge ranking number. The settings of the ranking display number will be displayed immediately after being modified.

### Note

**Please do not modify the conditions when moving logs or using Log Analyzer function or Report Output Tool**

This may cause conflicts and errors in the aggregation result and diagnosis result or in the report output result.

1. Select [Ranking Settings] of the function menu.  
→ The following window is displayed.

Items to be set		
Ranking by Group	<input checked="" type="radio"/> Display <input type="radio"/> Not Display	Ranking Display Number <input type="text" value="5"/>
Ranking by Terminal	<input checked="" type="radio"/> Display <input type="radio"/> Not Display	Ranking Display Number <input type="text" value="5"/>
Ranking by User	<input checked="" type="radio"/> Display <input type="radio"/> Not Display	Ranking Display Number <input type="text" value="5"/>
Ranking by User + Terminal	<input checked="" type="radio"/> Display <input type="radio"/> Not Display	Ranking Display Number <input type="text" value="5"/>

2. Set each ranking as follows:

- Settings of [Display]/[Not Display]

[Display] (initial value): The ranking is displayed.

[Not Display]: The ranking is not displayed.

- Settings of [Ranking Display Number]

Set the displayed ranking number to within 1-99. The initial value is "5".

If the same sequence exists, a maximum of 99 lines can be displayed for ranking.

3. Click the [Apply] button.

→ The [Information Disclosure Prevention Diagnosis] window with an updated configuration value is displayed again and a message indicating the completion of settings appears.

## 2.7.2.2.2 Set Screening Condition

In order to easily detect dangerous operations such as access to important files, E-mail sending to unauthorized domains and ever increasing logs, screening conditions during aggregation can be set.

Due to reasons such as adding, modifying or deleting settings, the time for screening conditions to be updated to aggregation information may be inconsistent.

When performing log transmission as follows:

- Transferring logs on March 1
- Transferring logs on March 2
- Transferring logs on March 3,

if screening condition settings have been set after log transmission on March 2, the screening conditions will be applied and aggregation will be performed after the aggregation during log transmission on March 3. (For logs before March 2, the screening conditions cannot be applied as the conditions have not been set at that time)

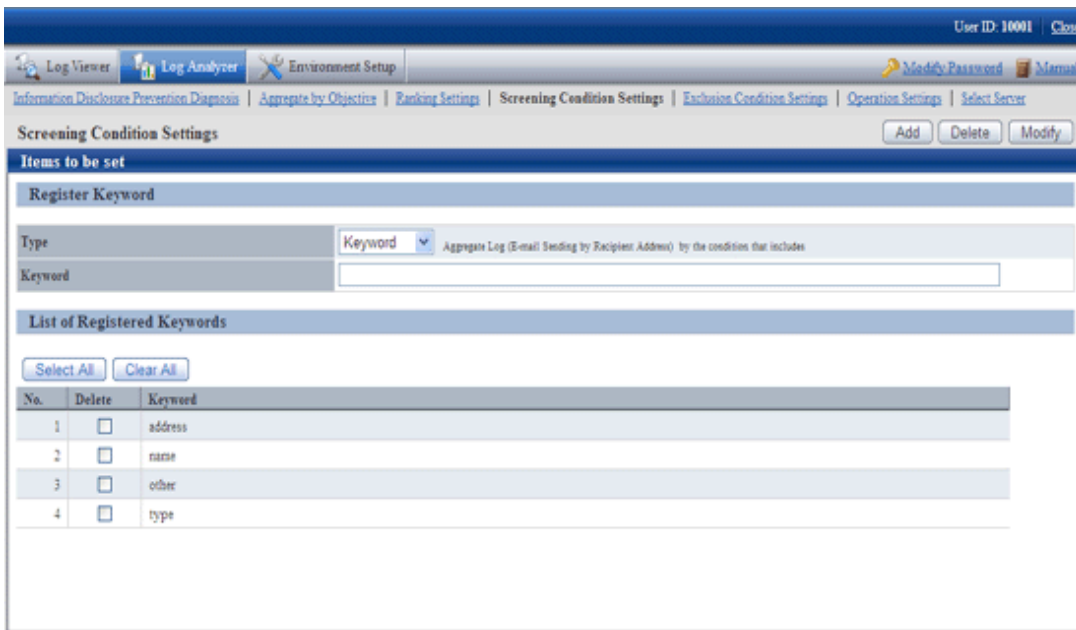
In order to apply the screening condition settings and aggregate before March 2, aggregation should not be performed again after the re-aggregation option of "DTTOOLEX.EXE (data transmission or deletion for the Log Analyzer Server)" has been executed.


## Note

**Please do not modify the conditions when moving logs or using when Log Analyzer function or Report Output Tool**

This may cause conflicts and errors in the aggregation result and diagnosis result or in the report output result.

1. Select [Screening Condition Settings] of the function menu.  
→ The following window is displayed.



Item Name	Description
[Register Keyword]	
[Type]	Set the type of screening condition.
[Keyword]	Specify the keywords for judging aggregation target log. According to the conditions selected in [Type], labels displayed on the left of the input field may be different.   <b>Note</b> After the setting, it is likely that multi-byte characters cannot be input in the keyword field. At this time, click the input field to enable the input of multi-byte characters.
[List of Registered Keywords]	The list of registered keywords is displayed.
[Select All]	Select all keywords in [List of Registered Keywords].
[Clear All]	Cancel the selection of all keywords in [List of Registered Keywords].
[Add]	Register the specified keyword in keyword input field.
[Delete]	Delete the keyword selected in [List of Registered Keywords].
[Modify]	Modify the registered keywords.

- Select the type of the screening conditions in [Type] and specify the keyword in the keyword input field.

The characters that can be entered are as follows:

- Up to 80 byte characters can be registered. However, strings that contain “,” “” “\_” “%” “\_\_” “%%” cannot be registered.
- When entering the characters, external characters and platform dependent characters may be replaced by other characters and cannot be displayed correctly.

The items that can be selected, keywords can be specified and aggregation target logs are shown as follows.

Items that can be Selected	Type of Analysis for Validity of Exclusion Conditions	Aggregation Target log	Keywords can be Specified (Notes)	Aggregation conditions
Keyword	Information disclosure analysis	File export File operation Printing operation E-mail sending by recipient address	Strings containing file or file path	Aggregate the content that matches with the specified keyword in [Keywords] (partially matching).
Domain	Information disclosure analysis	E-mail sending by recipient address	Strings contained in E-mail address	Aggregate the content that does not match (backward matching) with the specified keyword in [Keywords].
	Terminal usage analysis	E-mail sending by recipient address		
URL	Terminal usage analysis	Window title obtaining with URL	Strings contained in the domain part in URL	Aggregate the content that does not match (partially matching) with the specified keyword in [Keywords].
Application	Terminal usage analysis	Application startup	Name of result file excluding extension	Aggregate the content that does not match (complete matching) with the specified keyword in [Keywords].

Notes: The specified string is case-sensitive.

The result file name of the application may be modified by the OS to uppercase and lowercase letters. Please confirm how to record the logs.

For the keyword specified by the application, please do not use capital single-byte letters and register it after modifying all of them to lowercase ones.

- Click the [Add] button.  
→ Keywords are displayed in [List of Registered Keywords].
- Execute the DTTOOLEX.EXE command and perform aggregation again.

If aggregation is not performed again, the number in aggregation results might be inconsistent with the number in the log list in the Web Console and report output.

In addition, as the logs saved on the Log Analyzer Server are taken as the target for re-aggregation, re-aggregation cannot be performed if there is no log on the current Log Analyzer Server.

For the re-aggregation process, please refer to the “-r option” of “DTTOOLEX.EXE (for moving and deleting data of Log Analyzer Server)” in “Systemwalker Desktop Keeper Reference Manual”.

#### Delete keywords in registered list

1. Select the keyword to be deleted in [List of Registered Keywords].  
To delete all the registered keywords, click the [Select All] button.
2. Click the [Delete] button.  
→ The display of [List of Registered Keywords] is updated.

#### Modify keywords in registered list

1. Select the strings of keyword to be modified in [List of Registered Keywords].
2. Enter the modified keywords in the input field.
3. Click the [Modify] button.  
→ The display of [List of Registered Keywords] is updated.

### 2.7.2.2.3 Set Items Excluded From Aggregation Target

For terminals that must access important files for business and terminals that perform large amount of file access daily, each operation can be set as a non-aggregation target according to the judgment of the system administrator.

Set group information and CT information managed in the Management Server required for exclusion condition Settings . When moving administrator information or logs from the Management Server to the Log Analyzer Server, the information will be imported to the Log Analyzer Server.

The date on which the logs on this client (CT) are moved is not consistent with the date on which the exclusion conditions set for this client (CT) are updated.

When moving logs as follows:

- Move terminal information and logs of terminal A, B and C on March 1
- Move terminal information and logs of terminal A, B, C and D on March 2
- Move terminal information and logs of terminal A, B, C and D on March 3,

the exclusion conditions can be set for terminal D after completing log moving on March 2.

In addition, the update of exclusion settings for terminal D will be started from the aggregation process when moving logs on March 3 (even if logs of terminal D exist in the logs moved on March 2nd, these logs will not be aggregated due to the settings of exclusion conditions at this time).

In order to apply the screening conditions and perform the counting before March 2nd, re-counting should not be performed after executing the re-counting option of “DTTOOLEX.EXE (for moving and deleting data of Log Analyzer Server)”.

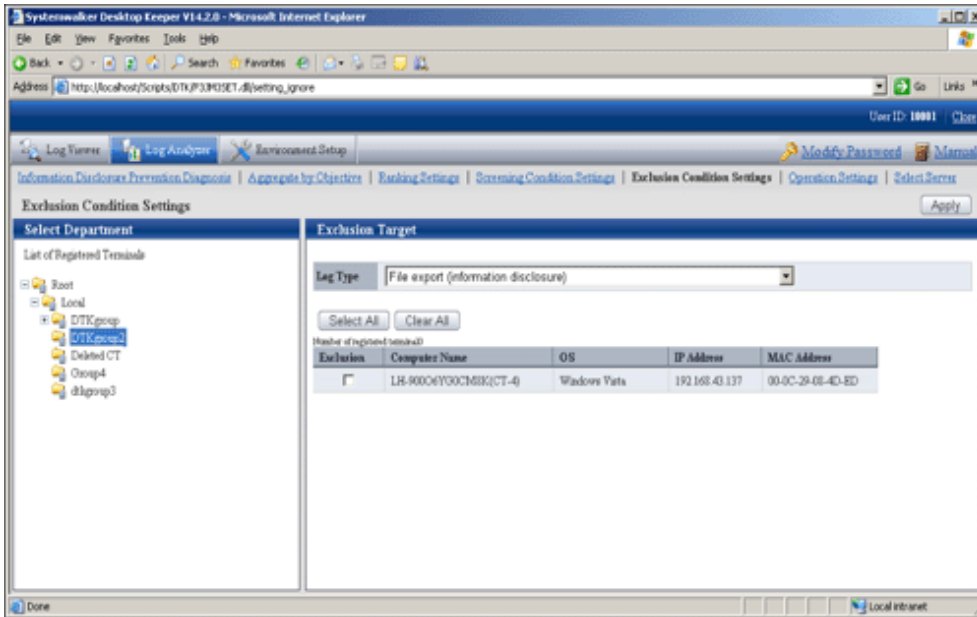



#### Note

**Please do not modify conditions when moving logs or using Log Analyzer Server and Report Output Tool.**

This may cause conflicts and errors in the aggregation result and diagnosis result or in the report output result.

1. Select [Exclusion Condition Settings] of the function menu.  
→ The following window is displayed.



Item Name	Description
[Select Department]	<p>Level relations of each department can be displayed in the tree structure. Select the department to which the terminal that requires the settings of exclusion conditions belongs.</p> <p> <b>Note</b></p> <p><b>About Not Configured group</b></p> <p>If [Manage under the group that is not configured] has been set in [System settings] - [Set group that is not configured] of Server Settings Tool, the groups displayed in [Select Department] will manage the client (CT) in “Root ” group instead of “Not Configured” group.</p> <ul style="list-style-type: none"> <li>- Folder icon When a sub-folder exists, display/hide can be modified by clicking the icon.</li> <li>- Department name After clicking the department name, the terminal list under direct control of the department will be displayed in [Excluded Target]. The color will be changed after a department is selected.</li> </ul>
[List of Registered Terminal]	<p>After clicking, all terminals registered as excluded target will be displayed in the list for this operation log. It is used in the cases such as when all registered terminals are deleted.</p>
[Exclusion Target]	<p>The list of terminal as excluded target is displayed. As the list of terminals excluded from the aggregation target will be managed by each operation, the display of the terminal list will change after [Log Type] is changed.</p> <ul style="list-style-type: none"> <li>- [Number of Registered Terminals]: This is the current number of terminals that are registered as excluded ones.</li> <li>- [Exclude]: This is selected when the item has become the excluded target.</li> </ul>

Item Name	Description
	- [Computer name]: the computer name is displayed. If the computer has been set with an alias that is different from the computer name, the alias will be displayed in the bracket.
[Log Type]	Select the operation log as settings target of exclusion condition Settings .
[Select All]	Select all terminals in the terminal list.
[Clear All]	Cancel the selection of all terminals in the terminal list.
[Apply]	Update the exclusion condition settings according to specified content.

- In the [Select Department] tree, select the department to which the terminals with set exclusion conditions belongs.
- Select terminals to be excluded from the aggregation target in [Exclusion Target].  
Up to 400 logs can be registered.
- Select operation logs as settings target of exclusion condition Settings in [Log Type] of [Exclusion Target].

The name of the operation that can be selected and logs excluded from the aggregation target are shown as follows.

Name of Operation that can be Selected	Type of Analysis with Valid Exclusion Conditions	Operation Log of Counting Excluded Targets
File export	Information disclosure analysis	File Export Log
File operation	Information disclosure analysis	File Operation Log
Printing operation	Information disclosure analysis	Printing Operation Log
E-mail sending by recipient address	Information disclosure analysis Terminal usage analysis	Log of E-Mail sending by recipient address
Window title with URL	Terminal usage analysis	Window Title Obtaining Log with URL
Application startup	Terminal usage analysis	Application Startup Log

- Click the [Apply] button.  
→ The message indicating the completion of settings appeared.
- Execute the DTTOOLEX.EXE command and perform the aggregation again.

If re-aggregation is not performed, the number in the aggregation result may be inconsistent with the number in the log list in the Web Console and report output.

In addition, as the logs saved on the Log Analyzer Server are taken as the target for re-aggregation, re-aggregation cannot be performed if there are no logs on the current Log Analyzer Server.

For the re-aggregation process, please refer to the “-r option” of “DTTOOLEX.EXE (for moving and deleting data of Log Analyzer Server)” in “Systemwalker Desktop Keeper Reference Manual”.

#### 2.7.2.2.4 Set Other Conditions

Set the ranking display of information disclosure prevention diagnosis, set the day of a week to start weekly report in the report output, set the target value used for judging improvement/deterioration of the situation and set eco auditing, etc.

The settings of other conditions will be updated immediately after they are modified.

## Note

**Please do not modify conditions when moving logs or using Log Analyzer Server and Report Output Tool.**

This may cause conflicts and errors in the aggregation result and diagnosis result or in the report output result.

1. Select [Operation Settings] of the function menu.  
→ The following window is displayed.

The screenshot shows the 'Operation Settings' window with the following visible settings:

- Information Disclosure Prevention Settings:**
  - Worst ranking of violation:  Display,  Not display. Ranking Display Number: 5. Display in red: 10 items or more.
  - Set the day of a week to start weekly report:  Monday,  Tuesday,  Wednesday,  Thursday,  Friday,  Saturday,  Sunday.
  - Start the start date of monthly report: 21 Day.
  - Information Disclosure Prevention Diagnosis Operation:  Desktop Log AnalyzerRun with compatibility.
- Eco auditing settings:**
  - Settings of Start Month in a Year: 4 Month.
  - Paper cost equivalent to 1 page (or 1 piece): 0.60 Yen.
  - CO2 emission equivalent to 1 page (or 1 piece): 5.16g.
  - Auditing Judgment Standard 1: 100 Page(s).
  - Auditing Judgment Standard 2: 200 Page(s).

2. Enter the configuration value in each item.

[Information disclosure prevention Settings]

Item Name	Description
[Worst ranking of violation]	<ul style="list-style-type: none"> <li>- [Display]/[Not Display] the radio button. Select display/hide the worst ranking of violation operations displayed in the information disclosure prevention diagnosis window.</li> <li>- [Ranking Display Number] Specify a ranking display number within 1-99.</li> <li>- [Display in red] In the worst ranking of violation operations displayed in the TOP window, specify the number threshold value used for a warning display (cell displayed in red) with numbers 1-9999. Cells indicating the number above the threshold value will be displayed in red.</li> </ul>
[Set the day of a week to start weekly report]	<p>Specify the day of the week as the start date of monthly report. When [Sunday] is specified, the period of monthly report is from this Sunday to next Saturday. The default configuration value is [Sunday]. The configuration value here will be updated to [Analysis Period] ([Monthly Report]) of the <a href="#">Settings of [Basic Information] tab</a> in the [Report Output Tool] window.</p>
[Start the start date of monthly report]	<p>Specify the date as the start date of the monthly report. When [21] is specified, the period of monthly report is from 21st of this month to 20th of next month. The default configuration value is [21].</p>



Item Name	Description
	<p>The date can be set are from [1] to [28].</p> <p>The configuration value here will be updated to [Analysis Period] ([Monthly Report]) of the <a href="#">Settings of [Basic Information] tab</a> in the [Report Output Tool] window.</p>
[Information Disclosure Prevention Diagnosis Operation]	<p>When [Operation in Compatible with Desktop Log Analyzer] is selected, the Aggregate by objective window will be displayed after clicking terminal name in the ranking of information disclosure prevention and diagnosis, and it will run in the same way as Systemwalker Desktop Log Analyzer.</p> <p>The detailed description is as follows. It is not selected in default.</p> <p>[When this item is not selected]</p> <p>After clicking the number of [Aggregation Result by Operations] in the [Information Disclosure Prevention and Diagnosis] window, ranking by operations will be displayed.</p> <p>As the item of each ranking, after clicking the link displayed in group name, terminal name, terminal+user name, the correspondent window of [CT Operation Log - Log Search] of Log Viewer will be displayed.</p> <p>During the period of screening with Log Analyzer, in the [CT Operation Log - Log Search] window, target group/terminal/user and operations will be displayed in the status of being set as search input items. In addition, the search result based on this condition will be displayed in the log list.</p> <p>Through the user name and PC name ranked by higher possibility for information disclosure, the detailed operation (logs) can be carried out smoothly for information disclosure investigation.</p> <p>[If this item is selected]</p> <p>After clicking the number of [Aggregation Result by Operations] in the [Information Disclosure Prevention and Diagnosis] window, ranking by operations will be displayed. As the item of each ranking, after clicking the link displayed in group name, terminal name, terminal+user name, the Aggregate by objective window will be displayed.</p> <p>Set the conditions such as the screening period manually in the Aggregate by objective window and re-perform the counting. Through the ranked user name and PC name, the detailed operation (logs) cannot be carried out.</p>

[Eco auditing settings]

Item Name	Description
[Settings of Start Month in a Year]	<p>When counting the annual accumulation, specify the start month of the year as a reference in the printing volume auditing report and all-in-one PC/printer paper usage report*.</p> <p>Select from 1-12.</p> <p>The initial value is 4.</p>
[Printing volume auditing settings]	<p>[Paper cost equivalent to 1 page (or 1 piece)]</p> <p>In the printing volume auditing report and all-in-one machine/printer paper usage report*, specify the coefficient for calculating paper cost in RMB.</p> <p>Accurate to the second decimal place.</p> <p>Value from 0.01 to 99.99 can be specified.</p> <p>The initial value is 0.60.</p> <p>In the printing volume auditing report, use this coefficient as the Paper cost equivalent to 1 page.</p> <p>In the all-in-one machine/printer paper usage report, use this coefficient as the paper cost equivalent to 1 page.</p>

Item Name		Description
	[CO2 emission equivalent to 1 page (or 1 piece) g]	<p>In the printing volume auditing report and the all-in-one machine/printer paper usage report*, specify the coefficient for calculating CO2 emission in terms of g. Accurate to the second decimal place. Value from 0.01 to 99.99 can be specified. The initial value is 5.16.</p> <p>In the printing volume auditing report, use this coefficient as the CO2 emission equivalent to 1 page of printing paper.</p> <p>In the all-in-one machine/printer paper usage report, use this coefficient as the CO2 emission equivalent to 1 page of printing paper.</p>
	[Auditing Judgment Standard 1] [Auditing Judgment Standard 2]	<p>When the terminal that exceeds the printing upper limit is output from the printing volume auditing report, specify the judgment standard value for the exceeded amount (pages) in terms of pages.</p> <p>Standard 1 can be specified with a value larger than 2 but smaller than 999999998. Standard 2 can be specified with a value larger than 3 but smaller than 999999999. In addition, standard 1 must be smaller than standard 2. The initial value of standard 1 is 100 and the initial value of standard 2 is 200.</p> <p>The configuration value here will be updated to “Ratio of Terminal by Exceeded Amount” of “Status of Exceeding Upper Limit of Printing” sheet and “[▲] or [△]” of “List of Exceeded Terminals” sheet in printing volume auditing report.</p>

\*For a report on paper usage status of all-in-one machine/printer, please refer to “[Appendix B Appendix B Visualize Information through Linking with All-in-one PC/Printer](#)”.

3. Click the [Apply] button.

### 2.7.2.2.5 Select Log Analyzer Server

Select/change the Log Analyzer Server in use in the system where multiple Log Analyzer Servers exist.



#### Note

**Please do not select Log Analyzer Server when using Log Analyzer function and moving logs**

This may cause conflicts and errors in the aggregation result.

**Please do not modify server structure and settings during login**

This may cause situations such as being unable to identify correctly and unable to set and process correctly. If this is the case, please login again.

**It will take some time to display the window.**

When Log Analyzer Server cannot be connected due to reasons such as server stoppage or network interruption, it may take several minutes to display the window, based on the environment and number of servers.

**When the status of Log Analyzer Server changes, it will take some time until the change is reflected.**

When the status changes, for example if the disconnected the Log Analyzer Server becomes connectable, the status will not be updated immediately. Please confirm it again later.

1. Select [Select Server] of the function menu.

→ The following window is displayed.



The window will be automatically displayed if all of the following conditions are satisfied:

- When there are multiple Log Analyzer Servers in the system structure
- When login from the main menu and Log Analyzer is used for the first time

2. Select Log Analyzer Server

Select the Log Analyzer Server displayed in blue (server name and IP address are displayed) from the tree structure.

The selected Log Analyzer Server will be displayed in reverse color.

Click the [+] button and the Management Server from which the log data are moved to Log Analyzer Server is displayed.

Log Analyzer Server displayed in red is not available, so it cannot be selected. For this server, please refer to “Messages Output in Web Console” in “Systemwalker Desktop Keeper Reference Manual” to process [ERR-DTLAC001].

3. Click the [Apply] button.

## Chapter 3 Set Policy in Management Console

After reviewing the current guideline for operation, policy may need to be modified.

In this case, in order to select the client (CT) and user for modification, it is needed to search and modify the policy.

This chapter describes how to search CT information/User information in The Management Console and how to modify policies.

### 3.1 Search CT Information/User Information

#### Search CT Information

The following describes the procedure of searching the CT group and CT displayed in the Management Console.

When the “Deleted CT” group is displayed in the CT group tree of the Management Console, the client (CT) to which the “Deleted CT” group belongs will also be searched.

The client (CT) of the “Deleted CT” group will be displayed as “Deleted CT” in “Group Name” of the area for displaying search result.

1. Start [Management Console].
2. Select the [Root directory] or [CT Group] to be searched from the CT group tree.

3. Select [Search CT/CT Group] from the [File] menu (or right-click and select [Search CT/CT group] from the displayed pop-up menu).

→ The [Management Console Search CT/CT group] window is displayed.

The screenshot shows the 'Management Console Search CT/CT group' window. The search form includes the following fields and options:

- Search Location: Root directory
- Search Condition: Computer Name (Search with partially match)
- IP Address (999.999.999.999) (Search with forward match)
- MAC Address (XX-XX-XX-XX-XX-XX) (Search with completely match)
- Owner (Search with partially match)
- CT Version (Search with completely match)
- Name/CT Group Name (Search with partially match)
- DTPID (Search with partially match)
- Notes (Search with partially match)
- Last Logon Date (YYYYMMDD) ~
- Client Policy Update Date (YYYYMMDD) ~
- Applied Policy:  As Condition,  CT,  Group
- Active Directory Linkage Target:  As Condition,  Linkage Target,  Not Linkage Target
- Virtual PC:  As Condition,  Physical PC,  Virtual PC,  Master Image

Buttons: Search, Close Window

Group name	Apply policy	Name/CT group name	Computer name	MAC address	IP address	OS	CT classification	CT version	DTI
Search Result Case(s)									

Select

4. Enter the following information as the search condition.

The search is the “AND search” that includes multiple conditions.

**[Search CT group]**

Specify [Name/CT Group Name] and [Notes] only. In addition, the [As condition] checkbox of [Applied policy] should not be selected.

**[Search Condition]**

Specify the items of search condition.

Item Name		Description
[Computer Name]		Search according to the computer name of the client (CT). Results that partially match with the input conditions will be displayed. Up to 15 bytes of single-byte and double-byte characters can be entered.
[IP Address]		Search according to the IP address of the client (CT). The result of which the front part matches with the input conditions will be displayed. When searching with "10.1", the result will include "10.1.", "10.1X." and "10.1XX.". ("X" indicates one numeral character) Enter in the format of "XXX.XXX.XXX.XXX". [Example] 140.48.23.12
[MAC Address]		Search according to the MAC address of the client (CT). The result that completely matches with the input conditions will be displayed. Enter in the format of "XX-XX-XX-XX-XX-XX". ("X" indicates one alphanumeric character) [Example] 02-E0-32-33-A3-C0
[Owner]		Search according to the owner set in the OS of the client (CT). Results that partially match with the input conditions will be displayed. Up to 93 bytes of single-byte and double-byte characters can be entered.
[CT Version]		Search according to the version of the client (CT) of the Systemwalker Desktop Keeper installed. Results that completely match with the input conditions will be displayed. Enter in the format of "X.X.X.X". ("X" indicates more than one numeral characters) [Example] 2.1.0.1
[Name/CT Group Name]		Search according to the name of the CT group or client (CT). Results that partially match with the input conditions will be displayed. Up to 40 bytes of single-byte and double-byte characters can be entered.
[DTPID]		This is displayed when the client (CT) of Systemwalker Desktop Keeper and the client (CT) of Systemwalker Desktop Patrol are installed on the same PC. Enter "User ID (+) PC name" of the client (CT) of Systemwalker Desktop Patrol. Perform search with partial matching.
[Notes]		Search according to the notes entered when updating the client (CT) policy. Results that partially match with the input conditions will be displayed. Up to 128 bytes of single-byte and double-byte characters can be entered.
[Last Logon Date]		The client (CT) communicates with the Master Management Server or Management Server at startup. Search according to the date when this communication is enabled Enter in the format of "XXXXXXXX". ("X" indicates one numeral character) [Example] 20050701
[Client Policy Update Date]		Search according to the last date when the client (CT) obtains policy from the Master Management Server or Management. Enter in the format of "XXXXXXXX". ("X" indicates one numeral character) [Example] 20050922
[Applied Policy]	[As Condition]	When this checkbox is selected, the policy being applied to the client (CT) will be included in the search condition.
	[CT]	The search target is the client (CT) to which the CT policy is applied.
	[Group]	The search target is the client (CT) to which the CT group policy is applied.
[Active Directory]	[As Condition]	When this checkbox is selected, whether it is the client (CT) that imports information from Active Directory will be included in the search condition.

Item Name		Description
Linkage Target]	[Linkage Target]	The search target is the client (CT) that imports information from Active Directory.
	[Not Linkage Target]	The search target is the client (CT) that does not import information from Active Directory.
[Virtual PC]	[As Condition]	When this checkbox is selected, the environment with client (CT) installed will be included in the search condition.
	[Physical PC]	This refers to the client (CT) installed in a physical PC.
	[Virtual PC]]	This refers to the client (CT) installed in a virtual PC.
	[Master Image]	This refers to the client (CT) installed in the master image of a virtual PC.
[Search]		The search will be started and the results will be displayed.
[Close Window]		The entered search condition will be saved.

5. Click the [Search] button.

→ The search results are displayed.

The displayed items are the ones selected from the [Setting of CT List Display Column] window. For the [Setting of CT List Display Column], please refer to “[When modifying the displayed items and sequence](#)”.

When double-clicking on the CT or CT group that has been found, the [Management Console] window will be displayed, and the corresponding CT or CT group will be in selected state. The [Search CT/CT group] window will not be closed and will be displayed in minimized status.

6. Click the [Close Window] button.

→ The entered search condition is saved.

The saved search condition will be displayed at the next time when the [Search CT/CT group] window is started. However, the search condition that is currently input will not be saved if the window is closed by clicking the [×] button at the top right of the [Search CT/CT group] window.

## Search User Information

Search of user and user group can be executed in the Management Console.

The search procedure is as follows.

1. Start [Management Console].
2. Select [User Policy Settings] from the [User Settings] menu.  
→ The [User Policy Settings] window is displayed.
3. Select the [Root directory] or [User Group] to be searched from the user group tree.

4. Select [Search User/User Group] from the [File] menu (or right-click and select [Search User/User Group] from the displayed pop-up menu).

→The [Management Console Search User/User Group] window is displayed.

Management Console Search User/User Group

Search Location Root directory

Search Condition User Name/Group Name (Search with partially match)

User's Name (Search with partially match)

Employee No. (Search with partially match)

POST (Search with partially match)

Organization (Search with partially match)

Organization Code (Search with partially match)

Notes (Search with partially match)

Applied Policy  As Condition  User  Group

Do not Apply User Policy  As Condition  Applied  Not Applied

Search Close Window

Group name	Apply policy	Do not apply po...	User name/Gro...	User name	Employee No.
------------	--------------	--------------------	------------------	-----------	--------------

Search Result Case(s) Select

5. Enter the following information as the search condition.

The search is the “AND search” that includes multiple conditions.



**[Search user group]**

Specify [User Name/Group Name] and [Notes] only. In addition, the [Applied Policy] and [Do not Applied User Policy] checkboxes should not be selected.

**[Search user]**

Specify the items of search condition.

Item Name		Description
[User Name/Group Name]		Search according to user name and user group name. Results that partially match with the input conditions will be displayed. Up to 40 bytes of single-byte and double-byte characters can be entered.
[User's Name]		Search according to the name of user that uses the user name. Results that partially match with the input conditions will be displayed. Up to 128 bytes of single-byte and double-byte characters can be entered.
[Employee No.]		Search according to the Employee No. of the user that uses the user name. Results that partially match with the input conditions will be displayed. Up to 40 bytes of single-byte and double-byte characters can be entered.
[POST]		Search according to the title of the user that uses the user name. Results that partially match with the input conditions will be displayed. Up to 128 bytes of single-byte and double-byte characters can be entered.
[Organization]		Search according to the organization to which the user that uses the user name belongs. Results that partially match with the input conditions will be displayed. Up to 128 bytes of single-byte and double-byte characters can be entered.
[Organization Code]		Search according to the organization code to which the user that uses the user name belongs. Results that partially match with the input conditions will be displayed. Up to 40 bytes of single-byte and double-byte characters can be entered.
[Notes]		Search according to the remark information of the user that uses the user name. Results that partially match with the input conditions will be displayed. Up to 128 bytes of single-byte and double-byte characters can be entered.
[Applied Policy]	[As Condition]	When this checkbox is selected, the policy that is applied to user will be included in the search condition.
	[User]	The search target is the user to which the user policy is applied.
	[Group]	The search target is the user to which the user group policy is applied.
[Do not Apply User Policy]	[As Condition]	When this checkbox is selected, whether the user policy is applied will be included in the search condition.
	[Applied]	The search target is the user to which the user policy is applied.
	[Not Applied]	The search target is the user to which the user policy is not applied.

- Click the [Search] button.  
→The search results are displayed.

Group name	Apply policy	Do not apply policy	User name/Group name	User name	Employee No.	Ti
System Development Div.	User		FujitsuTom	Fujitsu Tom		
System Development Div.	User		FujitsuKate	Fujitsu Kate		

Search Result      2 Case(s)      Select

When double-clicking on the user or user group that has been found, the [Management Console] window will be displayed, and the correspondent user or user group will be in selected state. The [Search User/User Group] window will not be closed and will be displayed in minimized status.

7. Click the [Close Window] button.

→ The input search condition is saved.

The saved search condition will be displayed at the next time when the [Search User/User Group] window is started. However, the search condition that is currently input will not be saved if the window is closed by clicking the [×] button at the top right of the [Search User/User Group] window.

## 3.2 Modify Group Policy

---

After creating the configuration information tree, group policy will be set for each group.

Modify the group policy as needed.

The following are ways to modify group policy:

- The system administrator manages policy of all groups.
- Set a department administrator to be responsible for modification of policy for the group he or she manages.

### 3.2.1 Modify CT Group Policy

---

#### Modify CT Group Policy

When policy has been updated in the Management Console, the policy of all tabs will be updated (for the part where the setting is not modified, it will be updated with the same value).

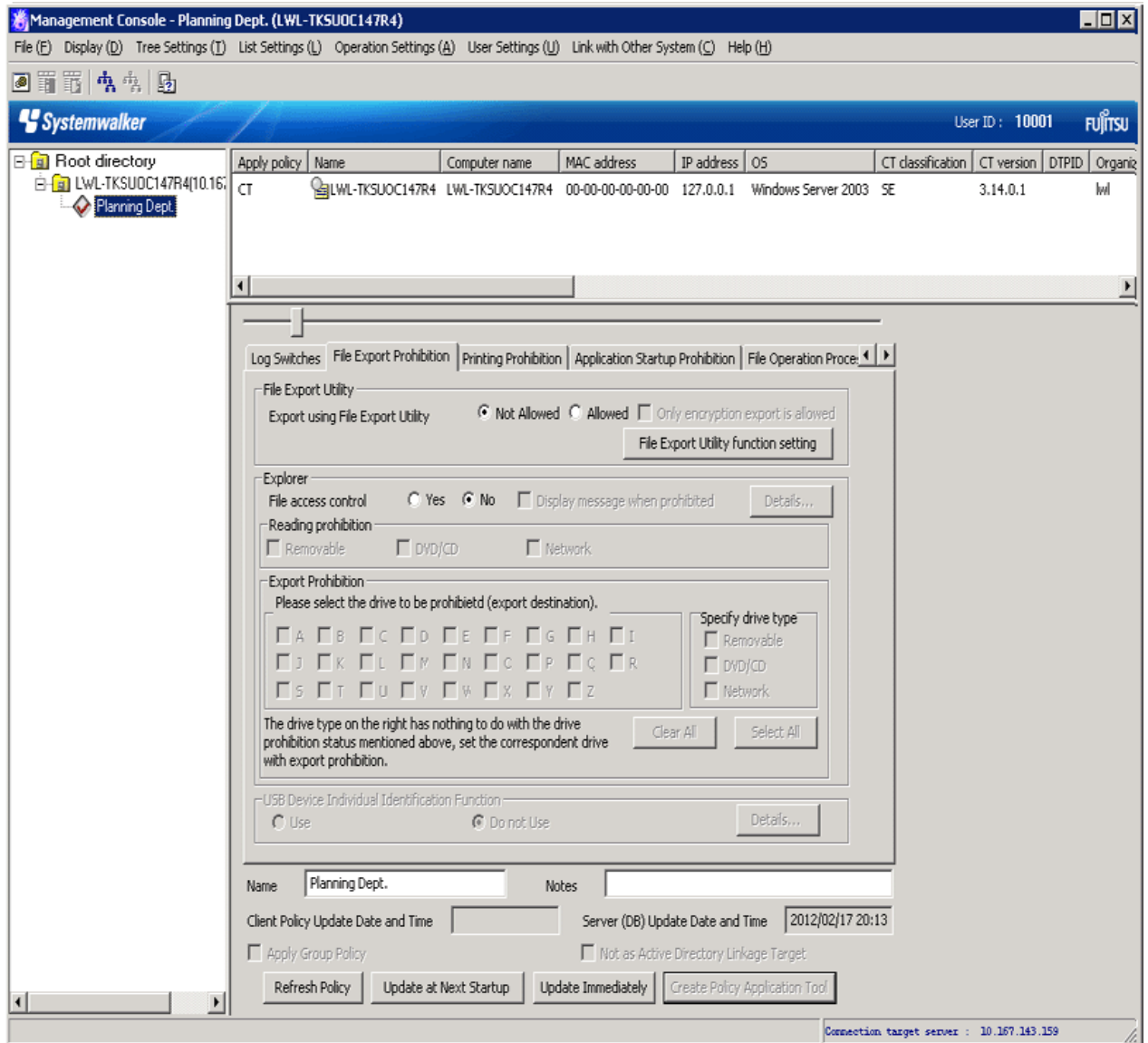
It is unable to update only the tabs or items with modified settings.

The following describes the procedure for modifying a CT group policy.

1. Start [Management Console].

2. Select the CT group for policy setting from the CT group tree.

→ The latest policy information is displayed.



## Note

### In the following cases, please update the information of CT group and CT list

When any of the following conditions are satisfied, the information of the CT group or CT list of the Management Server under the Master Management Server displayed in the window may not be updated.

- When the CT group is modified on the Management Server side
- When Active Directory Linkage is performed and the group tree is modified

Please select [Refresh Tree] from the [Tree Settings] menu to update.

3. Modify policy in each tab of the policy list.

For description of policy setting items, please refer to “[2.4.1 Perform Terminal Initial Settings](#)”.

4. Modify [Name] or [Notes] of CT group as needed.

For characters that can be entered in [Name] and [Notes], please refer to “[Modify group information](#)”.

5. Click any of the following buttons to update policy to the CT group:

- When clicking the [Update at Next Startup] button

The policy of each tab will be updated to the database, but it will not be updated to the client (CT) immediately. Instead, the latest policy will be updated at the next time when the client (CT) is started and communicates with the target server (Master Management Server or Management Server).

- When clicking the [Update Immediately] button

- The policy of each tab will be updated both in database and the running client (CT).

However, the setting of [File Export Prohibition] tab will update policy at the next startup of file export utility when the file export utility has been started at the client (CT) on which the immediate update is performed.

- When the application permitted in the [Printing Prohibition] tab has already been started in the client (CT) on which the immediate update is performed, policy will be updated at the next application startup.

- When logoff or shutdown has been set in the [Logon Prohibition] tab, it will be updated to the running client (CT). In addition, for the client (CT) that is not running and the client (CT) that is unable to communicate with the upper level server, the latest policy will be updated at the next time when the client (CT) is started and communicates with the target server (Master Management Server or Management Server).

When the [Update at Next Startup] button or the [Update Immediately] button is grayed out, the configuration may not be updated after a CT group has been created, moved or deleted. At this time, please select [Reflect CT Group Structure] from the [Tree Settings] menu to update configuration.



.....

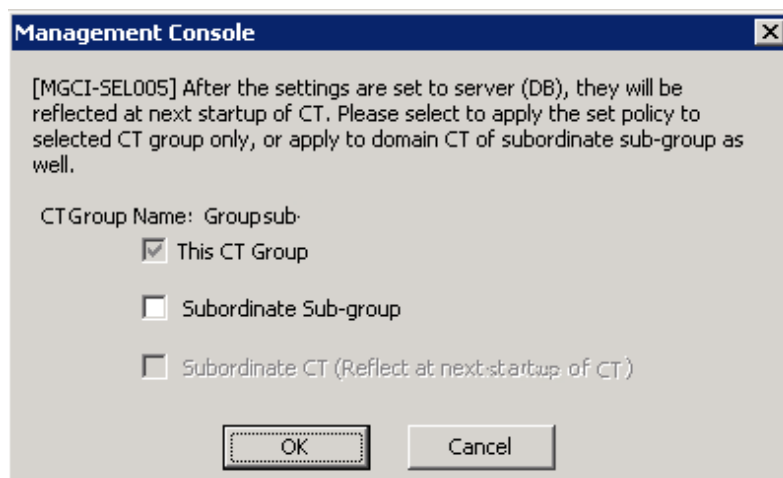
**When there are a large number of clients (CTs) in a CT group, it is recommended to select [Update at Next Startup]**

The timeout period for the connection of the client (CT) that is not connected to the Master Management Server or Management Server is 5 seconds for each client (CT). In addition, in spite of dependence on network environment, when performing [Update Immediately] for the client (CT) that is connected to the Master Management Server or Management Server, the time required for each client (CT) to apply policy is approximately 1 second.

Therefore, when immediate update is performed for a CT group, if there are a large number of CTs for which the policy needs to be set, it is recommended to click the [Update at Next Startup] button to use this option.

.....

→ The following window is displayed.



6. Select the method for applying policy and click the [OK] button.
  - **[This CT Group]:**
    - Apply the set policy to the selected CT group. It cannot be modified.
  - **[Subordinate Sub-group]:**
    - Apply the set policy to the subordinate subgroup of the selected CT group.
  - **[Subordinate CT (Reflect at next startup of CT)]:**
    - Apply the set policy to the subordinate client (CT) of the selected CT group.  
The [Name] and [Notes] of the subordinate client (CT) will not be overwritten.  
Selection can be performed when [Subordinate Sub-group] has been selected.
7. After [Name] or [Notes] has been modified, selected [Refresh Tree] from the [Tree Settings] menu.
  - The information entered in [Name] or [Notes] will be updated to the [Management Console] window.

### **Copy CT Group Policy or CT Policy**

This section describes the method for copying the policy that has been set in the client (CT) or CT group policy to another client (CT) or CT group.

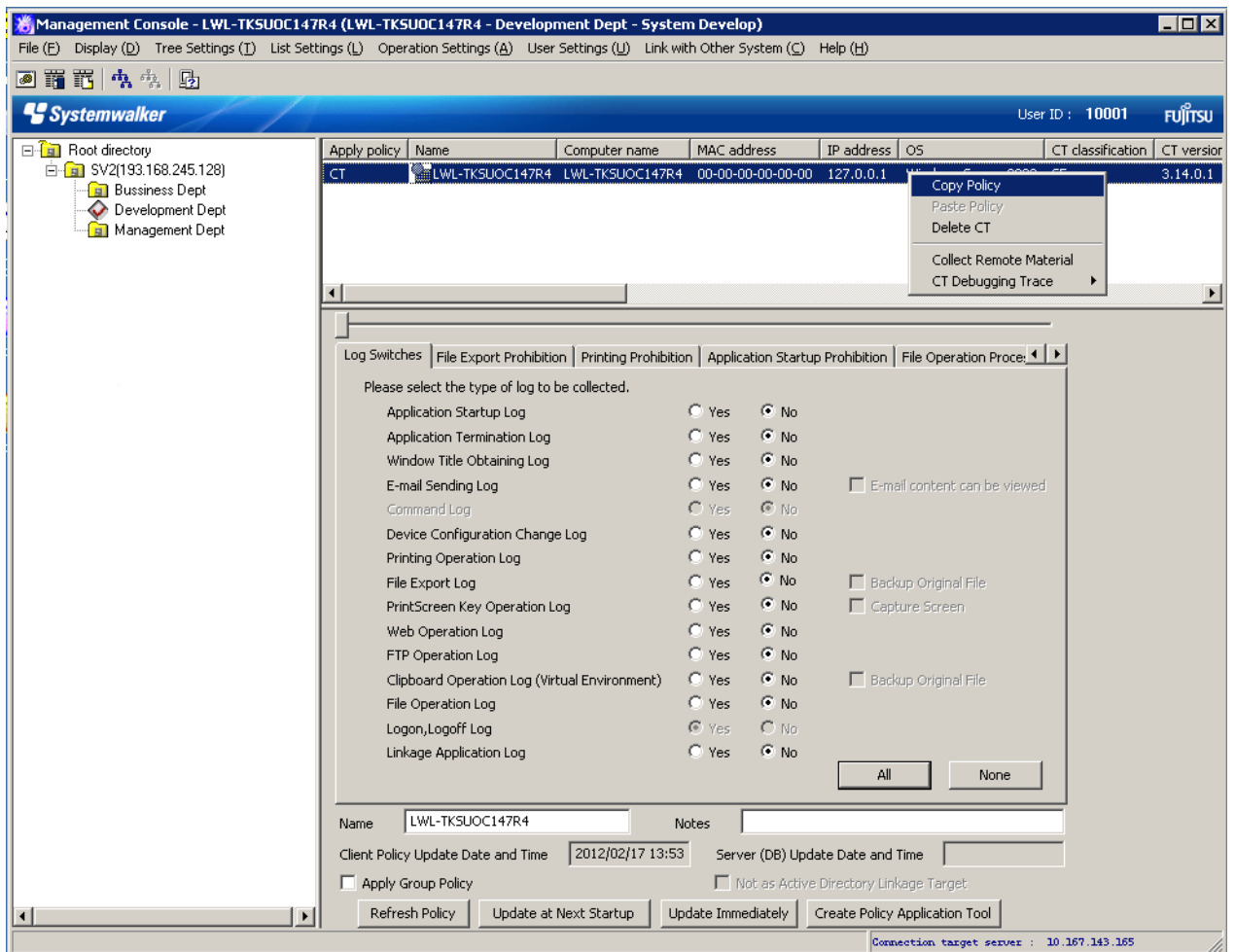
After the copy of policy has been used, the same policy can be set at another client (CT) or CT group.

The procedure is as follows:

1. Start the [Management Console] window.
2. Select the client (CT) or CT group as the copy source.
  - When client (CT) is selected
    1. Select the CT group with the client (CT) registered as copy source from the CT group tree.
    2. Select the client (CT) as the copy source from the CT list.
  - When CT group is selected
    1. Select the CT group as the copy source from the CT group tree.

3. Right-click on the selected client (CT) or CT group.

→ The pop-up menu is displayed. (The following image shows the situation of copying CT policy.)



4. Select [Copy Policy] from the displayed pop-up menu.

5. Select client (CT) or CT group as the copy target.

- When client (CT) is selected

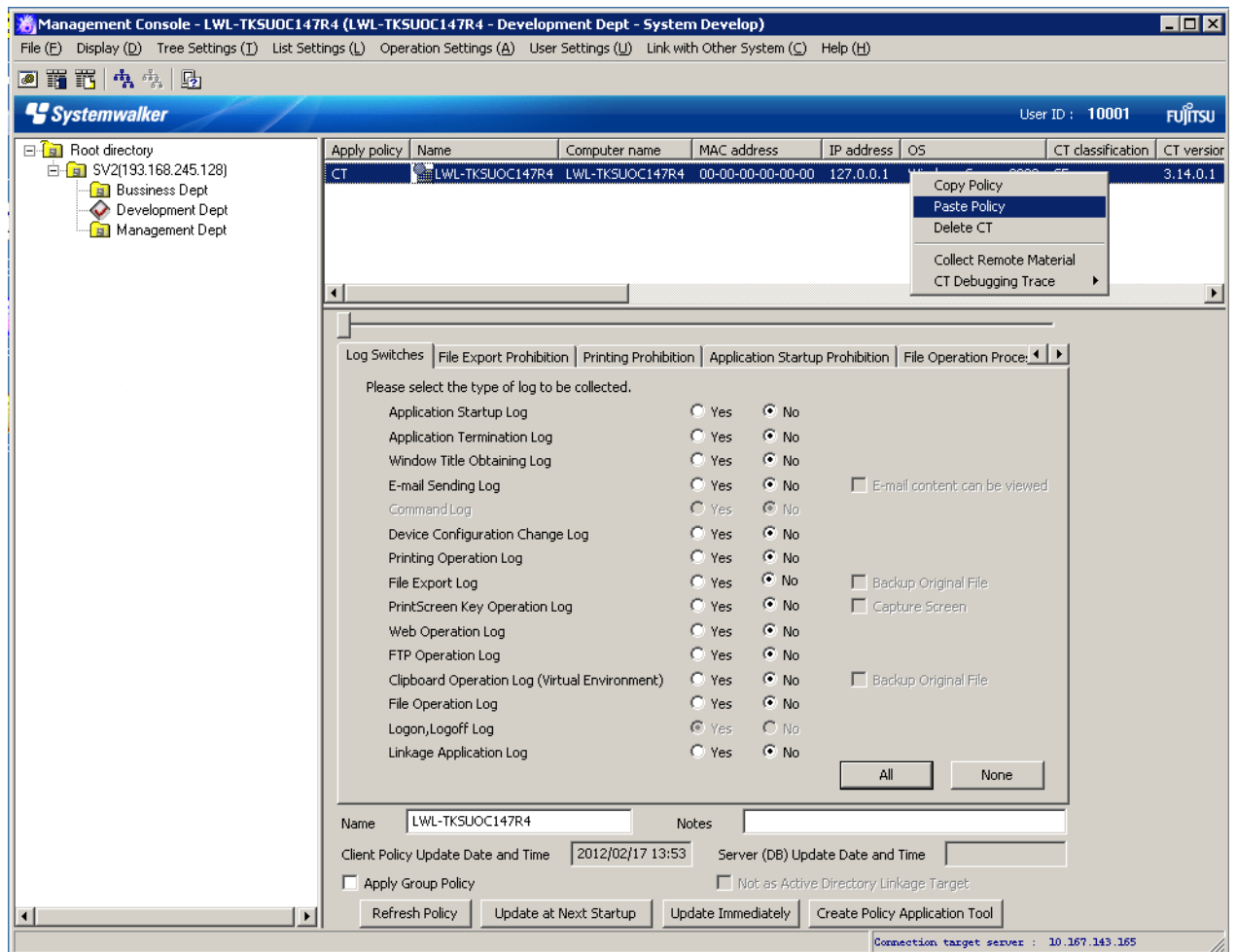
1. Select the CT group with client (CT) registered as the copy target from the CT group tree.
2. Select the client (CT) as copy target from the CT list.

- When CT group is selected

1. Select the CT group tree as copy target from the CT group tree.

6. Right-click on the selected client (CT) or CT group.

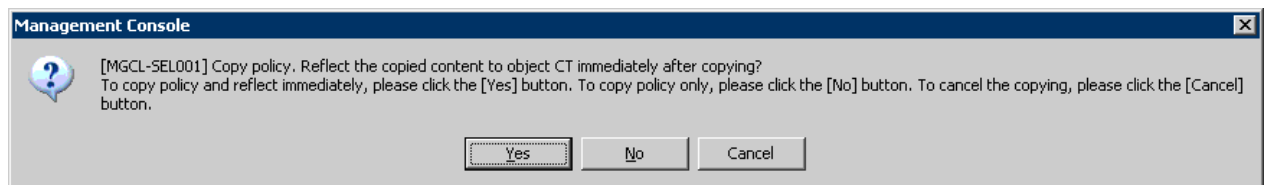
→ The pop-up menu is displayed. (The following image shows the situation of copying to client (CT))



7. Select [Paste Policy] from the displayed pop-up menu.

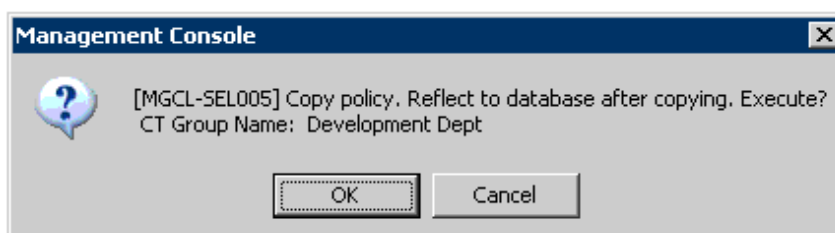
→ The confirmation window for policy copying is displayed.

- When pasting to client (CT)



Click [Yes] to copy policy and update the copied policy in the client (CT) immediately. Click [No] to copy policy and update the copied policy at next startup. Click [Cancel] to cancel the copy of policy.

- When pasting to CT group





Click [OK] to copy policy and click [Cancel] to cancel the copy of policy.

## 3.2.2 Modify User Group Policy

### Modify User Group Policy

When updating policy in the Management Console, the policy of all tabs will be updated (for the part where the setting is not modified, it will be updated with the same value).

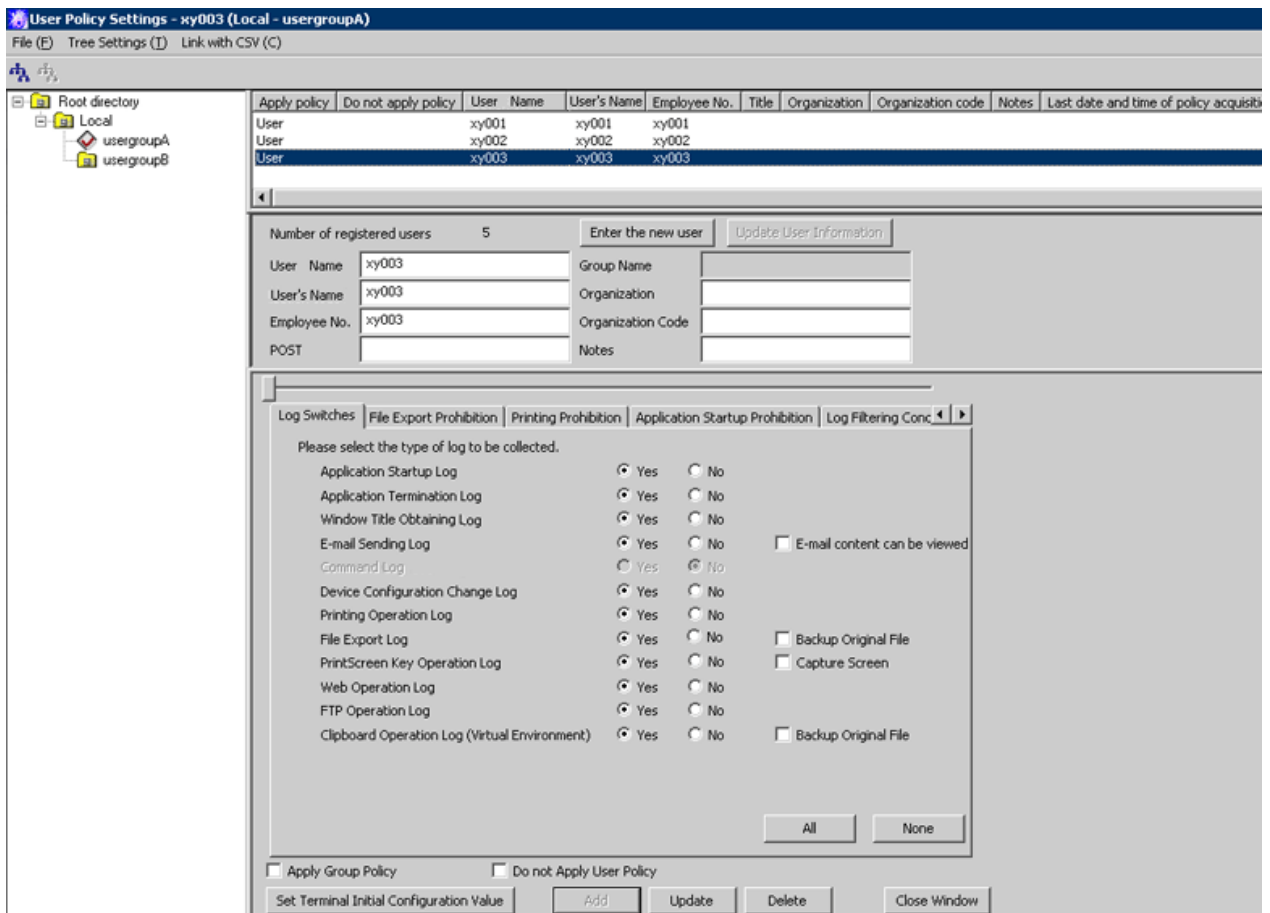
It is unable to update only the tabs or items with modified settings.

The following describes the procedure of modifying user group policy:

1. Start [Management Console].
2. Select the [User Policy Settings] from the [User Settings] menu.

→ The [User Policy Settings] window is displayed.

For details of content displayed in the [User Policy Settings] window, please refer to “[Content Displayed in Window](#)”.



3. Select the user group that requires policy modification from the user group tree.

4. Modify policy in each tab of the user policy list.

For description of policy setting items, please refer to “[2.4.1 Perform Terminal Initial Settings](#)”.

5. Click the [Update] button.

→ The set policy will be updated into the user group at next time of logon.

## Content Displayed in Window

The following describes the items displayed in the [User Policy Settings] window.

### User Group Tree

The user group information imported through Active Directory Linkage and the created user group is displayed.

When confirming the information of the latest user group tree, select [Refresh Tree] from the [Tree Settings] menu.

When [Unfold All Trees] is selected from the [Tree Settings] menu, all user groups will be displayed.

When [Fold All Trees] is selected from the [Tree Settings] menu, only the user group under the Root directory (under the domain when domain is displayed).

After a user group has been selected, the latest user policy that is set in user group unit will be displayed.

### User List

The users belong to the user group will be displayed. The items displayed in the user list are shown as follows.

Item Name	Displayed Content
[Apply policy]	Which one among user policy and user group policy is applied will be displayed. <ul style="list-style-type: none"> <li>- [User]: Indicates the user policy has been set.</li> <li>- [Group]: Indicates the user group policy has been set.</li> </ul>
[Do not apply policy]	Whether the user policy is applied will be displayed. <ul style="list-style-type: none"> <li>- [Not Applied]: Indicates no user policy is applied.</li> <li>- (Blank): Indicates a user policy is applied.</li> </ul>
[User Name]	The user name that logs on Windows (different from the "Full Name" that can be set in user name).
[User's Name] (Note)	This refers to the name of the user that uses the user name.
[Employee No.] (Note)	This refers to the employee number of the user that uses the user name.
[Title] (Note)	This refers to the title of the user that uses the user name.
[Organization] (Note)	This refers to the organization to which the user that uses the user name belongs.
[Organization code] (Note)	This refers to the organization code to which the user that uses the user name belongs.
[Notes]	This refers to the notes of the user that uses the user name.
[Last date and time of policy acquisition]	This refers to the date on which the latest policy is set.
[Date and time of Server(DB) update]	This refers to the date on which the Master Management Server or Management Server updates the policy of the client (CT) and policy is updated in database (including immediate update).
[Registration date and time]	This refers to the date on which the user is registered.

Note: Users imported through Active Directory Linkage cannot be modified in The Management Console.

### User Properties

The properties of the user selected in tree configuration information part can be input. The displayed [Number of Registered User] does not include the number of user groups. The input information is as follows.

Item Name	Input Content
[User Name] (Note 1) (Note 2)	Enter the user name for logging on Windows (different from the “Full Name” that can be set in user name). Up to 40 single-byte characters (20 double-byte characters) can be entered. Single-byte uppercase letters and single-byte lowercase letter will be recognized as the same character. However, errors will occur in the following cases:  <ul style="list-style-type: none"> <li>- User name with a period “.” only</li> <li>- User name with space only</li> <li>- User name that contains “”/”\”“”[”]”“:”“;”“ ”“=”“,”“+”“*”“?”“&lt;”“&gt;”</li> </ul>
[User’s Name]	Enter the name of the user that uses the user name. Up to 128 single-byte characters (64 double-byte characters) can be entered.
[Employee No.]	Enter the employee number of the user that uses the user name. Up to 40 single-byte characters (20 double-byte characters) can be entered.
[Title]	Enter the title of the user that uses the user name. Up to 128 single-byte characters (64 double-byte characters) can be entered.
[Group Name]	Enter the group name of the user group. Up to 40 single-byte characters (20 double-byte characters) can be entered.
[Organization]	Enter the organization to which the user that uses the user name belongs. Up to 128 single-byte characters (64 double-byte characters) can be entered.
[Organization Code]	Enter the organization code to which the user that uses the user name belongs. Up to 40 single-byte characters (20 double-byte characters) can be entered.
[Notes]	Enter the notes of the user that uses the user name. Up to 128 single-byte characters (64 double-byte characters) can be entered.

Note 1: It must be entered when adding a user.

Note 2: It cannot be entered when updating user information.

### User Policy List



The policy set for the user selected in tree configuration information part can be specified.

For details of the settings, please refer to “[2.4.1 Perform Terminal Initial Settings](#)”.

### Menu Bar/Tool Bar

The following describes the menu bar and tool bar of the [User Policy Settings] window.

	Menu Bar	Tool Bar	Function Summary
[File]	[Search User/User Group]	-	→ Display the [Search User/User Group] window.
	[Create User Group]	-	Display the [Create User Group] window.
	[Delete user group]	-	Display the [Delete User Group] window.
	[Set Department Administrator of User Group]	-	→ Display the [Set the Department Administrator of User Group] window. This menu cannot be selected when the department administrator logs on.
	[Import Department Administrator of User Group in CSV Format]	-	Display the [Specify a file for importing department administrator of user group in CSV format] window.
	[Export Department Administrator of User Group in CSV Format]	-	Display the [Specify a file to export department administrator of user group in CSV format] window.

	Menu Bar	Tool Bar	Function Summary
	[Close]	-	Close the [User Policy Settings] window.
[Tree Settings]	[Refresh Tree]		Display the latest information of level status of user group tree.
	[Unfold All Trees]	-	Display all user groups.
	[Fold All Trees]	-	Display only the user group under the Root directory (display only the one under domain when domain is displayed).
	[Do not Display Empty Group]	-	Do not display the user group under which no user or user group is registered.
	[Reflect User Group Structure]		Save the level status of user group tree.
[Link with CSV]	[Import User Information in CSV Format]	-	Display the [Specify a File for Importing User Information in CSV Format] This menu cannot be selected when linking with Active Directory or the department administrator logs on.
	[Export User Information in CSV Format]	-	Display the [Specify a File for Exporting User Information in CSV Format] window.

### Copy User Group Policy or User Policy

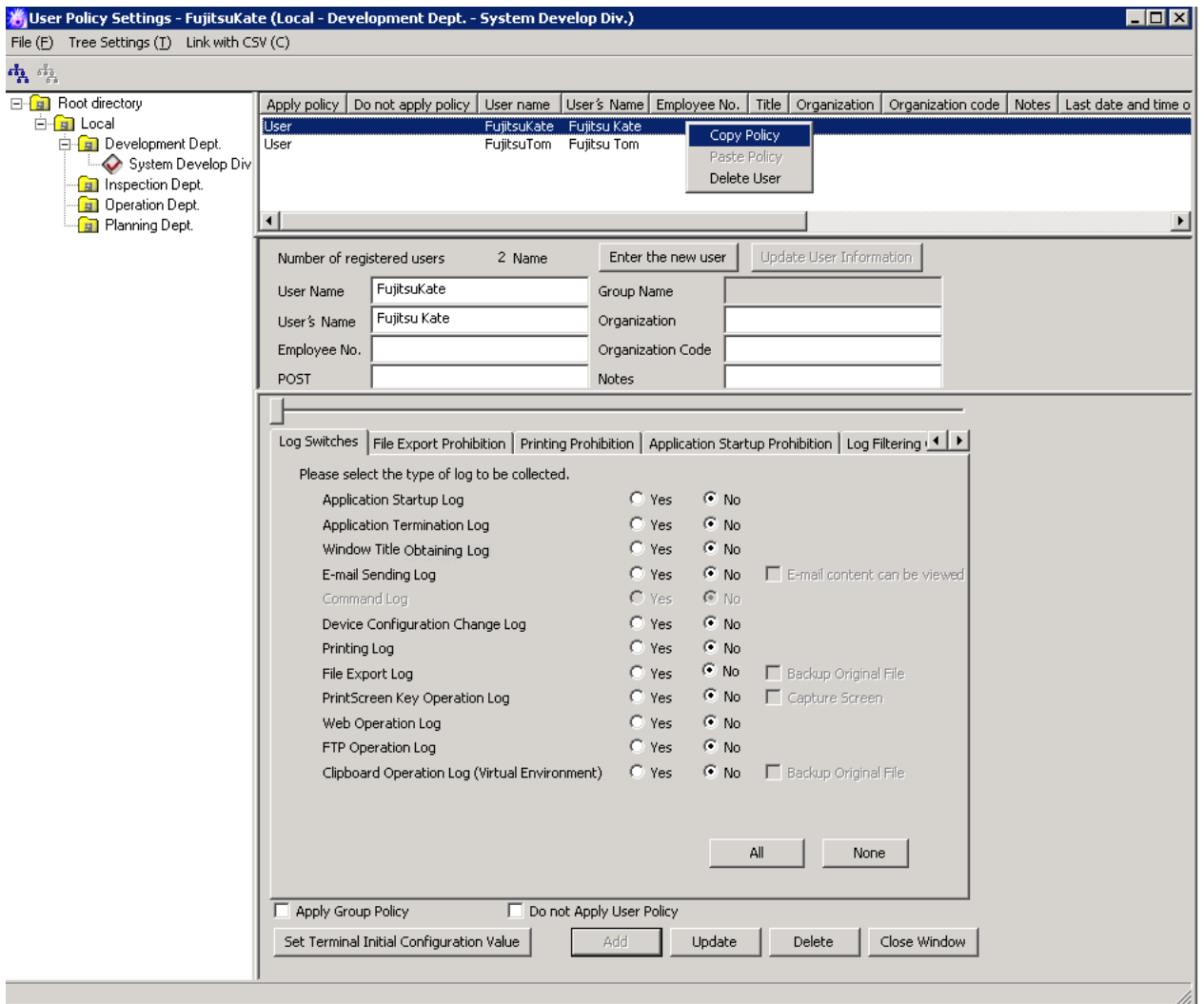
This section describes the method for copying the user group policy or user policy that has been set to another user group or user.

The procedure is as follows:

1. Start [Management Console].
2. Select [User Policy Settings] from the [User Settings] menu.  
→ The [User Policy Settings] window is displayed.
3. Select user or user group as the copy source
  - When user is selected
    1. Select the user group with user registered as copy source from the user group tree.
    2. Select the user as the copy source from [User List].
  - When user group is selected
    1. Select the user group as the copy source from the user group tree.

4. Right-click the selected user or user group.

→ The pop-up menu is displayed. (The following image shows the situation of copying user policy.)



5. Select [Copy Policy] from the displayed pop-up menu.

6. Select user or user group as the copy target.

- When user is selected

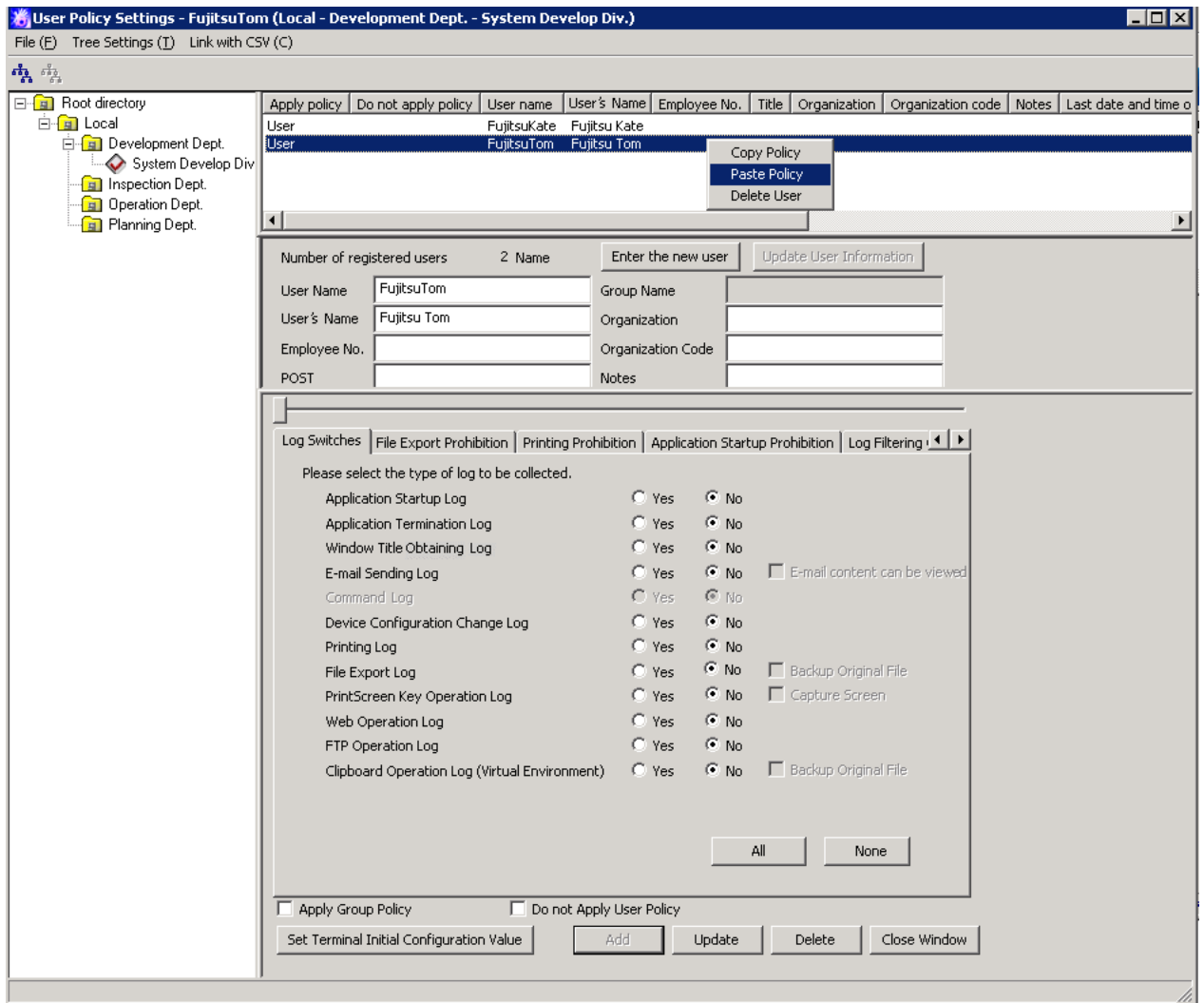
1. Select the user group with user registered as the copy target from the user group tree.
2. Select the user as copy target from [User List].

- When user group is selected

1. Select the user group as the copy target from the CT group tree.

7. Right-click on the selected user or user group.

→The pop-up menu is displayed. (The following image shows the situation of copying to user)



8. Select [Paste Policy] from the displayed pop-up menu.

→The confirmation window for policy copying is displayed.

9. Click the [Yes] button.

→ The copied policy will be updated during the next logon.

In addition, when the user of copy target logs on the client (CT), if the client (CT) policy is updated immediately, the copied user policy will be updated immediately.

### 3.3 Allocate CT/User to Group

If the configuration information tree has been created and the group policy of each group has been decided, CT and user will be allocated to groups.

The following are two ways that allocation of the CT and user to groups can occur:

- The system administrator allocates all CTs and users to groups.

- Set a department administrator to be responsible for allocating CTs and users to the group it manages. After a department administrator has been set, the responsibility of policy operation and log management within a section can be transferred to the department administrator, so that the workload of the system administrator can be reduced.

### 3.3.1 Add/Move/Delete CT

---

#### Add CT

When adding a new client (CT) in the Management Console, a client (CT) needs to be installed in the PC that is a managed target. The following are two methods for allocating to the CT group of the client (CT):

- Manually move the client (CT) under Root directory to a CT group
- Automatically allocate the client (CT) to a CT group using the automatic allocation file during CT registration

#### Manually move the client (CT) under root directory to a CT group

To add a new client (CT) in the CT group tree and CT list of the Management Console, install a CT in the PC that is the managed target. For more information about the installation of CT, please refer to “Install CT” of “Systemwalker Desktop Keeper Installation Guide”.

By rebooting the client (CT) after it has been installed, communication with the Master Management Server or Management Server will be enabled, and the client (CT) will be added to the CT group tree and CT list. Since the client (CT) is displayed under the Root directory at the time, please move it to the corresponding CT group.

For the location where the client (CT) is displayed in the CT group tree, please refer to “[Relationship between CT Group Policy and CT Policy](#)” or “[Display Configuration Information Tree](#)”.

For details on how to move the client (CT), please refer to “[Move CT](#)”.

#### Automatically allocate the client (CT) to CT group using the automatic allocation file during CT registration

Before installing the CT in the PC that is the managed target, the automatic allocation file during CT registration needs to be set. For methods of setting this, please refer to “[Create automatic distribution file during CT registration](#)”.



#### Note

---

#### Cause for the same CT being registered multiple times

When the same CT is registered multiple times under The Management Console, please consider the following causes.

[Cause 1]

When computer names are identical while the settings (MAC address, owner, and OS type) during CT registration in the system settings of the Server Settings Tool for the CT that has been registered are different, the CT has been installed (when the CT is installed after the MAC address has changed due to the exchange of LAN card)

[Cause 2]

When computer names are identical while the settings (MAC address, owner, and OS type) during CT registration in the system settings of the Server Settings Tool for the CT that has been registered are different, the command for re-registering CT is executed (when the command for re-registering CT is executed after the MAC address has changed due to the exchange of LAN card)

---

#### Move CT

This section describes how to move a client (CT) displayed in the CT list to a CT group of the CT group tree.

The client (CT) displayed in the following locations can only be moved by the system administrator:

- Under Root directory
- Under domain group
- Under Local group

In a system with a 3-level structure, when operating in a Management Console that is connected to the Master Management Server, the CT cannot be moved across Management Servers.

When importing configuration information from Active Directory, for the moving of CT, please refer to [“Display Configuration Information Tree”](#).

The procedure is as follows:

1. Start the [Management Console] window.
2. Select the CT group in which the client (CT) to be moved is registered, from the CT group tree.
3. Select the client (CT) to be moved from the CT list.
4. Move the client (CT) to the target CT group by drag&drop.  
→The client (CT) is moved.
5. Select [Reflect CT Group Structure] from the [Tree Settings] menu.  
→The moved CT will be updated to the database through [Reflect Structure].

When [Reflect CT Group Structure] is not executed, all the [Refresh Policy], [Update at Next Startup] and [Update Immediately] buttons are grayed out, and the message for reminding [Reflect CT Group Structure] is displayed.

## Delete CT

This section describes how to delete a CT that is displayed in the CT list.

The client (CT) displayed in the following locations can only be deleted by the system administrator.

- Under Root directory
- Under domain group
- Under Local group

When importing configuration information from Active Directory, for the deletion of CT, please refer to [“Display Configuration Information Tree”](#).

After a CT has been deleted, it will be moved to “Deleted CT” group

After a client (CT) has been deleted and the configuration information has been updated in the Management Console, the client (CT) will no longer be displayed in the Management Console.

At this time, the client (CT) will be moved to the “Deleted CT” group. The “Deleted CT” group usually not displayed. It will be displayed after the [Display “Deleted CT” Group] has been selected in the [Tree Settings] menu of the Management Console (operation can only be performed by system administrator). The “Deleted CT” group cannot be moved. In addition, a new group cannot be created under the “Deleted CT” group.

Since the management information of the client (CT) that has been moved to the “Deleted CT” group still remains in the (Master) Management Server, the accumulated logs can be viewed in the Log Viewer afterwards.

In addition, the client (CT) that has been moved to the “Deleted CT” group can be re-used. In this case, move the client (CT) of the “Deleted CT” group to another group. When linking with Active Directory, it can be moved to the Local group. Configuration information needs to be updated after moving.

For the client (CT) that has been deleted since it is considered as no needed, if logs need to be viewed in the Log Viewer, it is recommended to move to the “Deleted CT” group.

After the “Deleted CT” group has been deleted, CT cannot be restored

After the client (CT) that belongs to the “Deleted CT” group has been deleted and the configuration has been updated, the client (CT) will no longer be displayed in the “Deleted CT” group, and the management information will also be deleted from the (Master) Management Server. Therefore, the accumulated logs cannot be viewed in the Log Viewer. If the backup command is executed and the CSV file is output, log can still be confirmed.

In addition, to display the deleted client (CT) in the Management Console again, the CT needs to be uninstalled and re-installed in the target PC. For installation of CT, please refer to “Install CT” of “Systemwalker Desktop Keeper Installation Guide”.



However, the client (CT) displayed in the Management Console after re-installation will be regarded as a CT that is different from the deleted client (CT). Therefore, even it is displayed again, logs before deletion cannot be viewed in the Log Viewer.

The procedure is as follows:

1. Start the [Management Console] window.
2. Select the CT group in which the CT to be deleted is registered, from the CT group tree.
3. Select the CT to be deleted from the CT list, and then right-click on it.  
→A pop-up menu is displayed.
4. Select [Delete CT] from the displayed pop-up menu.  
→The window for confirming the deletion is displayed.
5. To delete, click the [OK] button.  
→The selected client (CT) is deleted.
6. Select [Reflect CT Group Structure] from the [Tree Settings] menu.  
→The deleted CT is moved to the “Deleted CT” group

When [Reflect CT Group Structure] is not executed, all the [Refresh Policy], [Update at Next Startup] and [Update Immediately] buttons are grayed out, and the message for reminding [Reflect CT Group Structure] is displayed.

When the CT belongs to the “Deleted CT” group, logs can be viewed in Log Viewer and CT can be restored to other groups.

7. Select the “Deleted CT” group in the configuration information tree.
8. Select the CT to be deleted from the CT list, right-click on it and select [Delete CT].
9. To delete, click the [OK] button.  
→The selected client (CT) is deleted.
10. Select [Reflect CT Group Structure] from the [Tree Settings] menu.  
→ Through updating configuration, the deleted CT will be updated to the database. CT cannot be restored.

When [Reflect CT Group Structure] is not executed, all the [Refresh Policy], [Update at Next Startup] and [Update Immediately] buttons are grayed out, and the message for reminding [Reflect CT Group Structure] is displayed.

### 3.3.2 Register a User

---

In order to allocate users to groups, users should be registered in the corresponding group.

When importing configuration information from Active Directory, for the registration of a user, please refer to “[Display Configuration Information Tree](#)”.



.....

#### **When managing user policies collectively, please operate from Master Management Server**

In the Server Settings Tool, when user policies are collective management, please add, update, move and delete users through the Master Management Server.

.....

The following are two methods for registering users:

- Register users one by one
- Register users collectively using CSV file

When Active Directory Linkage is not performed, up to 10000 cases can be registered at one operation.

When Active Directory Linkage is performed, up to 100000 cases can be registered under the Local group of configuration information tree at one operation.

It is necessary to have [Import CSV File] authority for the Management Console during operation. The setting of authority is performed in the [Detail authority] of the [Administrator information settings] window of the Server Settings Tool.

The CSV file of allocated user information should be created in advance. For details on the CSV file, please refer to “User Information” of “Systemwalker Desktop Patrol Reference Manual”.

## Note

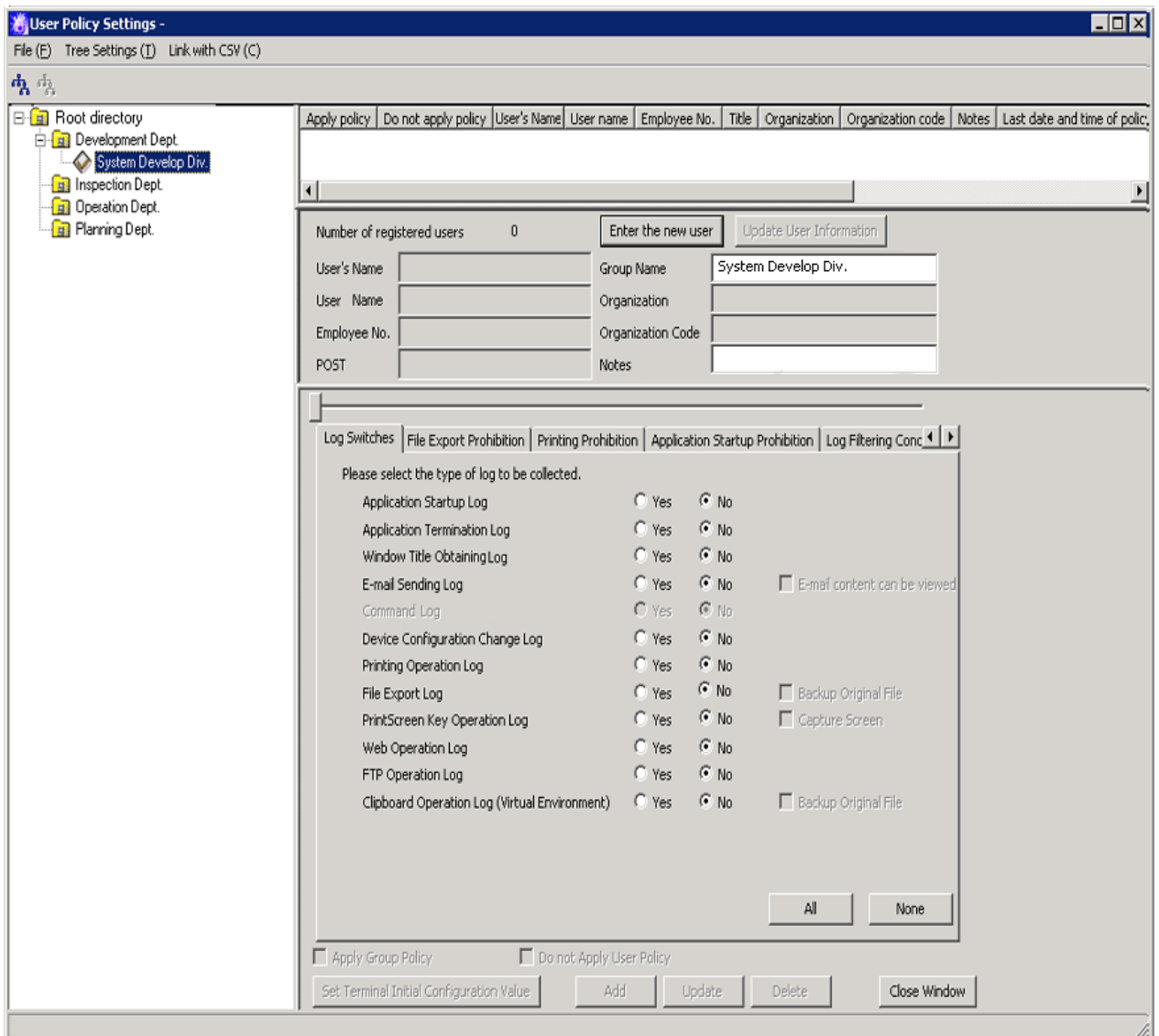
### Please set registration information correctly

Please set registration information correctly in the CSV file. When the CSV file is not created according to the following description, even if error exists in one line, none of the users be registered (the part with correct setting will not be registered at the end of processing). Therefore, all users need to be registered again.

## Register Users One by One

The procedure is as follows:

1. Start [Management Console].
  2. Select [User Policy Settings] from the [User Settings] menu.
- The [User Policy Settings] window is displayed.



Nothing will be displayed in the user list and user properties.

The initial value that is set in the each tab of [Terminal Initial Settings] window will be displayed in the user policy list.

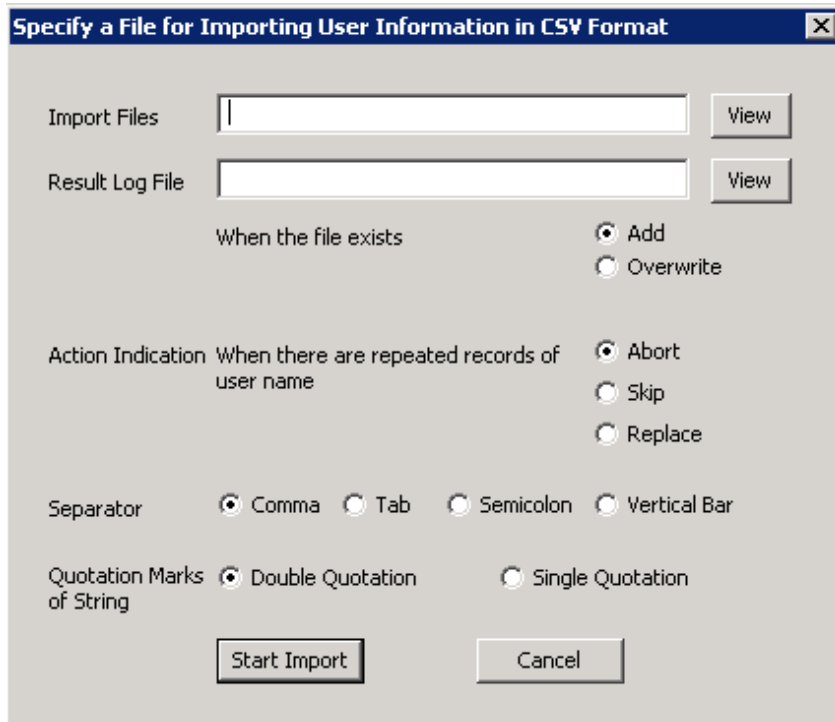
The collection of following logs cannot be set as user policy. Therefore, in the [Log Switches] tab of the [User Policy Settings] window, the buttons for collecting these logs do not exist. When collecting the following logs, please set it as CT policy.

- File Operation Log
  - Logon/Logoff Log
  - Linkage Application Log
3. Select the user group with users to be registered from the user group tree.
  4. Click the [New user] button of user properties.
  5. Enter the required information into user properties and click the [Add] button.  
For details of input information, please refer to “[User Properties](#)”.
  - The value of terminal initial settings is set as user policy and the confirmation window is displayed.
  6. Click the [OK] button.

### Register Users Collectively Using CSV File

This section describes how to allocate users collectively using the CSV file.

1. Start [Management Console].
2. Select [User Policy Settings] from the [User Settings] menu.  
→ The [User Policy Settings] window is displayed.
3. Select [Import User Information in CSV Format] of the [Link with CSV] menu  
→ The [Specify a File for Import User Information in CSV Format] window is displayed.



Item Name	Description
[Import Files] (Required)	Specify the created CSV file. The specification method is as follows:

Item Name	Description
	<ul style="list-style-type: none"> <li>- Enter the file name with full path</li> <li>- Enter the full path of a CSV file in the input field.</li> <li>- Enter by the [View] button</li> <li>- When the [Specify an imported file] window is displayed, click the [Open] button after the imported CSV file has been specified.</li> </ul> <p>The maximum length of the full path is 218 characters. In addition, the following symbols cannot be used in a file name: “\” “/” “:” “*” “?” “#” “&lt;” “&gt;” “ ”</p>
[Result Log File] (Required)	<p>Specify the file for outputting execution result when importing CSV files. Errors during import will also be output to this file. The specification method is as follows:</p> <ul style="list-style-type: none"> <li>- Enter the file name with full path</li> <li>- Enter the full path up to the output log file in the input field.</li> <li>- Enter by the [View] button</li> <li>- When the [Specify result log file] window is displayed, click the [Open] button after the output log file has been specified.</li> </ul> <p>The maximum length of the full path is 218 characters. In addition, the following symbols cannot be used in a file name: “\” “/” “:” “*” “?” “#” “&lt;” “&gt;” “ ”</p>
[When the file exists] (Required)	<p>In [Specify result log file], select an output method when the log output file has already been specified:</p> <ul style="list-style-type: none"> <li>- [Add] Add operation log in case when the previous information still remains.</li> <li>- [Overwrite] Delete the remaining information and output the operation log to a new file.</li> </ul>
[Action Indication When there are repeated records of user name] (Required)	<p>Select one of the following operations if duplicate [User Name] exists when importing a CSV file:</p> <ul style="list-style-type: none"> <li>- [Abort] When there are duplicated [User Name], suspend the import operation. The user information before suspension will be imported.</li> <li>- [Skip] Only the duplicated [User Name] will not be imported. Instead, user information of unduplicated [User Name] will be imported.</li> <li>- [Replace] Use imported information to update the information of duplicated [User Name]. The user information of [User Name] that is not duplicated in the CSV file is imported normally. In addition, when duplicates exist, the user information will be replaced by the information in a CSV file while the user policy will not be changed.</li> </ul>
[Separator] (Required)	<p>Select the separator that has been input when creating a CSV file. An error may occur in the case of wrong selection.</p>
[Quotation marks of String] (Required)	<p>Select the quotation of string that has been input when creating a CSV file. The following problems may occur in the case of wrong selection:</p> <ul style="list-style-type: none"> <li>- If a double quotation is used during the creation of a CSV file, but the single quotation is selected here, an error will occur.</li> <li>- If a single quotation is used during the creation of a CSV file, but double quotation is selected here, the single quote will be considered as part of user information to be registered.</li> </ul>

4. After entering all the above information, click the [Start Import] button.
  - The [Display the Status of Importing User Information in CSV Format] window is displayed and the import of CSV files starts. If an error occurs, it will be displayed in the [Display the Status of Importing User Information in CSV Format] window. In addition, the same content will also be output to the operation log file. After the error has been confirmed and corrected, please register all the user information again.
5. Return to the [User Policy Settings] window, and click the [Refresh] button.
  - The user information imported from the CSV file is displayed.

### 3.3.3 Update/Move/Delete User

---

#### Update a User

The following are two methods of updating:

- Update through a CSV file
- Update through a window

#### Update through a CSV file

For method of updating, please refer to “[Register Users Collectively Using CSV File](#)”.

#### Update through a window

The procedure is as follows:

1. Start [Management Console].
2. Select [User Policy Settings] from the [User Settings] menu.
  - The [User Policy Settings] window is displayed.
3. The user information can be updated by any of the following method.
  - When updating users one by one
  - When updating multiple users simultaneously

[When updating users one by one]

- a) Select the line to be updated from the [User List], and click the [Update] button after the following information has been entered. The [User Name] cannot be updated.

Item Name	Description
[User's Name]	Enter the name of the user that uses the user name Up to 128 single-byte characters (64 double-byte characters) can be entered.
[Employee No.]	Enter the employee number of the user that uses the user name. Up to 40 single-byte characters (20 double-byte characters) can be entered.
[POST]	Enter the title of the user that use the user name Up to 128 single-byte characters (64 double-byte characters) can be entered.
[Organization]	Enter the organization to which the user that uses the user name belongs. Up to 128 single-byte characters (64 double-byte characters) can be entered.

Item Name	Description
[Organization Code]	Enter the organization code to which the user that uses the user name belongs. Up to 40 single-byte characters (20 double-byte characters) can be entered.
[Notes]	Enter the notes of the user that uses the user ID Up to 128 single-byte characters (64 double-byte characters) can be entered.

b) After the confirmation window is displayed, click the [OK] button.

→The input information is updated to the database and displayed in [User List].

[When updating multiple users simultaneously]

Select the lines to be updated from the [User List] by pressing the [Shift] or [Ctrl] key, and click the [Update User Information] button after the following information has been entered.

- [POST]
- [Organization]
- [Organization Code]
- [Notes]

[User's Name], [User Name] and [Employee No.] cannot be updated.

For items without information being updated, the information displayed in current [User List] will remain unchanged.

However, when a single-byte or double-byte space is entered, it will be updated with a space  
Please refer to the table of "[When updating users one by one]" for input value.

→The input information is updated to the database and displayed in [User List].

## Move a User

When moving a user, the user policy will not be changed. (Same as the condition before moving)

The procedure is as follows:

1. Start the [User Policy Settings] window.
2. From the user group tree, select the user group to which the user needs to be moved belongs.  
→ The selected user group is highlighted.
3. Move the user to be moved to the target user group under the same server through drag&drop.  
→The user is moved.
4. Select [Reflect User Group Structure] from the [Tree Settings] menu.  
→The moved user is updated to the database.

If [Reflect User Group Structure] is not executed, the message for reminding [Reflect User Group Structure] will be displayed when closing the [User Policy Settings] window.

## Delete a User

This section describes how to delete a registered user.

The procedure is as follows:

1. Start [Management Console].
2. Select [User Policy Settings] from the [User Settings] menu.  
→ The [User Policy Settings] window is displayed.

3. Select the line to be deleted from the [User List] and click the [Delete] button.  
→The confirmation window is displayed.
4. Click the [OK] button.  
→The deleted information is updated to the database and deleted from [User List].

## **3.4 Modify CT Policy/User Policy**

---

After creating the configuration information tree, modify the policy of the CT and user that are allocated to groups as needed.

The following are two ways to modify policy:

- The system administrator modifies the policy.
- Set a department administrator to be responsible for modification of policy for the group that he or she manages.

### **3.4.1 Modify CT Policy**

---

#### **Modify CT Policy**

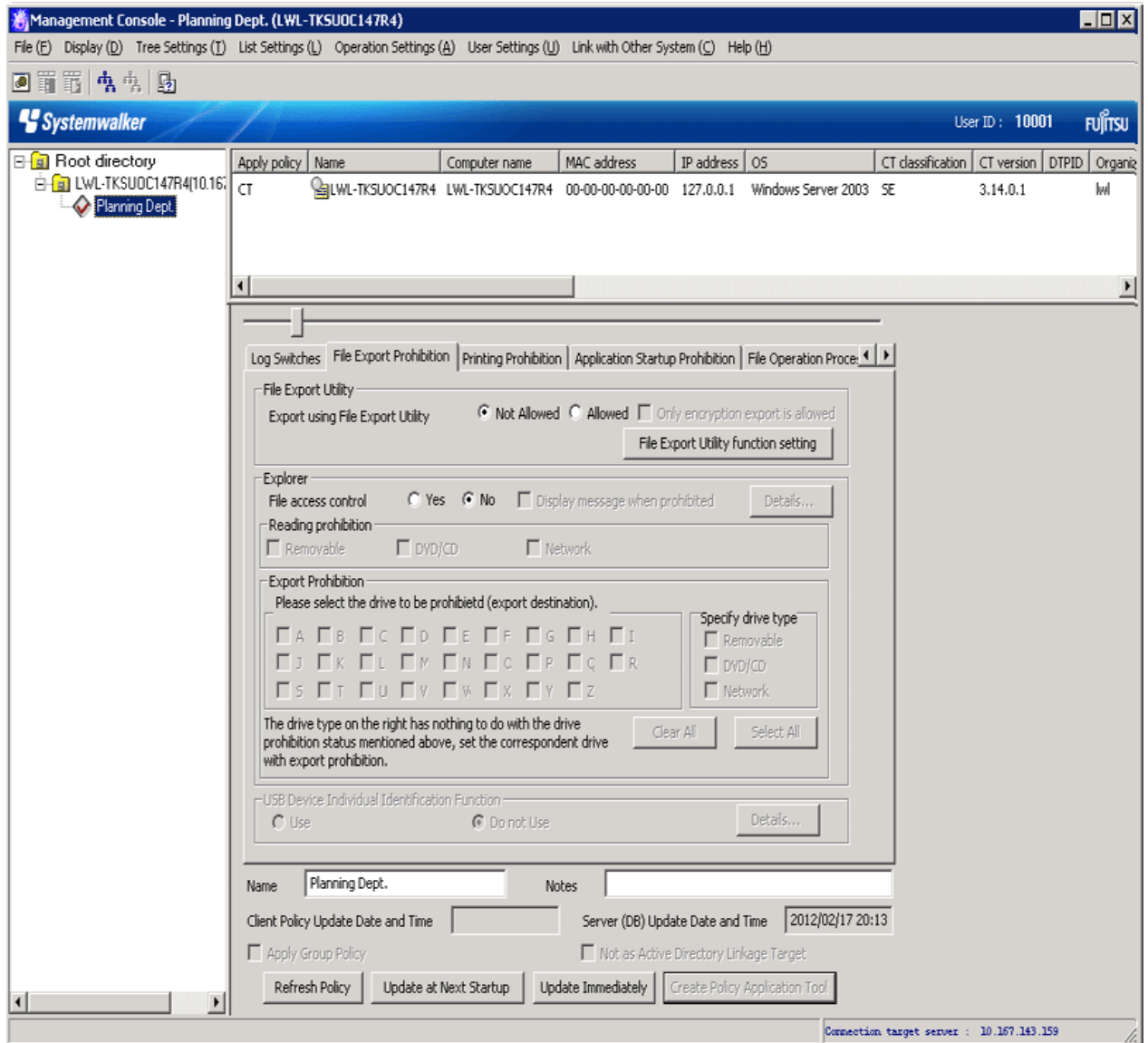
The CT policy of the client (CT) that belongs to the “Deleted CT” group cannot be changed. The name and notes cannot be modified as well.

The following describes the procedure of modifying CT policy:

1. Start [Management Console].

2. Select the CT group to which the CT that requires modification of policy belongs from the CT group tree.

→The latest policy information is displayed.



## Note

### In following cases, please update the information of CT group and CT list

When any of the following conditions is satisfied, the information of the CT group or CT list of the Management Server under the Master Management Server displayed in the window may not be updated.

- When the CT group tree is modified at Management Server side
- When Active Directory Linkage is performed and the group tree is modified

Please select [Refresh Tree] from the [Tree Settings] menu to update.

3. Select the CT that requires change of policy from the CT list.
4. Modify policy in each tab of the policy list.

For description of policy setting items, please refer to “[2.4.1 Perform Terminal Initial Settings](#)”.



5. Modify the [Name] or [Notes] displayed in the CT list as needed.

Characters that can be entered in [Name] and [Notes] are as follows.

- [Name]: Up to 40 single-byte characters (20 double-byte characters) including alphanumeric characters, Chinese characters, Hiragana and Katakana can be entered.
- [Notes]: Up to 127 single-byte characters (63 double-byte characters) including alphanumeric characters, Chinese characters, Hiragana and Katakana can be entered.

6. Click any of the following buttons to update policy to the CT.

- When clicking the [Update at Next Startup] button

The policy of each tab will be updated to the database, but it will not be updated to the client (CT) immediately. Instead, the latest policy will be updated at the next time when the client (CT) is started and communicates with the target server (Master Management Server or Management Server).

- When clicking the [Update Immediately] button

- The policy of each tab will be updated both in database and the running the client (CT).

However, the setting of [File Export Prohibition] tab will update policy at the next startup of file export utility when the file export utility has been started at the client (CT) on which the immediate update is performed.

- When the application permitted in the [Printing Prohibition] tab has already been started in the client (CT) on which the immediate update is performed, policy will be updated at next application startup.

- When logoff or shutdown has been set in the [Logon Prohibition] tab, it will be updated to the running client (CT). In addition, for the client (CT) that is not running and the client (CT) that is unable to communicate with the upper level server, the latest policy will be updated at the next time when the client (CT) is started and communicates with the target server (Master Management Server or Management Server).



.....  
**When there are a large number of clients (CTs) in a CT group, it is recommended to select [Update at Next Startup]**

The timeout period for the connection of a client (CT) that is not connected to the Master Management Server or Management Server is 5 seconds for each client (CT). In addition, in spite of dependence on network environment, when performing [Update Immediately] for the client (CT) that is connected to Master Management Server or Management Server, the time required for each client (CT) to apply policy is approximately 1 second.

Therefore, when there are a large number of CTs that are the target for policy setting, it is recommended to click the [Update at Next Startup] button.

.....  
→ When [Name] or [Notes] have been modified, after the policy is updated, the input information will be updated to CT list.

#### When applying group policy to client (CT)

Even if the CT policy is not applied to the client (CT), the group policy of the CT group to which the client (CT) belongs can still be applied. At this time, please select the [Apply Group Policy] checkbox to perform the policy update.

#### Select a CT group to collectively modify its subordinate CT policies

When setting CT group policy, policy can also be set collectively for the subordinate client (CT) under the CT group. In this case, the configuration value of CT policy is the same as the value of CT group policy.

For details of the setting procedure, please refer to “[3.2.1 Modify CT Group Policy](#)”.

### Copy CT Policy

The policy that has been set for the client (CT) or CT group policy can be copied to another client (CT) or CT group.

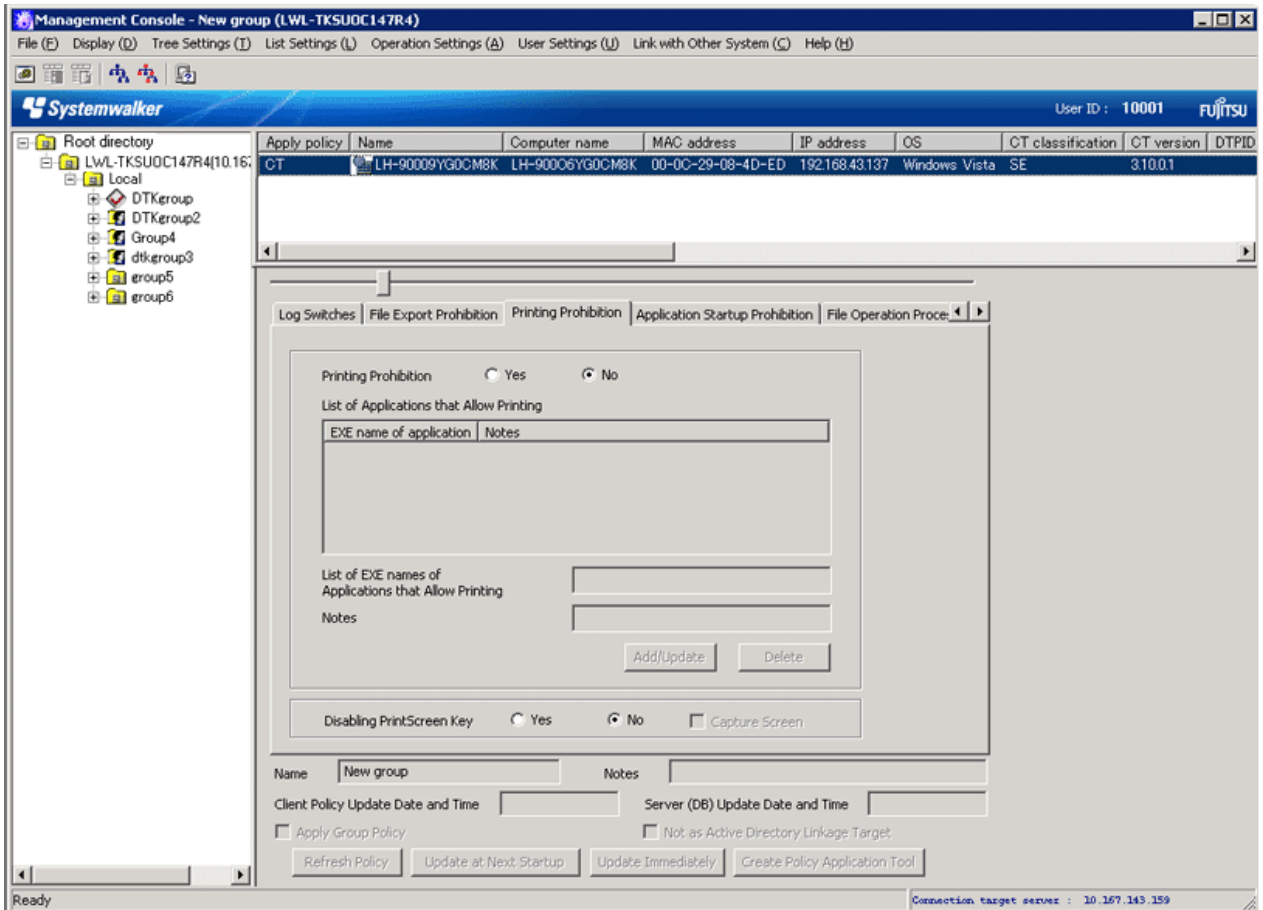
Please refer to “Copy CT Group Policy or CT Policy” for setting method.

## Create Policy Application Tool

The tool that modifies the CT policy of the client (CT) that cannot connect to Management Server can be created.

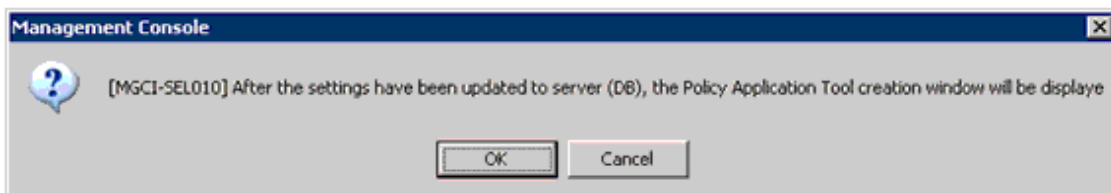
The procedure is shown as follows:

1. Start [Management Console].
2. Select the client (CT) to create the policy application tool.



3. Click the [Create Policy Application Tool] button.

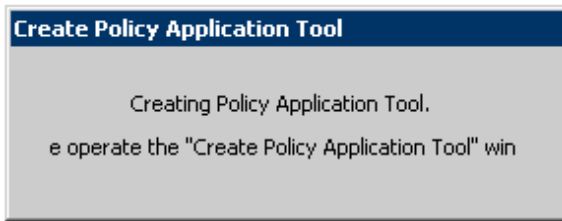
→The confirmation window is displayed.



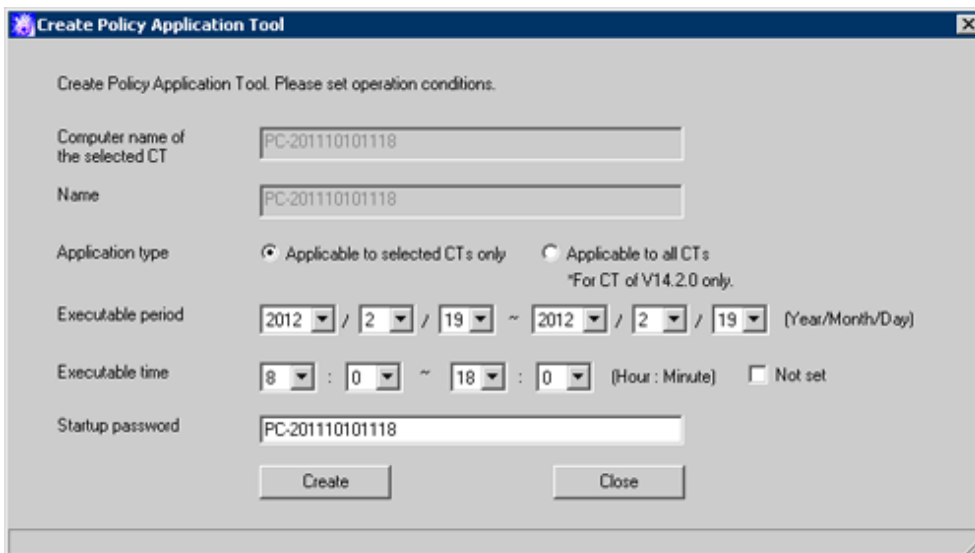
4. Click [OK] to display the policy creation window, and click [Cancel] to cancel the policy creation.

## Point

After [OK] is selected, the following window will be displayed in [Management Console]. During this period, the Management Console cannot be operated.



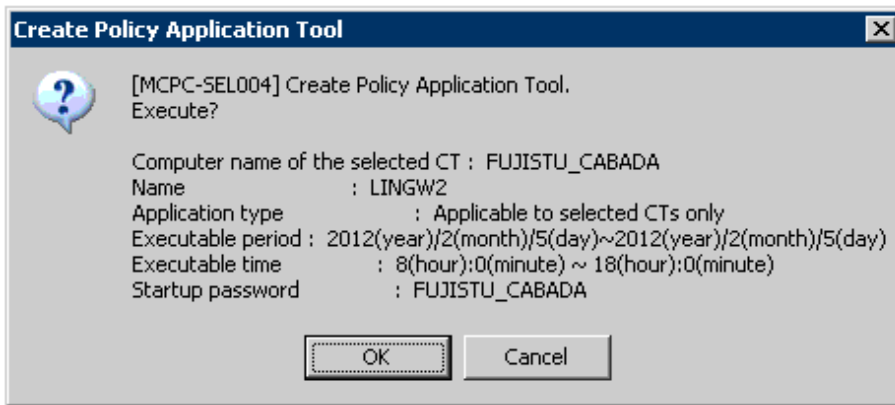
5. Perform setting in the [Create Policy Application Tool] window.



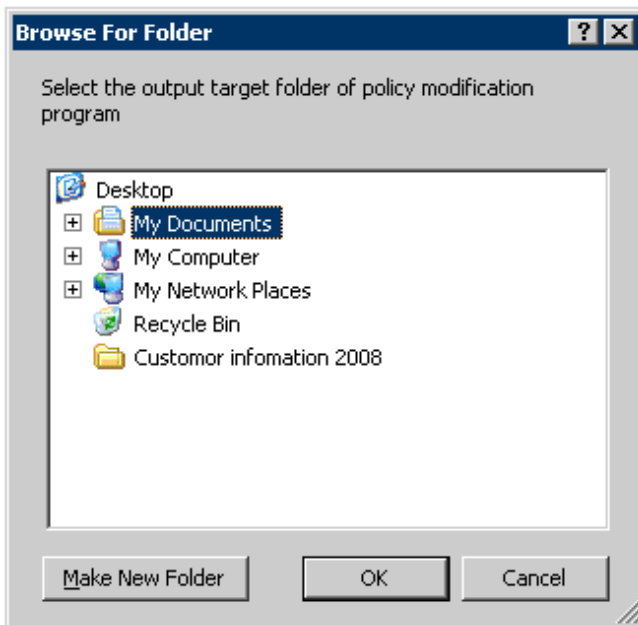
Item Name	Description
[Computer name of the selected CT]	Display the computer name of the selected client (CT). It cannot be modified.
[Name]	Display the name of the selected client (CT). It cannot be modified.
[Application type]	Select the range of the client (CT) on which the policy application tool can be executed. <ul style="list-style-type: none"> <li>- Applicable in the selected computer only Policy application tool can be executed in the selected client (CT) only.</li> <li>- Applicable in all computers Policy application tool can be executed in all clients (CTs).</li> </ul>
[Executable period]	Specify the period in which the policy application tool can be executed. The period can be specified is as follows. Year: 2000-2037 Month: 1-12 Day: 1-31
[Executable time]	Specify the time in which the policy application tool can be executed. The time can be specified is as follows. Hour: 0-23 Minute: 0-50 (in 10 mins) If [Not set] is ON, this setting will be invalid and only the period will be determined.

Item Name	Description
[Startup password]	Set the password entered when booting the policy application tool. <ul style="list-style-type: none"> <li>- Up to 32 bytes can be entered.</li> <li>- Only single-byte characters are allowed.</li> <li>- It is case sensitive.</li> <li>- The following characters cannot be used: &amp;, \, :, ?, ", ~, ^, ', &lt;, &gt;,  , and single-byte space.</li> </ul>

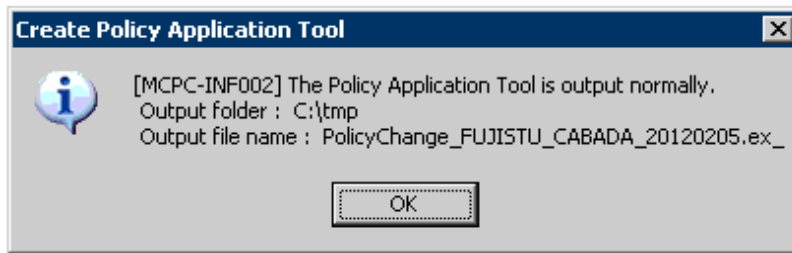
6. Please click the [Create] button.  
 → The following confirmation window is displayed.



7. Please select the [OK] button if there is no problem.  
 →The following window is displayed. Please select the destination for saving the policy application tool.



8. After the saving destination is selected, please select the [OK] button. The following window is displayed.



9. Please click the [OK] button to exit [Create Policy Application Tool].

10. Copy the saved policy application tool to the client (CT). For how to execute the policy application tool, please refer to “Apply Offline Policy” of “Systemwalker Desktop Keeper - User's Guide: For Client”.

### Note

#### **When executing policy application tool in the PC with valid user policy**

When the policy application tool is executed in the PC with valid user policy, though the CT policy can be modified, the user policy cannot be modified.

## 3.4.2 Modify User Policy

---

### Modify User Policy

The following are three methods for modifying user policy:

- Modify user policy one by one
- Select multiple users to modify user policy collectively
- Select the user group to modify its subordinate user policy collectively

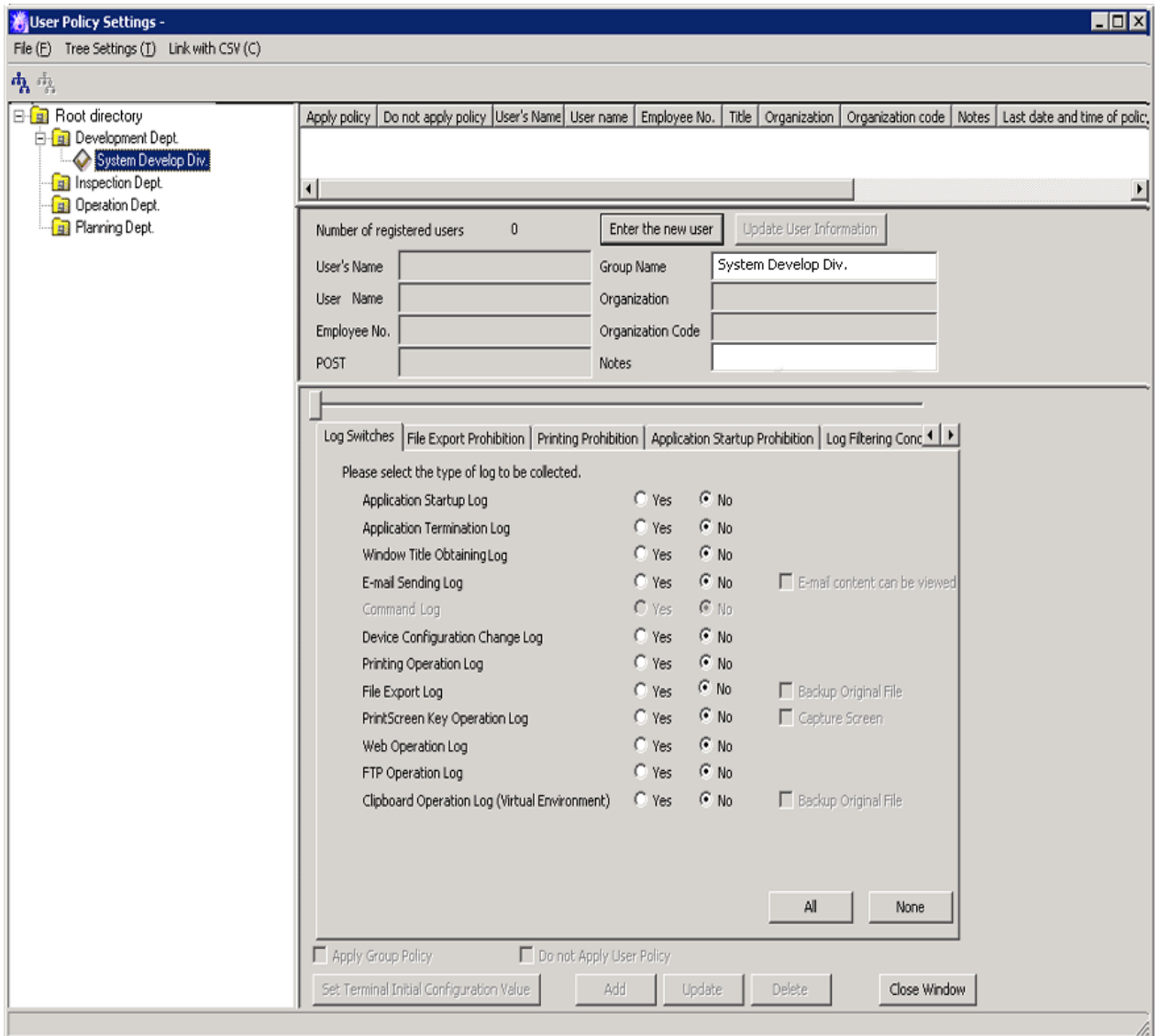
#### Modify user policy one by one

The procedure is as follows:

1. Start [Management Console].

2. Select [User Policy Settings] from the [User Settings] menu.

→The [User Policy Settings] window is displayed.



When modifying [User's Name], [Employee No.], [POST], [Organization], [Organization Code] and [Notes], the modified value will be updated as the information of that [User Name]

3. Modify policy in each tab of the policy list.

The user specific policy can be set. For description of policy setting items, please refer to “[2.4.1 Perform Terminal Initial Settings](#)”.

- When setting the value of the [Terminal Initial Settings] window, please click the [Set Terminal Initial Configuration Value] button. For the [Terminal Initial Settings] window, please refer to “[2.4.1 Perform Terminal Initial Settings](#)”.
- When applying the user group policy of the user group to which the user belongs, please select the [Apply Group Policy] checkbox. (This is also applicable when multiple users are selected.)
- To temporarily cancel the application of user policy and apply the CT policy, please select the [Disable User Policy] checkbox. To apply the user policy again, please cancel the selection.

4. Click the [Update] button.

→The set policy will be updated at the next time of logon.

In addition, when the user with modified policy has already logged on to the client (CT), if immediate update of CT policy is executed for this client (CT), the modified user policy will be updated immediately.

### Select multiple users to modify user policy collectively

The procedure is as follows:

1. Start [Management Console].
2. Select [User Policy Settings] from the [User Settings] menu.  
→The [User Policy Settings] window is displayed.
3. Select the lines that require policy setting from the [User List] by pressing the [Shift] or [Ctrl] key.  
→The value of the [Terminal Initial Settings] is set in policy.  
Mask input cannot be performed in [User Name], [User's Name] and [Employee No.].  
The value of [POST], [Organization], [Organization Code] and [Notes] are not specified (not set).  
For the [Terminal Initial Settings] window, please refer to "[2.4.1 Perform Terminal Initial Settings](#)".
4. Modify policy in each tab of the policy list.  
For description of policy setting items, please refer to "[2.4.1 Perform Terminal Initial Settings](#)".
5. Click the [Update] button.  
→The set policy will be updated at the next time of logon.  
When the [Update] button is clicked after values have been input into [Title], [Organization], [Organization Code] and [Notes], the input value will be set for all the selected users. In addition, when a single-byte or double-byte space is entered, it will be updated with a space.

### Select the user group to modify its subordinate user policy collectively

During the setting of user group policy, policy can be set collectively for the users under that user group.  
For details of the setting procedure, please refer to "[3.2.2 Modify User Group Policy](#)".

## Copy User Policy

The policy that has been set for a user group or a user can be copied to another user group or user.  
For details of the setting method, please refer to "[Copy User Group Policy or User Policy](#)".

## 3.5 Export CT information/User information

---

According to the results of log viewing, if the existence of the client (CT) and user that perform violation is confirmed, the search result of client (CT) information and user information can be exported in CSV format.

The following section describes how to export the information displayed in the CT list of The Management Console, CT policy information and user information of user policy to CSV files.

### Export CT Information

This section describes how to export the information displayed in the CT list of the Management Console to a CSV file.

The users who satisfy all the following conditions can perform the operation:

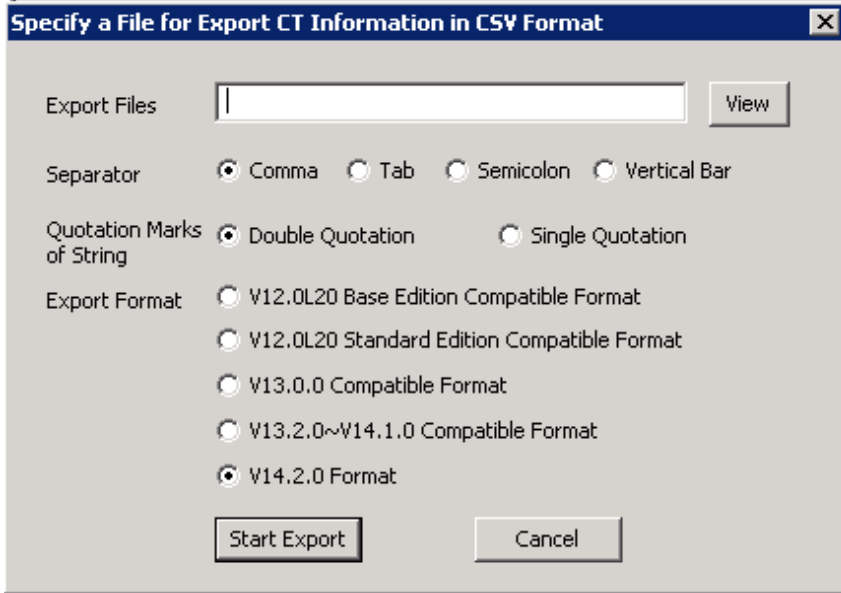
- Registered as system administrator or department administrator.
- Have the authority to access the Management Console.
- Have the authority to save CSV files.

The settings of all these conditions are configured in the Server Settings Tool during installation.

The CT information that belongs to the "Deleted CT" group cannot be exported to CSV files.

The procedure is as follows:

1. Start [Management Console].
2. Select [Export CT Information in CSV Format] from the [File] menu.  
→ The [Specify a File for Export CT Information in CSV Format] window is displayed.



3. After entering the following information, click the [Start Export] button.

Item Name	Description
[Export Files]	<p>Specify the CSV file for export. The specification method is as follows:</p> <ul style="list-style-type: none"> <li>- Enter a file name with full path Enter the full path of imported CSV file in the input field.</li> <li>- Enter by clicking the [View] button The [Specify an Export File] window is displayed, after entering the drive and the file name of the CSV file to be exported, click the [Save] button.</li> </ul> <p>The length of the full path should be within 218 characters. The following symbols are not allowed in a file name: “\” “/” “.” “*” “?” “ ” “&lt;” “&gt;” “ ”</p>
[Separator]	Select the Separator when the CSV file is exported.
[Quotation Marks of String]	Select the String Quotation when the CSV file is exported.
[Export Format]	<p>Select the format of the exported CSV file.</p> <p>[V12.0L20 Base Edition Compatible Format]: Export in V12.0L20 Base Edition format.  [V12.0L20 Standard Edition Compatible Format]: Export in V12.0L20 Standard Edition compatible format  [V13.0.0 Compatible Format]: Export in V13.0.0 format.  [V13.2.0~V14.1.0 Compatible Format]: Export in V13.2.0 format.  [V14.2.0 Format]: Export in format of V14.2.0 or later.</p> <p>For item names of the exported CSV file and exported information, please refer to “CT Information” of “Systemwalker Desktop Keeper Reference Manual”.</p>

→ The CSV file is exported.



Among the exported items, if there is a character that is identical to the one selected in the [String Quotation], one character selected in [Quotation Marks of String] will be added in front of that character.

When a file with same name exists in the export destination, the window for selecting whether to overwrite will be displayed. To overwrite, please click the [OK] button.

## Export CT Group Information

This section describes how to export the information displayed in the CT group tree of the Management Console to CSV files.

The users who satisfy all the following conditions can perform the operation. The settings of all these conditions are configured in Server Settings Tool during installation.

- Registered as system administrator.
- Have the authority to access The Management Console.
- Have the authority to save CSV files.

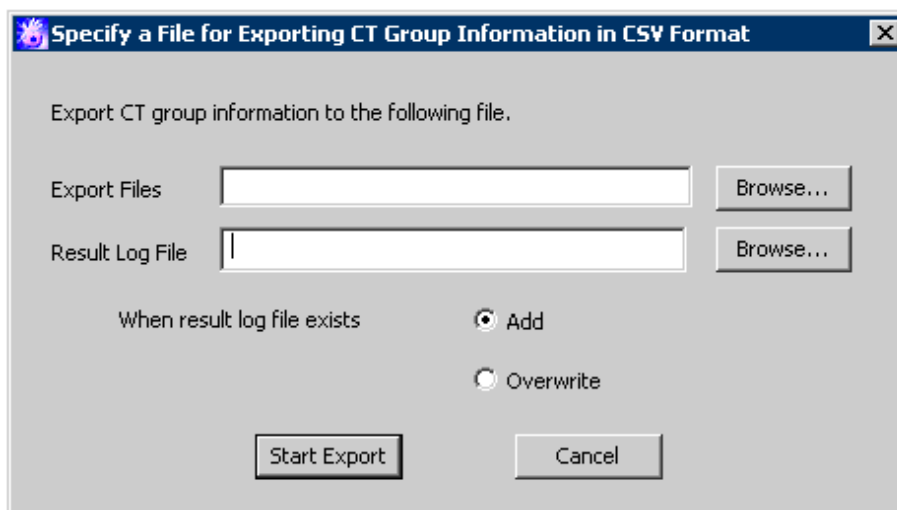
CT group information can be exported to every Management Server.

When CT group information is exported from the Management Server that connects to the Master Management Server, the group information of the client (CT) under the Master Management Server will be exported.

When linking with Active Directory, only the information of the Local group can be exported.

The Procedure is as follows:

1. Start [Management Console].
2. Select [Export CT Group Information in CSV Format] from the [File] menu.  
→ The [Specify a File for Exporting CT Group Information in CSV Format] window is displayed.



3. After entering the following information, click the [Start Export] button.

Item Name	Description
[Export Files] (Required)	Specify the CSV file for exporting CT group information with a full path. The length of the full path should be within 218 characters. The following symbols are not allowed in a file name: “\” “/” “:” “*” “?” “ ” “<” “>” “ ” - When it is not Windows Vista®, Windows® 7 or Windows Server® 2008 <b>Initial Value:</b> [OS Installation Drive]\Documents and Settings\Logon User Name\My Documents\DTKCTEntry.csv

Item Name	Description
	- When it is Windows Vista®, Windows® 7 or Windows Server® 2008 <b>Initial Value:</b> [OS Installation Drive]\User\Logon User Name \Documents \DTKCTEntry.csv
[Result Log File] (Required)	Specify the file for saving the execution result with a full path. Up to 218 single-byte characters can be entered. However the following symbols are not allowed in a file name: “\” “/” “.” “*” “?” “ ” “<” “>” “ ” - When it is not Windows Vista®, Windows® 7 or Windows Server® 2008 <b>Initial Value:</b> [OS Installation Drive]\Documents and Settings\Logon User Name\My Documents\DTKCTEntry.log - When it is Windows Vista®, Windows® 7 or Windows Server® 2008 <b>Initial Value:</b> [OS Installation Drive]\User\Logon User Name \Documents \DTKCTEntry.log
[When result log file exists]	When the original result log file exists, please make sure to set it. - [Add]: Select to add new files to the original result log file. - [Overwrite]: Select to overwrite the original result file.

→ The CSV file is exported.

For item names of the exported CSV file and exported information, please refer to “CT Group Information” of “Systemwalker Desktop Keeper Reference Manual”.

## Export User Information

The following section describes how to export the information that is displayed in the user list of the [User Policy Setting] window in CSV format.

The users who satisfy all the following conditions can perform the operation:

- Registered as system administrator or department administrator.
- Have the authority to access the Management Console.
- Have the authority to save CSV files.

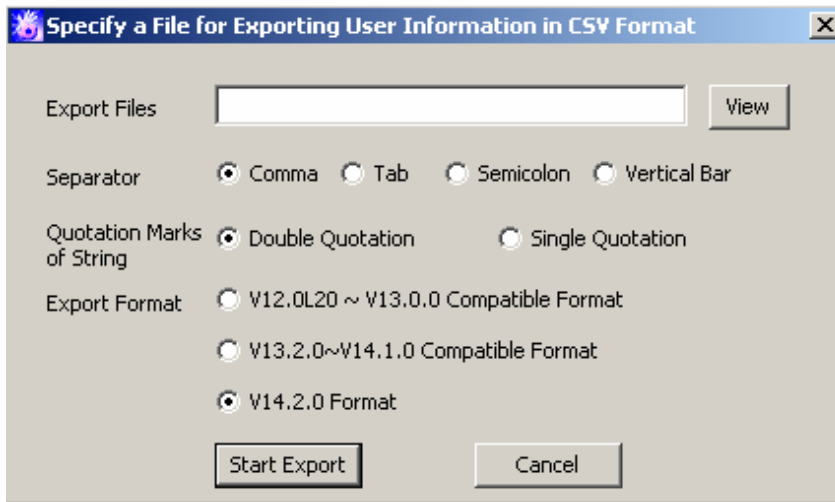
The settings of all these conditions are performed in the Server Settings Tool during installation.

The procedure is as follows:

1. Start [Management Console].
2. Select [User Policy Settings] from the [User Settings] menu.

→The [User Policy Settings] window is displayed.

3. Select [Export User Information in CSV Format] from the [Link with CSV] window  
→ The [Specify a File for Exporting User Information in CSV Format] window is displayed.



4. After entering the following information, click the [Start Export] button.

Item Name	Description
[Export Files] (Required)	Specify the CSV file for export. The specification method is as follows: <ul style="list-style-type: none"> <li>- Enter a file name with full path Enter the full path of imported CSV file in the input field.</li> <li>- Enter by clicking the [View] button The [Specify an Export File] window is displayed, after entering the drive and the file name of the CSV file to be exported, click the [Save] button.</li> </ul> <p>The length of the full path should be within 218 characters. The following symbols are not allowed in a file name:  “\” “/” “:” “*” “?” “ ” “&lt;” “&gt;” “ ”</p>
[Separator] (Required)	Select the Separator when the CSV file is exported.
[Quotation Marks of String] (Required)	Select the String Quotation when the CSV file is exported.
[Export Format]	Select the format of the exported CSV file. [V12.0L20 ~ V13.0.0 Compatible Format]: Export in the format that is same as V13.0.0 or earlier. [V13.2.0 ~ V14.1.0 Compatible Format]: Export in V13.2.0 format. [V14.2.0 Format]: Export in format of V14.2.0 or later. For the item name of the exported CSV file and exported information, please refer to “User Information” of “Systemwalker Desktop Keeper Reference Manual”.

→The CSV file is exported.

Among the exported items, if there is a character that is identical to the one selected in [String Quotation], one character selected in [String Quotation] will be added in front of that character.

When a file with same name exists in the export destination, the window for selecting whether to overwrite will be displayed. To overwrite, please click the [OK] button.

## Export IP Address of Client (CT)

In following cases, the client (CT) with self version upgrade can be selected. The IP address of client (CT) under the server or CT group is exported as the format of file to be used at the time.

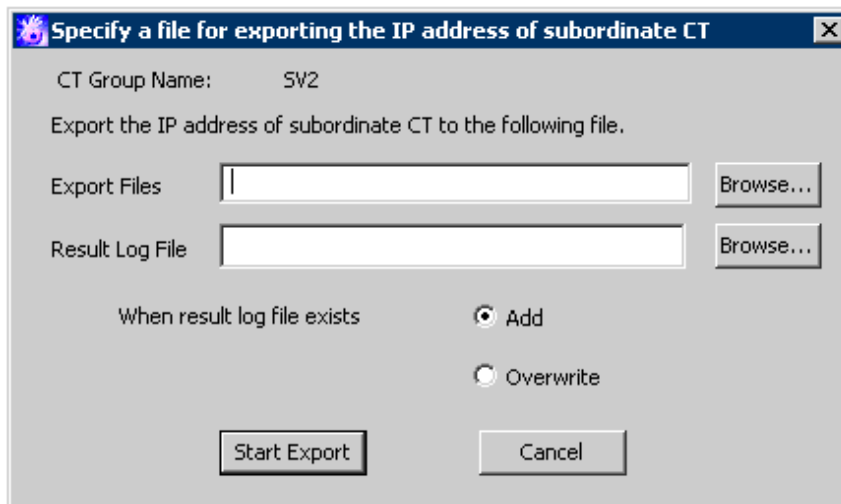
- When the administrator expects to test in a specific department before fully carrying out version upgrade for the client (CT)
- When the administrator expects to perform a version upgrade for the client (CT) in sequence at each department and office
- When the administrator expects to divide the number of clients (CTs) for version upgrade for the purpose of distributing the load

For details on how to use the exported file, please refer to “Upgrade CT Version” of “Systemwalker Desktop Keeper Installation Guide”.

In addition, the system administrator and department administrators can also confirm the managed PC in the CT group unit.

The procedure of exporting file is as follows:

1. Start [Management Console], and select a server or CT group in the CT group tree.
2. Select [Output IP Address of Subordinate CT] from the [File] menu.  
Or right-click on a server or a CT group and select [Output IP Address of Subordinate CT].  
→ The [Specify a file for exporting the IP address of subordinate CT] window is displayed.



- **[Export Files]** (Required): Specify the CSV file for exporting IP address with full path.  
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in a file name.  
“\” “/” “:” “\*” “?” “” “|” “<” “>” “|”
  - **[Result Log File]** (Required): Specify the file for saving the execution result with full path.  
Up to 218 single-byte characters can be entered. However the following symbols are not allowed in a file name.  
“\” “/” “:” “\*” “?” “” “|” “<” “>” “|”
  - **[When result log file exists]:** When the original result log file exists, please make sure to set it.  
**[Add]:** Select to add new files to the original result log file.  
**[Overwrite]:** Select to overwrite the original result file.
3. Set the above information and click the [Start Export] button.  
For the item name of exported CSV file and exported information, please refer to “IP Address Export File of CT under a Group” of “Systemwalker Desktop Keeper Reference Manual”.

## 3.6 Control Client (CT)

The system administrator must control the client (CT) on which violation has been detected.

Modify the service status of the client (CT) and end the process.

## 3.6.1 Control Services of Client (CT)

---

This section describes how to view and control the services registered in the client (CT).

### View Service List

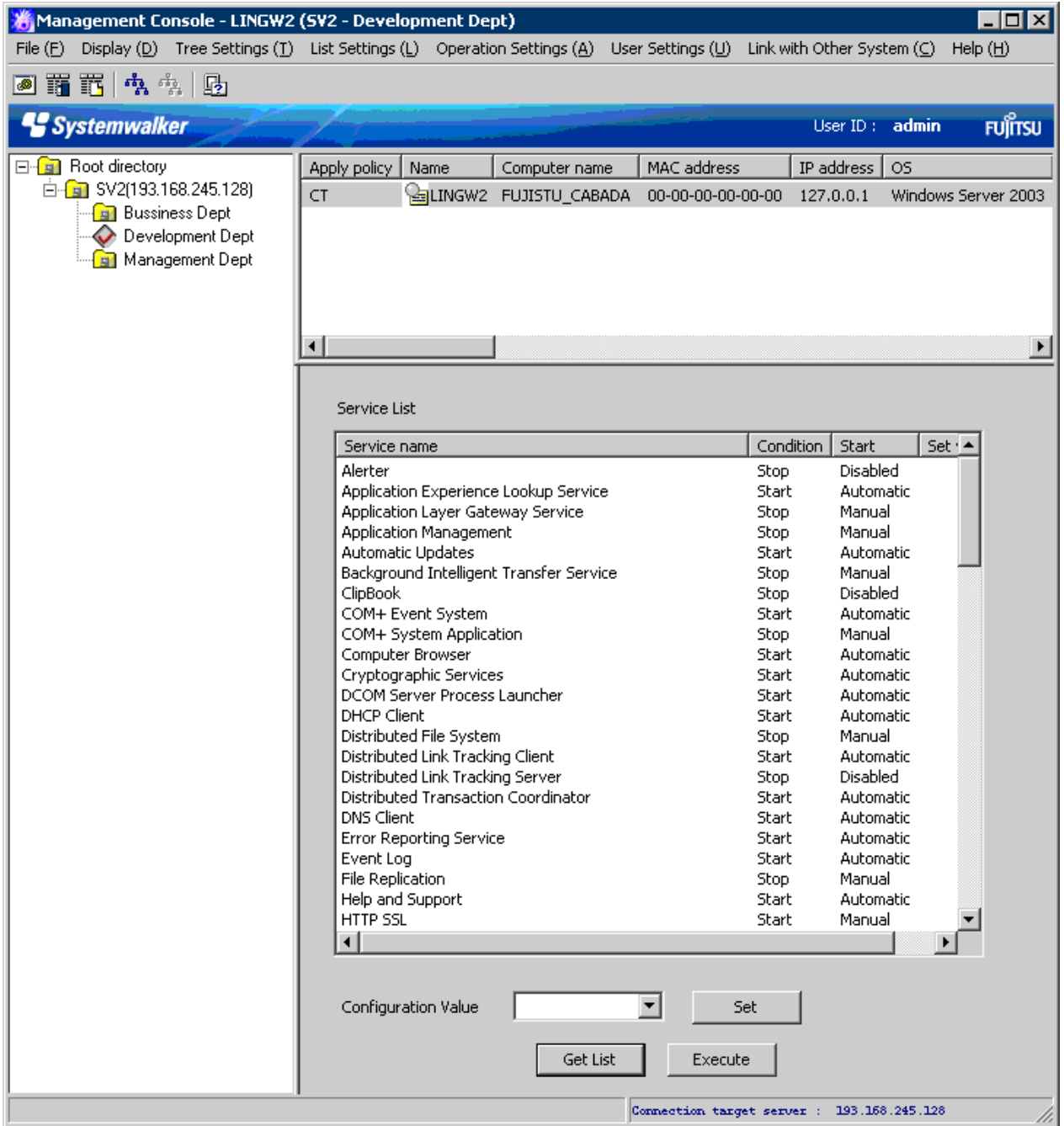
This section describes how to view the list of services registered in the client (CT).

The procedure of viewing the service list is shown as follows:

1. Start the [Management Console] window.
2. From the CT group tree, select the CT group to which the client (CT) is registered.
3. From the CT list, select the client (CT) for viewing the service list, and select [Get/Control Service List] from the [Display] menu.  
→ The service list window is displayed.

4. Click the [Get List] button.

→ The list of services registered in the selected client (CT) is displayed.



Item Name	Description
[Service name]	The name of service registered in the client (CT) is displayed. The service name refers to the information when the Window service and properties of each item are displayed.
[Condition]	The status of services registered in the client (CT) is displayed.
[Start]	As the type of startup, [Automatic], [Manual] or [Disabled] is displayed.
[Set Value]	When service control is performed according to "Control Services", the selected configuration value will be displayed. The configuration value includes [Start], [Stop], [Automatic], [Manual] or [Disabled].

## Control Services

This section describes how to modify the status of services registered in the client (CT) and the type of startup.



---

### About the modification of service status and startup type

For the services of which the status and startup type cannot be modified manually in the client (CT), even if this function is used, the status and startup type still cannot be modified.

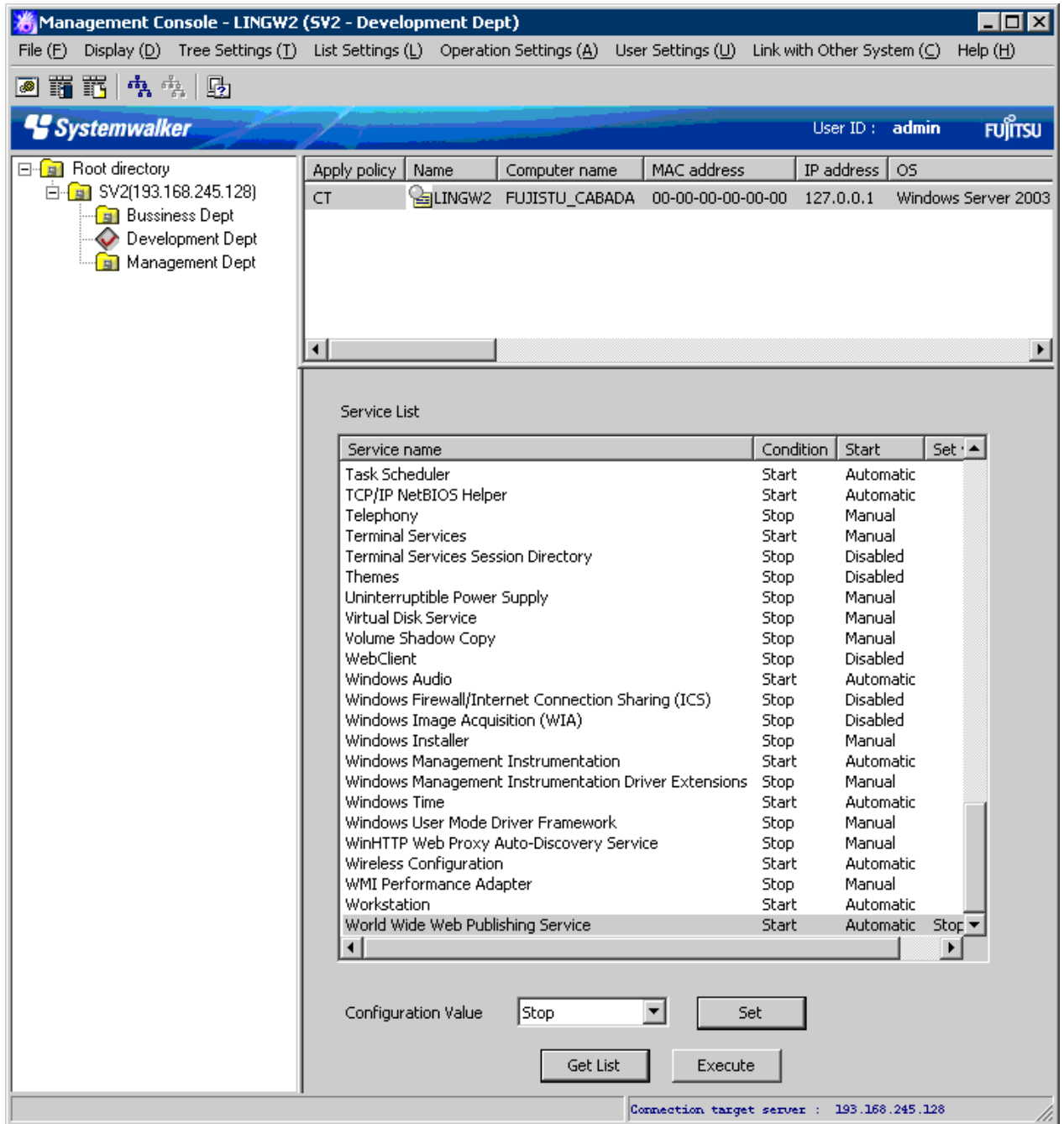
---

The procedure of service control is shown as follows:

1. Start the [Management Console].
2. From the CT group tree, select the CT group to which the client (CT) with service control has been registered.
3. From the CT list, select the client (CT) for service control, and select [Get/Control Service List] from the [Display] menu.
4. Click the [Get List] button.  
→The list of services registered in the selected client (CT) is displayed.
5. Select the lines to modify status from [Service List].

6. Select [Configuration Value] from the pull-down menu and click the [Set] button.

→The value selected from the pull-down menu of [Configuration Value] is displayed.



7. Click the [Execute] button.

→ The set status is updated to the client (CT).

### 3.6.2 Control the Processes of Client (CT)

This section describes how to view and control the processes running in the client (CT).



## View Process List

This section describes how to view the list of processes running in the client (CT).

If multiple users log on, the process list of all users can be viewed.



**In the case of Windows Vista® 64-bit Edition, Windows® 7 64-bit Edition, Windows Server® 2008 64-bit Edition and Windows Server® 2008 R2, the processes running in 64-bit cannot be viewed**

### Part of the processes cannot be viewed

Part of the processes relating to Windows systems cannot be viewed.

[Example]

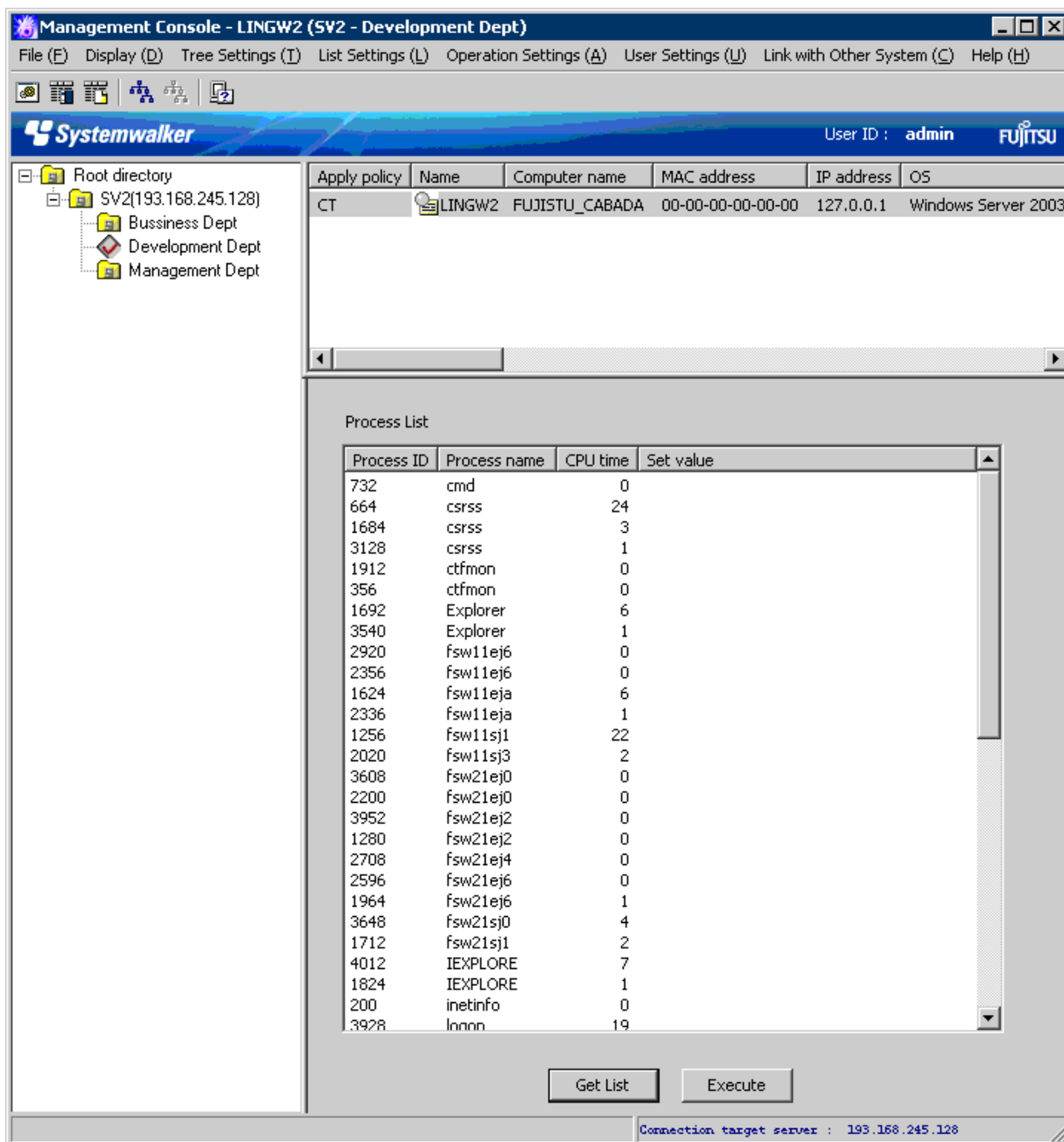
- System Idle process
- system

The procedure of viewing the process list is as follows:

1. Start the [Management Console] window.
2. From the CT group tree, select the CT group to which the client (CT) for viewing process list has been registered.
3. From the CT list, select the client (CT) for viewing process list, and select [Get/Control Process List] from the [Display] menu.

4. Click the [Get List] button.

→The list of processes running in the selected client (CT) is displayed.



Item Name	Description
[Process ID]	The process ID is displayed.
[Process name]	The execution name of process is displayed.
[CPU time]	The running time of process is displayed.
[Set value]	When process control is performed according to "Control Processes", status will be displayed as "Terminated".

## Control Processes

This section describes how to terminate a process that is running in the client (CT).



### [View Processes]

- In case of Windows Vista® 64-bit Edition, Windows® 7 64-bit Edition, Windows Server® 2008 64-bit Edition and Windows Server® 2008 R2, processes running in 64-bit cannot be viewed.
- Part of the processes relating to Windows systems cannot be viewed.  
[Example]
  - System Idle process
  - system

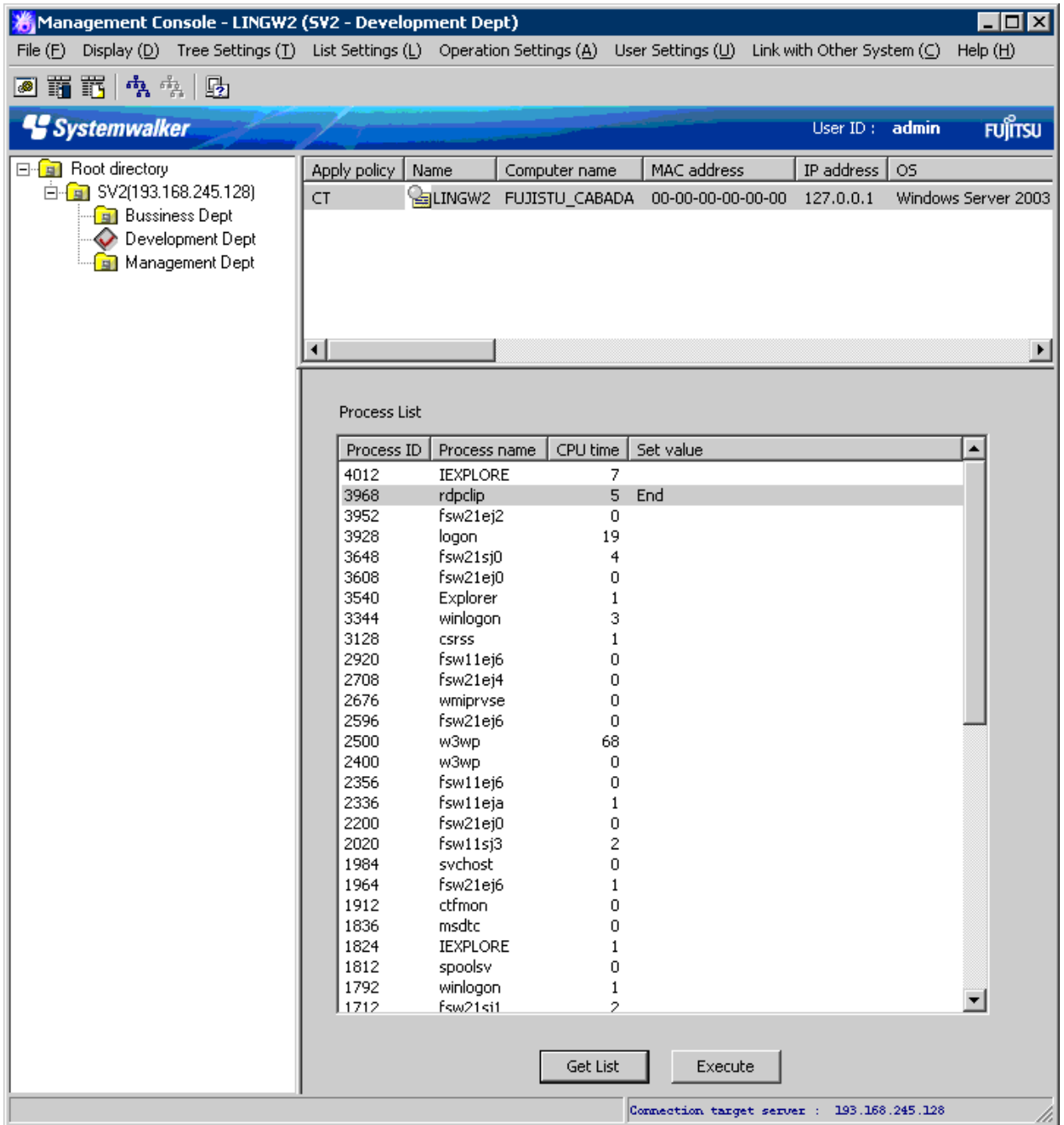
### [Terminate Processes]

- Some processes may not be able to be terminated.
- When terminating a process, the process with the same name as the selected process has been started multiple times will also be terminated.  
In addition, if multiple users log on, processes will be terminated for all users.
- In the case of Windows Vista® 64-bit Edition, Windows® 7 64-bit Edition, Windows Server® 2008 64-bit Edition and Windows Server® 2008 R2, processes cannot be terminated.

The procedure of process control is shown as follows:

1. Start the [Management Console] window.
2. From the CT group tree, select the CT group to which the client (CT) for viewing process list has been registered.
3. From the CT list, select the client (CT) for viewing process list, and select [Get/Control Process List] from the [Display] menu.  
→The process list window is displayed.
4. Click the [Get List] button.  
→The list of processes running in the selected client (CT) is displayed.
5. Select the lines to [End] its status from [Process List].

- Double-click the selected line.  
→ [End] is displayed in [Set value].



- Click the [Execute] button.  
→ The End of process will be updated to the client (CT).

## Chapter 4 Check Trend of Client (CT) Operation

This chapter describes how to use the Status Window and Log Analyzer.

According to the collected operation logs, the number of operations that may cause information disclosure and number of violations can be aggregated and the trend of operation in the client (CT) can be known.

### When Status Window is used

The logs related to the items that has high possibility of information disclosure will be aggregated and the correspondent number of PCs will be displayed.

- PC Having Exported Files
- PC Used Out of Working time
- PC Having Performed Suspicious Access
- PC Not Connected for a Long Time
- PC Having Blocked the Use of Prohibited USB Memory
- PC Having Blocked the Use of Prohibited Account Group
- PC Having Blocked the Use of Prohibited Application
- PC Having Blocked Prohibited Printing
- PC Having Blocked the Sending of E-mail with Prohibited Attachment

Based on the result of aggregation, confirm the details of the department to which the correspondent PC belongs and the details of correspondent PC (Computer name, Applied policy and Group name, etc.).

When the department and PC that requires attention is found, the actual situation of the performed operation can be found by searching the log of that PC.

### When Log Analyzer is used

To know the number of operations in operation type

The following operations have a high possibility of information disclosure and aggregate the number of operations:

- File export log
- File operation log
- Printing operation log
- E-mail sending log

Since the result of aggregation can be shown in a graph and the worst ranking of operations can be displayed according to users and terminals, the executor of corresponding operations, the executing terminal and the times of execution can be easily known.

The time frame of aggregation is set from Jan. 1, 2005 to present.

Please refer to "[4.2.2 Diagnose Risk of Information Disclosure](#)" for details.

To know the number of research objectives

According to the following research objectives, multiple operation types can be aggregated in combination:

- Know the violation status
- Know the file export status
- Know the file operation status
- Know the status of applications and E-mail
- Know the printing status

- Know the Web access status
- Know the information disclosure status

Please refer to “4.2.3 Aggregate by Objectives” for details.

## Note

### Notes relating to the start of Web Console

Please do not start multiple Web Consoles on one PC.

### About handling PrintScreen key prohibition log

This chapter only takes the PrintScreen key prohibition log that is classified as “Violation” type as the target for handling.

## 4.1 Check the Trend in Status Window

---

### Note

#### Please do not modify configuration information while browsing the Status Window

Please do not perform any modification to configuration information, such as adding, deleting or moving a CT or a department, since it may cause an error or the incorrect information may be displayed.

### 4.1.1 Display Status Window

---

1. Start Web Console through any of the following approaches:

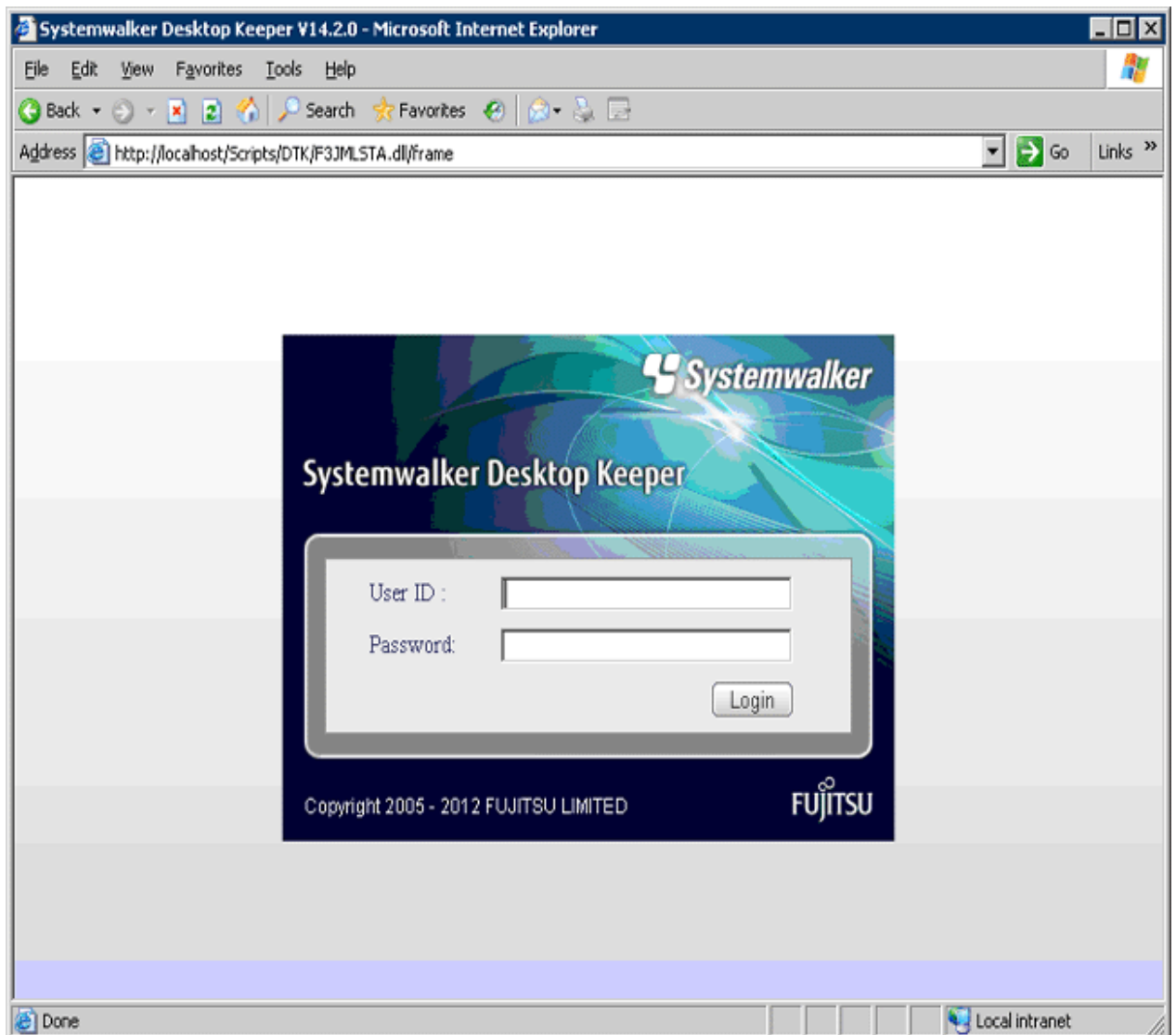
**In the case of a 2-level system structure:** Please connect to the Management Server.

- Select [Programs] - [Systemwalker Desktop Keeper] - [Server] - [Desktop Keeper Main Menu] from the [Start] menu of Management Server.
- Specify the address of browser to “http://host name or IP address of Management Server /DTK/index.html”.  
When the port number of IIS is changed, specify as follows.  
http://IP address: Port Number/DTK/index.html

**In the case of a 3-level system structure:** Please connect to the Management (Master Management) Server. To display the result of aggregation in every Management Server, please connect to each Management Server.

- Select [Programs] - [Systemwalker Desktop Keeper] - [Server] - [Desktop Keeper Main Menu] from the [Start] menu of Management (Master Management) Server.
- Specify the address of browser to “http://host name or IP address of Management (Master Management) Server /DTK/index.html”.  
When the port number of IIS is changed, specify as follows.  
http://IP address: Port Number/DTK/index.html

→ The [Login] window is displayed.



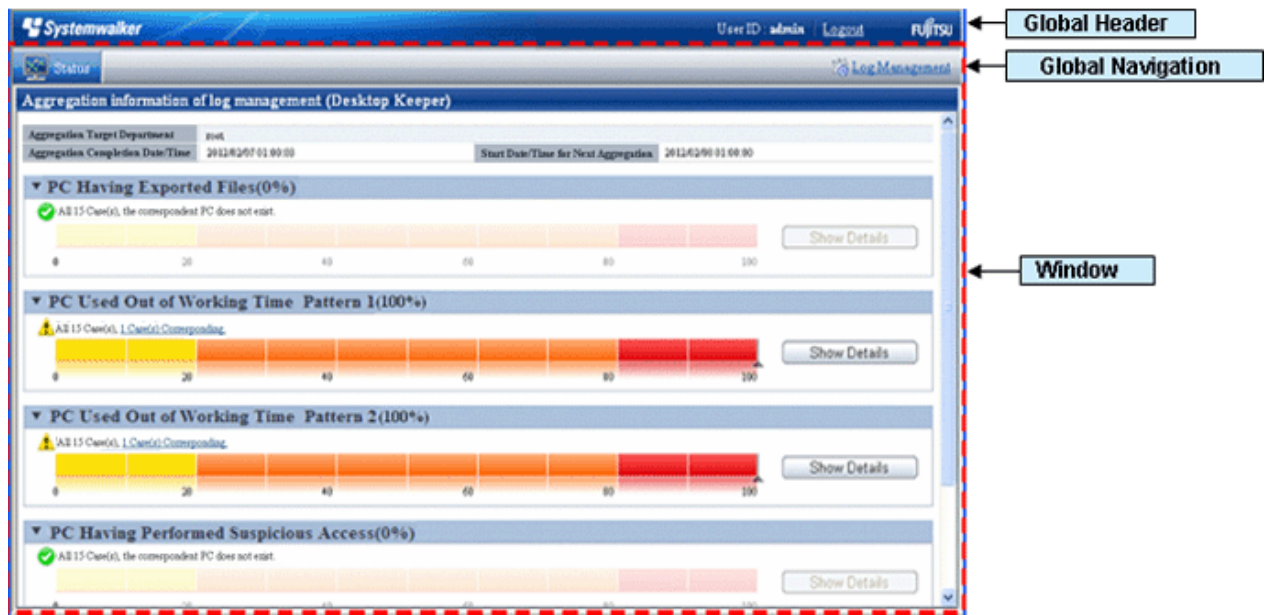
2. Enter the following information and click the [Login] button.

The system administrator and department management use the same login method.

When Systemwalker Desktop Patrol is linking with single sign on, the input of User ID is case-sensitive.

- **[User ID]:** this is the [User ID] that is set in the [Administrator Information Settings] window of the Server Settings Tool.
- **[Password]:** this is the [Password] that is set in the [Administrator Information Settings] window of the Server Settings Tool. It is recommended to change the password regularly. For details on how to change the password, please refer to "[Change password](#)".

→ The Status Window is displayed.



Displayed Content of Window

#### Global Header

- User ID: The login user ID is displayed.
- Logout: Perform logout.

#### Global Navigation

- Status: The Status Window is displayed.
- Log Management: The Log Viewer window is displayed.

#### Window

- [AggregationTarget Department]: Select the department for log aggregation.

When the system administrator logs in, it is displayed as [root].

When the department management logs in, the department management that manages multiple department selects the target department (CT group) for aggregation from the pull-down menu. Only the department (CT group) with department management being configured will be displayed in the pull-down menu, and the sub-groups will not be displayed.

- [Aggregation Completion Date/Time]: This indicates the date and time on which the aggregation has finished.

In the aggregation process, "(Aggregating)" will be displayed after the date and time.



#### Note

##### When modifying settings after the completion date and time of aggregation

When modifying configuration information and environment setup after the date and time on which the aggregation has completion, modification information will not be reflected in the aggregation information displayed currently. After modification, please view the information after the next aggregation.

##### Please view the Status Window after the aggregation has completion

When "(Aggregating)" is displayed, an error may exist in the result of the aggregation displayed in the window. Please view it after the aggregation has finished.



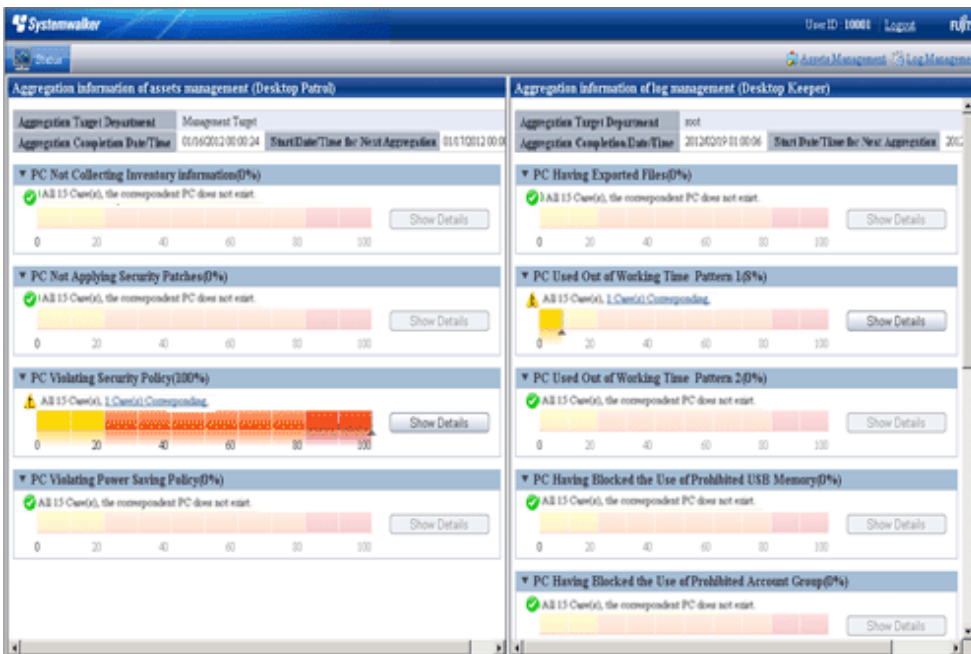
**Please confirm the event log of Management (Master Management) Server**

If it shows the aggregation has finished more than two days earlier than the predetermined date and time, the aggregation process may have been terminated due to an error. In this case, please check the event log of Management (Master Management) Server and confirm whether an error occurred.

- [Start Date /Time for Next Aggregation]: This indicates the start date and time of next aggregation.
- The result of aggregating the number of PCs corresponding to each item is displayed.

**When linking with Systemwalker Desktop Patrol**

In the case of linking with Systemwalker Desktop Patrol, assets management information (information of Systemwalker Desktop Patrol) and log management information (information of Systemwalker Desktop Keeper) will be displayed in the Status Window.



After [Assets Management] of Global Navigation is clicked, the Web Console of Systemwalker Desktop Patrol will be started. Please refer to Systemwalker Desktop Patrol Manual for details.

### 4.1.2 Confirm Result of Log Aggregation

In the Status Window, the number of PCs corresponding to the following auditing items is displayed in graph:

- PC Having Exported Files

The number of PCs that have executed file export is displayed. For the file export log/file operation log, aggregation is performed after the conditions such as aggregation period, drive type of external memory media and folder path of export source have been added.

- PC Used Out of Working time

The number of PCs that have logged on/logged off out of the time frame for PC operation defined by administrator is displayed. For logon/logoff log, aggregation is performed after the conditions such as aggregation period, day of a week and time frame have been added.

- PC Having Performed Suspicious Access

The number of PCs that have performed suspicious access is displayed. When the PC was started in safe mode and domain is used, aggregation is performed for logon/logoff logs after the conditions such as login as local user and login with administrator authority have been added.

- PC Not Connected for a Long Time

The number of PCs that have not been connected or used for a long time is displayed. For policy distribution status of Systemwalker Desktop Keeper, aggregation is performed after the condition of time period in which the PC is not connected has been added.

- PC Having Blocked the Use of Prohibited USB Memory

The number of PCs on which the use of prohibited USB memory has been blocked is displayed.

For the log of violation (\*) to the category of device configuration change log, aggregation is performed after the condition of aggregation period has been added.

\* The use of USB memory that is not registered through the individual identification function of the “File Export Prohibition” policy will be recorded as a violation.

- PC Having Blocked the Use of Prohibited Account Group

The number of PCs on which the logon with the User ID that belongs to a prohibited account group has been blocked is displayed.

For logon prohibition log (\*), aggregation is performed after the condition of aggregation period has been added.

\* The user of the User ID that belongs to the group specified in the “Logon Prohibition” policy will be recorded as a violation.

- PC Having Blocked the Use of Prohibited Application

The number of PCs on which the startup of prohibited application has been blocked is displayed.

For application startup prohibition log (\*), aggregation is performed after the condition of aggregation period has been added.

\* The startup of an application that is specified in the “Application Startup Prohibition” policy will be recorded as a violation.

- PC Having Blocked Prohibited Printing

The number of PCs on which the prohibited printing has been blocked is displayed.

For printing prohibition log (\*), aggregation is performed after the condition of aggregation period has been added.

\* Printing through an application that is not specified as the permitted application in “Printing Prohibition” policy will be recorded as a violation.

- PC Having Blocked the Sending of E-mail with Prohibited Attachment

The number of PCs on which the transmission of prohibited E-mail file attachment has been blocked is displayed.

For E-mail attachment prohibition log (\*), aggregation is performed after the condition of aggregation period has been added.

Only the E-mail sending through SMTP will be the target.

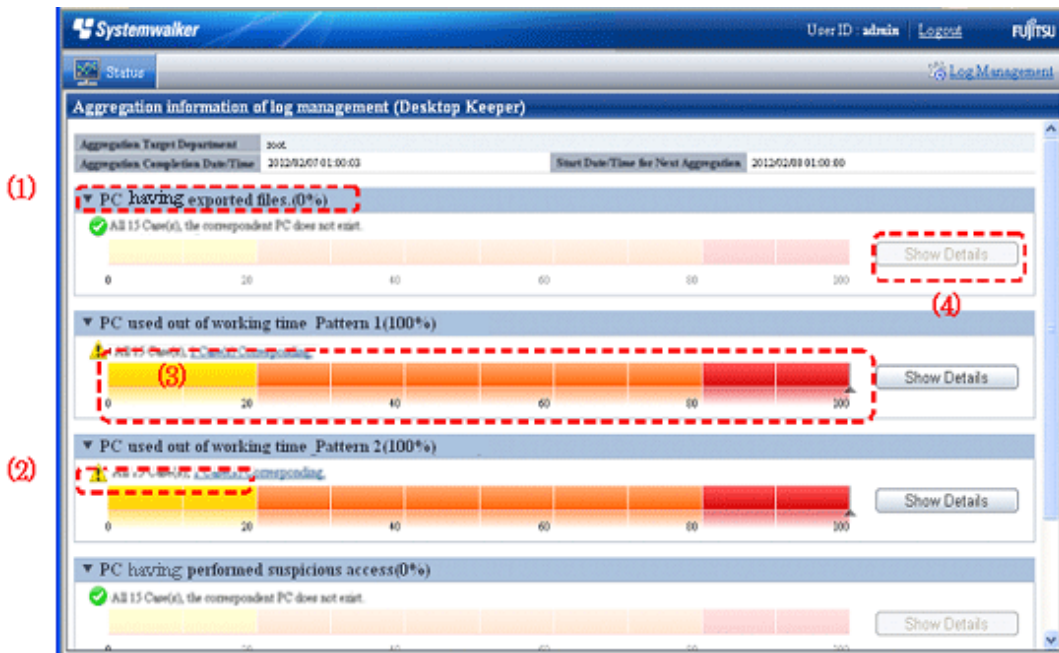
\* Sending of an E-mail with the prohibited attachment specified in the “E-mail Sending” policy will be recorded as a violation.

The system administrator can set whether to show/hide each item.

For details on setting these items, please refer to “[2.7.1 Prepare for Using Status Window](#)”.

The confirmation procedure is as follows:

1. Determine the auditing items in the Status Window.



(1) **Title (proportion):** This is the title of the auditing item. The scale in ( ) indicates whether the percentage of PCs that become the managed targets are in correspondence.

(2) **Correspondent number of PCs:** The correspondent number of PCs is displayed. After clicking the number of PC, the [CT Operation Log - List of fault PC] window is displayed. Please refer to “[CT Operation Log - List of fault PC] window” for details.

Status icon: It shows the status of correspondent number of PCs using icons.

✔: This is displayed when the correspondent number is 0.

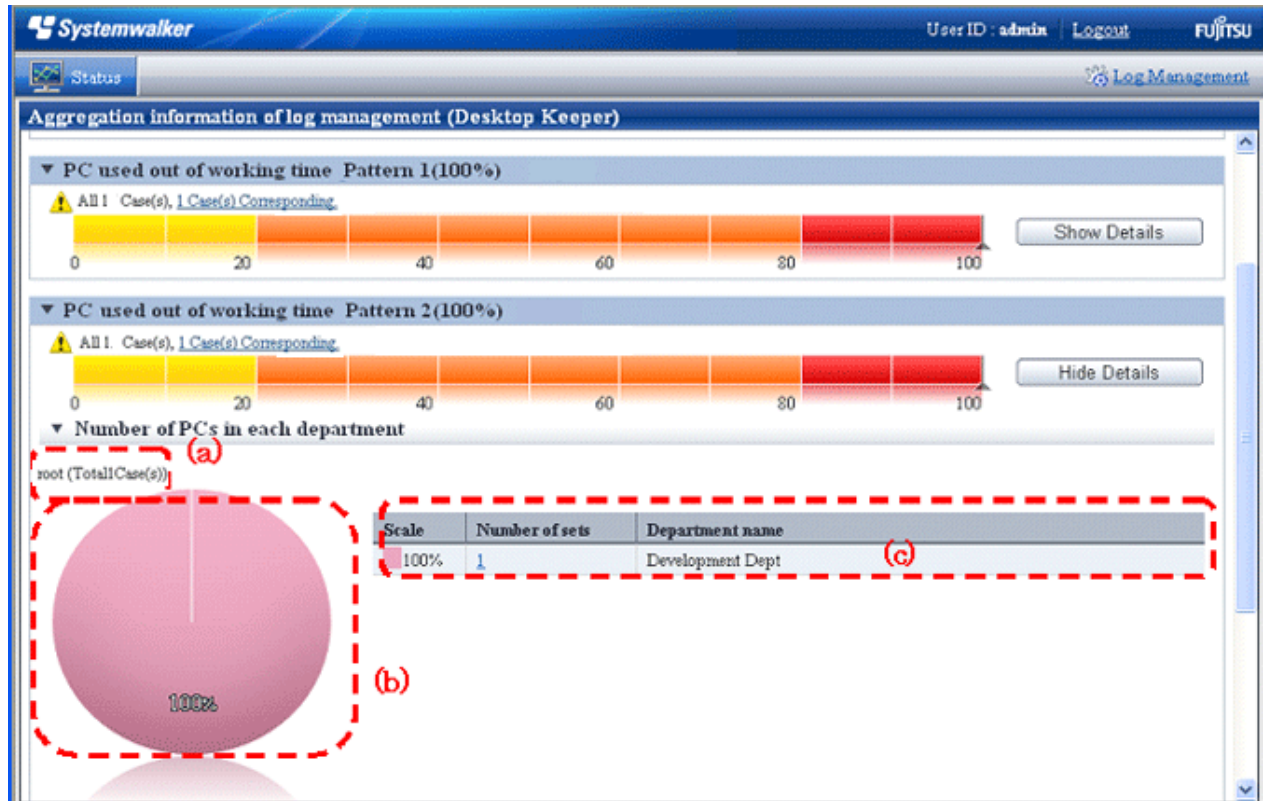
⚠: This is displayed when the correspondent number is more than 1.

(3) **Proportion Bar Chart:** This shows the proportion of correspondent number of PCs using a bar chart.

(4) **[Show Details]:** Under the bar chart, the number of PCs at each department is shown in tables and pie chart. Please refer to “Number of PCs in Each Department ” for details.

- Click the [Show Details] button of the item and the department to which the error PC belongs can be known. During a log search in Log Viewer, which CT group is more suitable to be a search target can be clarified.

Number of PCs in each department



The number of PCs in each department is displayed.

The initial status is that the information of the top management department that manages the login user is displayed.

(a) **Target Department:** This shows the level of the displayed department. The department selected in [ Department of Aggregation Target] is displayed at the far left.

(b) **Pie chart:** This shows the number of correspondent PCs of each department and its proportion to the number of all PCs.

(c) **Ranking table:** This shows the number of correspondent PCs of each department and its proportion to the number of all PCs in sequence.

After clicking the number, [List of fault PC] will be displayed.

After clicking the department name, the target department, pie chart and ranking table will be changed to the information under the selected department.

[Example] When the target department is displayed as “xx headquarter > xx business department”

After clicking the [Department Name] of the ranking table, the display of target department will change to “xx headquarter > xx business department> xx department”, while the pie chart and ranking table will be displayed under the unit of the subordinate xx division level.

- Click the number of correspondent PC  
→ [List of Fault PC] is displayed.

[CT Operation Log - List of fault PC] window

(a) **[Search place]:** When the system administrator logs in, it is displayed as [Root]. When the department management logs in, the department (CT group) selected by the department management is displayed.

(b) **[Description conditions]:** The conditions when aggregation the title of auditing items and number of correspondent is displayed.

(c) **[List of fault PC]:** The list of PC that conforms to the content of [Description Conditions] is displayed. Item names such as [Group] and [Name] will show the information configured in the [Display Item Settings] window of Log Viewer. For details of the setting method, please refer to “[Set visible columns in \[List of searched CT\]](#)”.

However, [Management Server] of item name cannot be set in the [Display Item Settings] window of Log Viewer. Items must be displayed on the right.

After clicking [Name], Log Viewer is started and the search window is displayed. For operation method, please refer to “[5.2.1 View Logs in \[CT Operation Log\] Window](#)”.

- From [List of fault PC], click the client (CT) name to perform log search.  
→ Log Viewer is started and the search results are displayed. Operations performed in an error PC can be known.  
The search result will also contain the content that does not conform to the conditions specified in [Environment Settings].

## 4.2 Check the Trend in Log Analyzer



Note

About the Not Configured group

When [Manage under the group that is not configured] has been set in [System Settings] - [Set group that is not configured] of the Server Settings Tool, Log Analyzer will manage the client (CT) through the “Root” group instead of the “Not Configured” group.

---

## 4.2.1 Start Log Analyzer

---

### Conditions of Using Web Console

- The system administrator or department management can use the Web Console.
- The Web browsers that can be used as the Web console are as follows:
  - Microsoft® Internet Explorer® 6.0 (ServicePack1)
  - Windows® Internet Explorer® 7
  - Windows® Internet Explorer® 8
  - Windows® Internet Explorer® 9

### Start Log Analyzer

1. Start the Main Menu through any of the following approaches.



---

#### About the Web server connected with Log Analyzer (Web Console)

When Log Analyzer is started, one Web server can be connected. In the case of a 3-level structure, though the Log Viewer window can also be displayed by collecting to the Management Server, the window of the Log Analyzer cannot be displayed.

---

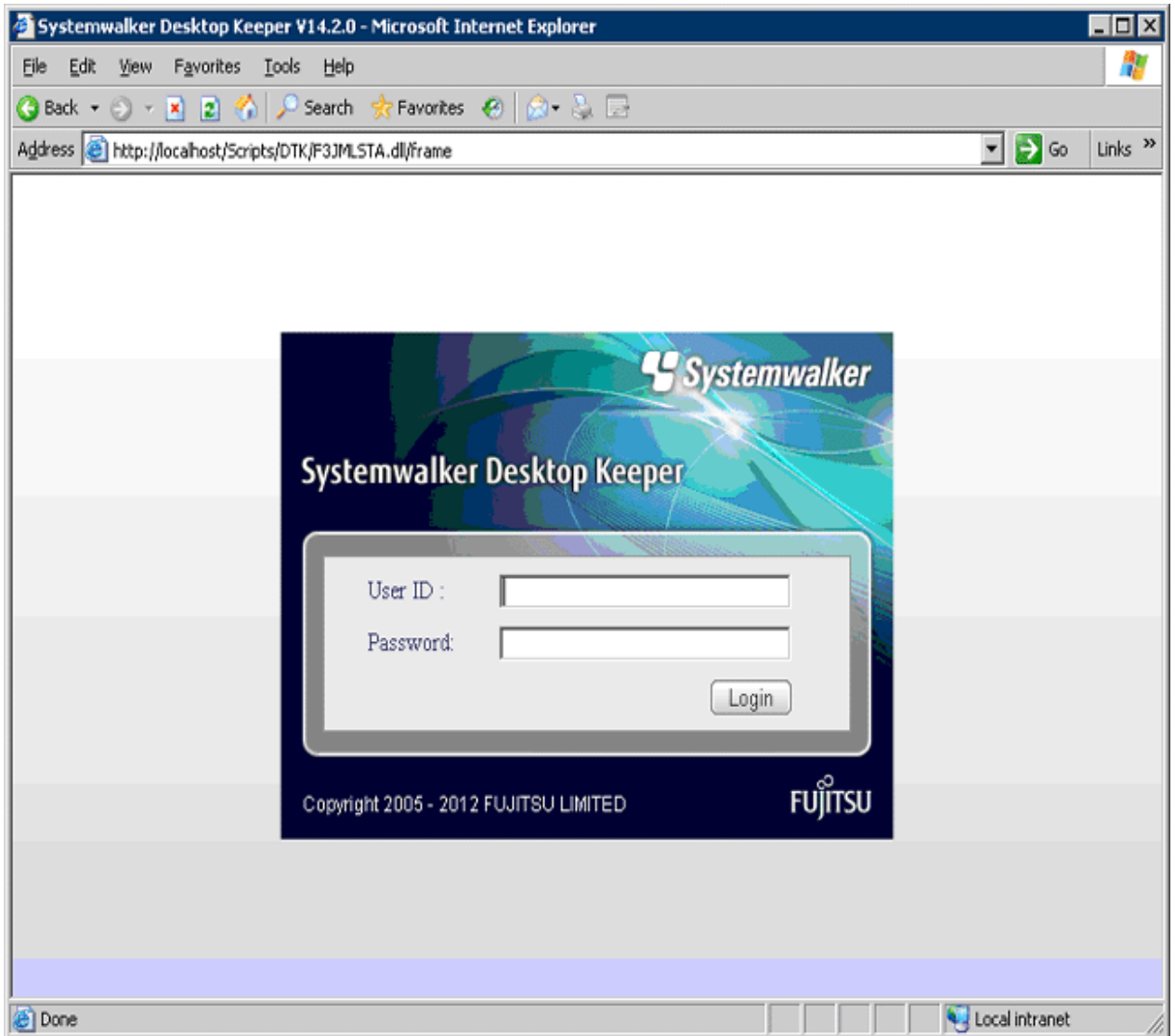
**In the case of 2-level structure:** Please connect to the Management Server.

- Select [Programs] - [Systemwalker Desktop Keeper] - [Server] - [Desktop Keeper Main Menu] from the [Start] menu of Management Server.
- Specify the address of browser to “http://host name or IP address of Management Server/DTK/index.html”.  
When the port number of IIS is changed, specify as follows.  
http://IP address: Port Number/DTK/index.html

**In the case of 3-level structure:** Please connect to the Master Management Server.

- Select [Programs] - [Systemwalker Desktop Keeper] - [Server] - [Desktop Keeper Main Menu] from the [Start] menu of Master Management Server.
- Specify the address of browser to “http://host name or IP address of Master Management Server /DTK/index.html”.  
When the port number of IIS is changed, specify as follows.  
http://IP address: Port Number /DTK/index.html

→ The [Login] window is displayed.



2. Enter the following information and click the [Login] button.

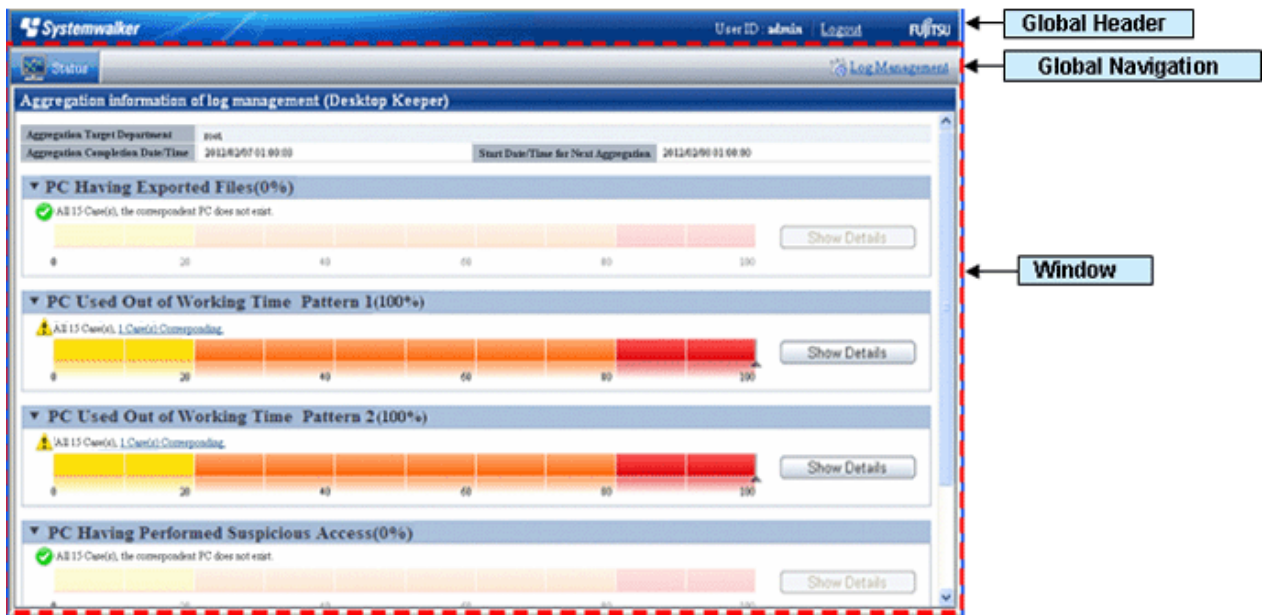
The system administrator and department management use the same login method.

When Systemwalker Desktop Patrol is linking with a single sign on, the input of the User ID is case-sensitive.

- **[User ID]:** this is the [User ID] that is set in the [Administrator Information Settings] window of the Server Settings Tool.
  - **[Password]:** this is the [Password] that is set in the [Administrator Information Settings] window of the Server Settings Tool.
- It is recommended to change the password regularly. For details on how to change the password, please refer to “[Change password](#)”.

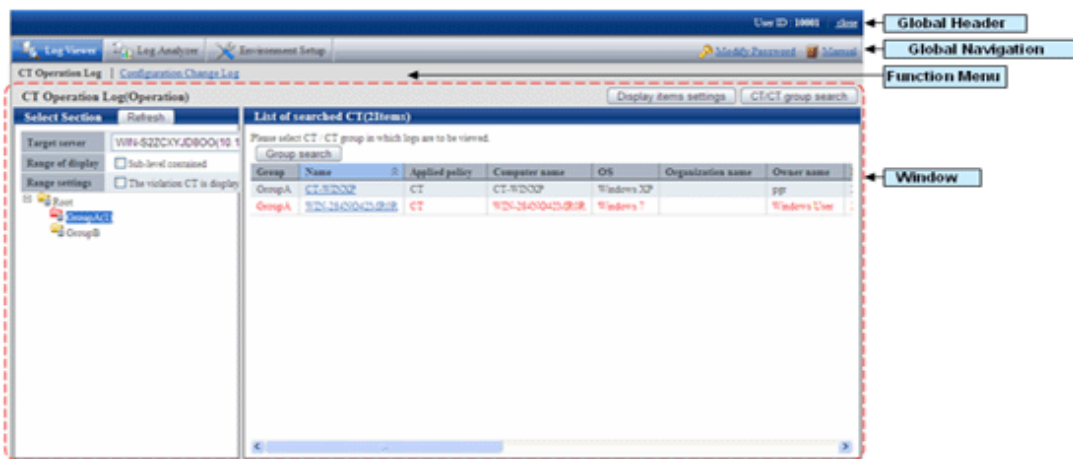


→ The Status Window is displayed.



3. Click [Log Management] of Global Navigation.

→ Log Viewer is started and the [CT Operation Log] window is displayed.

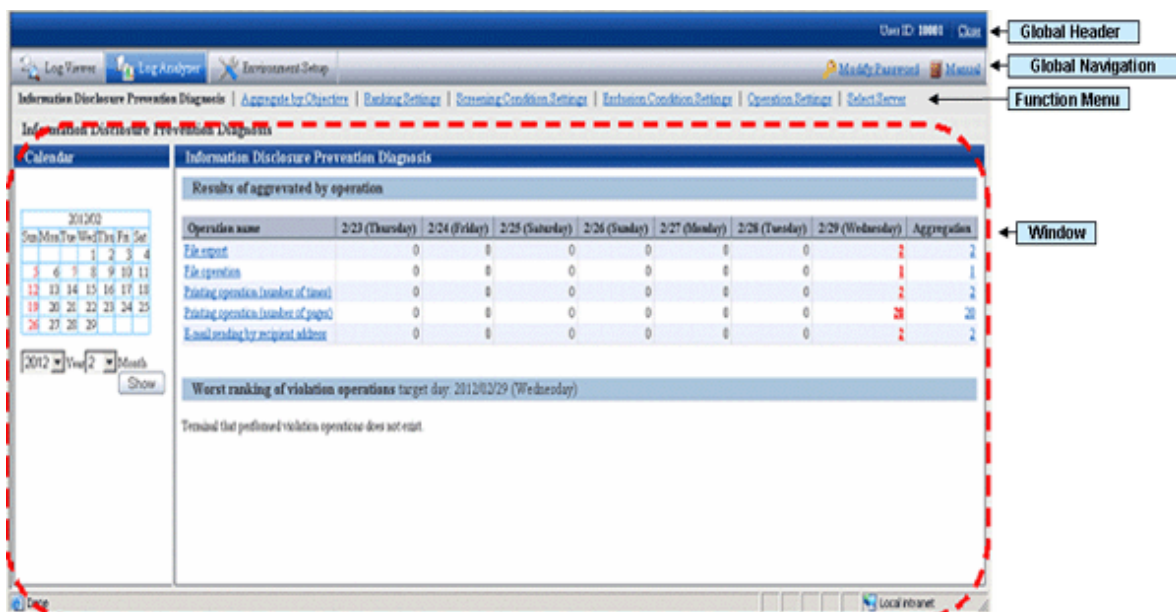


4. Click [Log Analyzer] of Global Navigation.

→ The [Information Disclosure Prevention Diagnosis] window is displayed.



In addition, in a system with multiple Log Analyzer server, when Log Analyzer is selected for the first time after login, the window for server selection will be displayed. For details about the window for server selection, please refer to “2.7.2.2.5 Select Log Analyzer Server”.



#### Displayed Content of Window

##### Global Header

- User ID: The login user ID is displayed.
- Close: Close the Log Viewer window.

##### Global Navigation

- Log Viewer: The window of Log Viewer is displayed.
- Log Analyzer: The window of Log Analyzer is displayed.
- Environment Setup: The options window (the window for setting the conditions of aggregation on which the result of aggregation displayed in the Status Window is based).
- Modify Password: Change the password for starting the Web window. For details on how to change the password, please refer to “Change password”.
- Manual: The manual is displayed.

##### Function Menu

- Information Disclosure Prevention Diagnosis: Display the window of Information Disclosure Prevention Diagnosis.
- Aggregate by Objectives: Display the window of Aggregate by Objectives. Perform aggregation by objectives after specifying date and time and keyword.
- Ranking settings: Set “Show/Hide” various ranking methods including by group, by terminal, by user and by terminal + user, as well as the number to of items to be displayed.
- Screening Condition Settings: Set the keyword, domain, URL or application during log aggregation as the filtering conditions.
- Exclusion Condition Settings: Set the terminal that is not to be aggregated during log aggregation.
- Operation Settings: Perform settings for displaying the worst ranking of violations of information disclosure prevention diagnosis and start day of weekly report and Eco- auditing in report output.
- Select Server: Display the server selection window. Click it when changing the Log Analyzer server currently selected. When all of the following conditions are satisfied, this window will be displayed automatically:

- When there are multiple Log Analyzer server in the system structure
- When Log Analyzer is used for the first time after login from the Main Menu

### Note

#### Sometimes, it may take some time before the window is displayed

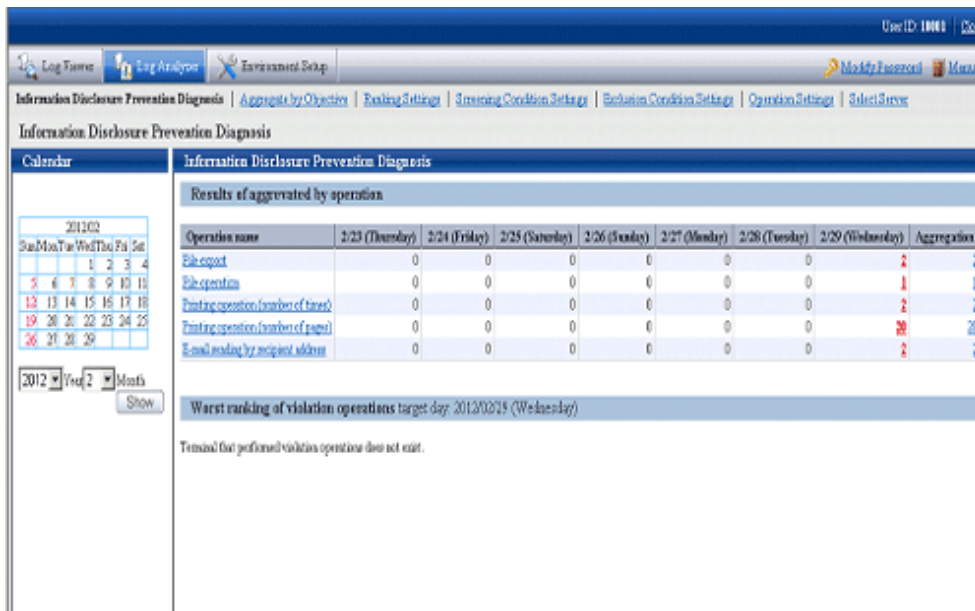
When a connection to the Log Analyzer server cannot be made due to the stop of the server and interruption of the network, depending on the environment and number of servers, it may take several minutes before the window is displayed.

#### Window

- Calendar: Select the date to display the result of aggregation.
- Result of aggregation by Operation: Display the frequency of file export operation, file operation, printing operation (frequency and pages) and E-mail sending operation as well as the total number of operations within recent 7 days.
- Worst Ranking of Violations: Display the number of logs on the date before logon or a selected date and the total value of operations relating to the following logs:
  - Application startup prohibition
  - Printing prohibition
  - Logon prohibition
  - PrintScreen key prohibition
  - E-mail attachment prohibition

## 4.2.2 Diagnose Risk of Information Disclosure

Diagnosis of information disclosure risk is performed in the [Information Disclosure Prevention Diagnosis] window.



Operation name	2/23 (Thursday)	2/24 (Friday)	2/25 (Saturday)	2/26 (Sunday)	2/27 (Monday)	2/28 (Tuesday)	2/29 (Wednesday)	Aggregation
File export	0	0	0	0	0	0	2	2
File operation	0	0	0	0	0	0	1	1
Printing operation (number of times)	0	0	0	0	0	0	2	2
Printing operation (number of pages)	0	0	0	0	0	0	20	20
E-mail sending by recipient address	0	0	0	0	0	0	2	2

### Note

The number of logs displayed in the Information Disclosure Prevention Diagnosis window may be inconsistent with the number of logs in the result of aggregation by objectives

The number of logs displayed in the Information Disclosure Prevention Diagnosis window is the result of aggregation according to the filtering condition and exclusion condition during the transfer of logs from the Management Server to the Log Analyzer Server.

Therefore, the filtering condition/exclusion condition modified after aggregation and the logs transferred in after aggregation (\*) cannot be reflected.

On the other hand, aggregation by objectives is a real-time aggregation, which means aggregation of the logs that have already been transferred according to the latest filtering condition/exclusion condition will occur.

Therefore, the number of logs displayed in the Information Disclosure Prevention Diagnosis window may be inconsistent with the number of logs in the result of aggregation by objectives.

If it is expected to display the result of aggregation that includes the logs transferred after aggregating according to the filtering condition/exclusion condition modified after aggregation (when it is expected to aggregate again according to the latest data and conditions), re-aggregation is required.

For re-aggregation, please refer to “DTTOOLEX.EXE (Move or Delete Data from Log Analyzer Server)” of “Systemwalker Desktop Keeper Reference Manual”.

**\*) When logs are transferred after aggregating**

Due to reasons such as a lack of connection between the client (CT) and network, sending of operation logs to the Management Server may be delayed. Therefore, the reflection of logs transferred to the Log Analyzer Server may be delayed.

---

### 4.2.2.1 Display the Result of aggregation by Operation

In [Result of aggregation by Operation] of the [Information Disclosure Prevention Diagnosis] window, the result of aggregation during log transfer from Management Server to Log Analyzer Server is used to display the number of operation logs collected at each terminal in the last week.

Aggregation is executed according to the filtering condition (keywords) and exclusion condition (file export, file operation, printing operation, E-mail sending according to recipient address) that are set in “[2.7.2.2 Set Conditions for Aggregation /Report Output](#)”.

The following operation logs will be aggregated:

- File export operation log  
According to this log, the number of operations for exporting files to removable media using the file export utility is aggregated.
- File operation log  
According to this log, the number of operations for creating, updating, moving and copying files on the media identified as removable drive and DVD/CD is aggregated.  
Though file operation also includes deleting, renaming and viewing, since these operations have very low risk of information disclosure, they will not be aggregated.
- Printing operation log  
Aggregate the times of printing operation and the total number of printed pages.  
Even if the printed file contains many pages, the count of printing operation is still 1.  
When the printed file contains many pages, the number of printed pages is counted (the total number of pages of the file is counted).
- E-mail sending log  
The number of operations for sending E-mail to the outside of company is aggregated (the domain of company internal E-mail address needs to be registered as the filtering condition).  
In addition, the emails sent to groups will be counted as multiple operations.

When there are a large number of logs, the possibility of information disclosure can be considered. In each operation, the cell of date with most number of logs is shown in red.

In addition, the number of each operation can be shown in graph, or the details of the number can be displayed in ranking.

If the setting of “[2.7.2.2 Set Conditions for Aggregation /Report Output](#)” is not performed, the number will increase rapidly with the growth of business and scale. In this case, not only the processing time and data amount for displaying will be increased, but it will also be difficult to identify dangerous operations. Please make sure to apply this setting.

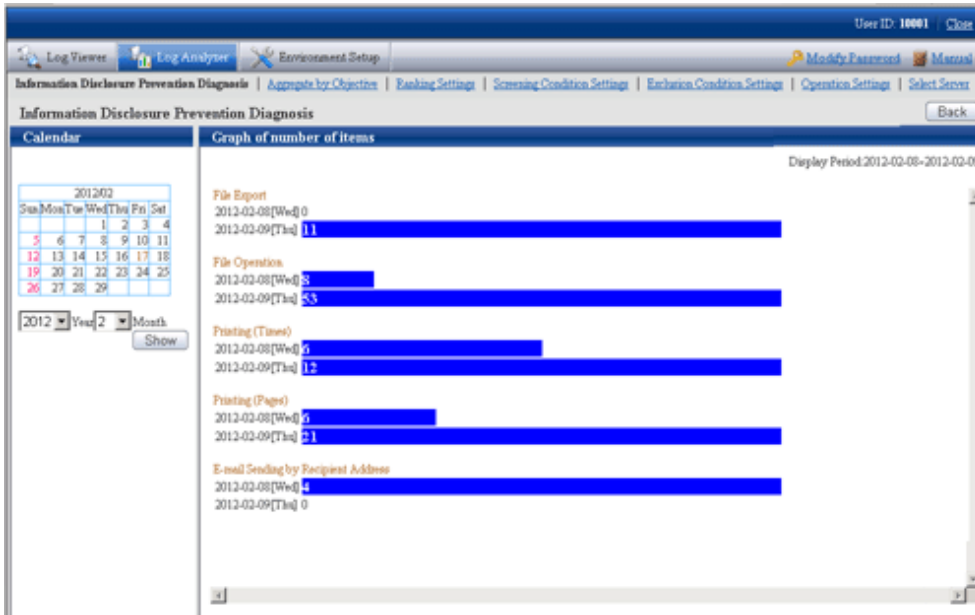
### Display the Number in Graph

After clicking the various operation names displayed in the result of aggregation by objectives, the variation of number within one week will be displayed in graph.

The scale of graph varies with operations (The length displayed in a graph as the maximum number of each kind of operation in a week is in 100% status).

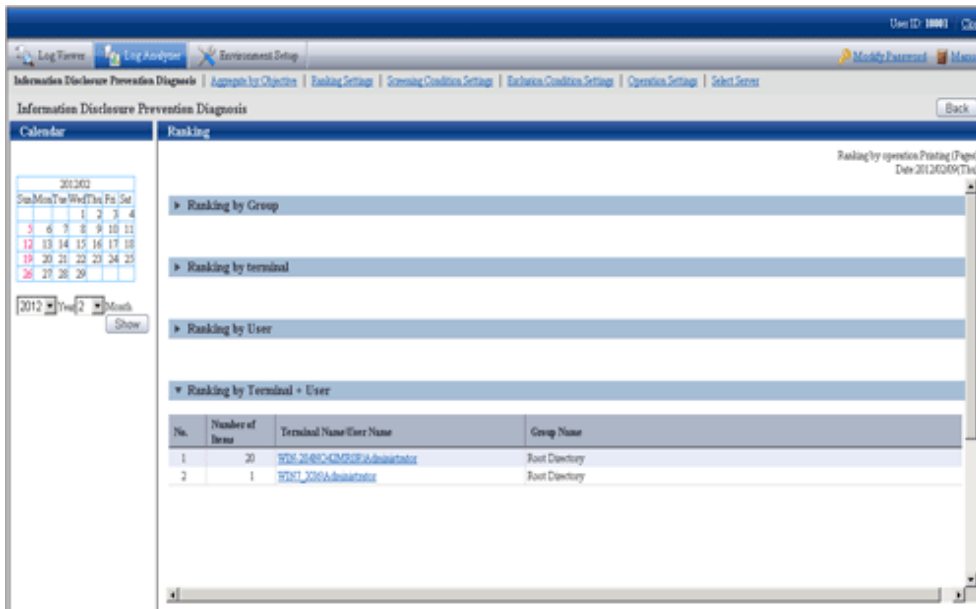
The procedure is as follows:

1. Click the operation displayed in graph in [Operation name] of the result of aggregation by operation.  
→ The graph is displayed.



### Display Details of Number in Ranking

After clicking the date column and total column of the result of aggregation by operation, the details of number will be displayed in ranking.



The ranking is shown as follows:

- Ranking by Group

The number is aggregated in the unit of group and displayed in order from more to less. The displayed group name can contain maximum 1024 bytes.

In the CT group tree of Management Console, the [Group Name] of client (CT) exists under the root directly is displayed as “Root”. The group managed by level structure is displayed as “1-Level/2-Level/3-Level”.

- Ranking by terminal (Note)

The number is aggregated in the unit of terminal and displayed in order from more to less. The group name to which the terminal belongs will also be displayed.

- Ranking by User

The number is aggregated in the unit of user name and displayed in order from more to less. Even if the terminals are different, total aggregation can still be performed when user names are the same.

- Ranking by Terminal + User(Note)

The number is aggregated in the unit of combination of terminal name and user name and displayed in order from more to less. The group name to which the terminal belongs will also be displayed.

In the case of the same number, it is displayed in the sequence set in ranking settings (the display order of same ranking is random), but a maximum of 99 lines can be displayed.

Note: “Terminal name” and “Terminal + User Name” of ranking items are displayed in the following forms:

- When the [Name] and [Computer Name] displayed in the CT list of Management Console are the same

The conditions to make [Name] and [Computer Name] the same are as follows:

- Since [Name] is not updated after CT installation, the [Computer Name] will be displayed as the initial value.
- In the Management Console, the [Name] is updated to the name that is same as [Computer Name]

At this time, in ranking by terminal, it will be displayed in form of “Computer Name”.

[Example] PC001

In ranking by terminal, it will be displayed in form of “Computer Name + User Name [Group Name]”.

[Example] PC001+Administrator

- When the [Name] and [Computer Name] displayed in the CT list of the Management Console are different

The conditions to make [Name] and [Computer Name] different are as follows:

- In the Management Console, the [Name] is updated to the name that is different from [Computer Name]

At this time, in ranking by terminal, it will be displayed in form of “Computer Name (Name)”.

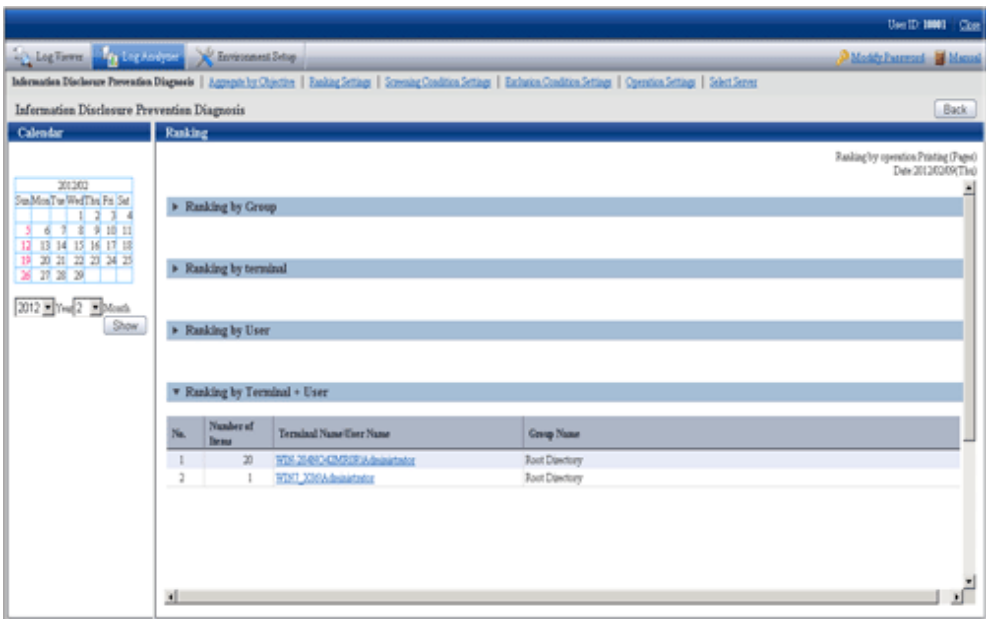
[Example] BLONO (Fujitsu Taro)

In ranking by terminal + user name, it will be displayed in form of “Computer Name (Name) + user name”.

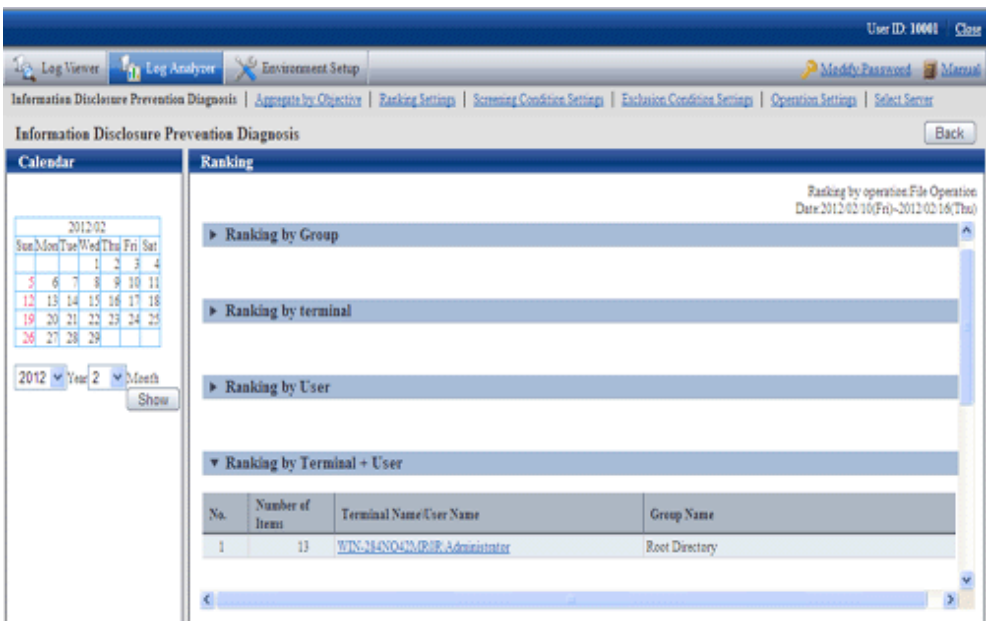
[Example] BLONO (Fujitsu Taro) + Administrator

When clicking the number on the date column

→ The ranking of operations on the selected date is displayed.



When clicking the number on the total column  
 →The ranking of target operations in the aggregation period is displayed.



In the displayed ranking result, after the link of group name, terminal name and terminal + user name is clicked, the window will switch to Log Viewer (when the “Operate in Compatible with Desktop Log Analyzer” checkbox is selected, it will switch to the window of aggregating by objectives). In Log Viewer, the result of log search executed according to the conditions (Aggregation period, user name, terminal name .etc) during aggregation will be displayed in [Log List]. When viewing the number of [E-mail sending by recipient address] in Log Viewer, since the group E-mail that exists in the Log Analyzer will be counted by recipient address while the group E-mail is counted as 1 in Log Viewer, the number of logs may be inconsistent. When [Operate in Compatible with Desktop Log Analyzer] is selected in [Operation Settings], after the link of clicking the link of group name, terminal name and terminal + user name is clicked, the window will switch to aggregate by objectives.

However, when the result of aggregation by operation contains more than 100,000 cases, it is unable to switch to the Log Viewer window (the Log list cannot be viewed).

In addition, the groups under the names of [Root], [Local] and [Deleted CT] in ranking by group cannot be switched to the Log Viewer window as well.

### 4.2.2.2 Display the Worst Ranking of Violations

In the worst ranking of violations, the ranking based on the total number of violations is displayed.

The number of violations is aggregated according to the following violation logs and the ranking is displayed according to the total number of each kind of operation.

- Application startup prohibition log
- Printing prohibition log
- Logon prohibition log
- PrintScreen key prohibition log
- E-mail attachment prohibition log

In the displayed result of ranking, after the link of terminal name is clicked, the window will switch to Log Viewer. In Log Viewer, the result of log search executed according to the conditions (Aggregation period, terminal name .etc) during aggregation will be displayed in [Log List].

### 4.2.2.3 Specify a Past Date to Display Aggregation Result

Specify a date in the calendar and the aggregated number of each operation in the last week will be displayed based on the specified date.

Before execution, please confirm whether the logs within the period for aggregation exist on the Log Analyzer Server. The number of logs that can be transferred is the logs recorded in the past year.

Specify a date within the range of Jan. 1, 2005 to present and the aggregation result can be viewed.

Click the correspondent date in the calendar.

Or, select year and month in the combo-box under the calendar and click the [Show] button.

The screenshot shows the 'Information Disclosure Prevention Diagnosis' window. On the left is a calendar for February 2012. The main area displays a table titled 'Results of aggregated by operation' with columns for dates from 2/23 (Thursday) to 2/29 (Wednesday) and an 'Aggregation' column. The table lists operations such as 'File export', 'File operation', 'Printing operation (number of times)', 'Printing operation (number of pages)', and 'E-mail sending by recipient address'. Below the table, it shows 'Worst ranking of violation operations target day: 2012/02/15 (Wednesday)' and a message: 'Terminal that performed violation operations does not exist.'

Operation name	2/23 (Thursday)	2/24 (Friday)	2/25 (Saturday)	2/26 (Sunday)	2/27 (Monday)	2/28 (Tuesday)	2/29 (Wednesday)	Aggregation
File export	0	0	0	0	0	0	2	2
File operation	0	0	0	0	0	0	1	1
Printing operation (number of times)	0	0	0	0	0	0	2	2
Printing operation (number of pages)	0	0	0	0	0	0	20	20
E-mail sending by recipient address	0	0	0	0	0	0	2	2

### 4.2.3 Aggregate by Objectives

After selecting aggregation content corresponding to the objective, setting the conditions such as aggregation unit, aggregation period and keywords and performing log aggregation, the result can be displayed.

**When there are many cases in aggregation result, it may take some time before the result is displayed**

When there are many target data, the process of displaying [Aggregation Result] and [Result Details] may take a long time and browser timeout may occur (aggregation condition and the performance of the Management Server will also affect the processing time).

[Standard of Processing Time]

- To know printing operation status - during printing operation (frequency), 4.2 million cases require about 27 seconds
- To know file operation status - during file operation, 3.4 million cases require about 24 seconds
- To know Web access status - during the Window title obtaining with URL, 23 million cases require about 81 seconds

Under the environment of Microsoft® Internet Explorer® 6.0, the timeout duration is usually 60 minutes, but timeout may also occur due to the reasons such as network environment and other network machines.

For example, when accessing the Management Server through a proxy, timeout may occur due to the proxy. In this case, timeout can be prevented if accessing to Management Server without using a proxy according to the following procedure.

Please set the address of Management Server in [Do not Use Proxy to Access the Following Addresses] of [Tool] - [Internet Options] - [Connection] - [LAN Settings] - [Details].

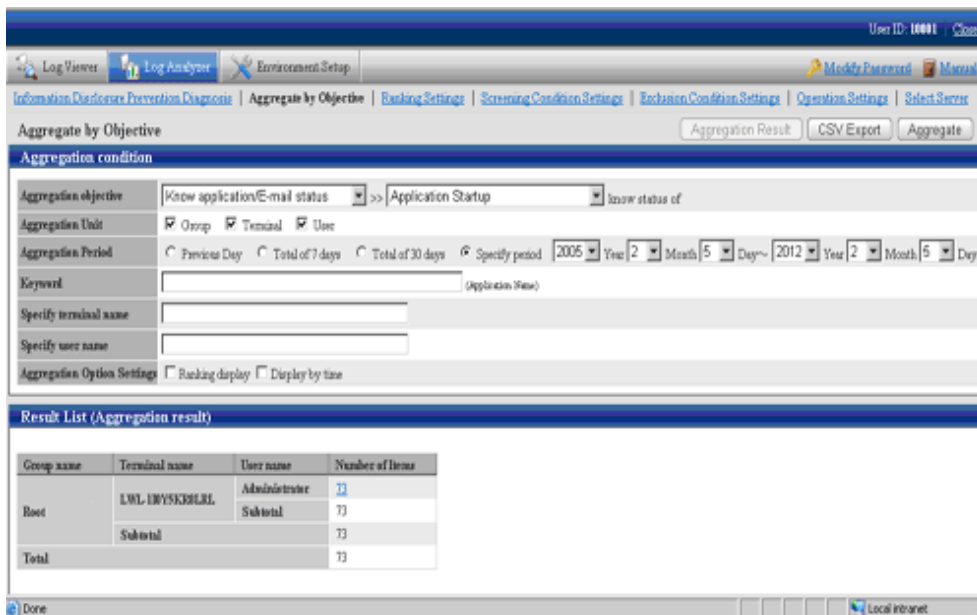
**When there is large amount of displayed content, it may take some time before the result is displayed properly, but it may also fail to display**

When a large amount of information such as a large amount of log lists and aggregation results without 24 hours are displayed in a window, it may take some time to display the result. Before the result is displayed properly, blank page may appear with only part of tables being displayed or flashing, and it looks like the page may collapse. In addition, when a large amount of information is displayed, the response of the button and browser resizing may be delayed.

**Aggregate**

The procedure is as follows:

1. After confirming that it is not in data transfer, select [Aggregate by Objective] from the function menu.  
→ The [Aggregate by Objective] window is displayed.



**Aggregation condition**



The list of log aggregation objectives is displayed.

After each objective is selected, the detailed menu (objective) is displayed.

Set aggregation unit, aggregation period and keywords, etc.

### Result List

The aggregation result is displayed.

- In [Aggregation objective], select an aggregation objective and its sub-menu.

Aggregation Objective	Sub-menu of Aggregation Objective	Content
To know violation status	To know the status of application startup prohibition	Aggregate the number corresponding to application startup prohibition .
	To know the status of printing prohibition	Aggregate the number corresponding to printing prohibition.
	To know the status of logon prohibition	Aggregate the number corresponding to logon prohibition.
	To know the status of PrintScreen key prohibition	Aggregate the number corresponding to PrintScreen key prohibition.
	To know the status of E-mail attachment prohibition	Aggregate the number corresponding to E-mail attachment prohibition.
To know file export status	To know the status of file export	Aggregate the number of file export.
	To know the status of file export (according to drive)	Aggregate the number of file export by the type of target drive as export destination.
To know file operation status	To know the status of file operation	Aggregate the number of file operation.
	To control the status of file operation (remote)	Aggregate the number of file operation on network.
	To control the status of file operation (removable)	Aggregate the number of file operation on removable media.
To know status of applications and E-mail	To know the status of application startup	Aggregate the number of application startup.
	To know the status of E-Mail sending according to recipient	Aggregate the number of E-mail sending,
To know printing operation status	To know the status of printing operation (frequency)	Aggregate the number of printing.
	To know the status of printing operation (pages)	Aggregate the total number of printed pages.
To know the Web access status	To know the window title obtaining with URL	Aggregate the number of internet access.
	To know the window title obtaining with URL (by site)	Aggregate the number of Internet access by site.
To know information disclosure status	To know the status file export	Filter logs according to filtering condition/exclusion condition and aggregate the number of file export for external media.
	To control the status of file operation	Filter logs according to filtering condition/exclusion condition and aggregate the number of file operation for external media.

Aggregation Objective	Sub-menu of Aggregation Objective	Content
	To control the status of printing operation (frequency)	Filter logs according to filtering condition/exclusion condition and aggregate the number of printing.
	To control the status of printing operation (pages)	Filter logs according to filtering condition/exclusion condition and aggregate the total number of printed pages.
	To control the status of E-mail sending according to recipient	Filter logs according to filtering condition/exclusion condition and aggregate the number of E-mail sending.

3. Set the following items.

The setting items and configuration values are shown as follows.

Item Name	Description																												
[Aggregation Unit]	<p>Specify the unit for aggregation. Multiple units can be selected.</p> <ul style="list-style-type: none"> <li>- [Group]: Aggregate in the unit of the CT group</li> <li>- [Terminal]: Aggregate in the unit of computer name (*). *) It is displayed in the CT list of the Management Console.</li> <li>- [User]: Aggregate in the unit of user name.</li> </ul> <p>When multiple units are selected, the relationship between units is in sequence of [Group]&gt;[Terminal]&gt;[User]. It is displayed from the left in large to small order.</p> <table border="1"> <thead> <tr> <th>Terminal name</th> <th>User name</th> <th>Number of items</th> </tr> </thead> <tbody> <tr> <td rowspan="2">CT-DOMAIN-Y</td> <td>Administrator</td> <td>21</td> </tr> <tr> <td>Subtotal</td> <td>21</td> </tr> <tr> <td rowspan="2">CT-WINXP</td> <td>Administrator</td> <td>15</td> </tr> <tr> <td>Subtotal</td> <td>15</td> </tr> <tr> <td rowspan="2">CT-WINXP-ZHA</td> <td>Administrator</td> <td>22</td> </tr> <tr> <td>Subtotal</td> <td>22</td> </tr> <tr> <td rowspan="2">LWL-TKSUOCI</td> <td>Administrator</td> <td>2</td> </tr> <tr> <td>Subtotal</td> <td>2</td> </tr> <tr> <td rowspan="2">PC-XY(WIN-AF)</td> <td>Administrator</td> <td>6</td> </tr> <tr> <td>Subtotal</td> <td>6</td> </tr> </tbody> </table>	Terminal name	User name	Number of items	CT-DOMAIN-Y	Administrator	21	Subtotal	21	CT-WINXP	Administrator	15	Subtotal	15	CT-WINXP-ZHA	Administrator	22	Subtotal	22	LWL-TKSUOCI	Administrator	2	Subtotal	2	PC-XY(WIN-AF)	Administrator	6	Subtotal	6
Terminal name	User name	Number of items																											
CT-DOMAIN-Y	Administrator	21																											
	Subtotal	21																											
CT-WINXP	Administrator	15																											
	Subtotal	15																											
CT-WINXP-ZHA	Administrator	22																											
	Subtotal	22																											
LWL-TKSUOCI	Administrator	2																											
	Subtotal	2																											
PC-XY(WIN-AF)	Administrator	6																											
	Subtotal	6																											
[Aggregation Period]	<p>Specify the collection date for logs to be aggregated.</p> <ul style="list-style-type: none"> <li>- [Previous Day]: Aggregate the logs 1 day before the execution of aggregation by objectives.</li> <li>- [Total of 7 days]: Aggregate the logs in the last week (7 days till the last day).</li> <li>- [Total of 30 days]: Aggregate the logs in last 30 days (30 days till the last day).</li> <li>- [Specify period]: Aggregate the logs in any time period. Please set the start date and end date. The period can be specified is from Jan. 1, 2004 to Dec. 31, 2024.</li> </ul> <p>When a large target of data that requires a long aggregation period exists like [Total of 30 days] and [Specify period], a certain amount of processing time may be consumed, so it may not be able to display properly after timeout occurs. Please aggregate by weeks and set appropriate value in aggregation period.</p>																												
[Keyword]	<p>Specify the keyword for search during aggregation. Maximum 50 characters can be entered. Aggregate the logs that partially match with the specified keyword.</p> <p>Valid keyword varies with aggregation objectives. Please refer to “<a href="#">Appendix A List of Aggregation Objectives</a>” for details.</p>																												
[Specify terminal name]	<p>Aggregate the logs that contain the specified computer name (partially match). A maximum of 60 characters can be entered.</p>																												

Item Name	Description																																																																																																																																																										
[Specify user name]	Aggregate the logs that contain the specified user name (partially match). A maximum of 40 characters can be entered.																																																																																																																																																										
[Aggregation Option Settings]	<p>Specify the display format of the aggregation result.</p> <ul style="list-style-type: none"> <li>- [Ranking display]: In the display of aggregation result, set a sequence column at the right of the number column, and it is displayed by the sequence of number of cases from more to less (when [Display by time] is specified, it is displayed by the sequence of [Total] from more to less). When display in ranking is specified, "Subtotal" will not be displayed in the aggregation result.</li> </ul> <table border="1" data-bbox="520 618 820 860"> <thead> <tr> <th>Group name</th> <th>Number of Items</th> <th>Sequence</th> </tr> </thead> <tbody> <tr><td>CT-WINXP-Z</td><td>22</td><td>1</td></tr> <tr><td>CT-DOMAIN-Y</td><td>21</td><td>2</td></tr> <tr><td>CT-WINXP</td><td>15</td><td>3</td></tr> <tr><td>WIN_XM6</td><td>2</td><td>4</td></tr> <tr><td>PC-XI(WIN-AF)</td><td>6</td><td>5</td></tr> <tr><td>WIN-204NO42</td><td>4</td><td>6</td></tr> <tr><td>LWL-TKSUO</td><td>2</td><td>7</td></tr> </tbody> </table> <ul style="list-style-type: none"> <li>- [Display by time]: The aggregation result of each time frame (1 hour) will be displayed. The time without corresponding data within the aggregation range will not be displayed.</li> </ul> <table border="1" data-bbox="520 1039 1123 1227"> <thead> <tr> <th>Time</th> <th>#1</th> <th>#2</th> <th>#3</th> <th>#4</th> <th>#5</th> <th>#6</th> <th>#7</th> <th>#8</th> <th>#9</th> </tr> </thead> <tbody> <tr> <td>Group name</td> <td>Number of Items</td> <td>Number of Items</td> <td>Number of Items</td> <td>Number of Items</td> <td>Number of Items</td> <td>Number of Items</td> <td>Number of Items</td> <td>Number of Items</td> <td>Number of Items</td> </tr> <tr><td>Root</td><td>15</td><td>2</td><td>2</td><td>2</td><td>2</td><td>5</td><td>5</td><td>5</td><td>5</td></tr> <tr><td>Child Group</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>15</td><td>15</td><td>15</td><td>15</td></tr> <tr><td>Parent</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>5</td><td>5</td><td>5</td><td>5</td></tr> <tr><td>Subtree Group</td><td>1</td><td>13</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>Leaf</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>5</td><td>5</td><td>5</td><td>5</td></tr> <tr><td>Full Group</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>Internal</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>Empty</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>Leaf</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>FullLeaf</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>Empty</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> </tbody> </table> <p>The above image shows correspondent data exists at 3pm, 4pm, 5pm, 6pm and 11pm.</p>	Group name	Number of Items	Sequence	CT-WINXP-Z	22	1	CT-DOMAIN-Y	21	2	CT-WINXP	15	3	WIN_XM6	2	4	PC-XI(WIN-AF)	6	5	WIN-204NO42	4	6	LWL-TKSUO	2	7	Time	#1	#2	#3	#4	#5	#6	#7	#8	#9	Group name	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Root	15	2	2	2	2	5	5	5	5	Child Group	1	2	2	2	2	15	15	15	15	Parent	1	2	2	2	2	5	5	5	5	Subtree Group	1	13	2	2	2	1	1	1	1	Leaf	1	2	2	2	2	5	5	5	5	Full Group	1	2	2	2	2	1	1	1	1	Internal	1	2	2	2	2	1	1	1	1	Empty	1	2	2	2	2	1	1	1	1	Leaf	1	2	2	2	2	1	1	1	1	FullLeaf	1	2	2	2	2	1	1	1	1	Empty	1	2	2	2	2	1	1	1	1
Group name	Number of Items	Sequence																																																																																																																																																									
CT-WINXP-Z	22	1																																																																																																																																																									
CT-DOMAIN-Y	21	2																																																																																																																																																									
CT-WINXP	15	3																																																																																																																																																									
WIN_XM6	2	4																																																																																																																																																									
PC-XI(WIN-AF)	6	5																																																																																																																																																									
WIN-204NO42	4	6																																																																																																																																																									
LWL-TKSUO	2	7																																																																																																																																																									
Time	#1	#2	#3	#4	#5	#6	#7	#8	#9																																																																																																																																																		
Group name	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items	Number of Items																																																																																																																																																		
Root	15	2	2	2	2	5	5	5	5																																																																																																																																																		
Child Group	1	2	2	2	2	15	15	15	15																																																																																																																																																		
Parent	1	2	2	2	2	5	5	5	5																																																																																																																																																		
Subtree Group	1	13	2	2	2	1	1	1	1																																																																																																																																																		
Leaf	1	2	2	2	2	5	5	5	5																																																																																																																																																		
Full Group	1	2	2	2	2	1	1	1	1																																																																																																																																																		
Internal	1	2	2	2	2	1	1	1	1																																																																																																																																																		
Empty	1	2	2	2	2	1	1	1	1																																																																																																																																																		
Leaf	1	2	2	2	2	1	1	1	1																																																																																																																																																		
FullLeaf	1	2	2	2	2	1	1	1	1																																																																																																																																																		
Empty	1	2	2	2	2	1	1	1	1																																																																																																																																																		

4. Click the [Aggregate] button.

- Aggregate by objectives cannot be used by multiple users at the same time.

When another user has already obtained the aggregation result or the aggregation process is being executed, the following message will be displayed:

Aggregation function may be in use by another user. Do you want to continue?

When another user has already obtained the aggregation result, after clicking the [OK] button, the aggregation will be executed while the aggregation result of another user will be aborted.

When another user is performing the aggregation process, an error message will be displayed, and execution cannot be performed until the other user finishes the processing.

- In the process of aggregation or cancellation of aggregation, please do not execute the following operations. If the execution is started, the uncompleted processing will be remained and processing may not be able to be performed in a certain time.
  - Move to windows displayed in Global Navigation and function menu
  - Logout operation
  - Window operation based on browser functions ([Close], [Back], [Update], etc.)

## Aggregation Result

The screenshot shows the 'Aggregate by Objective' interface. The 'Aggregation condition' section includes the following settings:

- Aggregation objective: Know application/E-mail status >> Application Startup
- Aggregation Unit:  Group,  Terminal,  User
- Aggregation Period:  Previous Day,  Total of 7 days,  Total of 30 days,  Specify period (2005 Year 2 Month 5 Day ~ 2012 Year 2 Month 5 Day)
- Keyword: (Application Name)
- Specify terminal name: (empty)
- Specify user name: (empty)
- Aggregation Option Settings:  Ranking display,  Display by time

The 'Result List (Aggregation result)' table is as follows:

Group name	Terminal name	User name	Number of Items
Root	LWL-IMPVSKRRLK	Administrator	73
		Subtotal	73
	Subtotal		73
Total			73

- The name of the aggregation unit ([Group], [Terminal], [User]) is displayed in the left column of the table. The root group in the CT group tree of Management Console will be displayed as "Root" in [Group name]. In addition, the group managed by level structure is displayed as "1-level/2-level/3-level".
- When display in ranking is selected, the sequence column at right is ranked in the sequence of displayed number of times from more to less.
- The total value is displayed in the last line.
- When multiple aggregation units are selected, the subtotal line will be displayed. However, during display in ranking, the subtotal line will not be displayed.
- The aggregation value of each aggregation unit can be displayed in the Number column. After clicking the aggregation value, details can be displayed. When the value of [Number] is relatively large, the error "[ERR-DTLAC199] Error occurred during processing]" will occur when displaying the detailed result. In this case, please execute the following countermeasures to display the detailed result after specifying a smaller value for [Number].
  - Reduce [Aggregation Period]
  - Increase [Aggregation Unit] (since each item of [Group], [Terminal] and [User] is AND condition, conditions needs to be filtered)
  - Filter by [Keyword]
  - Aggregate by time

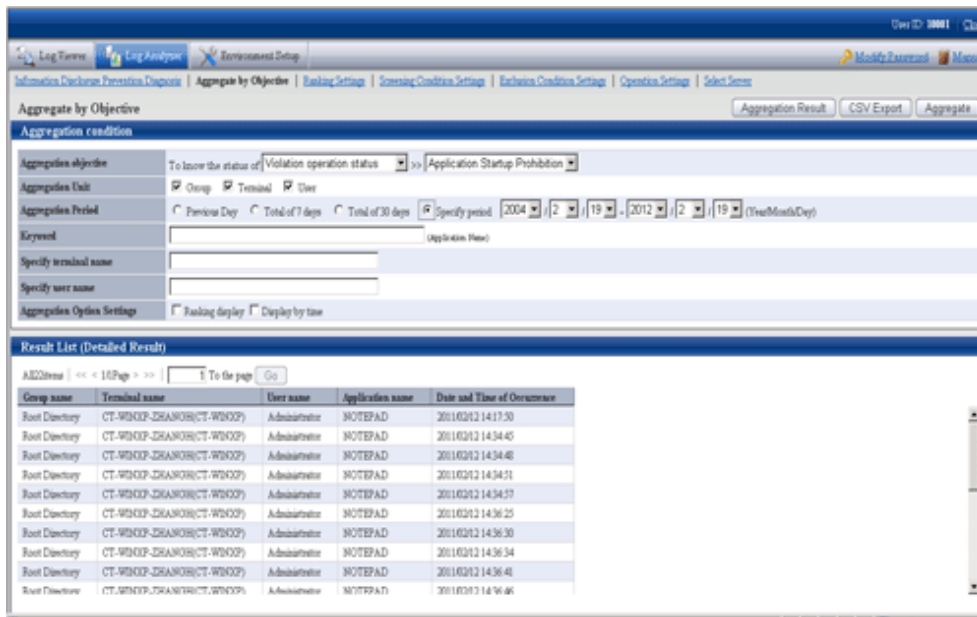
## Detailed Result

After the link of [Number] is clicked, the details of the aggregation value will be displayed. If the log has no detailed item or has blank detailed items, it will be displayed with "-".

During "Show Details" display, when there is a large number of cases, the result will be displayed in unit of 1000 cases. The average size of data displayed on each page is 0.5MB. When a large amount of detailed results is displayed (for example, when 100,000 cases of "Show Details" results are displayed) a disk capacity of about 50MB is required. When the disk capacity is not enough, to reduce the aggregation value as much as possible, please refine the aggregation unit and reduce the aggregation period before detailed displayed.

In the process of aggregation or cancellation of aggregation, please do not execute the following operations. If the execution is started, the uncompleted processing will be remained and processing may not be able to be performed in a certain time.

- Move to windows displayed in Global Navigation and function menu.
- Logout operation
- Window operation based on browser functions ([Close], [Back], [Update] .etc)



Displayed content varies with aggregation objectives. Please refer to “[Appendix A List of Aggregation Objectives](#)” for details.  
To return to the aggregation result, please click the [Aggregation Result] button.

### Export Aggregation Result or Detailed Result in CSV Format

In aggregation by objectives, the aggregation result or detailed result can be exported to files in CSV format.

The aggregation result can be used by taking the downloaded CSV file as Microsoft® Office Excel data.

The procedure is as follows:

1. Click the [CSV Export] button displayed at the bottom of the table of the aggregation result or detailed result.
  - In the environment with Microsoft® Office Excel installed, the [File Download] window is displayed.
2. Click [Open] or [Save].
  - The name of file for saving the aggregation result is “report.csv”.
  - The name of file for saving the detailed result is “detail.csv”.

Any file name can be renamed.

# Chapter 5 Audit Operations on Client (CT) via Log Viewer

Operations of the client (CT) users will be saved on the server as various logs. The system administrator or department administrator confirms operation content of CT users as daily operations via the log viewer.

Special processing is not required when the user operates in accordance with operation guidelines. However, it is required to investigate what client (CT) users want to do and whether these operations may result in possibilities of information leakage when any operation suspected to violate operation guidelines or misoperation is detected.

The file names left in the log can be used to trace file operation by the user or search the information of the CT that performed the misoperation.

If it is required to review policies according to investigation results, the policy corresponding to the client (CT) and user should be modified. Thus, violation can be prevented from happening again and system operation will protect internal information more safely.

## 5.1 Start Log Viewer



### Note

#### Notes concerning the startup of web console

Please do not start multiple web consoles on one PC.

### Start Log Viewer

1. Start the web console through any of the following methods:

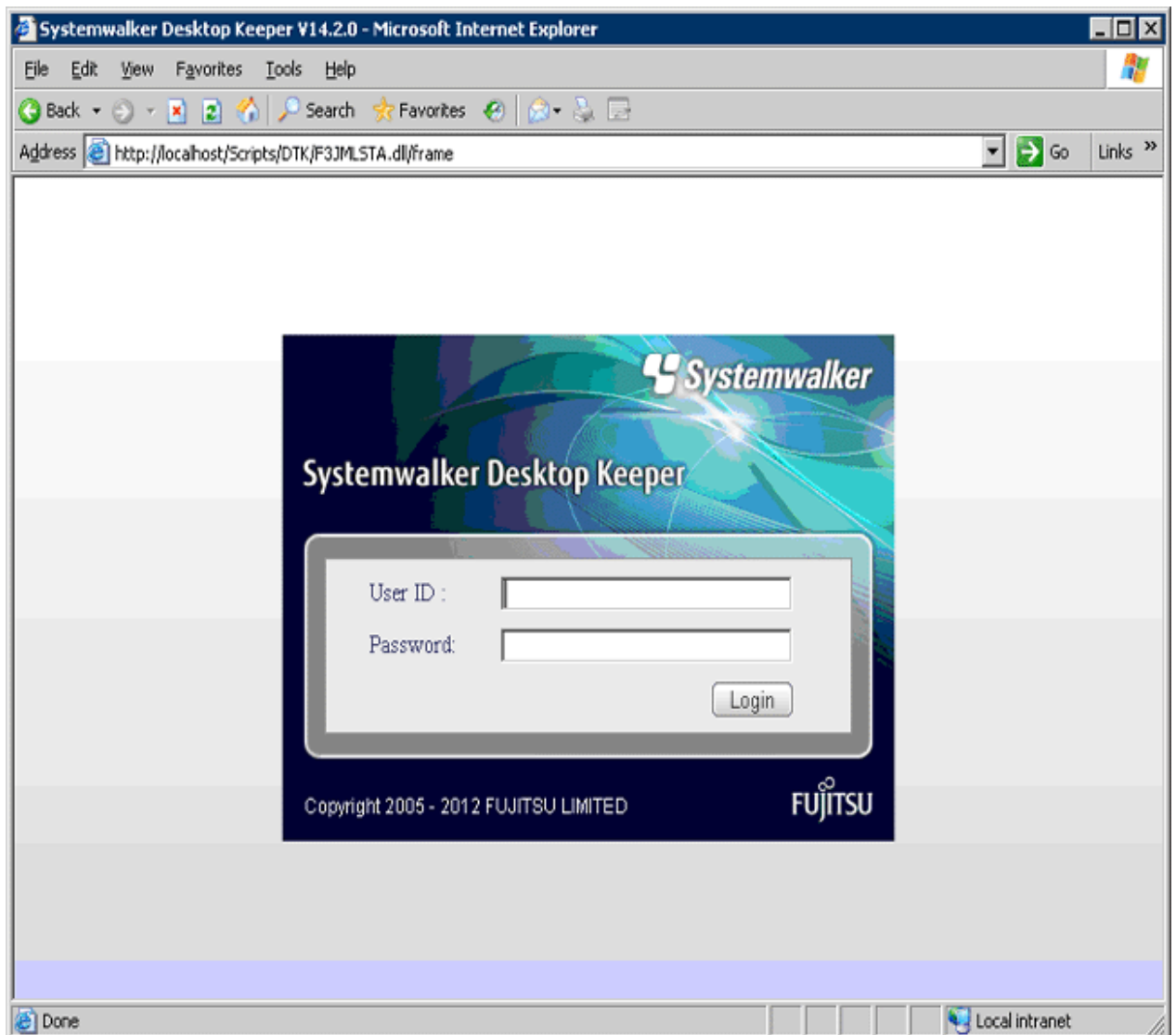
**In a 2-level structure:** Please connect to the Management Server.

- Select [Programs] - [Systemwalker Desktop Keeper] - [Server] - [Desktop Keeper Main Menu] from the [Start] menu of Management Server.
- Specify the address of browser to “http://host name or IP address of management server/DTK/index.html”  
If IIS port number has been changed, specify as follows:  
http:// IP address: port number/DTK/index.html

**In a 3-level structure:** Please connect to the Master Management Server.

- Select [Programs] - [Systemwalker Desktop Keeper] - [Server] - [Desktop Keeper Main Menu] from the [Start] menu of Master Management Server.
- Specify the address of browser to “http://host name or IP address of master management server/DTK/index.html”  
If IIS port number has been changed, specify as follows:  
http:// IP address: port number/DTK/index.html

→The [Login] window is displayed.



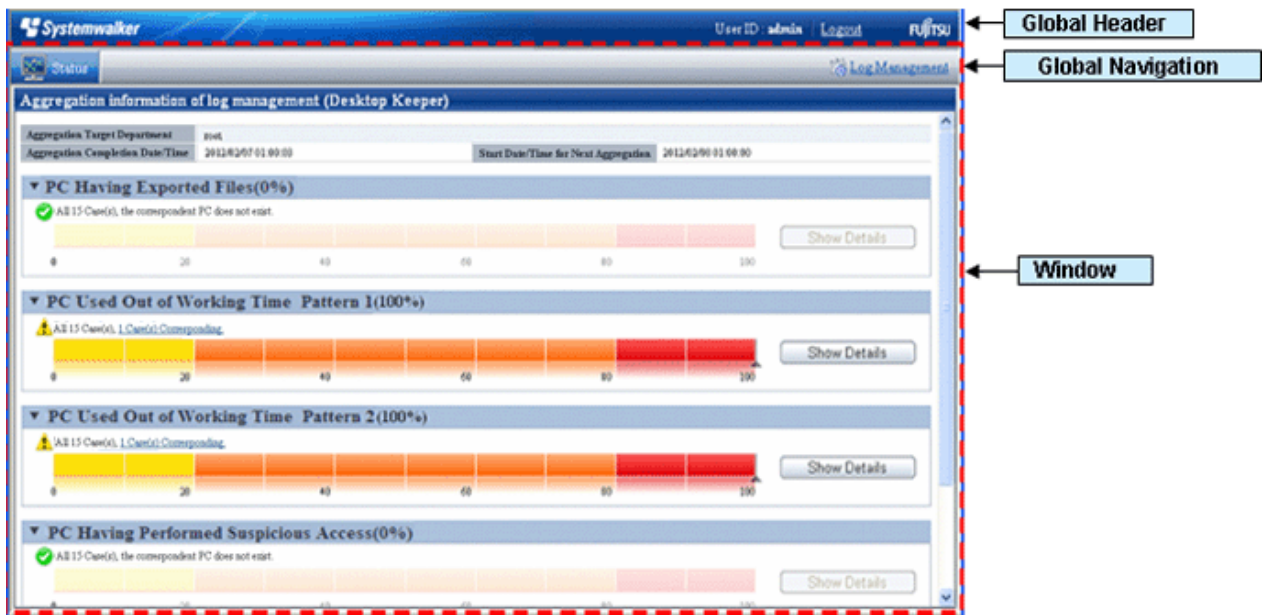
2. Enter the following information and click the [Login] button.

The system administrator and department administrator log in the same way.

When performing a single sign-on link with Systemwalker Desktop Patrol, the entered User ID should be case-sensitive.

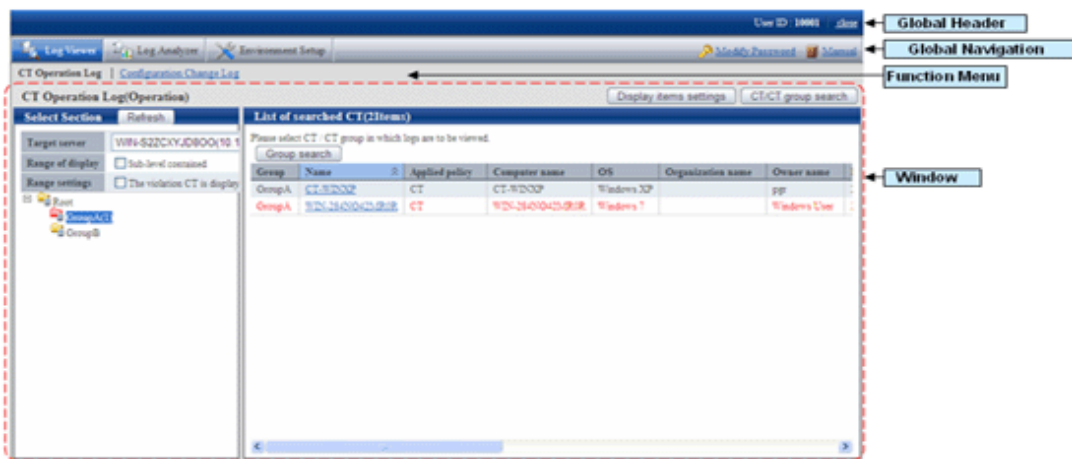
- **[User ID]:** [User ID] set in the [Administrator Information Settings] window of the Server Settings Tool.
- **[Password]:** [Password] set in the [Administrator information settings] window of the Server Settings Tool  
It is recommended to change the password regularly. For details on how to do so, please refer to "[Change password](#)".

→ The status window is displayed.



3. Select [Log Management] from Global Navigation.

→Log Viewer is started, and the [CT Operation Log] window is displayed.



Window content

#### Global Header

- User ID: The user ID for login is displayed.
- close: Close the Log Viewer window.

#### Global Navigation

- Log Viewer: The Log Viewer window is displayed.
- Log Analyzer: The Log Analyzer window is displayed.
- Environment Setup: The option window (the window used to set aggregation condition on which the aggregation results displayed in the status window are based).
- Modify Password: Change the password for starting the Web Window. (Please refer to “Change password” for how to change password)
- Manual: Display the manual.

#### Function Menu



- CT Operation Log: Search and display CT Operation Logs.
- Configuration Change Log: Search and display Configuration Change Logs.

### Contents

- [Display items settings]: The selection of visible columns in [List of searched CT] and the display sequence can be modified. Please refer to “[Set visible columns in \[List of searched CT\]](#)” for details.
- [CT/CT group search]: The [CT operation log(Operation) - CT/CT group search] window is displayed. Search after setting the conditions if the location of client (CT) and CT group under Management Server is not known.
- [Select Section]: The server name next to the root directory and its subordinate CT groups are displayed.
  - [Refresh]: Import the latest tree structure and CT list information of server selected from [Target Server].
  - [Target server]: Select the Management Server or Master Management Server to be connected with.
  - [Range of display]
 

If the checkbox is selected, the selected CT group and all its subordinate CTs will be displayed in [List of searched CT].









If the checkbox is not selected, all CTs directly under the selected CT group will be displayed in [List of searched CT].
  - [Range settings]
 

When this item is selected, only the client (CT) that generates violation logs will be displayed in [List of searched CT]. When the client (CT) under the group has already been displayed in [List of searched CT], after this item is selected, it will change to display only the client (CT) that generates violation logs.

When this item is not selected, client (CT) under the group will be displayed in [List of searched CT].

### Icons of CT Group Tree

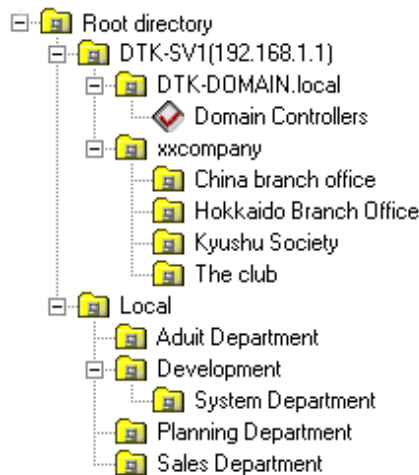
Icons displayed in the CT Group tree vary depending on the different users log in to Log Viewer. The following describes the conditions for displaying each icon.

User logs on to Log Viewer	Displayed icon	Meaning of icon
System administrator		All groups will be displayed with identical icons when the system administrator logs on to the Log Viewer.  This indicates the group in which “ <a href="#">Display the group or client (CT) that has generated violation logs in red</a> ” is not set; or no violation log has been generated though settings have been performed.
		This indicates the group in which “ <a href="#">Display the group or client (CT) that has generated violation logs in red</a> ” has been set and violation log has been generated in the set time.
		This indicates the “Deleted CT” group.
		This indicates the “Not Configured” group.
Department administrator		This indicates if a group has been set as the department administrator.
		This indicates if a group has not been set as the department administrator.
		This indicates the group in which <a href="#">Display the group or client (CT) that has generated violation logs in red</a> ” has been set and in which a violation log has been generated in the set time.
		This indicates that the CT group that has been set as the department administrator exists in the sub-group of this group.

### Domain display

When linking with Active Directory, the domain name is always displayed together with the server name.

[Example of domain displayed during link with Active Directory]

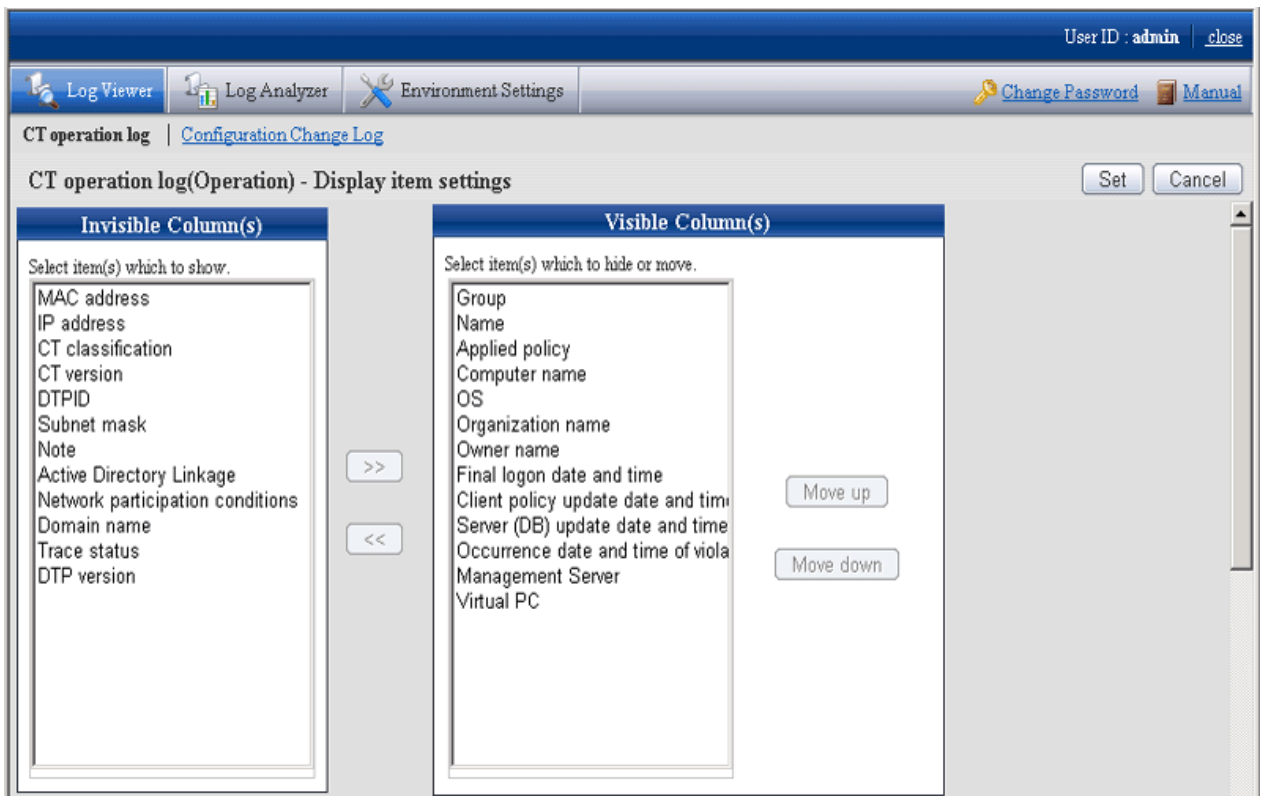


- [List of searched CT]: The client (CT) belongs to the selected group is displayed. The item to be displayed can be selected. For the method, please refer to “[Set visible columns in \[List of searched CT\]](#)”

### Set visible columns in [List of searched CT]

1. Click the [Display items settings] button in the [CT Operation Log] window.

→ The [Display items settings] window is displayed.



- [Invisible Column(s)]: Items that will not be displayed in “List of searched CT”.
- [Visible Column(s)]: Items that will be displayed in “List of searched CT”. The initial value will be displayed as the items with \* in the following table.

In addition, the display sequence can be modified. Items are displayed from left to right in “List of searched CT” by names in the order from top to bottom. Item description is as follows.

Item Name	Description
[Name] (*)	The name that can be added to client (CT), initial value is the computer name. Please refer to “ <a href="#">Modify CT Policy</a> ” during modification. [Name] cannot be set to a item not displayed.
[Group] (*)	This is the group to which the client (CT) belongs.
[Applied policy] (*)	This is the policy that is applied. [CT]: This indicates the CT policy that has been set. [Group]: This indicates the CT group policy has been set.
[Computer name] (*)	This is the computer name of client (CT).
[MAC address]	This is the MAC address of client (CT).
[IP address]	This is the IP address of client (CT)
[OS] (*)	This is the OS name of client (CT).
[CT classification]	This is displayed as [SE] (for Standard Edition versions prior to V13.2.0, it is displayed as [SE]; for Base Edition, it is displayed with blank)
[CT version]	This is the version of the client (CT) of Systemwalker Desktop Keeper that is installed. In addition, for correspondence of product version/edition, please refer to “CT version” of “Systemwalker Desktop Keeper Reference Manual”.
[DTPID]	This is “User ID (+) PC Name” of Systemwalker Desktop Patrol Client (CT) This will be displayed when both Systemwalker Desktop Keeper Client (CT) and Systemwalker Desktop Patrol Client (CT) are installed on the same PC.
[Organization name] (*)	This is the organization name set in the OS of client (CT).
[Owner name] (*)	This is the owner name set in the OS of client (CT).
[Subnet mask]	Subnet mask set up in the client (CT) network.
[Active Directory Linkage]	This shows whether the client imports information by Active Directory Linkage. - If the client (CT) imports information by Active Directory Linkage: (Blank) - If the client (CT) imports information by a method other than Active Directory Linkage: It is displayed as [Non-target]
[Network participation conditions]	Network participation situation of the client (CT) is displayed. - [Domain]: This is displayed it belongs to domain. - [Group]: This is displayed if it does not belong to domain.
[Domain name]	The name of domain to which the client belongs is displayed. The group name will be displayed when [Network Participation] is [Group].
[Final logon date and time] (*)	The client (CT) communicates with Master Management Server or Management Server during its startup. This is the final date and time when the server performs the following tasks on the client during communication, - Send CT policy. - Send user policy.

Item Name	Description
[Client policy update date and time] (*)	<p>This is the final date and time when the Master Management Server or Management Server sends CT policy to the client (CT).</p> <p>It is displayed or updated in the following cases:</p> <ul style="list-style-type: none"> <li>- The client (CT) added to the CT list starts to communicate with the Master Management Server or Management Server after it has been re-started;</li> <li>- When CT policy is reflected on the client (CT) after the [Update Immediately] button on the Management Console is clicked.</li> </ul>
[Server (DB) update date and time] (*)	<p>This is the latest date and time when the Management Server or Master Management Server updates the policy of client (CT) and reflects it to the database (including immediate update).</p>
[Note]	<p>This is the information input when updating policy of the client (CT). When it needs to be modified, please refer to "<a href="#">Modify CT Policy</a>".</p>
[DTP version]	<p>This is the version of Systemwalker Desktop Patrol Client installed in PC.</p>
[Trace status]	<p>This is the setting of trace collection in client (CT).</p> <ul style="list-style-type: none"> <li>- [Summary]: Collect the trace of the client (CT) at summary level.</li> <li>- [Details]: Collect the trace of the client (CT) at detail level.</li> <li>- Blank: Do not collect the trace of the client (CT), or the client (CT) is V12.0.</li> </ul>
[Occurrence date and time of violation log] (*)	<p>This is the date and time when violation logs are collected on client (CT).</p>
[Management Server]	<p>The computer name of the management server to which the client belongs.</p>
[Virtual PC]	<p>The following icons will be displayed if the client (CT) is installed in a virtual environment:</p> <ul style="list-style-type: none"> <li>- [-(Master)]: Master image of virtual PC</li> <li>- [-]: Virtual PC</li> </ul>

\*) Items displayed as initial value.

2. Set visible columns and display sequence and click the [Set] button.

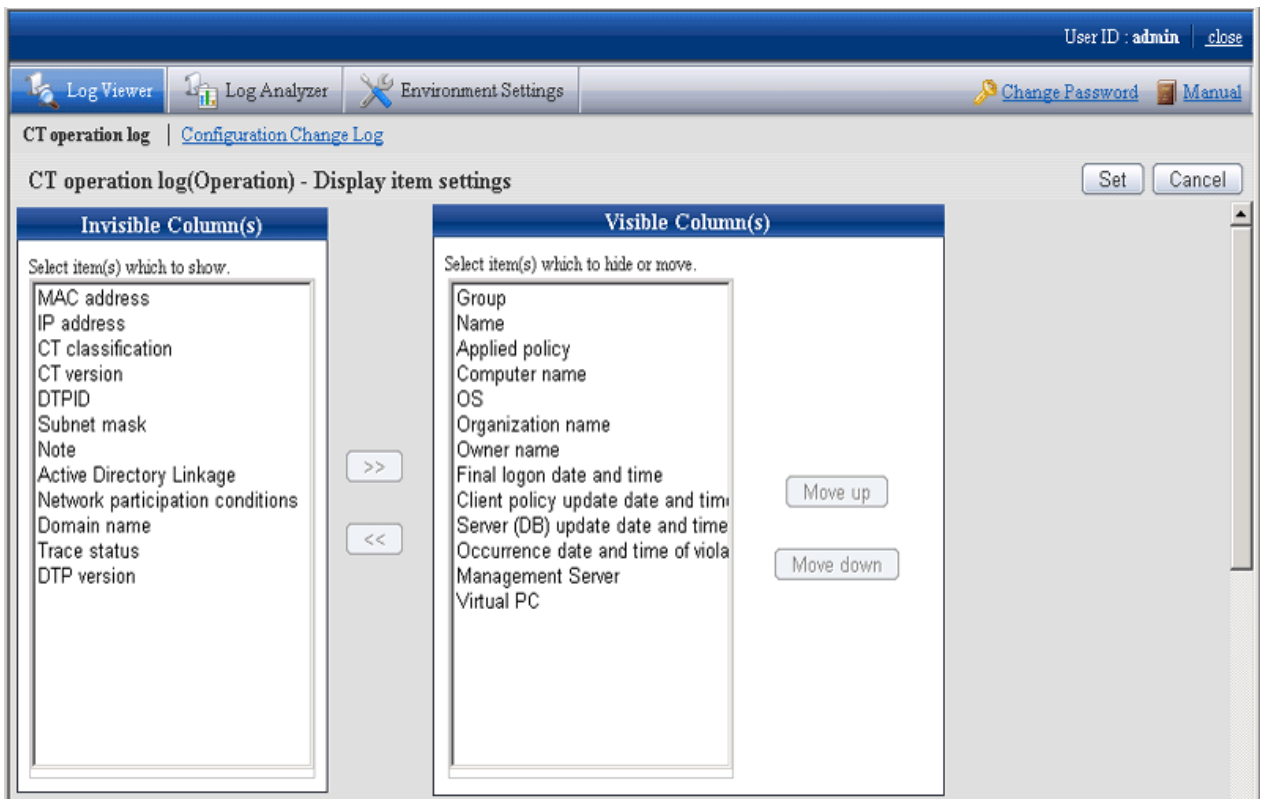
### Display the "Deleted CT" group in [Select Department] display domain

To view the logs of a deleted (moved to "Deleted CT" group) client (CT), the "Deleted CT" group needs to be displayed in the [Select Department] display domain.

Nobody but the system administrator can Perform this operation.

1. Click the [Display items settings] button in the [CT Operation Log] window.

→The following window is displayed.



2. Click the [Display] button in [Display deleted CT group] of [Department display settings].

3. Click the [Set] button.

When linking with Active Directory, it will be displayed as the last group under Local group.

When Active Directory Linkage is not performed, it will be displayed as the last group under the server.

The method of viewing and searching the logs of a client (CT) that belongs to the “Deleted CT” group is the same as that of viewing and searching logs of client (CT) of other CT group.

### Display the group or client (CT) that has generated violation logs in red

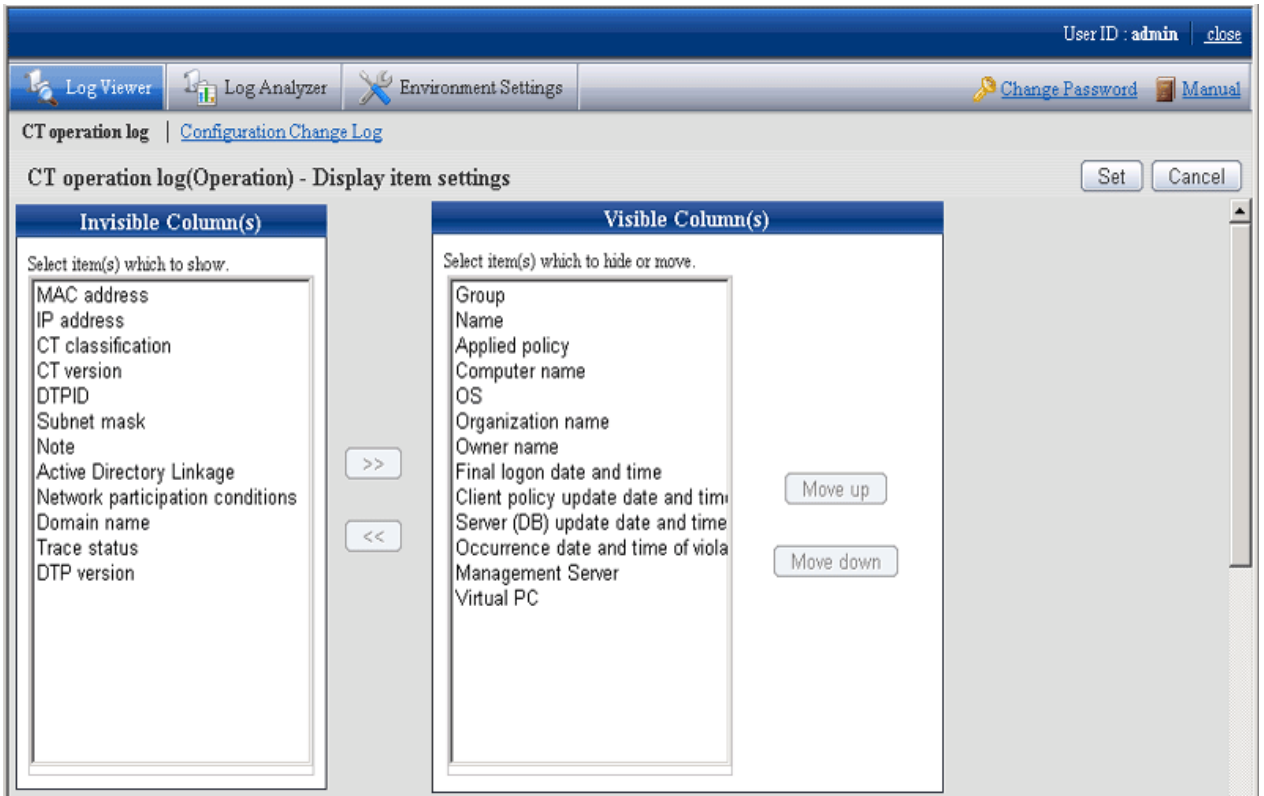
After [Violation CT display settings] has been performed, the CT group in which violation logs have occurred will be displayed in red when Log Viewer is started.

After selecting the CT group that is displayed in red, the column of the CT where violation log occurred will be displayed in red in [List of searched CT].

After clicking the [Select CT] button, the column of CT with violation log occurred will be displayed in red in [Select CT]. In addition, [Number of violation logs] will also be displayed in the visible columns.

1. Click the [Display items settings] button in the [CT Operation Log] window.

→ The following window is displayed.

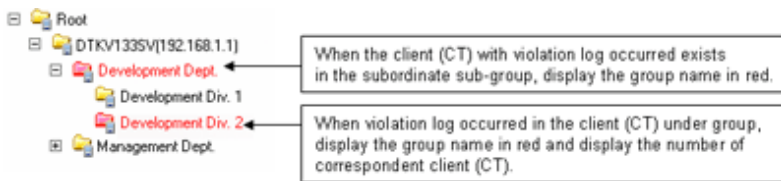


Item description is as follows.

Item Name	Description
[Display violation CT]	<p>Set the group to which the client (CT) that has generated violation log belongs in the “Select Department” window and the method of displaying the client (CT) that has generated a violation log.</p> <ul style="list-style-type: none"> <li>- <b>Display</b> Display the group to which the client (CT) that has generated a violation log belongs and the number of clients (CTs) that have generated a violation log in red.</li> <li>- <b>Not display</b> Do not display the clients (CTs) that have generated a violation log in red even if they exist.</li> </ul> <p>Initial value: [Not display] is select.</p>
[Violation range of display]	<p>Set whether to display the situation in which the client (CT) that has generated the violation log exists in a certain range of time prior to the startup date of Log Viewer in red. Setting can be performed when [Display] is selected from the [Display violation CT] window.</p> <ul style="list-style-type: none"> <li>- This day</li> <li>- If violation logs generate on the date of starting Log Viewer, display the client (CT) and CT group in red.</li> <li>- Within yesterday Display the client (CT) and CT group that have generated violation logs from the date of starting Log Viewer and one day before it in red. (Example) If the Log Viewer is started on Feb 10, 2010, the client (CT) and CT group</li> </ul>

Item Name	Description
	<p>that have generated violation logs on Feb. 9, 2010 and Feb. 10, 2010 will be displayed in red.</p> <ul style="list-style-type: none"> <li>- Within one week Display the client (CT) and CT group that have generated violation logs within a week before the day (included) of starting Log Viewer in red. (Example) If the Log Viewer is started on Monday, display the client (CT) and CT group that have generated violation logs from last Monday to the day of startup in red.</li> <li>- Within this month Display the client (CT) and CT group that have generated violation logs from the first day of startup month to the date of starting Log Viewer in red. (Example) If the Log Viewer is started on Feb 10, 2010, display the client (CT) and CT group that have generated violation logs from Feb 1 to 10, 2010 in red.</li> <li>- Within the specified date Display the client (CT) and CT group that have generated violation logs from the specified day to the date of starting Log Viewer in red.</li> </ul>
[The specified date]	<p>Setting can be performed when [Within the specified date] is selected from [Violation range of display].</p> <p>Display the client (CT) and CT group that have generated violation logs from the specified day to the date of starting Log Viewer in red.</p>

2. Set each item and click the [Set] button.



## Change the database to be viewed



Note

### About department administrator

The department administrator cannot view the log viewing database.

Select the database to view operation logs.

1. Click the [Display items settings] button in the [CT Operation Log] window.

→The following window is displayed.

A Item Description Item is as follows.

Item Name	Description
[Viewing database settings]	Set the database to be viewed by Log Viewer <ul style="list-style-type: none"> <li>- <b>Operation database</b> The operation database is viewed by Log Viewer.</li> <li>- <b>Log viewing database</b> The log viewing database is viewed by Log Viewer.</li> </ul> Initial value: Select [Operation database]. Setup is not possible if the Log viewing database has not been created

2. Select the database to be viewed and click the [Set] button.

### Modify search target

Set “Search the terminals that are specified as the search range of operation logs only”, or “Also search the connection source terminal and connection target terminal of specified terminal”.



1. Click the [Display items settings] button in the [CT Operation Log] window.

→The following window is displayed.

A Item description is as follows.

Item Name	Description
[Log search settings]	<p>Set the search range of operation log.</p> <ul style="list-style-type: none"> <li>- <b>Logs of the specified terminal are searched only</b> Search operation logs of specified terminals only.</li> <li>- <b>Logs of connection source terminal and connection target terminal of the specified terminal are also searched</b> Search operation logs including connection source terminal and connection target terminal of specified terminal.</li> </ul> <p>Initial value: [Logs of the specified terminal are searched only] is selected</p>

2. Select the database to be viewed and click the [Set] button.

## Change password

1. Select [Modify Password] of Global Navigation.

→The [Modify Password] window is displayed.

2. Enter the following information, and click the [OK] button.
  - [Current password]: Enter the password that is currently used.
  - [New password]: Enter the new password with single-byte alphanumeric characters or symbols (1-32 characters). However, “&”, “\”, “:”, “?”, “””, “~”, “^”, “””, “<”, “>”, “|” and space are not allowed. In addition, the password is case-sensitive.

- [Enter password again]: Enter the new password again.

## 5.2 View Logs

This department describes the range of logs that can be viewed by the System Administrator and department administrators, the types of logs that can be viewed and how to view logs.

### Range of logs can be viewed

#### System administrator views logs

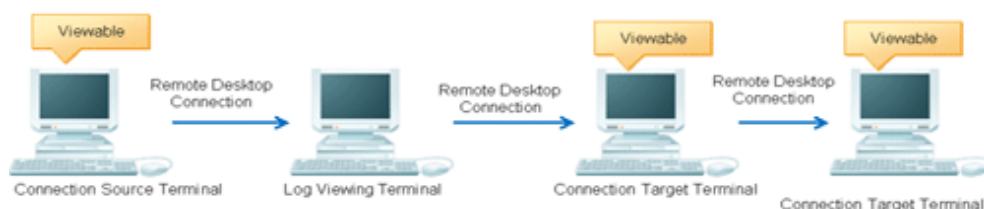
The System Administrator may view, search and perform CSV export of logs for all CTs/CT groups through Log Viewer.

#### Department administrator views logs

A department administrator may view, search and perform CSV export of logs for the CT group that has been set as the department administrator itself and its subordinate groups through Log Viewer.

Operation logs of remote connection source terminal and remote connection target terminal can be viewed as well

When viewing the operation logs of the terminal specified during remote connection via remote desktop, etc., the remote connection source terminal or remote connection target terminal can also be viewed.



The following settings are required using this function:

- Install the client (CT) in both the connection source terminal and connection target terminal
- Set [System settings] - [Connection Information between terminals] of Server Settings Tool to [Manage].
- Set [Log search settings] of the [Display items settings] window of Log Viewer to [Logs of connection source terminal and connection target terminal of the specified terminal are also searched].

### Type of logs can be viewed

The logs that can be viewed in Log Viewer are shown in the following list.

Policy needs be set and reflected in the Management Console for viewing logs. For details on policy setting and reflection, please refer to “2.4.1 Perform Terminal Initial Settings”, “Modify CT Policy” or “3.4.2 Modify User Policy”.

For details on the method of viewing logs, please refer to “5.2.1 View Logs in [CT Operation Log] Window”, “5.2.2 View in [Configuration Change Log]”.

View logs in the [CT Operation Log] window

Type of logs can be viewed	Log description	Policy set prior to log viewing
Application Startup Log	This is the log when starting an application in the (CT). When linking with Citrix XenApp, the application startup operation performed in Citrix XenApp client will be recorded.	Set [Application Startup Log] of the [Log Switches] tab to [Yes].

Type of logs can be viewed	Log description	Policy set prior to log viewing
Application Termination Log	This is the log when terminating an application in the client (CT). When linking with Citrix XenApp, the application termination in Citrix XenApp client will be recorded.	Set [Application Termination Log] of the [Log Switches] tab to [Yes].
Application Startup Prohibition Log	This is the log when starting a prohibited application in client (CT). It is displayed in red in [Log Switches].	Set [List of EXE names of startup prohibition application] in [List of startup prohibition application] of the [Application Startup Prohibition] tab.
Window Title Obtaining Log	This is the log when an application started in the client (CT) is displayed in the window. When linking with Citrix XenApp, the window title of the application started in the Citrix XenApp client will be recorded.	Set [Window title obtaining Log] of the [Log Switches] tab to [Yes].
E-mail Sending Log	This is the log when E-mails have been sent in the client.	Set [E-mail Sending Log] of the [Log Switches] tab to [Yes]. Set [Confirm recipient address when sending E-mail] of the [E-mail Sending] tab to [Confirm].
E-mail Sending Interruption Log ( <b>This function is not available.</b> )	<b>This function is not available.</b> This is the log when E-mail sending has been cancelled as the warning message for confirming recipient address appears during E-mail sending.	Set [E-mail Sending Log] of the [Log Switches] tab to [Yes]. Set [Confirm recipient address when sending E-mail] of the [E-mail Sending] tab to [Confirm].
E-mail Attachment Prohibition Log ( <b>This function is not available.</b> )	<b>This function is not available.</b> This is the log when a prohibited file is attached to the E-mail for sending or saving in the client (CT). It is displayed in red in [List of logs].	Set [Extension] in [List of Extensions] of the [E-mail Sending - E-mail Attachment Prohibition Extension Settings] window linked via the [E-mail Sending] tab. Select [Prohibit] of the [E-mail Sending] tab.
Device Configuration Change Log	This is the log when device configuration has been changed in the client (CT). When violations such as inserting an unauthorized USB device occur, they will be displayed in red in [List of logs].	Set [Device Configuration Change Log] of the [Log Switches] tab to [Yes].
Printing Operation Log	This is the log when Printing operation has been performed in the client (CT). When linking with Citrix XenApp, the printing performed in the Citrix XenApp Client will be recorded. A printing log will be recorded in both the Citrix XenApp Server and Citrix XenApp Client when printing is performed via a virtual printer.	Set [Printing Operation Log] of the [Log Switches] tab to [Yes].
Printing Prohibition Log	This is the log when printing is performed by an application that is not allowed to print in the client (CT). (Displayed in red in [List of logs])	Set [Printing Prohibition] of the [Printing Prohibition] tab to [Yes].

Type of logs can be viewed	Log description	Policy set prior to log viewing
Logon Prohibition Log ( <b>This function is not available.</b> )	<b>This function is not available.</b> This is the log when logging on with a prohibited group in the client (CT). It is displayed in red in [List of logs].	Set [Logon Prohibition Group] in [List of Logon Prohibition Groups] of the [Logon Prohibition] tab.
File Export Log	This is the log when exporting files with the File Export Utility in client (CT).	Set [File Export Log] window in the [Log Switches] tab to [Yes].
PrintScreen Key Operation Log	This is the log when operating the PrintScreen key in the client (CT).  When linking with Citrix XenApp, PrintScreen operations performed in the Citrix XenApp Client will be recorded.	Set [PrintScreen Key Operation Log] of the [Log Switches] tab to [Yes].
PrintScreen Key Prohibition Log	This is the log when the prohibited PrintScreen key is used in the client (CT). It is displayed in red in [List of logs].	Set [Disabling PrintScreen Key] of the [Printing Prohibition] tab to [Yes].
Web Operation Log	This is the log when the following operation is performed in client (CT):  - Upload or download from Web sites.  When linking with Citrix XenApp, Web operations performed in the Citrix XenApp Client will be recorded.	Set [Web Operation Log] of the [Log Switches] tab to [Yes].
Web Operation Prohibition Log	This is the log when the following operation is performed in the client (CT). It is displayed in red in [List of logs].  - Access to prohibited URL.  - Download from the prohibited URL.	Set [URL access] of the [URL Access Prohibition] tab to [Prohibit].  Set [Upload and Download] of the [Web Upload and Download Prohibition] tab to [Prohibit].
FTP Operation Log	This is the log when the following operation is performed in client (CT):  - Upload files to FTP server  - Download files from FTP server  When linking with Citrix XenApp, FTP operations performed in the Citrix XenApp Client will be recorded.	Set [FTP Operation Log] of the [Log Switches] tab to [Yes].
FTP Operation Prohibition Log	This is the log when connecting to a prohibited FTP server from the client (CT). It is displayed in red in [List of logs].	Set [FTP Server Connection] of the [FTP Server Connection Prohibition] tab to [Prohibit].
Clipboard Operation Log	This is the log when copying information (text, image) from the virtual environment to the physical environment or from the physical environment to the virtual environment via the clipboard.  When linking with Citrix XenApp, clipboard operations between the Citrix XenApp Server and Citrix XenApp client will be recorded.	Set [Clipboard Operation Log (Virtual Environment)] of the [Log Switches] tab to [Yes].
Clipboard Operation Prohibition Log	This is the log when copying a message (text, image) from the virtual environment to the physical environment or from the physical environment to the virtual environment via the clipboard is prohibited. It is displayed in red in [List of logs].	Set [Prohibition of clipboard operation between different environments] of the [Virtual Environment setup] tab to [Prohibit].

Type of logs can be viewed	Log description	Policy set prior to log viewing
File Operation Log	This is the log when a file operation is performed in the client (CT).	Set [File Operation Log] of the [Log Switches] tab to [Yes].  Set the items in the [File Operation Process] tab.  Set [Extension] in [List of File Operation Log Obtaining Extension] in the [File Operation Extension] tab.
Logon/Logoff	This is the log when the following operations are performed in the client (CT):  <ul style="list-style-type: none"> <li>- Logon</li> <li>- Logoff</li> <li>- PC startup</li> <li>- PC shut-down</li> <li>- PC sleep</li> <li>- PC recovery</li> <li>- PC connection</li> <li>- PC disconnection</li> </ul> <p>When linking with the Citrix XenApp, connection/disconnection from the Citrix XenApp Client to Citrix XenApp Server will be recorded. In addition, startup/shut-down of the Citrix XenApp Client will also be recorded.</p>	Set [Logon,Logoff Log] of the [Log Switches] tab to [Yes].
Linkage Application Log	This is the log of applications linked with the client (CT). For information about linking another applicatino to the client (CT), please refer to “Link with Other Products” in “Systemwalker Desktop Keeper Operation User’s Guide”.	Set [Linkage Application Log] of the [Log Switches] tab to [Yes].
Command Log ( <b>This function is not available.</b> )	This is the log of the command input in the client (CT) and command result.  When linking with Citrix XenApp, the command operation performed in the Citrix XenApp Client will be recorded.	Set [Command Log] of the [Log Switches] tab to [Yes].



.....

**How to distinguish “PrintScreen Key Operation Log” from “PrintScreen Key Prohibition Log”**

“PrintScreen Key Operation Log” and “PrintScreen Key Prohibition Log” are managed as the same log type. (Managed as log type of “PrintScreen Key Prohibition Log”)

Therefore, by displaying “PrintScreen Key Operation Log” as “Normal” and “PrintScreen Key Prohibition Log” as “Violation”, the logs can be distinguished. When it is displayed as “Violation”, it is displayed in red in [List of logs].

.....

**View logs in [Configuration Change Log] window**

“Configuration Change Log” refers to the logs of operation on the Management Console (modify the configuration information of CT policy/user policy and perform CSV export .etc) and operation in Log Viewer (log search and file trace, .etc). It is not required to

perform policy setting for the purpose of log collection.

The following 4 types of logs can be viewed in the [Configuration Change Log] window:

- [Terminal Settings]: Record of modified client (CT) policy.
- [Level composition settings]: Record of modification of CT group tree such as moving CT in the group tree.
- [Services Control]: Record of controlled service of client (CT).
- [Process Control]: Record of controlled process of client (CT).

For configuration change logs apart from the above, please execute the DTKSTCV.EXE (export configuration change log) command, and view the logs after exporting them as CSV files. Please refer to “DTKSTCV.EXE (export configuration change log)” in “Systemwalker Desktop Keeper Reference Manual” for details.



## Note

---

### After refreshing the tree, the window will return to status after logon

Press F5 to refresh the tree. At this time, the window will return to the status right after logon.

---

## 5.2.1 View Logs in [CT Operation Log] Window

---

### View logs

This department describes how to view logs in [CT Operation Log].

The procedure is as follows:

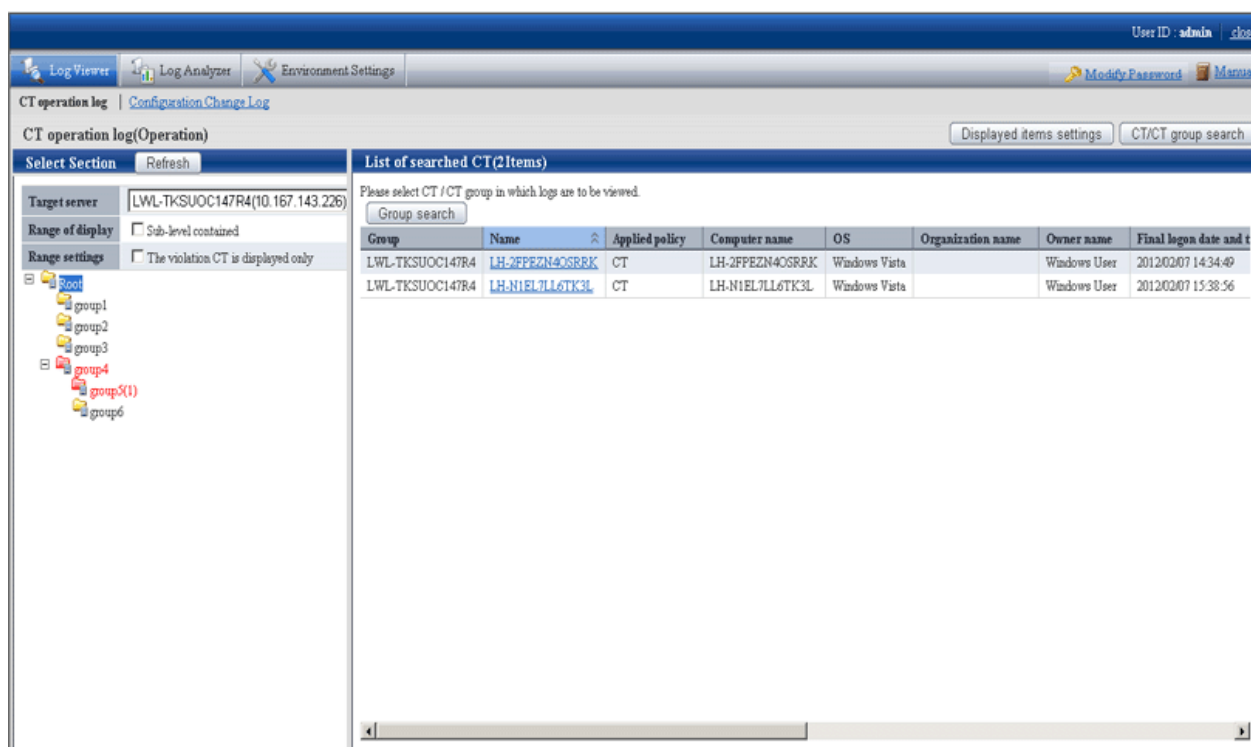
1. Start Log Viewer to display the [CT Operation Log] window.
2. Set the following items in [Select Section]
  - Select the Management Server that manages the client (CT) from [Target server].
  - Select “Display the client (CT) directly belongs to the selected group only”, or “Display all clients (CTs)” in the [Sub-level contained] check box under [Range of display].
  - Select “Display the client (CT) with violation logs only”, or “Display all clients (CTs)” in the [The violation CT is displayed only] check box in [Range settings].
3. Select the CT group to which the client (CT) for viewing logs belongs from the CT group tree of [Select Section].

Logs on the client (CT) can be searched and viewed with different ranges depending on the location selected in the group tree.

- When selecting server name: Logs can be searched and viewed on all clients (CTs) belonging to the Management Server. (\*)
- When selecting domain name: Logs can be searched and viewed on all clients (CTs) belonging to the domain selected during Active Directory Linkage. (\*)
- When selecting Local group: Logs can be searched and viewed on all clients (CTs) belonging to local groups during Active Directory Linkage.
- When selecting CT group: Logs can be searched and viewed on all clients (CTs) belonging to the CT group during Active Directory Linkage.

\*) The [Sub-level contained] check box in [Range of display] must be selected.

→The clients (CTs) belonging to the CT group will be displayed in [List of searched CT(2Items)].



The client (CT) and CT groups with violation logs will be displayed in red. Please refer to “[Display the group or client \(CT\) that has generated violation logs in red](#)” for details.

### Note

#### Please update information of CT group and CT list in following cases

When the Log Viewer performs the following operations, the information of the CT group and CT list of the Management Server displayed in the window will not be updated to the latest status.

- When the CT group tree has been modified via the Management Console
- When Active Directory Linkage is performed and the group tree is modified
- When adding a new client (CT) to the CT group of the Management Console using the automatic allocation file during CT registration
- When Log Viewer has been started one day before (violation information has been modified)

To update to the latest information, please click the [Refresh] button in the display area of [Select Section] window, and the latest information of the server selected in [Target server] can be displayed.

#### 4. Perform any of the following operations according to the purpose of viewing CT Operation Logs:

##### [View logs by client (CT)]

- a. Click [Name] of client (CT) for viewing logs in [List of searched CT(2Items)].

##### [View client (CT) logs within the selected range in CT group tree]

- a. Click the [Group search] button in [List of searched CT(2Items)].

→The [CT Operation Log(Operation) - Log search] window is displayed.

[Search conditions], [Detailed conditions] and [Type of log (Multiple choices)] can be opened or closed.

After clicking [Search conditions], [Detailed conditions] and [Type of log (Multiple choices)] (rightward triangle symbol), the [Search conditions] window will be opened.

After clicking [▼Search conditions], [▼Detailed conditions] and [▼Type of log (Multiple choices)], the [Search conditions] window will be closed.

## Note

### In case of IE6, the scroll bar cannot be displayed when unfolding “Detailed Conditions”

In case of IE6, if the scroll bar cannot be displayed for conforming log list when unfolding “Detailed conditions”, please check if “Log Type (Multiple choices)” and “Detailed conditions” are in folded status.

The screenshot shows the Log Analyzer interface. At the top, there are tabs for Log Viewer, Log Analyzer, and Environment Settings. The main area is titled "CT operation log(Operation) - Log search". Below this, there are sections for "Search conditions" and "Type of log (Multiple choices)".

**Search conditions:**

- Search target: LH-NIEL7LL6TK3L
- Search range: 2012 Year 2 Month 7 Day - 2012 Year 2 Month 7 Day
- Call search conditions: [Dropdown menu]
- Keyword: [Text input]
- User ID: [Text input]
- Type of log: Multiple choices
- Classification: All

**Type of log (Multiple choices):**

- Application startup prohibition
- FTP operation prohibition
- Application startup
- Logon/Logoff
- Command operation
- Printing prohibition
- Web operation prohibition
- Application termination
- Device configuration change
- FTP operation
- Logon prohibition
- Clipboard operation prohibition
- Window title obtaining
- Printing operation
- Web operation
- PrintScreen key prohibition
- E-mail attachment prohibition
- E-mail Sending
- File export
- Clipboard operation
- E-mail sending interruption
- File operation
- External application

**Detailed conditions:**

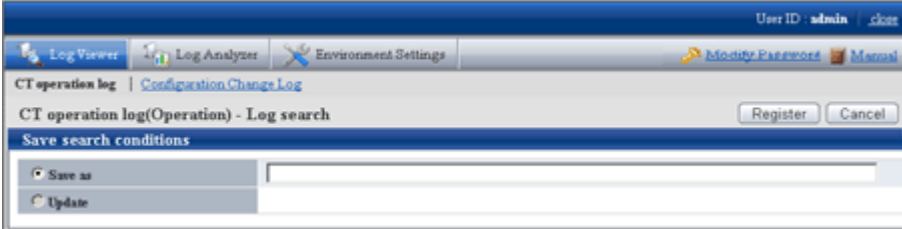
- Type of drive: Removable, Remote, CD/DVD, Fixed
- Time: Not specified, Specify range, Specify time

#### 5. Set [Search conditions]

Click [Detailed conditions] to set detailed conditions such as drive type and log collection time, etc.

Item Name	Description
[Search target]	The name of client (CT) in which the search logs are collected or CT group name will be displayed.
[Search range]	<p>Search in the specified time range.</p> <p>If the start time and end time of [Search range] are not specified, search may be performed in all periods</p> <p>If no start month or date is specified, search will begin from the beginning of the specified year (Jan. 1).</p> <p>If no start date is specified, search will begin from the beginning of the specified month (the first day).</p> <ul style="list-style-type: none"> <li>- Start date</li> <li>_ Sep 2009: 1 Sep. 2009 is assumed to be specified.</li> <li>__ 2009: 1 Jan. 2009 is assumed to be specified.</li> </ul>



Item Name	Description
	<p>_( Day)_(Month )_(Year): Start searching from the earliest saved log.  15_ 2009: Specification error  15 Sep. __: Specification error</p> <p>If no end month or day is specified, search till the end of the specified year (Dec 31).  If the end day is not specified, search till the end of the specified month (the last day).</p> <ul style="list-style-type: none"> <li>- End date</li> </ul> <p>_ Sep 2009: 30 Sep. 2009 is assumed to be specified.  __ 2009: 31 Dec 2009 is assumed to be specified.  _( Day)_(Month )_(Year): Search till the last saved log.  _ 15, 2009: Specification error  15 Sep _ : Specification error</p> <p>*If the specified year is omitted, the specified month and day should be omitted.  If the specified month is omitted, the specified day should be omitted.</p> <p>As initial values, the start date and end date will be displayed as the date on the [CT Operation Log - Search Log] window.</p> <p>[When selecting the [The violation CT is displayed only] check box of [Range settings] and clicking the [Group search] button]  The value set in [Violation Display Range] of the [Violation CT Display Settings] window will be displayed.</p>
[Call search conditions]	<p>This item can invoke the saved search conditions.</p> <p>The methods for saving/deleting search conditions are as follows:</p> <ul style="list-style-type: none"> <li>- Saving method  Set the search conditions to be saved; the conditions out of [Search range] can be saved.  After the setting has completed, please click the [Save search conditions] button, and the following window is displayed.</li> </ul>  <p>To save again, please select [Save as] and click the [Register] button. Every administrator can save up to 10 conditions. To save the 11<sup>th</sup> condition, delete the earliest search condition and register.  Up to 128 characters can be entered as the search condition name.  If desired to update search conditions, please select [Update] and click the [Register] button.</p> <ul style="list-style-type: none"> <li>- Deletion method  To delete a search condition, please select a search condition name, and click the [Delete search conditions] button.</li> </ul>
[Keyword]	<p>Keywords of logs can be used for searching. In addition, when specifying multiple keywords, the single-byte or double-byte space should be entered between keywords.</p> <p>After specifying [OR condition] in [Search condition], the search condition will become [OR Search] with more than one keyword, the multiple specified ones. Alternatively, after specifying [AND condition], the search condition will become [And Search] with all of the specified keywords.</p> <p>Select OR or AND Condition if multiple keywords are specified.</p> <p>In the information displayed in the content column and notes column of logs, the content marked with [ ] can be set as the keyword  The contents set as keyword varies with different log types. Please refer to the content column and</p>

Item Name	Description
	notes column of “Display Content” of <a href="#">8.2.1 Application Startup Log</a> ” and “ <a href="#">8.2.23 Configuration Change Log</a> ” for details.
[User ID]	Search according to user name. Only one user name can be entered.
[Classification]	The operation allowed or not allowed can be selected in policy setting. Select [Normal] to search the operations allowed and select [Violation] to search the operations not allowed. After [All] has been selected, both [Normal] and [Violation] will be selected.  [When selecting the [The violation CT is displayed only] check box of [Range settings] and clicking the [Group Search] button] [Violation] is displayed.
[Type of log]	Select the type of log to be displayed in [List of logs]. When two or more log types are set as the search condition, please select [Multiple Selection]. The [Log Type (Multiple Selection)] right under it will be opened, please select the corresponding log type.

[Log Type (Multiple Selection)]

Item Name	Descriptions
[Type of log]	Select the type of log to be displayed in [List of logs]. Please refer to “ <a href="#">Type of logs can be viewed</a> ” for information about log types.  [Select All] : Select all log types. [Clear All] : Cancel the selection of all log types Initial State: All are selected.

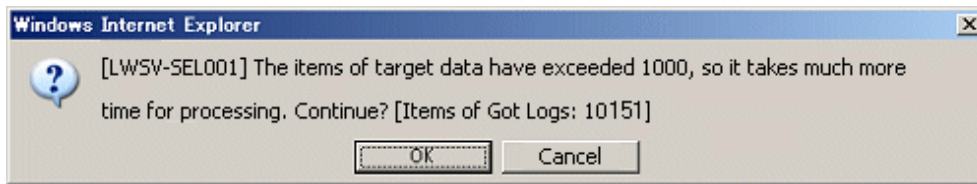
[Detailed Conditions]

Item Name	Descriptions
[Type of drive]	Search according to the type of drive. Drive type becomes a valid condition when setting the following items in [Type of log].  <ul style="list-style-type: none"> <li>- [All]</li> <li>- [File Operation]</li> <li>- [File Export]</li> </ul> <p>The following four types can be specified and multiple specifications at the same time are allowed:</p> <ul style="list-style-type: none"> <li>- Removable: The following media identified as a drive letter: <ul style="list-style-type: none"> <li>- Floppy disk</li> <li>- External hard disk (removable hard disk connection via USB, IEEE 1394 or PCMCIA .etc)</li> <li>- MO</li> <li>- USB memory</li> <li>- Compact flash memory</li> </ul> </li> <li>- Remote: Network drive</li> <li>- CD/DVD: CD/DVD drive</li> <li>- Fixed: Drive fixed in PC.</li> </ul> [Relationship between settings of [Type of log] and [Type of drive] and searched log]

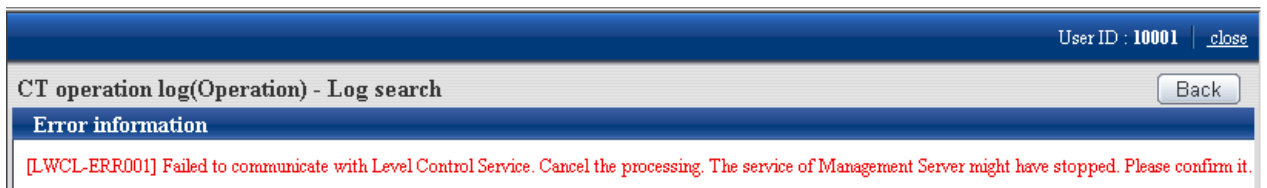
Item Name	Descriptions
	<ul style="list-style-type: none"> <li>- If [File Operation] is set in [Type of log], [Type of drive] (removable, remote, CD/DVD and fixed) will be specified as the following logs from A) to J) and displayed as search results: <ul style="list-style-type: none"> <li>- A) When creating a new file, file creation target</li> <li>- B) When updating, location of updated file</li> <li>- C) When viewing, location of viewed file</li> <li>- D) When deleting, location of deleted file</li> <li>- E) When renaming, location of the file before renaming</li> <li>- F) When renaming, location of the file after renaming</li> <li>- G) When copying, location of the copy source file</li> <li>- H) When copying, file copy destination</li> <li>- I) When moving, location of the move source file</li> <li>- J) When moving, file moving destination</li> </ul> </li> <li>- If [File Export] is set in [Type of log], [Type of drive] (removable, remote, CD/DVD and fixed) will be specified as the logs of file export target and displayed as search results</li> </ul>
[Time]	<ul style="list-style-type: none"> <li>- [Not specified]: [Time] is not included in search condition.</li> <li>- [Specify range]: The range of time for log collection is specified as search condition. <ul style="list-style-type: none"> <li>- If “a:00~b:59” is input, search with the condition of time range from a:00:00 to b:59:59.</li> <li>- If “a:00~ -:59” is input, search with the condition of time range from a:00:00 to 23:59:59.</li> <li>- If “ -:00~b:59” is input, search with the condition of time range from 0:00:00 to b:59:59.</li> </ul> </li> </ul> <p>If both a and b have been input, a must be equal to or less than b.  When two time range are specified, It does not matter if the two ranges are duplicated.  When the start time is specified as “-”, it means “0” is specified.  When t end time is specified as “-”, it means “23” is specified.  Initial value of all items are set to “-” (means no condition is set)</p> <ul style="list-style-type: none"> <li>- When log collection time is specified as the search condition by [Specify time], select the correspondent time. If multiple times are selected, the search will become an “OR Search” including more than one specified time. If none are selected, it means all are selected.</li> <li>- [Select all] : Select all check boxes in [Specify time].</li> <li>- [Clear all] : Cancel all selected check boxes in [Specify time].</li> </ul> <p>If [Day of the Week] is specified at the same time, the search will become the “AND Search” including all of the multiple conditions.</p>
[Day of the Week]	<p>[Select All] : Select all check boxes in [Day of a Week].</p> <p>[Clear All] : Cancel all selected check boxes in the [Day of a Week] menu.</p> <p>[Day of a Week] check box: When the day of the week for log collection is set as a search condition, select the correspondent day. When multiple days of the week are selected, the search will become the “OR Search” including more than one day of the week. When none are selected, it means that all are selected.</p> <p>If [Time] is specified at the same time, the search will become the “AND Search” including all of the multiple conditions.</p>

6. Click the [Search] button.

If the number of cases in search result exceeds 10000, the following window will be displayed. Click the [OK] button to continue search, or click the [Cancel] button to switch to the search condition window. When this window is displayed, it is recommended to click the [Cancel] button, and search again after modifying the search condition.



Too many cases in the search result may cause timeout and the following message will be displayed. At this time, please search again after refining the search condition.



**[Example of Refining Search Condition]**

- Reduce search time
- Reduce the Number of sets as search target
- Set to search keyword condition
- Set to search user name

→The search result is displayed in [List of logs].

**[View logs by CT]**

The CT operation log corresponding to the client (CT) will be displayed in [List of logs] .

**[View logs of client (CT) under the selected range in CT group tree]**

CT operation logs of all clients (CTs) under the CT group will be displayed in [List of logs] .

- a. Click the [Select CT] button.  
 → The CT list under the group is displayed in [Select CT].

The screenshot shows the Log Analyzer interface. The top navigation bar includes 'Log Viewer', 'Log Analyzer', and 'Environment Settings'. The main title is 'CT operation log | Configuration Change Log'. Below this, there's a search section with various filters: Search target (group4), Search range (2012 Year 2 Month 7 Day), Call search conditions, Keyword, User ID, Type of log (All), and Classification (All). There are buttons for 'Back', 'Output in CSV format', and 'Search'.

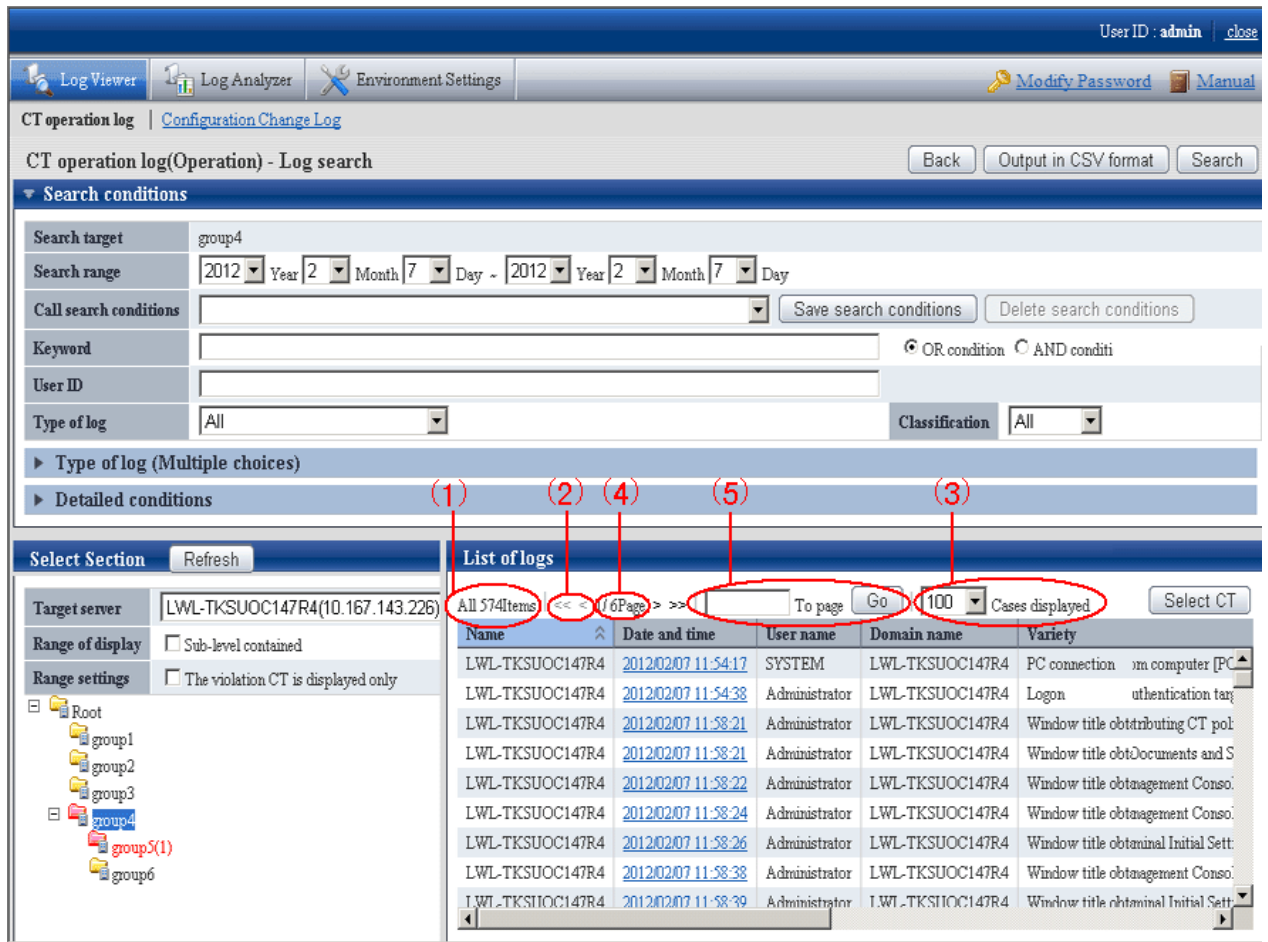
Below the search section, there are two main panels: 'Select Section' and 'Select CT'. The 'Select Section' panel shows a tree view of groups (group1 to group6) and a 'Target server' field with the value 'LWL-TKSUOC147R4(10.167.143.226)'. The 'Select CT' panel shows a table of clients with violation logs.

Number of total logs	Number of violation logs	Group	Name	Applied policy	Computer name	OS	Organization na
574	0		AllCT				
574	0	group5	LWL-TKSUOC147R4	CT	LWL-TKSUOC147R4	Windows Server 2003	lwl

The client (CT) and CT group that have generated violation logs will be displayed in red. Please refer to “[Display the group or client \(CT\) that has generated violation logs in red](#)” for details.

- b. When clicking [Name] of the client (CT) to view logs, only the CT operation log of the correspondent client (CT) will be displayed.

When clicking [Number of violation logs] the client (CT) to view logs, only the violation log of the correspondent client (CT) will be displayed.



Content displayed in [List of logs]

- (1) The number of logs corresponding to the search condition.
- (2) Click the “<” to go to the previous page. Click “>” to go to the next page. Click “<<” to return to the home page. Click “>>” to go to the last page.
- (3) Select the number of logs to be displayed in Window 1.
- (4) Display the page of logs being viewed currently.
- (5) To view logs of other pages, enter the page number and then click the [Go] button.

The information will be sorted after clicking the name of following items (Name, Occurrence Date and Time, User Name, etc).

Item Name	Description
[Name]	This is the name that can be attached to the client (CT). Its initial value is the computer name. When modifying, please refer to “ <a href="#">Modify CT Policy</a> ”.
[Date and time]	This is the date and time when logs are collected in the client.
[User name]	This is the user name entered when logging on the client (CT). If nobody logs on (when executing a program according to the task scheduler), the user name will be displayed as “System” when the following operation logs are collected: - File operation log

Item Name	Description
	<ul style="list-style-type: none"> <li>- E-mail sending log</li> <li>- E-mail attachment prohibition log</li> </ul>
[Domain name]	<p>This is the client domain name entered when logging on to a domain. It is also the computer name of the client (T) when logging on to the local computer. But it is blank when the system is Windows® 98 or Windows® ME (when connecting to the client (CT) of V12).</p> <p>If nobody logs on (when executing program according to task scheduler), the domain name will be displayed as the computer name of the client (CT) when the following operation logs are collected:</p> <ul style="list-style-type: none"> <li>- File operation log</li> <li>- E-mail sending log</li> <li>- E-mail attachment prohibition log</li> </ul>
[variety]	<p>This is the type of the log.</p> <p>This line will be displayed in red when the following prohibition logs are collected:</p> <ul style="list-style-type: none"> <li>- Application startup prohibition log</li> <li>- E-mail attachment Prohibition log</li> <li>- Printing prohibition log</li> <li>- Logon prohibition log</li> <li>- PrintScreen Key prohibition Log</li> <li>- Web operation prohibition log</li> <li>- FTP Operation prohibition log</li> <li>- Clipboard operation prohibition log</li> </ul>
[Classification]	<p>According to policy settings, the operation allowed will be displayed as [Normal], and the operation that is not allowed will be displayed as [Violation].</p> <p>When [Violation] logs are collected, this line will be displayed in red (settings concerning display are not required).</p>
[Add]	<ul style="list-style-type: none"> <li>- This is displayed as [1] or [2] when the captured screen is the obtained window title log. <ul style="list-style-type: none"> <li>- [1]: when the captured screen is the obtained window 1.</li> <li>- [2]: when the captured screen is the obtained window 2</li> </ul> </li> <li>- Displayed as [1] when the policy for obtaining screen capture is set in PrintScreen key prohibition log”.</li> <li>- Displayed as [1] when the policy for original backup is set in file export log, linkage application log, clipboard operation log or clipboard operation prohibition log.</li> <li>- Displayed as [1] when the policy that allows viewing of E-mail content is set in E-mail sending log.</li> </ul>
[Content]	<p>This is the content of the log</p> <p>Please perform the following operations to confirm all contents:</p> <ul style="list-style-type: none"> <li>- Click the [Date and time] of log display in [List of logs], and confirm it in the [Log Details] window.</li> <li>- Confirm that the log is exported as a CSV file. Please refer to “<a href="#">Export contents displayed in [List of logs] to CSV file</a>” for a method of export to a CSV file.</li> </ul> <p>Up to 519 bytes can be displayed as the path length of target file of file operation log. In the path name containing UNICODE characters, part of UNICODE characters will be displayed in escape format.</p>

Item Name	Description
	<p>UNICODE characters can be correctly displayed when all the following conditions are satisfied.</p> <ul style="list-style-type: none"> <li>- Logs are collected in the client (CT), the OS of which is Windows Vista®, Windows Server® 2008 or Windows® 7.</li> <li>- PC system of Log Viewer is Windows Vista®, Windows Server® 2008 or Windows® 7.</li> </ul> <p>If the above conditions are not satisfied, UNICODE characters contained in the log will be displayed as “?” or in the escape format (e.g. In “&amp;#xA4A4;”, A4A4 is a hexadecimal code with 4 or 5 digits.</p>
[Remarks]	This is the notes of the logs.

7. Click [Occurrence Date and Time] of the displayed log.

→The [CT operation log(Operation) - Log search - Log details] window is displayed.

The screenshot shows the Log Viewer application interface. At the top, there is a navigation bar with 'Log Viewer', 'Log Analyzer', and 'Environment Settings' tabs. On the right, there are links for 'Modify Password' and 'Manual'. Below the navigation bar, the current view is 'CT operation log | Configuration Change Log'. The main content area is titled 'CT operation log (Operation)- Log search - Log details' and includes 'Back' and 'File trace' buttons. A section titled 'Detailed information of log' contains a search bar with '3/624Items' and a 'Go' button. Below the search bar is a table with the following details:

Name	LWL-TKSUOC147R4
Occurrence date and time	2012/02/07 11:58:21
User ID	Administrator
Domain name	LWL-TKSUOC147R4
Type	Window title obtaining
Classification	Normal
Content	Window [Distributing CT policy] has been detected. Program name: [fsw21ej2]
Note	
Attachment	

Item Name	Description
[Name]	<p>For the name that can be attached to the client (CT), the initial value is the computer name.</p> <p>When modifying, please refer to “<a href="#">Modify CT Policy</a>”.</p>
[Occurrence date and time]	This is the date and time when logs are collected from the client.
[User name]	<p>This is the user name entered when logging on the client (CT).</p> <p>If nobody logs on (when executing program according to task scheduler), the user name will be displayed as “System” when the following operation logs are collected:</p> <ul style="list-style-type: none"> <li>- File operation log</li> <li>- E-mail sending log</li> <li>- E-mail attachment prohibition log</li> </ul>
[Domain name]	This is the client domain name entered when logging on to a domain. It is also the computer name of client (T) when logging on to the local computer. But it is blank when the system is Windows® 98 or Windows® ME (when connecting to the client (CT) of V12).



Item Name	Description
	<p>If nobody logs on (when executing program according to task scheduler), the domain name will be displayed as the computer name of client (CT) when the following operation logs are collected:</p> <ul style="list-style-type: none"> <li>- File operation log</li> <li>- E-mail sending log</li> <li>- E-mail attachment prohibition log</li> </ul>
[Type]	This is the type of log.
[Classification]	According to policy settings, the operation allowed will be displayed as [Normal], and the operation that is not allowed will be displayed as [Violation].
[Content]	<p>This is the content of the log</p> <p>Up to 519 bytes can be displayed as the path length of target file of file operation log. In the path name containing UNICODE characters, part of UNICODE characters will be displayed in escape format.</p> <p>UNICODE characters can be correctly displayed when all the following conditions are satisfied.</p> <ul style="list-style-type: none"> <li>- Logs are collected in the client (CT), the OS of which is Windows Vista®, Windows Server® 2008 or Windows® 7.</li> <li>- PC system of Log Viewer is Windows Vista®, Windows Server® 2008 or Windows® 7.</li> <li>- If the above conditions are not satisfied, UNICODE characters contained in the log will be displayed as “?” or in the escape format (e.g. In “&amp;#xA;”, A; is a hexadecimal code with 4 or 5 digits.</li> </ul> <p>For command log, the “·” may be displayed at the end of line as line feed.</p>
[Note] (Note 1)	This is the notes of the logs.
[Additional] (Note 1)	<p>The displayed information is as follows:</p> <ul style="list-style-type: none"> <li>- If the captured screen is the obtained window title log <ul style="list-style-type: none"> <li>- [Picture 1]</li> <li>- [Picture 1] , [Picture 2]</li> </ul> </li> <li>- When the captured screen is the obtained PrintScreen key prohibition log <ul style="list-style-type: none"> <li>- [Picture 1]</li> </ul> </li> <li>- When the original backup policy is set in file export log <ul style="list-style-type: none"> <li>- [File name] (display the backup file name)</li> </ul> </li> <li>- When original file is backed up in linkage application log <ul style="list-style-type: none"> <li>- [Original file]</li> </ul> </li> <li>- When the policy that allows viewing of E-mail content is set in E-mail sending log <ul style="list-style-type: none"> <li>- [E-mail Content]</li> </ul> </li> <li>- In case of clipboard operation log” or clipboard operation prohibition log <ul style="list-style-type: none"> <li>- The data copied via clipboard is text:[Details]</li> <li>- The data copied via clipboard is image:[Picture]</li> <li>- The data copied via clipboard is file:[Details]</li> </ul> </li> </ul>
[Session ID] (Note 2)	This is the ID indicating the command execute in command prompt of client (CT) and the result of command execution

Item Name	Description
[Download Content] (Note 2)	The message displayed in [Content] can be downloaded in text format.

Note 1: This cannot be displayed in case of command log.

Note 2: This will be displayed in case of command log.

## View attached data

When window title logs, file export log, clipboard operation logs and clipboard operation prohibition logs are being collected, the captured screen data, original file data of exported files and text and image data via clipboard can be saved simultaneously.

In addition, when collecting E-mail sending log, E-mails and attachments can also be saved.

By viewing these data, the actual content of displayed windows, exported files, sent E-mails and attachment can be known.

If the [View/save attached information] checkbox is selected in [Detail authority] of the [Administrator Information Settings] window of Server Settings Tool, the captured screen data, original file data of exported files, text and image data via clipboard can be viewed and saved.

If the [Save E-mail contents] checkbox is selected in [Detail authority] of the [Administrator Information Settings] window of the Server Settings Tool, the content of sent E-mails and attachments can be viewed.

If the file as attached data exists, it is possible to [Save original file backup](#)

In addition, if screen capture data exists, it is possible to [View/Save screen capture data](#).

## View/Save screen capture data

When screen capture data exists in window title logs and PrintScreen key prohibition log”, the captured screen can be viewed after clicking the link of the item value link of [Attachment] in the [CT operation Log(Operation) - Log Search - Log Details] window.

If two captured screens exist, there will be 2 links.

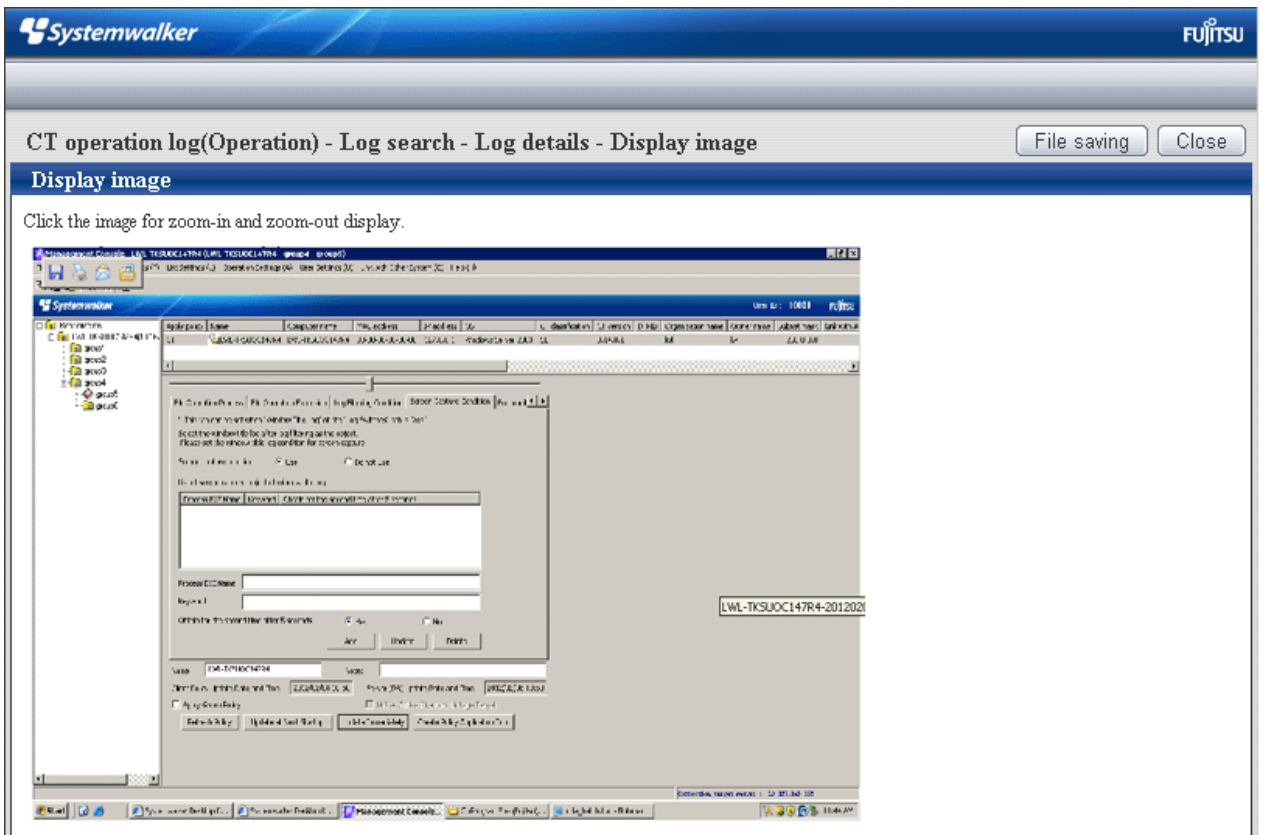
If one screen capture of window exists in the [Attachment] item of log list, the window title log with screen capture data existed will be displayed as [1]; when screen capture of two windows exists, the window title log will be displayed as [2].

If screen capture data exists in PrintScreen key prohibition log, [1] will be displayed in the [Attachment] item of the log list.

The screenshot shows the 'Log Viewer' application interface. At the top right, it displays 'User ID : 10001' and a 'close' button. The main navigation bar includes 'Log Viewer', 'Log Analyzer', 'Environment Settings', 'Modify Password', and 'Manual'. Below this, the current view is 'CT operation log | Configuration Change Log'. The main title is 'CT operation log (Operation)- Log search - Log details', with 'Back' and 'File trace' buttons. The section is titled 'Detailed information of log'. Below this, there is a search bar with '<< < 12/54Case(s) > >>' and a 'Case no.' field with a 'Go' button. The log entry details are as follows:

Name	LWL-TKSUOC147R4
Occurrence date and time	2012/02/07 13:18:26
User ID	Administrator
Domain name	LWL-TKSUOC147R4
Type	PrintScreen key prohibition
Classification	Violation
Content	PrintScreen key has been pressed.
Note	
Attachment	<a href="#">Image 1</a>

1. Click the link of item value of [Attachment]  
→The image of screen capture is displayed.



## Note

### When screen capture data cannot be displayed

The following message will be displayed after clicking the [Display Image] button.

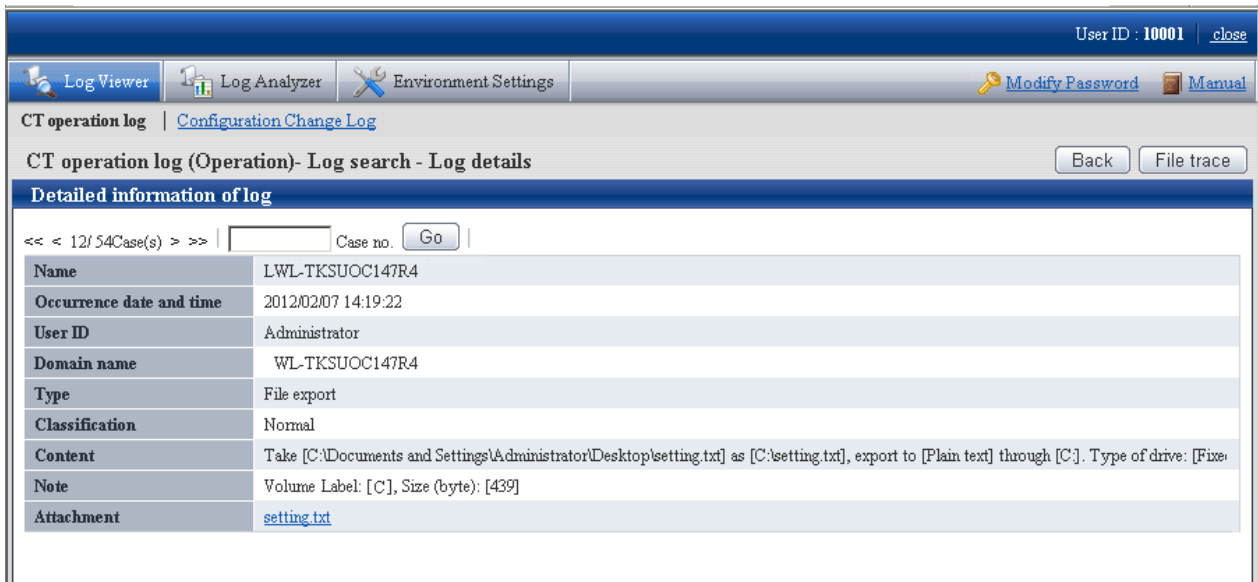
[LWSV-ERR007] screen data cannot be displayed because it has not been transferred to server.

It will be displayed when the screen capture data has not been sent from the client (CT) to the Management Server, or “Save screen capture data to CT” has been set. When screen capture data has not sent from the client (CT) to the Management Server, please view later after clicking the [OK] button. If “Save screen capture data to CT” has been set, the saving location must be modified. The location for saving and timing of sending screen capture data can be set in [Terminal Operation Settings] window of the Management Console. Please confirm the settings and modify them according to the execution situation. For the confirmation of [Terminal Operation Settings], please refer to “[2.4.2 Perform Terminal Operation Settings](#)”.

2. Click the [File Saving] button.  
→ In the [Saved as] window that is displayed, select the location for saving, and click the [Save] button. The image will be saved to the specified location in the png format with default file name.  
The file name of screen capture data: “CT name” + “-” + “Log occurrence date and time (yyymmddhhmmss)” + “-” + Page number (1or 2) + “-” + “Extension” (e.g. PC382686-20061215203412-1.png)
3. Click the [Close] button.

## Save original file backup

When the file export log, E-mail sending log, linkage application log, clipboard operation log and clipboard operation prohibition log contain original file backup s, after clicking the link of item value of [Attachment] in the [CT Operation Log - Log Search - Log Details] window, original file backup s can be saved to any location. The file export log and linkage application log that contain original file backup will be displayed as [1] in the [Add] item of [List of logs]. Clipboard operation log and clipboard operation prohibition log will be displayed as [Obtain] in the [Attachment] item of [List of logs].



The screenshot shows the 'Log Viewer' application interface. At the top, there are navigation tabs for 'Log Viewer', 'Log Analyzer', and 'Environment Settings'. The current view is 'CT operation log (Operation)- Log search - Log details'. Below this, there is a 'Detailed information of log' section with a search bar and a 'Go' button. The main content is a table with the following details:

Name	LWL-TKSUOC147R4
Occurrence date and time	2012/02/07 14:19:22
User ID	Administrator
Domain name	WL-TKSUOC147R4
Type	File export
Classification	Normal
Content	Take [C:\Documents and Settings\Administrator\Desktop\setting.txt] as [C:\setting.txt], export to [Plain text] through [C]. Type of drive: [Fixe
Note	Volume Label: [C], Size (byte): [439]
Attachment	<a href="#">setting.txt</a>

1. Click the link of item value in [Attachment].

→In the [Saved as] window that is displayed, select the location for saving, and click the [File saving] button.

The file name when backing up original files is displayed as the default value. Please modify the file name and save it if necessary.

- The original file backup name of file export log: Export source file name
- The original file backup name of linkage application log: “CT name” + “-” + “Log occurrence date and time (yyyymmddhhmss)” + “.” + “Extension” (e.g. PC382686-20061226132137.wmf)
- The original file backup name of E-mail sending log: “CT name” + “-” + “Log occurrence date and time (yyyymmddhhmss)” + “.” + “Extension” (e.g. PC382686-20061226132137.eml)
- The original file backup name of clipboard operation log and clipboard operation prohibition log: “CT name” + “-” + “Log occurrence date and time (yyyymmddhhmss)” + “.” + “Extension” (e.g. in case of text or file: PC382686-20061226132137.txt; In case of image: PC382686-20061226132137.png)



### When original file backup cannot be saved

The following message will be displayed after clicking the [File saving] button.

```
[LWSV-ERR010] The original file backup cannot be displayed because it has not been transferred to server.
```

It will be displayed when the original file backup has not been sent from the client (CT) to the Management Server, or “Save Original File Backup in CT” has been set. When the original file backup has not sent from the client (CT) to the Management Server, please view later after clicking the [OK] button. If “Save Original File Backup to CT” has been set, the saving location must be modified. The location for saving and timing of sending original file backup can be set in [Terminal Operation Settings] window of the Management Console. Please confirm the settings and modify them according to the execution situation. For the confirmation of [Terminal Operation Settings], please refer to “2.4.2 Perform Terminal Operation Settings”.

## Export contents displayed in [List of logs] to CSV file

After the [Save CSV file] check box is selected in [Detailed authority] in the [Administrator Information Settings] window of the Server Settings Tool, the content displayed in [List of logs] will be exported to a CSV file and saved.

1. In the status of displaying the logs to be exported to CSV file in [List of logs], click the [Output in CSV format] button.
2. In the file download window that is displayed, click the [Save] button.
3. After selecting the folder for saving and entering the file name, click the [Save] button.

When a file with same name exists in the export destination, the option window indicating whether to overwrite will be displayed. Please select the desired option.

For the item name and description of an exported CSV file, please refer to “Log List” of “Systemwalker Desktop Keeper Reference Manual”.

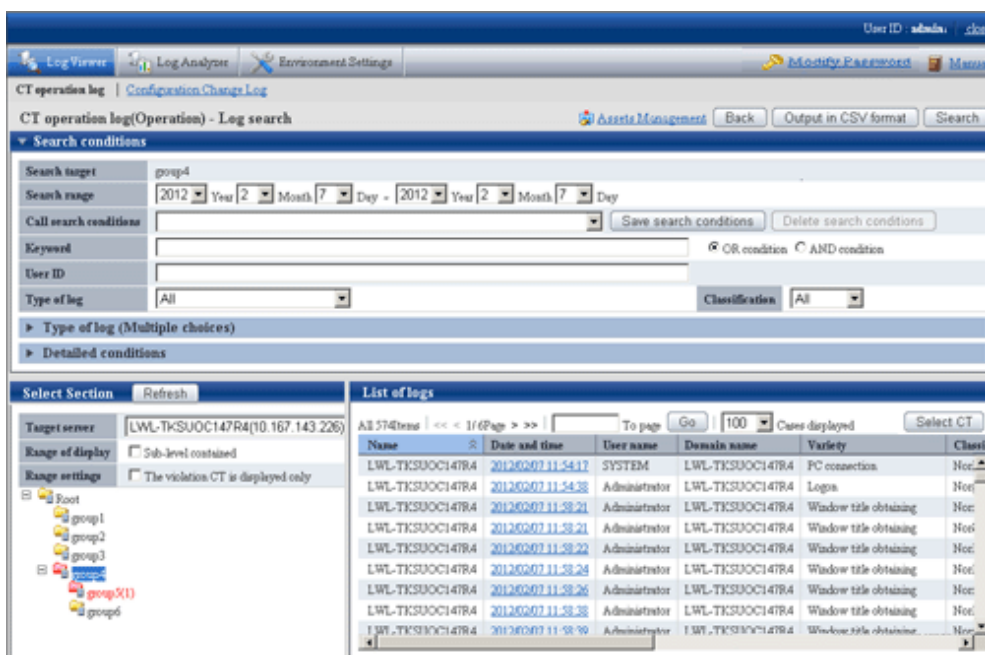
## When file download is not successful

When the download of CSV file, original file backup and command operation file is not successful, please refer to “Preparation of Using Web Browser in PC” of “Systemwalker Desktop Keeper Installation Guide” to modify the settings of Internet Explorer®.

## Link with Systemwalker Desktop Patrol

When linking with Systemwalker Desktop Patrol, assets management information (Systemwalker Desktop Patrol information) of the correspondent PC can be viewed.

1. Select the client (CT) that displays Systemwalker Desktop Patrol assets management information.
2. Select [Assets Management]



3. The asset information of Systemwalker Desktop Patrol will be displayed in other windows.

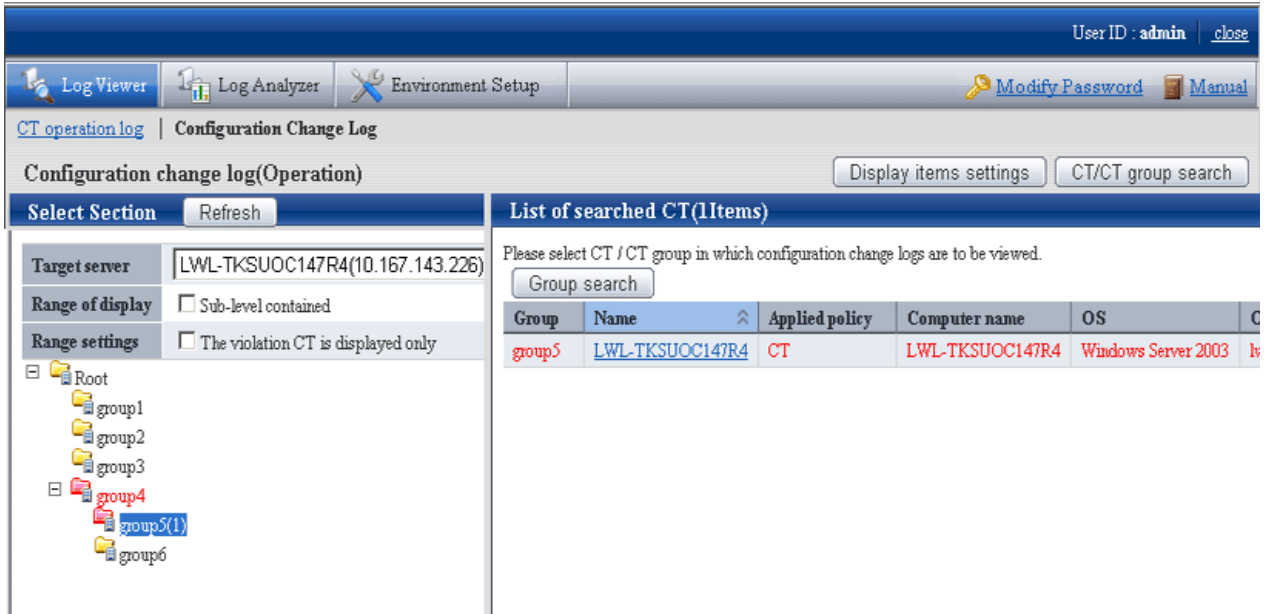
## 5.2.2 View in [Configuration Change Log]

This department describes how to display [Configuration Change Log List] and how to view logs when modifying configuration information of client (CT) in the Management Console.

When the viewing authority has been granted in [Detailed Authority] of the [Administrator Information Setting] window of the Server Settings Tool, [Configuration Change Log List] can be viewed.

The procedure is as follows:

1. Start Log Viewer and select [Configuration Change Log].  
→The [Configuration Change Log] window is displayed.



2. Select the Management Server that manages the client (CT) from [Target server] of [Select Section]. Select “Display client (CT) directly belongs to the selected group only”, or “Display all clients (CTs)” in the [Sub-level contained] check box in [Range Settings].
3. Perform the following operations according to the purpose of viewing configuration change log.

**[When viewing the configuration change log of “Terminal Initial Settings” policy set in Management Server]**

- a. Select the server displayed in CT group tree of [Select Section] .  
→The client (CT) is displayed in [List of searched CT] window.
- b. Click the [Group Search] button in [List of searched CT] window.  
→The [Configuration Change Log(Operation) - Log Search] window is displayed.  
At this time, the Step 4 is not needed.

**[View configuration change log of a single client]**

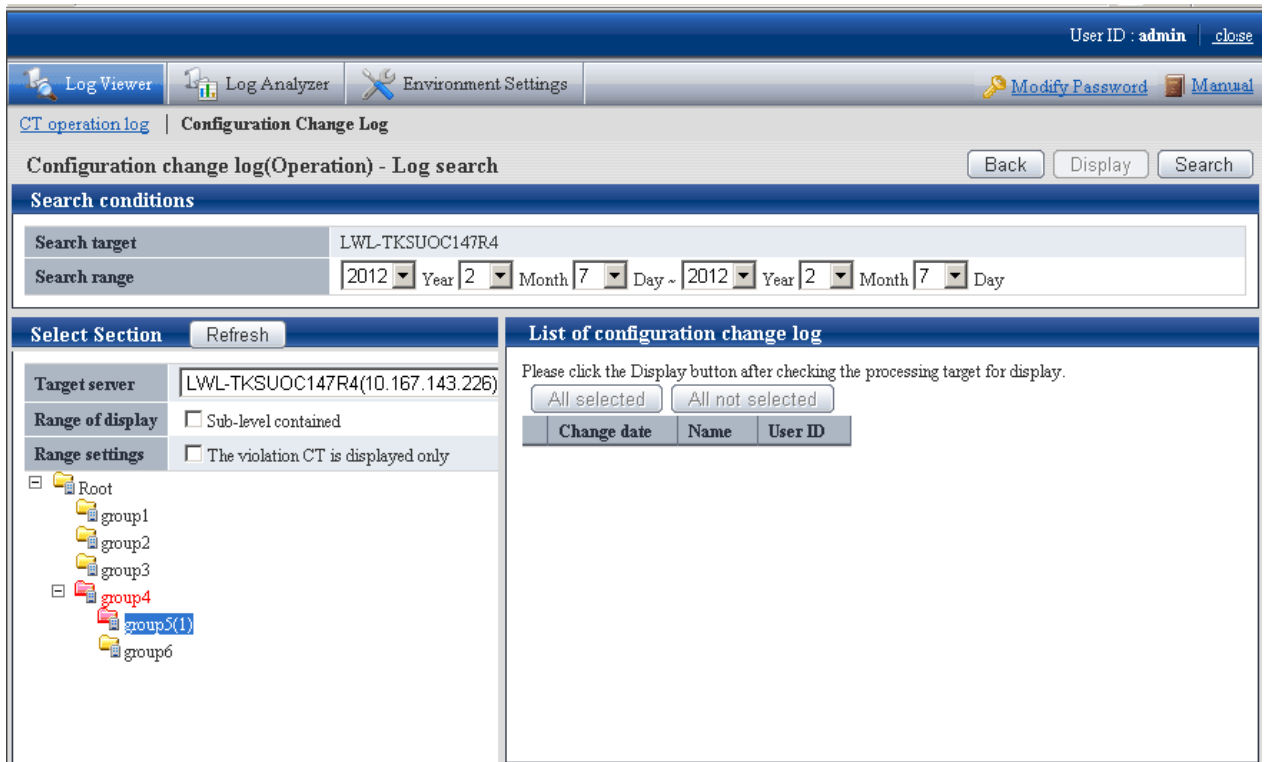
- a. Select the CT group to which the client (CT) for viewing logs belongs from the CT group tree of [Select Section].  
→ The client (CT) belongs to the CT group is displayed in [List of searched CT].

**[View configuration change log of CT group and its subordinate client (CT)]**

- a. Select the CT group for viewing logs from the CT group tree of [Select Section].
- b. Click the [Group Search] button of [List of searched CT].  
→The [Configuration Change Log(Operation) - Log Search] window is displayed.  
At this time, the Step 4 is not needed.

4. Click the [Name] of the client (CT) for viewing logs.

→The [Configuration change log(Operation) - Log Search] window is displayed.



5. Set [Search Conditions]

Item Name	Description
[Search range]	<p>Search in the specified range. If the start and end of [Search Range] is not specified, all periods will become the search target.</p> <p>If no start month or date is specified, search will begin from the beginning of the specified year (Jan. 1).</p> <p>If no start date is specified, search will begin from the beginning of the specified month (the first day).</p> <p>If no end month or day is specified, search will go until the end of the specified year (Dec 31).</p> <p>If the end day is not specified, search will go until the end of the specified month (the last day).</p> <p>As initial values, the start date and end date will be displayed as the date on the [CT Operation Log(Operation) - Log Search] window.</p> <ul style="list-style-type: none"> <li>- Start date <ul style="list-style-type: none"> <li>_ Sep 2009: 1 Sep. 2009 is assumed to be specified.</li> <li>__ 2009: 1 Jan. 2009 is assumed to be specified.</li> <li>_( Day)_(Month)_(Year): Start searching from the earliest saved log.</li> <li>15_ 2009: Specification error</li> <li>15 Sep. __: Specification error</li> </ul> </li> <li>- End date <ul style="list-style-type: none"> <li>_ Sep 2009: 30 Sep. 2009 is assumed to be specified.</li> <li>__ 2009: 31 Dec 2009 is assumed to be specified.</li> <li>_( Day)_(Month)_(Year): Search till the last saved log.</li> <li>_ 15, 2009: Specification error</li> <li>15 Sep _ : Specification error</li> </ul> </li> </ul>

Item Name	Description
	*If the specified year is omitted, the specified month and day should be omitted. If the specified month is omitted, the specified day should be omitted.

6. Click the [Search] button.

→The search result is displayed in [List of configuration change log].

The screenshot shows a web-based interface for searching configuration change logs. At the top, there are navigation tabs: Log Viewer, Log Analyzer, Environment Settings, Modify Password, and Manual. The current page is titled 'Configuration Change Log' and 'Configuration change log(Operation) - Log search'. Below the title are buttons for 'Back', 'Display', and 'Search'. The search conditions are set to 'Search target: LWL-TKSUOC147R4' and 'Search range: 2012 Year 2 Month 7 Day'. On the left, there is a 'Select Section' panel with a 'Refresh' button and a tree view showing a folder structure: Root, group1, group2, group3, group4, group5(1) (selected), and group6. The main area is titled 'List of configuration change log' and contains a table with the following data:

	Change date	Name	User ID
<input type="checkbox"/>	2012/02/07	LWL-TKSUOC147R4	10001

The information will be sorted after clicking the following items (e.g. Date of change, Name or User ID).

Item Name	Description
[Change date]	This is the year, month and day when the settings are changed.
[Name]	This is the name that can be attached to the client (CT), and the initial value is the computer name. When modifying terminal initial settings policy, [Terminal Initial Settings Policy] will be displayed. When modifying settings for CT group, CT group name will be displayed.
[User ID]	This is the user ID of the person who logs on the management console and modifies settings.



7. In the search result, select the displayed details of the configuration change and click the [Display] button.  
 Click the [All selected] button to select all search results.  
 Click the [All not selected] button to cancel all the selected search results.  
 → Details are displayed in the [Configuration Change Log(Operation) - Log Search - Display logs] window.

The screenshot displays the 'Configuration Change Log' interface. On the left, there is a search filter for 'Target server' set to 'LWL-TKSUOC147R4(10.167.143.226)'. Below this is a tree view of groups: Root, group1, group2, group3, group4, group5(1), and group6. The main area shows a table titled 'List of configuration change log' with the following data:

Change date	Name	User ID	Set variety	Content
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	Name: LW
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	File access
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	Specify th
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	Specify ti
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	Applicatic
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	PrintScree
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	File Opera
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	File Opera
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	File Opera
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	File Opera
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	URL Acce
2012/02/07 11:56:11	LWL-TKSUOC147R4	10001	Terminal settings	Apply Gn
2012/02/07 11:56:30	LWL-TKSUOC147R4	10001	Terminal settings	Name: LW
2012/02/07 11:56:30	LWL-TKSUOC147R4	10001	Terminal settings	File access
2012/02/07 11:56:30	LWL-TKSUOC147R4	10001	Terminal settings	Specify th

Item Name	Descriptions
[Change date]	This is the date and time when the settings are changed.
[Name]	This is the name that can be attached to the client (CT), and the initial value is the computer name. When modifying terminal initial settings policy, [Terminal Initial Settings Policy] will be displayed. When modifying settings for CT group, CT group name will be displayed.
[User ID]	This is the user ID of the person who logs on the management console and modifies settings.
[Set variety]	The types of settings are shown as follows: <ul style="list-style-type: none"> <li>- [Terminal settings]: Records of modifying CT policy.</li> <li>- [Level composition settings]: Records of modifying CT group tree such as moving CT, etc.</li> <li>- [Services Control]: Records of service control in the client (CT).</li> <li>- [Process Control]: Records of process control in the client (CT).</li> </ul>
[Content]	This is the content of the configuration change log. The displayed content should be within 259 characters. To confirm all contents, please export to CSV file. For details on how to export to CSV files, please refer to “Export Contents displayed in [Configuration Change Log List] to CSV File”.

## Export Contents displayed in [Configuration Change Log List] to CSV File

After selecting the [Save CSV file] checkbox in [Detailed Authority] of the [Administrator Information Settings] window of the Server Settings Tool, exporting to a CSV file and saving can be executed.

1. In the status of displaying the logs to be exported to a CSV file in [Configuration Change Log List], click the [Output in CSV format] button.
2. In the file download window that is displayed, click the [Save] button.
3. After selecting the folder for saving and entering the file name, click the [Save] button.

When a file with same name exists in the export destination, the option window indicating whether to overwrite will be displayed. Please select the desired option.

For the item name and a description of the exported CSV file, please refer to “Configuration Change Log List” of “Systemwalker Desktop Keeper Reference Manual”.

## When file download is not successful

When the download of the CSV file, original file backup and command operation file is not successful, please refer to “Preparation of Using Web Browser in PC” of “Systemwalker Desktop Keeper Installation Guide” to modify the settings of Internet Explorer®.

## 5.3 Trace File Operation

---

By viewing file operation log, the changes in file operation executed by the user can be searched/displayed when the user of a client (CT) with suspected misoperation is detected.

The File Tracing function is a tool for searching/displaying file operation changes that are executed in client (CT) according to “File Operation Log”, “File Export Log”, “E-mail Sending Log (with attachment)”, “E-mail Sending Suspension Log (with attachment)”, “E-mail Attachment Prohibition Log”, “FTP Operation Log (FTP upload or download)” and “Web Operation Log”. Following functions are provided by the File Tracing function.

From the logs that have been searched in Log Viewer, select a file as the file tracing target to trace the operation. In addition, the results of the tracing can be displayed in the window or exported to a CSV file.

The operation logs that can be selected as tracing targets are the following logs that contain file operation information:

- File Operation Log
- File Export Log
- E-mail Sending Log (with attachment)
- E-mail Sending Interruption Log (with attachment)
- E-mail Attachment Prohibition Log
- FTP Operation Log (FTP upload or download)
- Web Operation Log

In addition, the following logs will be contained in the results of tracing as supplement information of the above operation logs

- Printing Operation log
- Printing Prohibition log



### Note

---

[File operation in Citrix XenApp Client cannot be traced]

The file trace function cannot be used in the log viewer via file operation logs in the Citrix XenApp client.

[The range of file operation in Systemwalker Desktop Keeper Client (CT) can be traced]

The clients of the logs as trace targets are traceable; it is impossible to perform file trace among multiple clients.

---

## Trace File operation

This department describes how to set the file information to be used as tracing target.

To perform file tracing, the file information to be used as a tracing target must be set. To set file information, the following logs that include file operation information should be displayed at first:

- File Operation Log
- File Export Log
- E-mail Sending Log (with attachment)
- E-mail Sending Interruption Log (with attachment)
- E-mail Attachment Prohibition Log
- FTP Operation Log (FTP upload or download)
- Web Operation Log

“Printing Operation Log” and “Printing Prohibition Log” cannot be selected as file tracing targets.

To use the file names contained in those logs as tracing targets, please enter the "file name" contained in "Printing Operation Log" or "Printing Prohibition Log" in "Keywords" of the [CT Operation Log - Log Search] window and perform searching. If search results contain the above logs (File Operation Log, File Export Log, or E-mail Sending Log, E-mail Sending Interruption Log, E-mail Attachment Prohibition Log, FTP Operation Log, Web Operation Log), file trace can be executed by setting those logs as tracing targets.

The following describes how to perform file tracing through the file information set in tracing target.

Search (display the search result that includes path in “accuracy”) cannot be performed unless the file names of “File Operation Log”, “File Export Log”, “E-mail Sending Log”, “E-mail Sending Interruption Log”, “E-mail Attachment Prohibition Log”, “FTP Operation Log” and “Web Operation Log” completely match with those of the tracing target (except the path).

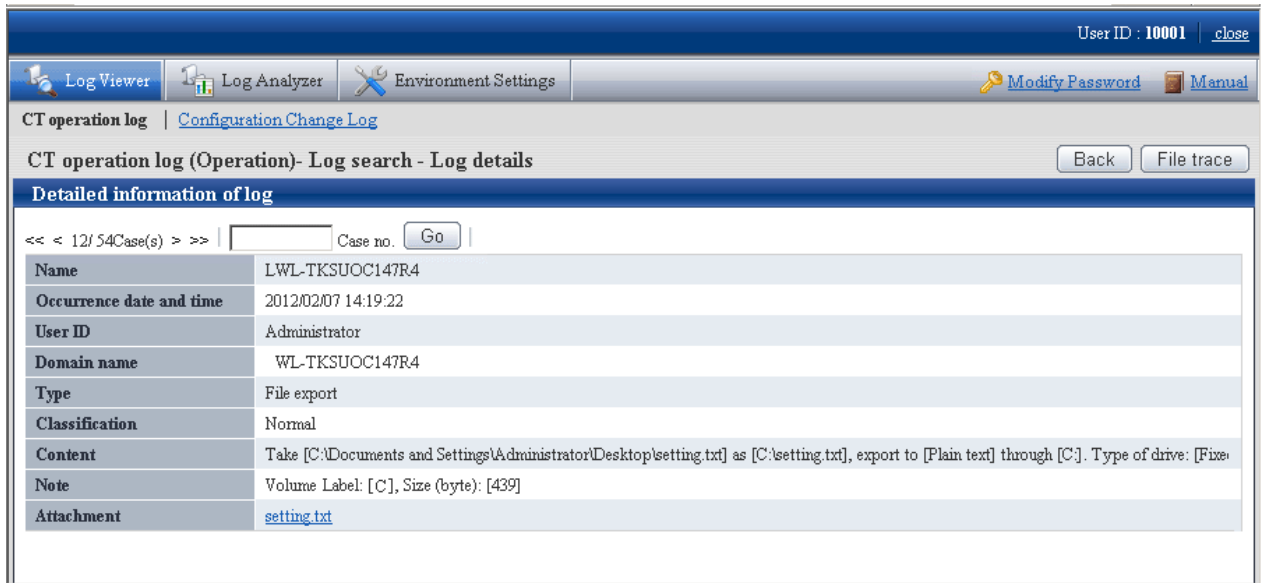
In addition, since “Printing Operation Log” and “Printing Prohibition Log” can be searched when their file names partially match with those of the tracing target, in the mean time of tracing the logs of file as tracing target, the logs with lower correlation with the tracing target file will also be searched.

Trace conditions shall be set up for the purpose of trace based on information about trace target files.

1. Start Log Viewer.

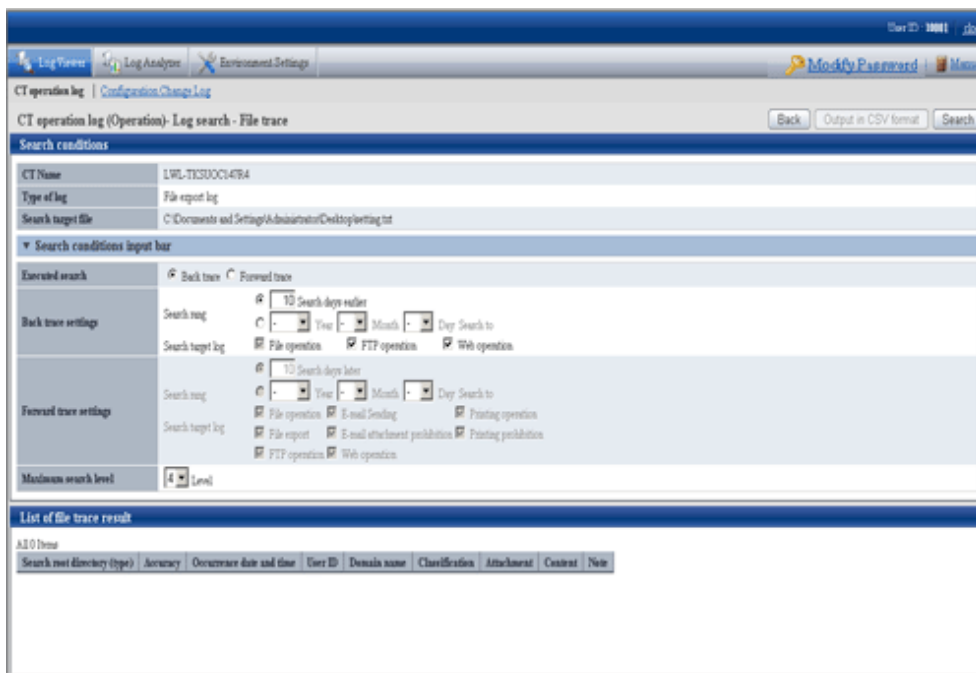
- The [CT Operation Log(Operation) - Log Search - Log Details] window of the operation logs for which the file tracing is executed is displayed.

For display method, please refer to “5.2.1 View Logs in [CT Operation Log] Window”.



- Click the [File trace] button.

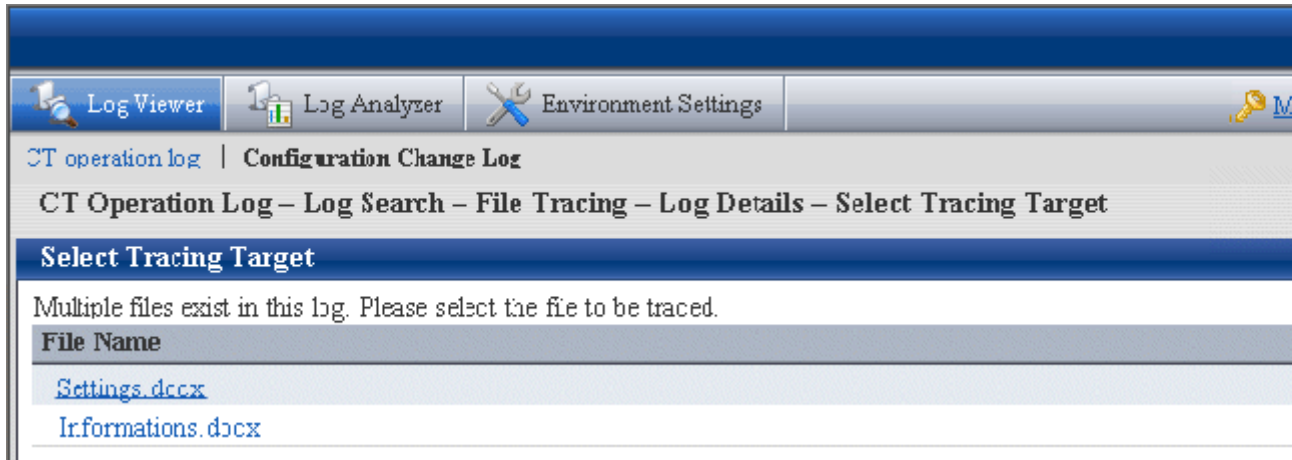
→When the selected log type is [E-mail Sending] and multiple attachments are contained in the log, the [CT Operation Log - Log Search - File Tracing - Log Details - Select Tracing Target] window will be displayed. If the display condition is not satisfied, the [CT Operation Log(Operation) - Log Search - File Trace] will be displayed.



About [CT Operation Log - Log Search - File Tracing - Log Details - Select Tracing Target] window

The [CT Operation Log - Log Search - File Tracing - Log Details - Select Tracing Target] window will be displayed if the following conditions are satisfied:

- When the selected log type is [E-mail Sending] and multiple attachments are contained in the log.
- a) The [CT Operation Log - Log Search - File Tracing - Log Details - Select Tracing Target] window will be displayed.



- b) Select a file from [Select Tracing Target] to perform file tracing.  
→The selected attachment name will be set as file tracing target.

#### 4. Set up [Search Conditions]

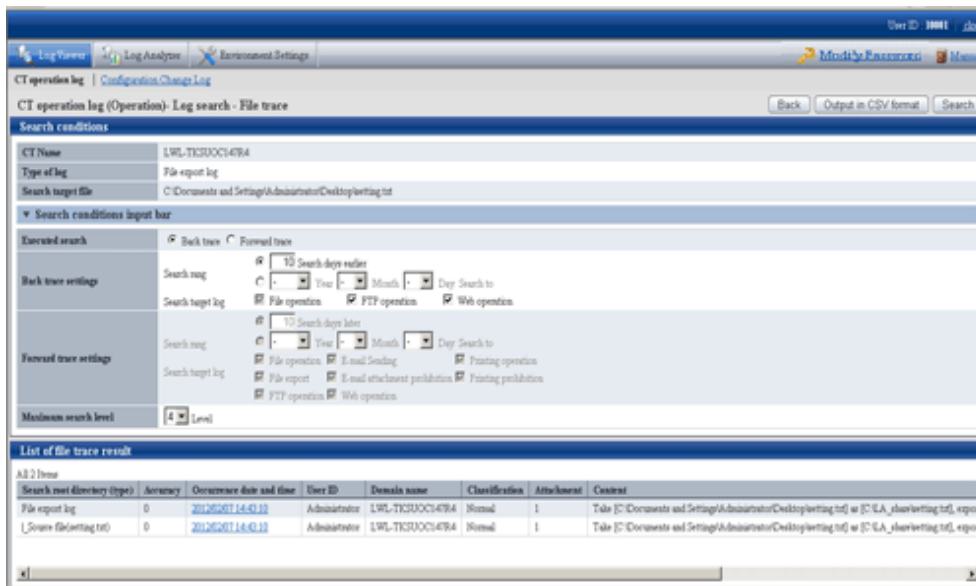
Item Name	Description
[CT Name]	This is the name of the client (CT) in which the logs selected in [Log Viewer] are displayed. The scope of file tracing will be the logs collected in this client (CT).
[Type of log]	This is the type of log selected in the [Log Viewer] window.
[Search target file]	This is the name of the file to be used as the tracing target.
[Executed search]	<p>[Back trace]</p> <p>Search how the files were processed before according to the selected log. "Back Trace" can only trace [Copy], [Cut], [Rename], [Create], [Update], [Delete] operations of the File Operation Log and export operations of File Export Log. This is used while investigating previous file operations.</p> <p>[Forward trace]</p> <p>Search how the files are processed later according to the selected log. The operation process since the generation occurrence date and time of the operation logs specified as tracing target can be investigated. One file may be changed to multiple files by using the copy operation, and the search result may increase, which results from an expanded search target in the log.</p>
[Search range]	<p>Specify the search range by time period (days) or date.</p> <p>The initial value is "Period (days)".</p> <p>The period (days) or date that can be specified is shown as follows:</p> <ul style="list-style-type: none"> <li>- Period (Days) <ul style="list-style-type: none"> <li>- "0" ~ "999" can be specified. The day when the operation log specified as tracing target has been generated is "0". The initial value is "10".</li> </ul> </li> <li>- Date</li> </ul> <p>Search in the specified range. If both start time and end time of [Search range] are not specified, the search target during back trace is all logs prior to the generation date; for forward trace, the search target is all logs after the generation date.</p>

Item Name	Description
	<p>[Forward trace]</p> <p>If no start month or date is specified, search will begin from the beginning of the current year (Jan 1) to the day of occurrence.</p> <p>If no start date is specified, search will begin from the beginning of the current month (the first day) to the day of occurrence.</p> <p>[Back trace]</p> <p>If no end month or date is specified, search will begin from the generation date to the end of the current year (Dec 31).</p> <p>If no end date is specified, search will begin from the generation date to the end of the current month (the last day).</p> <ul style="list-style-type: none"> <li>- The search range can be specified to "Jan 1, 2004 ~ Dec 31, 2024".</li> <li>- In case of back trace, it is unable to specify a date later than the date of the generating operation log specified as tracing target.</li> <li>- In case of back trace, it is unable to specify a date earlier than the date of the generating operation log specified as tracing target.</li> <li>- In case of both back trace and forward trace, it is unable to specify the date of generating operation log specified as tracing target.</li> <li>- Start date</li> </ul> <p>_ Sep 2009: 1 Sep. 2009 is assumed to be specified.  __ 2009: 1 Jan. 2009 is assumed to be specified.  _( Day)_(Month )_(Year): Start searching from the earliest saved log.  15_ 2009: Specification error  15 Sep. __: Specification error</p> <ul style="list-style-type: none"> <li>- End date</li> </ul> <p>_ Sep 2009: 30 Sep. 2009 is assumed to be specified.  __ 2009: 31 Dec 2009 is assumed to be specified.  _( Day)_(Month )_(Year): Search till the last saved log.  _ 15, 2009: Specification error  15 Sep _ : Specification error</p> <p>*If the specified year is omitted, the specified month and day should be omitted.  If the specified month is omitted, the specified day should be omitted.</p>
[Search target log]	When [Executed search] is [Forward trace], the type of logs as search target can be selected. File operation log is a mandatory option, so it cannot be set to "OFF".
[Maximum search level]	Specify the maximum level for searching. "1" ~ "9" can be specified. The initial value is "4".

5. Click the [Search] button.

→ Results are displayed in the [List of file trace result] window.

Search conditions will be saved automatically. The saved search conditions will be set as the initial value for next startup of the [File trace] window.



Item Name	Description
[Search root directory (type)]	The selected log is displayed at the beginning, and the results of the tracing log are displayed in the tree view.
[Accuracy]	Consistency (accuracy) of traced logs: 0: Log of the investigation start target A: Searched logs that are in complete consistency in drive or UNC description B: Searched logs with consistency under share name C: Searched logs with consistency under file name D: Result searched with only consistency in file name E: Searched logs with partial consistency in file name in printing operation log and printing prohibition log” *: Display when same logs exist in trace logs. Add to the front of the above accuracy (A ~ E) +: Display when the log can be traced further. Add to the front of the above accuracy (A ~ E)
[Occurrence Date and Time]	This displays the time when log occurrence date and time. After clicking on it, the details of log will be displayed.
[User ID]	Display the user name
[Domain name]	The domain name of the client (CT) when logging on to a domain. This is the computer name when logging on to a local computer.
[Classification]	Type of log (normal or Violation)
[Attachment]	Display whether the attached data of log exists or not. For the content of attached data, please refer to “ <a href="#">View attached data</a> ”.
[Content]	Display the content of the log.

Item Name	Description
[Notes]	Display the notes of the log.

When the number of cases in search result exceeds 1000, the following window will be displayed. Up to 1000 cases from the search result can be displayed.

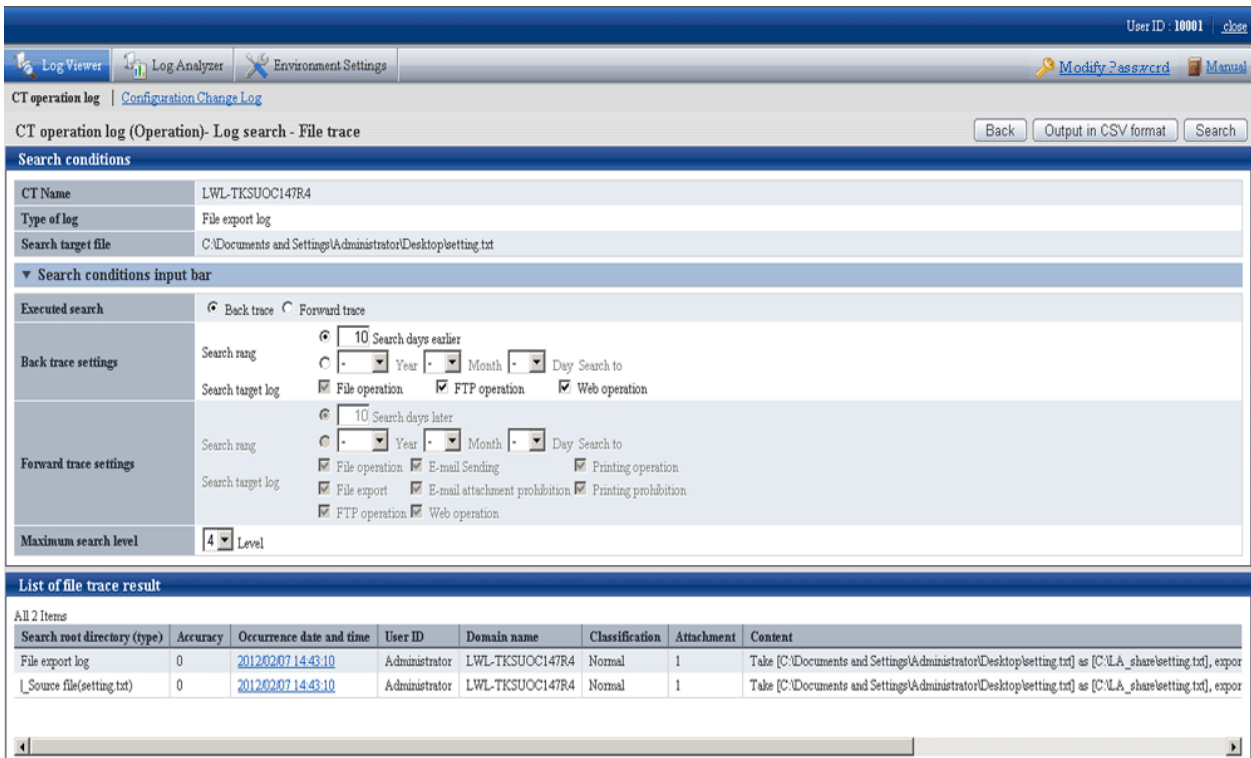


### Example of Back Trace Search

This refers to a process of searching how the files are processed in the past according to the selected log. Only [Copy], [Cut], [Rename], [Create], [Update], [Delete] operations of File Operation Log and export operations of the File Export Log will be traced. This is used while investigating previous file operations.

Example of back trace search

(Investigation target file: customer information.txt)



Please pay attention to [Content] in [List of File Tracing Results].

Information of [Search Route (Type)]	Information of [Content]
File Export Log	Export [C:\Documents and Settings\Administrator\Desktop\Customer Information.txt] to [A:] as [A:\Customer Information.txt] in [Plain text] . Drive type:[Removable]
Source File (Customer Information.txt)	Export [C:\Documents and Settings\Administrator\Desktop\Customer Information.txt] to [A:] in [Plaintext] as [A:\Customer Information.txt]. Drive type:[Removable]
File Operation Log (Copy)	Operation: [Copy]; Source file name: [\\192.168.1.11\share\Customer Information.txt]; Source drive type: [Remote]; Target file name: [C:



Information of [Search Route (Type)]	Information of [Content]
	\\Documents and Settings\Administrator\Desktop\Customer Information.txt]; Target drive type: [Fixed]; Name of application: [Explorer.exe]

The information of investigation target file (Customer Information List.xls) is displayed in the first line. As proceeding to different stages, the previous operation will be traced.

Viewing from the start record of search results, this file is in the client (CT) with the name of SV2

1. The target file for investigation (Customer Information.txt) is exported to a removable media in plain text.
2. The target file for investigation (Customer Information.txt) on the file server is copied to SV2.

This operation record indicates that after the file “Customer Information.txt“ is copied to desktop and exported to removable media in plain text.

### Example of Forward Trace Search

This refers to a process of searching how the files are processed later according to the selected log. The operation process since the generation occurrence date and time of the operation logs specified as tracing target can be investigated. One file may be changed to multiple files by using the copy operation, and the search result may increase, which results from an expanded search target in the log.

### Example of Forward Trace Search

(Investigation target file: customer information.txt)

The screenshot shows the Log Analyzer interface. The search conditions are as follows:

- CT Name: LWL-TKSUOC147R4
- Type of log: File export log
- Search target file: C:\LA\_worksettings.csv
- Executed search: Forward trace
- Back trace settings: Search range 10 days earlier, Search target log includes File operation, FTP operation, and Web operation.
- Forward trace settings: Search range 10 days later, Search target log includes File operation, E-mail Sending, Printing operation, File export, E-mail attachment prohibition, Printing prohibition, FTP operation, and Web operation.
- Maximum search level: 4 Level

The List of file trace result shows 3 items:

Search root directory (type)	Accuracy	Occurrence date and time	User ID	Domain name	Classification	Attachment	Content
File export log	0	20120207 14:43:10	Administrator	LWL-TKSUOC147R4	Normal	1	Take [C:\LA_worksettings.csv] as [C:\LA_share/settings.csv], export to [Plain text] through [C]. Type
Source file(settings.csv)	0	20120207 14:43:10	Administrator	LWL-TKSUOC147R4	Normal	1	Take [C:\LA_worksettings.csv] as [C:\LA_share/settings.csv], export to [Plain text] through [C]. Type
Target file(settings.csv)	0	20120207 14:43:10	Administrator	LWL-TKSUOC147R4	Normal	1	Take [C:\LA_worksettings.csv] as [C:\LA_share/settings.csv], export to [Plain text] through [C]. Type

Please pay attention to [Content] in [List of file tracing result].

[Search Route (Type)]	[Content]
File Export Log	Export [C:\Documents and Settings\Administrator\Desktop\Customer Information.txt] to [A:] as [A:\Customer Information.txt] in [Plain text] . Drive type: [Removable]

[Search Route (Type)]	[Content]
File Operation Log (Delete)	Operation: [Delete]; Source file name: [C:\Documents and Settings\Administrator\Desktop\Customer Information.txt]; Drive type: [Fixed] ; Name of application: [Explorer.exe]

The information of the investigation target file (Customer Information List.xls) is displayed in the first line. As proceeding to different stages, information on how the investigation target file has been processed up to now will be displayed.

Viewing from the start record of search results, this file is in the client (CT) with the name of SV2

1. Export Customer Information.txt.
2. Delete Customer Information.txt from local disk.

This operation record indicates that the customer information is deleted after exporting to the external.

### Export tracing result of file operation to CSV file

This department describes how to export searched file trace results to a CSV file.

1. When the trace logs to be exported to a CSV file are displayed in [List of file tracing result], click the [Output in CSV format] button.
2. When the file download window is displayed, click the [Save] button.
3. After selecting the saving folder and entering the file name, click the [Save] button.

The following symbols cannot be used as file name:

“\”, “/”, “:”, “\*”, “?”, ” ””, “<”, “>”, “|”

When a file with same name exists in the export destination, the option window indicating whether to overwrite will be displayed. Please select the desired option.

For item name and description of an exported CSV file, please refer to “Log List of File Trace Result” of “Systemwalker Desktop Keeper Reference Manual”.

### Reset tracing file to trace file again

This department describes how to execute file tracing again after modifying the tracing target file according to the searched file trace result.

1. Select a log with the file information needed to be reset from [List of file trace result] of the [CT Operation Log (Operation) - Log Search - File Trace] window, and click [Occurrence date and time].

“Printing Operation Log” and “Printing Prohibition Log” will be displayed as additional information in [File Trace Results], but they cannot be selected as search target.

2. Click the [Reset Trace object] button.

→ The file name is set in [Search target file] .

When selecting an E-mail sending log that has multiple attachments, the [Select Tracing Target] window will be displayed first. Please select a file name in the [Select Tracing Target] window and set it as [Search Target File].

3. Set search conditions, and click the [Search] button.

→The results of tracing will be displayed in [List of file trace results].

### When file download is not successful

When the download of CSV file, original file backup and command operation file is not successful, please refer to “Preparation of Using Web Browser in PC” of “Systemwalker Desktop Keeper Installation Guide” to modify the settings of Internet Explorer®

## 5.4 Search CT Information in Log Viewer

This department describes how to search the client (CT) and CT group.

When the “Deleted CT” group is displayed in the CT group tree of [Select Department] domain, the client (CT) that belongs to the “Deleted CT” group will also be searched.

The client (CT) of the “Deleted CT” group will be displayed as “Deleted CT” in [Group] of [List of searched CT].

1. Start Log Viewer.
2. Select [Root] or “CT Group” from the CT group tree as a search target.
3. Click the [CT/CT group search] button.

→The [CT/CT group search] window is displayed.

The screenshot shows the 'Configuration change log(Operation) - CT/CT group search' window. The search conditions input bar includes the following fields:

- Computer name (partially match)
- IP address (099.999.999.999) (forward match)
- MAC address (XX-XX-XX-XX-XX-XX) (match)
- Owner name (partial match)
- CT Version (match)
- Name/CT group name (partial match)
- DTPID (partial match)
- Notes (partial match)
- Final logon date (Year, Month, Day)
- Client policy update date (Year, Month, Day)
- Applied policy (As conditions, CT, Group)
- Active Directory Linkage target (As conditions, Linkage object, Non-linkage target)
- Virtual PC (As conditions, Physical PC, Virtual PC, Master image)

The 'List of searched CT' table has the following columns:

Group	Name	Applied policy	Computer name	OS	Organization name	Owner name	Final logon date and time	Client policy update date and time	Server (DB) update date and time	Occurrence date
-------	------	----------------	---------------	----	-------------------	------------	---------------------------	------------------------------------	----------------------------------	-----------------

4. Enter the following information as search condition.

The search is the “AND Search” that contains all the multiple conditions.

### [Search CT Group]

Specify [Name/CT Group Name] and [Notes] only. In addition, the [As conditions] checkbox of [Applied policy] should not be selected.

### [Search Client (CT)]

Specify the items of search condition.

Item Name	Description
[Computer name]	Search according to the computer name of the client (CT). Results that partially match the input conditions will be displayed. Up to 15 bytes of single-byte and double-byte characters can be entered.
[IP address]	Search according to the IP address of client (CT). Results of which the front part matches the input conditions will be displayed. When searching with “10.1”, the result will include “10.1.”, “10.1X.” and “10.1XX.” ( “X” indicates one numeral character)

Item Name	Description
	Enter in the format of "XXX.XXX.XXX.XXX". [Example] 140.48.23.12
[MAC address]	Search according to the MAC address of client (CT). Results that completely match the input conditions will be displayed. Enter in the format of "XX-XX-XX-XX-XX-XX". ("X" indicates one alphanumeric character) [Example] 02-E0-32-33-A3-C0
[Owner name]	Search according to the owner set in the OS of client (CT). Results that partially match the input conditions will be displayed. Up to 93 bytes of single-byte and double-byte characters can be entered.
[CT Version]	Search according to the version of client (CT) of the Systemwalker Desktop Keeper installed. Results that completely match the input conditions will be displayed. Enter in the format of "X.X.X.X". ("X" indicates more than one numeral characters) [Example] 2.1.0.1
[Name/CT group name]	Search according to the name of CT group or client (CT). Results that partially match the input conditions will be displayed. Up to 40 bytes of single-byte and double-byte characters can be entered.
[DTPID]	This is displayed when the client (CT) of Systemwalker Desktop Keeper and the client (CT) of Systemwalker Desktop Patrol are installed on the same PC. Enter "User ID (+) PC name" of the client (CT) of Systemwalker Desktop Patrol. Perform search with partially matching.
[Notes]	Search according to the notes entered when updating the client (CT) policy. Results that partially matches the input conditions will be displayed. Up to 128 bytes of single-byte and double-byte characters can be entered.
[Final logon date]	<p>The client (CT) communicates with the Master Management Server or Management Server at startup. Search according to the date and time when this communication is enabled.</p> <p>Specify the range of period. If the start and end of [Search Range] is not specified, all period will become the search target.</p> <p>If no start month or date is specified, search will begin from the beginning of the specified year (Jan. 1).</p> <p>If no start date is specified, search will begin from the beginning of the specified month (the first day).</p> <p>If no end month or day is specified, search till the end of the specified year (Dec 31). If the end day is not specified, search till the end of the specified month (the last day).</p> <p>If the initial value is displayed as "-" (search in all periods).</p> <ul style="list-style-type: none"> <li>- Start date <ul style="list-style-type: none"> <li>_ Sep 2009: 1 Sep. 2009 is assumed to be specified.</li> <li>__ 2009: 1 Jan. 2009 is assumed to be specified.</li> <li>_( Day)_(Month)_(Year): Start searching from the earliest saved log.</li> <li>15_ 2009: Specification error</li> <li>15 Sep. __: Specification error</li> </ul> </li> <li>- End date <ul style="list-style-type: none"> <li>_ Sep 2009: 30 Sep. 2009 is assumed to be specified.</li> <li>__ 2009: 31 Dec 2009 is assumed to be specified.</li> <li>_( Day)_(Month)_(Year): Search till the last saved log.</li> </ul> </li> </ul>

Item Name	Description						
	<p>_ 15, 2009: Specification error 15 Sep _ : Specification error</p> <p>*If the specified year is omitted, the specified month and day should be omitted. If the specified month is omitted, the specified day should be omitted.</p>						
[Client policy update date]	<p>Search according to the last date when the client (CT) obtains policy from the Master Management Server or Management Server</p> <p>Specify the range. If the start and end of [Search Range] is not specified, the search target will be all periods.</p> <p>If no start month or date is specified, search will begin from the beginning of the specified year (Jan. 1).</p> <p>If no start date is specified, search will begin from the beginning of the specified month (the first day).</p> <p>If no end month or day is specified, search will go until the end of the specified year (Dec 31).</p> <p>If the end day is not specified, search will go until the end of the specified month (the last day).</p> <p>If the initial value is displayed as “-” (search in all periods).</p> <p>- Start date</p> <p>_ Sep 2009: 1 Sep. 2009 is assumed to be specified. __ 2009: 1 Jan. 2009 is assumed to be specified. _( Day)_(Month )_(Year): Start searching from the earliest saved log. 15_ 2009: Specification error 15 Sep. __ : Specification error</p> <p>- End date</p> <p>_ Sep 2009: 30 Sep. 2009 is assumed to be specified. __ 2009: 31 Dec 2009 is assumed to be specified. _( Day)_(Month )_(Year): Search till the last saved log. _ 15, 2009: Specification error 15 Sep _ : Specification error</p> <p>*If the specified year is omitted, the specified month and day should be omitted. If the specified month is omitted, the specified day should be omitted.</p>						
[Applied policy]	<table border="1"> <tr> <td data-bbox="384 1413 555 1491">[As conditions]</td> <td data-bbox="555 1413 1367 1491">When this checkbox is selected, the policy being applied to the client (CT) will be included in the search condition.</td> </tr> <tr> <td data-bbox="384 1491 555 1536">[CT]</td> <td data-bbox="555 1491 1367 1536">The search target is the client (CT) to which the CT policy is applied.</td> </tr> <tr> <td data-bbox="384 1536 555 1581">[Group]</td> <td data-bbox="555 1536 1367 1581">The search target is the client (CT) to which the CT group policy is applied.</td> </tr> </table>	[As conditions]	When this checkbox is selected, the policy being applied to the client (CT) will be included in the search condition.	[CT]	The search target is the client (CT) to which the CT policy is applied.	[Group]	The search target is the client (CT) to which the CT group policy is applied.
[As conditions]	When this checkbox is selected, the policy being applied to the client (CT) will be included in the search condition.						
[CT]	The search target is the client (CT) to which the CT policy is applied.						
[Group]	The search target is the client (CT) to which the CT group policy is applied.						
[Active Directory Linkage target]	<table border="1"> <tr> <td data-bbox="384 1581 555 1659">[As conditions]</td> <td data-bbox="555 1581 1367 1659">When this checkbox is selected, whether this is the client (CT) that imports information from Active Directory will be included in the search condition.</td> </tr> <tr> <td data-bbox="384 1659 555 1738">[Linkage object]</td> <td data-bbox="555 1659 1367 1738">The search target is the client (CT) that imports information from Active Directory.</td> </tr> <tr> <td data-bbox="384 1738 555 1816">[Non-linkage object]</td> <td data-bbox="555 1738 1367 1816">The search target is the client (CT) that does not import information from Active Directory.</td> </tr> </table>	[As conditions]	When this checkbox is selected, whether this is the client (CT) that imports information from Active Directory will be included in the search condition.	[Linkage object]	The search target is the client (CT) that imports information from Active Directory.	[Non-linkage object]	The search target is the client (CT) that does not import information from Active Directory.
[As conditions]	When this checkbox is selected, whether this is the client (CT) that imports information from Active Directory will be included in the search condition.						
[Linkage object]	The search target is the client (CT) that imports information from Active Directory.						
[Non-linkage object]	The search target is the client (CT) that does not import information from Active Directory.						
[Virtual PC]	<table border="1"> <tr> <td data-bbox="384 1816 555 1895">[As conditions]</td> <td data-bbox="555 1816 1367 1895">When this checkbox is selected, the environment with the client (CT) installed will be included in the search condition.</td> </tr> <tr> <td data-bbox="384 1895 555 1939">[Physical PC]</td> <td data-bbox="555 1895 1367 1939">This refers to the client (CT) installed in a physical PC.</td> </tr> <tr> <td data-bbox="384 1939 555 1980">[Virtual PC]]</td> <td data-bbox="555 1939 1367 1980">This refers to the client (CT) installed in a virtual PC.</td> </tr> </table>	[As conditions]	When this checkbox is selected, the environment with the client (CT) installed will be included in the search condition.	[Physical PC]	This refers to the client (CT) installed in a physical PC.	[Virtual PC]]	This refers to the client (CT) installed in a virtual PC.
[As conditions]	When this checkbox is selected, the environment with the client (CT) installed will be included in the search condition.						
[Physical PC]	This refers to the client (CT) installed in a physical PC.						
[Virtual PC]]	This refers to the client (CT) installed in a virtual PC.						

Item Name		Description
	[Master image]	This refers to the client (CT) installed in the master image of a virtual PC.
[Search]		The search will be started and the results will be displayed.
[Cancel]		The entered search condition will be saved.

### Note

#### **Input of Double-byte characters must be noticed**

If the following items are displayed in double-byte characters, the size of input character strings may exceed the specified upper limit, but such operation may result in error during search:

- Computer name
- Owner
- Name/CT Group Name
- Notes Text (Any)

#### 5. Click the [Search] button.

→ Search results are in the [List of searched CT] window.

The display items are those selected from the [Visible Columns Settings] window. For details about the [Visible Columns Settings] window, please refer to “[Set visible columns in \[List of searched CT\]](#)”.

After clicking [Name] of a searched CT or CT group, the [Log Search] window will be displayed and the CT groups corresponding to the configuration information tree will be selected. In addition, the entered search conditions will be saved during the logon process, but they will be cleared once the password is changed or the search conditions are updated.

# Chapter 6 Create Auditing Material

This chapter describes how to use the Report Output Tool.

## 6.1 How to Make Flexible Use of Report Output Tool



**The number of logs displayed in the report created by Report Output Tool may be inconsistent with the number of logs in the result of aggregate by objective of Log Analyzer.**

The number of logs displayed in the report is the result of aggregation according to the screening condition and exclusion condition of moving logs from the Management Server to the Log Analyzer Server.

Therefore, the modified screening condition/exclusion condition and logs moved after aggregation cannot be reflected (\*).

In addition, the aggregate by objective in Log Analyzer is a real-time aggregation. That is, the result of aggregating the logs that have completed moving is according to the latest screening condition/exclusion condition.

Therefore, the number of logs displayed in the report created by Report Output Tool may be inconsistent with the number of logs in the result of aggregate by objective of Log Analyzer.

If the aggregation result of logs moved after aggregation is expected to be displayed in the report (when it is expected to aggregate again according to the latest data and condition) according to the screening condition/exclusion condition modified after aggregation, re-aggregation is required.

For re-aggregation, please refer to “DTTOOLEX.EXE (Data Moving and Deletion for Log Analyzer Server)” of “Systemwalker Desktop Keeper Reference Manual”.

\*) What is the case when logs are moved in after aggregation

Due to reasons such as the client (CT) not being connected to the network, log transmission to the Management Server may be delayed. Therefore, the reflection of logs moved to Log Analyzer Server may be delayed.

### **When the department of non-target group is displayed in [Group Name] of report**

When the terminal to which the target group belongs includes the terminals from other departments, the logs collected when these terminals belong to the other department will be aggregated.

In addition, these logs are aggregated according to the group name at collection time point.

Therefore, if the above terminal exists, the department name of non-target group will be displayed as the group name.

### **Processing of PrintScreen key prohibition log**

This chapter only treats the PrintScreen Key Prohibition Logs that are classified as “violation” as the processing target.

### **About printing paper cost and CO2 emission output report of printing volume auditing**

The printing paper cost and CO2 emission output report of printing volume auditing is the result of multiplying the total number of pages printed during the all target period with the cost of each printed page and CO2 emissions.

Therefore, it is only an approximate value rather than an accurate cost of printing paper and CO2 emission.

### **About Not Configured group**

When [Manage under the group that is not configured] is set in [Set group that is not configured] of [System Settings] in the Server Settings Tool, the Report Output Tool will manage the client (CT) in the "Root" group instead of the "Not Configured" group.

## What is Report Output Tool

Using the Report Output Tool, reports can be created, printed and output according to the following purposes. The report will be output as a file in Microsoft® Excel format, which can be used directly or after the process.

- The system administrator can know the security status and reduction of CO2 emission calculated according to paper usage amount.
- The security status, compliance status and reduction of CO2 emission will be reported to the security administrator of organization, compliance administrative organization and upper level of organization.

The reports that can be generated are as follows:

Report Type	Summary
Information disclosure analysis	
Information disclosure analysis	Output the result of aggregating and analyzing operation logs according to the viewpoint of danger of information disclosure.
Terminal usage analysis	Output the result of aggregating and analyzing operation logs according to the viewpoint of whether the terminal is used properly or not.
Violation operation analysis	Output the result of aggregating and analyzing the logs recorded when the prohibited operation is performed.
Comprehensive analysis	Output the summary of diagnosis of the above three viewpoints.
Eco auditing	
Printing volume auditing	Calculate the print volume and printing cost of each month as well as CO2 emissions by using printing operation log. Output the analysis result as a report of print volume, printing cost and reduced amount of CO2 compared to last month. In addition, the list of terminals that have exceeded the upper limit of printing can also be output.

## Person who can use

The system administrator and department administrator can use the Report Output Tool. However, when the report is being generated, the scope of the logs that can be analyzed varies depending on administrator's status.

Administrator Type	Scope of Logs can be Analyzed
System Administrator	All logs that can be read on the Management Server or Master Management Server on which this user ID is registered.
Department Administrator	All logs belong to the department managed by the department administrator.

## Environment can be used

When using the Report Output Tool, please prepare an environment that satisfies all the following conditions:

- The Report Output Tool has been installed in the PC that outputs report.
- Microsoft® Excel of any of the following versions has been installed in the PC that outputs report:
  - Microsoft® Excel 2002
  - Microsoft® Office Excel 2003
  - Microsoft® Office Excel 2007
  - Microsoft® Office Excel 2010



- The printer that will be printing the report is set.

The factors that affect the processing time of report output are the amount of logs saved in the database and the amount of logs output to CSV files.

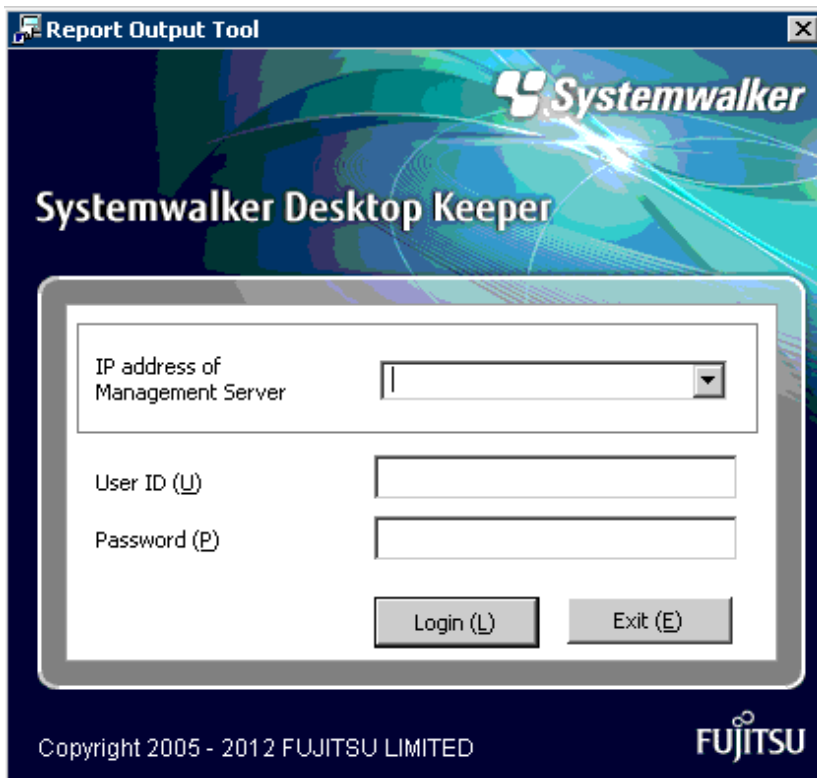
When the amount of logs saved in the database is about 30 million, the following amount of time is required approximately. (However, the processing time is only for reference. The time may vary depending on the CPU of the PC, memory, disk performance and execution of other applications, etc.)

- When outputting report only: about 12 seconds
- When outputting report and one type of CSV file: about 85 seconds

## 6.2 Start Report Output Tool

The startup procedure is as follows:

1. Log on to Windows with the Windows account to which the Administrator or the Domain Admins group belongs.
2. Select [Programs] - [Systemwalker Desktop Keeper] - [Log Analyzer] - [Report Output Tool] from the [Start] menu  
→ The login window is displayed.



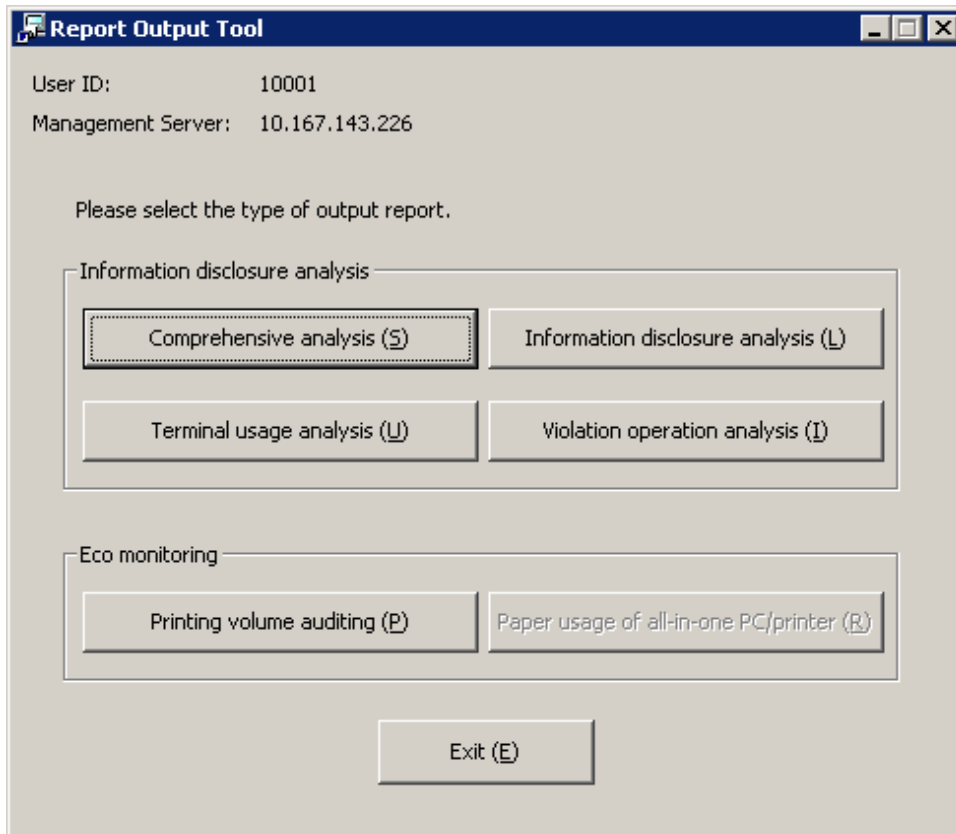
Item Name	Description
[IP address of Management Server]	Specify the IP address of the Master Management Server or Management Server. Enter the string in IP address format within 15 characters. Up to 10 IP addresses that have been authenticated once can be recorded. From the next time, selection can be made from the pull-down menu of the login window.
[User ID]	It is user ID of the system administrator or department administrator.

Item Name	Description
[Password]	Specify the password of user ID entered in [User ID].

The information moved from the Management Server to Log Analyzer Server will be used during authentication. The authentication information modified in the Management Server cannot be reflected to the Log Analyzer Server immediately (The information will be reflected at the next time of moving management information and logs). Therefore, before moving the modified authentication information from the Management Server to the Log Analyzer Server, please logon with the previous authentication information.

3. Enter the required information and click the [Login] button.

→ The following window is displayed.



- User ID: This is the login user ID.
- Management Server: This is the IP Address of the Management Server on which the report output logs are saved.

4. Select the type of report to be output.

## 6.3 Information Disclosure Analysis Report

The Information disclosure analysis report outputs the result of aggregating and analyzing the following logs according to the evaluating information disclosure risk:

- File Export Log
- File Operation Log
- Printing Operation log
- Logs of E-mail Sending Log by Recipient Address

## 6.3.1 Output Information Disclosure Analysis Report

The procedure is as follows:

1. Select [Information disclosure analysis] in the [Report Output Tool] window.  
→ The following window is displayed.

- User ID: This is the login user ID.
- Management Server: This is the IP address of the Management Server on which the report output logs are saved.

2. Set the items of each tab.

The settings of each tab will be saved in the Log Analyzer Server as inherent information of the login user when [Print] or [Save File] is performed. The saved information will be displayed at next startup.

Settings of [Basic Information] tab

Set the following items.

Input Item		Content
[Report title]		Specify the title (up to 64 characters) of report to be output.
[Created by]		Specify creator (up to 40 characters) of report.
[Analysis period]	[Daily report] (Initial Value)	Specify the aggregation target of daily report. The default setting is the day before the login day.

Input Item		Content
	[Weekly report]	Specify the aggregation target of weekly report. The default setting is the last start day of weekly report. In the pull-down menu of start day, the date corresponding to the week set in the [Start Day Setting of Weekly Report] of [Operation Settings] tab in Log Analyzer of the Desktop Keeper Main Menu will be displayed.
	[Monthly report]	Specify the month of aggregation target of monthly report. The default setting is the latest start day of monthly report. The displayed date is the value set in the [Start Day Setting of Monthly Report] of [Operation Settings] tab in Log Analyzer of the Desktop Keeper Main Menu.
[Index value]	[Difference value compared with the last time]	As the standard index value of information disclosure risk, when a certain degree of change has occurred since last report output, specify to judge whether it has deteriorated or improved within the range of “1~99” percent. The initial value is 10%.
	[Long-term difference]	As the standard index value of information disclosure risk, when a certain degree of change has occurred during the last ten times of diagnosis output by report, specify to judge whether it has deteriorated or improved within the range of “1~99” percent. The initial value is 5%.

Settings of [Option] tab

Set the following items.

Select the ranking items to be output to report.  
Please make sure to select more than one item (All items are selected in default).

Item Name	Description
[Ranking by group]	Display the result of aggregation by group with the worst ranking based on number of cases.
[Ranking by terminal]	Display the result of aggregation by terminal with the worst ranking based on number of cases.
[Ranking by user]	Display the result of aggregation by user name with the worst ranking based on number of cases. Even if the same user name appears in different terminals, it will be processed as the same user.
[Ranking by terminal+user name]	Display the result of aggregation by terminal + user name with the worst ranking based on number of cases. Even if the same user name appears in different terminals, it will be processed separately.

[Log Information]

Select when outputting the logs used in the aggregation of ranking (All items are selected in default).  
The Information disclosure analysis report is a single file output in CSV format.

Item Name	Description
[File export log]	Output file export log as a single file.
[File operation log]	Output file operation log as a single file.
[Printing operation log]	Output printing log as a single file.

Item Name	Description
[E-mail sending log by recipient address]	Output logs of e-mail sending by recipient address as a single file.

Settings of [Object Group] tab

Set the following items.

The screenshot shows the 'Report Output Tool' window with the 'Object Group' tab selected. The window displays the following information:

- User ID: 10001
- Management Server: 10.167.143.226
- Navigation tabs: Basic Information, Option, Object Group (selected)
- Section: Report output of target group
  - Output list of target groups as report
- Buttons: Print (P), Save File (S)
- List of object (Number of groups 2)
 

No	Group Name
1	Root
2	Deleted CT
- Bottom button: Close (C)

Item Name	Description
[Report output of target group] [Output list of target groups as report]	<ul style="list-style-type: none"> <li>- When it is selected: Output [List of object] to report.</li> <li>- When it is not selected (<b>Initial Value</b>): Do not output [ List of object] to report.</li> </ul>
[List of object]	<p>The department of the log analysis target and its subordinate units will be output to report.</p> <p>The department name will be separated by “/” and displayed with the full path starting from the root.</p> <p>[Example] Development Department/Development Unit 3</p> <p>The total number of set departments is displayed beside the title.</p>

3. Click the [Print] or [Save File] button.

### Note

#### **Please do not operate Microsoft® Excel in the process of report output**

Please do not perform the [New] and [Open] operation of Microsoft® Excel file during the report output process, as report output may not be performed normally.

In addition, please confirm whether Microsoft® Excel was started correctly before the report output. When Microsoft® Excel is not started correctly, problems such as the report output process taking too much time and being unable to finish will occur.

#### **[When clicking the [Print] button]**

Print the generated report and logs used for the aggregation of ranking.

In the displayed [Print] window, set the printer and print the report.

### Point

#### **The Printing Dialog Box may hide behind the Report Output Tool.**

When the Printing Dialog Box has not displayed after a long time, it may be hidden behind the Report Output Tool.

#### **[When clicking the [Save File] button]**

Save the generated report and logs used for the aggregation of ranking as a file.

### Note

#### **Please save the output report to a safe place**

The output report may contain personal information and system configuration information. Please specify a folder that has been implemented sufficient security policy as the target for saving the file.

[Example]

Set the access authority of folder to allow only the administrator to view.

In the displayed saving window, specify the destination for saving and click the [Save] button.

Each file will be saved with the following name.

[Report File]

Default Name: Leak\_ [Analysis Period] \_ [Start Date of Analysis Period].xls

(When a file with same name exists, the confirmation dialog for overwriting will be displayed.)

- Analysis period  
Daily report: daily  
Weekly report: weekly  
Monthly report: monthly
- Start date of analysis time: YYYYMMDD (date set in [Analysis Period] of the [Basic Information] tab)

[CSV File of Log]

Log Type	CSV File Name
File export	Leak_Log_Filebringout_YYYYMMDD.csv
File Operation	Leak_Log_Fileaccess_YYYYMMDD.csv
Printing Operation	Leak_Log_Print_YYYYMMDD.csv

Log Type	CSV File Name
E-mail Sending Log by Recipient Address	Leak_Log_Mailsend_YYYYMMDD.csv

When a file with same name exists, the number with () will be added to the end of file name.

Example: Leak\_Log\_Filebringout\_YYYYMMDD (2).csv

The following will be are (3) and (4), etc.

### Note

#### **Please confirm UNICODE character in Internet Explorer®**

When the UNICODE characters (including JIS2004) that do not correspond to the Shift JIS font are used in the log data, they will be displayed in the HTML Escape format in the CSV file.

Please open the following HTML files using Internet Explorer®, and confirm the font of JIS2004 that contains UNICODE character:

- File location: HTML folder under the target folder for saving report file.
- File name: it has the same name as CSV file (The extension is “.html”).

The content that is same as the log data that is output to the CSV file will be displayed in this HTML file.

## 6.3.2 Content of Information Disclosure Analysis Report

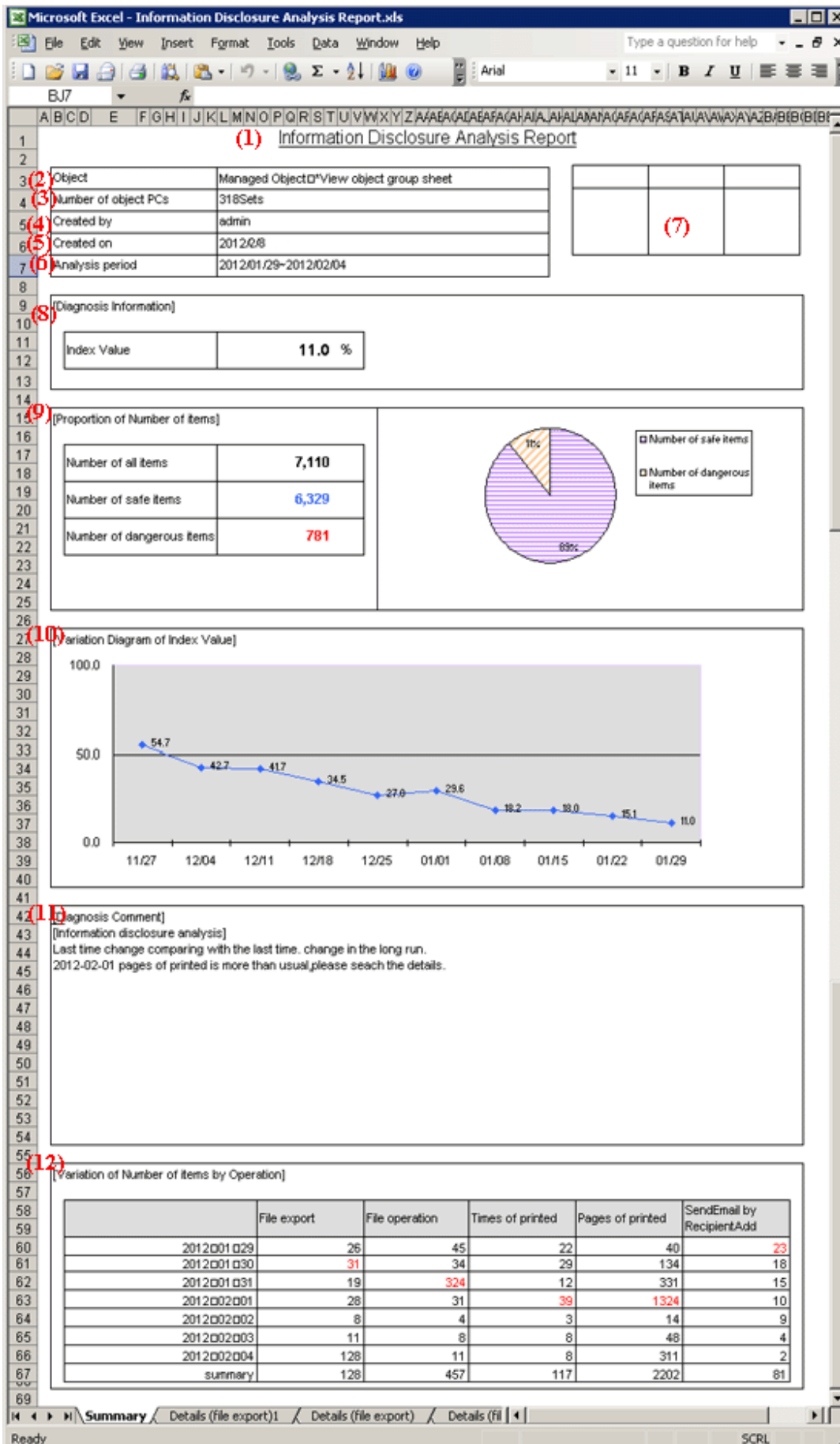
The structure of Information disclosure analysis report is as follows:

Classification	Sheet Name	Description
Summary Sheet	Summary	Summary of the generated report is recorded.
Detail Sheet	Detail (File export)	All kinds of aggregation information (ranking information) of each operation log is recorded.
	Detail (File Operation)	
	Detail (Times of Printing Operation)	
	Detail (Pages of Printing Operation)	
	Detail (E-mail Sending Log by Recipient Address)	
Target Group Sheet	Target Group	The list of departments that has collected analysis target logs is recorded.

The layouts of the generated report file and printing result may vary depending on the version of Microsoft® Excel and service pack being used.



Summary sheet



(1) Report title

The title specified in the basic information settings is recorded.

(2) Object

Display the managed target. It is always displayed as "Managed Target".

(3) Number of object PCs

Display the number of all PCs of managed target.

- When the target PC does not exist, 0 will be displayed.

(4) Created by

The creator name specified in the basic information settings is recorded.

(5) Created on

The date of report output is recorded.

(6) Analysis period

The analysis period specified in the basic information settings is recorded.

(7) Approval column

It is the approval column (The number of columns cannot be modified) when it is used as a report.

(8) Diagnosis information: index value

The proportion of dangerous cases (Refer to "Number of Dangerous Cases" of "(9) Proportion") in all operations is indicated in percentage.

(9) Proportion of Number of items

- Number of all items

The following section varies depending on the analysis content.

[Information Disclosure Analysis]

Number of file export cases (number of cases exported to a removable device or DVD/CD) + number of file operation cases (number of cases copied or moved to DVD/CD, or created and viewed in a removable device or DVD/CD) + number of printing operation cases + number of cases of E-mail sending Log by recipient address (number of cases of E-mail sending log by recipient address that does not match the screening condition)

[Terminal Usage Analysis]

Number of cases of Window title obtaining with URL + number of cases of E-mail sending log by recipient address + number of cases of application startup

[Violation Operation]

Number of all cases of information disclosure + number of all cases of terminal usage + number of dangerous cases of violation operations

- Number of safe items

Total number of operation cases excluding the dangerous ones.

- Number of dangerous items

The following section varies depending on the analysis content:

[Information disclosure analysis]

Number of cases in all cases that match the screening condition (keywords).

[Terminal usage analysis]

Number of cases of Window title obtaining with URL that does not match the screening condition (domain) + number of cases of E-mail sending log by recipient address that does not match the screening condition (domain) + number of cases of application startup that does not match the screening condition (application)

[Violation Operation Analysis]

Number of application startup prohibition cases + number of printing prohibition cases + number of logon prohibition cases + number of PrintScreen key prohibition cases + number of E-mail file attachment prohibition cases

- Pie chart

The pie chart can be used to display the proportion of safe cases to dangerous cases.

When the number of cases is 0, the pie chart will not be displayed (“1%” will be displayed in the location of the pie chart.).

#### (10) Variation Diagram of Index Value

The variation of the index value is displayed by curve graph (the last 10 times).

The vertical axis of the chart is the numerical value of the index value. The bottom end indicates the dangerous rate to be 0 while the top end indicates the dangerous rate to be 100. Therefore, the closer to zero the index value is, the more ideal the state is.

The horizontal axis shows the start day of each analysis period. On the horizontal axis, the index value of analysis period without data is 100.

#### (11) Diagnosis comment

- Inspection of comparison with the last time

Through the difference value of the index value obtained by comparing the result with the previous diagnosis, information on whether the danger level has increased or decreased can be obtained. Based on this, comment about risk status judgment can be proposed for the index value of this analysis result.

- Long-term tendency

According to the increased or decreased index value compared to the past, comment about risk status judgment can be proposed for the index value predicted based on the variation of the index value from the past analysis result.

- Inspection about day/operation that requires attention

The date and operation with the highest risk in the period that requires investigation will be prompted. (Only when monthly report or weekly report is selected)

#### (12) Variation of Number of Items by Operation

The variation of the number of each operation item set in the analysis period is displayed in table format.

The analysis period is one month for a monthly report, 7 days for a weekly report, and one day for a daily report.

In addition, the maximum number of operation cases within the period is displayed in red character in each operation log.

## Detail sheet

The information output to the detail sheet is described using “Detail (File Export) Sheet” as an example.

The other operations such as file access are output in the same format.

Up to 512 bytes can be displayed in the contents of each item in ranking table.



.....

### Please confirm UNICODE character in Internet Explorer®.

When the UNICODE characters (including JIS2004) that do not correspond to the Shift JIS font are used in the log data, they will be displayed in the HTML Escape format in CSV file.

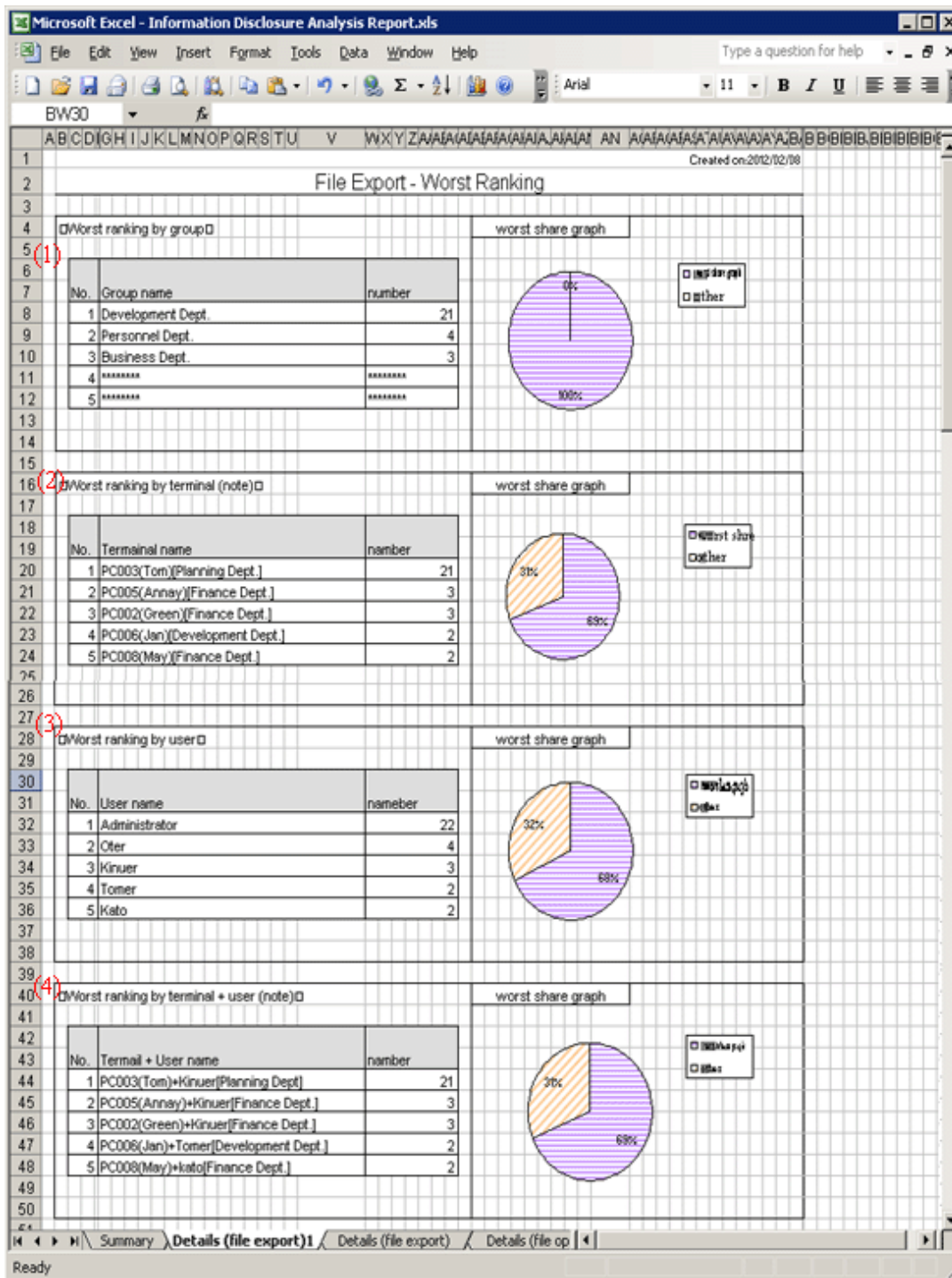
Please open the following HTML files using Internet Explorer®, and confirm the font of JIS2004 that contains UNICODE character.

- File location: HTML folder under the target folder for saving report file.
- File name: it has the same name as CSV file (The extension is “.html”).

The content that is same as ranking information displayed in the detail sheet will be displayed in this HTML file (Though each type of log has one sheet in the Microsoft® Excel format, all types will be gathered in one file in HTML.).

However, it cannot be displayed correctly outside the environment that supports the font of UNICODE character containing JIS2004.

.....



When the same ranking exists and the displayed data amount exceeds the set value of ranking number, up to 30 cases can be displayed.

(1) Worst ranking by group

Display the aggregation result by group with the ranking in descending sequence of number of cases. In addition, the proportion of number of operation cases performed by groups in top ranking to all operations will be shown in the worst share graph.

(2) Worst ranking by terminal (note)

Display the aggregation result by terminal with the ranking in descending sequence of number of cases. At the same time, the graph will also be displayed, and the proportion of number of operation cases performed by terminals in top ranking to all operations will be shown in the worst share graph.

(3) Worst ranking by user

Display the aggregation result by user with the ranking in descending sequence of number of cases. At the same time, the graph will also be displayed, and the Proportion of number of operation cases performed by users in top ranking to all operations will be shown in the worst share graph.

(4) Worst ranking by terminal + user (note)

Display the aggregation result by terminal + user with the ranking in descending sequence of number of cases. At the same time, the graph will also be displayed, and the Proportion of number of operation cases performed by terminals corresponding to the users in top ranking to all operations will be shown in the worst share graph.

Note: "Computer Name" and "Computer Name + User Name" of ranking cases are displayed in the following format.

- When [Name] displayed in the CT list of the Management Console is the same as [Computer Name]

The following are conditions that make [Name] and [Computer Name] the same:

- Because [Name] is not updated after CT installation, the initial value will be displayed as [Computer Name].
- The [Name] is updated to the same name as [Computer Name] in the Management Console.

At this time, it will be displayed in the format of "Computer Name [Group Name] in ranking by terminal.

[Example] PC001 [Personnel Department]

In ranking by terminal + user name, it will be displayed in the format of "Computer Name + User Name [Group Name".

[Example] PC001 + Administrator [Personnel Department]

- When the [Name] displayed in the CT list of the Management Console is different from [Computer Name]

The following are conditions that make [Name] and [Computer Name] different:

- The [Name] is updated to a different name from [Computer Name] in the Management Console.

At this time, it can be displayed in the format of "Computer Name (Name) [Group Name]" in ranking by terminal.

[Example] BLONO (Fujitsu Taro) [Personnel Department]

In ranking by terminal + user, it can be displayed in the format of "Computer Name (Name) + User Name [Group Name)".

[Example] BLONO (Fujitsu Taro) + Administrator [Personnel Department]

### Target group sheet

The department information that has been analyzed will be output.

(1) Object Group	
(2)	(3)
No	Group name
1	Root Directory
2	Operation Dept.
3	Operation Dept./Operation Div. 1
4	Operation Dept./Operation Div. 2
5	Development Dept.
6	Planning Dept.
7	Management Dept.
8	Finance Dept.
9	Product Evaluation Dept.
10	Business Dept.

(1) Report title

This is recorded as “Object Group”.

(2) Target group list

The department of analysis target is recorded.

The group name can be recorded with the full path beginning from the root.

[Example] Development Department/ Development Unit 3

When multiple managed departments exist, they can be displayed after adding rows.

Up to 50,000 departments can be recorded.

Up to 512 bytes can be displayed in the content of each item in target group.

## **6.4 Terminal Usage Analysis Report**

---

The Terminal usage analysis report can output the result of aggregating and analyzing the following logs according to whether the PC is used correctly according to organization policy.

- Window Title Obtaining Log with URL
- Log of E-mail Sending Log by recipient address
- Application startup log

## 6.4.1 Output Terminal Usage Analysis Report

1. Select [Terminal Usage Analysis] in the [Report Output Tool] window.  
→The following window is displayed.

The screenshot shows the 'Report Output Tool' window with the following settings:

- User ID: admin
- Management Server: 193.168.245.128
- Basic Information tab is selected.
- Report title (T): Terminal Usage Analysis Report
- Created by (N): admin
- Analysis period:
  - Daily report (D): Year 2012, Month 2, Day 4
  - Weekly report (W): Year 2012, Month 1, Day 29, In one week from this day
  - Monthly report (M): Year 2011, Month 12, Day 21, In one month from this day
- Index value:
  - Difference value compared with the last time (B): 10 % (1~99)
  - Long-term difference (L): 5 % (1~99)

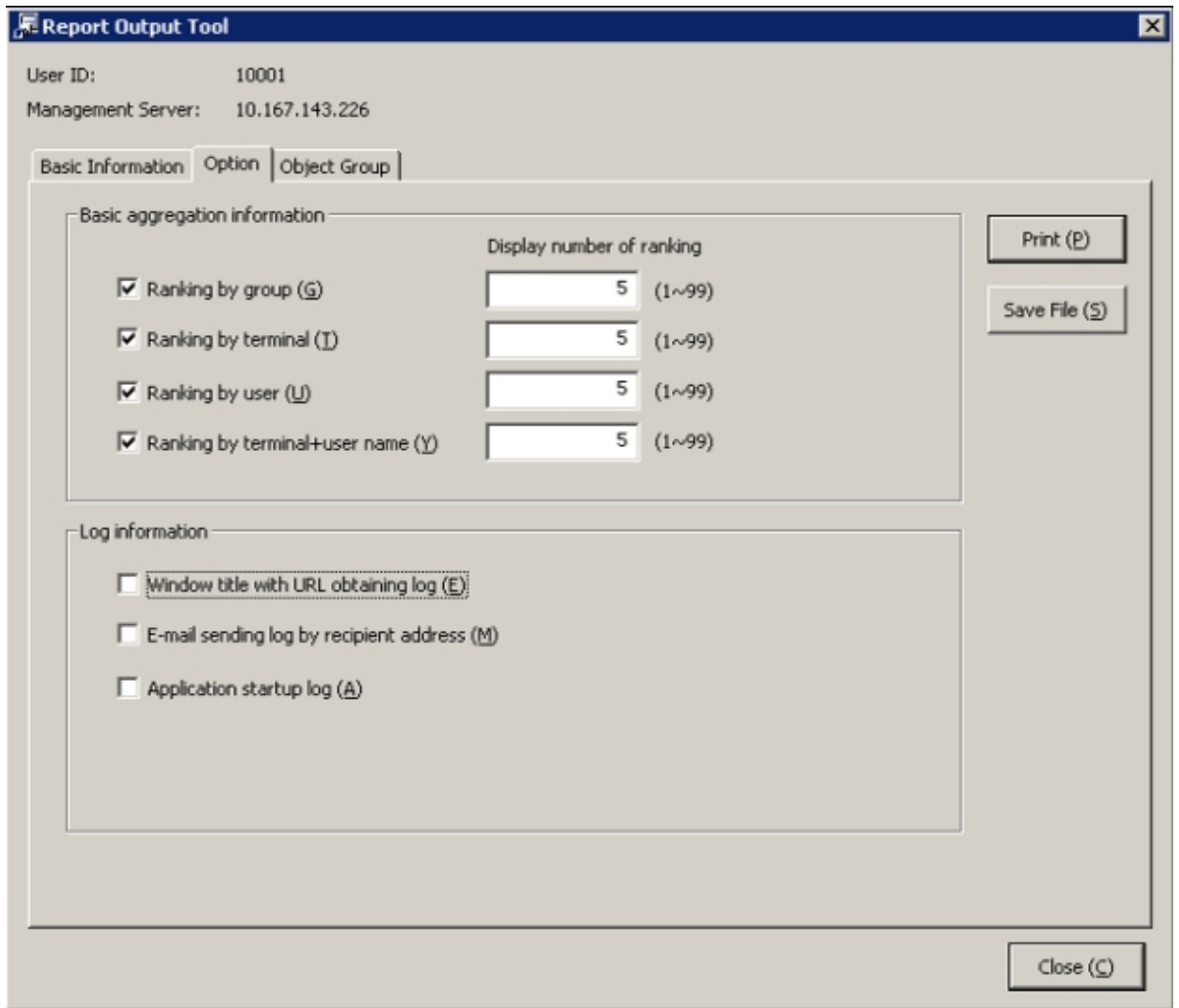
Buttons: Print (P), Save File (S), Close (C)

2. Set the items of each tab.  
The settings of each tab will be saved in Log Analyzer Server as inherent information of login user when [Print] or [Save File] is performed. The saved information will be displayed at next startup.

### Settings of [Basic Information] tab

The settings of the basic information tab can be applied to the output of the Information disclosure analysis report. Please refer to "[Settings of \[Basic Information\] tab](#)".

Settings of [Option] tab



[Basic aggregation information]

The settings of the basic aggregation information tab can be applied to the output of Information disclosure analysis report. Please refer to “[Settings of \[Option\] tab](#)”.

[Log information]

Select this when outputting the log used in the aggregation of ranking.  
Output the file that is different from the terminal usage analysis report in CSV format.

Item Name	Description
[Window title with URL obtaining log ]	Output Window title obtaining log with URL as a single file.
[E-mail sending log by recipient address]	Output log of E-mail sending log by recipient address as a single file.
[Application startup log]	Output application startup log as a single file.

Settings of [Target Group] tab

Set whether the [Target Group List] can be output to report.

The settings of this tab can be applied can be applied to the output of the Information disclosure analysis report. Please refer to “[Settings of \[Object Group\] tab](#)”.



3. Click the [Print] or [Save File] button.

### Note

#### **Please do not operate Microsoft® Excel in the process of report output**

Please do not perform the [New] and [Open] operation of Microsoft® Excel file in the report output process, as report output may not be performed normally.

In addition, please confirm whether Microsoft® Excel was started correctly before doing the report output. When Microsoft® Excel is not started correctly, problems such as the report output process taking too much time and being unable to finish will occur.

#### **[When clicking the [Print] button]**

Print the generated report and logs used for the aggregation of ranking.

In the displayed [Print] window, set the printer and print the report.

### Point

#### **The Printing Dialog Box may hide behind the Report Output Tool.**

When the Printing Dialog Box is not displayed after a long time, it may hide behind the Report Output Tool.

#### **[When clicking the [Save File] button]**

Save the generated report and logs used for the aggregation of ranking as a file.

### Note

#### **Please save the output report to a safe place.**

The output report may contain personal information and system configuration information. Please specify a folder that has been implemented sufficient security policy as the target for saving the file.

[Example]

Set the access authority of the folder to allow only the administrator to view.

In the displayed saving window, specify the destination for saving and click the [Save File] button.

Each file will be saved with the following name.

[Report File]

Default Name: Cmuse \_ [Analysis Period] \_ [Start Date of Analysis Period].xls

(When a file with same name exists, the confirmation dialog for overwriting will be displayed..)

- Analysis period
  - Daily report: daily
  - Weekly report: weekly
  - Monthly report: monthly
- Start date of analysis period: YYYYMMDD (date set in the [Analysis Date] of the [Basic Information] tab)

[CSV File of Log]

Log Type	CSV File Name
Window Title Obtaining with URL	Cmuse_Log_Webaccess_YYYYMMDD.csv
E-mail Sending Log by Recipient Address	Cmuse_Log_Mailsend_YYYYMMDD.csv

Log Type	CSV File Name
Application Startup	Cmuse_Log_AppStartup_YYYYMMDD.csv

When a file with same name exists, the number with () will be added to the end of file name.

Example: Cmuse\_Log\_Webaccess\_YYYYMMDD(2).csv

The following will be are (3) and (4), etc.

### Note

**Please confirm UNICODE character in Internet Explorer®.**

When the UNICODE characters (including JIS2004) that do not correspond to the Shift JIS font are used in the log data, they will be displayed in the HTML Escape format in a CSV file.

Please open the following HTML files using Internet Explorer®, and confirm the font of JIS2004 that contains UNICODE character.

- File location: HTML folder under the target folder for saving report file.
- File name: it has the same name as CSV file (The extension is “.html”).

The content that is same as the log data that is output to CSV file will be displayed in this HTML file.

## 6.4.2 Content of Terminal Usage Analysis Report

The structure of Terminal usage analysis report is shown as follows.

Classification	Sheet Name	Description
Summary Sheet	Summary	The summary of generated report is recorded.
Detail Sheet	Detail (Window Title Obtaining with URL)	All kinds of aggregation information (ranking information) of each operation log is recorded.
	Detail (E-mail Sending Log by Recipient Address)	
	Detail (Application Startup)	
Target Group Sheet	Target Group	The list of departments that have collected analysis target logs is recorded.

The layouts of generated report file and printing result may vary depending on the version of Microsoft® Excel and service pack being used.

The output format of the report is the same as the Information disclosure analysis report.

However, the logs as the aggregation target of ranking output to the detail sheet are Window Title Obtaining Log with URL, log of E-mail Sending Log by recipient address and application startup log.

Please refer to “[Summary sheet](#)”, “[Detail sheet](#)”, “[Target group sheet](#)” for output format.

## 6.5 Violation Analysis Report

In the violation analysis report, output the result of aggregating and analyzing the following logs collected when the operations prohibited in Systemwalker Desktop Keeper is performed knowing the violation operations according to the organization policy.

- Application startup prohibition
- Printing prohibition
- Logon prohibition
- PrintScreen key prohibition

- E-mail file attachment prohibition.

## 6.5.1 Output Violation Analysis Report

1. In the [Report Output Tool] window, select the [Violation Analysis].  
→The following window is displayed.

The screenshot shows the 'Report Output Tool' window with the following configuration:

- User ID: admin
- Management Server: 193.168.245.128
- Basic Information tab is selected.
- Report title (T): Violation Analysis Report
- Created by (N): admin
- Analysis period:
  - Daily report (D): Year 2012, Month 2, Day 4
  - Weekly report (W): Year 2012, Month 1, Day 29, In one week from this day
  - Monthly report (M): Year 2011, Month 12, Day 21, In one month from this day
- The start date of weekly report and monthly report can be modified in Web Console.
- Index value:
  - Difference value compared with the last time (B): 10 % (1~99)
  - Long-term difference (L): 5 % (1~99)
- Buttons: Print (P), Save File (S), Close (C)

2. Set the items of each tab.  
The settings of each tab will be saved in the Log Analyzer Server as inherent information of the login user when [Print] or [Save File] is performed. The saved information will be displayed at next startup.

### Settings of [Basic Information] tab

The settings of basic information tab can be applied to the output of information disclosure analysis report. Please refer to “[Settings of \[Basic Information\] tab](#)”.

Settings of [Option] tab

Report Output Tool

User ID: 10001  
Management Server: 10.167.143.226

Basic Information | **Option** | Object Group

Basic aggregation information

	Number of displayed ranking
<input checked="" type="checkbox"/> Ranking by group (G)	5 (1~99)
<input checked="" type="checkbox"/> Ranking by terminal (I)	5 (1~99)
<input checked="" type="checkbox"/> Ranking by user (U)	5 (1~99)
<input checked="" type="checkbox"/> Ranking by terminal+user name (Y)	5 (1~99)

Log information

- Application startup prohibition log (A)
- Printing prohibition log (G)
- Logon prohibition log (L)
- PrintScreen key prohibition log (K)
- E-mail attachment prohibition (M)

Print (P)  
Save File (S)  
Close (C)

[Basic aggregation information]

The settings of basic aggregation information tab can be applied to the output of information disclosure analysis report. Please refer to “[Settings of \[Option\] tab](#)”.

[Log information]

Select when outputting the logs used in aggregation of ranking

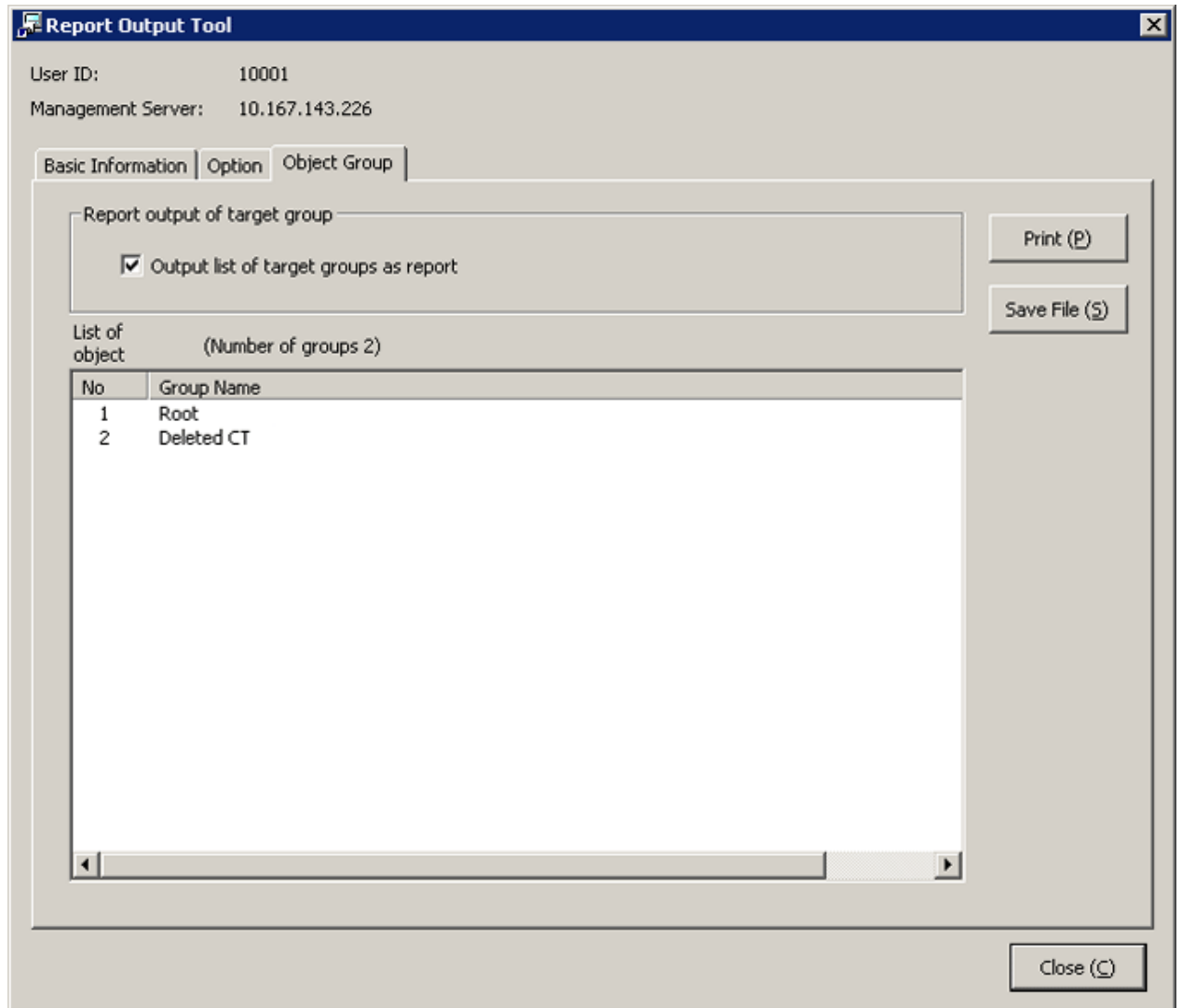
The file that is different from violation analysis report is output in CSV format.

Item Name	Description
[Application startup prohibition log]	Output application startup prohibition log as a single file.
[Printing prohibition log]	Output printing prohibition log as a single file.
[Logon prohibition log]	Output logon prohibition log as a single file.
[PrintScreen key prohibition log]	Output PrintScreen key prohibition log as a single file.
[E-mail attachment prohibition]	Output E-mail file attachment prohibition log as a single file.

### Settings of [Object Group] tab

Set whether to output [List of object] to report.

The settings of this tab can be applied to the output of the information disclosure analysis report. Please refer to “Settings of [Object Group] tab”.



3. Click the [Print] or [Save File] button.

### Note

#### Please do not operate Microsoft® Excel in the process of report output

Please do not perform the [New] and [Open] operation of Microsoft® Excel file in the report output process, as report output may not be performed normally sometimes.

In addition, please confirm whether Microsoft® Excel was started correctly before the report output. When Microsoft® Excel is not started correctly, problems such as the report output process taking too much time and being unable to finish will occur.

#### [When clicking the [Print] button]

Print the generated report and logs used for the aggregation of ranking.

In the displayed [Print] window, set the printer and print the report.



**The Printing Dialog Box may hide behind the Report Output Tool.**

When the Printing Dialog Box is not displayed after a long time, it may hide behind the Report Output Tool.

**[When clicking the [Save File] button]**

Save the generated report and logs used for the aggregation of ranking as a file.



**Please save the output report to a safe place**

The output report may contain personal information and system configuration information. Please specify a folder that has been implemented sufficient security policy as the target for saving the file.

[Example]

Set the access authority of folder to allow only the administrator to view.

In the displayed saving window, specify the destination for saving and click the [Save] button.

Each file will be saved with the following name.

[Report File]

Default name: Islegale\_\_[Analysis Period]\_[Start Date of Analysis Period].xls

(When a file with same name exists, the confirmation dialog for overwriting will be displayed.)

- Analysis period
  - Daily report: daily
  - Weekly report: weekly
  - Monthly report: monthly
- Start date of analysis period: YYYYMMDD (date set in the [Analysis Date] of [Basic Information] tab)

[CSV File of Log]

Log Type	CSV File Name
Application Startup Prohibition	Islegal_Log_AppSuppress_YYYYMMDD.csv
Printing Prohibition	Islegal_Log_PrintSuppress_YYYYMMDD.csv
Logon Prohibition	Islegal_Log_LogonSuppress_YYYYMMDD.csv
PrintScreen Key Prohibition	Islegal_Log_PSKeySuppress_YYYYMMDD.csv
E-mail File Attachment Prohibition	Islegal_Log_MailattachedSuppress_YYYYMMDD.csv

When a file with same name exists, the number with () will be added to the end of file name.

Example: Islegal\_Log\_AppSuppress\_YYYYMMDD(2).csv

The following will be are (3) and (4), etc.



**Please confirm UNICODE character in Internet Explorer®.**

When the UNICODE characters (including JIS2004) that do not correspond to the Shift JIS font are used in the log data, they will be displayed in the HTML Escape format in a CSV file.

Please open the following HTML files using Internet Explorer®, and confirm the font of JIS2004 that contains UNICODE character.

- File location: HTML folder under the target folder for saving report file.
- File name: it has the same name as CSV file (The extension is “.html”).

The content that is same as the log data that is output to a CSV file will be displayed in this HTML file.

---

## 6.5.2 Contents of Analysis Report of Violation Operation

---

The structure of the analysis report of violation operation is shown as follows.

Classification	Sheet Name	Description
Summary Sheet	Overview	The summary of generated report is recorded.
Detail Sheet	Detail (Application Startup Prohibition Log)	All kinds of aggregation information (ranking information) of each operation log is recorded.
	Detail (Printing Prohibition Log)	
	Detail (Logon Prohibition Log)	
	Detail (PrintScreen Key Prohibition Log)	
	Detail (E-mail File Attachment Prohibition Log)	
Target Group Sheet	Target Group	The list of departments that have collected analysis target logs is recorded.

The layouts of the generated report file and printing result may vary depending on the version of Microsoft® Excel and service pack being used.

The output format of the report is the same as the information disclosure analysis report.

However, the logs of the aggregation target of ranking output to the detail sheet are shown as follows:

- Application startup prohibition log
- Printing prohibition log
- Logon prohibition log
- PrintScreen key prohibition log
- E-mail file attachment prohibition log

Please refer to “[Summary sheet](#)”, “[Detail sheet](#)”, “[Target group sheet](#)” for output format.

## 6.6 Comprehensive Analysis Report

---

Comprehensive analysis report collects the diagnosis summary of Information disclosure analysis, Terminal usage analysis and violation analysis, and outputs a comprehensive diagnosis result.

## 6.6.1 Output Comprehensive Analysis Report

1. Select [Comprehensive Analysis] in the [Report Output Tool] window.  
→ The following window is displayed.

The screenshot shows the 'Report Output Tool' window with the following details:

- User ID:** admin
- Management Server:** 193.168.245.128
- Tabs:** Basic Information (selected), Option, Object Group
- Report title (T):** Comprehensive Analysis Report
- Created by (N):** admin
- Buttons:** Print (P), Save File (S)
- Analysis period:**
  - Daily report (D):** Year 2012, Month 2, Day 4
  - Weekly report (W):** Year 2012, Month 1, Day 29, In one week from this day
  - Monthly report (M):** Year 2011, Month 12, Day 21, In one month from this day

The start date of weekly report and monthly report can be modified in Web Console.
- Index value:**
  - Difference value compared with the last time (B):** 10 % (1~99)
  - Long-term difference (L):** 5 % (1~99)
- Close (C)** button at the bottom right.

2. Set the items in each tab.  
The settings of each tab will be saved in Log Analyzer Server as inherent information of login user when [Print] or [Save File] is performed. The saved information will be displayed at next startup.

### Settings of the [Basic Information] tab

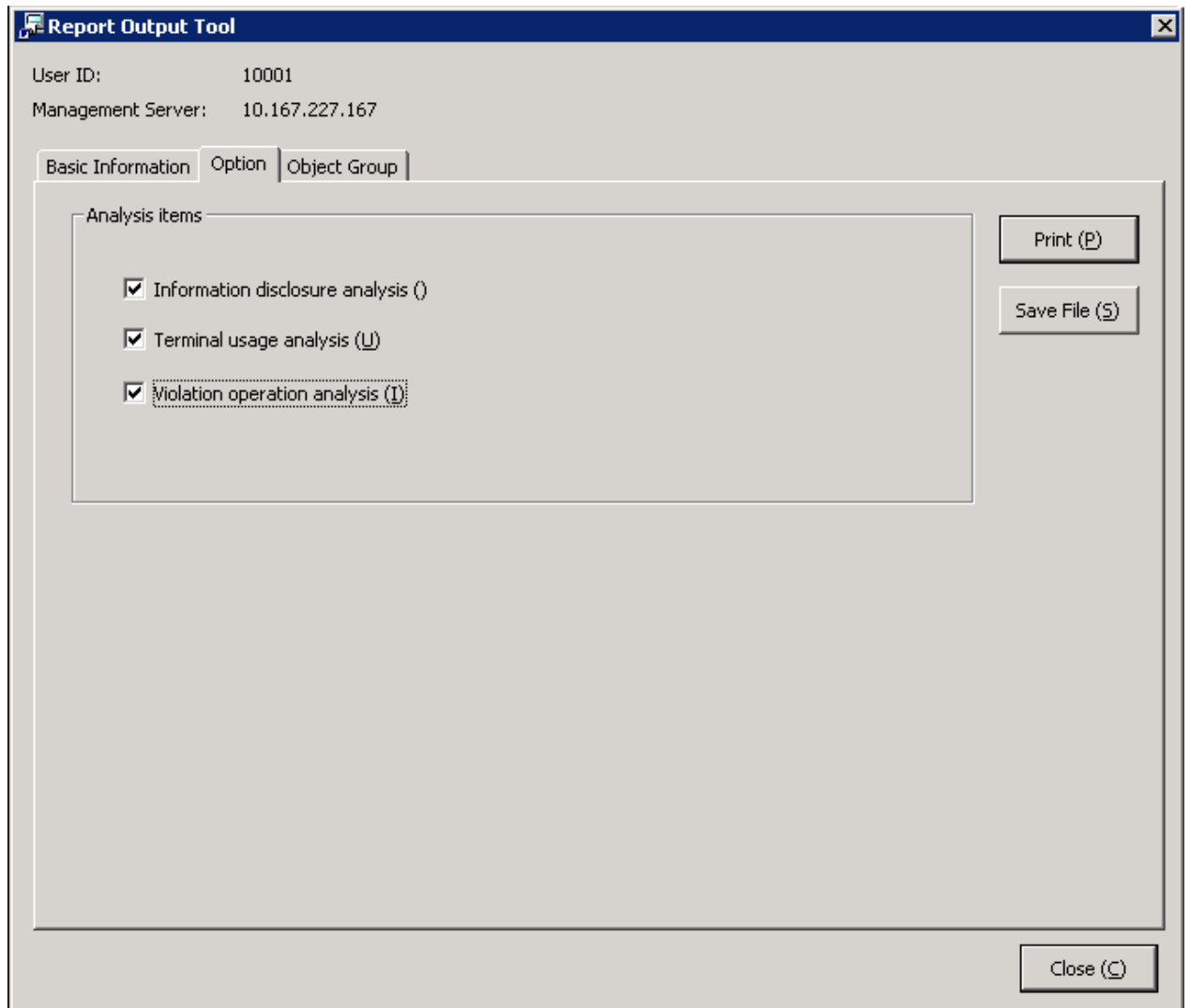
The settings of the basic information tab can be applied to the output of the information disclosure analysis report. Please refer to “[Settings of \[Basic Information\] tab](#)”.

### Settings of the [Option] tab

Select analysis items.

Please select more than one item (all items are selected in default).

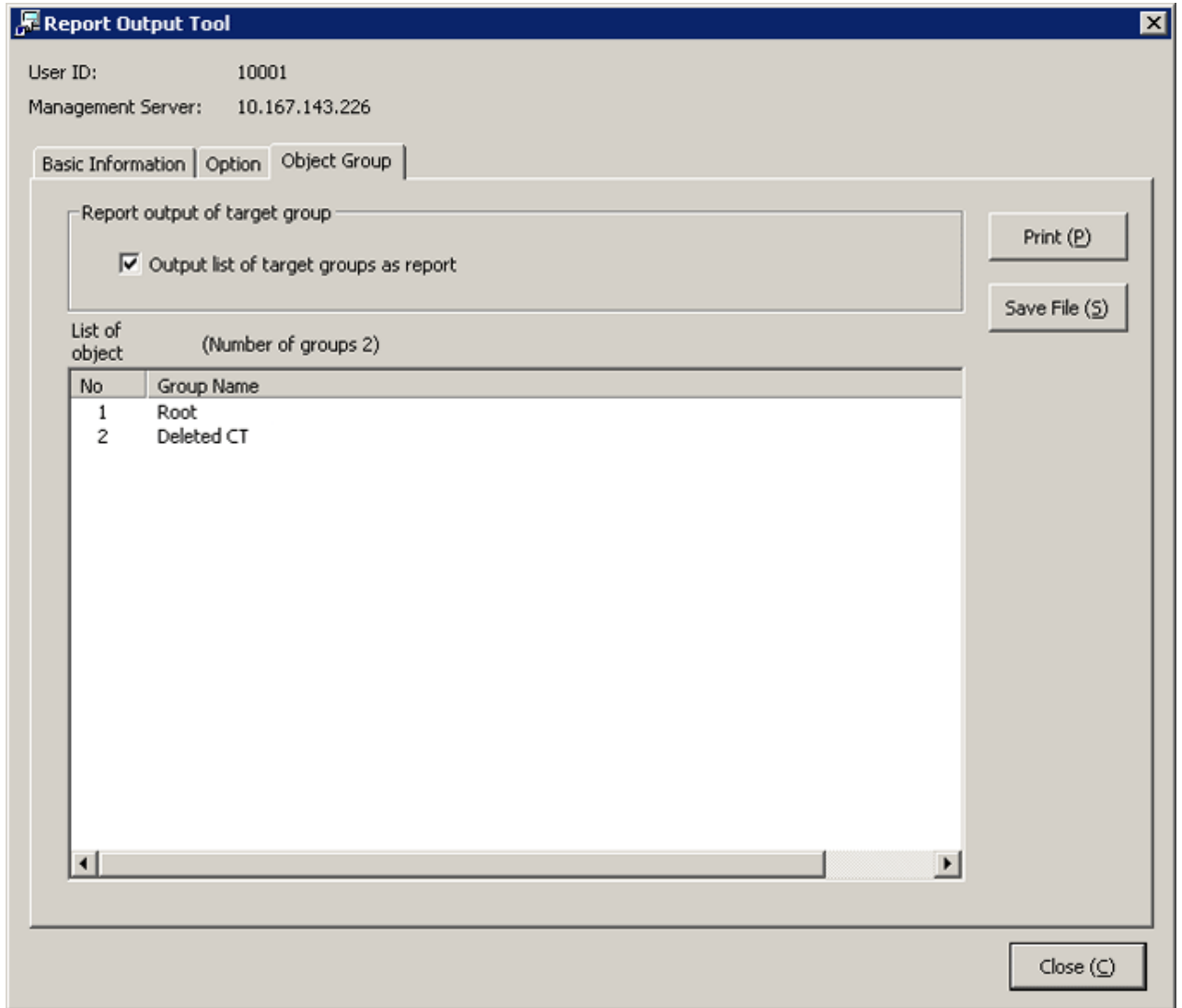




#### Settings of the [Object Group] tab

Set whether to output [List of object] to report.

The settings of this tab can be applied to the output of Information disclosure analysis report. Please refer to "[Settings of \[Object Group\] tab](#)".



3. Click the [Print] or [Save File] button.

### Note

#### **Please do not operate Microsoft® Excel in the process of report output**

Please do not perform the [New] and [Open] operation of Microsoft® Excel file during the report output process, as the report output may not be performed normally.

In addition, please confirm whether Microsoft® Excel was started correctly before the report output. When Microsoft® Excel is not started correctly, problems such as the report output process taking too much time and being unable to finish will occur.

#### **[When clicking the [Print] button]**

Print the generated report.

In the displayed [Print] window, set the printer and print the report.

### Point

#### **The Printing Dialog Box may hide behind the Report Output Tool.**

If the Printing Dialog Box has not displayed after a long time, it may be hidden behind the Report Output Tool.

[When clicking the [Save File] button]

Save the generated report as a file.



---

**Please save the output report to a safe place**

The output report may contain personal information and system configuration information. Please specify a folder that has been implemented sufficient security policy as the target for saving the file.

[Example]

Set the access authority of the folder to allow only the administrator to view.

---

In the displayed saving window, specify the destination for saving and click the [Save] button.

Each file will be saved with the following name.

Default name: Summary\_[Analysis Period]\_[Start date during analysis period].xls

(When a file with same name exists, the confirmation dialog for overwriting will be displayed.)

- Analysis time
  - Daily report: daily
  - Weekly report: weekly
  - Monthly report: monthly
- Start date of analysis time: YYYYMMDD (date set in [Analysis Period] of the [Basic Information] tab)

## 6.6.2 Content of Comprehensive Analysis Report

---

The structure of comprehensive analysis report is as follows:

The layouts of the generated report file and printing result may vary depending on the version of Microsoft® Excel and service pack being used.

# Comprehensive diagnosis sheet

Microsoft Excel - Comprehensive Analysis ReportLads

File Edit View Insert Format Tools Data Window Help

Type a question for help

B166

Comprehensive Analysis Report

(2) Object Managed Object/View object group sheet

(3) Number of object PCs 818Sets

(4) Created by admin

(5) Created on 2/8/2012

(6) Analysis period 2012/01/29~2012/02/04

(7)

(8) [Information Disclosure Prevention]

Index Value 0.4 %

Number of all items 6,337

Number of safe items 6,229

Number of dangerous item 28

No.	Group name	file export	file operation	printed	SendEmailby	summary
1	Planning Dept.	9	9	21	9	21
2	Development Dept.	9	9	6	9	6
3	Management Dept.	9	9	5	9	5
4	*****	*****	*****	*****	*****	*****
5	*****	*****	*****	*****	*****	*****

(9) [Terminal Usage Status]

Index Value 100.0 %

Number of all items 298,793

Number of safe items 91,049

Number of dangerous item 267,744

No.	Group name	file export	file operation	printed	SendEmailby
1	Planning Dept.	11,256	150	20,549	31,955
2	Development Dept.	5,276	196	24,646	30,119
3	Management Dept.	5,042	19	11,675	16,736
4	Finance Dept.	2,124	26	21,004	23,154
5	Business Dept.	5,955	19	11,618	17,532

(10) [Violation Status]

Index Value 0.1 %

Number of all items 363,226

Number of safe items 363,130

Number of dangerous item 70

No.	Group name	file export	file operation	printed	SendEmailby	summary
1	Planning Dept.	9	9	9	9	46
2	*****	*****	*****	*****	*****	*****
3	*****	*****	*****	*****	*****	*****
4	*****	*****	*****	*****	*****	*****
5	*****	*****	*****	*****	*****	*****

(11) [Diagnosis Comment]

[Information disclosure analysis]  
No change comparing with the last time.No change in the long run.

[Terminal usage analysis]  
No change comparing with the last time.No change in the long run.

[Violation analysis]  
No change comparing with the last time.No change in the long run.

Comprehensive diagnosis / Object group /

Ready

(1) Report Title

The title specified in basic information settings is recorded.

(2) Object

Display the managed target. It is always displayed as “Managed Object”.

(3) Number of object PCs

Display the number of all PCs of the managed target.

- If target PC does not exist, 0 will be displayed.

(4) Created by

The creator name specified in basic information settings is recorded.

(5) Created on

The data on which report output is performed is recorded.

(6) Analysis period

The analysis period specified in basic information settings is recorded.

(7) Approval column

This is the approval column when used as a report (the number of columns cannot be modified).

(8) Information Disclosure Prevention

The main content of the Information disclosure analysis result is recorded.

(9) Terminal Usage Status

The main content of the Terminal usage analysis result is recorded.

(10) Violation Status

The main content of the violation analysis result is recorded.

(11) Diagnosis Comment

Record the following content for each analysis item in the diagnosis comment of the “Comprehensive analysis” report.

- Inspection of comparison with the last time

Through the difference value of the index value obtained by comparing the result with the previous diagnosis, information on whether the danger level has increased or decreased can be obtained. Based on this, comment about risk judgment can be proposed for the index value of this analysis result.

- Long-term tendency

According to the increased or decreased index value compared to the past, comment about risk judgment can be proposed for the index value predicted based on the variation of the index value from the past analysis result.

※) The content described in each analysis result is an abstract of the Summary Sheet (in general format) of each analysis report. For item description, please refer to “[Summary sheet](#)”.

## Target Group Sheet

The department information that has been analyzed will be output.

(1) Object Group	
(2)	(3)
No	Group name
1	Root Directory
2	Operation Dept.
3	Operation Dept./Operation Div. 1
4	Operation Dept./Operation Div. 2
5	Development Dept.
6	Planning Dept.
7	Management Dept.
8	Finance Dept.
9	Product Evaluation Dept.
10	Business Dept.

(1) Report Title

It is described as “Object Group”.

(2) Target group list

The department of analysis target is recorded.

The group name can be recorded with the full path beginning from the root.

[Example] Development Department/ Development Unit 3

When multiple managed departments exist, they can be displayed after adding rows.

Up to 50,000 departments can be recorded.

Up to 512 bytes can be displayed in the content of each item in target group.

## 6.7 Printing Volume Auditing Report

A printing volume auditing report is used to evaluate CO2 emission and printing cost reduction given print volume, and it also outputs the result of aggregating and analyzing in the following log:

- Printing operation log

## 6.7.1 Output Printing Volume Auditing Report

1. Select [Printing Volume Auditing] in the [Report Output Tool] window.  
→ The following window is displayed.

The screenshot shows a software window titled "Report Output Tool". At the top, it displays "User ID: 10001" and "Management Server: 10.167.143.226". Below this are three tabs: "Basic Information", "Option", and "Object Group". The "Basic Information" tab is selected and contains the following fields and controls:

- "Report title (T)": A text box containing "Printing Volume Auditing Report".
- "Created by (N)": A text box containing "admin".
- "Monitoring period": A section containing a "Year" dropdown menu set to "2012", a "Month" dropdown menu set to "1", and the text "In one month starting from the first day".

On the right side of the window, there are three buttons: "Print (P)", "Save File (S)", and "Close (C)".

- User ID: The login user ID.
  - Management Server: IP address of the Management Server for saving logs of report output.
2. Set items of each tab.  
The settings of each tab will be saved in the Log Analyzer Server as inherent information of the login user when [Print] or [Save File] is performed. The saved information will be displayed during the next startup.

### Settings of the [Basic Information] tab

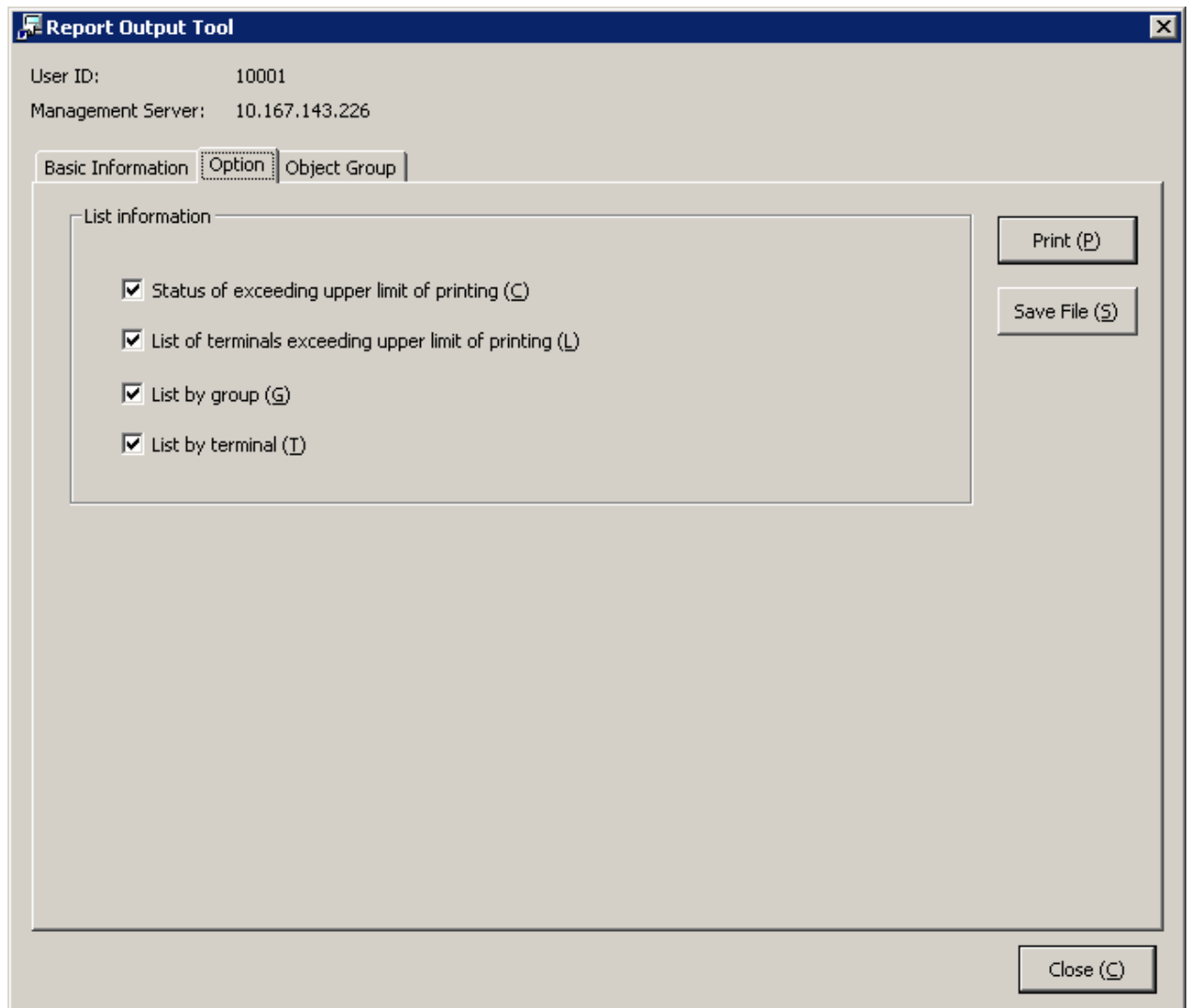
Set the following items.

Input Item	Content
[Report title]	Specify the title of the report to be output. Up to 64 bytes of single-byte alphanumeric characters, single-byte symbols and double-byte 2 byte characters can be set. Initial value: "Printing Volume Auditing report".
[Created by]	Specify the creator of report. Up to 40 bytes of single-byte alphanumeric characters, single-byte symbols and

Input Item	Content
	double-byte 2 byte characters can be set. Initial value: The user ID that logs in.
[Monitoring period]	Set the auditing time of the report to be output. The auditing period can be selected from January, 2005 to the latest month and year in which the report is finished.

#### Settings of the [Option] tab

Set the following items.



[List information]

Select the items to be output to report.

Item Name	Description
[Status of exceeding upper limit of printing]	This is selected when outputting the report of the status of the upper limit of printing in the auditing month. Initial value: Selected.
[List of terminals exceeding upper limit of printing]	This is selected when outputting the list of terminals that exceeded upper limit of printing in the auditing month. The initial value: Selected.
[List by group]	This is selected when outputting print volume by group in the auditing month. Initial value: Not selected.



Item Name	Description
[List by terminal]	This is selected when outputting print volume by terminal in the auditing month. Initial value: Not selected.

Settings of the [Object Group] tab

Set the following items.

The screenshot shows the 'Report Output Tool' window with the 'Object Group' tab selected. The window displays the following information:

- User ID: 10001
- Management Server: 10.167.143.226
- Navigation tabs: Basic Information, Option, **Object Group**
- Section: Report output of target group
  - Output list of target groups as report
- Buttons: Print (P), Save File (S)
- Section: List of object (Number of groups 2)
 

No	Group Name
1	Root
2	Deleted CT
- Button: Close (C)

Item Name	Description
[Report output of target group] [Output list of target groups as report ]	<ul style="list-style-type: none"> <li>- When selected: [Target group list] will be output to report.</li> <li>- When not selected (initial value): [Target group list] will not be output to report.</li> </ul>
[List of object]	<p>Group as log analysis target will be output to report. Group names are separated by “/” and displayed with the full path starting from the root. [Example] Development Department/Development Unit 3</p> <p>The total number of groups is displayed next to the title. Up to 50,000 groups can be displayed.</p>

3. Click the [Print] or [Save File] button.

### Note

#### **Please do not operate Microsoft® Excel in the process of report output**

Please do not perform the [New] and [Open] operation of the Microsoft® Excel file in the report output process, as report output may not be performed normally.

In addition, please confirm whether Microsoft® Excel was started correctly before the report output. When Microsoft® Excel is not started correctly, problems such as the report output process taking too much time and being unable to finish will occur.

#### **[When clicking the [Print] button]**

Print the generated report.

In the displayed [Print] window, set the printer and print the report.

### Point

#### **The Printing Dialog Box may hide behind the Report Output Tool.**

If the Printing Dialog Box has not displayed after a long time, it may be hidden behind the Report Output Tool.

#### **[When clicking the [Save File] button]**

Save the generated report as a file.

### Note

#### **Please save the output report to a safe place**

The output report may contain personal information and system configuration information. Please specify a folder that has been implemented sufficient security policy as the target for saving the file.

[Example]

Set the access authority of folder to allow only the administrator to view.

In the displayed saving window, specify the destination for saving and click the [Save] button.

The file will be saved with the following name.

Default name: Ecoprint\_monthly\_YYYYMMDD.xls (weekly report)

(When a file with same name exists, the confirmation dialog for overwriting will be displayed.)

- Start date of report: YYYYMMDD (date set in [Auditing Period] of the [Basic Information] tab)

## 6.7.2 Content of Printing Volume Auditing Report

The output content of printing volume auditing report is as follows.

Classification	Sheet Name	Description
Summary Sheet	Summary	Output according to printing paper cost and CO2 emission for the auditing month.
Detailed Sheet	Status of Exceeding Upper Limit of Printing	Output the status of exceeding the upper limit of printing for the auditing month.

Classification	Sheet Name	Description
	List of Exceeded Terminals	Display the list of terminals that exceeded upper limit of printing of the auditing month.
	List by Group	Output print volume for the auditing month by group.
	List by Terminal	Output print volume for the auditing month by terminal.
Target Group Sheet	Target Group	Output the information of report auditing target group.

The layouts of the generated report file and printing result may vary depending on the version of Microsoft® Excel and service pack being used.

For numeric values output to the report, round to the displayed decimal unless stated particularly. In addition, when there is no data, 0 is displayed.

For the problem that the concept of year is included in the value output to report, data after the auditing month will not be contained in the aggregation value. Besides, it will not be displayed in the report.

For “Year (start date)”, “Printing cost of each page” and “CO2 emission of each page” described in the report, “Setting of Start month of Year”, “Cost of each page (or each piece of paper)” and “CO2 emission of each page (or each piece of paper)” of [Eco Auditing Settings] in Operation Settings of Log Analyzer of each Web Console. Please modify the settings in Web Console to modify these values. For details, please refer to [“2.7.2.2.4 Set Other Conditions”](#).

# Summary Sheet: Summary

Microsoft Excel - Printing Volume Auditing Report.xls

(1) Printing Volume Auditing Report

(2) Object	Managed Object.*View object group sheet		
(3) Number of object PCs	24 Set(s)		
(4) Created by	admin		(7)
(5) Created on	2012/02/08		
(6) Monitoring period	2012/01/01-2012/01/31		

(8) (Estimate value of printing paper cost and reduction effect) (Reference information of print volume)

	Estimate value of current month	Annual Total(*)	2012/01/	2011/12/
Cost of printing paper	8Yen	52Yen	13551.00Piece(s)	13680.00Piece(s)
	Compared to last month	Compared to last year (*)	Average print volume of each printer	64.43Piece(s)
Increase or decrease amount of printing paper cost	-70Yen	-22,506Yen	Number of object PCs	24Set(s)
Increase or decrease amount of CO2	-0.6kg	-198.6kg	Number of PCs exceeding upper limit of printing	3Set(s)
			Change rate of print volume compared to last month	-0.8%

(\*)

(9) [Variable of print volume in This Year] (pages)

(11) [Compared to last year] (Unit: Hundred Pages)

(12) [Worst Ranking] (Unit: Page)

Order	Group name	average print volume per The last month	This month
1	Development Dept.	185.9	1345.6
2	Planning Dept.	426.7	674.3
3	Product Evaluation Dept.	442.5	423.5
4	Management Dept.	267.8	467.3
5	Business Dept.	478.9	432.1

(13) Comment

(1) Report Title

Title of report specified in the Report Output Tool is displayed.

(2) Object

The managed target is displayed. It is always displayed as “Managed Target”.

(3) Number of Object PCs

Display the number of all PCs of managed target.

(4) Created by

The name of creator specified in the Report Output Tool is displayed.

(5) Created on

The date on which the report is output is displayed.

(6) Monitoring period

The auditing period specified in the Report Output Tool is displayed.

(7) Stamping column

This is an area for stamping the created file. It must be output.

(8) Estimate value of printing paper cost and reduction effect

Increase and decrease of printing paper cost obtained by comparing the estimated value of accumulated printing paper cost and CO2 emissions in this month and year to that in last month and year is displayed.

- Method of calculating estimated value of printing paper cost in this month  
printing paper cost= print pages × printing cost of 1 page
- Method of calculating estimated value of CO2 emissions in this month  
CO2 emissions= print pages × CO2 emissions of 1 page
- Method of calculating estimated value of annually accumulated printing paper cost  
printing paper cost= total printing pages from start month to the auditing month of this year × printing cost of 1 page
- Method of calculating estimated value of annually accumulated CO2 emission  
CO2 emission= total printing pages from annually start month to the auditing month in this year × CO2 emission of 1 page
- In the “(※) Accumulation period”, the period corresponding to the auditing period is displayed.
- When comparing with the last month, calculate as follows. When the numerical value of comparison with the last month is negative, it is judged as improvement trend.  
  
Increase or decrease of printing paper cost= printing paper cost of this month- printing paper cost of last month  
Increase or decrease of CO2= CO2 emissions of this month- CO2 emissions of last month
- When comparing with the last year, calculate as follows. When the numerical value of comparison with the last year is negative, it is judged as improvement trend.  
  
Increase or decrease of printing paper cost = accumulated printing paper cost of this year (※) - accumulated print paper cost of last year (※)  
  
Increase or decrease of CO2= accumulated CO2 emissions of this year (※) - accumulated CO2 emissions of last year (※)  
  
※ Target: From target start month of the year to the auditing month

About “Print cost of 1 page”, “CO2 emissions of 1 page” and “Start month of Year”, please confirm “[2.7.2.2.4 Set Other Conditions](#)”.

(9) Variation of print volume in This Year

Variation of the print volume (pages) in this year and number of PCs (number of all PCs, number of PCs that exceed the upper limit of printing) will be output in graphs.

- If the print volume data of last year is contained in print volume, they will be displayed together.
- The vertical and horizontal lines are fixed as years (from the start month to end month of a year).

(10) Reference information of print volume

For the following data, information of both this month and the last month is displayed.

- Print volume
- Average print volume of each PC

- Number of PCs
- Number of PCs that exceed the upper limit of printing  
Number of PCs that exceed the upper limit of printing is the number of “PCs in which the total printing pages of this month exceed the upper limit of printing of this month”.  
The method of calculating the upper limit of printing varies depending on the settings in “Printing Monitoring Operation Settings”.  
The calculation method is as follows.  
(The value of upper limit of printing abandons digits after the decimal point.)

- Terminals in which the “Aggregation Unit of Printed Pages” is “Daily”  
Upper limit of printing = (terminal reference value) × number of days in this month (days)
- Terminals in which “Aggregation Unit of Printed Pages” is “Weekly”  
Upper limit of printing = (terminal reference value ÷ 7) × number of days in this month (days)
- Terminals in which “Aggregation Unit of Printed Pages” is “Monthly”  
Upper limit of printing = (terminal reference value)

Method of calculating terminal reference value:

- As [Operation when the set number of printed pages is reached], only the terminals with “Warning” are selected.  
Terminal reference value= Set number of pages for “Warning”
- As [Operation when the set number of printed pages is reached], terminals with “Warning” and “Printing prohibition” are selected.  
Terminal reference value= set pages for “print prohibition”
- Increase or decrease rate of print volume compared to the last month (if the value is negative, it is judged as improvement trend.)
- Increase or decrease rate of print volume compared to the last month refers to the value by which the print volume of this month can be reduced compared to that of the last month. It is calculated with following method.  
Increase or decrease rate= (print volume of this month- print volume of last month) ÷ (print volume of last month) × 100
- When the print volume of the last month is 0, the increase or decrease rate will not be calculated, and a hyphen (-) will be displayed.

(11) Compared to last year

The print volume and predicted value of this year and last year are shown in the graph.

- The predicted value is the value obtained by multiplying the monthly average value of print volume by number of the remaining number of months.

(12) Worst Ranking

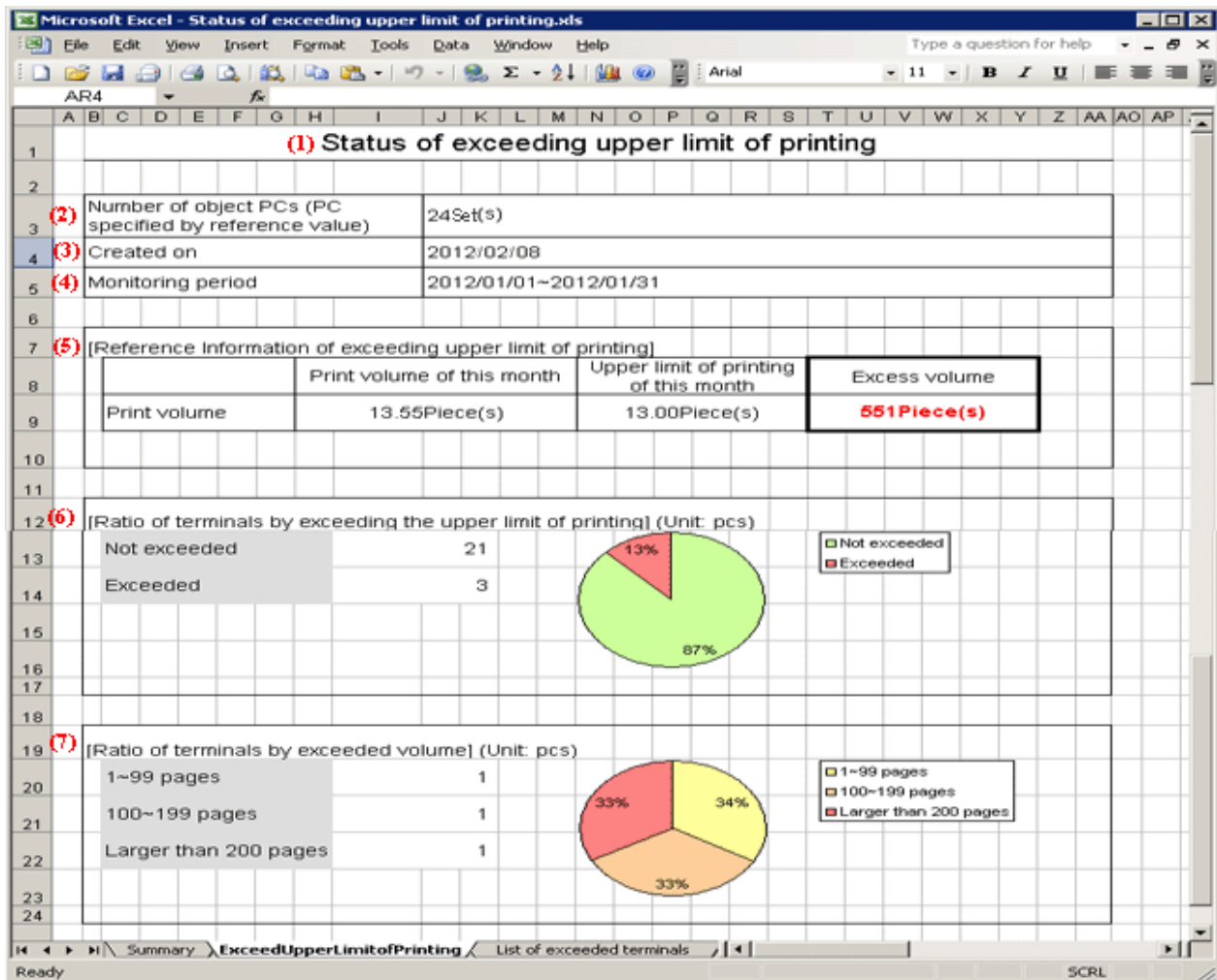
Display the print volume in ranking from the group with larger print volume on one PC in this month. It is also displayed in the graph.

- If the data of last month exists, they will be displayed together.
- Up to 5 groups can be displayed (even if the same ranking exists, no more than 6 groups will be displayed).
- When there are less than 5 groups, a hyphen (-) will be displayed in the blank.

(13) Comment

This is a free comment column for users.

## Detail Sheet: Status of Exceeding Upper Limit of Printing



### (1) Report Title

“Status of exceeding upper limit of printing” is displayed.

### (2) Number of object PCs (PC specified by reference value)

Display the number of PCs that are targets of this sheet and the “Printing Monitoring Operation Settings” is ON.

### (3) Created on

The date on which the report is output is displayed.

### (4) Monitoring period

The auditing period specified in Report Output Tool is displayed.

### (5) Reference information of exceeding upper limit of printing

The print volume, upper limit of printing of this month and excess volume are displayed.

- When the print volume of this month does not exceed the upper limit of printing, 0 is displayed in excess volume.
- When the excess volume is larger than 1, it is displayed in red bold type.
- Only those PCs with “Warning” or “Print prohibition” selected in printing monitoring operation settings will become targets for aggregation.  
For printing monitoring operation settings, please refer to “2.4.1.11 Settings of [Eco monitoring settings] Tab”.

### (6) Ratio of terminals by exceeding the upper limit of printing

The terminals are displayed in two modes: “not exceeded” and “exceeded”, and the scale is displayed in the chart.

- Only the PCs with printing monitoring operation settings set to “ON” will be targets for aggregation.

(7) Ratio of terminals by exceeded volume

The exceeded terminals are displayed in three modes: “1~reference 1-1”, “reference 1~ reference 2-1” and “reference 2 and above” and the proportion is displayed in graph.

- “Reference 1” and “Reference 2” are correspondent to the values of “Auditing Judgment Reference 1” and “Auditing Judgment Reference 2” respectively set in the [Operation Settings] window of Log Analyzer.
- Only the PCs with printing monitoring operation settings being set “ON” will be targets for aggregation.

### Detail Sheet: List of Exceeded Terminals

(2) ▲	(3) No.	(4) Group name	(5) Computer name	(6) Print volume of this month (pages)	(7) Upper limit of printing of this month (pages)	(8) Excess volume (pages)	(9) Standard of print volume after this month (pages)		
							Daily	Weekly	Monthly
▲	1	Operation Dept./Operation Div. 1	CT005(Tom)	2,345	1,000	<b>1,345</b>	27	186	808
△	2	Development Dept.	CT010(Lindar)	1195	1000	<b>195</b>	32	224	972
	3	Development Dept.	CT011(Green)	595	500	<b>95</b>	16	112	486

(1) Report title

“Print volume Monitor Report [List of terminals exceeding the upper limit of printing]” is displayed.

(2) [▲] or [△]

It indicates the exceeding status of terminals.

▲: indicates terminals on which the printed pages exceed “Reference 2” pages.

△: indicates terminals on which the printed pages exceed “Reference 1” to “Reference 2” -1 pages.

- “Reference 1” and “Reference 2” are correspondent to the values of “Auditing Judgment Reference 1” and “Auditing Judgment Reference 2” respectively set in the [Operation Settings] window of Log Analyzer.

(3) No.

This is the No.

(4) Group name

This is the group name.

(5) Computer name

Computer name is displayed.

When computer name is different from the name, it is displayed in the format of the computer name (name).

(6) Print volume of this month

This is the print volume of this month.

(7) Upper limit of printing of this month

It is the upper limit of printing of this month

(8) Excess volume

It is the excess volume. Take this value as a key to rank in descending order. It is displayed in red bold type.

(9) Standard of print volume after this month



It is the print volume that must be complied with in following months when correspondent terminal complies with the upper limit of printing of this month in year unit. It is displayed in three modes including monthly, weekly and daily.

For the report of the last month of a year .etc, when the remaining days or remaining months of the year is 0, no calculation will be performed, and a hyphen (-) will be displayed.

- Figure out each value with the following formulas respectively.

$$\text{Daily} = (\text{upper limit of printing of this month} \times (\text{number of the remaining months of this year} + 1) - \text{print volume of this month}) \div (\text{number of the remaining days of this year})$$

$$\text{Weekly} = (\text{upper limit of printing of this month} \times (\text{number of the remaining months} + 1) - \text{print volume of this month}) \div (\text{number of the remaining days of this year}) \times 7$$

$$\text{Monthly} = (\text{upper limit of printing of this month} \times (\text{number of the remaining months} + 1) - \text{print volume of this month}) \div (\text{number of the remaining days of this year})$$

※ The digits after the decimal point will be abandoned.

For terminals on which the print volume significantly exceeds upper limit of printing of this month and are therefore unable to comply with the upper limit of printing of this year, the value will be displayed as negative.

### Detail Sheet: List by Group

(2) No.	(3) Group name	(4) Number of terminals of this month (sets)	(5) Print volume of this month (pages)	(6) The average print volume (pages) per set of this month	(7) Number of reference value settings terminals of this month (sets)	(8) Print volume of reference value settings terminals of this month (sets)	(9) Upper limit of printing of this month (pages)
1	Floor Directory	1	244	244.0	1	244	500
2	Operation Dept.	2	324	162.0	3	1,234	1,500
3	Operation Dept./Operation Div. 1	3	3,245	1,081.7	3	3,245	2,000
4	Operation Dept./Operation Div. 2	2	956	478.0	8	667	1,000
5	Development Dept.	2	3,245	1,622.5	2	3,245	3,000
6	Planning Dept.	5	900	180.0	5	790	1,000
7	Management Dept.	2	902	451.0	2	902	1,000
8	Finance Dept.	2	838	419.0	2	890	1,000
9	Product Evaluation Dept.	2	834	417.0	2	834	1,000
10	Business Dept.	2	554	277.0	2	504	1,000

(1) Report title

“Print volume Monitor Report [By Group List]” is displayed.

(2) No.

This is the No.

(3) Group name

This is the group name. This item is taken as the key for sorting and displaying group names.

(4) Number of terminals of this month

Number of terminals in this month is displayed.

(5) Print volume of this month

Print volume of this month is displayed.

(6) The average print volume per set of this month

Average print volume of one terminal in this month is displayed.

(7) Number of reference value settings terminals of this month

Display the number of terminal in which the printing monitoring operation settings are “ON” among the number of terminals in this month.

(8) Print volume of reference value settings terminals of this month

Display the print volume when print monitoring operation settings are “ON” in the displayed print volume of this month.

(9) Upper limit of printing of this month

This is the upper limit of printing for the terminal in which the printing monitoring operation settings of this month are set to “ON”.

- The groups that belong to the terminal in which all the printing monitoring operation settings are “OFF” are displayed as (-).

### Detail Sheet: List by Terminal

(1) Print volume Monitor Report [By Terminal List]				
(2) No.	(3) Group name	(4) Computer name	(5) Print volume of this month (pages)	(6) Upper limit of printing of this month (pages)
1	Root Directory	CT00(Tom)	344	500
2	Operation Dept.	CT002(Polcg)	496	500
3	Operation Dept.	CT003(Jam)	386	500
4	Operation Dept.	CT004(Jan)	443	500
5	Operation Dept./Operation Div. 1	CT005(Ping)	2345	1000
6	Operation Dept./Operation Div. 1	CT006(Jame)	450	500
7	Operation Dept./Operation Div. 1	CT007(Kobe)	450	500
8	Operation Dept./Operation Div. 2	CT008(Jm)	434	500
9	Operation Dept./Operation Div. 2	CT009(Ling)	300	500
10	Development Dept.	CT010(Yan)	1195	500
11	Development Dept.	CT011(Aneq)	596	1000
12	Development Dept.	CT012(Bob)	485	500
13	Development Dept.	CT013(Temng)	485	500
14	Development Dept.	CT014(Green)	480	500
15	Planning Dept.	CT015(Jame)	490	500
16	Planning Dept.	CT016(Maj)	484	500
17	Management Dept.	CT017(Frag)	400	500
18	Management Dept.	CT018(Sokg)	430	500
19	Finance Dept.	CT019(Bwly)	435	500
20	Finance Dept.	CT020(Dary)	400	500
21	Product Evaluation Dept.	CT021(Angl)	455	500
22	Product Evaluation Dept.	CT022(An)	439	500
23	Business Dept.	CT023(Tomng)	450	500
24	Business Dept.	CT024(Kei)	436	500

(1) Report title

“Print volume Monitor Report [By Terminal List]” is displayed.

(2) No.

This is the No.

(3) Group name

This is the group name. This item is given first priority for sorting and displaying group names.

(4) Computer name

Computer name and user name are displayed. This item is given second priority for sorting and displaying the list.

(5) Print volume of this month

Display the print volume of this month.

(6) Upper limit of printing of this month

This refers to the upper limit of printing for the month.

※ Terminals in which the printing monitoring operation settings are “OFF” are displayed as (-).

## Target Group Sheet: Target Group

Microsoft Excel - Status of exceeding upper limit of printing.xls

Created on: 2012/02/08

(1) Print volume Monitor Report [Object Group]

(2) No.

(3) Group name

No.	Group name
1	Root Directory
2	Operation Dept.
3	Operation Dept./Operation Div. 1
4	Operation Dept./Operation Div. 2
5	Development Dept.
6	Planning Dept.
7	Management Dept.
8	Finance Dept.
9	Product Evaluation Dept.
10	Business Dept.

(1) Report title

“Print volume Monitor Report [Object Group]” is displayed.

(2) No.

This is the No.

(3) Group name

This is the group name of the target group. This item is taken as the key for sorting and displaying group names.

## 6.8 Set Report Output Schedule

By setting batch commands for the report output in Task Scheduler, automatic report output can be executed regularly.

However, batch commands for report output cannot be used simultaneously. Please do not register the batch file that uses batch commands or batch commands more than once in Task Schedule.



### Note

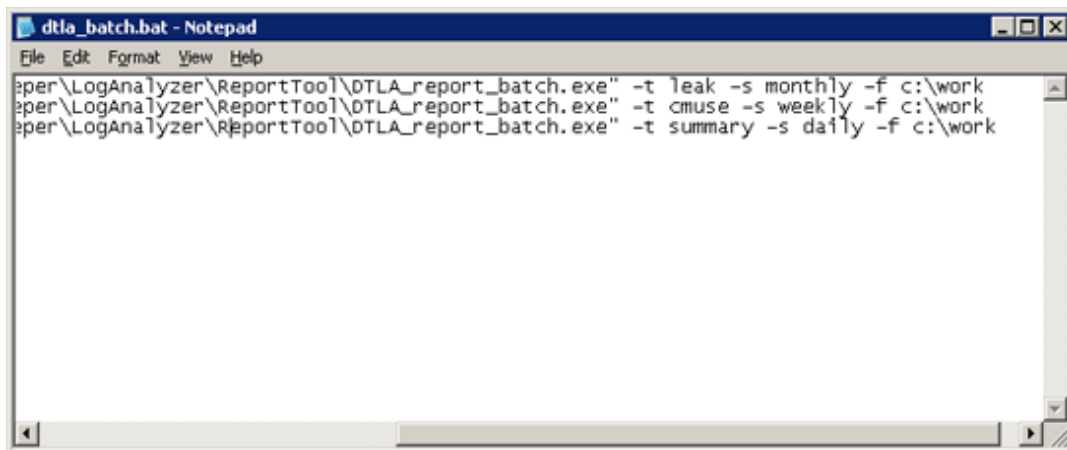
#### In Windows Vista®, Windows Server® 2008 and Windows® 7

In the environment of Windows Vista®, Windows Server® 2008 and Windows® 7, when operating in the command prompt, please open the command prompt through [Execute as Administrator].

The procedure is as follows:

1. Record report output commands in batch file according to the output report.  
For details of report output commands, please refer to “DTLA\_REPORT\_BATCH.EXE (report output)” in “Systemwalker Desktop Keeper Reference Manual”.
  - Please specify command name or output target folder with full path.
  - When space is contained in the path, please enclose it with “ (double quotes).

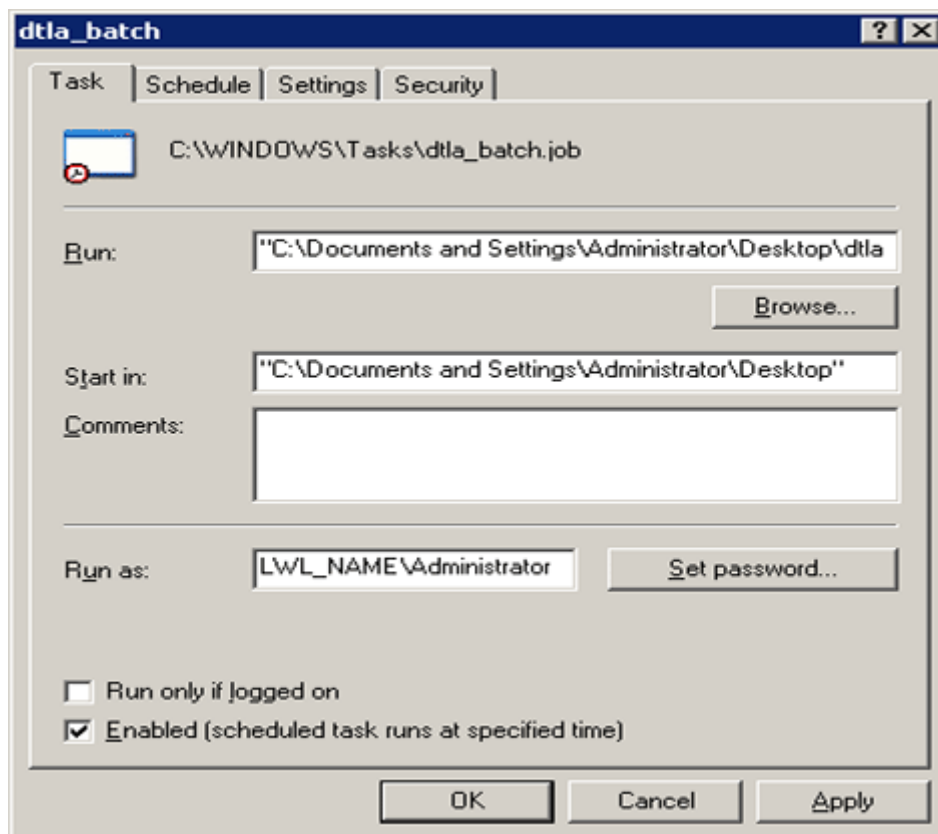
- When outputting multiple reports, please arrange and record commands.



2. Register the batch files to Task Schedule.

[In Windows® XP Professional]

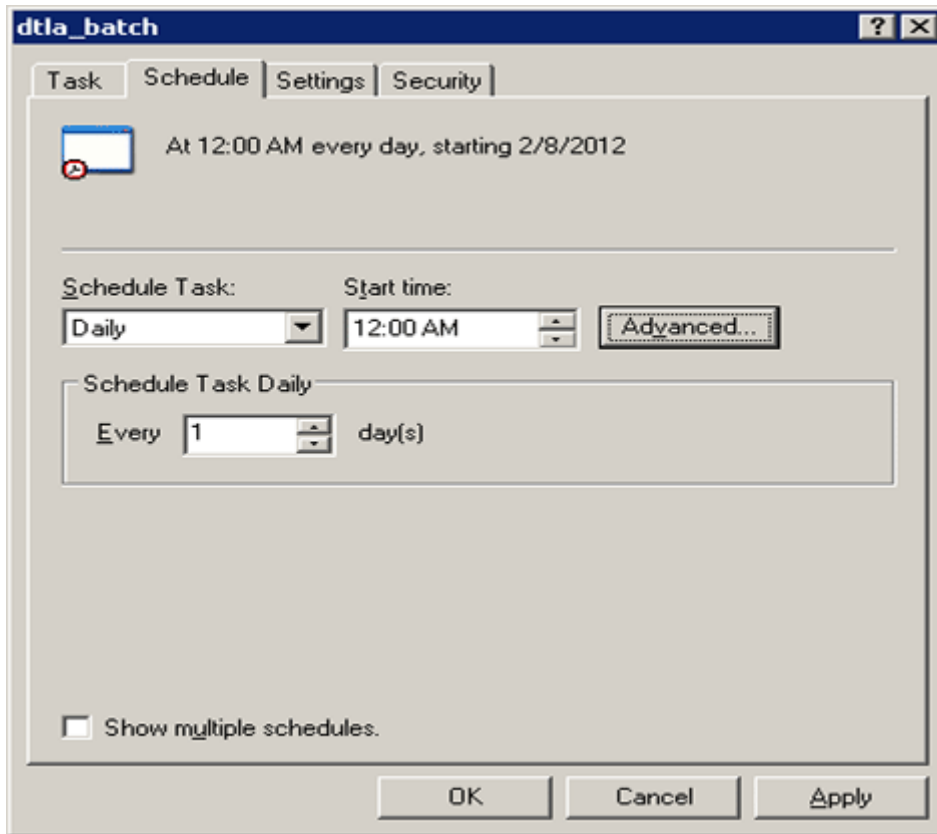
1. Start Task Scheduler and select the [Task] tab.



2. Set the following information.

- [Executing file name]: Specify batch files with full path. When space is contained in the path, please enclose it with " (double quotes).
- [Executing account name]: Specify user account of Windows. Specify the logon user account when setting batch users.
- [Execute]: Tick the check box.

3. Select the [Schedule] tab and set the start schedule for batch commands.



4. Click the [Apply] or [OK] button.

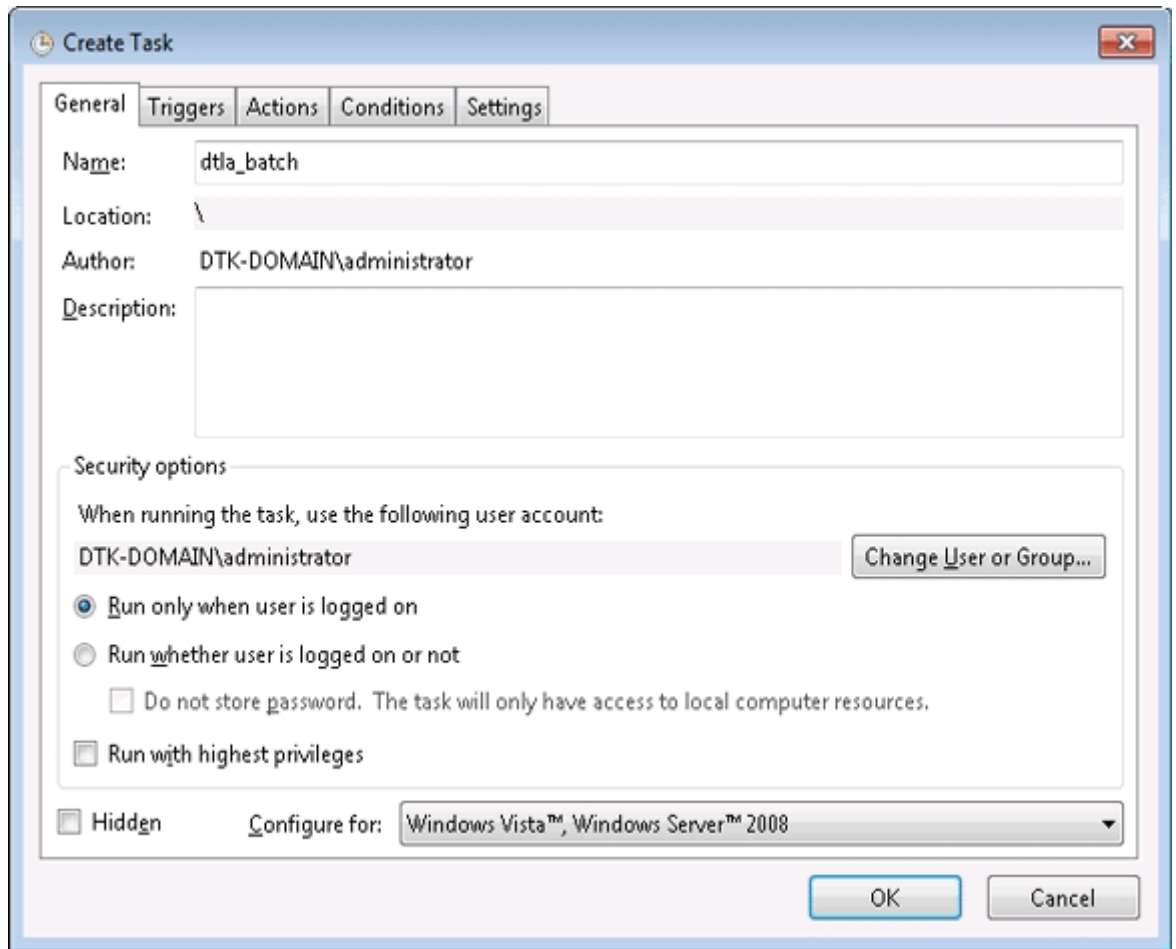
A log of report output commands will be saved to the following location.

```
%ALLUSERSPROFILE%\Application Data\Fujitsu\Systemwalker Desktop Keeper\LogAnalyzer
```

Environment variable %ALLUSERPROFILE% is usually "C:\Documents and Settings\All Users".

[In Windows Vista® and Windows® 7]

1. Start Task Scheduler and select the [General] tab.



2. Set the following information.

- [User account used during task execution]: Specify the user account of Windows. Specify the logon user account when setting batch users.
- [Execute only when users logon]: This item must be selected. If not, batch commands may not run normally.
- [Execute with top authority]: Tick the check box.

3. Select the [Triggers] tab and click the [New] button.

**New Trigger**

Begin the task: On a schedule

**Settings**

One time  
 Daily  
 Weekly  
 Monthly

Start: 2/11/2011 9:21:04 PM  Synchronize across time zones

**Advanced settings**

Delay task for up to (random delay): 1 hour

Repeat task every: 1 hour for a duration of: 1 day  
 Stop all running tasks at end of repetition duration

Stop task if it runs longer than: 3 days

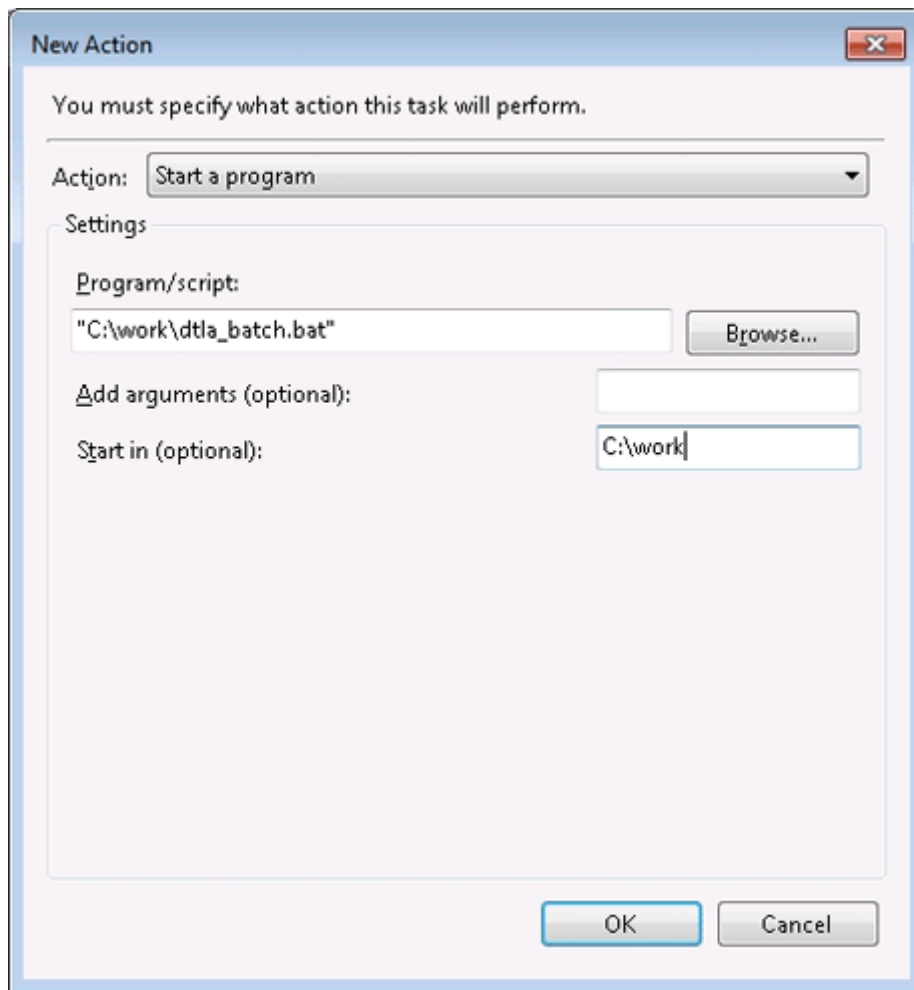
Expire: 2/11/2012 9:21:05 PM  Synchronize across time zones

Enabled

OK Cancel

4. Set the start schedule for batch command files and click the [OK] button.

5. Select the [Actions] tab and click the [New] button.



6. Set the following information and click the [OK] button.

- [Action]: Select [Start the Program].
- [Program/script]: Specify batch files with full path. When a space is contained in the path, please enclose it with “ (double quotes).
- [Start in (optional)]: Specify the folder that contains execution files with full path. Please do not enclose the path with “ (double quotes).

7. Click the [OK] button.

Logs of report output commands will be saved to the following location.

```
%ALLUSERSPROFILE%\Fujitsu\Systemwalker Desktop Keeper\LogAnalyzer
```

Environment variable %ALLUSERPROFILE% is usually “C:\ProgramData”.



# Chapter 7 Change Operating Environment

The chapter describes operations performed when it is necessary to change the environment in operation.

## 7.1 Change Import Method of Configuration Information

### When changing to import by linking with Active Directory from manual creation in Management Console

Please refer to "2.5.1 Import Information from Active Directory" for information required when the configuration information is imported from Active Directory server.

When the method of importing configuration information is changed, the user policy set before Active Directory Linkage cannot continue to be used. Please set the user policy again in the user information (user name) that is automatically created during Active Directory Linkage.

1. Stop the service of server.
2. Start the Server Settings Tool and click the [System settings] button.

→The [System Settings] window is displayed.

**System Settings**

Set the content related to whole system operation of Systemwalker Desktop Keeper Management Server

Set data linkage method  
Set the action related to data linkage of CT, CT group, user, user group and user administrator.

Active Directory linkage

Execute Active Directory linkage       Not execute Active Directory linkage

Status when creating user

Not apply user policy

Operation for CT/User who does not register to Active Directory

Allow administrators of all departments       Only limited to the specified department administrator

View CT registered location

Match with the computer location of Active Directory  
 Specify the computer responding to user name in the file

Corresponding file

Manage user information

Manage collectively on Master Management Server (recommended)  
 Manage on each Management Server (compatible with version earlier than V13.0)

\* When Management Server is 2-level system, the same action will be performed for all items, but it is recommended Select the collective management.  
\* When executing Active Directory linkage, user information will be collectively managed on Master Management Server.  
\* When Management Server is 3-level system, the settings of all Management Servers

Same CT determination condition when registering CT  
Specify the items for determination excluding "Computer Name". It is a item whose determination is the same as that of the existing CT when registering CT (register again).

- MAC Address       Use       Not use  
- Owner       Use       Not use  
- OS Type       Use       Not use

Tree displaying settings of department administrator  
When the department administrator is specified to log on Windows, the group with authority can be displayed only.

Display all groups (display forward compatibility)       Display group with management authority only

Set group that is not configured  
Specify whether the CT which do not belong to any group can be managed in the group that is not configured and can be operated by the department administrator.

Manage under the root directory (display forward compatibility)  
 Manage under the group that is not configured

Connection information between terminals

Manage       Not manage

\* When managing the connection information between terminals, it is sure to get the logon/logoff log on client (CT).

3. Select [Execute Active Directory linkage].  
Please refer to "Perform System Settings" of "Systemwalker Desktop Keeper Installation Guide" for details of other setting items.
4. Click the [Set] button.

5. Click the [Active Directory linkage settings] button of the [Server Settings Tool] window.

→ The [Active Directory Linkage Settings] window is displayed

Active Directory Linkage Settings

Set domain controller viewed by Management Server.

Domain list

Computer name	Domain name	NetBIOS name	Perform Linkage	User ID	Update date and time	Registration date and time
---------------	-------------	--------------	-----------------	---------	----------------------	----------------------------

Computer name

Domain name

Execute linkage

User Name

Password (first entry)

Password (re-entry)

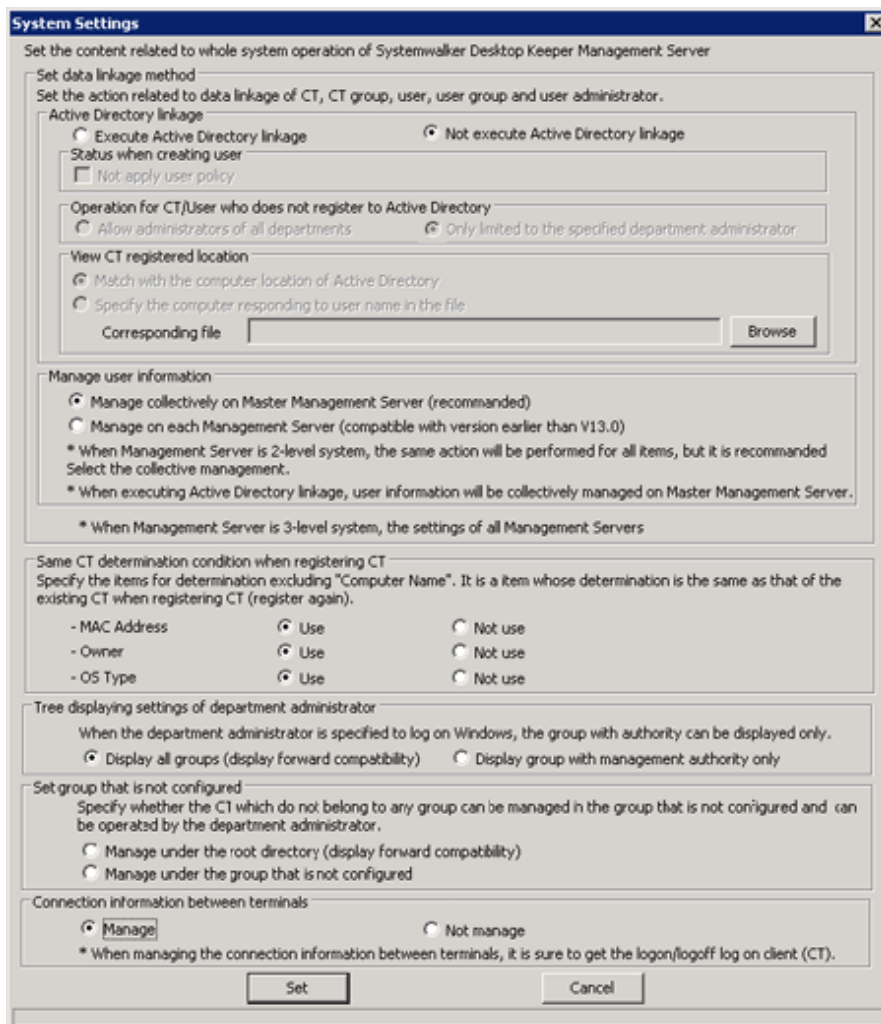
6. Set the linked Active Directory server information and click the [Add] button.  
Please refer to “Linking with Active Directory” of “Systemwalker Desktop Keeper Installation Guide” for details of setting items.
7. Run [Execute Directory Linkage settings] of the [Settings] during import menu of Server Settings Tool, or run the Active Directory Linkage command.  
For execution steps, please refer to “[2.5.1 Import Information from Active Directory](#)”.  
→The configuration information is imported.  
Move the existing group tree to the Local group.
8. Set the user policy in the user group (user name) that is automatically created when Active Directory Linkage is performed.  
For information on how to set, please refer to “[3.4.2 Modify User Policy](#)”.
9. Start the service.

### When import through linking with Active Directory is cancelled

1. Stop the service of the server.

2. Start the Server Settings Tool and click the [System settings] button.

→The [System Settings] window is displayed.



3. Select the [Not execute Active Directory linkage] and click the [Set] button.

4. Start the service.

After the import of configuration information by linking with Active Directory has been cancelled, all the group information, user information and policies that belong to the domain group will be deleted.

The group tree created under the Local group will be moved to the Root directory.

Please establish the configuration information manually or by linking with Systemwalker Desktop Patrol in the Root directory.

## 7.2 Change Management Method of User Information

When all the following conditions are satisfied, the management method of user information can be changed:

- In case of a 3-level system structure
- When it is not linked with Active Directory in the process of importing configuration information

## When managing in each Management Server is changed to collective management on Master Management Server

### 1. Move user information.

Use the DTKTBLCV.EXE (transfer user definition) command to transfer the information set in each Management Server to the Master Management Server.

For details of command, please refer to “DTKTBLCV.EXE (Transfer User Definition)” of “Systemwalker Desktop Keeper Reference Manual”.

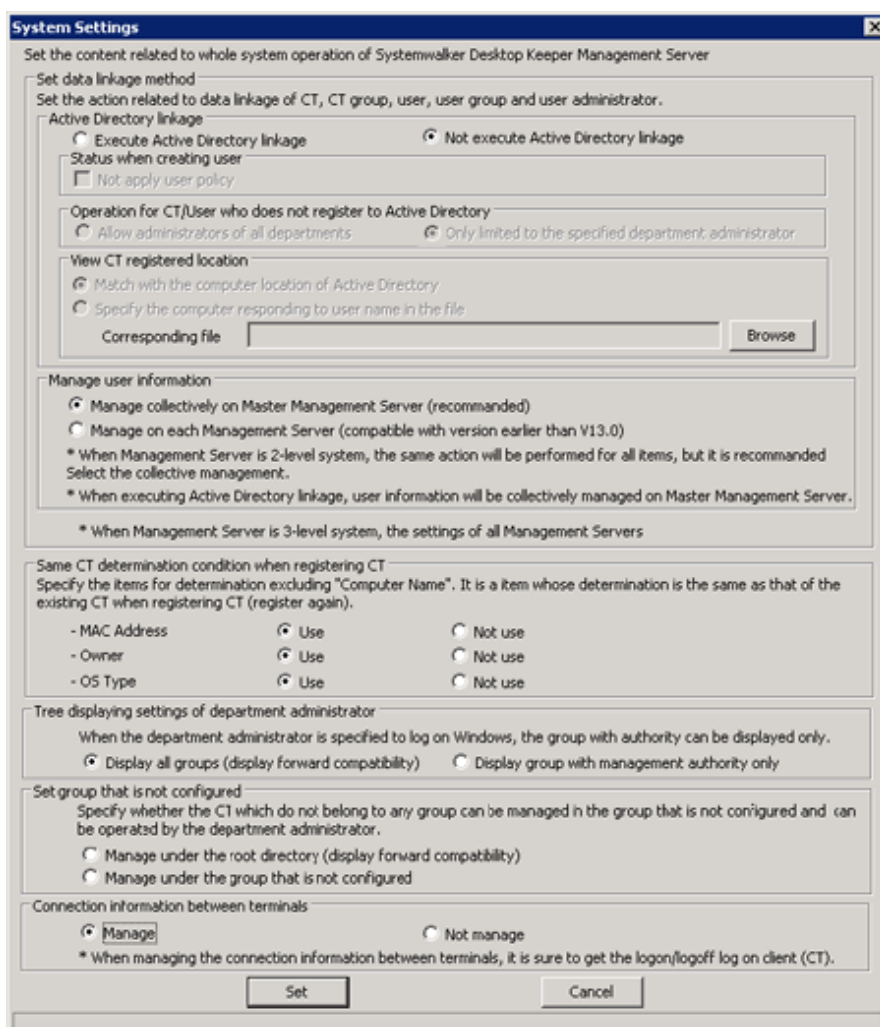
When user groups with the same name exist at the same level of each Management Server, the group with the same name will be created on the user group tree after centralization. In order to facilitate the management of user information, it is recommended to organize user information such as moving users and deleting user groups.

### 2. In the Management Console connected to the Master Management Server, manage the transferred user information.

a. Stop the service of the Master Management Server.

b. Start the Server Settings Tool and click the [System settings] button.

→The [System Settings] window is displayed.



c. Select [Not execute Active Directory linkage] in [Active Directory linkage].

d. Select [Manage collectively on Master Management Server] in [Manage user information].

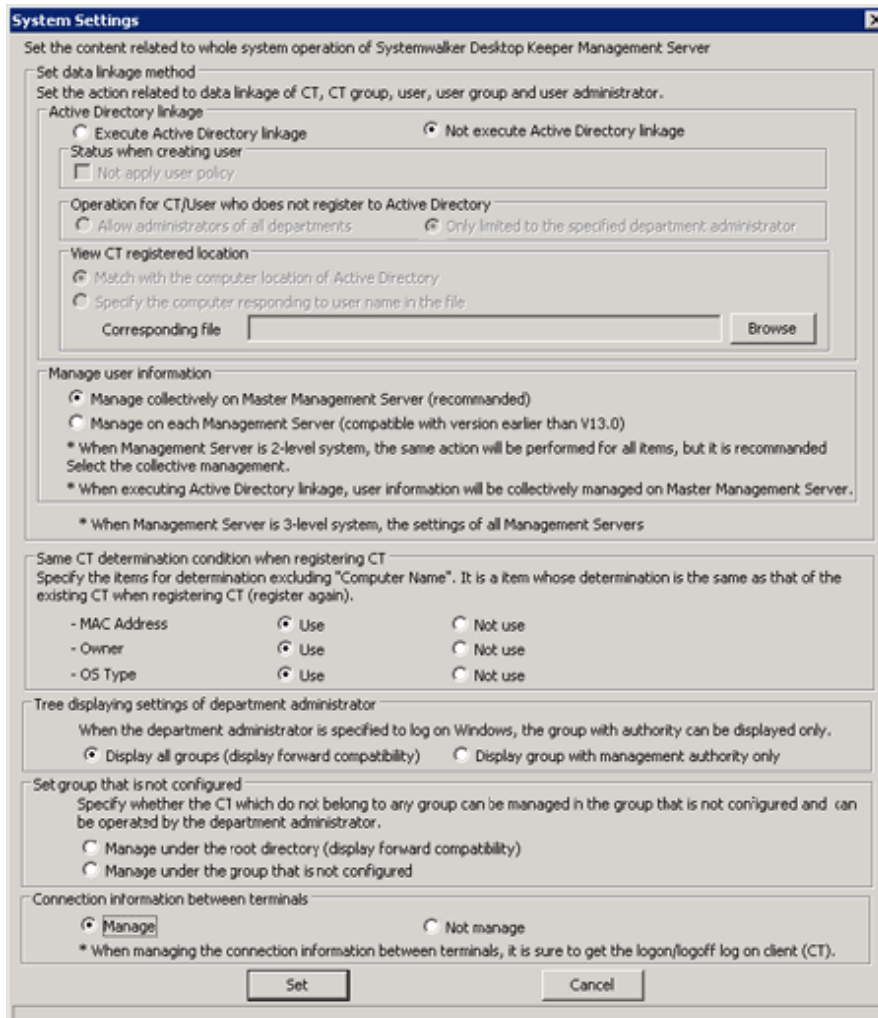
e. Click the [Set] button.

f. Start the service.

## When collective management in Master Management Server is changed to managing in each Management Server

1. Stop the service of the Master Management Server.
2. Start the Server Settings Tool and click the [System settings] button.

→The [System Settings] window is displayed.



3. Select [Not execute Active Directory linkage] in [Active Directory linkage].
4. Select [Manage on each Management Server] in [Manage user information].
5. Click the [Set] button.
6. Start the service.

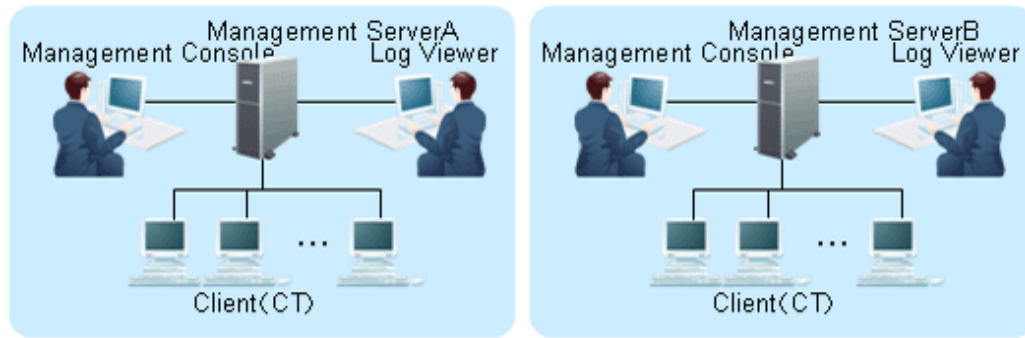
The transferred user information will be managed in the Management Console connected to each Management Server.

## 7.3 Change System Structure from 2-level to 3-level

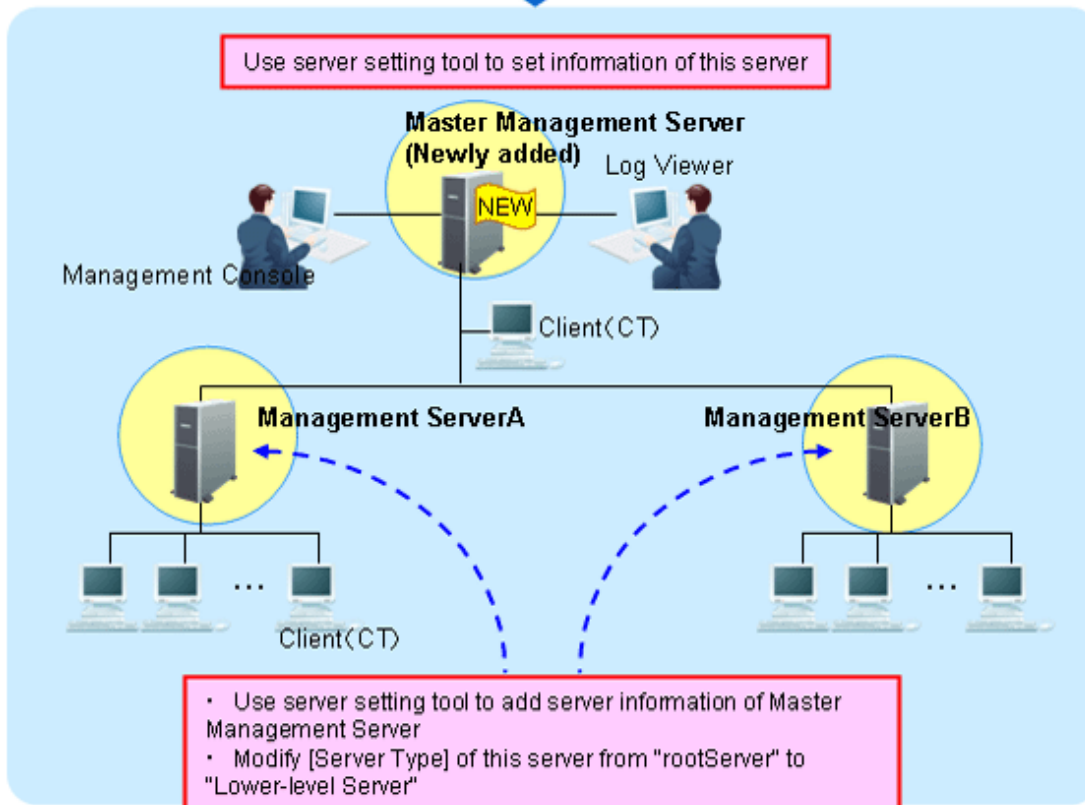
This section describes the following two methods for changing the system structure from 2-level to 3-level:

- When adding a new Master Management Server
- When changing an existing Management Server to the Master Management Server

## When adding a new Master Management Server



Newly add  
Master Management Server

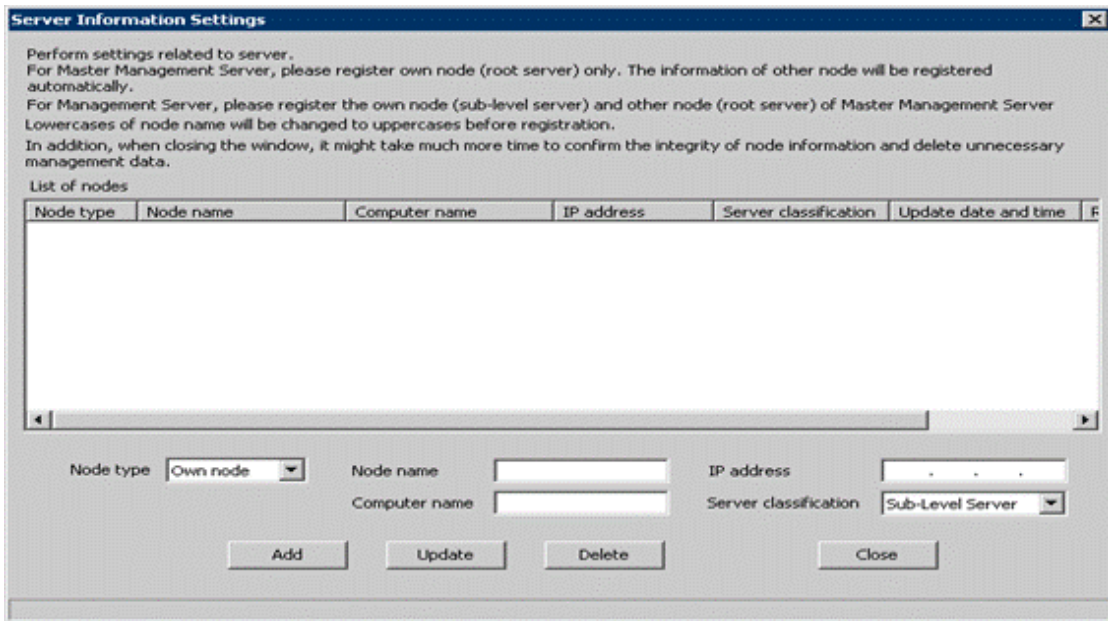




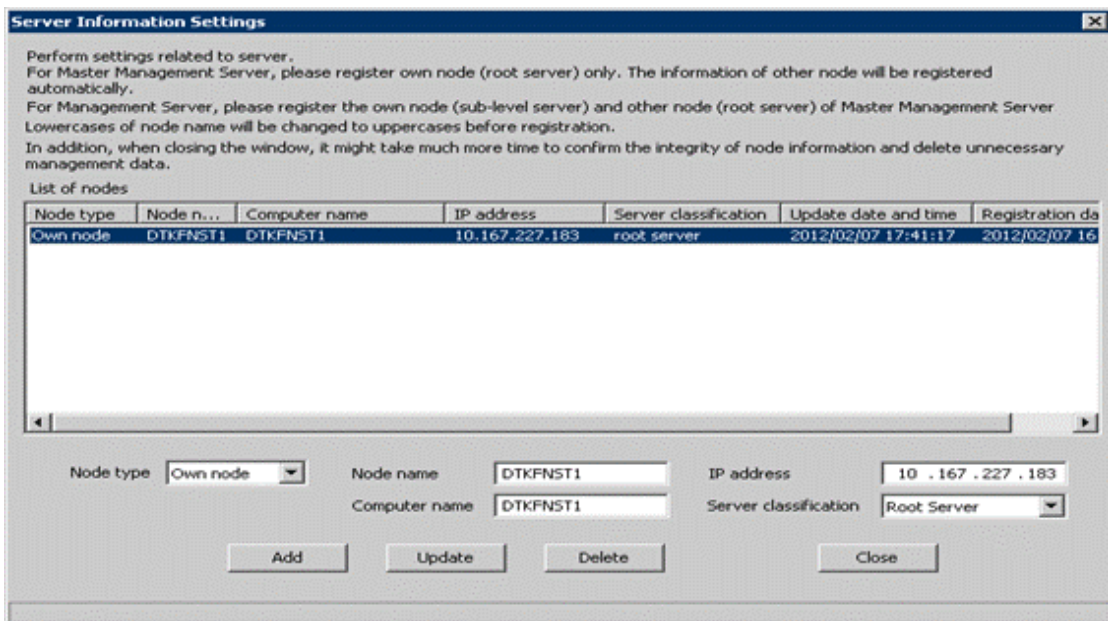
1. Construct a new Master Management Server.

For information on how to do so, please refer to “Installation” of “Systemwalker Desktop Keeper Installation Guide”.

Set the information of this server in the [Server Information Settings] window of the Server Settings Tool.



2. Stop the level control service and server service of the Management Server (Management Server A and Management Server B).
3. Set the following information in the [Server Information Settings] window of the Server Settings Tool on the Management Server.



- Change the [Server classification] of this server from “Root Server” to “Sub-Level Server”.
- Add the information of the Master Management Server.  
For details, please refer to “Set Server Information” of “Systemwalker Desktop Keeper Installation Guide”.

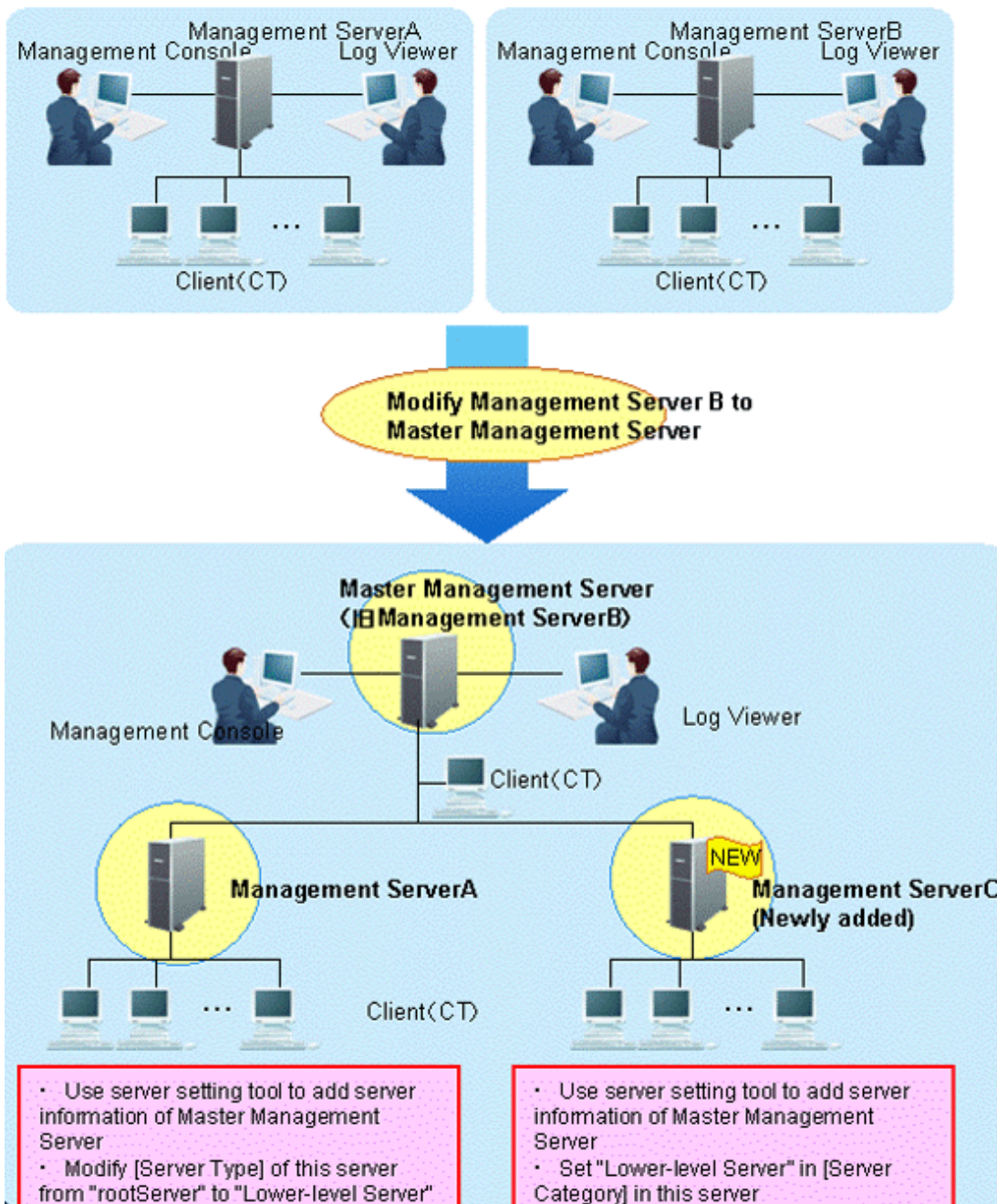
4. Start the level control service and server service of the Master Management Server.
5. Start the level control service and server service of the Management Server.

→ After the service of the Management Server has been started, the information of the subordinate Management Server will be set automatically in the Master Management Server.

6. When the client (CT) directly under the Master Management Server is connected, any of the following operations can be performed:
  - Install a new CT in the PC.  
Please refer to “Install CT” of “Systemwalker Desktop Keeper Installation Guide” for installation method.
  - Change the existing client (CT) environment.  
For information on how to do so, please refer to [“7.7.1 Change Management Server/Master Management Server To Be Connected”](#).
7. Set the Log Viewer environment and Management Console environment.  
Any of the following operations can be performed:
  - Install a new Management Console.  
For information on how to do so, please refer to “Install Management Console” of “Systemwalker Desktop Keeper Installation Guide”.
  - Change the existing environment of Log Viewer and Management Console.  
For information on how to do so, please refer to [“7.8 Change Management Console Environment”](#) or [“Start Log Viewer”](#).



## When changing the existing Management Server to Master Management Server

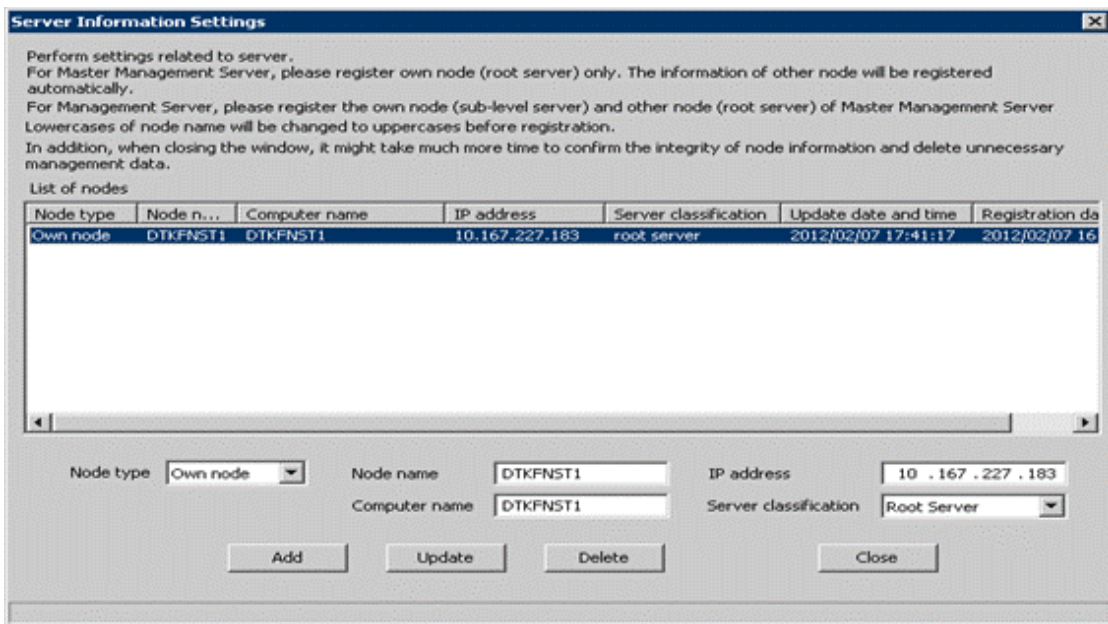


To directly use the server information of Management Server B, there is no need to change the Master Management Server (old Management Server B).

(In the Management Server B, the [Server Classification] is set to [Root]. This is because even if changes are made to the Master Management Server, [Server Classification] will not change.)

1. Stop the level control service and server service of the Master Management Server (old Management Server B) and Management Server A.

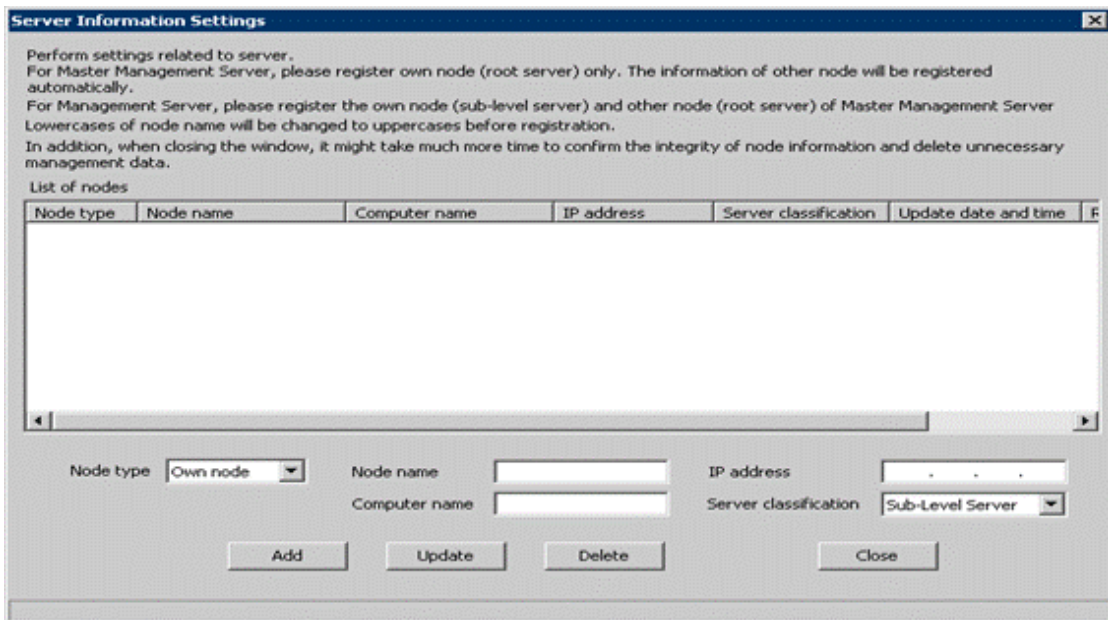
- Set the following information in the [Server Information Settings] window of the Server Settings Tool on Management Server A.



- Change the [Server classification] of this server from “Root Server” to “Sub-Level Server”.
- Add the information of the Master Management Server.  
 For details, please refer to “Set Server Information” of “Systemwalker Desktop Keeper Installation Guide”.

- Construct a new Management Server C.  
 For information on how to do so, please refer to “Installation” of “Systemwalker Desktop Keeper Installation Guide”.

Set the following information in the [Server Information Settings] window of the Server Settings Tool.



- Add the information of the Master Management Server.  
 For details of how to do so, please refer to “Set Server Information” of “Systemwalker Desktop Keeper Installation Guide”.
- Set the [Server classification] of this server to “Sub-Level Server”.

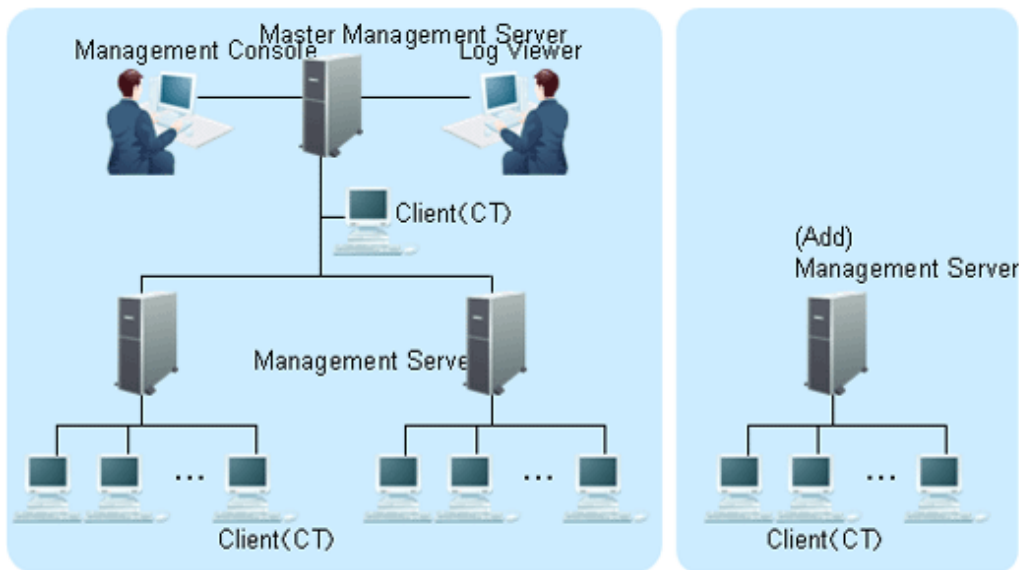
- Start the level control service and server service of the Master Management Server.

5. Start the level control service and server service of Management Server A and Management Server C.
  - After the service of the Management Server has been started, the information of the subordinate Management Server will be set automatically in the Master Management Server.
6. When the client (CT) directly under the Master Management Server is connected, any of the following operations can be performed:
  - Install a new CT in the PC.  
For information on how to do so, please refer to “Install CT” of “Systemwalker Desktop Keeper Installation Guide”.
  - Change the existing client (CT) environment.  
For information on how to do so, please refer to [“7.7.1 Change Management Server/Master Management Server To Be Connected”](#).

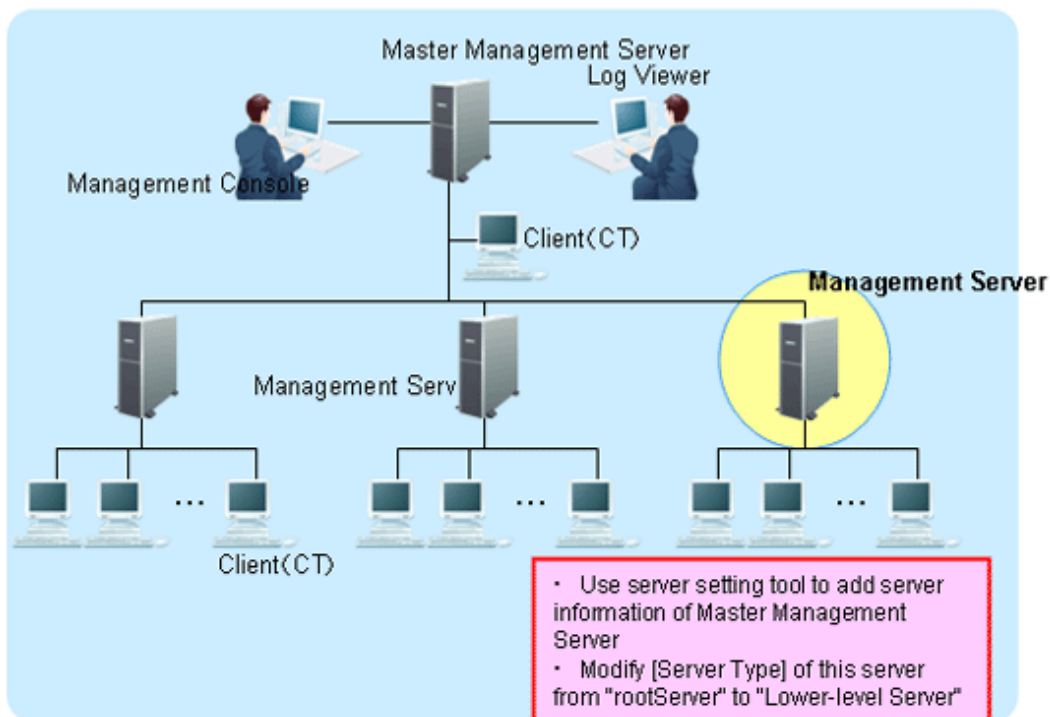
## **7.4 Add/Delete Management Server in 3-level System Structure**

### **Add management server**

This section describes how to add a Management Server in a 3-level system structure.



**Add Management Server**



1. When the user information is collective management in the Master Management Server, transfer the user information of the added Management Server to the Master Management Server.

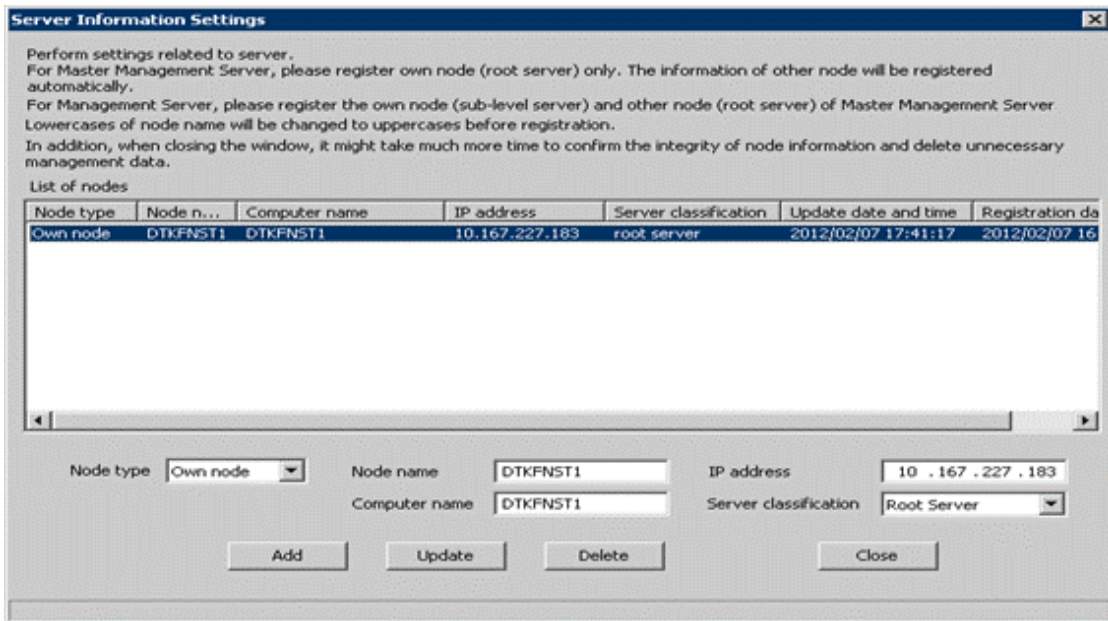
Use the DTKTBLCV.EXE (transfer user definition) command to transfer user information.

Please refer to "DTKTBLVCV.EXE (Transfer User Definition)" of "Systemwalker Desktop Keeper Reference Manual" for details.

2. Stop the level control service and server service of the Management Server to be added.



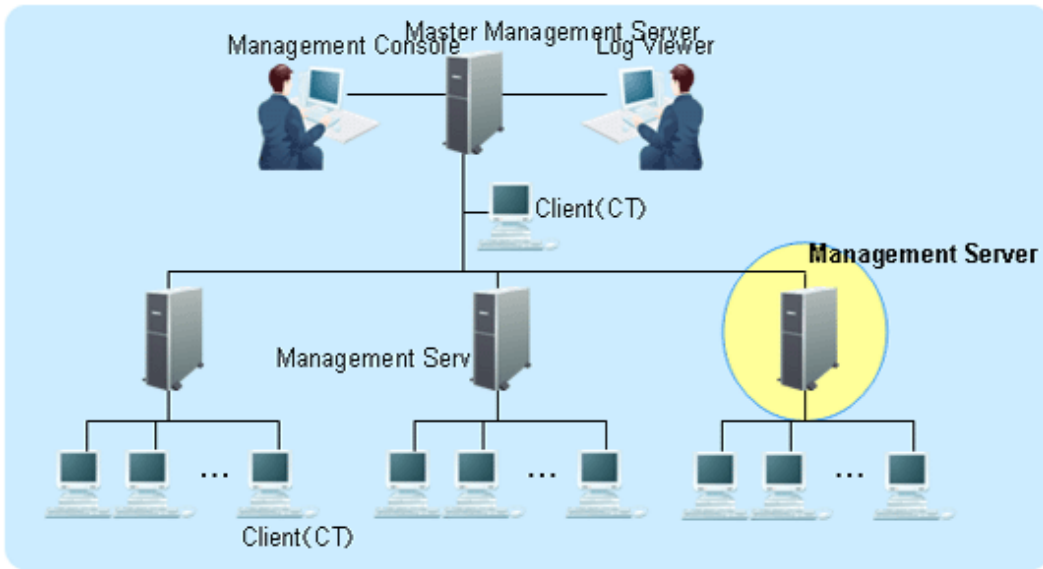
- Set the following information in the [Server Information Settings] window of the Server Settings Tool in the added Management Server.



- Modify the [Server classification] of this server from “Root Server” to “Sub-Level Server”.
  - Add the information of the Master Management Server.  
 For details of how to do so, please refer to “Set Server Information” of “Systemwalker Desktop Keeper Installation Guide”.
- Start the level control service and server service of the added Management Server.  
 →After the service of the Management Server has been started, the information of the added Management Server will be set automatically in the Master Management Server.

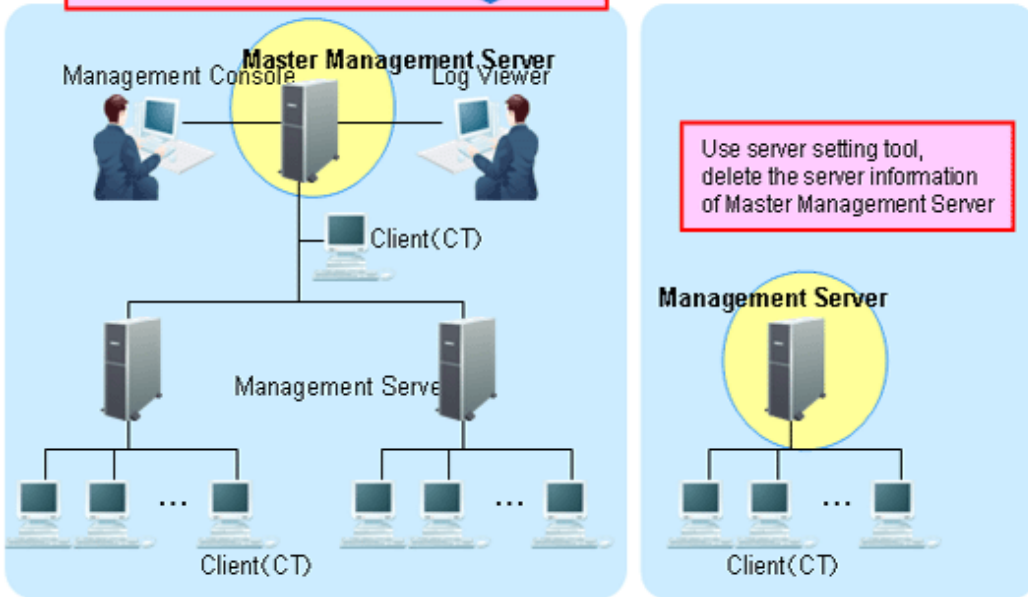
### Delete Management Server

When the server information of the Master Management Server is deleted in the Management Server, please delete the server information of the Management Server in the Master Management Server as well.  
 When the server information of the Management Server is deleted in the Master Management Server, please delete the server information of the Master Management Server in the Management Server as well.  
 The following is an example of mutually deleting server information.



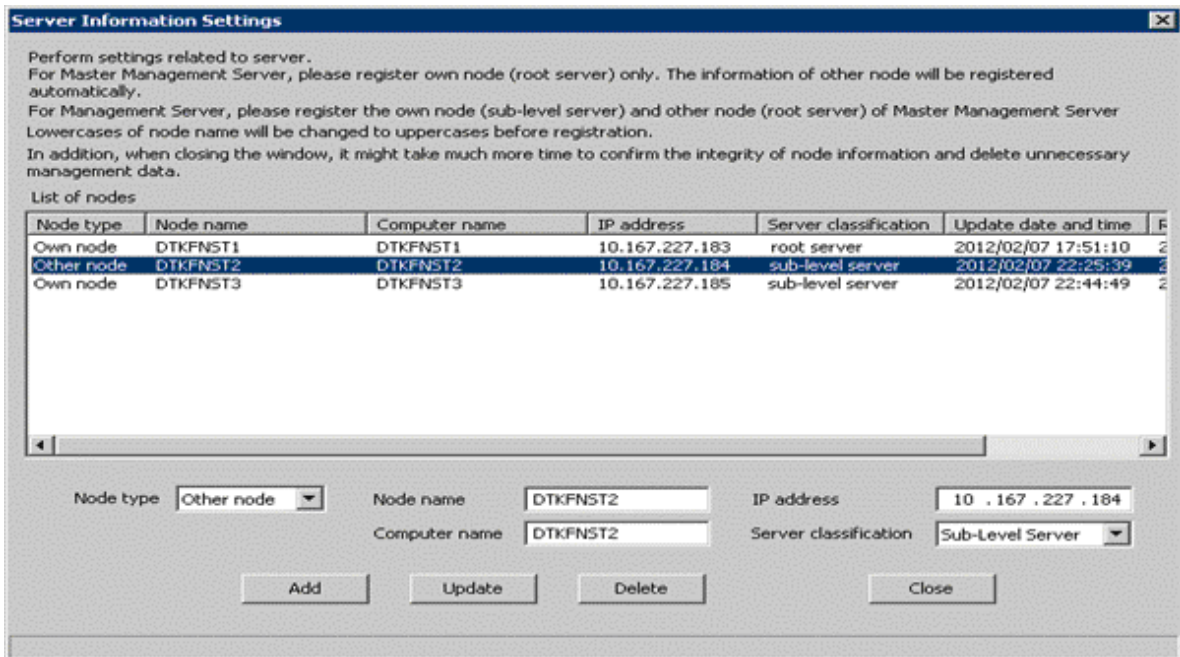
**Separate Management Server**

Use server setting tool,  
delete the server information of Management Server

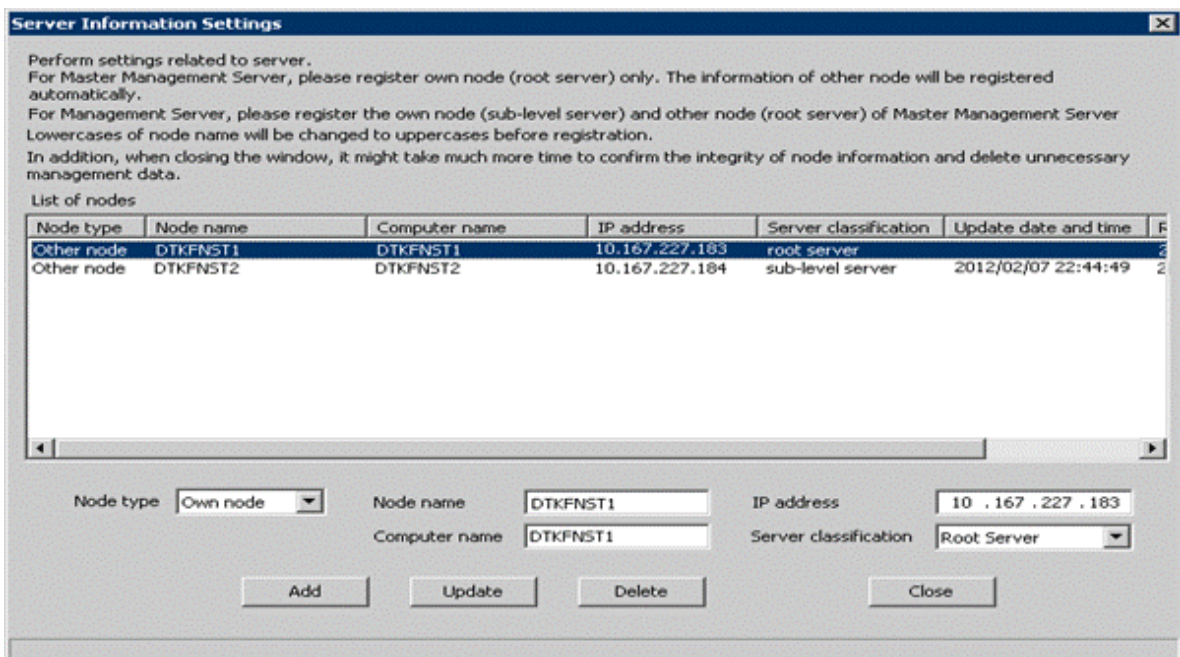


1. Stop the level control service and server service of the Master Management Server and separated Management Server.

2. Select a separated Management Server in the [Server Information Settings] window of the Server Settings Tool on the Master Management Server and click the [Delete] button.



3. Set the following information in the [Server Information Settings] window of the Server Settings Tool in the separated Management Server.



- Select the Master Management Server (other node) and click the [Delete] button.
  - Change the [Server classification] of this server c from “Root Server” to “Sub-Level Server”.
4. Start the level control service and server service according to the ranking of the Management Server and Master Management Server.

## 7.5 Export Files to Specified USB Device Only

---

**This function is not available.**

To reduce the risk of information disclosure, the USB devices that can be used can be restricted individually when exporting files and folders using the File Export Utility and Explorer, etc.

The permitted USB device requires policy setting in the Management Console.

Please refer to “[Register USB device](#)” and “[Set USB devices permitted to be used in policy setting.](#)” for these steps.

The information exported by File Export Utility, used media, export date and time and export person, etc., can be collected as a file export log.

The information exported by Explorer, used media, export date and time and export person, etc., can be collected as a file operation log. In addition, if the use of a USB device is restricted individually, and when the USB devices that are not permitted (it is limited to those identified as removable devices) are inserted, “Violation” will be recorded in the device configuration change log. This information can be sent to the administrator by E-mail. In addition, it can be recorded as an event log.

The registered USB device information includes the method of registering using the window and registering using a CSV file.

For the registration procedure, please refer to “[Register USB device](#)” and “[Register USB device information using CSV file](#)”.

In addition, the registered USB device information can be output to a CSV file. The functions are as follow:

- Confirm the USB device that has been registered.
- Transfer the registered USB device information to another Management Server.
- Change the registered USB device information.
- Delete the registered USB device information.

For the procedure, please refer to “[Export registered USB device information as CSV file.](#)” and “[Modify the registered USB device information](#)”.



### Point

---

**Conditions of [Individual Identification Function of USB Device] can be set.**

When the [File Export Prohibition] tab is set to the following patterns, the [Individual Identification Function of USB Device] can be set.

- Pattern 1
    - When [Export using File Export Utility] is set to [Yes]
  - Pattern 2
    - When [File Access Control] is set to [Yes]
    - When [Read Prohibition] is set to [Removable], Or
    - When [Specify Drive Type] is set to [Removable]
- 

### Application example

This describes the application example when the file export and reading are performed using only the USB devices that are permitted by the administrator.

Application example 1: only the files of USB device that prohibit or permit export of all files can be viewed.

Exporting any file to the USB device is prohibited; Access can occur when files saved in the permitted USB device are expected to be viewed or imported as a business requirement.





This application can be achieved through the following settings:

Export using File Export Utility is prohibited. In addition, export by Explorer (Not Export Utility) is also prohibited. Only reading by Explorer (Not Export Utility) is permitted.

For policy setting, please refer to “[Policy Setting of Application Example 1](#)”.

Application example 2: Limited to the use of permitted USB devices through File Export Utility.

File export is allowed only after encryption using the Export Utility. In addition, exporting (copying) from the outside through the software (unless done by the administrator) is prohibited, while access to the USB device through Explorer (Not Export Utility) is also prohibited.



This application can be achieved through the following settings.

File export is allowed only after encryption using the Export Utility. Exporting and reading using Explorer (Not Export Utility) are prohibited.

Please refer to “[Policy Setting of Application Example 2](#)” for policy setting.

Application example 3: Limited to file export to the permitted USB device through File Export Utility, and read of permitted USB device through the Explorer

File export is allowed only after encryption using the Export Utility. At this time reading is only permitted by Explorer (Non-File Export Utility).



This application can be achieved through the following settings.

File export is allowed only after encryption using the Export Utility. Reading through Explorer (Not Export Utility) is permitted, but the export is prohibited.

Please refer to “[Policy Setting of Application Example 3](#)” for policy setting.

Application example 4: exporting freely using Explorer is permitted for the permitted USB device (with lock and encryption function).

As the USB device with lock and encryption function has security functions, considering the convenience, it is expected to export using Explorer (Not Export Utility) (the File Export Utility will not be used and the accompanied security function of USB device will be used).

In addition, it is expected to connect the permitted USB with an external HDD to obtain backup files.

In the application example 4, files can be copied to the USB device by Explorer (Not Export Utility) instead of File Export Utility. However, since File Export Utility is not used, the file export logs cannot be collected and the original of exported files cannot be backed up. Access to the USB device can be confirmed by collecting file operation logs.

When collecting the file export logs and backing up the original of export files, please set File Export Utility and export files through File Export Utility.



This application can be achieved through the following settings.

Export and reading by Explorer (Not Export Utility) are permitted.

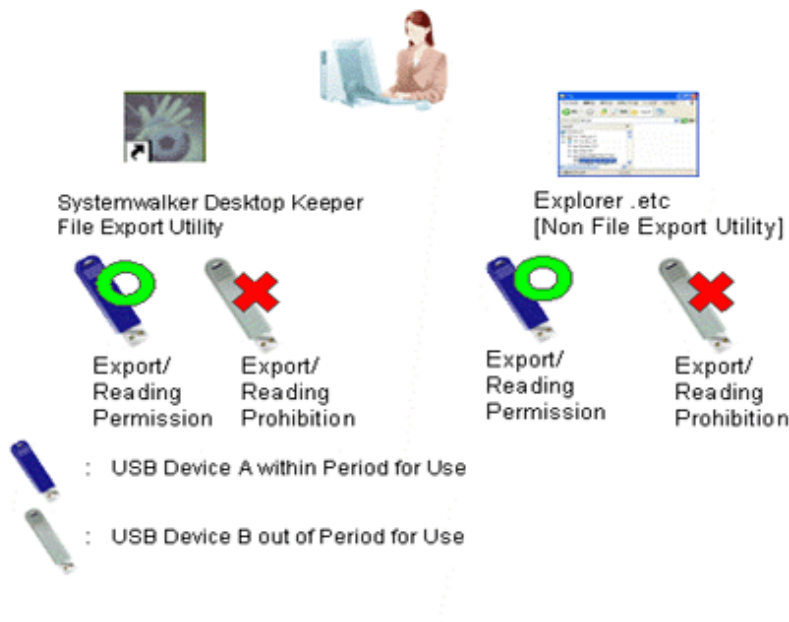
\*Though related settings of File Export Utility are not needed, the condition of the file export log expected to be collected and the original file exported by the backup file also need to be considered, and become the set example in the above picture.

Please refer to “[Policy Setting of Application Example 4](#)” for policy setting.

Application example 5: the period for use can be set for the permitted USB device.

By setting the period for use of the USB device, the USB device is permitted to be used within a set time only. The USB device that exceeds the period of use cannot be used. By setting the period for using the USB device again, the USB device that exceeds period of use can continue to be used.

## Period for Use



This application can be achieved through the following settings.

Set the period for use of the USB device, and permit exporting and reading.

※ It can also be limited to use by File Export Utility only or set to read only.

For policy setting, please refer to “[Policy Setting of Application Example 5](#)”.

Application example 6: the USB devices registered on Management Server/Master Management Server are allowed to be used.

When a large number of USB devices exist, it is difficult to set permissions of USB devices for each client (CT) and user. In this case, the problem can be solved by using USB devices registered on the Management Server/Master Management Server.

## Management Server Authentication



This application can be achieved through the following settings.

Permit the use of all USB devices registered on the Management Server/ Master Management Server, and permit exporting and reading.

※ It can also be limited to use by File Export Utility only or set to read only.

Please refer to “[Policy Setting of Application Example 6](#)” for policy setting.

## Register USB device

The registration can be performed by the system administrator or department administrator.

It is required to set the authority of [Register/Update/Delete USB Device] in [Detailed Authority] in the [Administrator Information Settings] window of the Server Settings Tool.

The registration can be performed through the Management Console.

In the case of a 3-level system structure, the registration can be performed through the Management Console that is connected to the Master Management Server. It has nothing to do with the execution of collective management of user information.

The number of USB devices that can be registered is 10,000.

The USB device that satisfies all the following conditions can be registered:

- It has a USB interface.
- The manufacturer ID/product ID/internal serial number can be obtained from the USB device.

An example of a USB device that can be registered is shown as follows:

USB Device	Description and Notes
USB Flash Memory	It can also be registered via USB-HUB.
USB Hardware	It can also be registered via USB-HUB.
SD Card via USB Card Reader .etc	Identify the device itself as the USB device that can be registered. The inserted memory media cannot be identified separately.
USB Floppy Disk Device	Identify the device itself as the USB device that can be registered and the inserted floppy media cannot be identified separately.
USB MO Device	Identify the device itself as the USB device that can be registered and the inserted MO media cannot be identified separately.
USB DVD/CD-R/RW Device	Sometimes, USB device information cannot be obtained through the [Get USB Device Information] button. In this case, please check the USB device information through device manager, etc., and manually input [USB Device Information].

After the registered device information has been set to “Permitted Device” in policy, it can be distributed as CT policy or user policy.

## Register

Register one by one in the [Register USB Device] window. One USB device will be registered as one item.

The procedure is as follows:

1. Start [Management Console].
2. Select [USB Device Registration] in the [Operation Settings] menu.  
→ The [USB Device Registration] window is displayed.

Item Name	Description
[USB Device Screening]	Screen the USB devices displayed in the [List of Registered USB Device]. The following items can be selected: - Within period for use Display the USB devices within period for use.

Item Name	Description
	<p>This can be used when the [Settings of Period for Using USB Device] is performed.</p> <ul style="list-style-type: none"> <li>- Beyond the period for use Display the USB devices that exceed period for use . This can be used when the [Settings of Period for Using USB Device] is performed.</li> <li>- All Display all USB devices.</li> <li>- USB device name Search the character string entered in [Keyword] with partially match and display the USB device.</li> <li>- Manufacturer ID Search the character string entered in [Keyword] with complete match and display the USB device. Please enter the keyword in hexadecimal digit.</li> <li>- Product ID Search the character string entered in [Keyword] with complete match and display the USB device. Please enter the Keywords in hexadecimal digit.</li> <li>- Device name Display the character string input in [Keyword] with partially match.</li> <li>- Internal serial number Display the character string input in [Keyword] with partially match.</li> <li>- Authentication method Display the character string input in [Keyword] with partially match. The character string that can be entered is as follows: <ul style="list-style-type: none"> <li>- Complete match</li> <li>- Product match</li> <li>- Serial number match</li> <li>- Not available</li> </ul> </li> <li>- Last used user name Display the character string entered in [Keyword] with partially match.</li> <li>- Last used computer name Display the character string entered in [Keyword] with partially match.</li> <li>- Notes Display the character string entered in [Keyword] with partially match.</li> </ul>
[Keyword]	<p>Specify the search condition of displayed USB device.</p> <p>Up to 128 single-byte characters (64 double-byte characters) can be entered.</p>
[Search]	<p>Perform the USB device search according to the conditions specified in [USB Device Screening] and [Keyword].</p>

Item Name		Description
[List of Registered USB Devices]		<p>Display the content of registered USB device.</p> <p>Display the following information:</p> <ul style="list-style-type: none"> <li>- USB device name Display the device name of USB device.</li> <li>- Notes Display the notes of USB device.</li> <li>- Manufacturer ID Display the manufacturer ID of USB device.</li> <li>- Product ID Display the product ID of USB device.</li> <li>- Device name Display the device name of USB device.</li> <li>- Internal serial number Display the internal serial number of USB device.</li> <li>- Identification method Display the identification method of USB device.</li> <li>- Last connection date Display the date of last used USB device.</li> <li>- Period for use Display the period for use of permitted USB device of use.</li> <li>- Last used user name Display the user name that uses USB device at last.</li> <li>- Last used computer name Display the computer name that uses USB device at last.</li> </ul>
[Drive Name]		<p>When reading USB device information through the [Get USB Device Information] button, select the drive to load this device. Initial value: the first drive that is not connected to the device after the C drive.</p>
[Get USB Device Information]		<p>After clicking, information will be read from the USB device inserted into the specified drive.</p>
[Setting Item]	[USB Device Name]	<p>Up to 80 single-byte characters can be entered. However, the following characters cannot be entered:</p> <ul style="list-style-type: none"> <li>•Control code</li> <li>•UNICODE character</li> <li>•Single-byte space or double-byte space only. (When the single-byte space or double-byte space is set at the beginning or end, the space will be deleted.)</li> </ul> <p>Please make sure to enter this item.</p>
	[Notes]	<p>Up to 128 single-byte characters can be entered. However, the following characters cannot be entered: Control code, UNICODE character</p>
[USB Device Information]	[Manufacturer ID] [Product ID] [Device Name] [Internal Serial Number]	<p>When clicking the [Get USB Device Information] button, the read USB device information will be displayed.</p> <p>When registering USB device manually, please enter the following items:</p>

Item Name		Description
		<ul style="list-style-type: none"> <li>- Manufacturer ID Four hexadecimal digits can be entered.</li> <li>- Product ID Four hexadecimal digits can be entered.</li> <li>- Device name Up to 80 single-byte characters can be entered. However, the following characters cannot be entered. <ul style="list-style-type: none"> <li>•Control code</li> <li>•UNICODE character</li> </ul> </li> <li>- Internal serial number Up to 64 single-byte characters can be entered.</li> </ul>
[Last User Information]	[Last Used User Name] [Last Used Computer Name] [Last Connection Date]	Display the information of the last user of USB device.
[Identification Method of USB Device]	When exporting files to the USB device using the Export Utility and Explorer, etc., this is a method to identify whether it is a permitted USB device.	
	[Complete match] (Initial Value)	Identify according to manufacturer ID + product ID + internal serial number. When the [Identification Method of USB Device] is [Complete match], and the media whose [Manufacturer ID], [Product ID] and [Internal Serial Number] are consistent has been registered in [Complete match], registration cannot be performed.
	[Serial number match]	Identify according to manufacturer ID + internal serial number. In [List of Registered USB Devices], the background color of [Product ID] will be displayed in gray.  When registering USB device attached with authentication function and the product ID before authentication is different from that after authentication (*), select this item.
	[Product match]	Identify USB device according to manufacturer ID + product ID. In the [List of Registered USB Devices], the [Internal Serial Number] will be displayed in gray.
	[Not available]	The registered USB device can be set as temporarily not available. Though it is set as an available USB device in policy, it cannot be used either. Under the following conditions, select this item: [Example] <ul style="list-style-type: none"> <li>•Though it can be used at any time, only registration is implemented at present.</li> <li>•It becomes idle resource temporarily without any user.</li> <li>•The corresponding USB device is lost.</li> </ul> In the [List of Registered USB Devices], all items of this line will be displayed in gray.
[Period for use of USB Device]	When [Set Period for Use of USB Device] is selected in the [Operation Settings of USB Device], set the period for use of the USB device.	



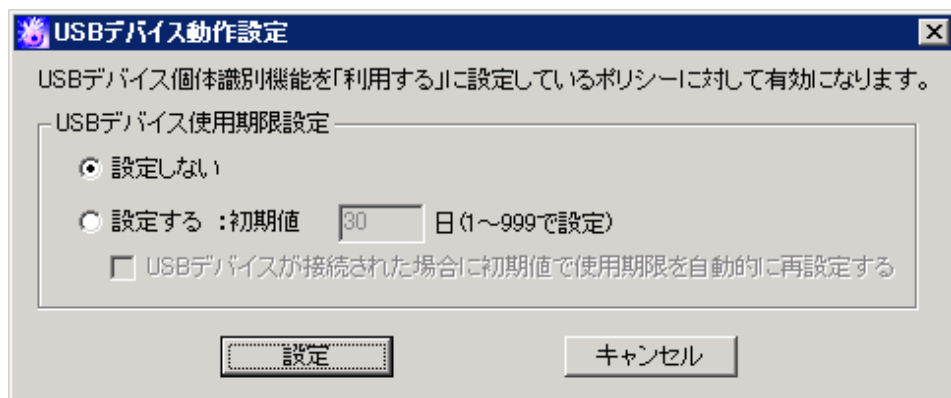
Item Name		Description
		Only the single-byte digits can be entered, and the input scope is as follow. <ul style="list-style-type: none"> <li>- Year: 2000-2037</li> <li>- Month: 1-12</li> <li>- Day: 1-31</li> </ul>
[Export/Import of Setting Contents]	[File Export]	Display the [Specify the File for Exporting USB Device Information] window. Set the condition of exporting USB device information in CSV format and export.
	[File Import]	Display the [Specify the File for Importing USB Device Information] window. This is used when the USB device information is moved to another Management Server.
[Add]		Register a USB device. Up to 10,000 devices can be registered.
[Update]		Update USB device information.
[Delete]		Delete a registered USB device.
[Operation Settings]		Perform operation settings of USB device.

\* It is recommended to confirm that the registration is performed before/after authentication in advance.

Please click the [Get USB Device Information] button before/after authentication, and confirm that only the [Product ID] displayed in the [USB Device Information] has modified.

3. Click the [Operation Settings] button.

→ The [Operation Settings of USB Device] window is displayed.



Item Name		Description
[Set Period for Use of USB Device]		Set the period for use of the USB device.
	[Not Set] (Initial Value)	The USB device can be used at any time.
	[Set]	Set the period in which the USB device can be used. Please specify the time to be extended when the period for use of USB device has been exceeded. 1-999 can be specified.
	[The period for use will be reset with the initial value when the USB device is connected]	Set whether the period for use will be automatically extended when the period for use of USB device is exceeded. The extended time is to add days specified in [Initial Value] of [Set]

Item Name		Description
		Period for Use of USB Device]. Select this item and the user can extend the period for use by using the USB device.

4. Click the [Settings] button.
5. Insert the USB device that requires registration into the PC of Management Console.
6. Select the drive identified by the PC selected in [Drive Name] and click the [Get USB Device Information] button.  
→ The information of the inserted USB device is displayed in [USB Device Information].  
The registration cannot be performed when the USB device information cannot be read from the media.

### Point

#### USB device with lock function

When using a USB device with a lock function, please click the [Get USB Device Information] button after unlocking.

### Point

About DVD/CD-R/RW devices of USB interface

DVD/CD-R/RW devices with a USB interface. etc., can be registered by manually entering the manufacturer ID/product ID/internal serial number.

7. Select [Identification Method of USB Device].
8. Enter [USB Device Name] and [Notes].  
  
In the case of a 3-level structure, the registration information will be saved on the Master Management Server; in the case of a 2-level structure, the registration information will be saved on Management Server and the information of multiple subordinating departments will co-exist. Therefore, when setting policy, it is expected that the USB devices permitted by the local department will be selected from a large number of registration information. Though each items displayed in [List of Registered USB Devices] can be sorted, it is recommended to set the identification information such as department and user name, etc., in [Notes] to facilitate selection.
9. click the [Add] button.  
→The registration content is displayed in [List of Registered USB Devices].

#### Modify

1. Start [Management Console], and the [USB Device Registration] window is displayed.
2. Select the USB device that requires update in [List of Registered USB Devices].  
→ The registered content is displayed.
3. Update the corresponding items and click the [Modify] button.  
→The update will be reflected to [List of Registered USB Devices].

#### Delete

1. Start [Management Console], and the [USB Device Registration] window is displayed.

2. Select the USB device that requires deletion in [List of Registered USB Devices].
  - The registered content is displayed.
  - When deleting the information, please refer to the identification information such as department and user name, etc., in [Notes] and execute after confirming that is the USB device information of the local department.
3. click the [Delete] button.
  - The information is deleted from the [List of Registered USB Devices].

## View

The computer name, user name and use date of last used USB device can be confirmed in the [USB Device Registration] window. Whether or not the USB device that has not been used for a long time due to reasons such as lost USB devices exists can be confirmed.

1. Start [Management Console] and the [USB Device Registration] window is displayed.
  - Confirm the usage status of USB device through the [Last Used User Name], [Last Used Computer Name] and [Last Connection Date].

## Set USB devices permitted to be used in policy setting.

The policy setting is performed by the system administrator or department administrator.

This section describes by [Application example](#) including policy setting from application example 1 to application example 4.

### Policy Setting of Application Example 1

In the [File Export Prohibition] tab, set as follows:

- [File Export Utility]
  - Select [No] in the [Export using File Export Utility].
- [Explorer]
  - Select [Yes] in [File Access Control].
  - Select [Disable] in [Read Prohibition] ([Read of Removable Drive]).
  - Select [Removable] in [Specify Drive Type] of [Export Prohibition].
- [Individual Identification Function of USB Device]
  - Select [Use].
  - Select [Read Only] in the [File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings] window.

### Policy Setting of Application Example 2

In the [File Export Prohibition] tab, set as follows:

- [File Export Utility]
  - Select [Yes] in [Export using File Export Utility].
  - Select [Export after Encryption Only].
- [Explorer]
  - Select [Yes] in [File Access Control].
  - Select [Disable] in [Read Prohibition] ([Read of Removable Drive]).
  - Select [Removable] in [Specify Drive Type] of [Export Prohibition].
- [Individual Identification Function of USB Device]
  - Select [Use].

- Select [Read and Write] in the [File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings] window.
- Select [Write using File Export Utility Only] in the [File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings] window.

#### Policy Setting of Application Example 3

In the [File Export Prohibition] tab, set as follows:

- [File Export Utility]
  - Select [Yes] in [Export using File Export Utility].
  - Select [Export after Encryption Only].
- [Explorer]
  - Select [Yes] in the [File Access Control].
  - Select [Disable] in [Read Prohibition] ([Read of Removable Drive]).
  - Select [Removable] in [Specify Drive Type] of [Export Prohibition].
- [Individual Identification Function of USB Device]
  - Select [Use].
  - Select [Read and Write] in the [File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings] window.
  - Select [Read and Write by File Export Utility Only] in the [File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings] window.

#### Policy Setting of Application Example 4

In the [File Export Prohibition] tab, set as follows:

- [File Export Utility]
  - Select [Yes] in the [Export using File Export Utility].
  - Select [Export Only after Encryption].
- [Explorer]
  - Select [Yes] in the [File Access Control].
  - Select [Disable] in the [Read Prohibition] ([Read of Removable Drive]).
  - Select [Removable] in the [Specify Drive Type] of [Export Prohibition].
- [Individual Identification Function of USB Device]
  - Select [Use].
  - In the [File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings] window, select [Read and Write]. Do not tick any of subordinate check boxes.

#### Policy Setting of Application Example 5

In the [Operation Settings of USB Device] of [USB Device Registration], set as follows:

- Select [Set Period for Use of USB Device].

In the [USB Device Registration] window, set as follows:

- Select the USB device required to set period for use in [List of Registered USB Devices], and set the permitted date of use in [Period for Use of USB Device].

In the [File Export Prohibition] tab, set as follows:

- [Individual Identification Function of USB Device]
  - Select [Use].
  - Select the permitted access settings of use in [File Export- Individual Identification Function of USB Device-Detailed Settings] window.

#### Policy Setting of Application Example 6

In the [File Export Prohibition] tab, set as follows:

- [Individual Identification Function of USB Device]
  - Select [Use].
  - Select [Yes] in [Use of all USB devices registered on the Management Server are permitted] of [File Export- Individual Identification Function of USB Device-Detailed Settings] and select the permitted access settings of use.

In addition, when the individual identification function of the USB device is used, the device configuration change log can be collected as “Violation” in the following patterns.

The following only explains the condition when the device configuration change log is collected as “Violation” and does not correspond to the above-mentioned application examples from 1 to 6.

- Pattern 1
  - When the [Identification Method of USB Device] of [USB Device Registration] is a USB device connection of [Not Available]
- Pattern 2
  - When the period for use set in [Period for use of USB Device] of the [USB Device Registration] window is exceeded
- Pattern 3
  - When the [Use of all USB devices registered on the Management Server are permitted] in the [File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings] window is set to [Yes] and the Management Server cannot be connected to the client (CT).

Click the [Update at Next Startup] or [Update Immediately] button, and set policies.

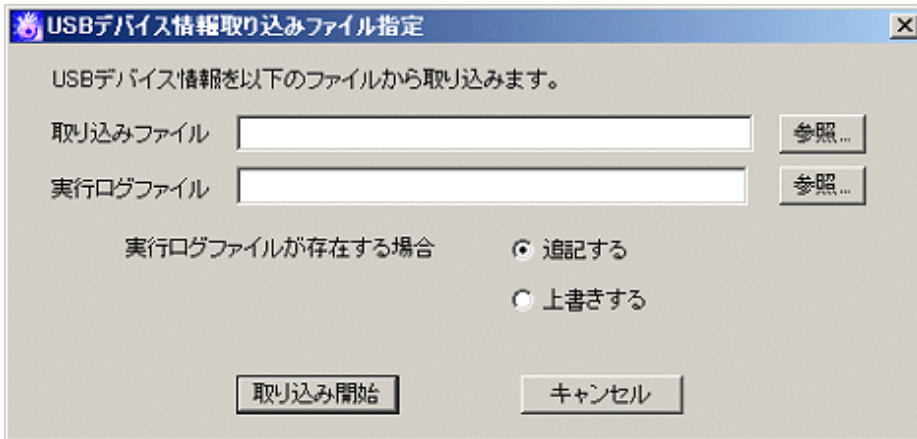
The CT policy will be reflected when the client (CT) is started, and the user policy will be reflected when logging on to the client (CT). This will be reflected by an immediate update of policy.

### Register USB device information using CSV file

1. Create USB device list file.
  - For details of the USB device list file, please refer to “USB Device List File” of “Systemwalker Desktop Keeper Reference Manual”.
2. Start [Management Console], and the [USB Device Registration] window is displayed.

3. Click [Import File] button.

→ The [Specify the File for Importing USB Device Information] window is displayed.



- **[Import File]** (Required): specify the USB device list file with full path.

Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in file name.  
The symbols not allowed: “\” “/” “:” “\*” “?” “|” “<” “>” “|”

- **[Result log file]** (Required): specify and save the file of execution results with full path.

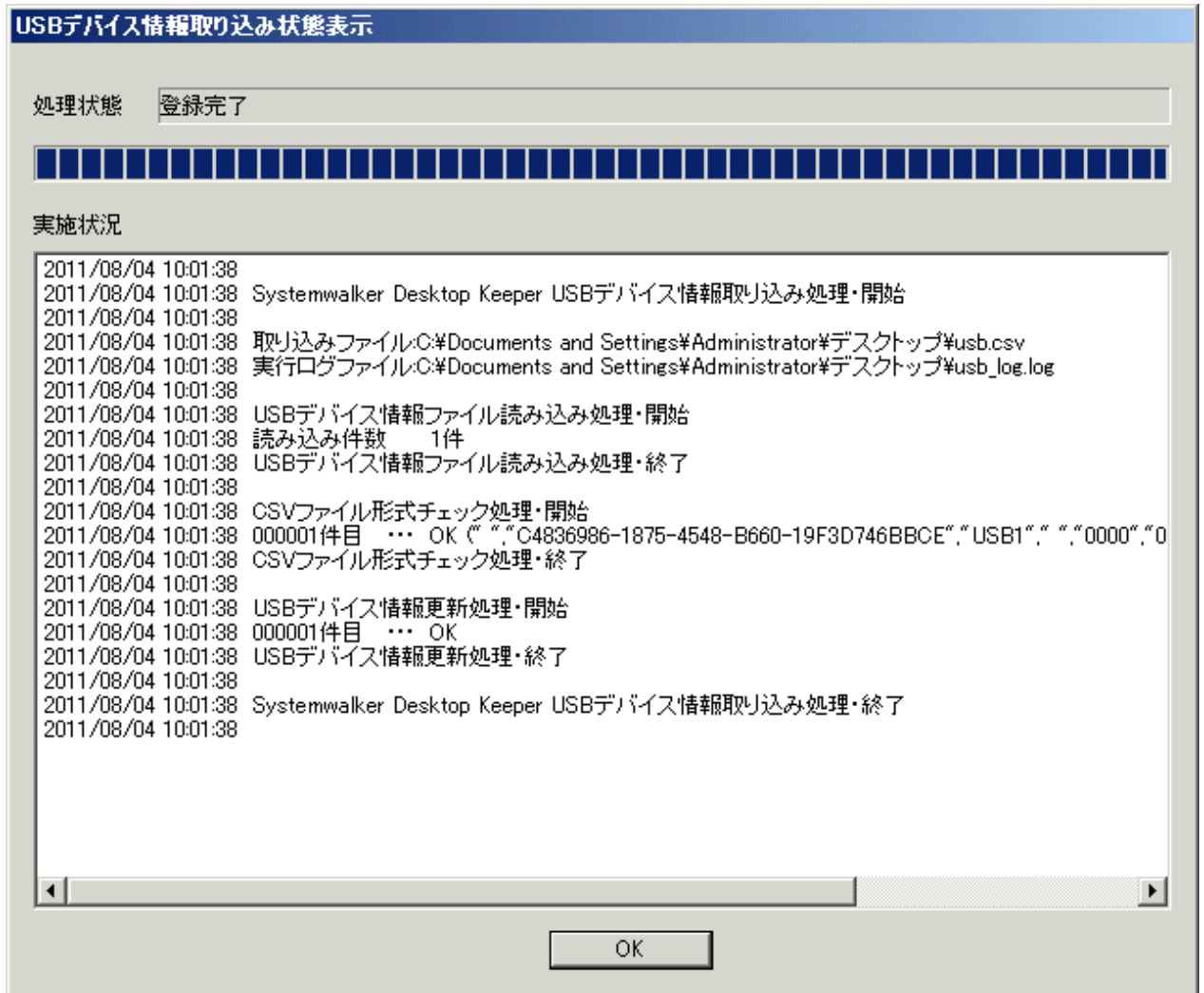
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in file name.  
The symbols not allowed: “\” “/” “:” “\*” “?” “|” “<” “>” “|”

- **[When the result log file exists]**: please make sure to set when the original result log file exists.

**[Add]**: select when the file is added to the original result log file.

**[Overwrite]**: select when the file overwrites the original result log file.

- Set the above-mentioned information and click the [Start Import] button.  
→ The [Display Import Status of USB Device Information] window is displayed.



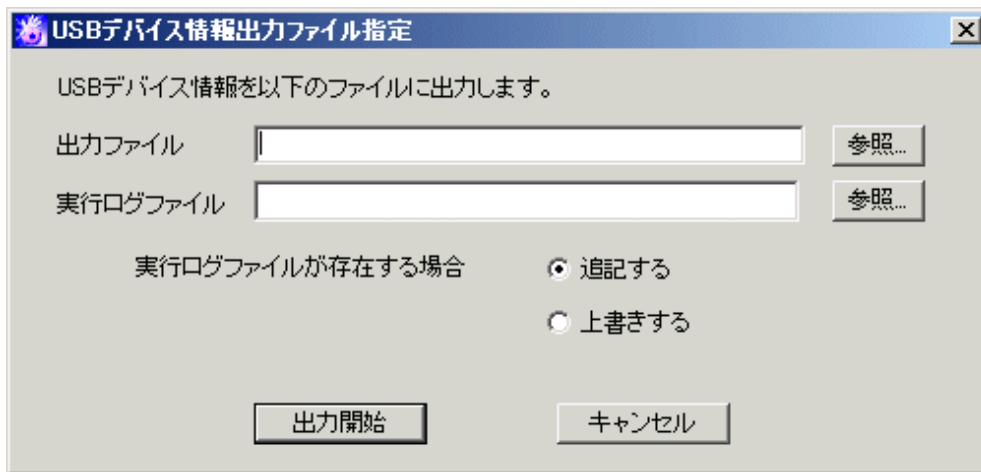
- After the import of the USB device information has completed, “Registration Completed” will be displayed in [Process Status]. Click the [OK] button.

### Export registered USB device information as CSV file.

- Start [Management Console] and the [USB Device Registration] window is displayed.

2. Click the [File Export] button.

→ The [USB Device Information Output File Specified] window is displayed.



- **[Output File]** (Required): specify the CSV file for exporting USB device information with full path.  
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in file name.  
The symbols not allowed: “\” “/” “:” “\*” “?” “” “<” “>” “|”
- **[Result log file]** (Required): specify the file for exporting execution results with full path.  
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in file name.  
The symbols that not allowed: “\” “/” “:” “\*” “?” “” “<” “>” “|”
- **[When the result log file exists]**: please make sure to set when the original result log file exists.  
**[Add]**: select when the file is added to the original result log file.  
**[Overwrite]**: select when the file overwrites the original result log file.

3. Set the above-mentioned information and click the [Start Export] button.

4. The message is displayed after export has completed, click the [OK] button.

## Modify the registered USB device information

Use the CSV file that exports the registered USB device information to perform the following operations:

- Modify the USB device name, notes or identification method of the registered USB device information.
- Delete the registered USB device information.
- Move the USB device information to another Management Server.

The procedure is as follows:

1. Click the [File Export] button to export the USB device information as CSV file.  
For information on how to do so, please refer to “[Export registered USB device information as CSV file.](#)”.
2. Modify the contents of the CSV file if needed.

Please enter the CSV file as text file to edit. After editing with software such as Microsoft® Excel, some necessary information such as double quotation marks may be lost.

The first item of each line in the CSV file output by Step 1 is blank. Under this status, when importing USB device information to the same Management Server, the information will be added as “Newly Added” information. When “Product match” is specified in the identification method, the same information will be registered several times. Therefore, to avoid registering information repeatedly, it is recommended to delete the lines not to be modified or deleted before importing to Management Server.

For details of the CSV file, please refer to “USB Device List File” of “Systemwalker Desktop Keeper Reference Manual”.



### Modify USB device name, notes or identification method

- a. Specify “U” in the first item (process flag).
- b. Modify the USB device name, notes or identification method. When importing the CSV file, all items should be recorded. Please do not modify the item apart from the USB device name, notes or identification method.

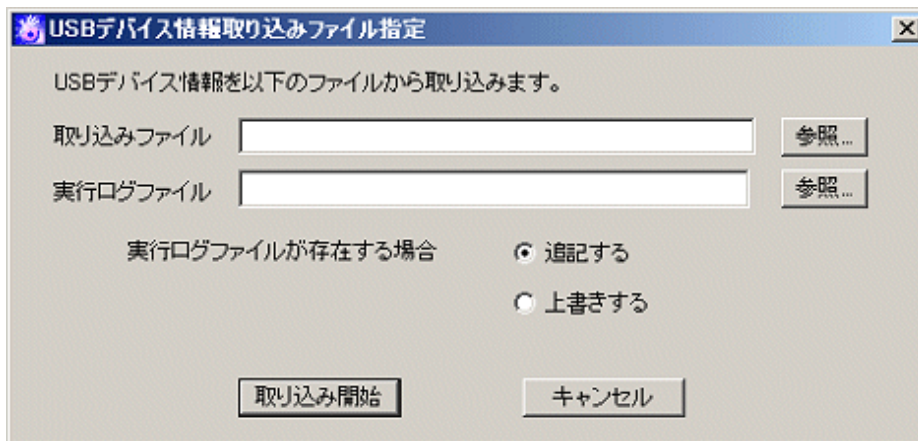
### Delete USB device information

- a. Specify “D” in the first item (process flag).
- b. Confirm that the second item (GUID) is specified.

### Move USB device information to another Management Server.

When modifying the USB device information registered on the moved Management Server, please refer to “[Modify USB device name, notes or identification method](#)” or “[Delete USB device information](#)”.

3. Save the CSV file.
4. In the Management Server that imports USB device information, click the [Import File] button.  
→ The [Specify the File for Importing USB Device Information] window is displayed.



- **[Import File]** (Required): specify the USB device list file with full path.  
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in file name.  
The symbols not allowed: “\” “/” “:” “\*” “?” “|” “<” “>” “|”
- **[Result log file]** (Required): specify and save the file of execution results with full path.  
Up to 218 single-byte characters can be entered. However, the following symbols are not allowed in file name.  
The symbols not allowed: “\” “/” “:” “\*” “?” “|” “<” “>” “|”
- **[When the result log file exists]**: please make sure to set when the original result log file exists.  
**[Add]**: select when adding to the original result log file.  
**[Overwrite]**: select when overwriting the original result log file.



- When executing regular backup of logs manually using backup tool (GUI)

In the [Backup Tool] window of [Backup Tool], modify [Backup object period] or [Deletion object period].

- When executing regular backup of logs automatically using scheduler

Modify the corresponding period through the parameter of registered command.

For information on how to consider the log saving period and timing for log backup, please refer to “Determine How to Use Logs” of “Systemwalker Desktop Keeper Installation Guide”.

For details of setting items of the backup tool, commands to be used, change procedures, etc., please refer to “Backup User Asset” of “Systemwalker Desktop Keeper Installation Guide”.

## 7.7 Change CT Environment

---

### 7.7.1 Change Management Server/Master Management Server To Be Connected

---

This section describes how to change the IP address of a (Master) Management Server to be connected and backup (Master) Management Server with the change of service environment as follows:

- Construct a new Management Server and move all the clients (CTs) that belong to the old Management Server to the new Management Server for management.
- Move part of the clients (CTs) that belong to the Management Server to other existing Management Servers.
- Change the IP address of the Management Server (backup Management Server) to be connected.
- Change the IP address of the Management Server (backup Management Server) to be connected and the client (CT).

There are following two methods to change the IP address of the Management Server to be connected.

- Change the IP address using files in the Management Server

This can be performed when the version of the client (CT) that requires a change of settings is V14.2.0 or later.

The “File To Be Moved” can be used to set the IP address of the Management Server after moving, the IP address of the corresponding client (CT) and the date of moving, etc., and can save them to the Management Server. The setting content will be notified to the client (CT) as CT policy. By restarting the PC after notification, the Management Server to be connected will be modified.

It is not required to change in each client (CT).

The communication port number used between client (CT) and the Management Server can also be modified at the same time.

- Change the IP address using command in the client (CT).

Change of settings can be performed in client (CT) of any version.

Execute command in each client (CT).

#### Change IP address using files in Management Server

This section describes how to change IP address in Management Server.

Construct a new Management Server and move all clients (CTs) that belong to the old Management Server to the new Management Server for management.

When this method is used, the management information and logs of old Management Servers will be moved to the new Management Server. Therefore, after they are moved to the new Management Server, the collected logs can also be searched in the old Management Server.

The procedure of moving is as follows:

1. Construct a new Management Server. For details of the procedure, please refer to “Systemwalker Desktop Keeper Installation Guide”.
2. Install and update the Management Server that is connected to the old Management Server and add the IP address of the new Management Server. For details of the procedure, please refer to “[7.8 Change Management Console Environment](#)”.

Based on this, the Management Console can be connected to both the old Management Server and the new Management Server temporarily.

3. Backup management information on the old Management Server.  
For management information, please refer to "User Asset" of "Systemwalker Desktop Keeper Installation Guide".
4. Restore management information to the new Management Server.
5. Change server information (Computer name, IP address) in the [Server Information Settings] window of the Server Settings Tool of the new Management Server.

The IP address will be modified as a value set in the "Server IP Address (CT Management Server)" of the information file to be moved. When the computer name is the same as the old Management Server, no change is required.

For details, please refer to "Set Server Information" of "Systemwalker Desktop Keeper Installation Guide".

6. Create the information file to be moved (DTKServerChange.txt) and save the file to the old Management Server.  
For details of the information file to be moved, please refer to "Information File To Be Moved" of "Systemwalker Desktop Keeper Reference Manual".

Location for saving

Under environment apart from Windows Server® 2008

```
C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper
```

Under Windows Server® 2008 environment

```
C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper
```

→When the client (CT) is started or immediate update is performed by the Management Console, the setting content will be notified to the client (CT) as CT policy.

The result of notification will be output to the following location of the old Management Server as information file to be moved and result log (DTKServerChange.log).

Under environment apart from Windows Server® 2008

```
C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper
```

Under Windows Server® 2008 environment

```
C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper
```

→After the client (CT) has been restarted, the Management Server to be connected to the client (CT) will be modified according to the specified content of the information file to be moved.

The change status of the Management Server to be connected can be confirmed according to the following:

- a. Start the Management Console and connect to the old Management Server.
  - b. Confirm that the [Last Logon Date and Time] of CT list is not updated.
  - c. Change the connection of the Management Console to a new Management Server.
  - d. Confirm that the corresponding client (CT) will be displayed in the configuration information tree and the [Last Logon Date and Time] of CT list has been updated.
7. After changes in all clients (CTs) have been completed, backup all logs of the old Management Server.
  8. Restore the logs to the database of the new Management Server.

Move part of clients (CTs) that belong to Management Server to other existing Management Server.

When this method is used, the moved client (CT) will be registered again on the Management Server of moving target.

Please do not move the management information and logs of the Management Server of moving source to a Management Server of the moving target. Otherwise, the client (CT) may not be managed correctly due to repeating management information.

The procedure of moving is as follows:

1. Create the information file to be moved (DTKServerChange.txt) and save the file to the Management Server of moving source. For details of the information file to be moved, please refer to “Information File To Be Moved” of “Systemwalker Desktop Keeper Reference Manual”.

Location for Saving

Under environment apart from Windows Server® 2008

```
C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper
```

Under Windows Server® 2008 environment

```
C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper
```

→When the client (CT) is started or immediate update is performed through the Management Console, the setting contents will be notified to client (CT) as CT policy.

The result of notification will be output to the following location of the old Management Server as information file to be moved and result log (DTKServerChange.log).

Under environment apart from Windows Server® 2008

```
C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper
```

Under Windows Server® 2008 environment

```
C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper
```

→After the client (CT) has been restarted, the Management Server to be connected to the client (CT) will be modified according to the specified content of information file to be moved.

The change status of the Management Server to be connected can be confirmed according to the following.

- a. Start the Management Console that connects to the Management Server of moving source or the moving target.
  - b. In the Management Console of the Management Server of moving source, confirm that [Last Logon Date and Time] of CT list is not updated.
  - c. In the Management Console of the Management Server of the moving target, confirm that the corresponding client (CT) will be displayed in the configuration information tree.
2. Through the information file to be moved and result log (DTKServerChange.log), confirm that the Management Server to be connected for all clients (CTs) to be moved has been modified, and delete the information file to be moved or move it to the place apart from the location for saving.

## Change the IP address of Management Server (backup Management Server) of connection target

There must be a change of IP address due to the change of network and moving of the Management Server. It is required to confirm the date when the IP address of the Management Server is modified in advance.

The procedure of moving is as follows:

1. Create the information file (DTKServerChange.txt) to be moved and then save the file to the Management Server. Please refer to “Information File To Be Moved” of “Systemwalker Desktop Keeper Reference Manual” for details of the information file to be moved.

Location for Saving

Under environment apart from Windows Server® 2008

```
C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper
```

Under Windows Server® 2008 environment

```
C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper
```

→ When the client (CT) is started or immediate update is performed through the Management Console, the setting contents will be notified to the client (CT) as CT policy.

The result of notification will be output to the following location of the old Management Server as an information file to be moved and a result log (DTKServerChange.log).

Under environment apart from Windows Server® 2008

C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper

Under Windows Server® 2008 environment

C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper

→After the client (CT) is restarted after the modified date set in the information file to be moved, the Management Server to be connected for the client (CT) will be modified according to the settings of information file to be moved.

2. Delete the information file to be moved or move it to a place apart from the location for saving.

## Change the IP address of both Management Server (backup Management Server) to be connected and client (CT)

There must be a change in the IP address of both the Management Server and client (CT) due to the change of entire network system. Before the IP address of the Management Server is modified, the client (CT) needs to obtain the information of information file to be moved from the Management Server, and it is required to confirm the date when IP address of the Management Server is modified in advance.

The procedure of moving is as follows:

1. Create the information file to be moved (DTKServerChange.txt) and save the file to the Management Server.  
For details of the information file to be moved, please refer to “Information File To Be Moved” of “Systemwalker Desktop Keeper Reference Manual”.

Location for Saving

Under environment apart from Windows Server® 2008

C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper

Under Windows Server® 2008 environment

C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper

→When the client (CT) is started or immediate update is performed through the Management Server, the setting contents will be notified to client (CT) as CT policy.

The result of notification will be output to the following location of the old Management Server as information file to be moved and result log (DTKServerChange.log).

Under environment apart from Windows Server® 2008

C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper

Under Windows Server® 2008 environment

C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper

2. As the change of network system, the IP address of the Management Server is modified. Change the IP address of client (CT).
  - When the client (CT) is fixed IP address:  
the IP address will be set manually in each client (CT).
  - When the client (CT) is DHCP environment:  
no operation is needed.

→After the client (CT) is restarted after the change date set in the information file to be moved, the Management Server to be connected for the client (CT) will be modified according to the settings of information file to be moved.

3. Delete the information file to be moved or move it to a place apart from the location for saving.

If the CT function exists on the Management Server at the same time, this CT function will ignore these settings. For the CT on the Management Server, the Management Server can be specified as a local computer only. Therefore, for changes of IP address of the Management Server and port number for sending, etc., please change the settings through maintenance commands.

## Change IP address using commands in client (CT).



### Note

#### Please do not tell the password to others

When executing this command through the command prompt, the password may be seen by a third party or end user. When using this command, please make sure to use a batch file and perform operations with security being considered so that the password absolutely cannot be seen.

The procedure is as follows.

1. Logon to the PC with a user that belongs to the Administrators group of the local computer or a user that belongs to the Domain Admins group.
2. Execute the following command through the command prompt of the client (CT) that changes the IP address of the (Master) Management Server to be connected.

```
fsw11ej7.exe <Password> /D /D
```

<Password>:

Enter the password specified during the installation of the client (CT).

→ [IP Address of Server] displayed in the command prompt is the IP address of the (Master) Management Server that is currently connected.

3. To change the IP address of the connected (Master) Management Server or backup (Master) Management Server, execute the following command through the command prompt of client (CT).

```
fsw11ej7.exe <Password> /C /I <Modified IP Address of (Master) Management Server> <Modified IP Address of Backup (Master) Management Server>
```

<Password>:

Enter the password specified during the installation client (CT).

<Modified IP Address of (Master) Management Server>:

Enter the IP address of the (Master) Management Server that has become the connection target for the client (CT).

< Modified IP Address of Backup (Master) Management Server>:

Enter the IP address of the backup (Master) Management Server when inquiring the user policy. When the IP address is omitted, a value that is the same as < Modified IP Address of (Master) Management Server> will be set.

4. To notify CT information to the (Master) Management Server connected to the client (CT), execute the following command through the command prompt of client (CT).

```
fsw11ej7.exe <Password> /R
```

<Password>:

Enter the password specified during the installation of client (CT).

5. Restart the client (CT).

The change status of the Management Server to be connected can be confirmed according to the following.

1. Start the Management Console that connects to the (Master) Management Server of moving source or the moving target.
2. In the Management Console of the (Master) Management Server of the moving source, confirm that [Last Logon Date and Time] of CT list is not updated.
3. In the Management Console of the (Master) Management Server of the moving target, confirm that the corresponding client (CT) will be displayed in the configuration information tree.

 **Point**

**When the information of client (CT) is lost from the server, it can be restored through the command for CT re-registration (Even if overwritten installation of CT is performed, it cannot be restored.).**

When any of the following situations occur, after the CT re-registration command (fsw11ej7.exe <Password> /R) has been executed in the corresponding client (CT), client (CT) information will be registered to the (Master) Management Server again.

- When the client (CT) on Management Console is deleted by mistake, and then the IP address of Management Server is not modified.
- When the (Master) Management Server loses client (CT) information due to trouble, and then the IP address of Management Server is not Modified

Please restart the client (CT) after executing “fsw11ej7.exe <Password> /R”.

After the client (CT) information is informed to the (Master) Management Server, it will be displayed in the Management Console.

- Display location in Management Console
  - When Active Directory linkage is used  
After the client (CT) is displayed, it will be registered to the local group. After updating the Active Directory linkage information, it will be displayed in the registration location in the Active Directory server.
  - When Active Directory linkage is not used  
The client (CT) displayed again will be registered to the Root directory.
- The applied CT policy  
The policy set in the [Terminal Initial Settings] of Management Console will be applied.
- Logs of client (CT)  
The logs before deletion will not be displayed in Log Viewer.

## 7.7.2 Change Operation Settings of Client (CT)

This section describes how to change the printing monitoring mode/E-mail control mode set during the installation of client (CT) and how to change the size of log file temporarily saved in the client (CT).

The change method includes execution in the Management Server and execution in the client (CT).

Change Method		Items that can be modified	Version of Client (CT) that can be modified
Change in Management Server	Use the Information File of CT operating parameter	- Use of dial-up connection	V14.2.0 or later
		- Compatibility record of network drive	
		- Confirmation message of recipient address during E-mail sending	V14.2.0 or later
		- IP address of backup Management Server - Size of result log file - Size of prohibition log file	V14.2.0 or later



Change Method		Items that can be modified	Version of Client (CT) that can be modified
		<ul style="list-style-type: none"> <li>- Size of error log file</li> <li>- Number of days to save error log</li> <li>- Size of trace log file</li> <li>- Printing monitoring mode (*)</li> <li>- E-mail control mode <ul style="list-style-type: none"> <li>- Port number for E-mail sending monitoring</li> <li>- Monitoring mode of E-mail attachment prohibition</li> <li>- Port number for communication of E-mail attachment prohibition</li> <li>- Port number 2 for communication of E-mail attachment prohibition</li> </ul> </li> <li>- Run immediately after logon</li> </ul>	
	Change in [Terminal Operation Settings] window	<ul style="list-style-type: none"> <li>- Printing monitoring mode</li> </ul>	All versions
Change in Client (CT)	Change in [Add or Remove Programs]	<ul style="list-style-type: none"> <li>- Printing monitoring mode</li> <li>- E-mail control mode <ul style="list-style-type: none"> <li>- Port number for E-mail sending monitoring</li> <li>- Monitoring mode of E-mail attachment prohibition</li> <li>- Port number for communication of E-mail attachment prohibition</li> <li>- Port number 2 for communication of E-mail attachment prohibition</li> </ul> </li> </ul>	All versions

\* The change of printing monitoring mode through the information file of the CT operating parameter is used to temporarily change the settings of the client (CT). When the information file of CT parameter is deleted or moved to another saving location after the configuration value has been modified, it will be performed with the configuration value in the [Terminal Operation Settings] window through the next policy notification.

### Use information file of CT operating parameter

Set the modified value in information file of the CT operating parameter and save it to the Management Server. The file information will be notified to the client (CT) as CT policy. The modified content will be reflected to the client (CT) according to [Timing of reflecting set value.](#)

1. Create the information file (DTKCTSetting.txt) of CT operating parameter, and save it to the Management Server.  
For details of information file of CT operating parameter, please refer to “Information File of CT Operating Parameter” of “Systemwalker Desktop Keeper Reference Manual”.

Location for Saving

Under environment apart from Windows Server® 2008

C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper

Under Windows Server® 2008 environment

C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper

→When the client (CT) is started or immediate update is performed through the Management Console, the settings contents will be notified to client (CT) as CT policy.

The result of notification will be output to the following location as the information file of CT operating parameter or result log (DTKCTSetting.log).

Under environment apart from Windows Server® 2008

C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper

Under Windows Server® 2008 environment

C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper

→After CT policy notification, the settings will be reflected to the client (CT). The timing of reflection depends on the setting items.

#### Timing of reflecting set value

Setting Item	Timing of Reflecting the Set Value
IP Address of Backup Management Server	It will be reflected after OS is restarted. When this item is also set in the information file to be moved, its configuration value will be reflected.
Size of Result log file	It will be reflected immediately.
Size of Prohibition Log File	It will be reflected immediately.
Size of Error Log File	It will be reflected when the date is modified and new error log file is created.
Number of Days to Save Error Logs	It will be reflected when the date is modified and new error log file is created.
Size of Trace Log File	It will be reflected immediately.
Printing Monitoring Mode	It will be reflected immediately. When this item is also set in the [Terminal Operation Settings] window, the configuration value of information file of CT operating parameter will be reflected. However, after the information file of CT parameter is deleted or moved to another saving location, it will run with the value set in the [Terminal Operation Settings] window.
Port Number for E-mail Sending Monitoring	It will be reflected after OS is restarted.
Monitoring Mode of E-mail Attachment Prohibition	It will be reflected after OS is restarted.
Port Number for Communication of E-mail Attachment Prohibition	It will be reflected after OS is restarted.
Port Number 2 for Communication of E-mail Attachment Prohibition	It will be reflected after OS is restarted.
Run Immediately after Logon	It will be reflected after OS is restarted.
Message for Confirming the Recipient Address during E-mail Sending	It will be reflected after OS is restarted.
Use of Dial-up Connection	It will be reflected immediately.
Compatibility Record of Network Drive	It will be reflected immediately.

2. Confirm the configuration value that is modified.  
 In each client (CT) with modified settings, the setting information of FSW11EJ7.EXE (system maintenance) command will be displayed and the output contents will be confirmed. For details, please refer to “Display Setting Information” of “Systemwalker Desktop Keeper Reference Manual”.
3. Delete the information file of the CT operating parameter or move it to another saving location.  
 (When this file exists in the saving location, the operating environment of the client (CT) will be changed again.)

## Change in the [Terminal Operation Settings] window

Please refer to [2.4.2 Perform Terminal Operation Settings](#) for operation procedure and setting items.

The modified information notified to the client (CT) will be reflected immediately.

When the [Printing Monitoring Mode] is also set in the information file of CT operating parameter, the configuration value of the information file of the CT operating parameter will be reflected.

The content set here will be distributed to terminal at next policy distribution.

**Attached data condition settings**

Attached data accumulation settings  Server (recommended)  CT

Invalid interval of screen capture  Second(s) (Specify within 1~999, it may lead to high load on CT in case of less than 60 seconds)

Maximum number of images can be saved in CT  Windows (Specify within 10 ~999)

**Terminal Operation Settings**

Start time of logon prohibition  Prohibit after 30 seconds  Prohibit immediately

Printer increasing/decreasing monitor interval  Seconds (Specify within 15~9999)

Number of times of printing job monitoring  Times (1 time = 10 seconds, specify within 3~9)

Printing Monitor Mode  Manage printing monitor mode in Management Server

Monitor printing of all printers set in CT (recommended)

Monitor printing of local printer only

**Settings of Collective Log Sending**

Interval of Log Sending  Seconds (Specify within 60~9999)

Interval during continuous sending  Seconds (Specify within 30~9999)

Maximum number of logs can be sent at one time  Cases (Specify within 100~5000)

Communication timeout  Seconds (Specify within 30~300)

**Settings of offline log sending**

Interval of sending each item of log  Milliseconds (Specify within 50~5000)

Interval of monitoring server connection  Seconds (Specify within 30~900)

**Settings of original file backup conditions**

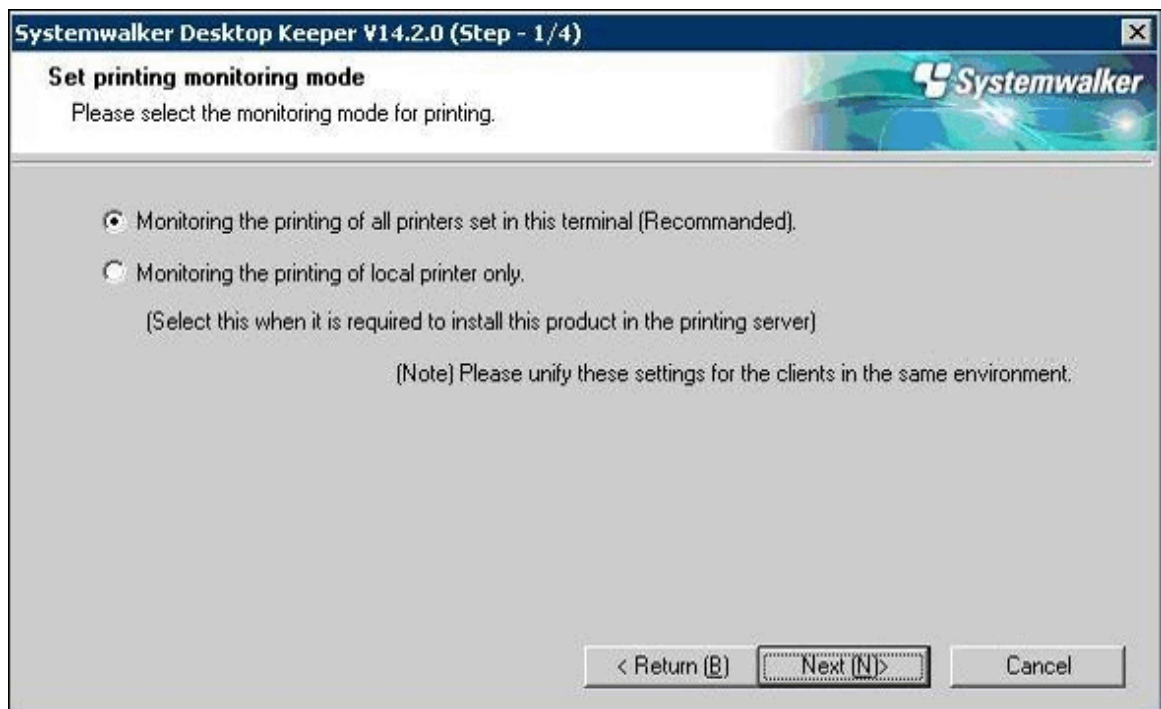
Maximum total size of original of file export  MB (Specify within 1~700)

Maximum size of a single file  MB (Specify within 1~50)

## Change in [Add or Remove Programs]

When changing the printing monitoring mode

1. Logon to the PC with a user that belongs to the Administrators group of local computer or a user that belongs to the Domain Admins group.
2. Select [Add or Remove Programs] of [Control Panel].
3. Select [Systemwalker Desktop Keeper Client ], and click the [Change] button.  
→ The installation window of CT is displayed.
4. Change the configuration value in the [Set printing monitoring mode] window.



For details of the configuration value, please refer to “Installation in Wizard Style” of “Systemwalker Desktop Keeper Installation Guide”.

## Change E-mail control mode

1. Logon to the PC with a user that belongs to the Administrators group of local computer or a user that belongs to the Domain Admins group.
2. Select [Add or Remove Programs] of [Control Panel].
3. Select [Systemwalker Desktop Keeper Client], and click the [Change] button.  
→The installation window of CT is displayed.

4. Change the configuration value of [Set E-mail Control Mode].

**Set E-mail Control Mode**  
Please enter the information related to e-mail sending and e-mail file attachment prohibition.

**E-mail Sending**  
Port Number for E-mail Sending and Monitoring: 25

**E-mail Attachment Prohibition**  
 Port Monitoring Mode (Recommended)  
Port Number for E-mail Attachment Prohibition: 10018  
Port Number 2 for E-mail Attachment Prohibition: 10019  
 V12.0L20 ~ V13.0.0 Compatible Mode

< Return (B)   Next (N)>   Cancel

For details of the configuration value, please refer to “Installation in Wizard Style” of “Systemwalker Desktop Keeper Installation Guide”.

### 7.7.3 Replace Client (CT)

When the replacement of the CT occurred due to the failure of terminal hardware that installs the client (CT), please set the (Master) Management Server and terminal according to the following procedure and to make terminal before replacement judged to be the same as that after replacement.

- Settings of the (Master) Management Server

1. Logon to the PC with a user that belongs to the Administrators group of local computer or a user that belongs to the Domain Admins group.
2. After selecting the [All Programs] - [Systemwalker Desktop Keeper] - [Server] - [Server Settings Tool] from the [Start] menu, the following window will be displayed.
3. Logon with the initial manager account.
4. Select [Stop Service] from the [Service] menu of the [Server Settings Tool] window.
5. The confirmation window for stopping service is displayed. Please click the [OK] button.
6. Click the [System Settings] button.  
→ The following window is displayed.
7. When the MAC Address, Owner and OS Type have been modified, the item modified as [Same CT determination condition when registering CT] will be modified as [Not use].
8. Click the [Set] button.
9. Select [Start Service] from the [Service] menu of the [Server Settings Tool] window.
10. The confirmation window for starting service is displayed. Please click the [OK] button.

- Settings of the terminal to install the client.

1. Please use the computer name before the change of hardware.

2. Install client (CT).

## 7.8 Change Management Console Environment

This section describes how to change the IP address or computer name of the (Master) Management Server to be connected that is set during the installation of the Management Console.

The method described here is the procedure when the IP address or computer name of connection target server of the Management Console is modified if the Management Console has already been installed.

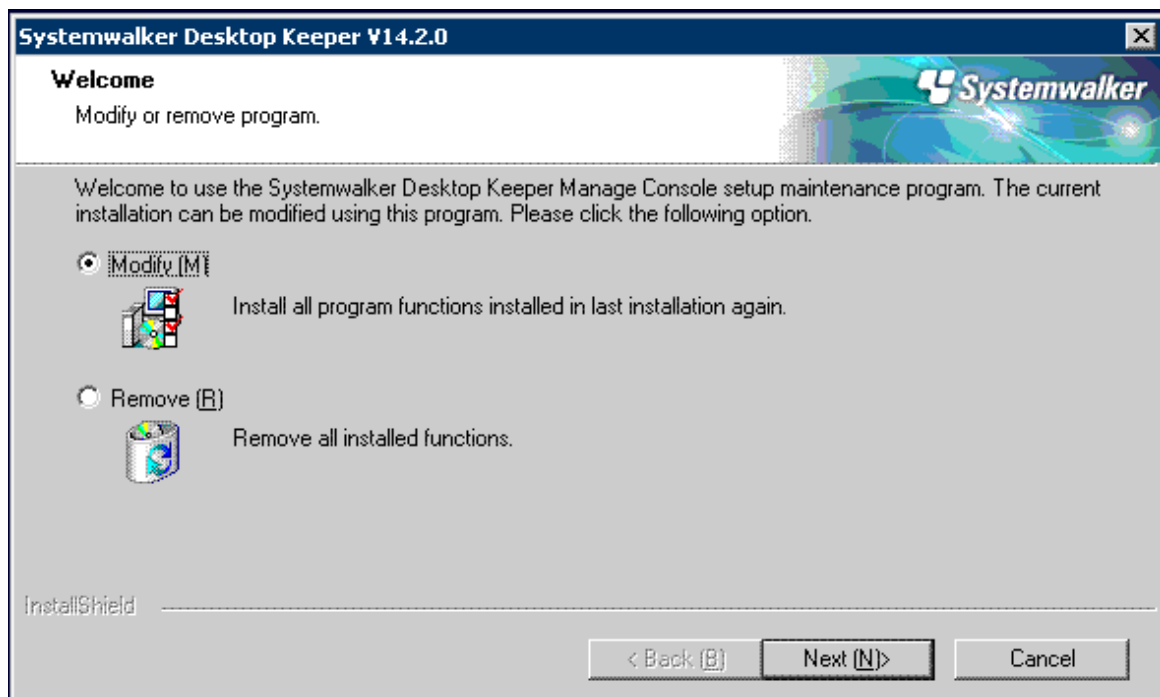
Before the procedure is started, it is required to complete the change of environment of the Management Server and the Management Console according to “[7.9.4 Change System Environment with the Change of IP Address/Computer Name of Management Server/Master Management Server](#)”.

In addition, in the case of specifying the computer name when changing the (Master) Management Server to be connected, please confirm that the name has been analyzed first.

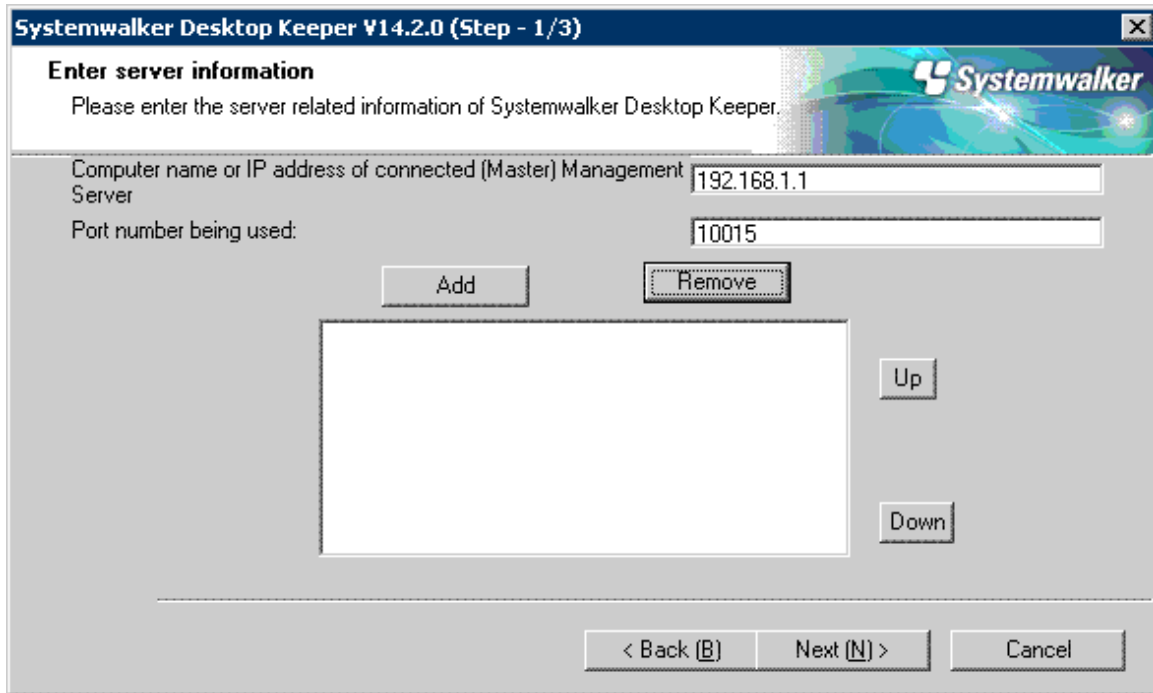
The procedure is as follows.

1. Logon to the PC with a user that belongs to the Administrators group of local computer or a user that belongs to the Domain Admins group.
2. Insert the setup disk. When the installer is not started, start “swsetup.exe” of the drive with setup disk inserted.
3. Select [Management Console Installation].

→ The following window is displayed.



4. Select [Modify] and click the [Next] button.  
→ The following window is displayed.



5. Change the computer name or IP address.

**[When Adding New Computer Name or IP Address]**

- a. Set [Computer name or IP address of connected (Master) Management Server].
- b. Set the [Port number being used].
- c. Click the [Add] button.

**[When Deleting the Set Computer Name or IP Address]**

- a. Select the “Computer name or IP address of connected (Master) Management Server: Port number being used” to be deleted.
- b. Click the [Remove] button.

**[When Changing the Computer Name or IP Address that has been Set]**

- a. Select the “Computer name or IP address of connected (Master) Management Server: Port number being used” to be modified.
- b. Click the [Remove] button.
- c. Set the [Computer name or IP address of connected (Master) Management Server].
- d. Set the [Port number being used].
- e. Click the [Add] button.

6. Click the [Next] button.
7. Click the [Install] button.
8. Click the [Finish] button.
9. When requested to restart the PC after the installation has completed, please restart.
  - During installation with overwriting when the Management Console has been started

## 7.9 Change Management Server Environment

---

This section describes how to change the Management Server environment.

It can be changed through the Server Settings Tool.

### 7.9.1 Start Server Settings Tool

---

#### Start Server Settings Tool

1. Logon to a PC with a user who belongs to the Administrators group of the local computer or one who belongs to the Domain Admins group.
2. Select [All Program] -[Systemwalker Desktop Keeper] - [Server] - [Server Settings Tool] from the [Start] menu.  
→ The [Systemwalker Desktop Keeper - Server Settings Tool] window is displayed.

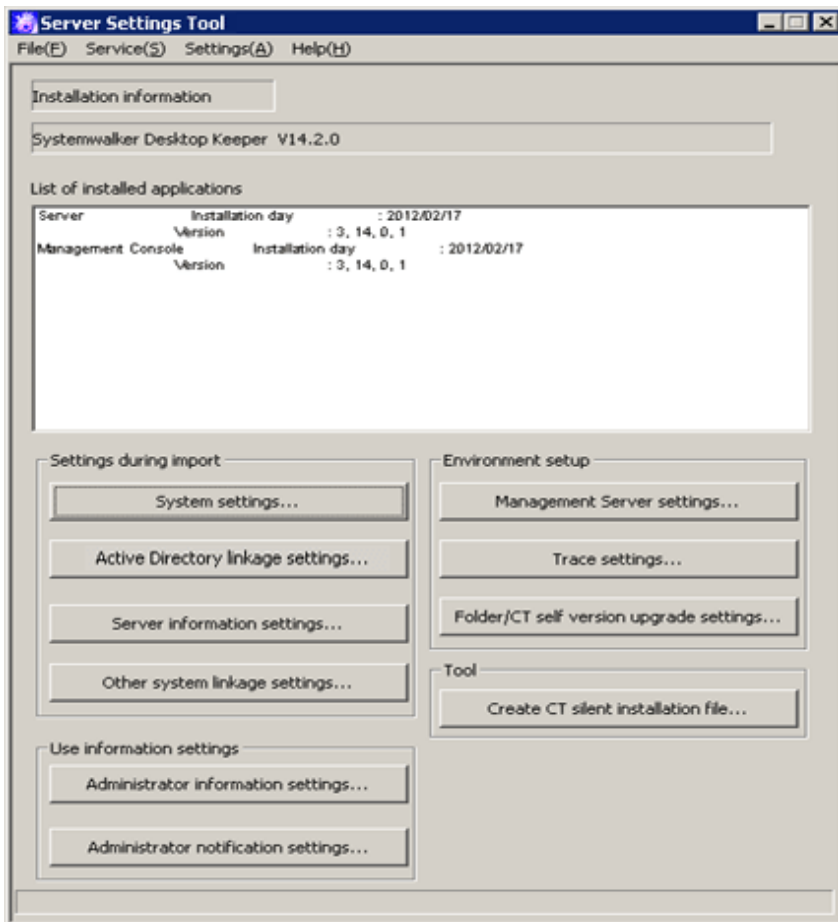


3. Logon with the initial administrator account. The account of the initial administrator is as follows:
  - **[User ID]:** SecureAdmin
  - **[Password]:** the password specified during the installation of Management Server and Master Management Server.It is recommended to change the password regularly. For information on how to do so, please refer to "[7.9.2 Change Password of Initial Administrator](#)".

Though logon with a user (access authority of Management Console is required) registered through the Server Settings Tool is also permitted, the functions that can be used are limited to "Administrator Notification Settings".



4. Click the [OK] button.  
 → The [Server Settings Tool] window is displayed.



#### Display content of window

This section describes the visible column(s) in the [Server Settings] window.

Item Name	Description
[Installation information]	The version of installed product will be displayed.
[List of installed applications]	<p>The installation date and version of installation application of each Systemwalker Desktop Keeper will be displayed.</p> <ul style="list-style-type: none"> <li>- Installed application              The following applications will be displayed when they are installed.             <ul style="list-style-type: none"> <li>- Management Server/Master Management Server (Name displayed: Server)</li> <li>- Management Console (Name displayed: Management Console)</li> </ul> </li> <li>- Installation date (The installation date will be displayed in the format of mm/dd/yyyy)</li> <li>- Version of installed application</li> </ul>
[Settings during import]	<p>[System settings...]</p> <p>Display the [System Settings] window.              Set all operations of the Master Management Server and Management Server.</p>

Item Name		Description
	[Active Directory linkage settings···]	Display the [Active Directory Linkage Settings] window. Register the domain server linked with the Master Management Server and Management Server.
	[Server information settings···]	Display the [Server Information Settings] window. Set the server information.
	[Other system linkage settings···]	Display the [Other System Linkage Settings] window. Perform the setting of automatically importing the configuration information of Systemwalker Desktop Patrol.
[Use information settings]	[Administrator information settings..]	Display the [Administrator Information Settings] window. Perform the following settings: <ul style="list-style-type: none"> <li>- Authentication user of Management Console, Log Viewer, Backup Tool, Restoration Tool and Report Output Tool</li> <li>- Department administrator</li> <li>- Authority given to the above mentioned registrants</li> </ul>
	[Administrator notification settings···]	Display the [Administrator Notification Settings] window. Set the method to notify the administrator when violation operation is detected.
[Environment setup]	[Management Server settings···]	Display the [Management Server Settings] window. Set the communication environment of Management Server.
	[Trace settings···]	Display the [Trace Settings] window. Perform the setting of trace.
	[Folder/CT self version upgrade settings···]	Display the [Folder/CT Self Version Upgrade Settings] window. Perform the setting of CT self version upgrade and folder.
[Tool]	[Create CT silent installation file···]	Display the [Create CT Silent Installation File] window. Set the conditions of silent installation.

## Menu bar

This section describes the menu bar of the [Server Settings Tool] window.

Menu Bar		Function Summary
[File]	[End]	Exit Server Settings Tool.
[Service]	[Confirm Service Status]	Display the operating status of [Level Control Service] and [Server Service] on the connected Management Server.
	[Start Service]	The [Level Control Service] and [Server Service] on the connected Management Server can be started.
	[Stop Service]	The [Level Control Service] and [Server Service] on the connected Management Server can be stopped.
[Settings]	[Execute Active Directory Linkage]	Perform the process of Active Directory Linkage.
	[Excute Systemwalker Desktop Patrol Linkage]	
	[Change Password]	Change the password of the initial administrator.  Please specify the password with no more than 32 single-byte alphanumeric characters and symbols.



[Administrator Notification Settings] window

Action when detecting the prohibition logs			
	E-mail notification to administrator	Write event log	
Application startup prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Printing prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Logon prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
PrintScreen key prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
E-mail attachment prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
FTP operation prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Web operation prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Clipboard operation prohibition	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Linkage application log violation	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Device configuration change log violation	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	

Action when the space is insufficient			
	E-mail notification to administrator	Write event log	Threshold value when the space is insufficient
Notification when DB space is insufficient	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="text" value="5"/> % Insufficient (1~20)
Notification when the disk space is insufficient (The second notification will not be performed within the notification days.)	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="text" value="3"/> % Insufficient (1~20) or <input type="text" value=""/> MB not reached (100~99999)

Monitoring action of CT			
	E-mail notification to administrator	Write event log	Notification
When the deviation exceeding the reference time exists	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="text" value="60"/> (30~999)
Notification when the client information is abnormal	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	
CT notification being collected and traced	<input type="radio"/> Yes <input checked="" type="radio"/> No	<input type="radio"/> Yes <input checked="" type="radio"/> No	

Other

## 7.9.4 Change System Environment with the Change of IP Address/Computer Name of Management Server/Master Management Server

This section describes how to change the Management Server/Master Management Server using the Server Settings Tool of Systemwalker Desktop Keeper when the IP address or computer name of the Management Server/Master Management Server is changed.

It describes the following conditions:

- When changing the environment of Master Management Server in a 3-level structure or Management Server in a 2-level structure
- When only the Management Server environment in a 3-level structure is changed
- When changing the environment of Master Management Server in 3-level structure and the Management Server that belongs to the Master Management Server



Note

[About Time Frame of Changing System Environment]

When changing the environment, it is necessary to stop the operation of the Management Server and Master Management Server. Therefore, in order not to affect business, please operate in the time frame when there are fewer users.

[About Viewing of Server Information]

When the information is incomplete under a 3-level structure, please do not view the information of subordinate Management Servers through the Master Management Server before completing the change of environment in all Management Servers and Master Management Server.

[About Consistence of Version and Edition]

When different Versions or Editions are used on the Master Management Server and Management Server, an exception will occur in the data linkage, which will lead to abnormal operation. In addition, please make sure that the Version or Edition of Management Console and Log Viewer are the same as those of the Master Management Server and Management Server.

[About Reflection of Change for Log Analyzer Server]

When the Log Analyzer Server is installed, it will take some time to automatically reflect the changes of Management Server/Master Management Server to Log Analyzer Server.

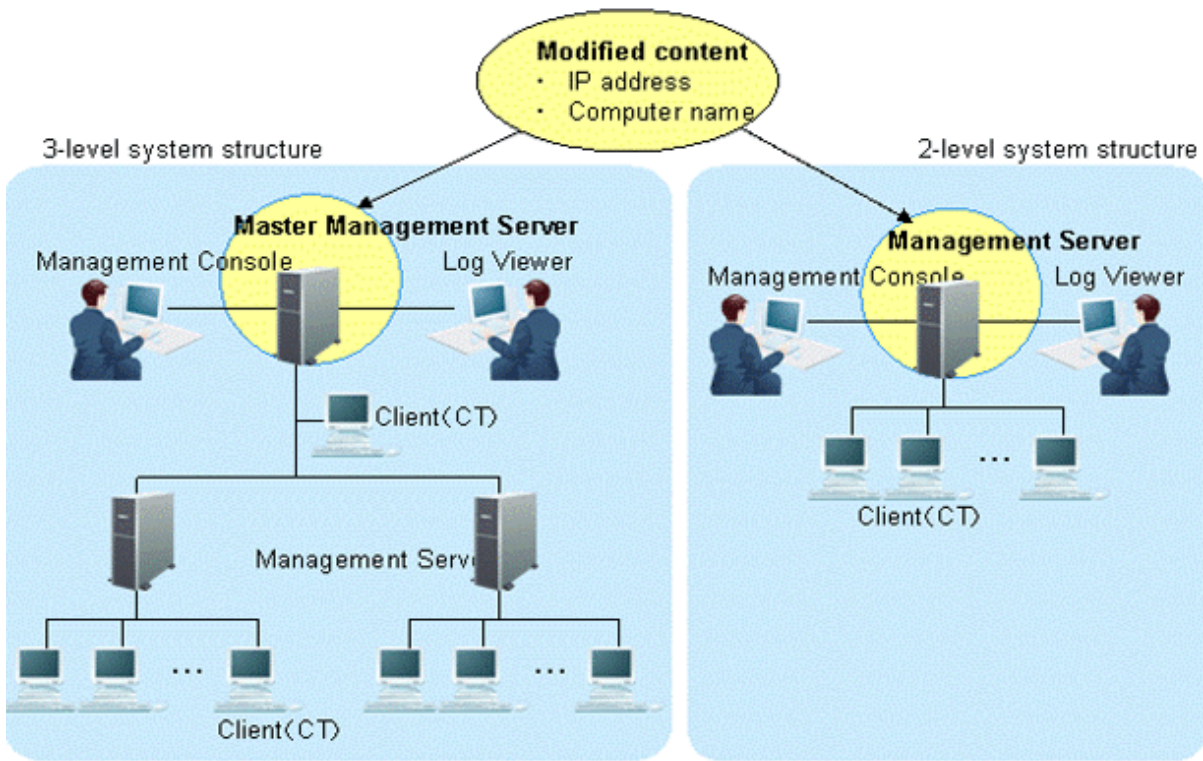
During the reflection period, the Log Analyzer of Web Console cannot be used. If you wish to use the Log Analyzer after changes are reflected immediately, please reflect according to “Transfer Administrator Information to Log Analyzer Server” and “Register Administrator Information on Log Analyzer Server” of “Set Environment of Log Analyzer Server” in “Systemwalker Desktop Keeper Installation Guide” after changes are performed.

In addition, after the log data and administrator information of the Management Server/Master Management Server before change has been transferred, the administrator information will return to the old status. Therefore, the Log Analyzer of Web Console cannot be used. In this case, please transfer the data and information from the changed Management Server/Master Management Server and register the administrator information.

In addition, when it is planned to transfer the information and data from the Management Server/Master Management Server before change, please cancel the transfer plan.



**When changing the environment of Master Management Server in a 3-level structure or Management Server in a 2-level structure**



This section describes how to change the environment of the Management Server/Master Management Server when the following information is changed on the Master Management Server in a 3-level structure or Management Server in a 2-level structure.

- IP address
- Computer name

After changing the environment of the Management Server or Master Management Server, the information required for returning to the original environment will not be saved. To return to the original environment, it is suggested to manage the node information (node name, computer name, IP address and server classification) according to the procedure.

The procedure is as follows.

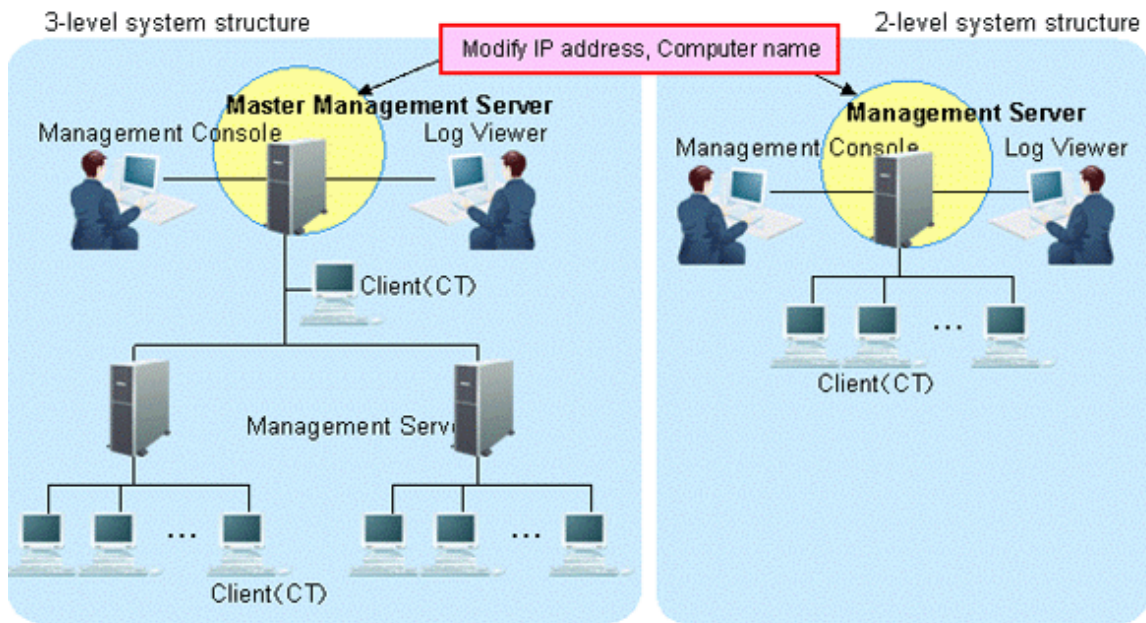
1. Stop the level control service and server service.



Under a 3-level structure, the Master Management Server and all Management Servers that belong to the Master Management Server can be stopped. (Start stopping from the Management Server.)

- a. Start [Server Settings Tool].
- b. Select [Stop service] from the [Service] menu.

2. Change IP address and computer name.

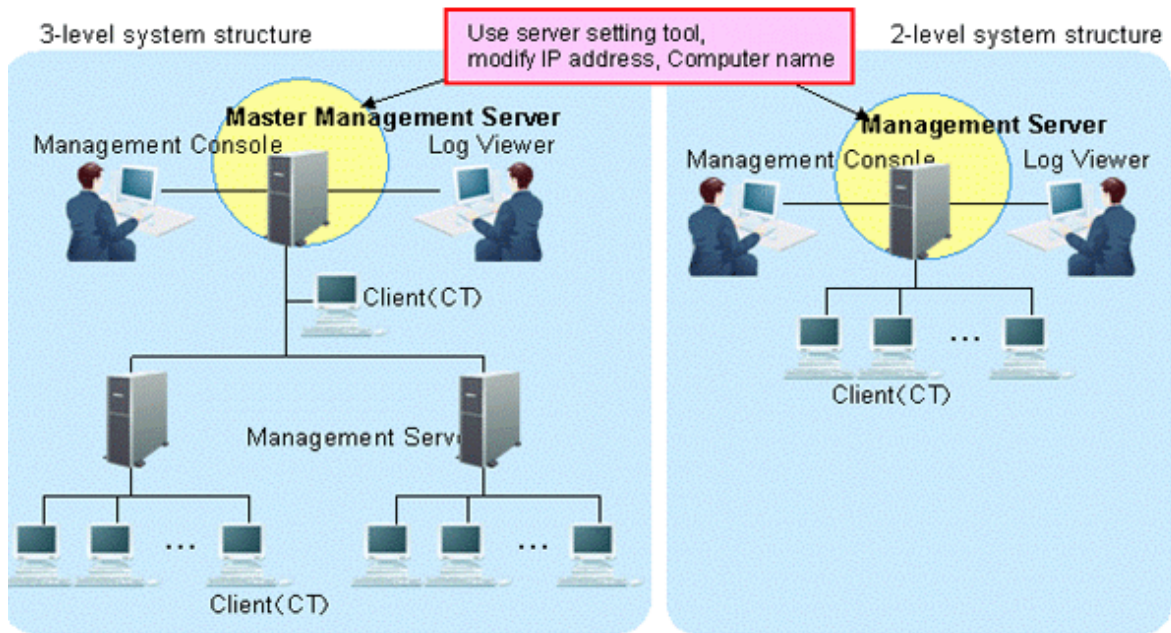


The targets are the Master Management Servers in a 3-level structure or the Management Servers in a 2-level structure. The settings of the computer itself can be modified.

- a. Modify the IP address. When it is not required to modify the IP address, please proceed to the next step.
  1. Select [Control Panel] - [Network Connection] - [Local Area Connection] from the [Start] menu. Click the [Properties] button on the [General] tab in the [Local Area Connection] window.
  2. Select [Internet Protocol] and click the [Properties] button.
  3. Modify and register the IP address.
- b. Modify the computer name. When it is not required to modify the computer name, please proceed to the next step.
  1. Select the [Control Panel] - [System] from the [Start] menu and the [Computer Name] tab of the [System Properties] window is displayed.
  2. Modify and register the computer name.
- c. Restart the server.

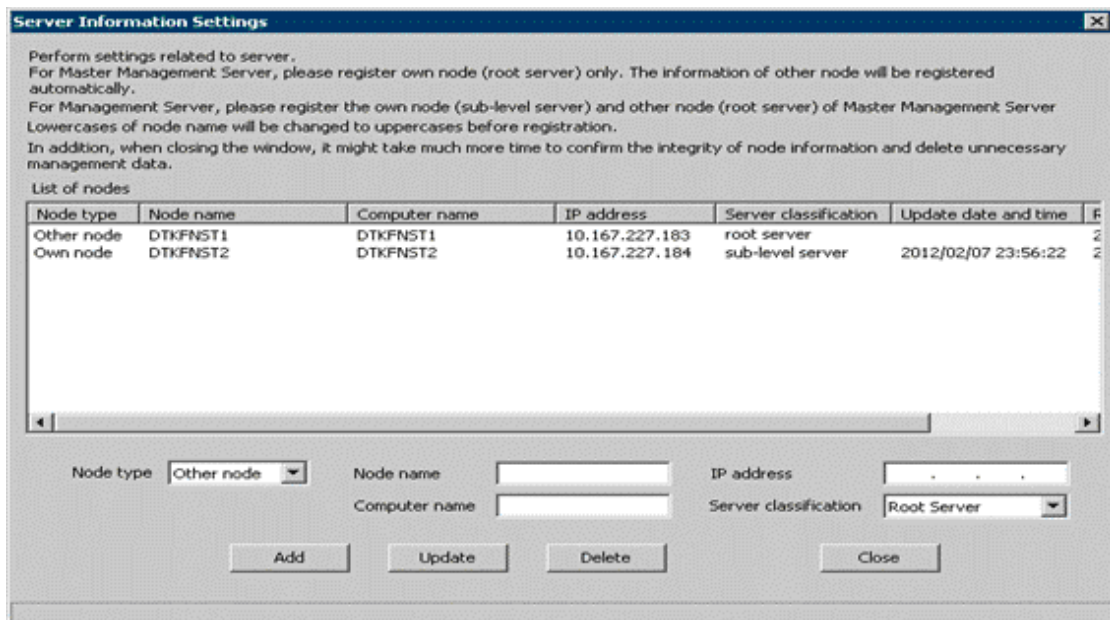


3. Change the settings of Systemwalker Desktop Keeper on Master Management Server in a 3-level structure or Management Server in a 2-level structure.



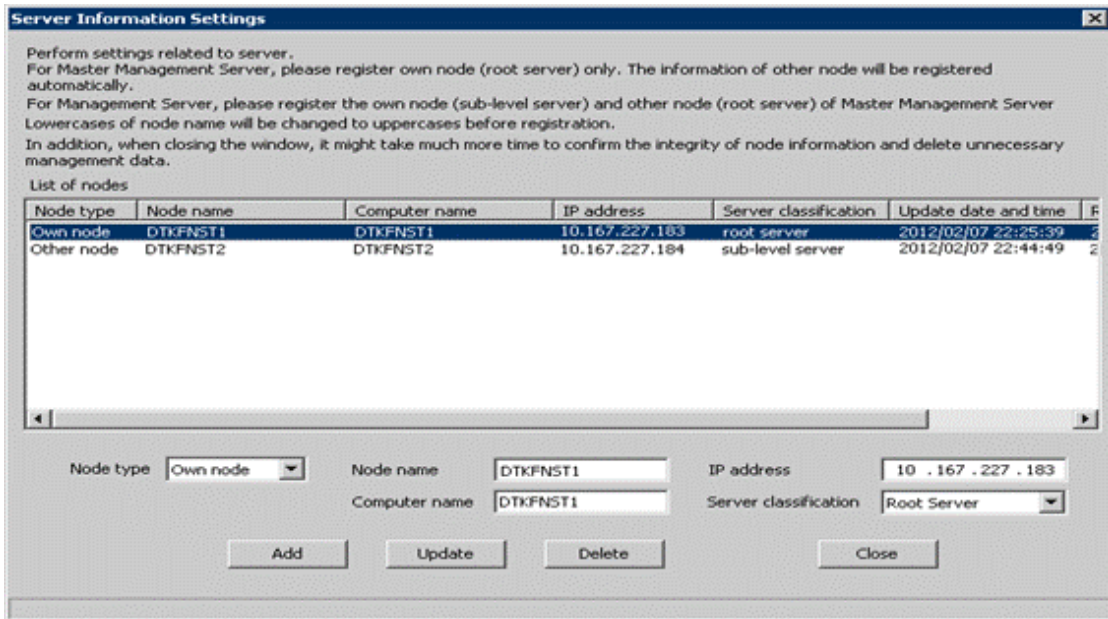
Modify the information settings of this registered server.

- a. Start Server Settings Tool.
- b. Click the [Server information settings] button.  
→ The [Server Information Settings] window is displayed.





- c. Click the data of node that is classified as self node.  
 →The information is displayed in the input field under the window.



- d. Modify [Computer name] or [IP address], click the [Update] button and click the [Close] button.



**Note**

**Please modify [Computer name] and [IP address] only.**

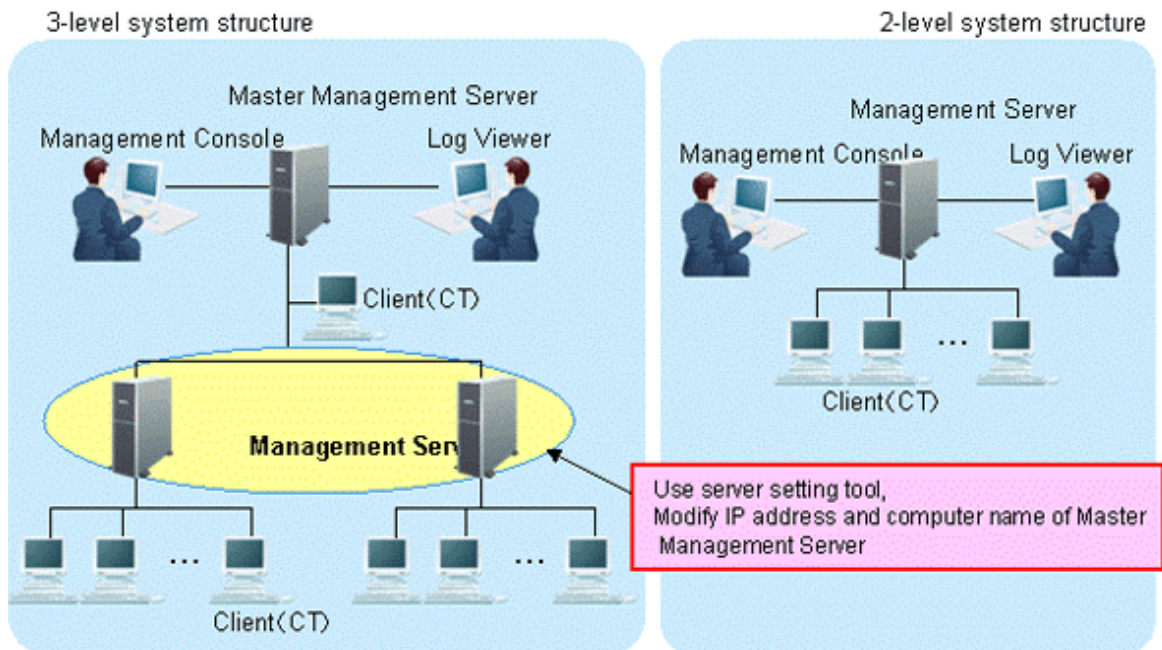
As the structure information may be inconsistent, please do not modify the value of items other than [Computer name] and [IP address].

- e. Start service.

The services of the Master Management Server in a 3-level structure or Management Server in a 2-level structure for settings change are started.

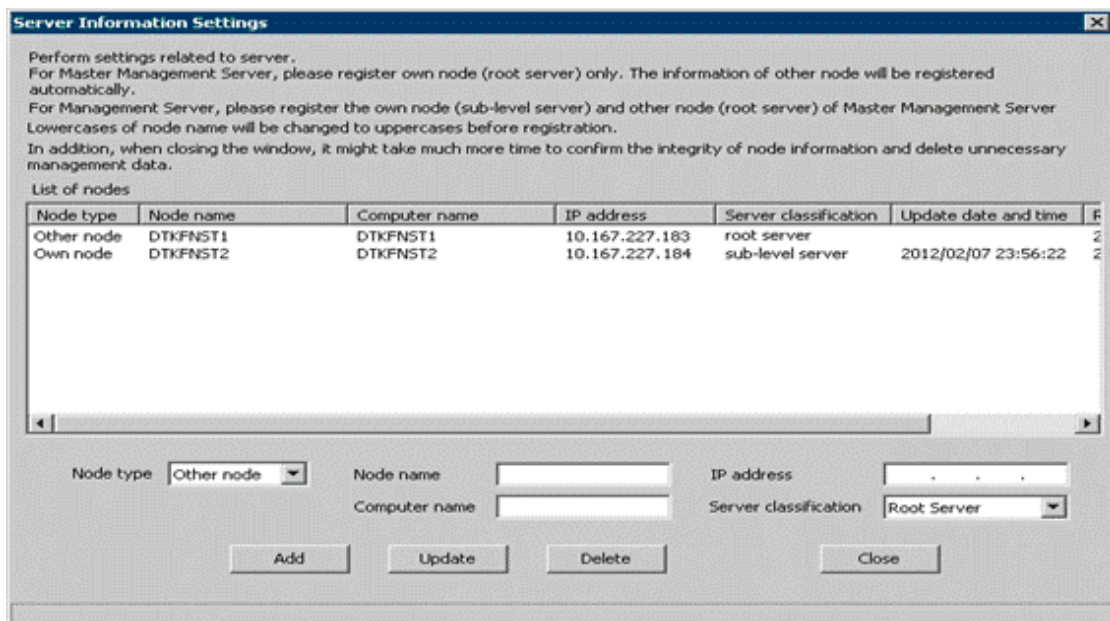
1. Start [Server Settings Tool].
2. Select [Start Service] from the [Service] menu.
3. Exit [Server Settings Tool].

4. Change the settings of Systemwalker Desktop Keeper on the Management Server that belongs to the Master Management Server in a 3-level structure (performed in a 3-level structure only).

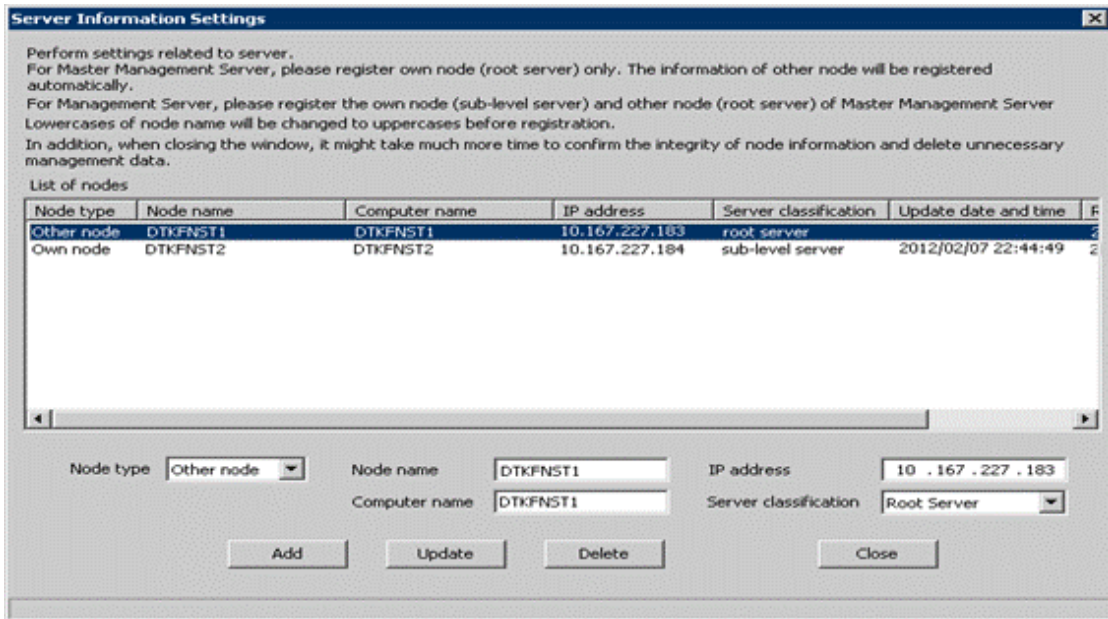


The server information settings of the Master Management Server registered on the Management Server can be changed.

- a. Start Server Settings Tool.
- b. Click the [Server information settings] button.  
→ The [Server Information Settings] window is displayed.



- c. Click the data of the node that is classified as other node (root server).  
 →The information is displayed in the input field under the window.



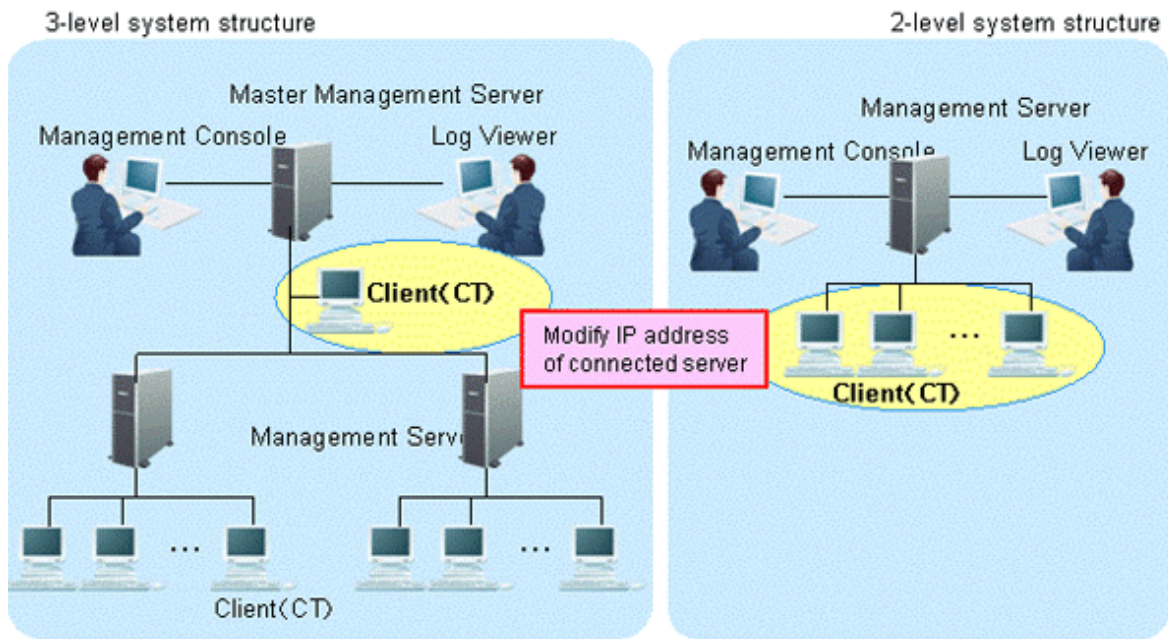
- d. Perform the following operations.
1. Check the displayed information of the other node (Node name, Computer name, IP address and Server classification).
  2. Click the [Delete] button to delete server information.
  3. Enter the following values and click the [Add] button.
    - [Node type]: Other node
    - [Node name], [Computer name] and [IP address] of Master Management Server to be modified
    - [Server classification]: Root Server
- e. Click the [Close] button.
- f. Start service.

Start the service of the Management Server that belongs to the Master Management Server in a 3-level structure.

1. Start [Server Settings Tool].
2. Select [Start Service] from the [Service] menu.



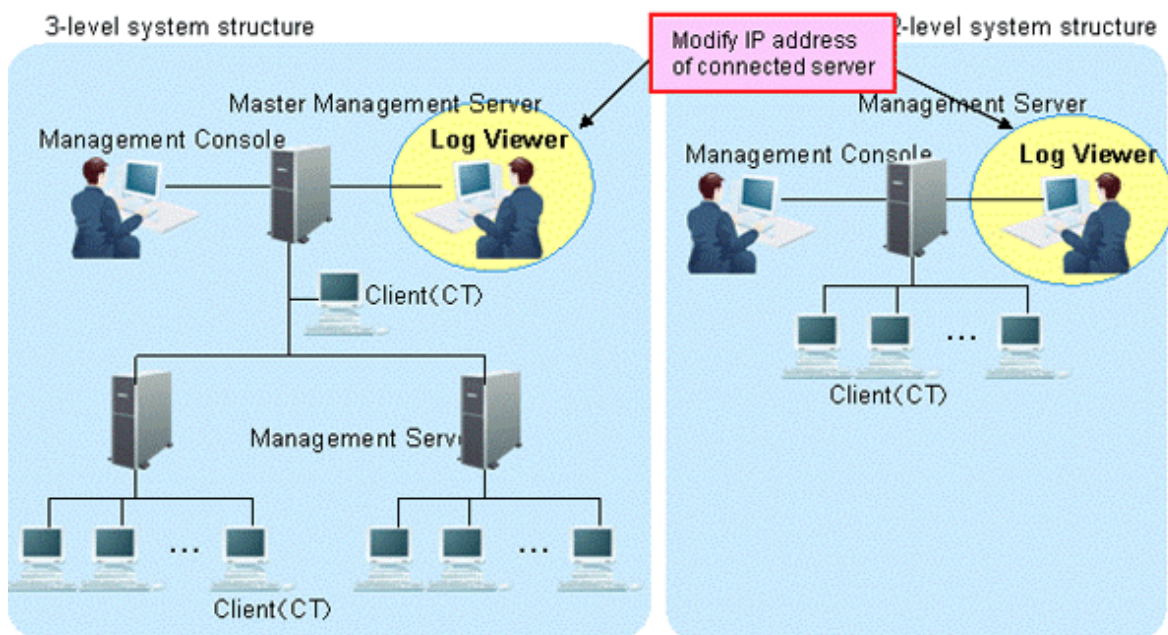
## 5. Change CT environment



For the following case, please refer to “[7.7.1 Change Management Server/Master Management Server To Be Connected](#)” and change the CT environment.

- When the IP address of the Master Management Server in a 3-level structure is modified and the client (CT) that belongs to this Master Management Server is connected
- When the IP address of the Management Server in a 2-level structure is modified and the client (CT) that belongs to this Management Server is connected

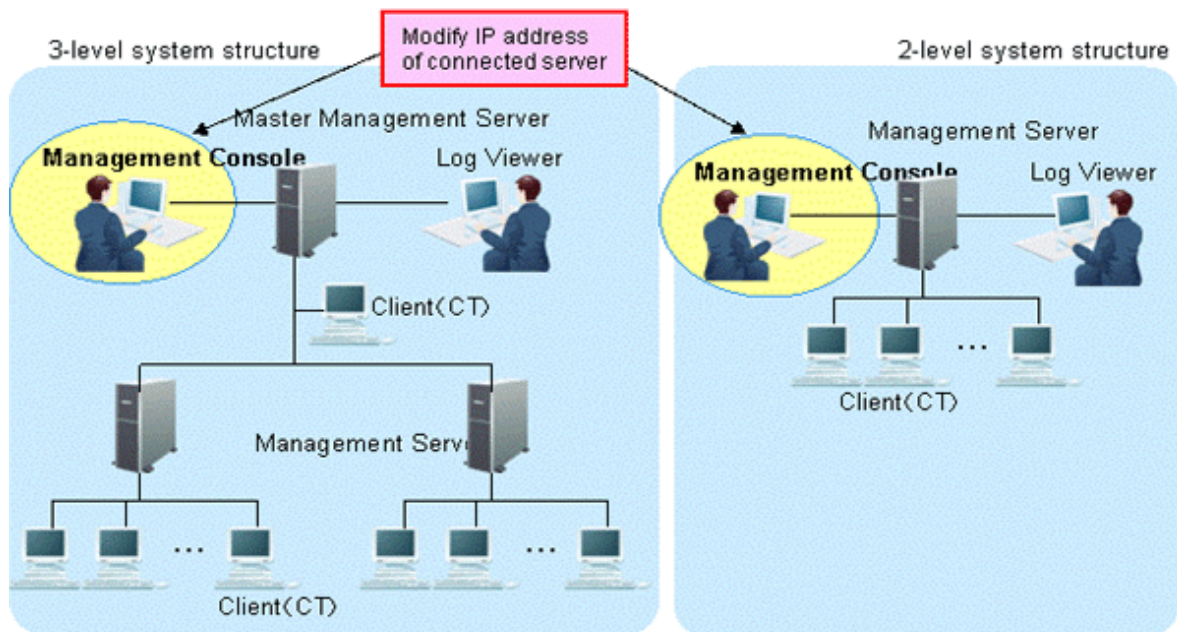
## 6. Change the Log Viewer environment



For the following cases, please refer to “[Start Log Viewer](#)” and change the Log Viewer environment.

- When the IP address of the Master Management Server in a 3-level structure is modified and the Master Management Server has been set in the connection target of Log Viewer
- When the IP address of the Management Server in a 2-level structure is modified and the Management Server has been set in the connection target of Log Viewer

## 7. Change the Management Console environment

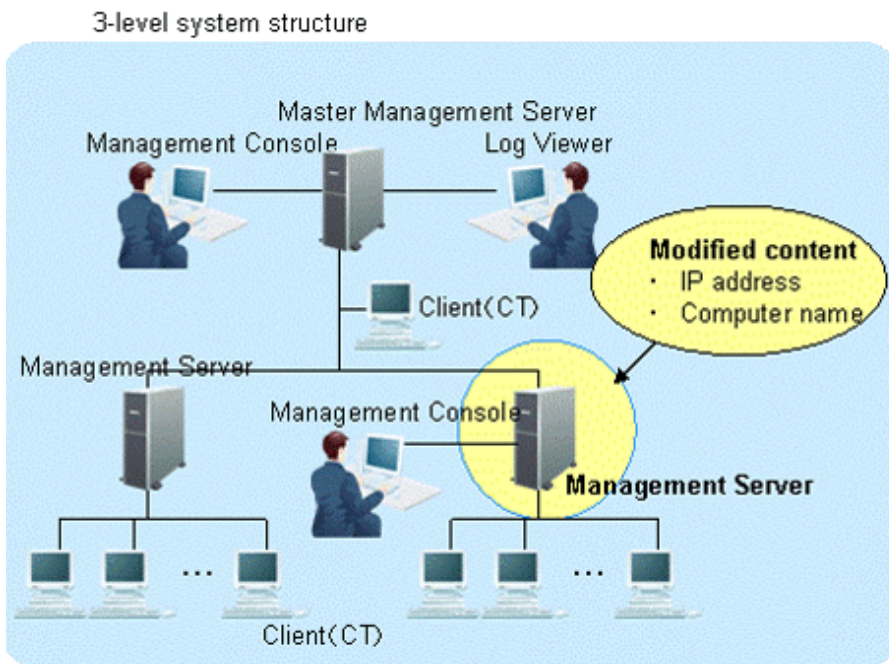


For the following cases, please refer to “7.8 Change Management Console Environment” and change the Management Console environment.

- When the IP address of the Master Management Server In a 3-level structure is changed and the Master Management Server has been set in the connection target of the Management Console
- When the IP address of the Management Server in a 2-level structure is changed and the Management Server has been set in the connection target of the Management Console



## When only the Management Server environment in a 3-level structure is changed

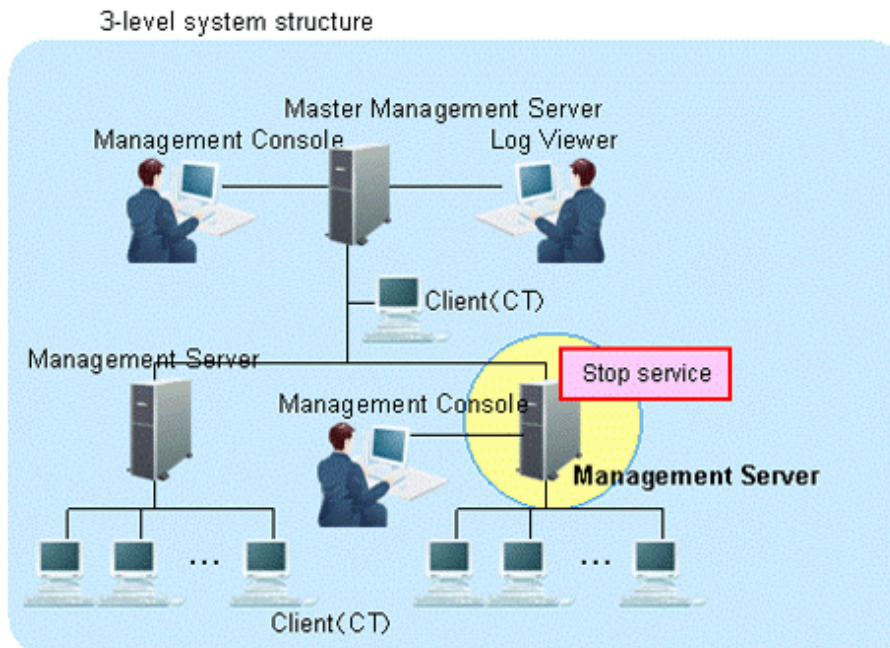


This section describes how to change the environment of the Management Server (when the Master Management Server in a 3-level structure is not changed) when the following information is modified only in the Management Server in a 3-level structure.

- IP address
- Computer name

The procedure is as follows.

1. Stop the level control service and server service.

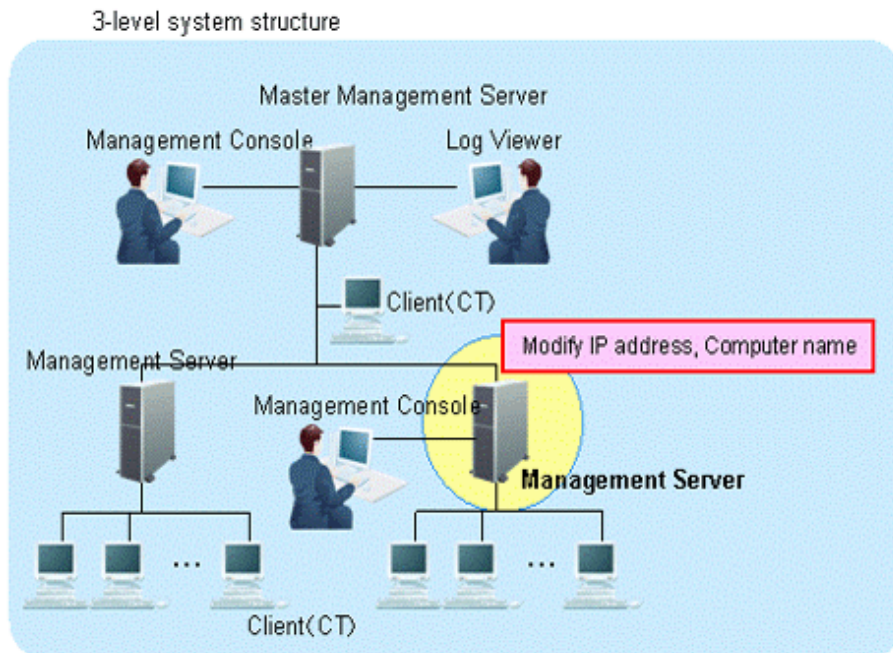


The Management Server with IP address or computer name to be modified can be stopped.

- a. Start [Server Settings Tool].

b. Select [Stop Service] from the [Service] menu.

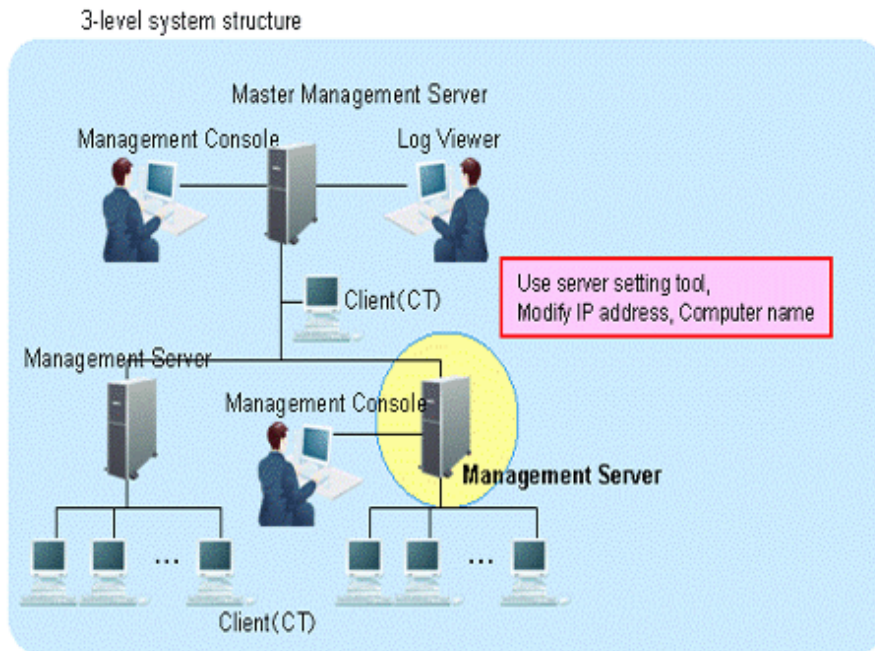
2. Modify IP address and computer name.



The target is the Management Server. Change the settings of computer itself.

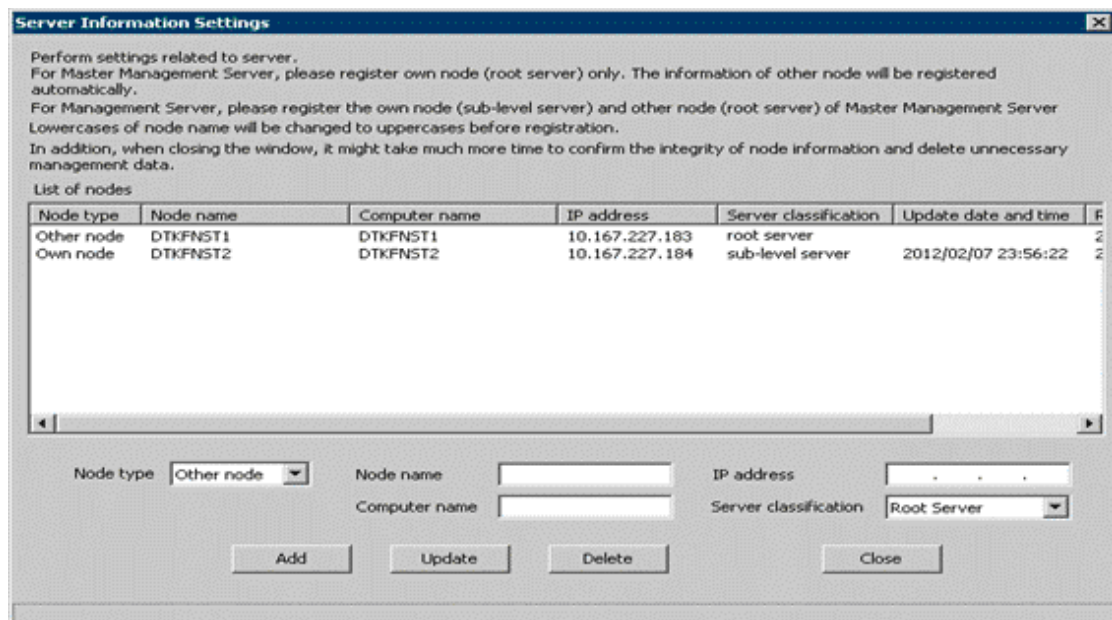
- a. Modify the IP address. When it is not required to change the IP address, please go on to the next step.
  1. Select [Control Panel] - [Network Connections] - [Local Area Connection] from the [Start] menu. Click the [Property] button on the [General] tab in the [Local Area Connection Status] window.
  2. Select the [Internet Protocol] and click the [Properties] button.
  3. Change and register the IP address.
- b. Change the computer name. When it is not required to change the computer name, please go on to the next step.
  1. Select the [Control Panel] - [System] from the [Start] menu and display the [Computer Name] tab of the [System Properties] window.
  2. Change and register the computer name.
- c. Reboot the server.

3. On the Master Management Server in a 3-level structure, change the settings of Systemwalker Desktop Keeper.



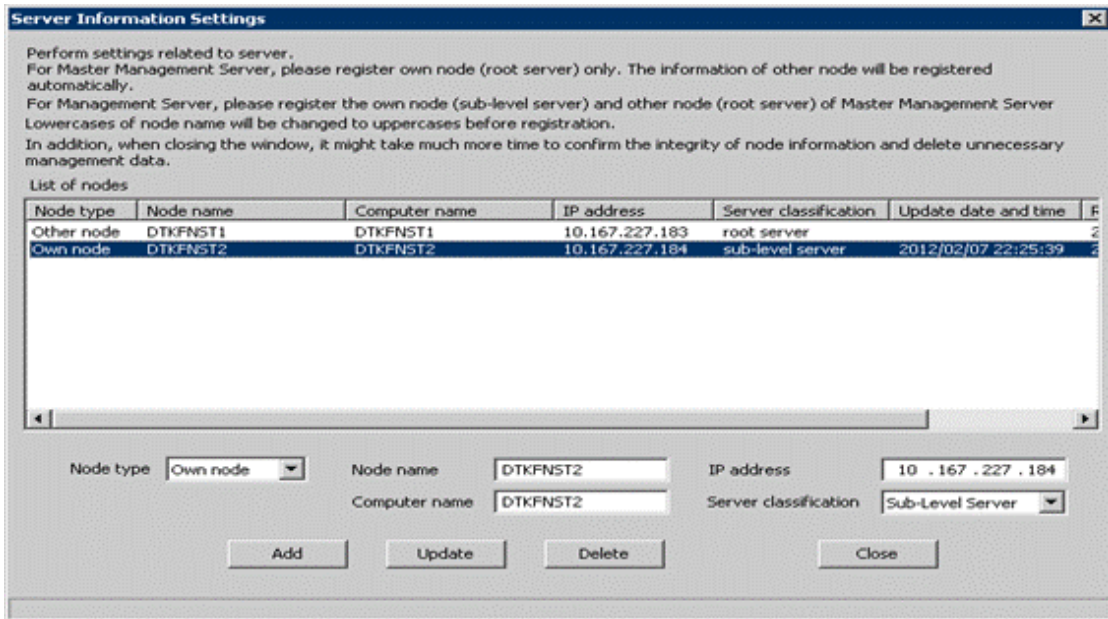
The information settings of this registered server can be changed.

- a. Start the Server Settings Tool.
- b. Click the [Server information settings] button.  
→The [Server Information Settings] window is displayed.





- c. Click the data of the node that is classified as this node (sub-level server).  
 → The information will be displayed in the input field under the window.



- d. Modify the [Computer name] or [IP address], click the [Update] button and then click the [Close] button.



### Note

**Please modify [Computer name] and [IP address] only.**

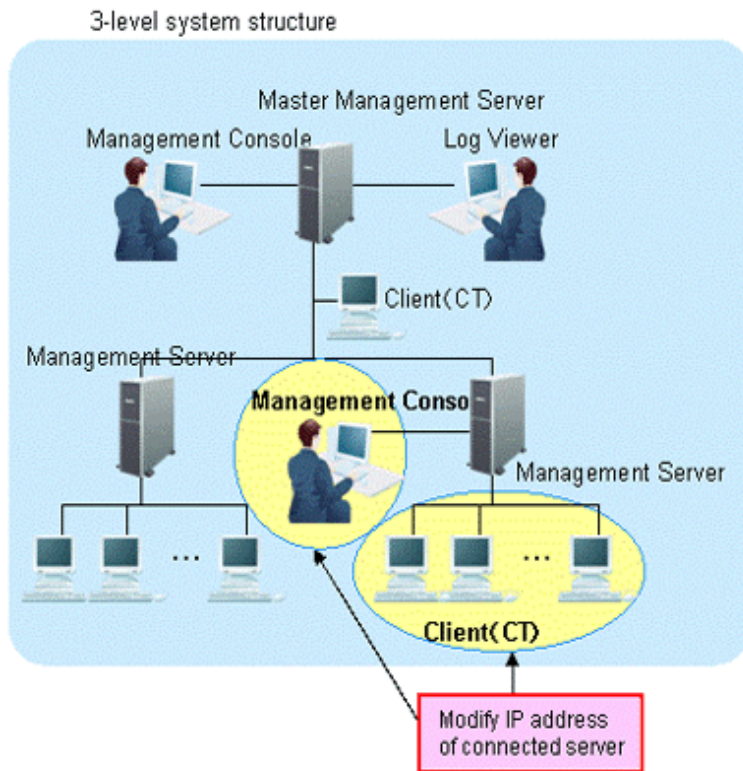
As the configuration information may not match, please do not modify the value of items apart from [Computer name] and [IP address].

- e. Start service.

Start the service of the Management Server in a 3-level structure for which the settings have been changed. At this moment, it is required to start the Master Management Server in advance.

1. Start [Server Settings Tool].
2. Select [Start Service] from the [Service] menu.
3. Exit [Server Settings].

#### 4. Change CT environment



For the following cases, please refer to “[7.7.1 Change Management Server/Master Management Server To Be Connected](#)” and change the CT environment.

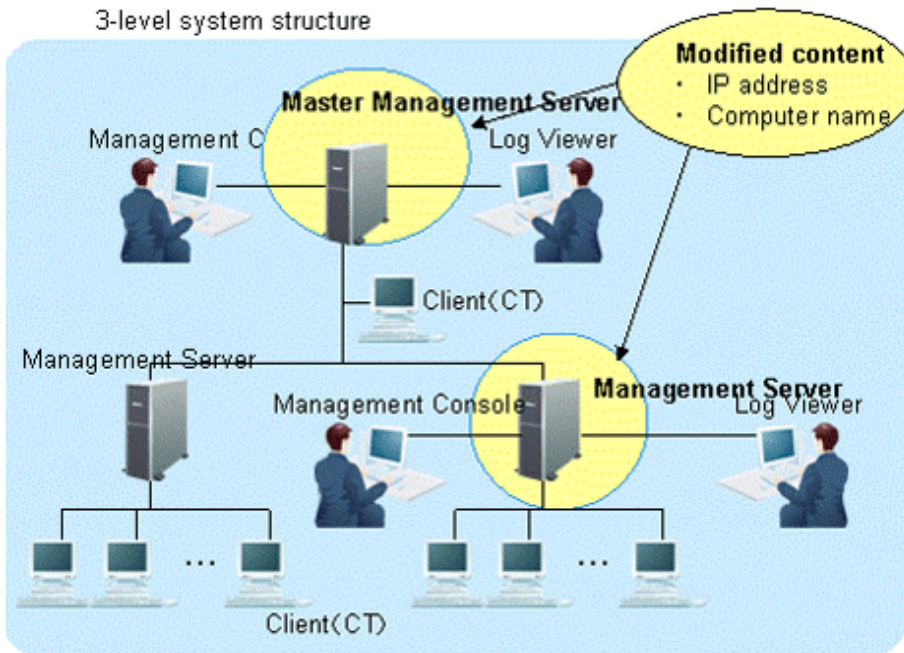
- When the IP address of the Management Server in a 3-level structure is modified and the client (CT) that belongs to this Management Server is connected

#### 5. Change Management Console environment

For the following case, please refer to “[7.8 Change Management Console Environment](#)” and change the Management Console environment.

- When the IP address of the Management Server in a 3-level structure is modified and this Management Server has been set in the connection target of the Management Console.

**When changing the environment of Master Management Server in 3-level structure and the Management Server that belongs to the Master Management Server**



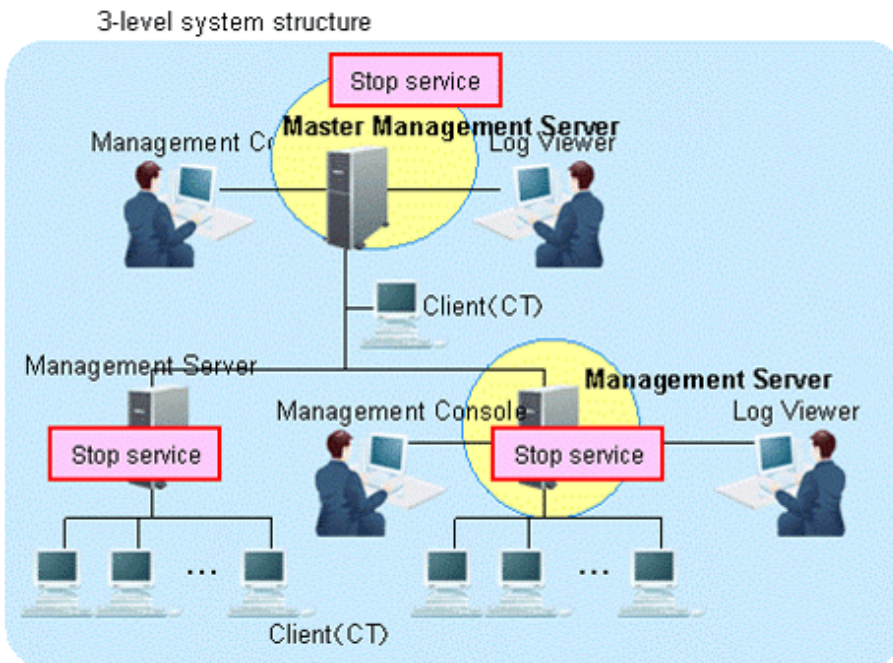
This section describes how to change the environment of the Management Server/Master Management Server when the following information is modified on the Master Management Server in a 3-level structure or a Management Server that belongs to the Master Management Server.

- IP address
- Computer name

After changing the environment of the Management Server and Master Management Server, the information required for returning to the original environment will not be saved. In this case, it is suggested to manage node information (Node name, Computer name, IP address and Server classification) according to the procedure.

The procedure is as follows.

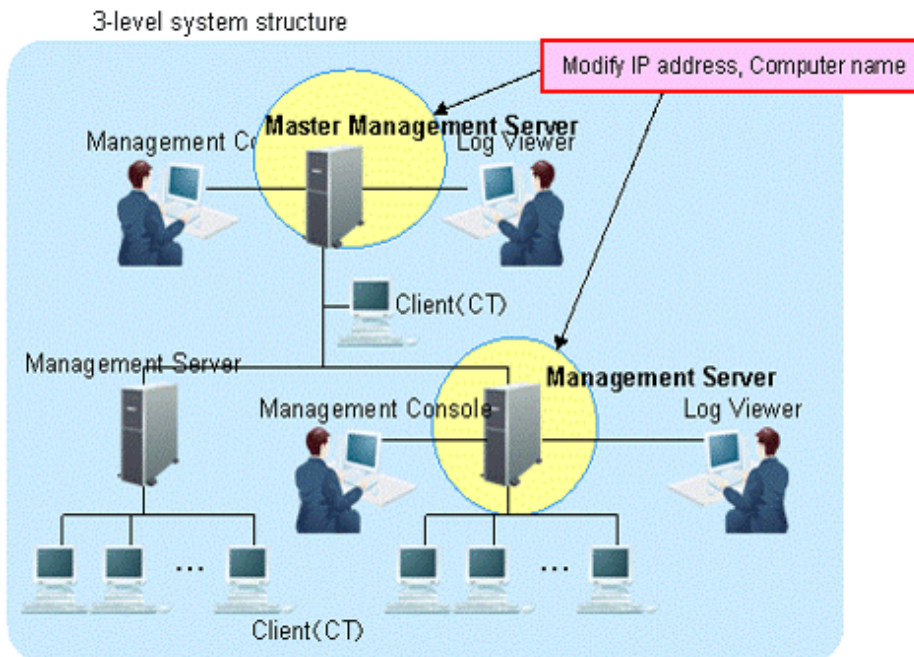
1. Stop the level control service and server service.



Under a 3-level structure, the Master Management Server and all Management Servers that belong to the Master Management Server can be stopped.

- a. Start the [Server Settings Tool].
- b. Select [Stop Service] from the [Service] menu.

2. Modify IP address and computer name.



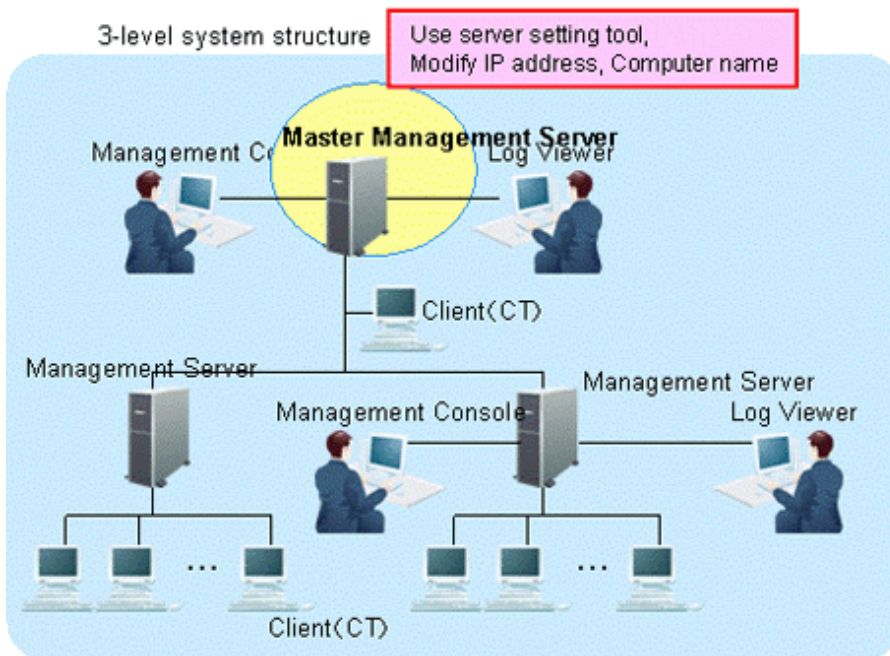
The targets are the Master Management Servers and Management Servers that belong to the Master Management Server in a 3-level structure.

Change the settings of computer itself.



- a. Modify the IP address. When it is not required to modify the IP address, please proceed to the next step.
  1. Select [Control Panel] - [Network Connection] - [Local Area Connection] from the [Start] menu. Click the [Properties] button on the [General] tab in the [Local Area Connection Status] window.
  2. Select the [Internet Protocol] and click the [Properties] button.
  3. Modify and register the IP address.
- b. Modify the computer name. When it is not required to modify the computer name, please proceed to the next step.
  1. Select [Control Panel] - [System] from the [Start] menu, the [Computer Name] tab of the [System Property] window is displayed.
  2. Modify and register the computer name.
- c. Restart the server.

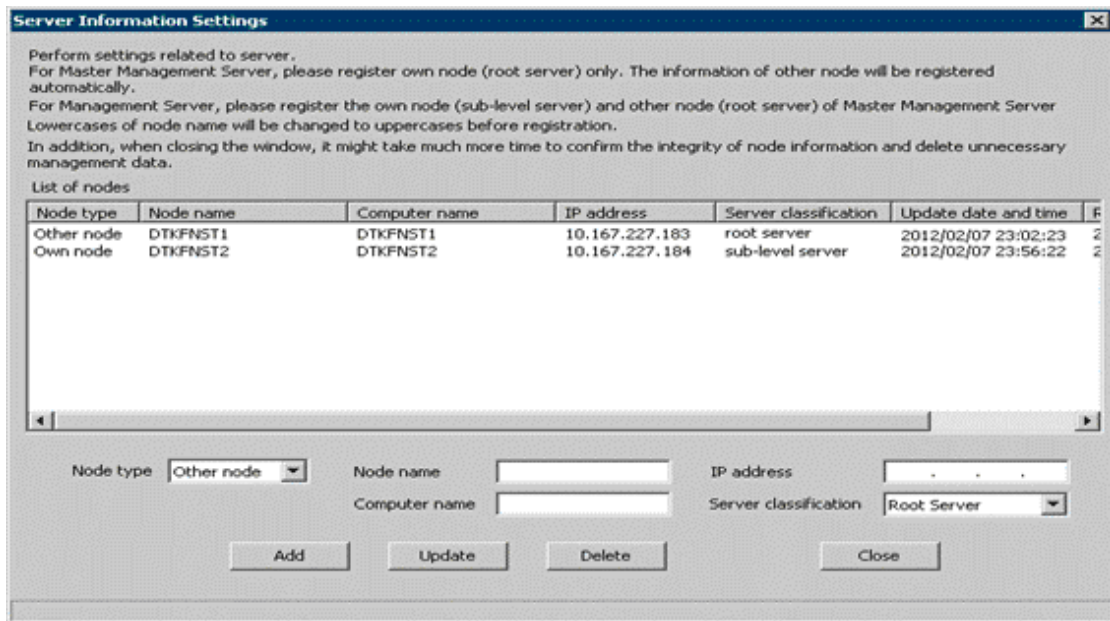
3. Change the settings of Systemwalker Desktop Keeper on Master Management Server.



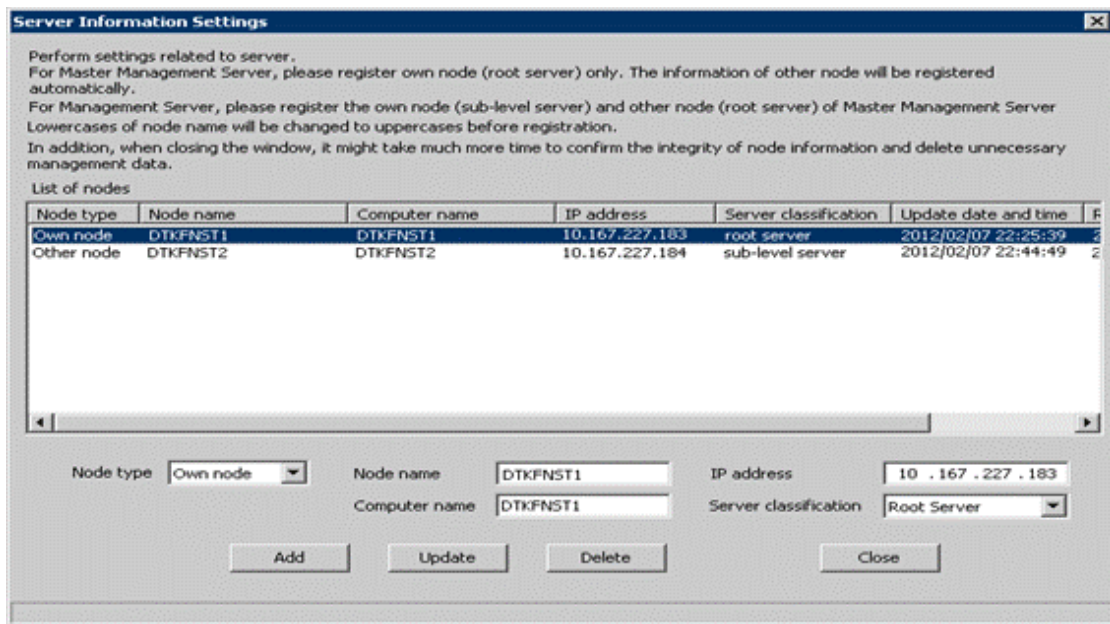
Modify the information settings of this registered server.

- a. Start Server Settings Tool.

- b. Click the [Server information settings] button.  
 → The [Server Information Settings] window is displayed.



- c. Click the data of the node that is classified as this node (root server).  
 → The information will be displayed in the input field under the window.



- d. Modify [Computer name] or [IP address], click the [Update] button and click the [Close] button.

 **Note**

**Please modify [Computer name] and [IP address] only.**

As the configuration information may not match, please do not modify the value of items apart from [Computer name] and [IP address].

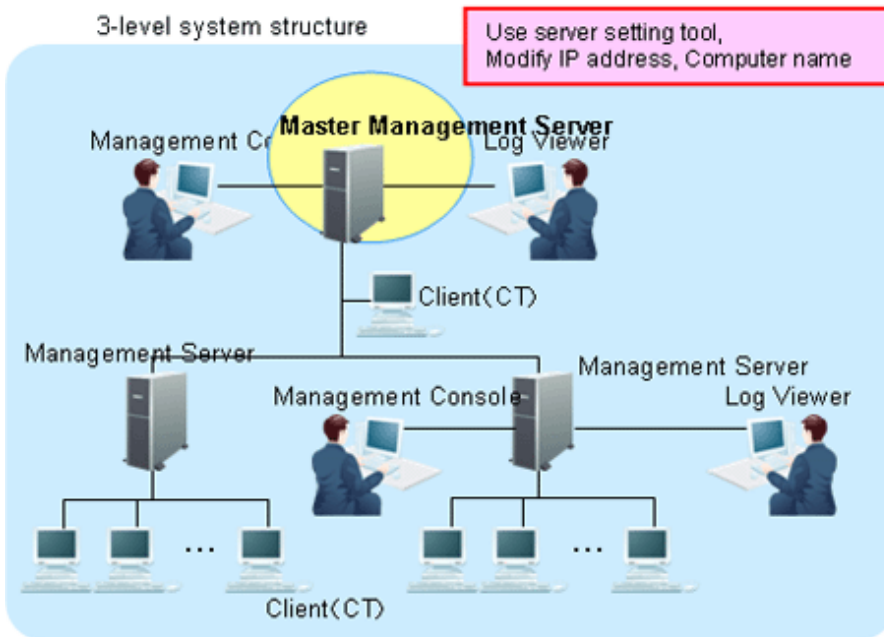
e. Start service.

Start the service of the Master Management Server in a 3-level structure for which the settings have been changed.

1. Start [Server Settings Tool].
2. Select [Start Service] from the [Service] menu.

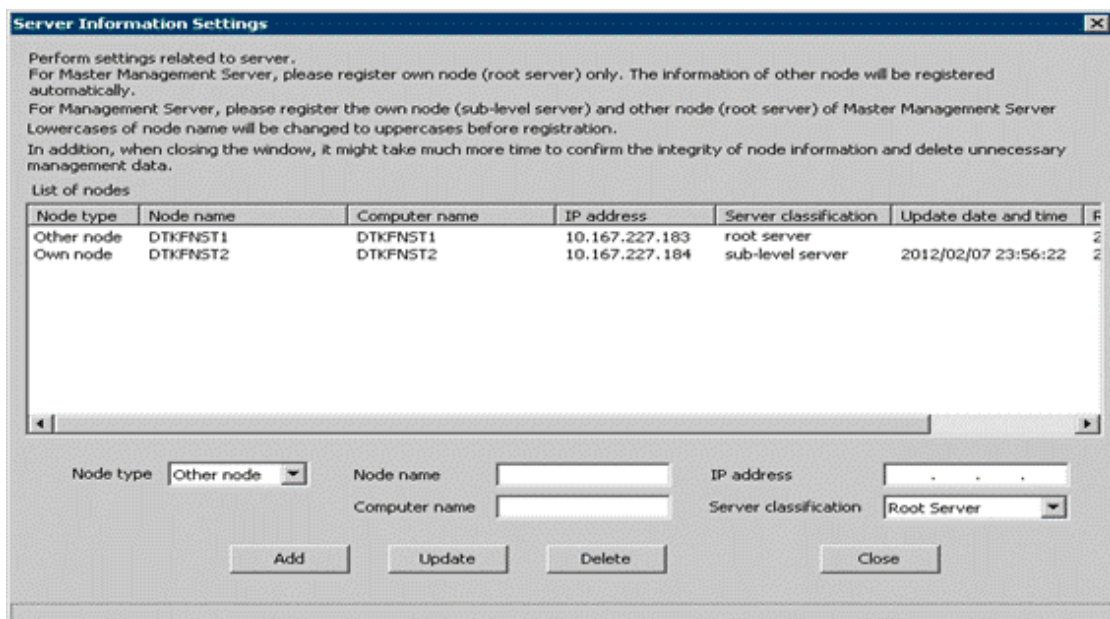
4. Change the settings of Systemwalker Desktop Keeper on Management Server.

(Settings in the Management Server whose IP address and computer name have been changed)

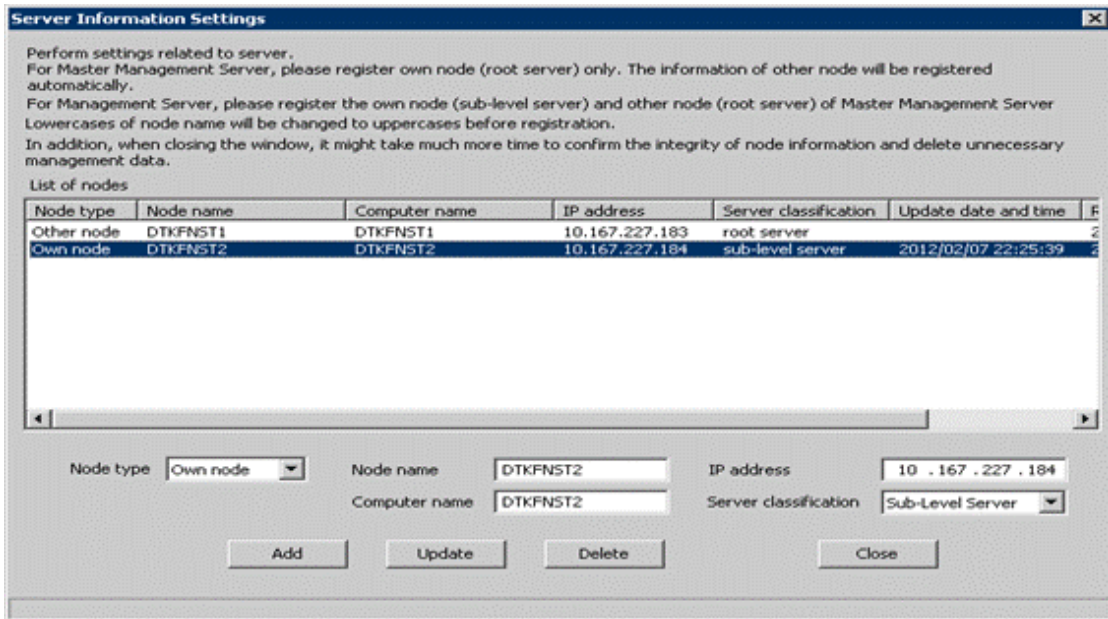


Change the server information settings of this registered Management Server and Master Management Server.

- a. Start Server Settings Tool.
- b. Click the [Server information settings] button.  
→The [Server Information Settings] window is displayed.

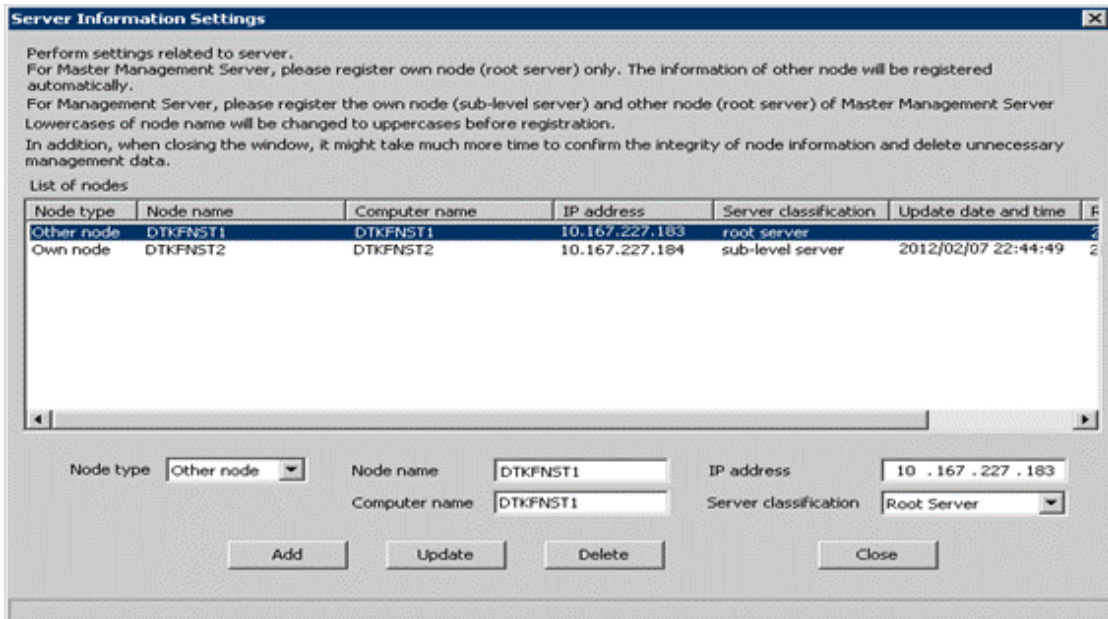


- c. Click the data of the node that is classified as this node (sub-level server).  
 →The information will be displayed in the input field under the window.



- d. Modify [Computer name] or [IP address] of the Management Server and click the [Update] button.

- e. Click the data of the node that is classified as other node (root server).  
 →The information will be displayed in the input field under the window.



- f. Perform the following operations.

1. Check the displayed information of the other node (Node name, Computer name, IP address and Server type).
2. Click the [Delete] button to delete the server information.
3. Enter the following values and click the [Add] button.
  - [Node classification]: Other node
  - [Node name], [Computer name] and [IP address] of changed Master Management Server
  - [Server classification]: Root Server

- g. Click the [Close] button.



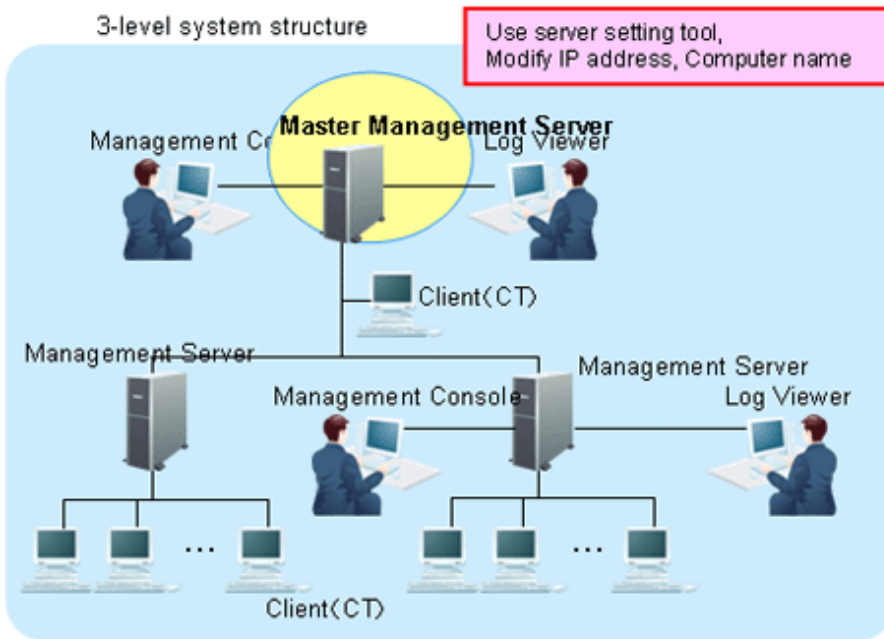
h. Start service.

Start the service of a Management Server that belongs to the Master Management Server in a 3-level structure.

1. Start [Server Settings].
2. Select [Start Service] from the [Service] menu.

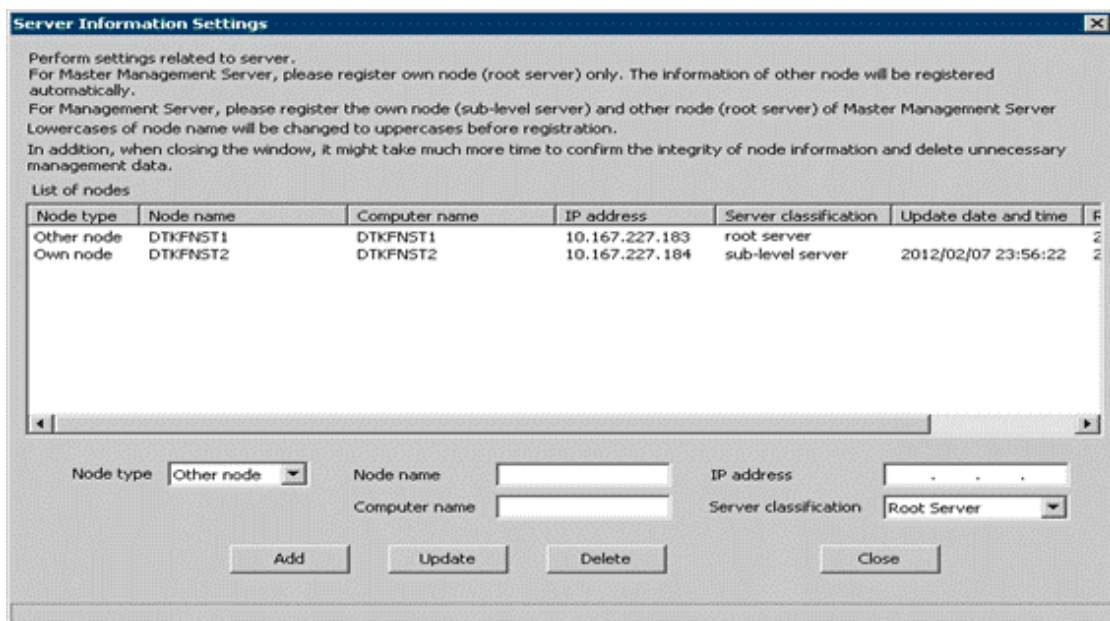
5. Change the settings of Systemwalker Desktop Keeper on Management Server.

(Settings of Management Server whose IP address and computer name are not changed)

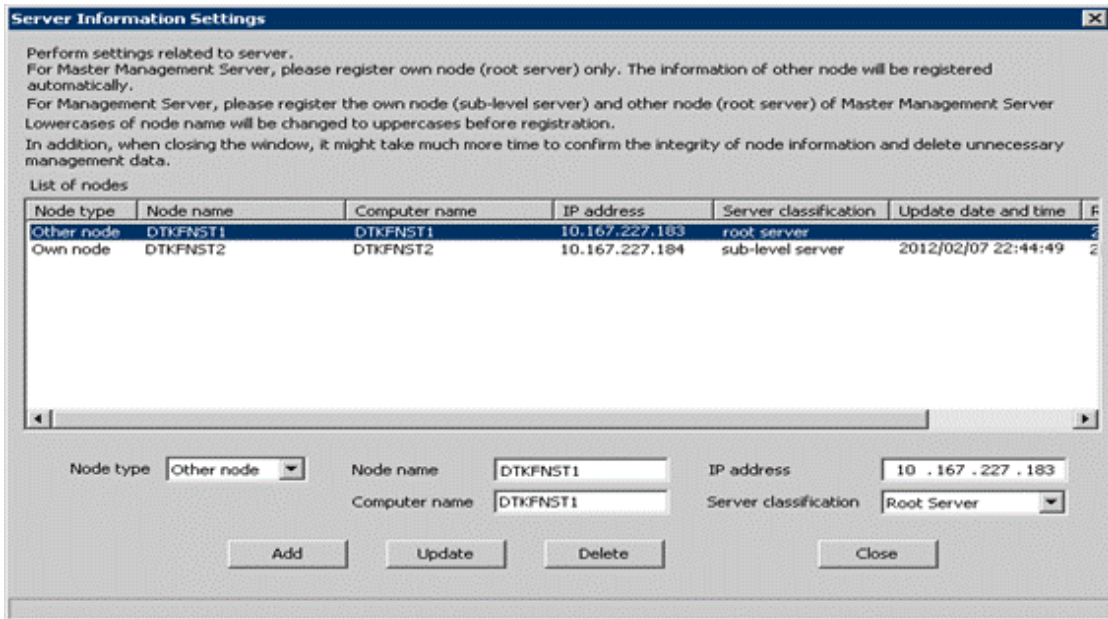


The server information settings of the registered Master Management Server can be changed.

- a. Start Server Settings Tool.
- b. Click the [Server information settings] button.  
→ The [Server Information Settings] window is displayed.



- c. Click the data of the node that is classified as other node (root server).  
 →The information will be displayed in the input field under the window.



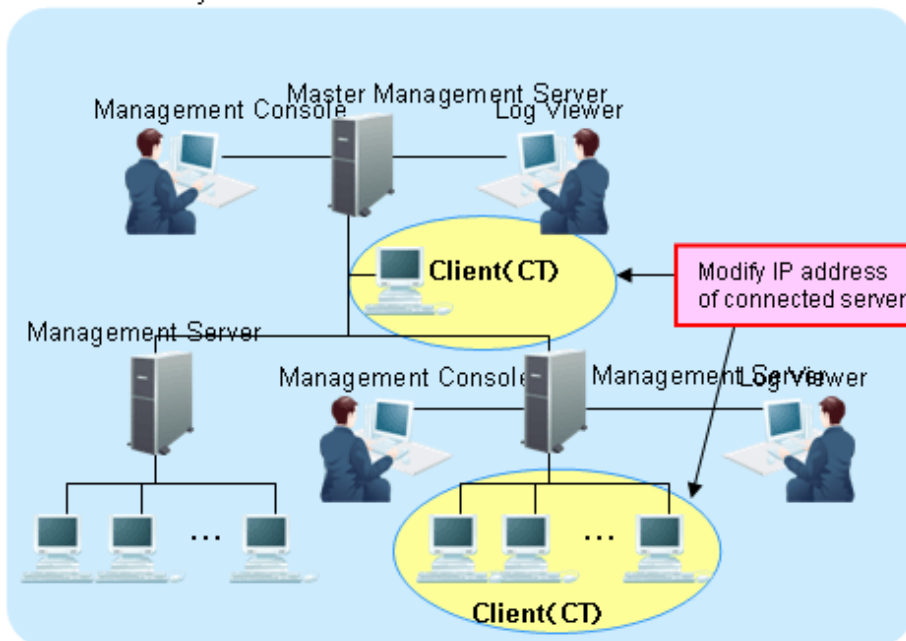
- d. Perform the following operations
1. Check the displayed information of the other node (Node name, Computer name, IP address and Server type).
  2. Click the [Delete] button to delete the server information.
  3. Enter the following values and click the [Add] button.
    - [Node classification]: Other node
    - [Node name], [Computer name] and [IP address] of changed Master Management Server
    - [Server classification]: Root Server
- e. Click the [Close] button.
- f. Start service.

Start the service of the Management Server that belongs to the Master Management Server in a 3-level structure.

1. Start [Server Settings Tool].
2. Select [Start Service] from the [Service] menu.

## 6. Change CT environment

3-level system structure

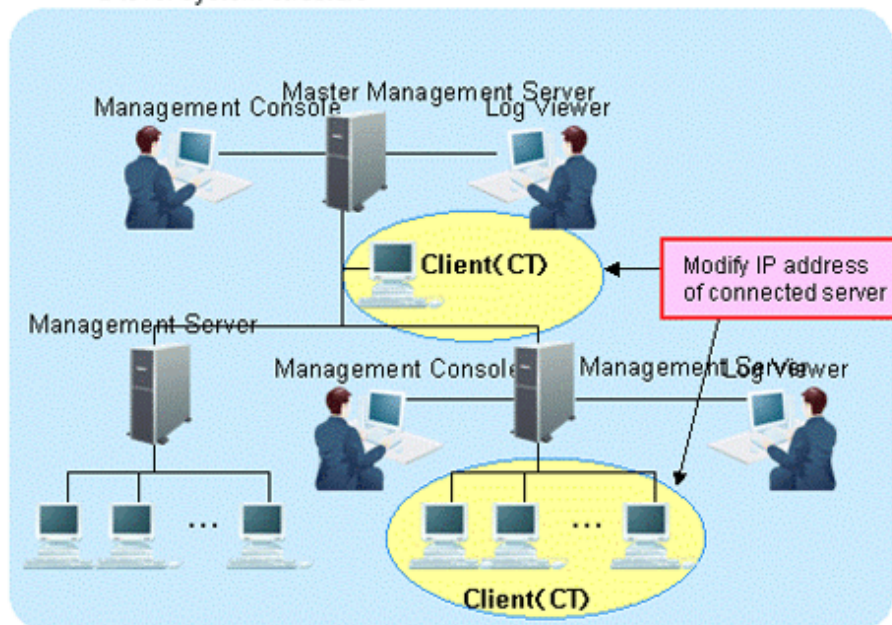


For the following cases, please refer to “7.7.1 Change Management Server/Master Management Server To Be Connected” and change CT environment.

- When the IP address of the Master Management Server and Management Server in a 3-level structure is modified and the client (CT) is connected to this server

## 7. Change the Log Viewer environment

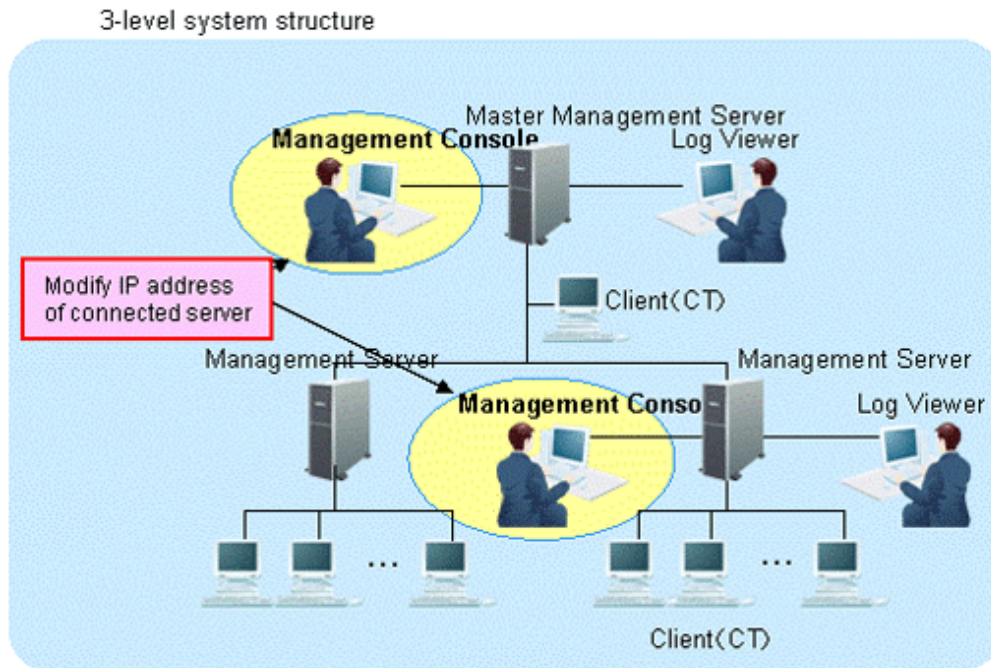
3-level system structure



For the following cases, please refer to “Start Log Viewer” and change the Log Viewer environment.

- When the IP address of the Master Management Server and Management Server in a 3-level structure is modified and this server has been set in the connection target of Log Viewer

## 8. Change the Management Console environment



For the following cases, please refer to “[7.8 Change Management Console Environment](#)” and change the Management Console environment.

- When the IP address of the Master Management Server and Management Server in a 3-level structure is modified and this Management Console has been set in the connection target of Log Viewer

## 7.9.5 Modify Communication Information of Management Server

The port number and communication settings between installed applications of Systemwalker Desktop Keeper can be changed.

After changing the port number, when the changed port number is blocked by the firewall, the blockage must be removed.



### Note

#### Please confirm the port number

Before changing the port number, please refer to “Port Number List” of “Systemwalker Desktop Keeper Reference Manual” and confirm the port number being used.

1. Select the [All Program] - [Systemwalker Desktop Keeper] - [Server] - [Server Settings Tool] from the [Start] menu.

→The [Server Settings Tool] window is displayed.

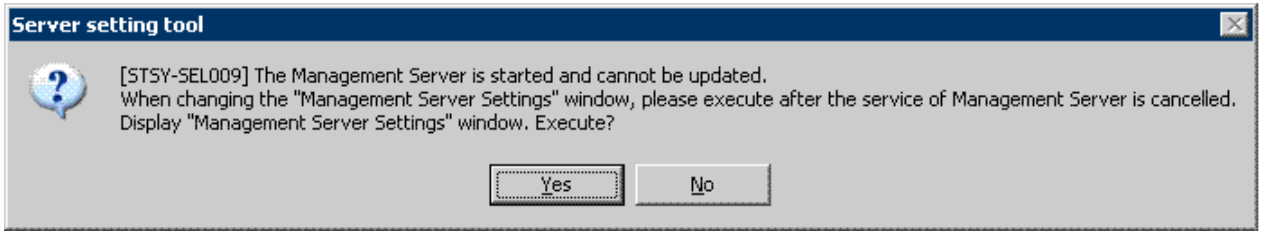
2. Perform the following operations according to purpose.

#### [When Modifying Settings]

Stop the service of the Management Server and Master Management Server that requires a change of settings. For information on how to stop the service, please refer to “[Stop Management Server service](#)”.

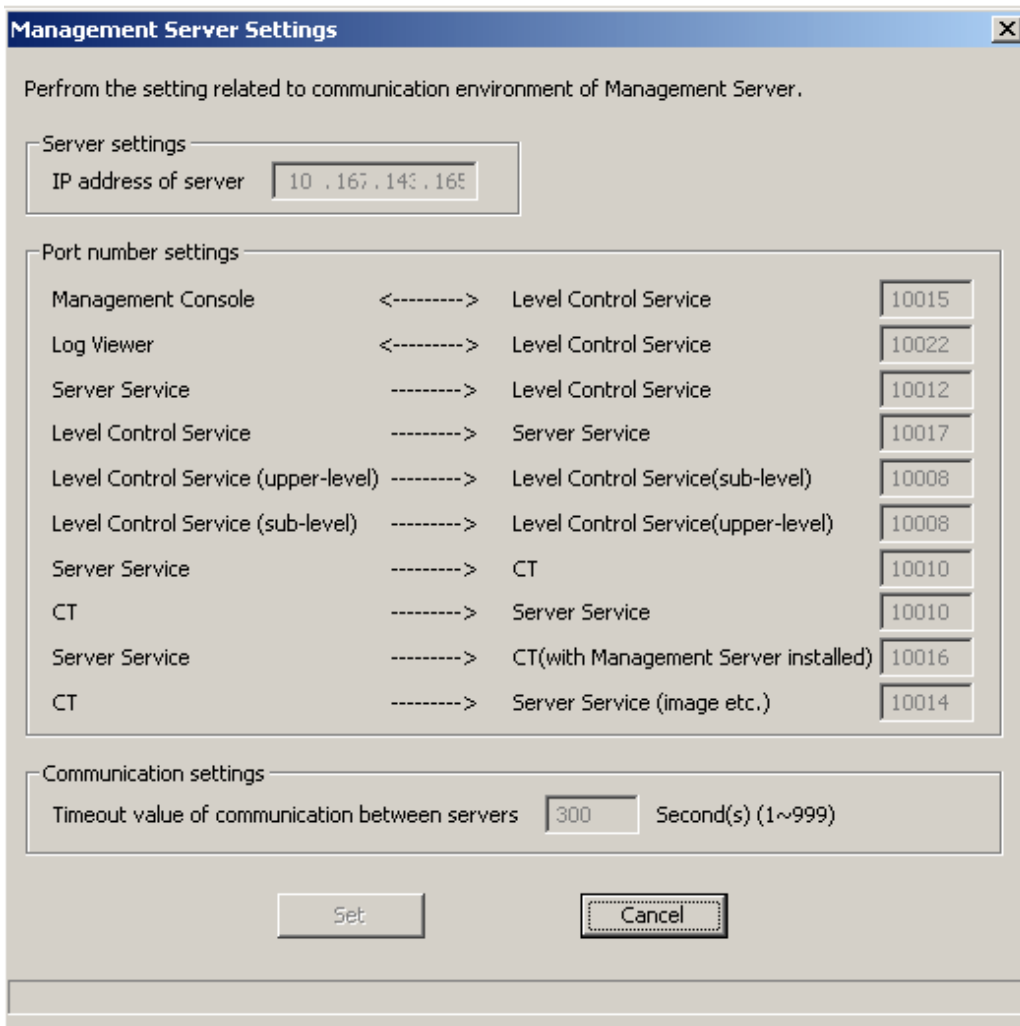
**[When Viewing Settings]**

Proceed to Step 3. When starting the service, the following confirmation window will be displayed. Please click the [Yes] button.



3. Click the [Management Server Settings] button.

→The [Management Server Settings] window is displayed (the value set when the Management Server is installed is displayed).



**[Server settings]**

Item Name	Description
[IP address of server]	The IP address of the Management Server for which the port number and communication settings need to be modified will be displayed.

**[Port number settings]**

Item Name	Description
[Management Console ↔ Level Control Service]	This is the port number used in the communication between Management Console and level control service.

Item Name	Description
[Log Viewer ↔ Level Control Service]	This is the port number used in the communication between Log Viewer and level control service.
[Server Service → Level Control Service]	This is the port number used in the communication from server service to level control service.
[Level control Service → Server Service]	This is the port number used in the communication from level control service to server service.
[Level Control Service (upper-level) → Level Control Service (sub-level)]	This is the port number used in the communication from level control service (upper-level) to level control service (sub-level).
[Level Control Service(sub-level) → Level Control Service(upper-level)]	This is the port number used in the communication from level control service(sub-level) to level control service(upper-level).
[Server Service → CT]	This is the port number used in the communication from server service to the client (CT).
[CT → Server Service]	This is the port number used in the communication from the client (CT) to server service.
[Server Service → CT (with Management Server installed)]	This is the port number used in the communication from server service to the client (CT) when installing the client (CT) in the server that is the same as server service (The port number specified in [Server Service→CT] cannot be specified).
[CT → Server Service (images etc.)]	This is the port number used when sending the screen capture data and summary logs from the client (CT) to server service. (The port number specified in [CT→Server Service] cannot be specified)

[Communication settings]

Item Name	Description
[Timeout value of communication between servers]	The timeout value of the connection that can be performed among Management Console, Log Viewer, level control service, server service and between upper level control service and lower level control service can be input.

4. After modifying the settings according to the requirement, click the [Set] button.

## 7.9.6 Change Saving Target Folder

---

The following saving targets set during installation can be changed in the process of operation.

- Command prompt and log saving target
- Attached data saving target
- Collective log receiving and data saving target

For procedure of change, please refer to “Set Saving Target Folder” of “Systemwalker Desktop Keeper Installation Guide”.

## 7.9.7 Transfer Management Server/Master Management Server

---

This section describes how to transfer the Management Server/Master Management Server to other servers.

1. Display the service window of Windows in the computer of the transfer source, select each service in the following sequence and select [Stop] from the [Operation] menu. It will take 30 seconds to 1 minute before stopping. In addition, after starting

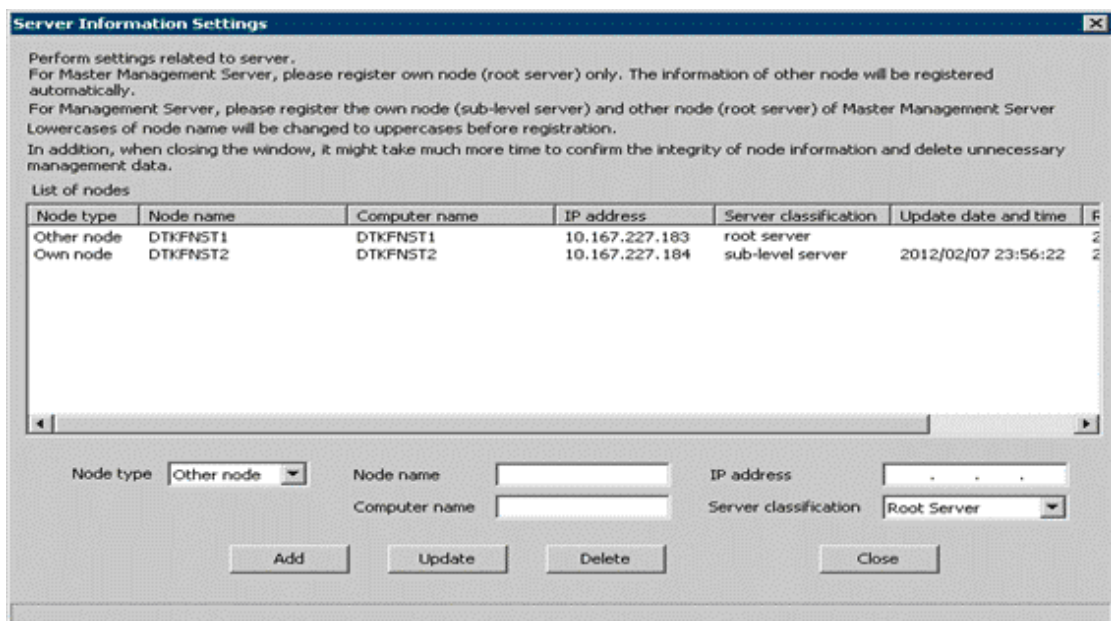


SWServerService or during date change (12am), confirmation of available database capacity will be performed. In the 15 minutes till the confirmation operation has completed, service may not be able to be stopped, please confirm later.

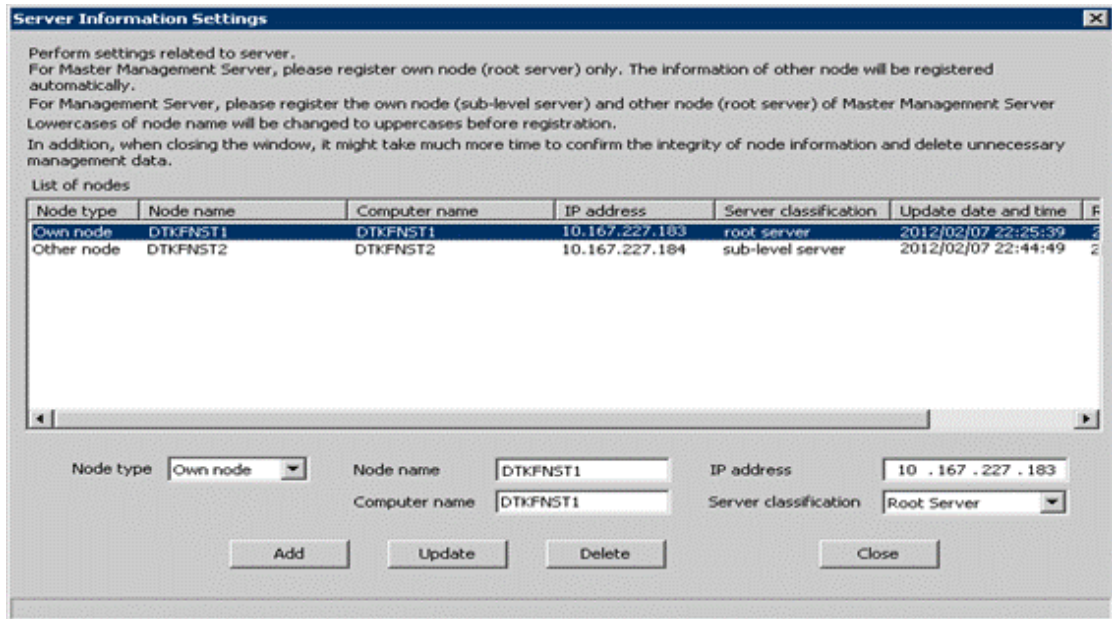
- SWLevelControlService
- SWServerService

In a 3-level structure, please stop the services of all Management Servers/Master Management Servers.

2. Please back up the management information and log information in the computer of the transfer source.  
For the backup method, please refer to "Backup User Asset" of "Systemwalker Desktop Keeper Installation Guide".
3. Construct Management Server/Master Management Server in the transfer target computer.  
For the construction method, please refer to "Installation and Settings of IIS", "Install Management Server/Master Management Server", "Construct Database" and "Settings of IIS" of "Systemwalker Desktop Keeper Installation Guide".
4. The backup data in the computer of the transfer source can be copied to any location of the computer of the transfer target.
5. Display the service window of Windows in the transferring target computer, select each service based on the following sequence and select [Stop] from the [Operation] menu., It will take 30 seconds to 1 minute before stopping. In addition, after starting SWServerService or during date change (12am), confirmation of available database capacity will be performed. In the 15 minutes till the confirmation operation has completed, service may not be able to be stopped, please confirm later.
  - SWLevelControlService
  - SWServerService
6. Please restore the backup data using restoration tool in the transfer target computer.  
For the restoration method, please refer to "Restore User Asset" of "Systemwalker Desktop Keeper Installation Guide".
7. When the name of the transfer target computer is different from the transfer source computer, please modify according to the following procedure.
  - a. Start Server Settings Tool.
  - b. Click the [Server information settings] button.  
→ The [Server Information Settings] window is displayed.



- c. Click the data of the node that is classified as this node.  
 →The information will be displayed in the input field under the window.



d. Modify [Computer name], click the [Update] button and click the [Close] button.

8. Display the Windows service window in the transfer target computer, select each service in the following sequence and select [Start] from the [Operation] menu.
- SWLevelControlService
  - SWServerService

In a 3-level structure, please start the services of all Management Servers/Master Management Servers.

## 7.9.8 Transfer Log Analyzer Settings with Transfer of Management Server/ Master Management Server

This section describes the procedure required to install the Log Analyzer Server when the Management Server/Master Management Server is transferred to another computer during operation.

Perform the following settings on the Management Server/Master Management Server that needs transferring:

1. Before the transfer, in the computer (currently in operation), backup the setting file (TRANS\_SETTING.ini) used by data transmission command to the external media.

The saving target of setting file is as follows:

```
[Systemwalker Desktop Keeper Installation Folder]\LogAnalyzer\TRANS
```

2. Also before transfer, in the computer (currently in operation), use the information output option of RegisterLAInfo.exe (command for registering Log Analyzer Server information) to output Log Analyzer Server information as files and backup to external media.

[Operation example when the path of output file is "C:\work\lasvinfo.csv" is performed]

```
[Systemwalker Desktop Keeper Installation Folder]\LogAnalyzer\TRANS\RegisterLAInfo.exe -e C:\work\lasvinfo.csv
```

3. Uninstall the Management Server in the computer before transfer.
4. Install the Management Server in the transfer target computer.



5. Copy the setting file (TRANS\_SETTING.ini) used by data transmission command that is backed up to external media to the transfer target computer.

The copy target of setting file is as follows:

```
[Systemwalker Desktop Keeper Installation Folder]\LogAnalyzer\TRANS
```

6. Copy the file of the Log Analyzer Server information that is backed up to external media to the transfer target computer and register the Log Analyzer Server information again using the information registration option of RegisterLAInfo.exe (command for registering Log Analyzer Server information).

[Operation Example when the copied file path is “C:\work\lasvinfo.csv” is performed]

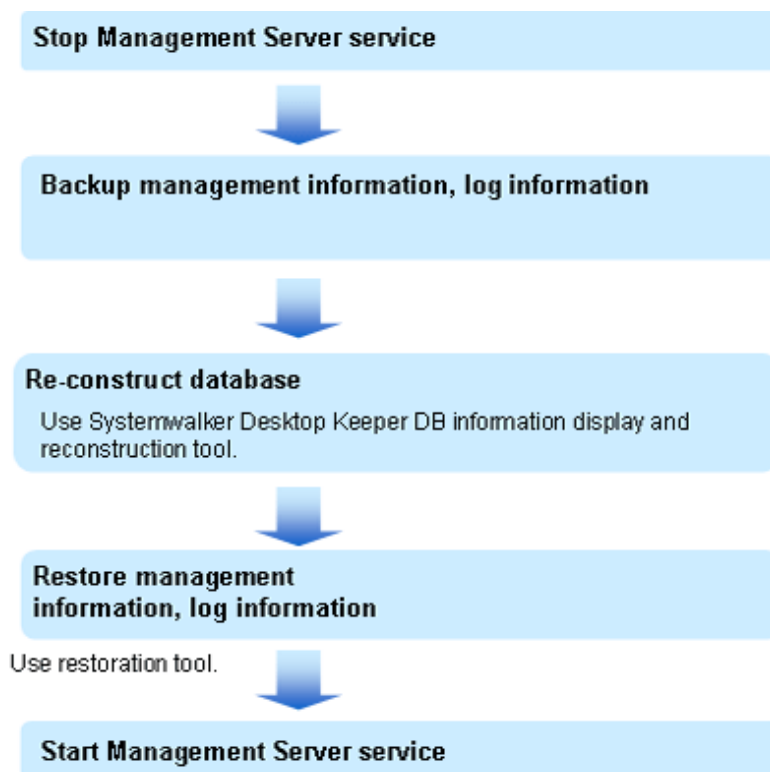
```
[Systemwalker Desktop Keeper Installation Folder]\LogAnalyzer\TRANS\RegisterLAInfo.exe -r C:\WORK\lasvinfo.csv
```

## 7.10 Reconstruct Database of Management Server

When modifying the database capacity during operation, the Operating Environment Maintenance Wizard can be used (display the reconstruction information).

In database reconstruction, the current database will be deleted temporarily. Therefore, please make sure to back up the management information and log information before reconstruction.

Reconstruct the database according to the following procedure.



### Stop Management Server service

Stop the service of the Management Server or Master Management Server that needs reconstruction.

Please be aware that previous client (CT) logs saved in the database may be lost if not executed according to the following procedure:

1. Start [Server Settings Tool].

2. Select [Stop Service] from the [Service] menu.

## Backup management information and log information

Perform backup of management information and log information using the backup tool or backup command. For details, please refer to “Use Backup Tool (GUI)” and “Use Backup Command” of “Systemwalker Desktop Keeper Installation Guide”.



.....

### **Please make sure to back up management information and log information.**

The database will be initialized through the reconstructing database. Please make sure to backup management information and log information before database reconstruction. When it is not implemented, the system cannot be restored.

.....

## Reconstruct database

The constructed database can be reconstructed using Operating Environment Maintenance Wizard (display and reconstruct information).

When reconstructing the database, the database in the old folder will be deleted after the database is created in the new specified folder. Therefore, when reconstructing database in the same drive, the capacity of database that can be newly constructed will be limited to the range of remaining capacity of drive (the range after subtracting the total capacity of drive by old database capacity).

Please estimate the capacity in advance.

1. Log on the PC with a user at the time of database construction.

2. Select the [All Program] - [Systemwalker Desktop Keeper] - [Server] - [Operating Environment Maintenance Wizard (Display or Reconstruct information)] from the [Start] menu.

→ The [Operating Environment Maintenance Wizard (Display or Reconstruct information)] window is displayed.

**Operating Environment Maintenance Wizard (Display Information and Re-construct)**

**Database information**  
Get and display database information. Please click the [Get Information] button.

Database allocation capacity

Database construction information

Database creation target

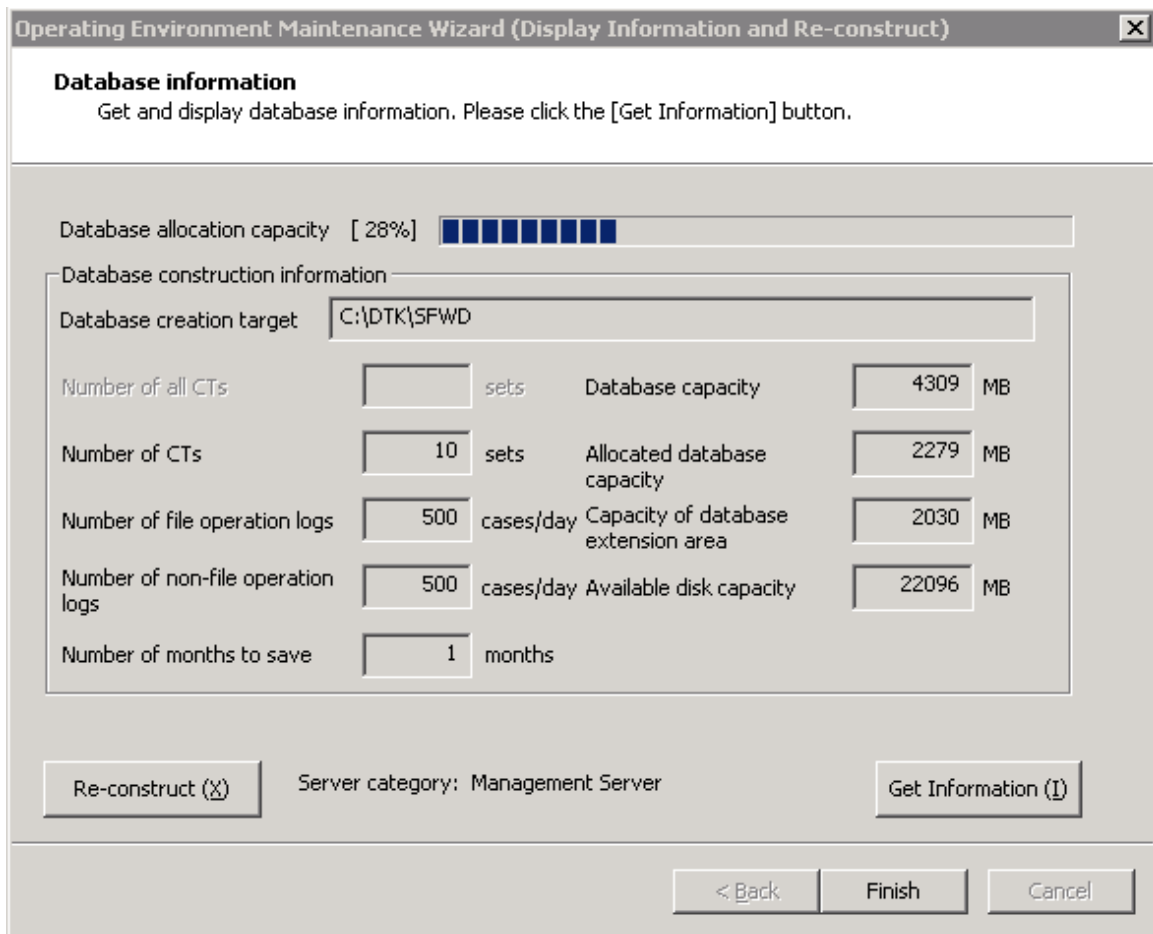
Number of all CTs	<input type="text"/>	sets	Database capacity	<input type="text"/>	MB
Number of CTs	<input type="text"/>	sets	Allocated database capacity	<input type="text"/>	MB
Number of file operation logs	<input type="text"/>	cases/day	Capacity of database extension area	<input type="text"/>	MB
Number of non-file operation logs	<input type="text"/>	cases/day	Available disk capacity	<input type="text"/>	MB
Number of months to save	<input type="text"/>	months			

Re-construct (X)      Server category: Management Server      Get Information (I)

< Back      Finish      Cancel

3. Click the [Get Information] button and confirm the current database capacity.

→ The following window is displayed.



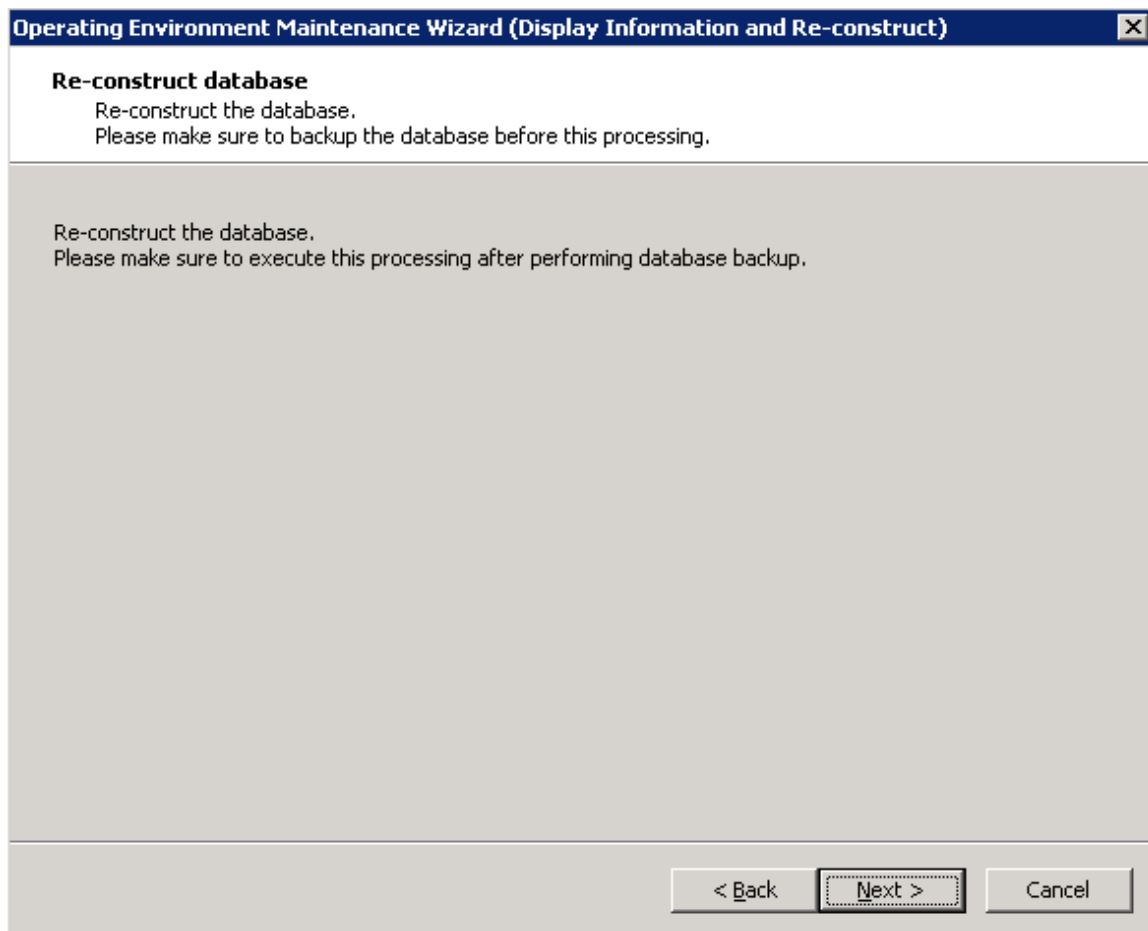
4. Confirm the displayed contents.

Item Name		Description
[Database allocation capacity]		This is the proportion of initially allocated database capacity against the allocated database capacity (used capacity of current database). The capacity value can be calculated by multiplying this value (%) with "Database Capacity". The remaining capacity will be used for expansion.
[Database constructing information]	[Database creation target]	Display target drive and folder created with the current data.
	[Number of all CTs]	This is the total Number of managed on the Master Management Server. It cannot be displayed when Management Server is selected.
	[Number of CTs]	The number of clients (CTs) specified when creating the database will be displayed.
	[Number of file operation logs]	The number of file operation logs in one day specified during database construction will be displayed.
	[Number of non-file operation logs]	The number of logs apart from file operation logs in one day specified during database construction will be displayed.
	[Number of months to save]	The number of months to save logs specified during database construction will be displayed.

Item Name		Description
	[Database capacity]	The current database capacity (MB) will be displayed.
	[Allcated database capacity]	The allocated capacity (MB) of current database will be displayed.
	[Capacity of database extension area]	The current capacity (MB) of database extended space will be displayed. This capacity is reserved for database expansion and is part of unused database space.
	[Available disk capacity]	The available capacity (MB) of target drive constructed by the current database will be displayed.

5. Click the [Re-construct] button.

→ The following window is displayed.



6. Click the [Next] button.

→ The following window is displayed.

Item Name		Description
[Database re-construction target ]		<p>Input when changing the construction target path of database.</p> <p>Please click the [View] button and specify the construction target path of new database.</p> <p>The folder on the network and file system that is not NTFS format cannot be specified.</p> <p>The number of characters in construction target file name of database can be specified with no more than 32 bytes. The multi-byte characters such as Space, Hiragana, Katakana and Chinese characters, etc., cannot be specified.</p>
[Estimate Database Capacity]	[Number of all CTs]	<p>The total Number of managed on the Master Management Server can be entered within the range from 1 to 50000.</p> <p>This cannot be entered when the Management Server is selected.</p>
	[Number of CTs managed in this server] (Required)	<p>Enter the Number of sets to be connected.</p> <p>1 - 2000 can be entered.</p>
	[Number of file operation logs] (Required)	<p>Enter the number of file operation logs in one day.</p> <p>Enter a number in the range of 1 - 99999.</p> <p>When the corresponding log is not obtained, enter "1".</p>

Item Name		Description
	[Number of non-file operation logs] (Required)	The number of logs apart from the file operation log in one day can be entered. Enter within 1 ~ 99999. When the corresponding log is not obtained, enter "1".
	[Number of months to save] (Required)	Enter the number of months to save.

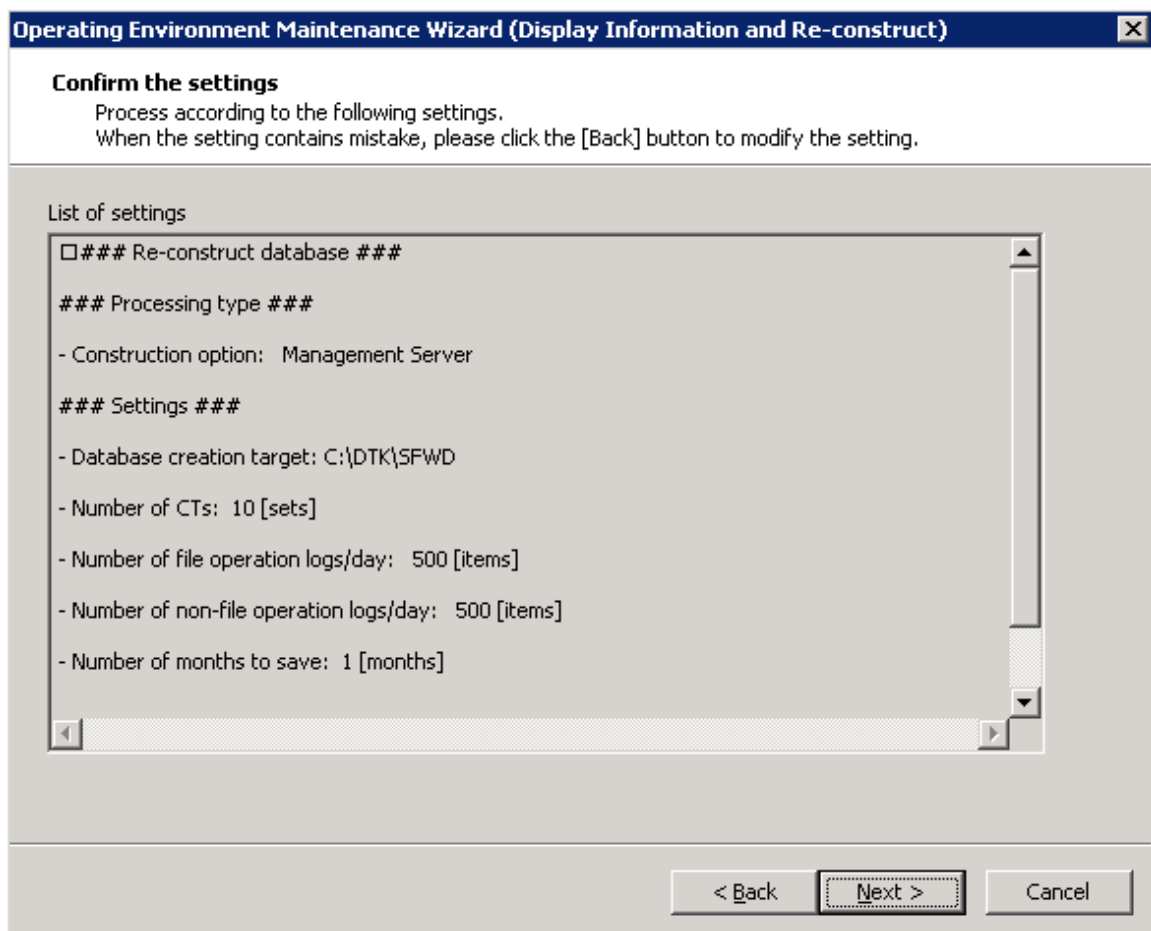
7. Enter the required items and click the [Capacity Estimation] button.

→The database capacity is calculated and displayed in the [Database capacity].

Please replace the displayed database capacity with the estimated value in advance.

8. Click the [Next] button.

→The following window is displayed.



9. Confirm the setting contents.

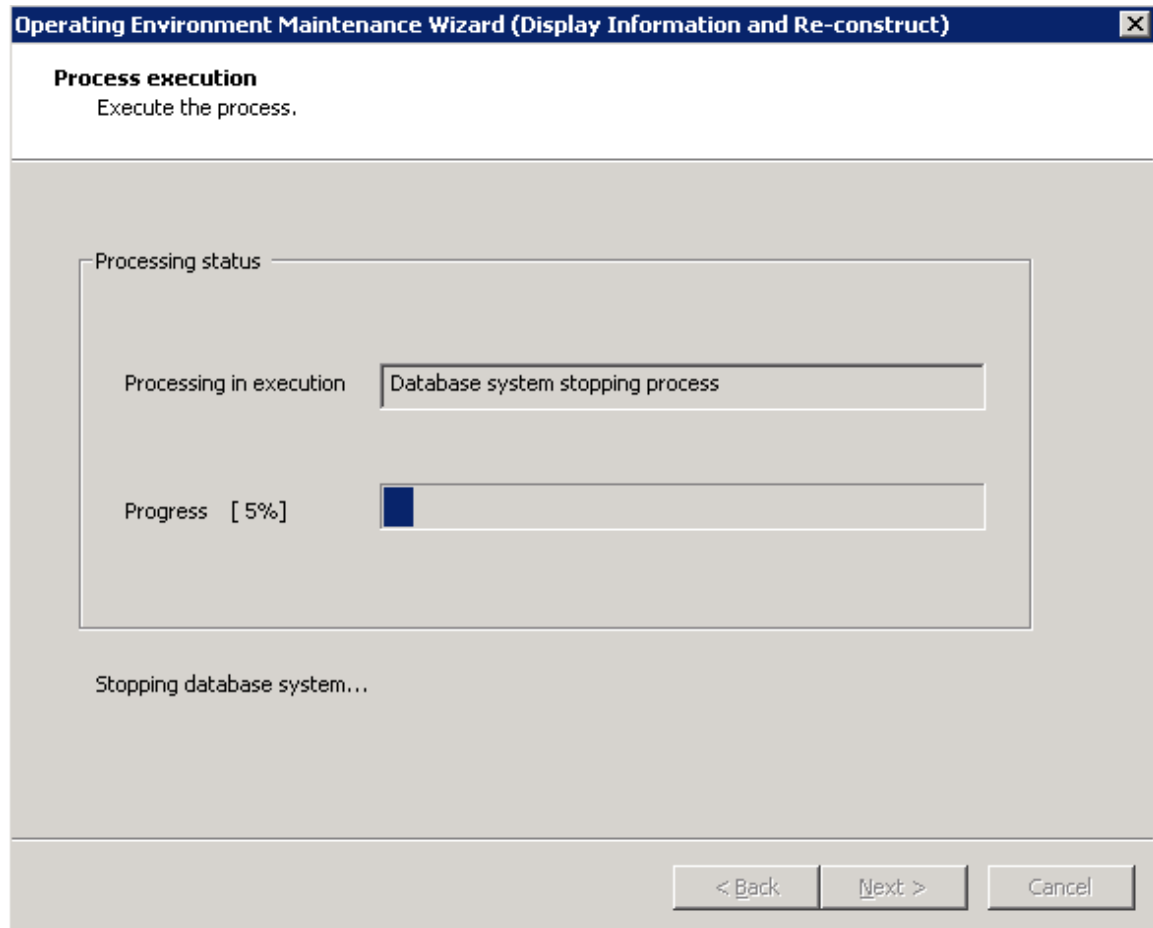
**[Displayed Confirmation Items]**

- Construction option
- Database creation target
- Number of CTs
- Number of file operation logs/day
- Number of non-file operation logs /day

- Number of months to save
- Database capacity
- Available disk capacity

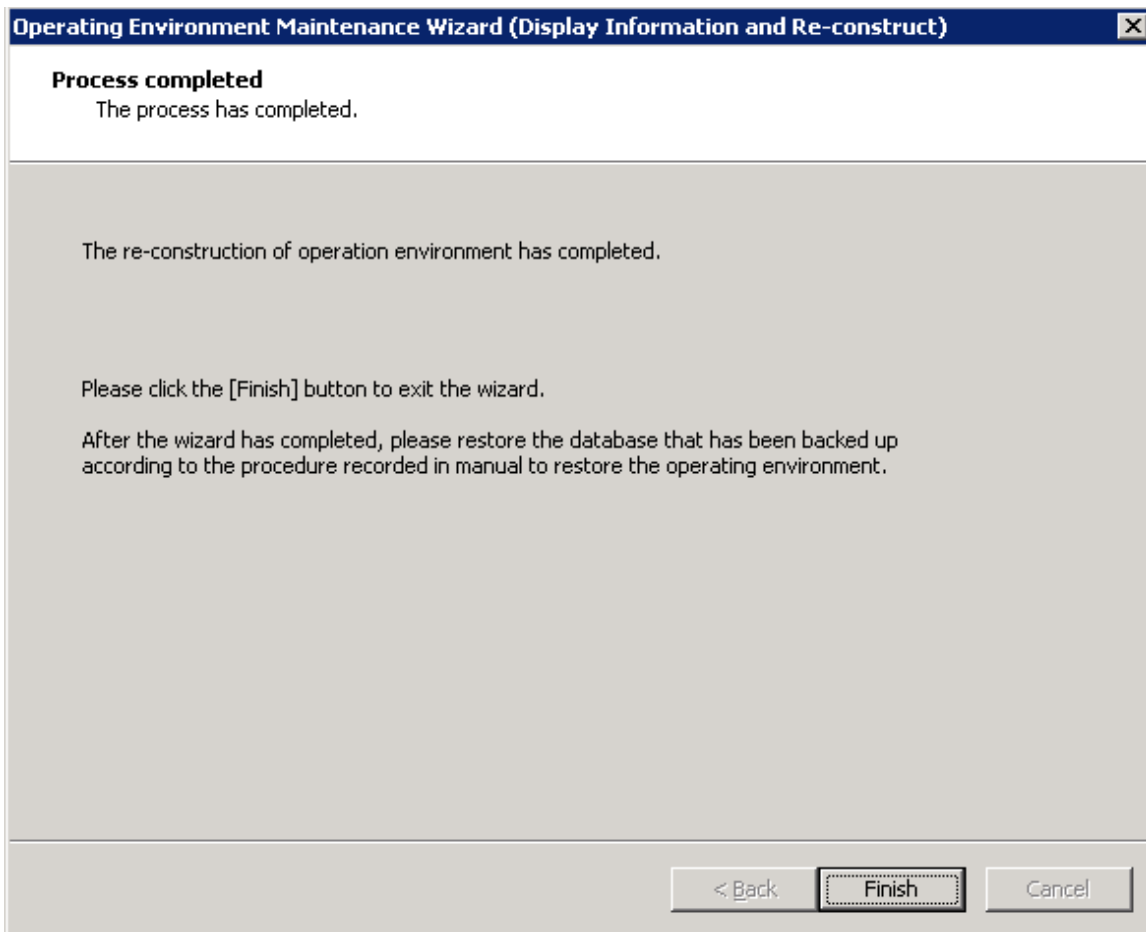
10. Click the [Next] button.

→The following window is displayed and reconstruction process is executed.





→ The following information is displayed after the process is finished.



After the reconstruction of the database has completed, please make sure to use the restoration tool and restore the management information and log information backed up before database reconstruction to the reconstructed database.



## Note

### About automatic backup settings

After reconstructing the database using Operating Environment Maintenance Wizard (display information and reconstruct), the [Automatic Backup Settings] window will not be displayed. When resetting the automatic backup, please set by the backup tool (GUI). For the setting method, please refer to “Back up and Delete Automatically” of “Systemwalker Desktop Keeper Installation Guide”.

### Restore management information and log information

Restore the management information and log information backed up before database construction to the reconstructed database using restoration tool.

Please refer to “Use Restoration Tool” of “Systemwalker Desktop Keeper Installation Guide” for restoration method of management information and log information.

### Start Management Server service

Please be aware that the previous client (CT) logs saved in the database may be lost if the following procedures are not executed.

Start the service of the Management Server or Master Management Server that has been stopped.

1. Start service.
2. Start [Server Settings Tool].
3. Select [Start Service] from the [Service] menu.

## 7.11 Create Log Viewing Database

---

For information on how to create the log viewing database after starting to use Systemwalker Desktop Keeper, please refer to “Construct Log Viewing Database” of “Systemwalker Desktop Keeper Installation Guide”.

## 7.12 Change Log Analyzer Server Environment

---

### 7.12.1 Transfer Log Analyzer Server

---

This section describes how to transfer the Log Analyzer Server to other computers during operation.

1. In the computer before transfer (currently in use), copy the backup CSV file of log information of the shared folders (folder specified during transmission of log data) to the external media with the folder structure being kept.
2. Backup the settings information of the Log Analyzer settings to external media using the backup option of LADBBKRS.bat (backup and restoration command of Log Analyzer settings information).

[Operation example when the path of backup target is “E:\LAMASTERINFO” is performed]

```
[Installation Folder of Log Analyzer Server] \bin\SWDTLAENV\LADBBKRS.bat -bs -d E:\LAMASTERINFO
```

3. Install the Log Analyzer Server in the transfer target computer.
4. In the transfer target computer, the operating environment can be constructed using Operating Environment Maintenance Wizard.
5. Restore the setting information of Log Analyzer settings using the restoration option of LADBBKRS.bat (backup and restoration command of the Log Analyzer settings setting information).

[Operation example when the path of backup source folder is “E:\LAMASTERINFO” is performed]

```
[Installation Folder of Log Analyzer Server]\bin\SWDTLAENV\LADBBKRS.bat -rs -d C:\LAMASTERINFO
```

6. Copy the data of shared folder backed up to the external media to the shared folder of transfer target computer with the folder structure being kept.

The transferred data volume should not exceed the [Number of Months to Save] specified during the construction of operating environment.

7. Modify the following files names in the copied folder:

- File name before change: conv\_end
- File name after change :trans\_end

The above mentioned files exist in the each period folder (Example: 20080421\_20080421).

When there are too many folders, change can be easier using the following batch commands.

[Example of Batch File]

```
ECHO OFF
IF %1.==. GOTO NOPARAM
FOR /R %1 /D %%f IN (*) DO (
  IF EXIST %%f\conv_end (
    move %%f\conv_end %%f\trans_end
  )
)
```

```
GOTO END
:NOPARAM
ECHO Please specify the folder path.
:END
ECHO ON
```

[Operation example when the batch file is “conv.bat” and the path of shared folder is “C:\LASVDATA” is performed]

```
conv.bat C:\LASVDATA
```

8. Add data to the Log Analyzer Server through DttoolEx.exe (data transfer and deletion command).

[Operation example when the path of shared folder is “C:\LASVDATA” is performed]

```
[Installation Folder of Log Analyzer Server]\bin\dttool\DttoolEx.exe -f C:\LASVDATA
```

9. Restore the Log Analyzer settings information again using the restoration option of LADBBKRS.bat (backup and restoration command for Log Analyzer settings information).

[Operation example when the path of backup source folder is “E:\LAMASTERINFO”]

```
[Installation Folder of Log Analyzer Server]\bin\SWDTLAENV\LADBBKRS.bat -rs -d C:\LAMASTERINFO
```



### Note

When the “Step 9: Restore the setting information of Log Analyzer settings again”, is not performed, there are situations in which restoration may not occur, such as when the user ID has been deleted or the setting content is not updated to the latest status, etc.

## 7.12.2 Modify IP Address/Port Number of Log Analyzer Server

This section describes how to change the operating environment when the IP address and port number of the Log Analyzer Server is modified during operation.

### The following settings can be performed on Master Management Server:

1. Use the information output option of RegisterLAInfo.exe (command for registering Log Analyzer Server information) to output the Log Analyzer Server information as a file.

[Operation example when the path of output file is “C:\work\lasvinfo.csv”]

```
[Installation Folder of Systemwalker Desktop Keeper] \LogAnalyzer\TRANS\RegisterLAInfo.exe -e C:\work\lasvinfo.csv
```

2. Edit the file output in Step 1.

Rewrite the IP address and port number of target Log Analyzer Server as new information.

3. Use the information registration option of RegisterLAInfo.exe (command for registering Log Analyzer Server information) to reregister the Log Analyzer Server information.

[Operation example when the file path edited in Step 2 is “C:\WORK\lasvinfo.csv” ]

```
[Installation Folder of Systemwalker Desktop Keeper]\LogAnalyzer\TRANS\RegisterLAInfo.exe -r C:\WORK\lasvinfo.csv
```

4. When the port number for aggregate by objective is modified, further editing of the “services” file is required.

The “services” file is saved in the following folder:

- Under Windows Server® 2008 environment: “C:\WINDOWS\system32\drivers\etc”
- Under Windows Server® 2003 environment: “C:\WINDOWS\system32\drivers\etc”

Modify the following settings of the “services” file.

rn Communication Port Number/TCP
----------------------------------

**Perform the following settings on the Management Server/Master Management Server that is transferring log data to changed Log Analyzer Server.**

**If only the port number is modified, this operation is not required.**

1. Start the Log Analyzer settings and modify the path of the transfer target shared folder as a new path.

[Operation example when the path of shared folder before change is “\\192.168.1.1\LASVDATA”, and the new IP address is “192.168.2.1”]

Please modify the path of shared folder before change to “\\192.168.2.1\LASVDATA”.

For details, please refer to “Set Environment of Log Analyzer Server” of “Systemwalker Desktop Keeper Installation Guide”.

**Perform the following settings in the Report Output Tool.**

1. Start the report output environment setup, and modify the IP address/port number of the [Server] tab to the new IP address/port number.

For details, please refer to “Set Report Output Environment” of “Systemwalker Desktop Keeper Installation Guide”.

# Chapter 8 Policies That Can be Set

This chapter describes the system actions when the set policy is valid and how to use the collected logs.

## 8.1 Set the Policies of Prohibition Function

This section describes the operations that can be prohibited by the prohibition function.

### Operations that can be prohibited

Policy can be set to prohibit operations. The operations that can be prohibited are as follows.

The policy is set by the system administrator or department administrator in the Management Console.



#### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

For details, please refer to “[1.2.8 File Export Prohibition](#)” - “[1.2.15 Clipboard Operation Prohibition](#)”.

- File export prohibition
- File reading prohibition
- Printing prohibition
- Logon prohibition
- This function is not available.
- Application startup prohibition
- PrintScreen key prohibition
- E-mail attachment prohibition
- This function is not available.
- URL access prohibition
- FTP server connection prohibition
- Web download prohibition
- Clipboard operation prohibition

### 8.1.1 File Export Prohibition

By setting the file export prohibition policy, exporting files or folders to drive, network drive, removable devices or DVD/CD drive of the client (CT) PC can be prohibited.



#### Functions may be restricted due to the environment being used

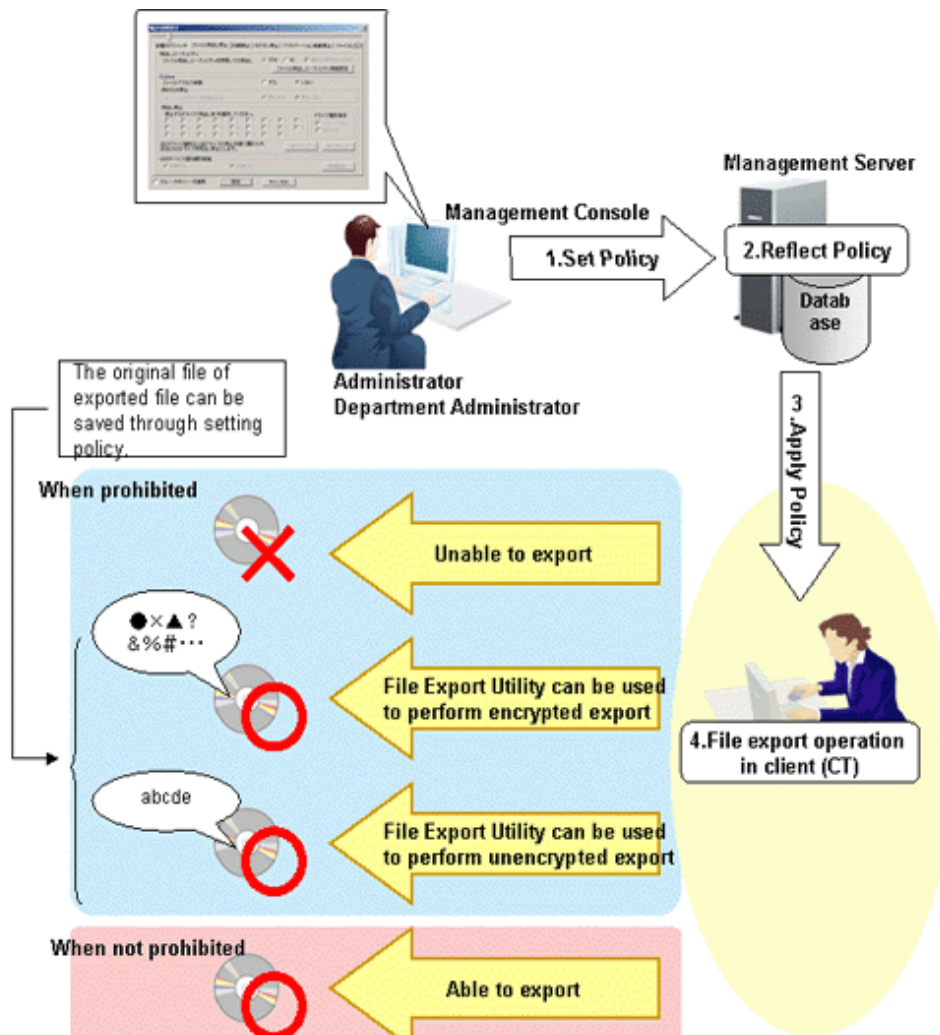
When setting the policy, functions may be restricted due to the environment being used.

For details, please refer to “[1.2.8 File Export Prohibition](#)”.

When prohibited, File Export Utility can still be used to export files and folders. Encrypted export or export directly in plain text can be selected.

For “File Export Utility”, please refer to “1.2.5 Export Utility” and “Systemwalker Desktop Keeper User’s s: for Client”.

### Steps to make prohibition effective through policy setting



1. Set Policy  
Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window right after the Management Console (the CT policy settings window) is started.  
The conditions for prohibiting file export are set in the [File Export Prohibition] tab.
2. Reflect Policy  
The set policy will be reflected to the database.
3. Apply Policy  
The set policy will be applied to the client (CT).
4. File export operation  
When intending to export files and folders in the client (CT), the status will become one of the following:
  - Unable to export
  - File Export Utility can be used to perform encrypted export
  - **Encryption Function is not available.**

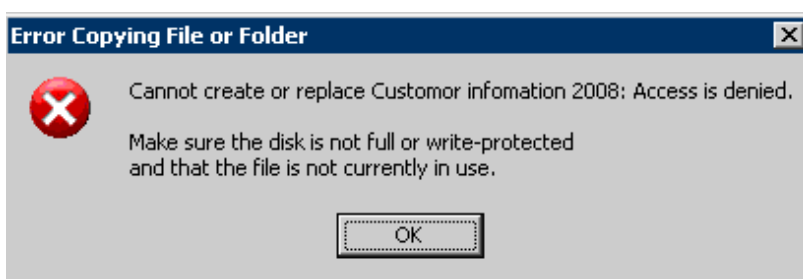
- File Export Utility can be used to perform unencrypted export
- Able to export

When exporting to DVD/CD, the operations will be different according to the media. For details, please refer to “[1.2.8 File Export Prohibition](#)” and “[1.2.5 Export Utility](#)”.

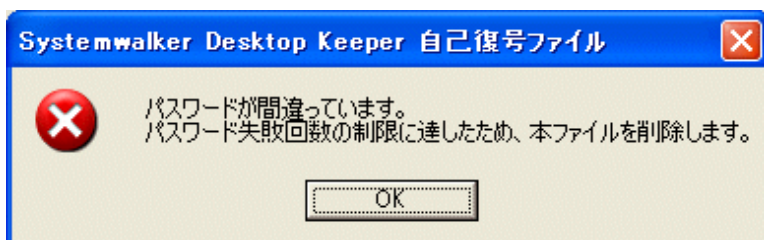
For operations, please refer to “Systemwalker Desktop Keeper User’s Guide: for Client”.

## When prohibited

When intending to export files and folders to the drive of a prohibited target without using “File Export Utility”, the prohibition window will be displayed in the client (CT). An example of prohibition window is as follows:



When decrypting the file exported with encryption using File Export Utility, the following window will be displayed if the number of times the user attempts to enter the password exceeds the [Password Attempts] displayed in the [Encrypted File Settings] window, and the encrypted file will be deleted.



When decrypting the file exported with encryption using File Export Utility, if [Password Attempts] in the [Encrypted File Settings] window is displayed as 4 or more, the following window will be displayed after password entry fails three times, and the decryption will be terminated.



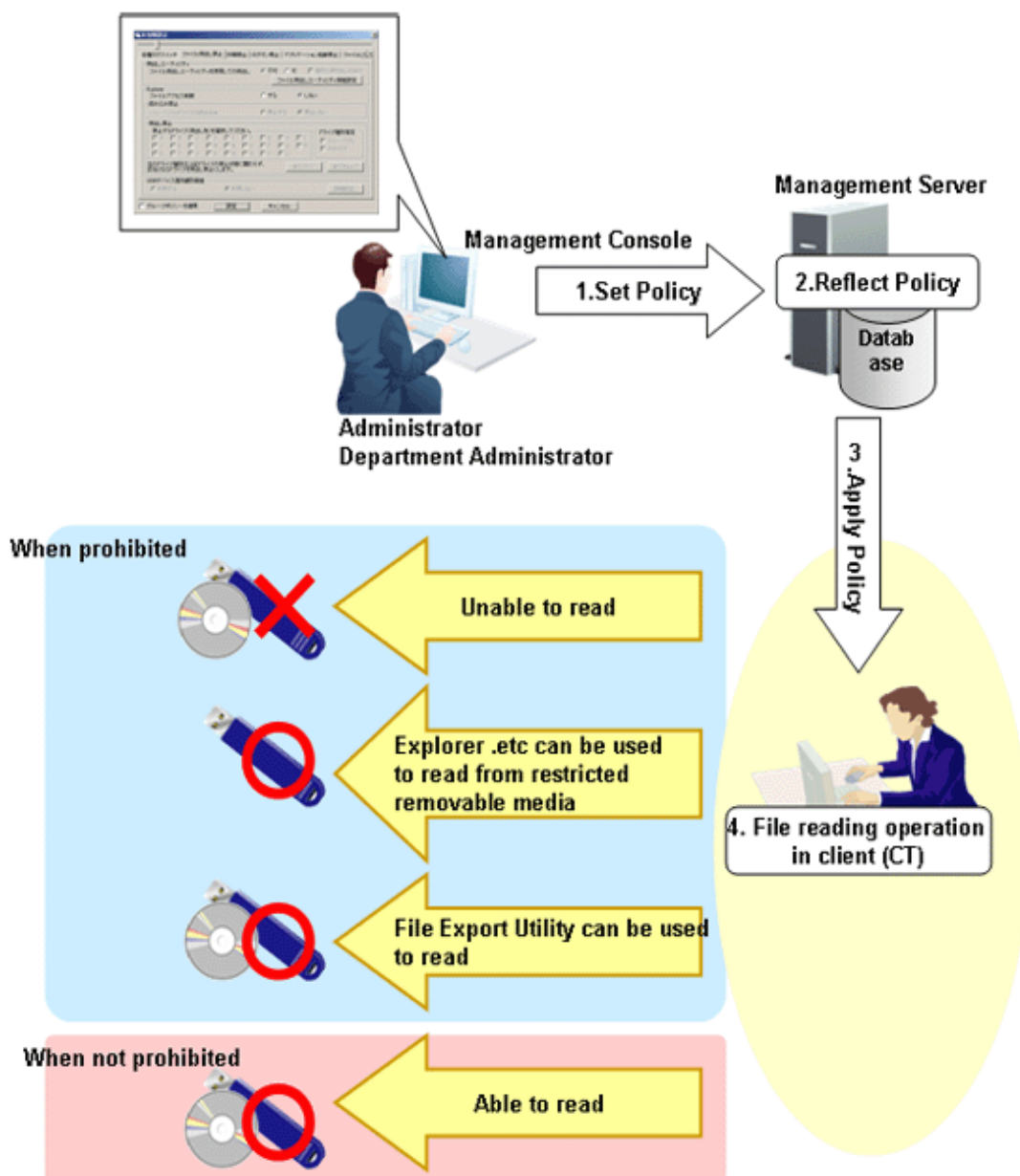
When decrypting the file exported with encryption by using File Export Utility, the following window will be displayed if the time has exceeded [Decryption Deadline] displayed in the [Encrypted File Settings,] but the decryption operation can still be performed, and the encrypted file will be deleted.



## 8.1.2 File Reading Prohibition

When the file reading prohibition policy has been set, reading data on a removable drive, network drive or DVD/CD of the client (CT) PC can be prohibited.

### Steps to make prohibition effective through policy setting





1. Set Policy  
Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after Management Console is started (CT policy settings window).  
Set [File access control] of the [File Export Prohibition] tab to [Yes].  
Select the media prohibited to be read in [Reading prohibition] of the [File Export Prohibition] tab.
2. Reflect Policy  
The set policy will be reflected to the database.
3. Apply Policy  
The set policy will be applied to the client (CT).
4. File reading operation  
When intending to read files and folders in the client (CT), the status will become one of the following:
  - Unable to read (Note 1)
  - Explorer .etc can be used to read from restricted removable media (Note 2)
  - File Export Utility can be used to read (Note 3)
  - Able to read

Note 1: Please set a policy that disables the use of File Export Utility.

Note 2: Please limit the available removable media in [USB Device Individual Identification Function] of the [File Export Prohibition] tab. USB devices that are not specified cannot be read. For how to register and set permitted USB devices, please refer to “[7.5 Export Files to Specified USB Device Only](#)”.

Note 3: When the policy that allows the use of File Export Utility is set. It indicates that the exported file name and folder structure can be confirmed in the [View export target] window of File Export Utility (file cannot be opened).

### 8.1.3 Printing Prohibition

---

By setting the printing prohibition policy, printing of applications that are specified can be prohibited in the client (CT) PC.

When the number of pages permitted to be printed has been set in the policy of monitoring the number of pages for printing, printing can be prohibited if the set number of pages is reached.



#### Note

---

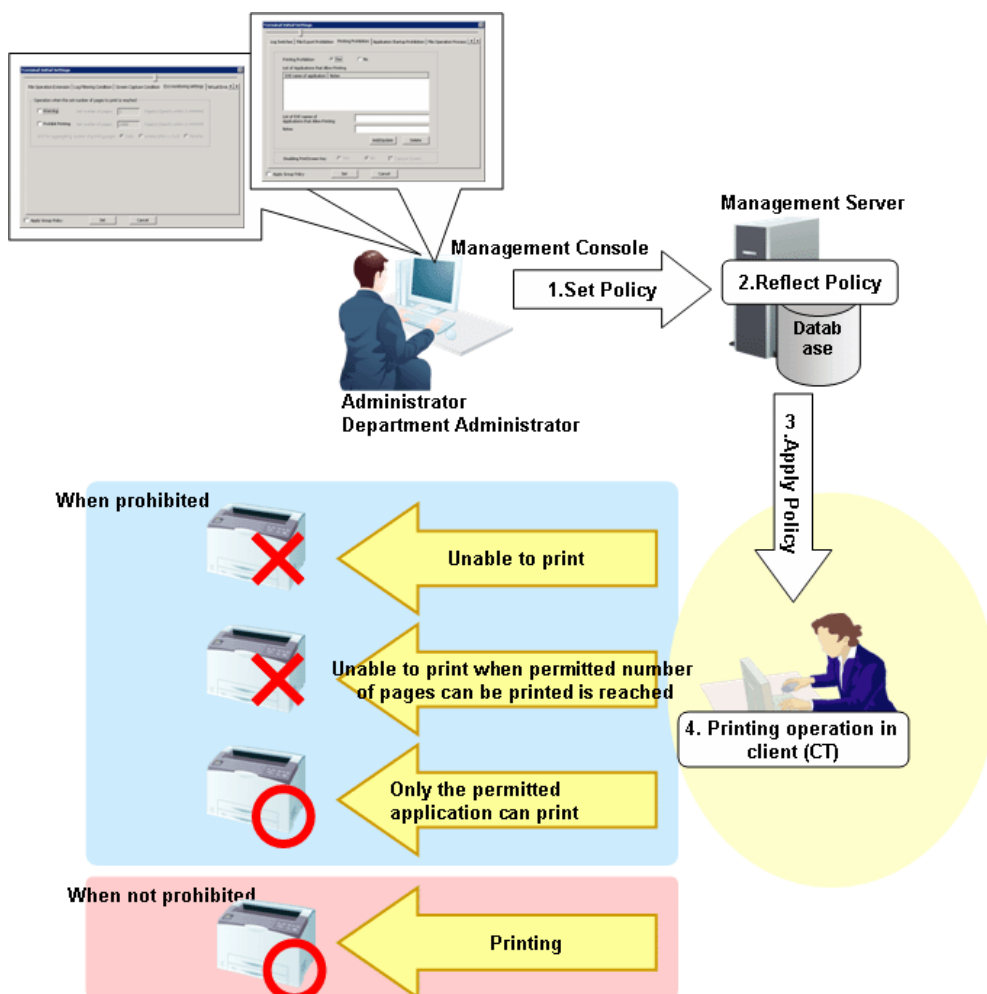
##### **Functions may be restricted due to the environment being used**

When setting the policy, functions may be restricted due to the environment being used.

For details, please refer to “[1.2.9 Printing Prohibition](#)”.

---

## Steps to make prohibition effective through policy setting



### 1. Set Policy

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after Management Console is started (CT policy settings window).

Set the conditions for prohibiting printing in the [Printing Prohibition] tab.

Set the conditions for prohibiting printing in the [Eco monitoring settings] tab.

### 2. Reflect Policy

The set policy will be reflected to the database.

### 3. Apply Policy

The set policy will be applied to the client (CT).

### 4. Printing operation

When intending to print through applications in the client (CT), the status will become one of the following:

- Unable to print
- The number of pages permitted to be printed is reached, unable to print
- Printing can be performed through permitted applications only
- Any printing can be performed

## When prohibited

When printing with an unpermitted application, the prohibition window will be displayed in the client (CT). The window is as follows:



## 8.1.4 Logon Prohibition

---

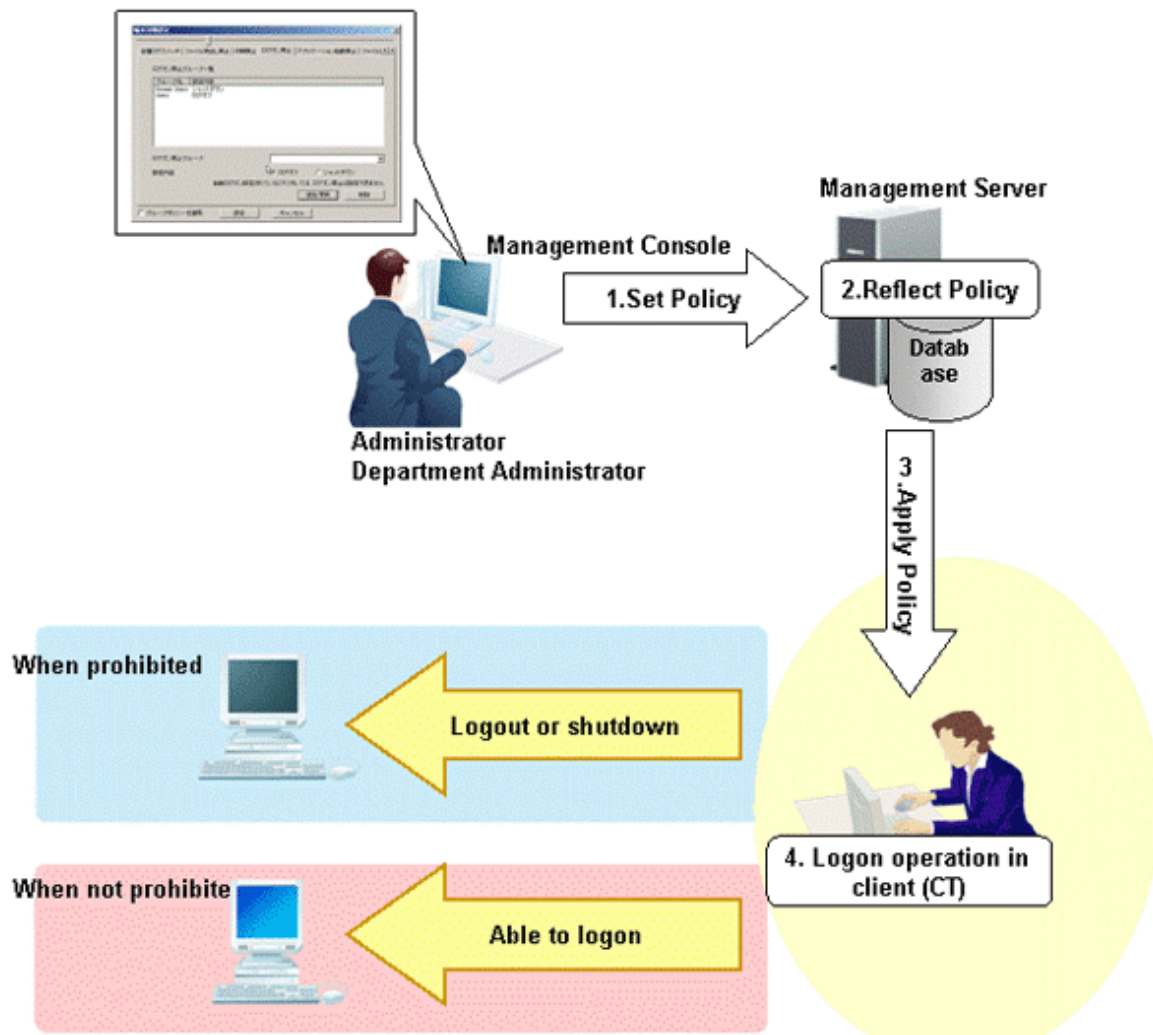
**This function is not available.**

By setting the logon prohibition policy, logon with a user name that belongs to the specified group can be prohibited in the client (CT) PC. Groups that can be prohibited are as follows:

- Administrators
- Backup Operators
- Debugger Users
- Power Users
- Guests
- Replicator
- Users
- Domain Admins
- Domain Guests
- Domain Users
- Enterprise Admins
- Group Policy Creator Owners

In case of domain logon, if the same user ID exists in the local computer, the group to which the local user belongs will be prohibited from logon.

## Steps to make prohibition effective through policy setting



### 1. Set Policy

Set the group prohibited from logon in the [Terminal Initial Settings] window or the [Logon Prohibition] tab in the window after the Management Console is started (CT policy settings window).

In [Start Time of Logon Prohibition] of the [Terminal Initial Settings] window, set the time interval from the time when logging on is detected to the time when prohibition is performed (logoff or shutdown).

### 2. Reflect Policy

The set policy will be reflected to the database.

### 3. Apply Policy

The set policy will be applied to the client (CT).

### 4. Logon operation

When logging on to the client (CT), the status will become one of the following:

- When logging on with a user name that belongs to a prohibited group, the client (CT) will be logged off or shut down.
- When logging on with the user name that belongs to any other group, the client (CT) will log on.

## When prohibited

When logging on to the client (CT) with a user name that belongs to a prohibited group, according to policy settings, the following prohibition window will be displayed in the client (CT).

However, if [Prohibit Immediately] is selected in [Start Time of Logon Prohibition] of the [Terminal Initial Settings] window, the prohibition window will not be displayed.

- When the client (CT) is logged off



- When the client (CT) is shut down



## 8.1.5 Application Startup Prohibition

---

By setting the application startup prohibition policy, the startup of specified applications can be prohibited in the client (CT) PC.

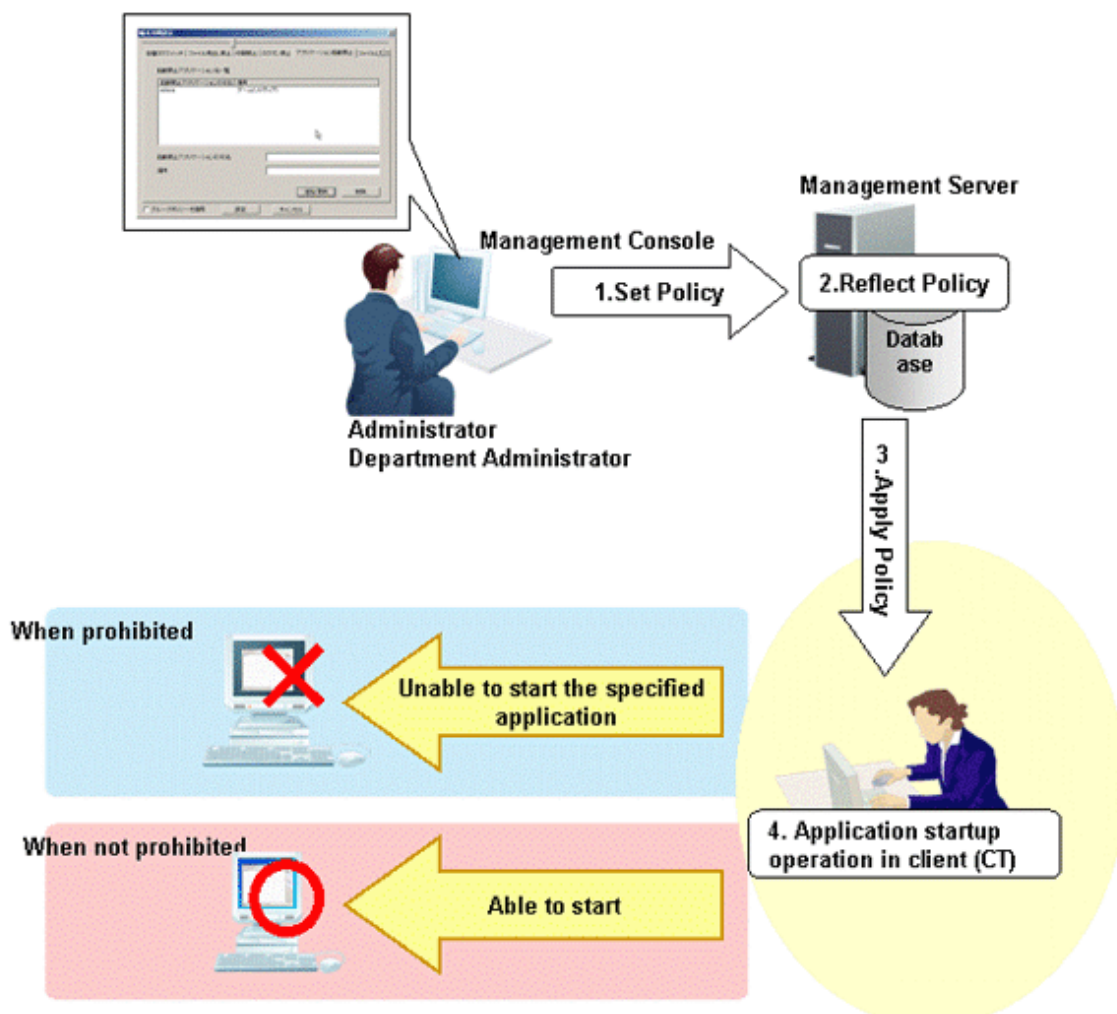


### Note

#### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.  
For details, please refer to "[1.2.11 Application Startup Prohibition](#)".

## Steps to make prohibition effective through policy setting



### 1. Set Policy

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set applications prohibited from startup in the [Application Startup Prohibition] tab.

### 2. Reflect Policy

The set policy will be reflected to the database.

### 3. Apply Policy

The set policy will be applied to the client (CT).

### 4. Application startup operation

When starting applications in the client (CT), the status will become one of the following:

- The specified applications cannot be started
- Any application can be started

## When prohibited

When the startup of application is prohibited, the prohibition window will be displayed in the client (CT). The window is as follows:



## 8.1.6 E-mail Attachment Prohibition

---

**This function is not available.**

By setting the E-mail attachment prohibition policy, attaching a prohibited file to an E-mail to send or save can be prohibited in the client (CT) PC.

Specify the file to be prohibited in the policy.

In case of port monitoring mode, even if there is only one prohibited file in the attachment, the E-mail (message body and all attachment) cannot be sent.

In V12.0L20-V13.0.0 compatible mode, it has nothing to do with the settings of recipient address confirmation when sending an E-mail; if a prohibited file and non-prohibited file exist at the same time, the E-mail will be sent only with the non-prohibited file attached. When an E-mail is sent with just a prohibited file attached, only the E-mail text will be sent.



### Note

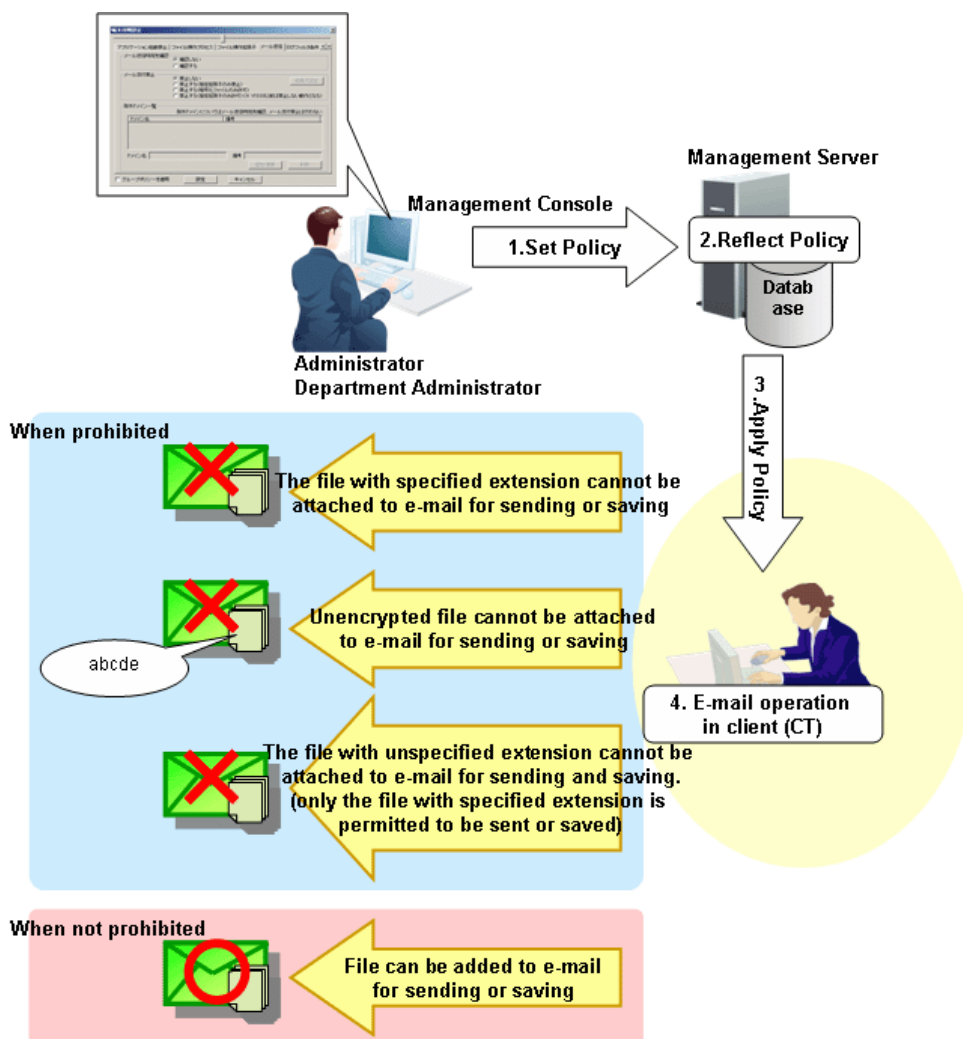
.....

**Functions may be restricted due to the environment being used**

When setting the policy, functions may be restricted due to the environment being used.

.....

## Steps to make prohibition effective through policy setting



1. Set Policy  
Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).  
Set the conditions for prohibiting E-mail attachments in the [E-mail Sending] tab.
2. Reflect Policy  
The set policy will be reflected to the database.
3. Apply Policy  
The set policy will be applied to the client (CT).
4. E-mail operation  
When sending an E-mail in the client (CT), the status will become one of the following:
  - Files with specified extension cannot be attached to the E-mail to send or save
  - Files that are not encrypted cannot be attached to the E-mail to send or save
  - Files without specified extension cannot be attached to the E-mail to send or save (Only files with specified extension can be sent or saved)
  - Files can be attached to the E-mail to send or save



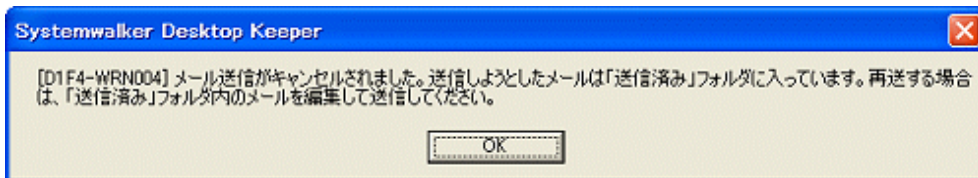
## When prohibited

When the E-mail attachment is prohibited, the prohibition window will be displayed in the client (CT). The window is as follows.

### In V12.0L20~V13.0.0 compatible mode



### In port monitoring mode



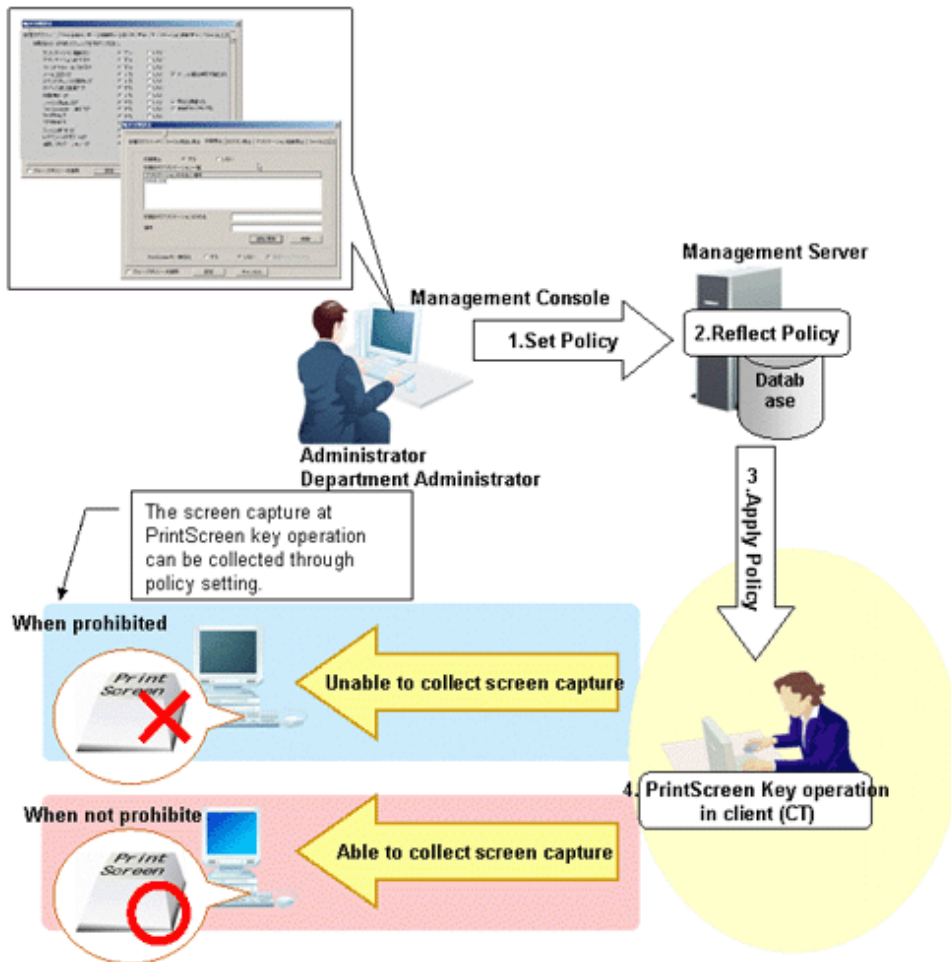
## 8.1.7 PrintScreen Key Prohibition

---

By setting the PrintScreen key prohibition policy, collecting a hard copy of screen using the PrintScreen key on the keyboard can be prohibited in the client (CT) PC.

In addition, the screen capture can still be collected during prohibition.

## Steps to make prohibition effective through policy setting



### 1. Set Policy

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set [Disabling PrintScreen Key] to [Yes] in the [Printing prohibition] tab.

When collecting the window with the PrintScreen key operation, select the [Capture Screen] checkbox.

### 2. Reflect Policy

The set policy will be reflected to the database.

### 3. Apply Policy

The set policy will be applied to the client (CT).

### 4. PrintScreen Key operation

When operating the PrintScreen key in the client (CT), the status will become one of the following:

- Hard copy of screen cannot be collected after pressing the PrintScreen key  
When the [Capture Screen] checkbox is selected in Step 1, the window of PrintScreen key operation will be collected
- Hard copy of screen can be collected after pressing the PrintScreen key

## When prohibited

When the use of PrintScreen key is prohibited, the prohibition window will be displayed in the client (CT). The window is as follows. When the collection of screen capture during prohibition is set, the screen capture at PrintScreen key operation will be collected.



## 8.1.8 URL Access Prohibition

---

By setting the URL access prohibition policy, access to the URL that is not permitted by the administrator can be prohibited in the client (CT) PC.



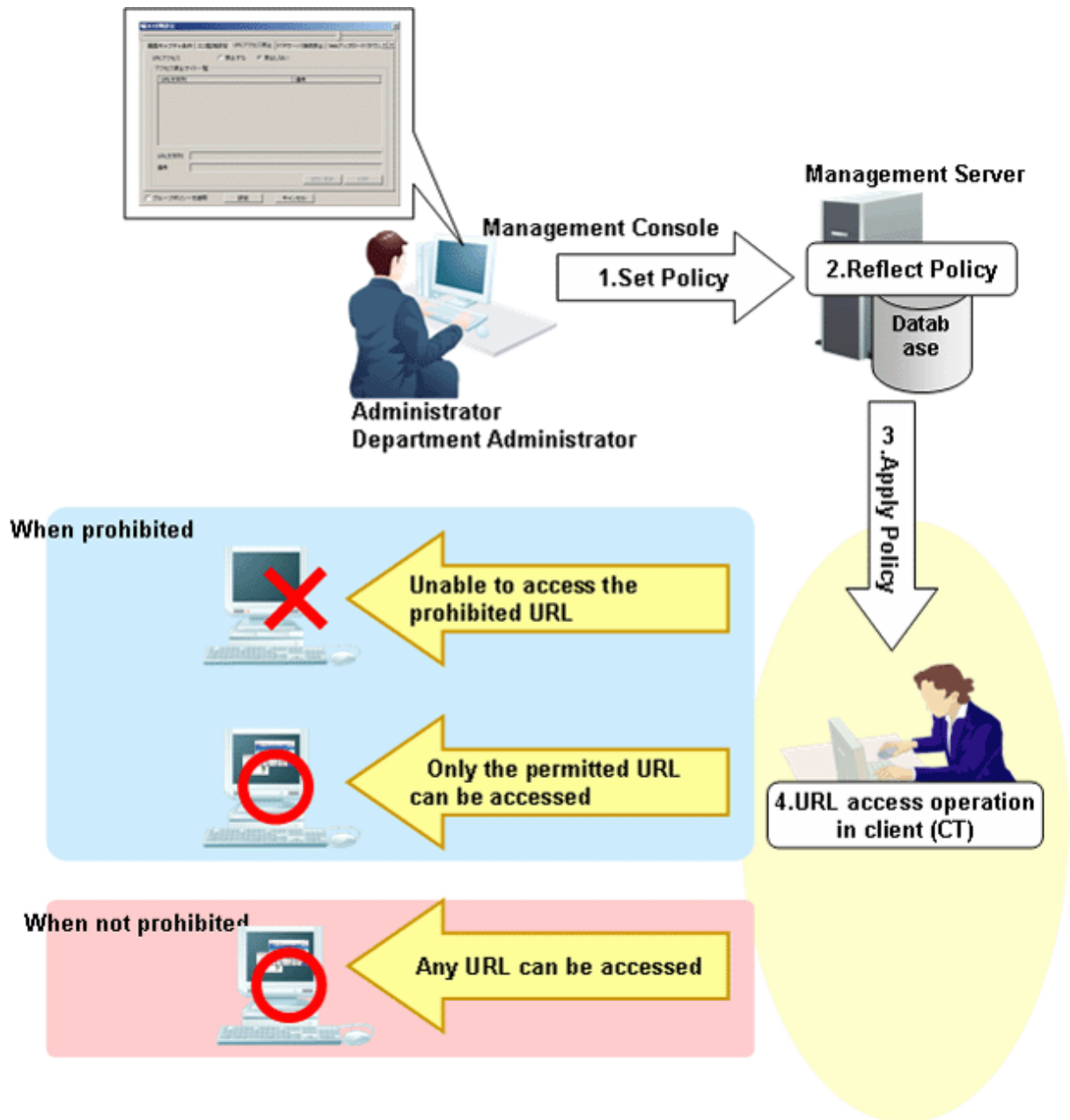
.....

### **Functions may be restricted due to the environment being used**

When setting the policy, functions may be restricted due to the environment being used.  
For details, please refer to "[1.2.12 URL Access Prohibition](#)".

.....

## Steps to make prohibition effective through policy setting

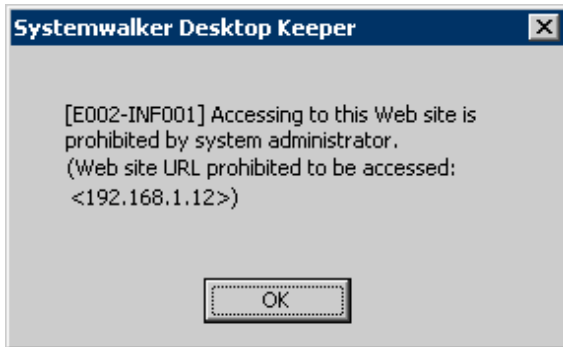


1. Set Policy  
Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).  
Set [URL access] to [Prohibit] in the [URL Access Prohibition] tab.
2. Reflect Policy  
The set policy will be reflected to the database.
3. Apply Policy  
The set policy will be applied to the client (CT).
4. URL access operation  
When accessing to URL in the client (CT), the status will become one of the following:
  - The Unable to access the prohibited URL
  - The Only the permitted URL can be accessed

- Any URL can be accessed  
Log at that time will be collected as window title obtaining log.

### When prohibited

When there is only one tab displayed on the Web page, Internet Explorer® will be closed by force when accessing the prohibited URL. When there are multiple tabs displayed on the Web page, only the tab that accesses the prohibited URL will be closed by force. Then, the following message will be displayed.



## 8.1.9 FTP Server Connection Prohibition

---

By setting the FTP server connection prohibition policy, access to the FTP server that is not permitted by the administrator can be prohibited in the client (CT) PC.



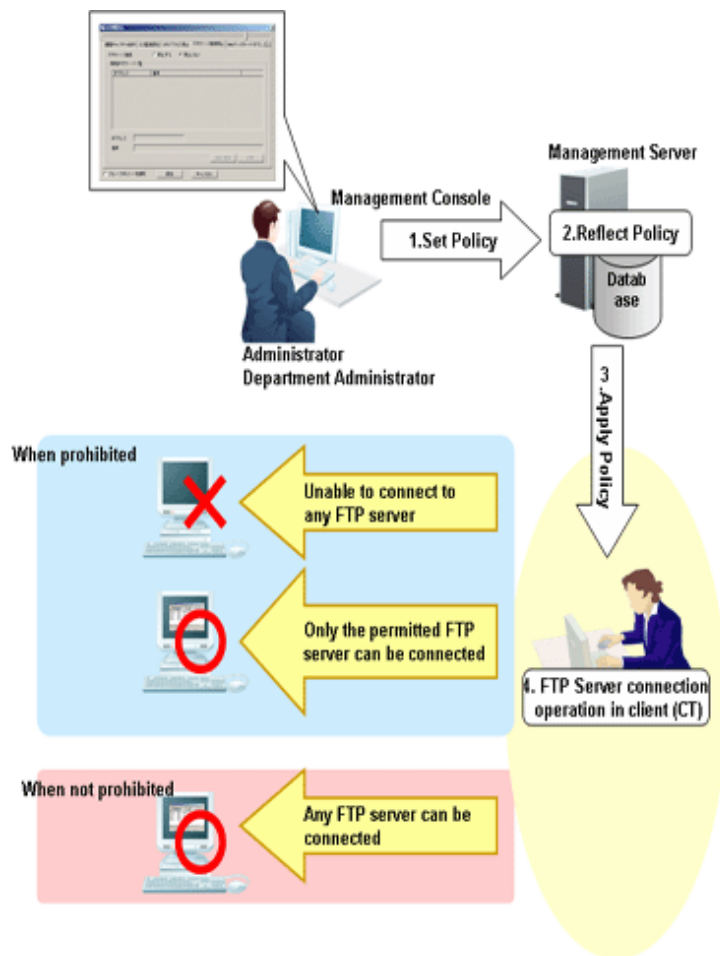
.....

### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used. For details, please refer to "[1.2.13 FTP Server Connection Prohibition](#)".

.....

## Steps to make prohibition effective through policy setting



### 1. Set Policy

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set [FTP Server Connection] to [Prohibit] in the [FTP Server Connection Prohibition] tab.

### 2. Reflect Policy

The set policy will be reflected to the database.

### 3. Apply Policy

The set policy will be applied to the client (CT).

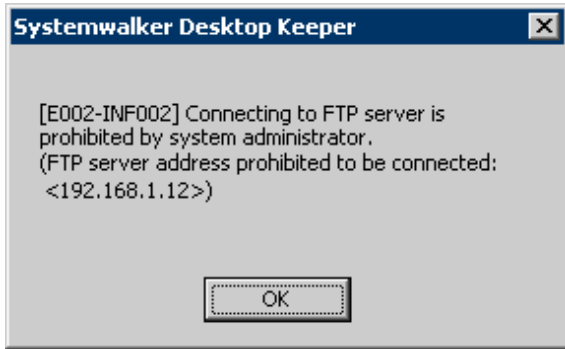
### 4. Operation of connecting to FTP server

When connecting to an FTP server in the client (CT), the status will become one of the following:

- No FTP server can be connected
- Only the permitted FTP server can be connected
- Any FTP server can be connected

## When prohibited

The following message will be displayed.



## 8.1.10 Web Upload and Download Prohibition

---

By setting the Web upload and download prohibition policy, uploading to and downloading from a Website that is not permitted by the administrator can be prohibited in the client (CT) PC.



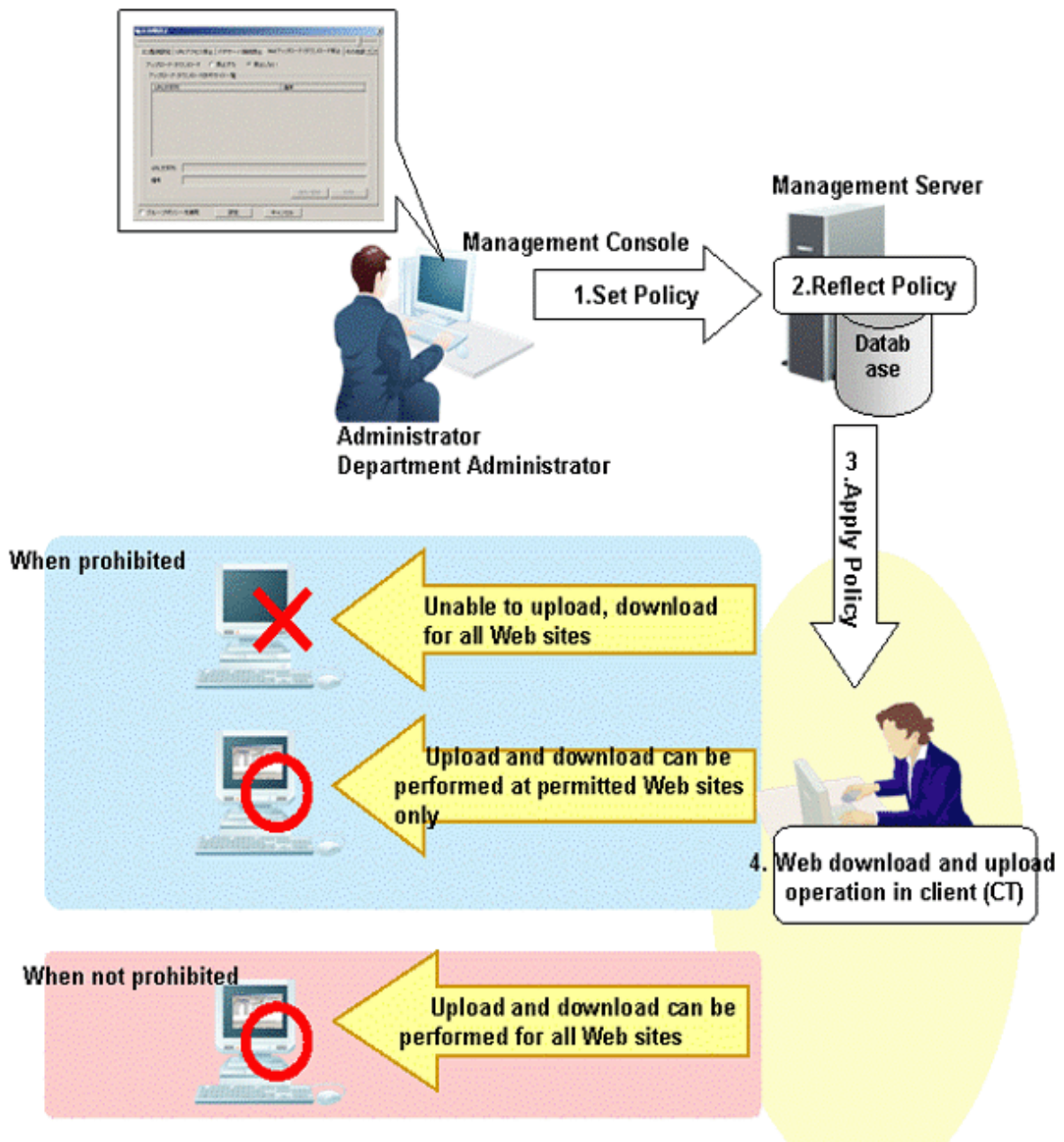
.....

### **Functions may be restricted due to the environment being used**

When setting the policy, functions may be restricted due to the environment being used. For details, please refer to “[1.2.14 Web Upload and Download Operation Prohibition](#)”.

.....

## Steps to make prohibition effective through policy setting



1. Set Policy  
Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).  
Set [Upload and Download] to [Prohibit] in the [Web Upload and Download Prohibition] tab.
2. Reflect Policy  
The set policy will be reflected to the database.
3. Apply Policy  
The set policy will be applied to the client (CT).
4. Web download and upload operation  
When accessing a Website in the client (CT), the status will become one of the following:
  - Upload and download cannot be performed on all Web sites
  - Upload and download can only be performed on the permitted Web sites

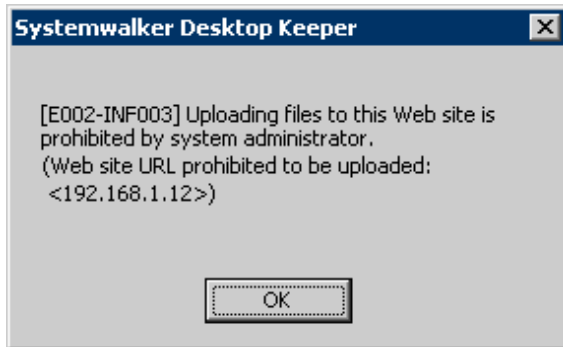


- Upload and download can be performed on all Web sites

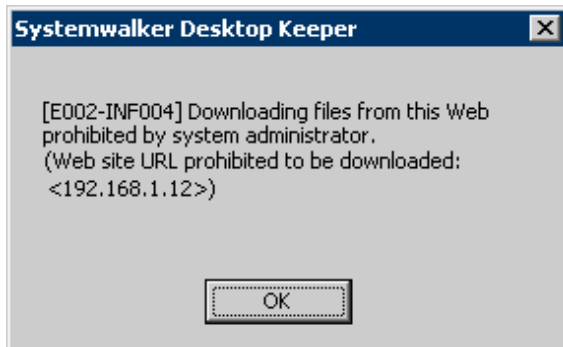
## When prohibited

The following message will be displayed.

- Example of upload prohibition



- Example of download prohibition



## 8.1.11 Clipboard Operation Prohibition

By setting the clipboard operation prohibition policy, copying information between the virtual environment and the physical environment with the client (CT) installed via clipboard can be prohibited. The prohibition will be performed in the environment where the information is pasted.



### Note

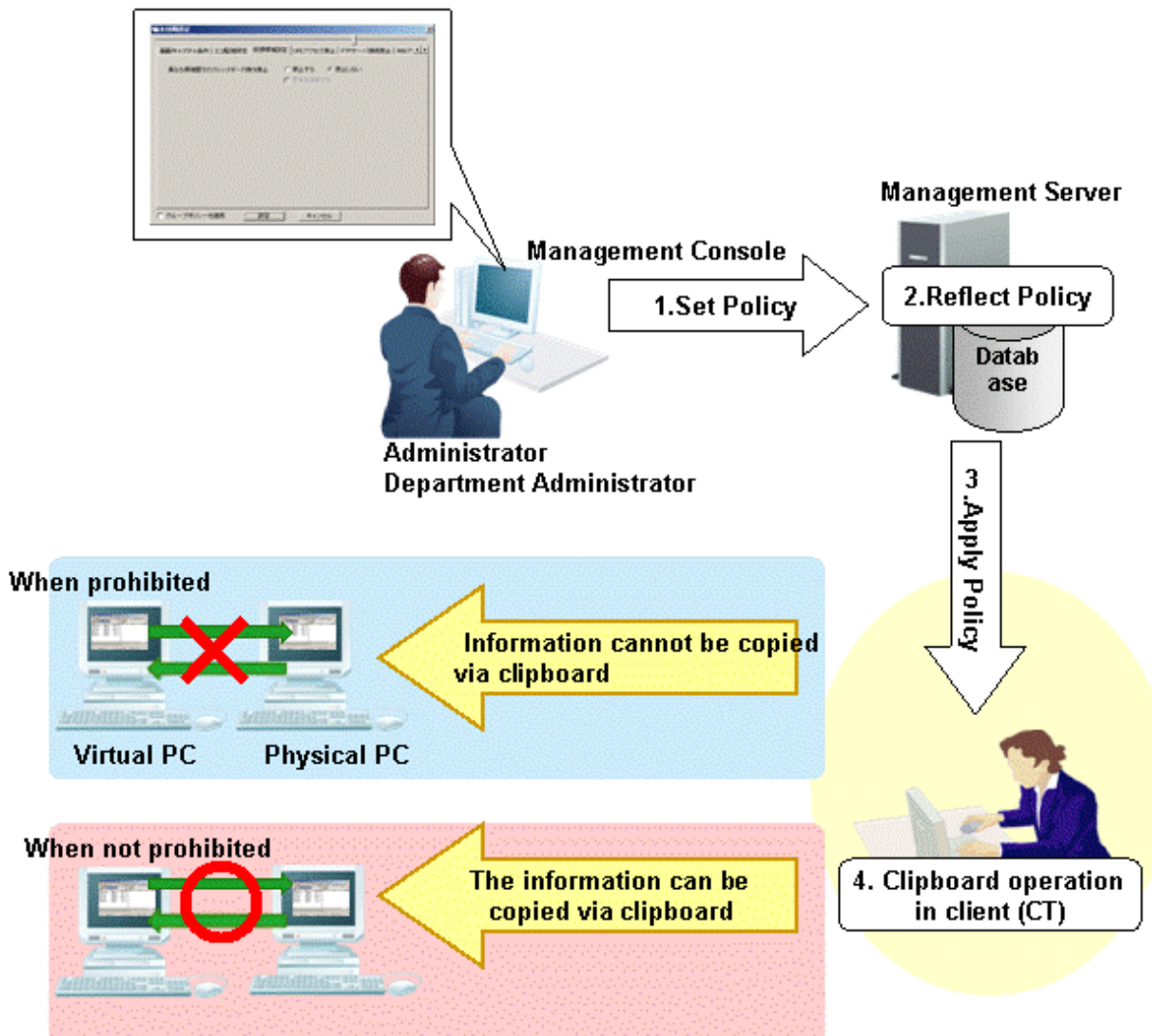
---

#### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used. For details, please refer to "[1.2.15 Clipboard Operation Prohibition](#)".

---

## Steps to make prohibition effective through policy setting



### 1. Set Policy

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set [Prohibit of clipboard operation between different environments] to [Prohibit] in the [Virtual Environment setup] tab.

### 2. Reflect Policy

The set policy will be reflected to the database.

### 3. Apply Policy

The set policy will be applied to the client (CT).

### 4. Clipboard operation

When copying information from the virtual environment to the physical environment or from the physical environment to the virtual environment via clipboard, the status will become one of the following:

- Information cannot be copied via clipboard
- The information can be copied via clipboard

## 8.2 Policy Settings of Record Function

This section describes the logs that can be collected by record function.

## Operation logs that can be collected

Set the policy to decide what kind of operation logs will be collected. Operation logs that can be collected are as follows. The policy is set by the system administrator or department administrator in the Management Console.



---

### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

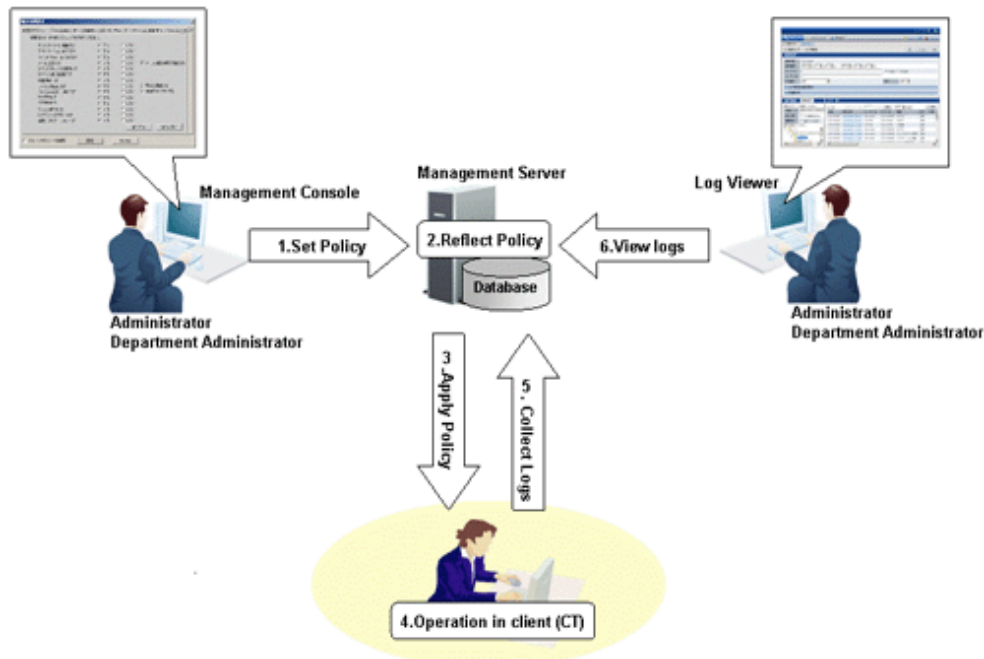
For details, please refer to “[1.2.16 All Logs](#)” - “[1.2.30 About Collection of Logs for Investigation of Client \(CT\)](#)”.

---

- Application startup log
- Application termination log
- Application startup prohibition log
- Window title obtaining log
- E-mail sending log
- E-mail sending interruption log
- **This function is not available.**
- E-mail attachment prohibition log
- **This function is not available.**
- Command log  
**This function is not available**
- Device configuration change log
- Printing log
- Printing prohibition log
- Logon prohibition log
- This function is not available.
- File export log
- PrintScreen key operation log
- PrintScreen key prohibition log
- Web operation log
- Web operation prohibition log
- FTP operation log
- FTP operation prohibition log
- Clipboard operation log
- Clipboard operation prohibition log
- File operation log
- Logon/logoff log
- Linkage application log
- Configuration change log

## Steps of viewing logs through policy setting

CT operation log



### 1. Set Policy

Set the policy for collecting various logs in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after starting the Management Console (the CT policy settings window).

### 2. Reflect Policy

The set policy will be reflected to the database.

### 3. Apply Policy

The set policy will be applied to the client (CT).

### 4. Operations in client (CT)

The client (CT) user performs various operations.

### 5. Collect Logs

Logs collected in the client (CT) will be sent to the Management Server.

When the client (CT) can communicate with the connected Management Server

The logs collected in the client (CT) will be sent to the Management Server according to the policy set in the [Other Settings] tab of the policy settings window.

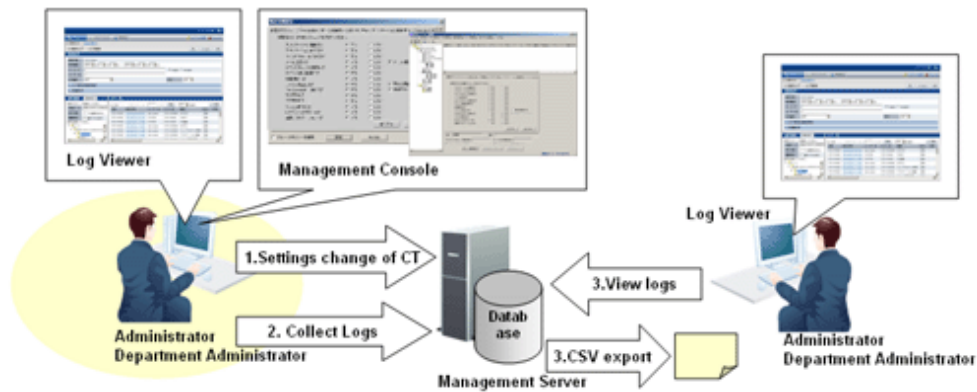
When the client (CT) cannot communicate with the connected Management Server

Logs collected in the client (CT) will be saved in the client (CT) temporarily. When the client (CT) can communicate with the connected Management Server, the logs collected in the client (CT) will be sent to the Management Server according to the policy set in the [Other Settings] tab of the policy settings window.

### 6. View logs

The collected logs are viewed in Log Viewer.

## Configuration change log



1. Configuration change of client (CT)  
Change the settings information of the client (CT) in the Management Console or Log Viewer.
2. Collect Logs  
The configuration change operation will be saved in the Management Server as a log.
3. View logs
  - View the configuration change operation performed in the Management Console in Log Viewer.
  - View the configuration change operation that is performed in Log Viewer (cannot be displayed in the [List of Configuration Change Logs]) and output to a CSV file. For details about the command for outputting configuration change logs in CSV format, please refer to “DTKSTCV.EXE (output configuration change log)” of “Systemwalker Desktop Keeper Reference Manual”.

## View logs

View the collected logs in Log Viewer.

[Example of CT Operation Log]

The screenshot shows the Log Viewer application interface. At the top, there are tabs for 'Log Viewer', 'Log Analyzer', and 'Environment Setup'. The main window title is 'CT Operation Log | Configuration Change Log'. Below this, there is a search section titled 'CT Operation Log(Operat) - Log search' with buttons for 'Back', 'Output in CSV format', and 'Search'. The search conditions are set to: Search target: WIN-264043-808, Search range: 2006 Year 2 Month 17 Day - 2012 Year 2 Month 17 Day, Keyword: (empty), User ID: (empty), Type of log: All, and Classification: All. Below the search section, there are expandable sections for 'Type of log (Multiple choices)' and 'Detailed conditions'. The main area displays a 'List of logs' table with columns: Name, Date and time, User name, Domain name, Variety, Classification, and Content. The table shows several log entries for the target server WIN-S220(YJ0800)10.197.143.166, including logons, logoffs, and system events like PC shutdown and startup.

Name	Date and time	User name	Domain name	Variety	Classification	Content
WIN-264043-808	2012/02/17 09:25	Administrator	WIN-264043-808	Logon	Normal	Logged on. Authentication
WIN-264043-808	2012/02/17 09:27	Administrator	WIN-264043-808	Logoff	Normal	Logged off
WIN-264043-808	2012/02/17 09:27	SYSTEM	WIN-264043-808	PC shutdown	Normal	Powered off the computer
WIN-264043-808	2012/02/17 09:28	SYSTEM	WIN-264043-808	PC startup	Normal	Started the computer. Sta
WIN-264043-808	2012/02/17 09:27	Administrator	WIN-264043-808	Logon	Normal	Logged on. Authentication
WIN-264043-808	2012/02/17 09:28	Administrator	WIN-264043-808	Logoff	Normal	Logged off

For items that can be viewed in Log Viewer, please refer to “5.2.1 View Logs in [CT Operation Log] Window ” or “5.2.2 View in [Configuration Change Log] ”.

## 8.2.1 Application Startup Log

This is the log when an application with a window is started in the client (CT). Application startup logs cannot be collected in the case of an application without a window.

Application startup logs without a window displayed (but with an invisible window) will be collected.

### How to apply

When collecting application startup logs, the user who starts the application and the application that is started can be known. An unnecessary application for business that has been started and the person who starts the application that might cause information disclosure can be found. Whether the system is being used according to the rules can be judged.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

In the [Log Switches] tab, set [Application Startup Log] to [Yes].

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [Application Startup] (fixed value)

**[Classification]:** normal

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed.

- Name of the started application (\*)

Example of [Content]

```
Started [iexplore].
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

**[Note]:** (not displayed)

## 8.2.2 Application Termination Log

---

This is the log when the application with a window is terminated in the client (CT). When terminating the application without a window, an application termination log cannot be collected.

### How to apply

When collecting an application termination log, the user who terminates the application and the application that is terminated can be known.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after Management Console is started (CT policy settings window).

In the [Log Switches] tab, set [Application Termination Log] to [Yes].

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [Application Termination] (fixed value)

**[Classification]:** normal

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed.

- Name of the terminated application (\*)

Example of [Content]

```
Ended [iexplore].
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Note]: (not displayed)

## 8.2.3 Application Startup Prohibition Log

---

This is the log when intending to start an application with a window that is prohibited from startup in the client (CT). When starting an application without a window, the application startup prohibition log cannot be collected.

The application startup prohibition log without a window displayed (but with an invisible window) will be collected.

### How to apply

When collecting the application startup prohibition log, whether the unnecessary application to the business, one that is prohibited to be used, has attempted to be started and the person who started the application that might cause information disclosure can be known. Whether the system is being used according to the rules can be judged.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set the name of the application that is prohibited from startup in the [Application Startup Prohibition] tab.

### Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user name of the client (CT)

[Domain Name]: it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

[Type]: [Application Startup Prohibition] (fixed value)

[Classification]: violation

[Attachment]: (not displayed)

[Content]: the following content is displayed:

- Name of the prohibited application (\*)
- Prohibition processing ([Ended by force])
- Prohibition results ([Succeeded] or [Failed])

Example of [Content]

```
Startup of [calc][Ended by force]. Result: [Succeeded]
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Notes]: (not displayed)



## 8.2.4 Window Title Obtaining Log

---

This is the log when the window is displayed in the case that the application with a window is started in the client (CT). When starting an application without an window, the window title obtaining log cannot be collected.

When using “Microsoft® Internet Explorer® 6.0 Service Pack1 or later”, “Windows® Internet Explorer® 7”, “Windows® Internet Explorer® 8”, “Windows® Internet Explorer® 9” or “Explorer”, if any of the following conditions is satisfied, “URL Information Displayed on Address Bar” will also be collected as window title obtaining log.

- “http://”, “https://” or “ftp://” is contained in URL information.
- “:\” is not contained in the second or third byte in URL information.
- The beginning of URL information is not “\”.

However, when switching among the following applications, if “Application Window Title” and “URL Information Displayed on Address Bar” are exactly the same as the previous ones, window title obtaining log will not be collected.

- Internet Explorer® and Explorer
- Internet Explorer® and Internet Explorer®
- Explorer and Explorer



### Note

---

#### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.  
For details, please refer to “[1.2.19 Window Title Obtaining Log](#)”.

---

### Set policy for collection

The Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after Management Console is started (CT policy settings window).

- In the [Log Switches] tab, set [Window Title Obtaining Log] to [Yes].
- In the [Log Filtering Conditions] tab, set the filtering conditions for window title obtaining log.  
The settings can be performed when [Window Title Obtaining Log] is set to [Yes].
- In the [Screen Capture Conditions] tab, set the conditions for collecting screen capture.  
The settings can be performed when [Window Title Obtaining Log] is set to [Yes].

For details about the configuration value, please refer to “[2.4.1.9 Settings of \[Log Filtering Condition\] Tab](#)” and “[2.4.1.10 Settings of \[Screen Capture Condition\] Tab](#)”.

### Log filtering conditions

Items that can be set in log filtering conditions are as follows:

- Filtering settings for repeated logs  
For logs with the same process name and the same window title, only the log at the first time will be collected.
- Keyword filtering  
Set the process name and keyword. Only the window title obtaining log of which the process name contains the keyword will be collected or excluded.



### Note

---

The settings of filtering conditions for repeated logs may be invalid sometimes

When logs with the same process ID switch windows mutually, the filtering settings for repeated logs will be invalid.

[Example]

When the word documents with window title A and B is opened, and active window switching of A→B→A is performed.

## Screen capture

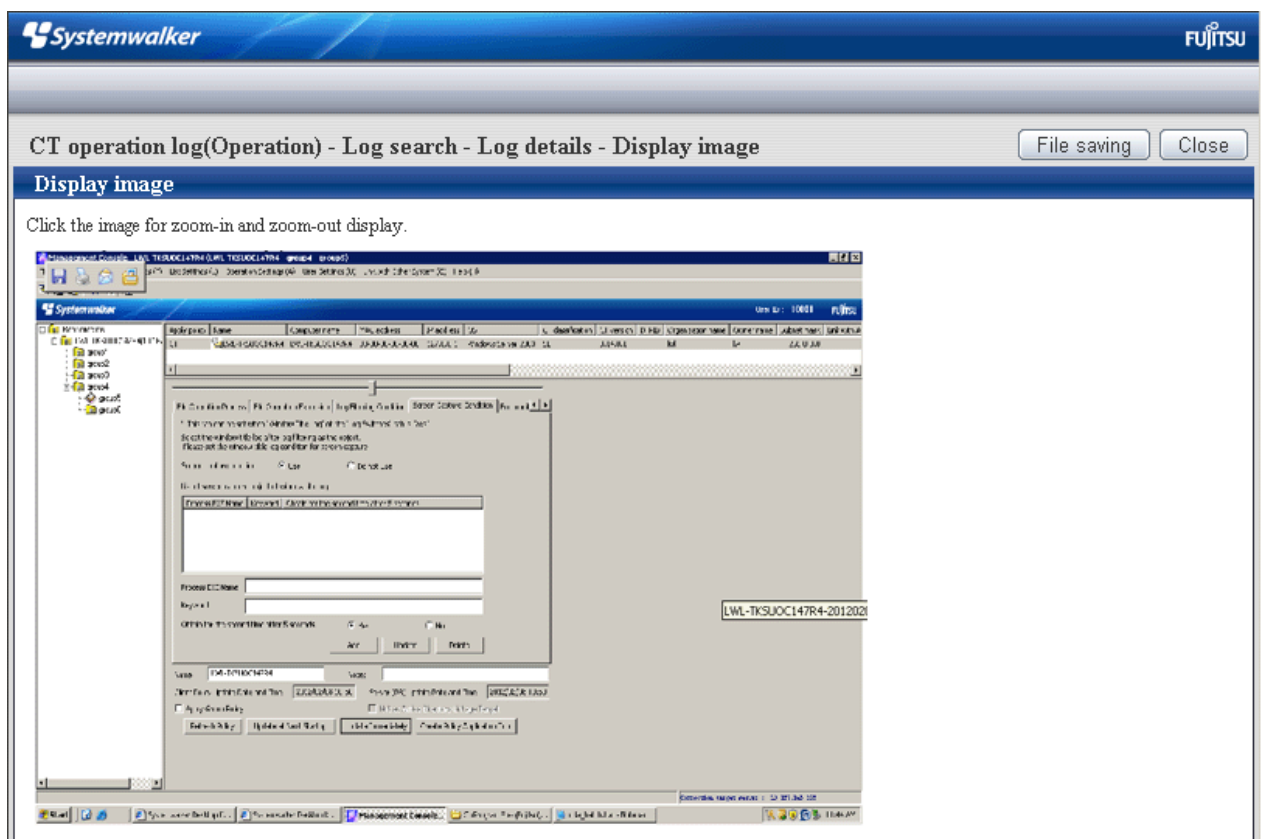
In screen capture conditions, set the name of the process to collect screen capture and the keyword contained in the window title.

The screen capture can be viewed in window title obtaining log.

In terminal operation settings, when [CT] is selected as [Attached data accumulation settings], screen capture data will be saved to the client (CT).

Logs that can be viewed are as follows:

- Collected window
- “Display Result of Logs”



## Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user name of the client (CT)

[Domain Name]: it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

[Type]: [Window Title] (fixed value)

[Classification]: normal

[Attachment]: when attached data (screen capture) exists, display "1" or "2"

[Content]: the following content is displayed.

- Window title name of application (\*)
- Name of started application (\*)

Example of [Content]

```
Window [Start menu] has been detected. Program name: [Explorer]
```

[Note]: The URL of page that is displayed through browser is displayed. (\*)

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

## 8.2.5 E-mail Sending Log

---

This is the log when an E-mail is sent in the client (CT).

When the warning message for confirming the recipient address is displayed during E-mail sending, the logs when sending after confirming the recipient address will also be collected.



### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

For details, please refer to "1.2.20 E-mail Sending Log".

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

- In the [Log Switches] tab, set [E-mail Sending Log] to [Yes].
- When [E-mail content can be viewed] is selected in the [Log Switches] tab, the content and the attachment of the sent E-mail will be saved and can be viewed in Log Viewer.  
The settings can be performed when [E-mail Sending Log] is set to [Yes].
- In the [E-mail Sending] tab, set [Confirm the Recipient Address When Sending E-mail] to [OK].
- **This function is not available.**

### Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: the following information will be displayed:

- When logging on: logon user name of the client (CT)
- When not logging on: SYSTEM (fixed)

[Domain Name]: the following information is displayed.

- When logging on to the domain: it is the domain name of client (CT).
- When logging on to the local computer: it is the computer name of client (CT).
- When not logging on: it is the computer name of client (CT)

[Type]: [E-mail Sending] (fixed value)

[Classification]: normal

[Attachment]: when attached data (content and attachment of the sent E-mail) exists, display "1"

[Content]: the following content is displayed:

- E-mail title (\*)
- Address of sender (\*)
- Address of recipient (To, Cc and Bcc information) (\*)
- Attachment name (\*)

Example of [Content]

```
E-mail has been sent. [Subject: Today's Business Report From: E-mail Address-A To: E-mail Address-B  
CC: E-mail Address-C E-mail BCC: Address-D]
```

\*\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Note]: the following content will be displayed when the warning message for confirming the recipient address is displayed during E-mail sending.

- E-mail address of the unauthorized domain (\*\*)
- Processing result after the warning message is displayed (\*\*)

Example of [Notes]

```
Warning address: [xxxx] Result: [Send After Confirmation]
```

\*\*) When performing keyword search in Log Viewer, it can be specified as keyword.

## 8.2.6 E-mail Sending Suspension Log

---

**This function is not available.**

This is the log collected when the sending is cancelled in case that the warning message for confirming the recipient address is displayed during E-mail sending.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

- In the [Log Switches] tab, set [E-mail Sending Log] to [Yes].
- When [E-mail content can be viewed] is selected in the [Log Switches] tab, the content and the attachment of the E-mail that is suspended to be sent will be saved and can be viewed in Log Viewer.
- In the [E-mail Sending] tab, set [Confirm Recipient Address When Sending E-mail] to [OK].

### Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user name of the client (CT)

[Domain Name]: the following information is displayed.

- When logging on to the domain: it is the domain name of client (CT).
- When logging on to the local computer: it is the computer name of client (CT).

[Type]: [E-mail Sending Suspension] (fixed value)

[Classification]: normal

[Attachment]: when attached data (content and attachment of the sent E-mail) exists, display "1"

[Content]: E-mail address of the unauthorized domain (\*)

E-mail sending has been suspended. Warning address: [xxxx]

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Note]: the following content is displayed:

- E-mail title (\*)
- Address of sender (\*)
- Address of recipient (To, Cc and Bcc information) (\*)
- Attachment name (\*)

Example of [Notes]

[Title: Today' s Business Report From: E-mail Address-A To: E-mail Address-B CC: E-mail Address-C E-mail BCC: Address-D Attachment: Attachment Name]

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

## 8.2.7 Device Configuration Change Log

This is the log when device configuration is changed (when a memory device is added along with the change of drive letter, and when device name and internal serial number change because the device in the same drive letter is changed) in the client (CT).

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

In the [Log Switches] tab, set [Device Configuration Change Log] to [Yes].

### Collected information

The information displayed in [Notes] will be different due to the type of drive.

Drive Type	Volume	Device Name	Internal Serial Number	Server Name, Shared Name
Fixed	○	—	—	—
Removable	—	○ (Note 1)	○ (Note 1)	—
CD-ROM	—	○ (Note 1)	○ (Note 1)	—
Remote (Note 2)	—	—	—	○

○: Collect information.

—: Do not collect information.

Note 1: The information is only recorded when a USB is connected.

Note 2: When sharing the floppy drive and USB memory device with another PC, the drive type will be recorded as "Remote".

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [Device Configuration Change] (fixed value)

**[Classification]:** [Normal] or [Violation] (Note 5)

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed.

- [Add] or [Change] (Note 3)
- Drive letter (Note 3)
- Drive Type (Note 3)

Note 3) When performing keyword search in Log Viewer, the value in [ ] can be specified as keyword.

Recorded as [Add] in the following cases:

- When logging on, if there is drive added comparing the information at last logoff with the current drive information
- When adding device in the logon status
- When logging on after adding device in the status of not logon
- When removing the connected device and connecting another device to the same drive in the logon status

Record as [Change] when any of the following operations is performed in the logon status.

- When changing the drive type
- When allocating the shared name of server to the existing network drive

**[Note]:** the following content is displayed:

- Volumename (Note 4)
- Device name (Note 4)
- Internal serial number (Note 4)
- Server name, shared name (Note 4)
- USB device name (Note 6)
- Manufacturer ID
- Product ID

Note 4: When performing keyword search in Log Viewer, the value in the [ ] can be specified as a keyword.

Note 5: The situation of recording as a violation will be different due to the status of policy, whether to reflect policy, whether the Management Server can be communicated with and the status of the connected USB device. Logs that are recorded as violations will be output in the following cases.

- Case 1  
When the USB device whose [USB Identification Method] in the [USB Device Registration] window is [Unavailable] is connected
- Case 2  
When the period for use set in [Period for Using USB Device] in the [USB Device Registration] window is exceeded

- Case 3

When [Allow to Use All USB Registered in Management Server] of the [File Export Prohibition - USB Device Individual Identification Function - Detailed Settings] window is set to [Yes], the Management Server cannot be connected to the client (CT)

- Case 4

When [Export Prohibition] (specify drive or removable device) is selected in the [File Export Prohibition] tab.

- Case 5

When [Read Prohibition] (specify removable device) is selected in the [File Export Prohibition] tab.

Note 6: When [USB Device Individual Identification Function] is set to [Available], the USB device name will be obtained.

Example of [Content] and [Notes]

When the information cannot be obtained, blank ([ ]) will be displayed.

When built-in hard disk is installed

Content	Notes
[Added D: fixed]	Volume [Windows2003]

When viewing the drive information in Explorer of OS, in case that “Local Disk (D:)” is displayed, the volume is displayed as blank ([ ]).

When USB memory device, hard disk and floppy drive, etc., connected via USB are connected

Content	Notes
[Added G: Removable]	Device Name [BUFFALO USB Flash Disk USB Device], Internal Serial Number [B32986]

When DVD/CD device connected via USB is connected

Content	Notes
[Added E: CD-ROM]	Device Name [MATSHITA UJD330], Internal Serial Number [ ]

For DVD/CD device not connected via USB (via IDE, IEEE, etc.), blank ([ ]) will be displayed in the notes column.

When network drive is added

Content	Notes
[Added G: Remote]	Volume [SOUMUDISK], Server Name, Shared Name [\\ServerSOUMU \SOUMUDISK]

“Server Name, Shared Name” may also be displayed as “\\IP Address of the Server\Shared Name”.

When individual identification of USB device is performed and the unauthorized USB device (identified as removable) is installed

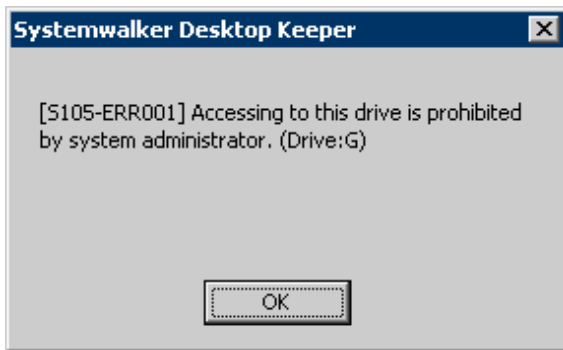
Classification	Content	Notes
Violation	[Added G: Removable]	Device Name [BUFFALO USB Flash Disk USB Device], Internal Serial Number [B32986]

When the hard disk is physically damaged, and other applications exclusively access the file that records the previous device configuration, [Content] of device configuration change log may become “Unknown”.

Content	Notes
[Changed A: Unknown→ Removable]	

## When violated

When the device configuration change log becomes violated, the following message will be displayed.



## 8.2.8 Printing Operation Log

---

This is the log when printing is performed through an application with printing permission in the client (CT).

After printing has been performed in the client (CT), an operation log will be sent to the Management Server.



---

### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

For details, please refer to “[1.2.18 Printing Operation Log](#)”.

---

## Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

In the [Log Switches] tab, set [Print Operation Log] to [Yes].

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [Printing] (fixed value)

**[Classification]:** normal

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed:

- Name of printed file (document name) (Notes)
- Name of printer (Notes)
- Total pages of printed file



- Date of printing

Example of Content

```
[imgfilelist.xls] Printed. Printer name: [KONICA MINOLTA 750/600 PCL], Number of pages: [1], print date: [2007/04/11 19:44:59]
```

[Note]: (not displayed)

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

## 8.2.9 Printing Prohibition Log

---

This is the log when printing is to be performed through an application without permission in the client (CT).

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

In the [Printing prohibition] tab, set [Printing Prohibition] to [Yes].

In addition, applications with printing permission should also be set in the [Printing prohibition] tab.

For details about the configuration value, please refer to “[2.4.1.3 Settings of \[Printing Prohibition\] Tab](#)”.

### Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user ID in the client (CT)

[Domain Name]: it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

[Type]: [Printing prohibition] (fixed value)

[Classification]: violation

[Attachment]: (not displayed)

[Content]: the following content is displayed:

- Name of the file that is prohibited from printing(\*)
- Name of prohibited application (\*)

Example of [Content]

```
Prohibited print [Microsoft Word - 13.Console.doc]. Program name: [C:\Program Files\Microsoft Office \OFFICE11\WINWORD.EXE]
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Note]: (not displayed)

## 8.2.10 Logon Prohibition Log

---

This function is not available.

This is the log when intending to logon with the user name that belongs to the group prohibited from logon in the client (CT).

## Set policy for collection

Set policy in the [Terminal Initial Settings] window or the window after the Management Console is started (CT policy settings window). Set the groups that is prohibited from logon in the [Logon Prohibition] tab. For details about the configuration value, please refer to “2.4.1.4 Settings of [Logon Prohibition] Tab”.

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [Logon Prohibition] (fixed value)

**[Classification]:** violation

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed.

- Prohibited user name (group) (Note 1)
- Prohibition processing ([Logoff] or [Shutdown]) (Note 2)
- Prohibition results ([Succeeded] or [Failed])

Example of [Content]

```
The logon of [dmn-user (Domain Users)] has been [Logoff]. Result: [Succeeded]
```

Note 1) When performing keyword search in Log Viewer, it can be specified as keyword.

The search target is user name and group name instead of brackets.

Note 2) When two or more logon users exist in the same PC, [Logoff] will be displayed when logging on is prohibited.

**[Note]:** (not displayed)

## 8.2.11 File Export Log

This is the log when exporting files and folders using File Export Utility in the client (CT). The original file of the exported file can also be saved at the same time when the log is collected.



### Note

#### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

For details, please refer to “1.2.17 File Export Log”.

## Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

- In [Log Switches] tab, set [File Export Log] to [Yes].
- When [Backup Original File] is selected in the [Log Switches] tab, the original file of the exported file can be saved. The settings can be performed when [File Export Log] is set to [Yes].

For details about the configuration value, please refer to “[2.4.1.2 Settings of \[File Export Prohibition\] Tab](#)”.

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** log collecting time of the client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [File Export] (fixed value)

**[Classification]:** normal

**[Attachment]:** when the attached data exists, display "1"

**[Content]:** the following content is displayed:

- File name of export source (\*)
- File name of export target (\*)
- Export method (in plain text)
- Drive letter of export target
- Drive type of export target
- Reason for export (\*)

Example of Content

When exporting after being encrypted

```
Take [C:\Documents and Settings\Administrator\Desktop>List of Customer Information.xls] as [G:\List of Customer Information.exe], export to [Plain text] through [G:]. Type of drive: [Removable]
```

When exporting in plain text

```
Take [D:\Product Customer October in 2007.XLS] as [E:\Product Customer October in 2007.XLS], export to [Plain Text] through [E:]. Type of drive : [CD/DVD]
```

When specifying the export target of encrypted file with UNC (address beginning with "\\")

```
Take [D:\Documents and Settings\Administrator\Desktop\New File.txt] as [\\Server1\UserDocument\New File.txt], export to [Plain text] through [Remote]. Type of drive: [Remote]
```

When policy of inputting export reason is set

```
Take [C:\Documents and Settings\Administrator\Desktop\Important Customer Information of A Company.xls] as [E:\Customer Information.ex_], export to [Plain text] through [E:]. Type of drive: [Removable], Export Reason: [For Exporting  Information to  Client in  Business]
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

**[Notes]:** the following content is displayed:

- Volume (\*1) (\*4)
- Size (\*1) (\*2) (\*4)

- Device name (\*3) (\*4)
- Internal serial number (\*1) (\*4)
- USB device name (\*3) (\*4) (\*5)

\*1) For file export log collected through V13.2.0 or earlier, [ ] is displayed as blank.

\*2) When exporting folder, [ ] is displayed as blank.

\*3) Displayed when the export target is media connected via USB.

\*4) When performing a keyword search in Log Viewer, it can be specified as a keyword.

\*5) Displayed only when a USB device has been registered in the [USB Device Registration] window of Management Server and the following policy settings has been performed. It is the information set in [USB Device Name] when registering a USB device.

- When setting [Device Configuration Change Log] to [Yes] in the [Terminal Initial Settings] window, the [User Policy Settings] window or the [Log Switches] tab of the CT policy settings window.
- When setting [Export Using File Export Utility] to [Yes] in the [Terminal Initial Settings] window or the [File Export Prohibition] tab in the policy settings window.
- When setting [Restrict the Use of USB Device of File Export Utility] to [Yes] in the [File Export Utility Function Settings] window and the [Allow Specified USB Device Only] checkbox is selected.

Example of [Notes]

For file export log collected through V13.2.0 or earlier

Volume label: [ ], Size (byte): [ ]

When exporting to the media not connected via USB

When exporting folder

Volume label: [USERVOL], Size (byte): [ ]

When exporting file

Volume label: USERVOL], Size (byte): [123,456]

When exporting to the media connected via USB in case that USB device individual identification is not performed

When exporting folder

Volume label:: [USERVOL], Size (byte): [ ], Device Name: [Strings of Device Name], Internal Serial Number: [0E40986050226896]

When exporting file

Volume label: [USERVOL], Size (byte): [123,456], Device Name: [Strings of Device Name], Internal Serial Number: [0E40986050226896]

When exporting to the media connected via USB in case that USB device individual identification is performed

When exporting folder

Volume: [USERVOL], Size (Byte): [ ], Device Name: [Strings of Device Name], Internal Serial Number: [0E40986050226896], USB Device Name: [I-O xxyyzz Company ED-123 Type]

When exporting file

Volume label: [USERVOL], Size (byte): [123,456], Device Name: [Strings of Device Name], Internal Serial Number: [0E40986050226896], USB Device Name: [I-O xxyyzz Company ED-123 Type]

## 8.2.12 PrintScreen Key Operation Log

---

This is the log when the PrintScreen key is used in the client (CT). In the meantime of logging, the screen capture of PrintScreen operations can also be collected.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

When two of the following are set, the PrintScreen key operation log will be collected:

- Set [Disable PrintScreen Key] to [No] in the [Printing prohibition] tab.
  - Set [PrintScreen Key Operation Log] to [Yes] in the [Log Switches] tab.
  - When the [Capture Screen] checkbox is selected in the [Log Switches] tab, screen capture of the time when PrintScreen key is used can be collected.
- The settings can be performed when [PrintScreen Key Operation Log] is set to [Yes].

### Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [PrintScreen key prohibition] (fixed value)

**[Classification]:** normal (fixed value)

**[Attachment]:** when the attached data exists, display “1”

**[Content]:** the following content is displayed.

- Information of pressing PrintScreen key.

Example of [Content]

```
PrintScreen key has been pressed.
```

When performing keyword search in Log Viewer, the character “PrintScreen key is pressed.” can be searched.

**[Note]:** (not displayed)

## 8.2.13 PrintScreen Key Prohibition Log

---

This is the log when the PrintScreen key is operated in the case that the use of the PrintScreen key is prohibited in the client (CT).

“The Use of PrintScreen Key is Prohibited” refers to the situation in which screen capture cannot be collected even if the PrintScreen key is pressed.

When logging, the screen capture at the time when the PrintScreen operation is performed can also be collected.

### How to apply

Though the use of the PrintScreen key is prohibited, the user who intends to collect screen capture and perform violation operations can be found. Because the kind of screen capture to be collected is known, what kind of operation is going to be performed can be predicted. This can help prevent behaviors that may lead to a significant security problem.

## Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

When two of the following has been set, the PrintScreen key prohibition log will be collected.

- Set [PrintScreen Key Operation Log] to [No] in the [Log Switches] tab.
- Set [PrintScreen Key Invalid] to [Yes] in the [Printing prohibition] tab.
- When the [Screen Capture] checkbox is selected in the [Printing prohibition] tab, the screen capture at the time when the PrintScreen key is used can be collected.

## Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user name of the client (CT)

[Domain Name]: it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

[Type]: [PrintScreen key prohibition] (fixed value)

[Classification]: [Violation] (fixed value)

[Attachment]: when the attached data exists, display “1”

[Content]: the following content is displayed.

- Information of pressing PrintScreen key.

Example of [Content]

```
PrintScreen key has been pressed.
```

When performing keyword search in Log Viewer, the character “PrintScreen key is pressed.” can be searched.

[Note]: (not displayed)

## 8.2.14 Web Operation Log

---

This is the log when the following operation is performed in the client (CT).

- Upload and download via Website

After file sending or receiving has been started, even if an exception occurred or the user has cancelled file sending or receiving, the log will still be collected.

## Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set [Web Operation Log] of the [Log Switches] tab to [Yes].

## How to search

When searching in Log Viewer, select “Web Operation” inlog type and select “Normal” in classification.

When “Web Operation”, “Web Upload” or “Web Download” is set as a keyword, Web upload and download logs can be searched. The keyword is searchable under partial match.

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** the name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** the following content is displayed according to the operation content (fixed value).

- Web upload
- Web download

**[Classification]:** normal

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed:

- Name of application displaying Web pages (\*)
- URL strings of access target (\*)
- File name (\*)

The maximum length of the string displayed in the content is 519 bytes. Because only the length within 519 bytes is displayed when the length of string displayed in the content exceeds 519 bytes, the length of the content will be adjusted.

Example of [Content]

When [Web Upload Operation]

```
Uploaded to [www.aaa.com]. Application name: [iexplore.exe], File name: [c:\test\test.txt]
```

When [Web Download Operation]

```
Downloaded from [www.aaa.com]. Application name: [iexplore.exe], File name: [c:\test\test.txt]
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

**[Note]:** (not displayed)

## 8.2.15 Web Operation Prohibition Log

---

This is the log when the following operations are performed in the client (CT):

- Access to the prohibited URL (URL access prohibition log)
- Download from unpermitted websites (Web download prohibition log)  
When file download is selected through the button, link, menu, etc., on the window of the Website
- Upload to unpermitted websites (Web upload prohibition log)  
When file upload is selected through the button, linkage, menu, etc., on the window of Website

## Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

- Set [URL Access] of the [URL Access Prohibition] tab to [Prohibit].
- Set [Upload and Download] of the [Web Upload and Download Prohibition] tab to [Prohibit].

## How to search

- In the case of a URL access prohibition log

When searching in Log Viewer, input “Web Operation Prohibition” in log type, “Violation” in classification and “iexplore.exe”, “Web Operation Prohibition” and “URL Access Prohibition” as a keyword in the search conditions. URL strings of Website to be accessed can also be specified in keyword.

The keyword is searched for under partial match.

- In the case of a Web download prohibition log

When searching in Log Viewer, input “Web Operation Prohibition” in log type, “Violation” in classification, “Web Download” as a keyword in the search conditions. The name of the application displaying Web pages and URL strings of the access target can also be specified as a keyword.

The keyword is searched for under partial match.

- In the case of a Web upload prohibition log

When searching in Log Viewer, input “Web Operation Prohibition” in log type, “Violation” in classification, “Web Upload” as a keyword in the search conditions. The name of the application displaying Web pages and URL strings of the access target can also be specified as a keyword.

The keyword is searched for under partial match.

## Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** the following information is displayed according to the content of the operation (fixed value).

- URL access prohibition
- Web upload prohibition
- Web download prohibition

**[Classification]:** violation

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed:

- Name of application displaying Web pages (\*)
- URL strings of access target (\*)

The maximum length of the string displayed in the content is 519 bytes. Because only the length within 519 bytes is displayed when the length of string displayed in the content exceeds 519 bytes, the length of the content will be adjusted.

Example of [Content]



In case of [URL Access Prohibition]

Prohibited connection to [www.aaa.com]. Application name: [iexplore.exe]

In case of [Web Upload Prohibition]

Prohibited uploading to [www.aaa.com]. Application name: [iexplore.exe]

In case of [Web Download Prohibition]

Prohibited downloading from [www.aaa.com]. Application name: [iexplore.exe]

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Note]: (not displayed)

## 8.2.16 FTP Operation Log

---

This is the log when the following operations are performed in the client (CT):

- Upload a file to an FTP Server (FTP upload log)
- Download a file from an FTP Server (FTP download log)

Only the FTP communication log of the connection target server of the FTP client with the communication port set as “21” is recorded.

After file transmission starts, even if an exception occurs or the user cancels file transmission, the log will still be collected.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set [FTP Operation Log] of the [Log Switches] tab to [Yes].

### How to search

When searching in Log Viewer, select “FTP Operation” in type of log and “Normal” in classification.

When “FTP Operation” is set as a keyword, the FTP upload log and FTP download log can be searched.

When “FTP Upload” is set as a keyword, FTP upload log can be searched. In addition, when “FTP Download” is set, FTP download log can be searched.

The keyword can be searched for under partial match.

### Displayed content

Logs that can be viewed are as follows:

[Name]: the name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user name of the client (CT)

[Domain Name]: it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

[Type]: the following content is displayed according to type of log (fixed value):

- FTP uploading
- FTP downloading

[Classification]: normal

[Attachment]: (not displayed)

[Content]: the following content is displayed.

The maximum length of the string displayed in the content is 519 bytes. Because only the length within 519 bytes is displayed when the length of string displayed in the content exceeds 519 bytes, the length of the content will be adjusted.

- FTP client program name (\*)
- IP address of FTP Server (\*)
- File name (\*)

Example of [Content]

When [FTP Upload]

```
Uploaded to [192.168.1.100]. Application name: [FTP.EXE], File name: [Test.txt]
```

When [FTP Download]

```
Downloaded from [192.168.1.100]. Application name: [FTP.EXE], File name: [Test.txt]
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Note]: (not displayed)

## 8.2.17 FTP Operation Prohibition Log

---

This is the log when an unpermitted FTP connection is made in the client (CT).

Only the FTP communication log of the connection target server of the FTP client with the communication port set as “21” is recorded.



### Note

---

#### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

For details, please refer to “[1.2.13 FTP Server Connection Prohibition](#)”.

---

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set [FTP Server Connection] as [Prohibited] in the [FTP Server Connection Prohibition] tab.

### How to search

When searching in Log Viewer, input “FTP Operation Prohibition” in type of log, “Violation” in classification, “FTP Server Connection Prohibition” as a keyword in the search conditions. FTP client process name and IP address of the accessed FTP server can also be specified in keyword.

The keyword can be searched under partial match.

### Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user name of the client (CT)

[Domain Name]: it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

[Type]: [FTP Connection Prohibition] (fixed value)

[Classification]: violation

[Attachment]: (not displayed)

[Content]: the following content is displayed.

- FTP client program name (\*)
- IP address of FTP server (\*)

The maximum length of the string displayed in the content is 519 bytes. Because only the length within 519 bytes is displayed when the length of string displayed in the content exceeds 519 bytes, the length of the content will be adjusted.

Example of [Content]

```
prohibited connecting to [192.168.1.100]. Application name: [FTP.EXE]
```

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

[Note]: (not displayed)

## 8.2.18 Clipboard Operation Log

---

This is the log when information is copied from the virtual environment to the physical environment or from the physical environment to the virtual environment via clipboard. The log will be collected in both environments.



### Note

#### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used. For details, please refer to “[1.2.26 Clipboard Operation Log](#)”.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

In the [Log Switches] tab, set [Clipboard Operation Log (Virtual Environment)] to [Yes].

### Displayed content

Logs that can be viewed are as follows:

[Name]: name of the client (CT)

[Occurrence Date and Time]: time for collecting logs at client (CT)

[User ID]: logon user name of the client (CT)

[Domain Name]: it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

[Type]: [Clipboard Operation] (fixed value)

[Classification]: normal

[Attachment]: when the attached data (original file) exists, display “1”

**[Content]:** the following content is displayed:

- Direction
- Operation source PC
- Operation target PC
- Application name
- Format: the following content is displayed:
  - Text: text data
  - Image: image data
  - File: file path
  - META: extended META file data
  - SYLK: data in symbolic link format
  - DIF: data in data exchange format
  - TIFF: image data in TIFF format
  - PALETTE: handling of color pallet
  - PEN: data used for PEN extended function
  - RIFF: audio data in RIFF format
  - WAVE: audio data in WAVE format
  - LOCALE: locale ID handling of text data
  - WIN\_VERSION: version of Windows
  - DSPTEXT: text data in private format
  - DSPBITMAP: bitmap data in private format
  - PICT: data in image display format
  - EXTRA (0x0080): data defined by application alone
  - EXTRA (letters or 0x9999): data defined by application alone
  - Letters are in data format.
- Content

Example of [Content]

In text format

```
Clipboard operation has been performed between different environments. Direction: [Virtual party-  
>Physical party], Operation source PC: [PC001], Operation target PC: [PC002], Application name:  
[Notepad.exe], Format: [Text], Content: [Clipboard Copy]
```

In image format

```
Clipboard operation has been performed between different environments. Direction: [Virtual party-  
>Physical party], Operation source PC: [PC001], Operation target PC: [PC002], Application name:  
[Notepad.exe], Format: [Image], Content: [Clipboard Copy]
```

In file format

```
Clipboard operation has been performed between different environments. Direction: [Virtual party-  
>Physical party], Operation source PC: [PC001], Operation target PC: [PC002], Application name:  
[Notepad.exe], Format: [File], Content: [Clipboard Copy]
```

**[Note]:** (not displayed)

## 8.2.19 Clipboard Operation Prohibition Log

---

This is the log when copying information from the virtual environment to the physical environment or from the physical environment to the virtual environment via clipboard is prohibited. The log will be collected in both environments.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window, the [User Policy Settings] window or the window after the Management Console is started (CT policy settings window).

Set [Prohibit of clipboard operation between different environments] of the [Virtual Environment setup] tab to [Prohibit].

### Displayed content

Logs that can be viewed are as follows:

**[Name]: name of the client (CT)**

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** logon user name of the client (CT)

**[Domain Name]:** it is the domain name of the client (CT) when logging on to domain while it is the computer name of the client (CT) when logging on to local computer

**[Type]:** [Clipboard Operation] (fixed value)

**[Classification]:** violation

**[Attachment]:** when the attached data (original file) exists, display "1"

**[Content]:** the following content is displayed:

- Direction
- Operation source PC
- Operation target PC
- Application name
- Format
- Content

Example of [Content]

In text format

```
Clipboard operation has been performed between different environments. Direction: [Virtual party-
>Physical party], Operation source PC: [PC001], Operation target PC: [PC002], Application name:
[Notepad.exe], Format: [Text], Content: [Clipboard Copy]
```

In image format

```
Clipboard operation has been performed between different environments. Direction: [Virtual party-
>Physical party], Operation source PC: [PC001], Operation target PC: [PC002], Application name:
[Notepad.exe], Format: [Image], Content: [Clipboard Copy]
```

In file format

```
Clipboard operation has been performed between different environments. Direction: [Virtual party-
>Physical party], Operation source PC: [PC001], Operation target PC: [PC002], Application name:
[Notepad.exe], Format: [File], Content: [Clipboard Copy]
```

**[Note]:** (not displayed)

## 8.2.20 File Operation Log

---

This is the log of file operations and folder operations in the following drives that are performed in the client (CT):

- Local drive
- Network drive
- Removable drive



---

### Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.  
For details, please refer to “[1.2.27 File Operation Log](#)”.

---

### Set policy for collection

Set policy in the [Terminal Initial Settings] window or the window after the Management Console is started (CT policy settings window).

- In the [Log Switches] tab, set [File Operation Log] to [Yes].
- In the [File Operation Process] tab, set the filtering conditions for file operation log.  
The settings can be performed when [File Operation Log] is set to [Yes].
- In the [File Operation Extension] tab, set whether to collect logs while operating files with which extension.  
The settings can be performed when [File Operation Log] is set to [Yes].

For details about the configuration value, please refer to “[2.4.1.6 Settings of \[File operational process\] Tab](#)” and “[2.4.1.7 Settings of \[File operation extension\] Tab](#)”.

### Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** the following information is displayed.

- When logging on: logon user name of the client (CT)
- When not logging on yet: SYSTEM (fixed)

**[Domain Name]:** the following information is displayed.

- When logging on to domain: the domain name of client (CT).
- When logging on to local computer: the computer name of client (CT).
- When not logging on yet: the computer name of client (CT)

**[Type]:** [File Operation] (fixed value)

**[Classification]:** normal

**[Attachment]:** (not displayed)

**[Content]:** for details, please refer to “[Collected operation logs](#)”.

## Example of [Content]

```
Operation: [Rename], Source file name:[C:\Documents and Settings\Administrator\Desktop\New Microsoft Excel Worksheet.xls], Type of drive: [Fixed], Target file name: [C:\Documents and Settings\Administrator\Desktop\List of Customer Information.xls], Type of target drive: [Fixed], Program name: [Explorer.exe]
```

[Note]: the following information is displayed:

- When file operation is [View], [Update], [Create], [Copy], [Cut], [Rename], the file size after operation will be displayed. When file size information cannot be obtained normally, single-byte blank (size (byte): [ ]) is displayed. In addition, when the file size exceeds 2147483647 bytes, “size (byte) [2147483647]” is displayed.
- When performing file operation or [Delete] in file operation, the note column will be blank.

When performing keyword search in Log Viewer, numerals can be specified as keyword.  
0 to 2147483647 can be specified.

[Example]

When “0123” is specified in search condition, logs with “size (byte): [201,235]” displayed in notes will be searched. Logs with “size (byte): [123]” displayed in notes cannot be searched.

## Collected operation logs

The following describes the logs collected when operating files and folders on the local drive and network drive in the client (CT) where file operation log policy has been set.



### The following software and commands are described

When running the following software or commands, operation logs displayed in the following table will be collected:

- Explorer
- Notepad
- Tablet
- Microsoft® Word (2000, 2002, 2003, 2007 and 2010) (Note)
- Microsoft® Excel (2000, 2002, 2003, 2007 and 2010) (Note)
- Microsoft® PowerPoint® (2000, 2002, 2003, 2007 and 2010) (Note)
- Command in command prompt (COPY, XCOPY, MOVE, DEL, ERASE, RD, REN, MD)

Note: In case of Windows Vista®, Windows Server® 2008 or Windows® 7, only 2003, 2007 and 2010 are supported.

However, please be aware of the following points:

- [Update] operation of Microsoft® Word will be collected as [Create] log.
- Like Explorer and XCOPY, in the [File Operation Process] tab, [View] log of the process that has been registered as [Get Operations Apart from Viewing] will not be collected.
- Even if the software and commands above are used, redundant logs may be collected.
- When using software and commands other than the above ones, operation logs not corresponding to the actual operation (eg, [Copy] and [Cut] logs cannot be collected, but they can be collected as [View], [Create], [Delete] or [Rename] logs) may be collected.
- When using the redirection command (> or >>) and MD command in command prompt, logs may not be output.

When operating file and folder in the client (CT), the types of logs collected are as follows.

Log Type	[Content] Display of Log Viewer
View	Operation: [View], File name: [(Note 1)], Type of drive: [(Note 2)], Program name: [(Note 5)]
Update	Operation: [Update], File name: [(Note 1)], Type of drive: [(Note 2)], Program name: [(Note 5)]
Create	Operation: [Create], File name: [(Note 1)], Type of drive: [(Note 2)], Program name: [(Note 5)]
Delete	Operation: [Delete], File name: [(Note 1)], Type of drive: [(Note 2)], Program name: [(Note 5)]
Copy	Operation: [Copy], Source file name: [(Note 1)], Type of drive: [(Note 2)], Target file name: [(Note 3)], Type of target drive: [(Note 4)], Program name: [(Notes5)]
Cut	Operation: [Cut], Source File Name: [(Note 1)], Type of drive: [(Drive 2)], Target file name: [(Note 3)], Type of target drive: [(Note 4)], Program name: [(Note 5)]
Rename	Operation: [Rename], Source File Name: [(Note 1)], Type of drive: [(Note 2)], Target file name: [(Note 3)], Type of target drive: [(Note 4)], Program name: [(Note 5)]

Note 1: The name of the file or folder in the local drive is described in full path, the name of the file or folder in the network drive is described with UNC or UNC and the machine name part is the IP address

Note 2: Type of source drive

Note 3: The name of the file or folder in the local drive is described in full path, the name of the file or folder in the network drive is described by UNC or UNC and the machine name part is the IP address

The name of the file of folder is described in full path in the following cases:

- Allocate drive letter for the network drive and perform rename operation in the allocated letter
- Allocate drive letter for the network drive and perform cut operation in the allocated letter
- Allocate drive letter for the network drive and access the network drive directly for performing cut operation of folder

Note 4: Type of target drive

Note 5: Name of the application that performs the operation

#### Conditions for log collection

Under what kind of conditions and operations the above “log type” can be collected is displayed as follows:

Condition			File and Folder Operations						
			View	Update	Create	Delete	Copy	Cut	Rename
File Operation	Log for files	In the same drive (Note 1)	View (Note 3)	Update (Note 3)	Create	Delete	Copy	Rename (Cut)	Rename
		In the same drive (Note 2)	-	-	-	-	Copy	Cut	-
Folder Operation	Log for files under a folder	In the same drive (Note 1)	-	-	-	Delete	Copy	×(Note 4) (Cut)	-
		Between different drives (Note 2)	-	-	-	-	Copy	Cut	-
	Log for folders	In the same drive (Note 1)	-	-	Create	Delete	Create (×)	Rename (Rename) (Delete)	Rename
		Between different drives (Note 2)	-	-	-	-	Create (×)	Create Delete (Delete)	-



-: impossible operations.

×: operation log cannot be collected.

View/update/create/delete/copy/cut/rename: indicates the type of collected operation log.

() : indicates the type of the collected operation file when files or folders with the same name exist in copying target or moving target. When there is no ( ), the type of recorded log will be collected.

Note 1: Operations in the same local drive or network drive. For example, see following case:

- Operation from C drive to C drive in the local drive
- Operation in the network drive “\\dtk\common\”

Note 2: Operations between different local drives, between the local drive and network drive or between different network drives. For example, see the following case:

- Operations from C drive to D drive in the local drive
- Operations between the local drive and network drive.
- Operations from the network drive “\\dtk\common\” to the network drive “\\dtk\com\”

Note 3: Viewing of file properties in Explorer and command prompt is not a log target.

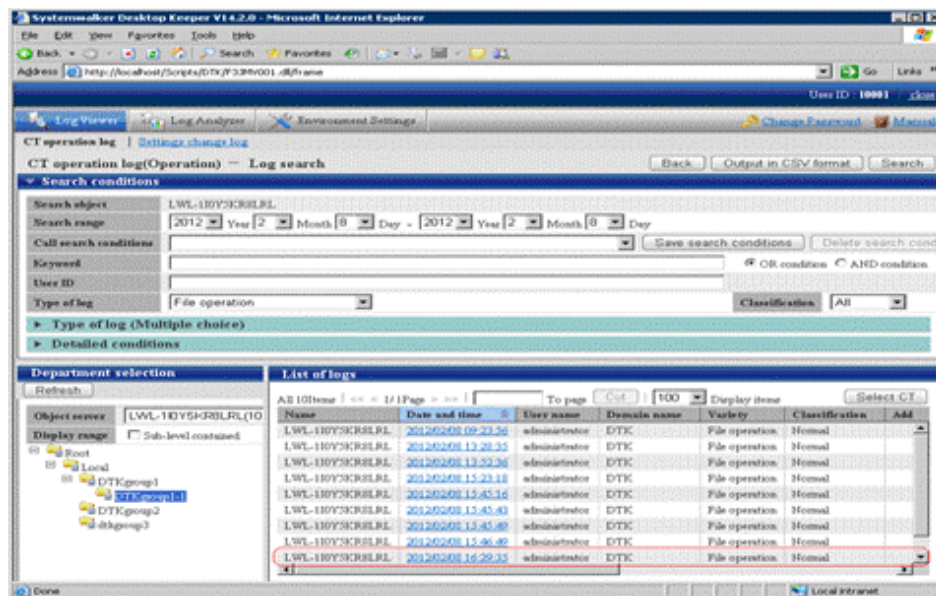
Note 4: When the folder name of the moving source is the same as that of the moving target, [Rename] log is collected only for files existing in the moving source folder but not in the moving target folder.

The meaning of the above table and the output logs are illustrated as follows:

[Example 1]

When viewing files in the same local drive, logs displayed in [View] of type of log above are collected.

The window for viewing logs in Log Viewer is displayed as follows. Logs collected in this case are shown in the frame part.



The content displayed in the [Content] column in the frame of the above window is as follows:

Operation: [View], File name: [D:\report.doc], Type of drive: [Fixed], Program name: [winword.exe]

This indicates that file “report.doc” in D disk root directory is viewed through Word.

#### [Example 2]

When copying files in the same local drive, no matter whether files with the same name exist in the directory of copy target, log displayed in [Copy] of the above log type will be collected.

Log displayed in the [Content] column of Log Viewer is as follows:

```
Operation: [Copy], Source File Name: [D:\report.doc], Type of drive: [Fixed], Target file ame: [D:\tmp\report.doc], Type of Target Drive: [Fixed], Program name: [Explorer.exe]
```

This indicates that file “report.doc” in the root directory of D drive is copied to “D:\tmp” through Explorer.

#### [Example 3]

When moving an empty folder from the local drive to a different drive and there is no folder with the same name in the moving target, two logs displayed in [Delete] and [Create] of the above log type are collected.

Log displayed in the [Content] column of Log Viewer is as follows:

```
Operation: [Create], Folder Name: [D:\log], Type of drive: [Fixed], Program name: [Explorer.exe]
Operation: [Delete], File name: [C:\log], Type of drive: [Fixed], Program name: [Explorer.exe]
```

This indicates that folder “log” in the root directory of C drive is moved to the root directory of D drive through Explorer.

#### [Example 4]

When moving an empty folder from the local drive to a different drive and there is folder with the same name in the moving target, log displayed in [Delete] of the above log type is collected.

Log displayed in the [Content] column of Log Viewer is as follows:

```
Operation: [Delete], File name: [C:\log], Type of drive: [Fixed], Program name: [Explorer.exe]
```

This indicates that folder “log” in the root directory of C drive is moved to a different drive through Explorer and there is folder with the same name in moving targets.

#### [Example 5]

When viewing files in the same network drive, log displayed in [View] of the above log type is collected.

Log displayed in the [Content] column of Log Viewer is as follows:

```
Operation: [View], File name: [\\dtk\common\report.doc], Type of drive: [Remote], Program name: [winword.exe]
```

This indicates that file “report.doc” in Shared Folder “common” under the root directory of machine “dtk” is viewed through Word.

## 8.2.21 Logon/Logoff Log

---

This is the log when the following operations are performed in the client (CT).

- Logon
- Logoff
- PC Startup
- PC Shutdown
- PC Sleep
- PC Restoration
- PC Connection
- PC Disconnection

## How to apply

When collecting logon/logoff log, the following application can be performed:

- Illegal operations performed by malicious third party such as file export, etc., after the PC is started in safe mode (records will not be left in Systemwalker Desktop Keeper) can be found.
- Compliance with operation guidelines such as powering off after completing business and starting sleep mode when the PC is not in use for a long time can be confirmed.
- The user who has used the PC for a long time after power on can be found.

## Set policy for collection

Set policy in the [Terminal Initial Settings] window or the window after the Management Console is started (CT policy settings window). In the [Log Switches] tab, set [Logon/Logoff Log] to [Yes].

## Collected information

This section describes the information collected in the logon/logoff log.

The corresponding operations in the following cases are collected as logs.

- PC startup log

Information when starting the OS of the client (CT).

Information of any of the following startup modes is obtained:

- [Start in Normal Mode]
- [Start in Safe Mode] (including the safe mode with command prompt)
- [Start in Safe Mode with Network Connection]

- Logon log

Information when logging on to Windows in the client (CT).

The computer name of the authentication target is obtained.

- PC sleep log

Information when the client (CT) enters standby mode or sleep mode.

Time from power on the last time to PC sleep is obtained.

- PC restoration log

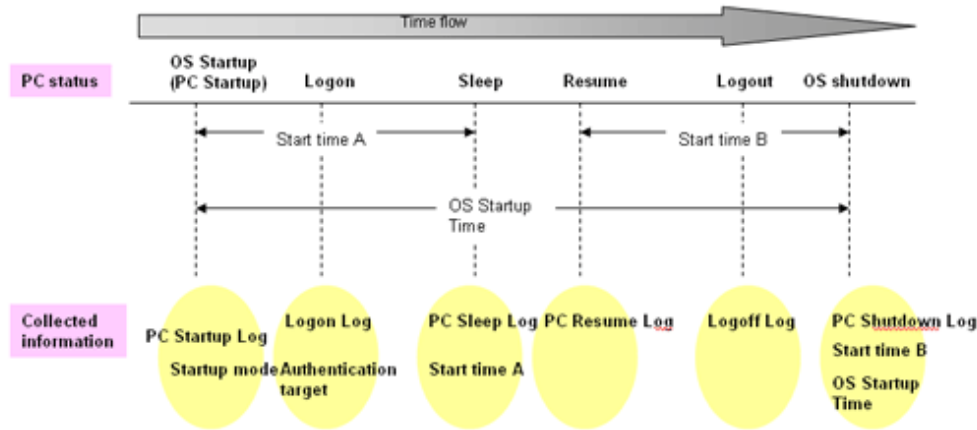
Information when the client (CT) restores from standby mode or sleep mode.

- Logoff log

Information when logging off from Windows in the client (CT).

- PC shutdown log

Information when shutting down the OS in client (CT).  
 Time from last power on to the shutdown is obtained.  
 In addition, time from OS startup to shutdown is also obtained.



- PC connection log

Information when connecting to the remote terminal.

- PC disconnection log

Information when disconnecting from the remote terminal.

**How to search**

- When illegal operations performed by malicious third parties such as file export are found after the PC is started in safe mode (record will not be remained in Systemwalker Desktop Keeper)

By setting the following conditions in the log list window of Log Viewer, only the PC startup log of startup in safe mode can be searched.

- Enter "Safe" in [Keyword].
- Set [Logon/Logoff] in [Type].

- When confirming power off after business has been completed, starting sleep mode when the PC has not been in use for a long time, whether the PC is being used according to the system operation guideline

By setting the following conditions in the log list window of Log Viewer, PC sleep log and PC restoration log can be searched. The PC in which sleep mode has been set can be identified through these logs.

- Enter "Sleep" and "Restoration" in [Keyword].
- Select the [OR Condition] button.
- Set [Logon/Logoff] in [Type].

If the PC on which PC sleep log and PC restoration log are collected on the second day still exists, whether or not the power of the PC has been cut off can be predicted.

- When the user who has used the PC for a long time after power on is found

By setting the following conditions in the log list window of Log Viewer, PC shutdown log and PC sleep log can be searched. PC that is in use for a long time can be identified through [OS Startup Time] of PC shutdown log.

In addition, by aggregating [Startup Time] of PC shutdown log and PC sleep log, startup time other than sleep time can be known.

- Enter "PC Shutdown" and "PC Sleep" in [Keyword].
- Select the [OR Condition] button.
- Set [Logon/Logoff] in [Type].

#### About keyword search items

The search can be performed in PC startup log by using strings such as "Startup in Normal Mode", "Startup in Safe Mode" and "Startup in Safe Mode with Network Connection".

Please enter a keyword in double-byte when searching for the first time. Strings input previously can be selected in the drop-down menu starting from the next search.

The search can be performed in the PC shutdown log by using string "XX hours YY minutes". Time is searched for under partial match or complete match. Size search cannot be performed.

Please enter the numerals ("XX" and "YY") in single-byte.

Please enter "hour" and "minute" in double-byte.

#### Displayed content

Logs that can be viewed are as follows:

**[Name]:** name of the client (CT)

**[Occurrence Date and Time]:** time for collecting logs at client (CT)

**[User ID]:** the following information is displayed. (Notes)

- At PC startup: SYSTEM (fixed)
- At PC shutdown: SYSTEM (fixed)
- At PC sleep: SYSTEM(fixed)
- At PC restoration: SYSTEM (fixed)
- At logon: logon user name of the client (CT)
- At logoff: logon user name of the client (CT)
- At PC connection: logon user name for logon to the remote terminal
- At PC disconnection: logon user name for logon to the remote terminal

**[Domain Name]:** the following information is displayed:

- At PC startup: computer name of client (CT)
- At PC shutdown: computer name of client (CT)
- At PC sleep: computer name of client (CT)
- At PC restoration: computer name of client (CT)
- At logon: it is the domain name of the client when logging on to domain while the computer name of the client when logging on to the local computer
- At logoff: it is the domain name of the client when logging on to domain while the computer name of the client when logging on to the local computer
- At PC connection: it is the domain name when logging on to domain in the remote terminal while the computer name when logging on to the local computer

- At PC disconnection: it is the domain name when logging on to domain in the remote terminal while the computer name when logging on to the local computer

**[Type]:** the following content is displayed according to log type (fixed):

- PC Startup
- PC Shutdown
- PC Sleep
- PC Restoration
- Logon
- Logoff
- PC Connection
- PC Disconnection

**[Classification]:** normal (fixed value)

**[Attachment]:** (not displayed)

**[Content]:** the following content is displayed:

- At PC startup: the computer is started. Startup mode: [Display Startup Mode] (\*)  
The following content is displayed in the [Display Startup Mode].
  - [Startup in Normal Mode]
  - [Startup in Safe Mode] (including that with command prompt)
  - [Startup in Safe Mode with network connection]
- At PC shutdown: the computer is powered off. Startup time: [Display Startup Time] (\*), OS startup time: [Display Startup Time] (\*)  
The time and minutes are displayed in the format of [× × hours × × minutes] in [Display Startup Time].  
The seconds is displayed after it is carried over to the next place.  
[Example] 0 hour 3 minutes 0 second: output as [0 hours 03 minutes]. 0 hour 3 minutes 1 second: output as [0 hour 04 minutes].
- At PC sleep: the computer sleeps. Startup time: [Display Startup Time] (\*)
- At PC restoration: the computer is restored.
- At logon: the computer is logged on. Authentication target: [Display Authentication Target] (\*)  
[Computer Name] (in local authentication) or [Domain Name] (in domain authentication) is displayed in the [Display Authentication Target].
- At logoff: the computer is logged off.
- At PC connection: connect the computer [Computer Name (Virtual PC)] from the computer [Computer Name (Physical PC)].
- At PC disconnection: disconnect the computer [Computer Name (Physical PC)] and the computer [Computer Name (Virtual PC)].

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

**[Note]:** the following content is displayed.

- When [Type] is [Logon]
  - Connection method (\*)
  - Operation terminal (\*)
  - Logon method (\*)
  - Logon authority (\*)
- When [Type] is [PC Shutdown] and the power of PC is cut off by force
  - Shutdown action: [Abnormal Shutdown (\*)]

\*) When performing keyword search in Log Viewer, it can be specified as keyword.

Example of [Notes]

When performing local logon to the client (CT) as user directly

```
Connection method: [Local], operation terminal: [This Computer Name], logon method: [Local Logon],
logon authority: [User Authority]
```

When performing domain logon with administrator authority through terminal service

```
Connection method: [Remote], operation terminal: [Name of This Computer Performing Connection
Operation], logon method: [Domain Logon], logon authority: [Administrator Authority]
```

When cutting off the power of PC by force

```
Shutdown action: [Abnormal Shutdown]
```

Example of log

```
CLIENT1 2007/11/1 14:15 SYSTEM D-GALAXY PC startup Normal The computer is started. Startup mode:
[Startup in normal mode]
CLIENT1 2007/11/1 14:20 higashi D-GALAXY Logon Normal Logged on. Authentication target: [D-GALAXY]
Connection method: [Local], Operation terminal: [D-GALAXY]
CLIENT1 2007/11/1 14:15 SYSTEM D-GALAXY PC sleep Normal Computer sleep. Startup time: [3 hours 12
minutes]
CLIENT1 2007/11/1 14:15 SYSTEM D-GALAXY PC restoration Normal The computer is restored.
CLIENT1 2007/11/1 14:18 higashi D-GALAXY Logoff Normal Logged off.
CLIENT1 2007/11/1 14:15 SYSTEM D-GALAXY PC shutdown Normal The computer is shutdown. Startup time: [6
hours 28 minutes], OS startup time: [6 hours 28 minutes]
```

Notes:

Active Directory running in Windows Server® 2003 does not distinguish double-byte/single-byte, type of Kana (Hiragana/Katakana), and the Japanese phonetic symbol of the target. On the other hand, the log of Systemwalker Desktop Keeper is created according to the actual login information.

Thus, the user name registered in Active Directory may be different from that output from the log of Systemwalker Desktop Keeper log.

[Example]

The user name entered during registration to Active Directory is “fujitsu” (single-byte), when login by entering “FUJITSU” (double-byte), the user name that records logs will be “FUJITSU” (double-byte).

## 8.2.22 Linkage Application Log

---

This is the log sent by the application linked with the client (CT).

For applications linked with the client (CT), please refer to “Link with Other Products” of “Systemwalker Desktop Keeper User’s Guide”.

### Set policy for collection

Set policy in the [Terminal Initial Settings] window or the window after Management Console is started (CT policy settings window). In the [Log Switches] tab, set [Linkage application log] to [Yes].

### Displayed content

The log content that can be viewed is as follows:

[Name]: name of the client (CT)

[**Occurrence time**]: time for collecting logs at client (CT)

[**User ID**]: logon user name of the client (CT)

[**Domain name**]: it is the domain name of the client (CT) when logging on to domain while computer name of the client (CT) when logging on to local computer

[**Type**]: [Linkage application] (fixed value)

[**Classification**]: [Normal] or [Violation]

[**Attachment**]: when the attached data (original file) exists, display “1”

[**Content**]: the following content is displayed:

- Product name notified by linkage application
- Message code notified by linkage application
- Message notified by linkage application

[**Note**]: (not displayed)

The backup original information is output to log through linkage application.

When original file data exists, “1” is displayed in [Attachment] of list of linkage application logs.

## 8.2.23 Configuration Change Log

---

This is the log when settings information of the client (CT) is modified through the Management Console.

Timing for log collection is as follows:

- When modifying settings information of the client (CT) through the Management Console
- When controlling service through the Management Console
- When controlling process through the Management Console

### Set policy for collection

Policy settings are not required.

### Displayed content

Logs that can be viewed are as follows:

[**Date and time for modification**]: set the date and time for change

[**Type of setting**]: the following information is displayed:

- [Terminal settings]: when the client (CT) is changed
- [Level composition settings]: when the client (CT), etc. are moved or CT group tree is changed in the client (CT) group tree
- [Service control]: when the service of the client (CT) is controlled
- [Process control]: when the process of the client (CT) is controlled

[**Content**]: the following content is displayed:

- The client (CT) settings information modified through Management Console
- The client (CT) service name and content ([Start], [Stop], [Automatic], [Manual] or [Disable]) controlled through Management Console
- The process name of the client (CT) controlled through Management Console



Example of [Content]

Moving target name: [FUJITSU-PC], Upper-level group name of moving source: [Planning Department],  
Upper-level group name of moving target: [Sales Department]  
Name: FUJITSU-PC, Notes: , Printing prohibition: Yes, Disable PrintScreen key: No  
Application with printing permission: notepad.exe, notes:

**[Note]:** (not displayed)

# Appendix A List of Aggregation Objectives

This appendix describes the Aggregation objectives that are set in the log analyzer.

## To know the violation status

No.	Objective	Content	Keyword specified Item	Show Details Item
1	To know the status of application startup prohibition	Analyze the data corresponding to application startup prohibition.	Application name	<ul style="list-style-type: none"> <li>- Application name</li> <li>- Occurrence date and time</li> </ul>
2	To know the status of printing prohibition	Analyze the data corresponding to printing prohibition.	Name of printed file	<ul style="list-style-type: none"> <li>- Name of printed file</li> <li>- Occurrence date and time</li> </ul>
3	To know the status of logon prohibition	Analyze the data corresponding to logon prohibition.	User name	<ul style="list-style-type: none"> <li>- User name</li> <li>- Occurrence date and time</li> </ul>
4	To know the status of PrintScreen key prohibition	Analyze the data corresponding to PrintScreen key prohibition.	N/A	<ul style="list-style-type: none"> <li>- Occurrence date and time</li> </ul>
5	To know the status of E-mail attachment prohibition	Analyze the data corresponding to E-mail attachment prohibition.	Name of file attachment	<ul style="list-style-type: none"> <li>- Name of file attachment</li> <li>- Occurrence date and time</li> </ul>

## To know file export status

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
1	To know the status of file export	Analyze the data corresponding to file exporting.	Source file name	<ul style="list-style-type: none"> <li>- Name of the export source file</li> <li>- Name of export destination file</li> <li>- Type of destination drive</li> <li>- Export type</li> <li>- Occurrence date and time</li> </ul>
2	To know the status of file export (according to drive)	Analyze the data corresponding to the file exporting according to the destination drive for export.	Source file name	<ul style="list-style-type: none"> <li>- Name of the export source file</li> <li>- Name of export destination file</li> <li>- Export type</li> <li>- Occurrence date and time</li> </ul>

## To know file operation status

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
1	To know the status of file operation	Analyze the data corresponding to file access.	File name	<ul style="list-style-type: none"> <li>- Operation type</li> <li>- Name of source file</li> <li>- Name of destination file</li> <li>- Type of destination drive</li> <li>- Application name</li> <li>- Occurrence date and time</li> </ul>
2	To control the status of file operation (remote)	Analyze the data corresponding to access to network files.	File name	<ul style="list-style-type: none"> <li>- Operation type</li> <li>- Name of source file</li> <li>- Name of destination file</li> <li>- Type of destination drive</li> <li>- Application name</li> <li>- Occurrence date and time</li> </ul>
3	To control the status of file operation (removable)	Analyze the data corresponding to access to removable files.	File name	<ul style="list-style-type: none"> <li>- Operation type</li> <li>- Name of source file</li> <li>- Name of destination file</li> <li>- Type of destination drive</li> <li>- Application name</li> <li>- Occurrence date and time</li> </ul>

#### To know the status of applications and E-mails

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
1	To know the status of application startup	Analyze the data corresponding to application startup	Application name	<ul style="list-style-type: none"> <li>- Occurrence date and time</li> </ul>
2	To know the status of E-mail Sending according to recipient	Analyze data corresponding to E-mail Sending according to receivers.	Name of file attachment	<ul style="list-style-type: none"> <li>- Subject</li> <li>- From</li> <li>- To/CC/BCC</li> <li>- Attachment</li> <li>- Occurrence date and time</li> </ul>

#### To know Printing operation status

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
1	To know the status of printing operation (frequency)	Analyze the data corresponding to printing operation.	Name of printed file	<ul style="list-style-type: none"> <li>- Name of printed file</li> <li>- Pages</li> <li>- Printer name</li> </ul>

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
				- Occurrence date and time
2	To know the status of printing operation (pages)	Analyze the data corresponding to printed pages.	Name of printed file	- Pages - Name of printed file - Occurrence date and time

#### To know Web access status

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
1	To know the acquisition of Window title obtaining with URL	Analyze the data corresponding to URL access.	URL	- Application name - URL - Window title - Occurrence date and time
2	To know the acquisition of Window title obtaining with URL (sites)	Analyze the data corresponding to the sites.	URL	- Application name - URL - Window title - Occurrence date and time

#### To know information disclosure status

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
1	To know the status file export	Analyze the data corresponding to file export to removable devices.	Name of source file	- Name of export source file - Name of export destination file - Type of destination drive - Export type - Occurrence date and time
2	To control the status of file operation	Analyze the data corresponding to file access to removable devices by the copying target/moving target or creating source/updating source.	File name	- Operation type - Name of source file - Type of source drive - Destination file name - Type of destination drive - Application name - Occurrence date and time
3	To control the status of printing operation (frequency)	Analyze the data corresponding to printing operation.	Name of printed file	- Name of printed file - Number of pages - Printer name - Occurrence date and time

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
4	To control the status of printing operation (pages)	Analyze the data corresponding to printing pages.	Name of printed file	<ul style="list-style-type: none"> <li>- Number of pages</li> <li>- Name of printed file</li> <li>- Occurrence date and time</li> </ul>
5	To control the status of E-mail Sending according to recipient	Analyze the data corresponding E-mail Sending according to recipient.	Name of file attachment	<ul style="list-style-type: none"> <li>- Subject</li> <li>- From</li> <li>- To/CC/BCC</li> <li>- Attachment</li> <li>- Occurrence date and time</li> </ul>

# Appendix B Appendix B Visualize Information through Linking with All-in-one PC/Printer

This function is not available.

The conversion result of paper usage and CO<sub>2</sub> emission is output as a report using the information collected from an all-in-one PC/printer. Then, the paper usage status will be reported to the PC installed with the client (CT).

Reporting the paper usage status to the client (CT) will raise the issue of environmental awareness to users, and unnecessary printing can be controlled to contribute to reducing the cost of printing and the emission of CO<sub>2</sub>.

Administrators may create reports on paper usage of each all-in-one PC/printer and each user, and visualize the changes of actual performance to control paper usage.

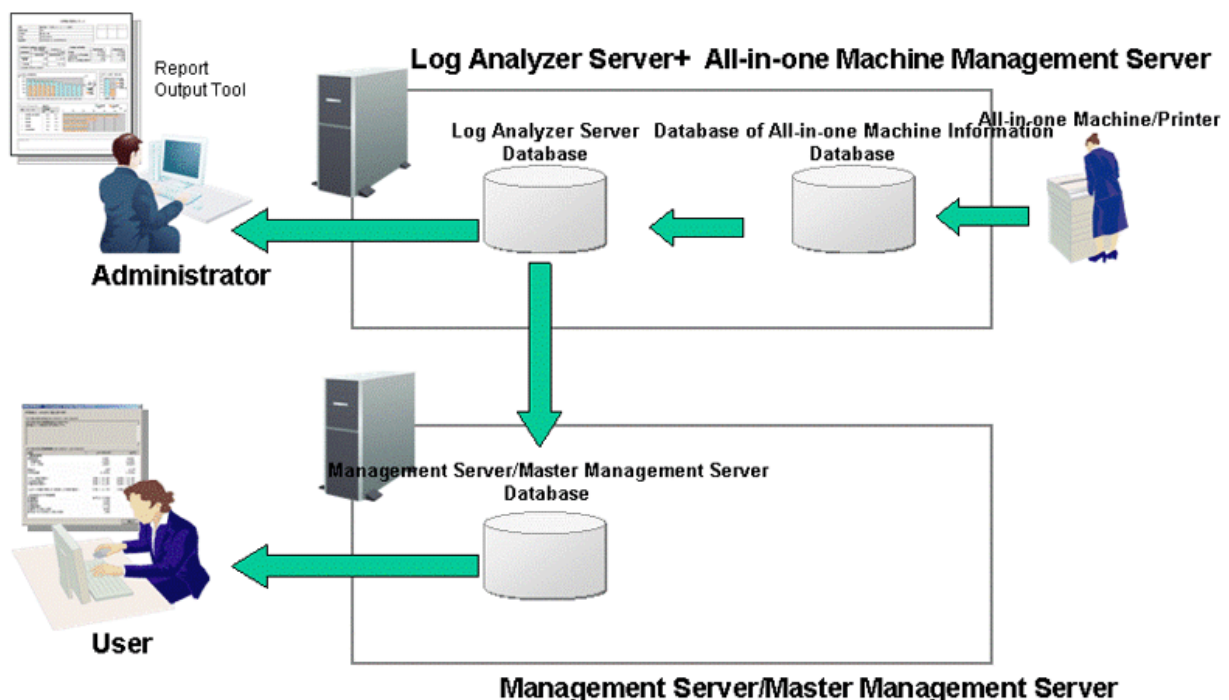
In addition, because the usage status of an all-in-one PC/printer can be output, it will also be helpful as judging material for the reduction of operation costs, such as reducing the number of all-in-one PC/printers or changing to low function models with lower maintenance cost.

For details of supported all-in-one PC/printer, please consult with the manufacturer of printer as stated in the software specification.

## B.1 Design

### B.1.1 Application pattern

Logs are imported from an all-in-one PC/printer to the log analyzer server regularly through the management server of the all-in-one PC/printer. This management server is based on the software provided by the manufacturer as stated in the software specification.



The management server and log analyzer of the all-in-one PC/printer are installed on the same server.

The aggregation result in the information database of the all-in-one/printer on the management server of the all-in-one PC/printer is imported into the database of the log analyzer server once a day. Results are also imported to the database of the management server/master management server once a day.

Administrators can output the paper usage report of an all-in-one PC/printer on the PC installed with the report output tool.

User should confirm the paper usage status reported on the PC installed with the client (CT), and implement improvements towards the reduction objective.



---

### **Errors during import**

When an error occurs at the time of importing to the database of the log analyzer server or management server/master management server, content will be exported to the event log. For the causes and the processing methods, please refer to “Messages Output during Aggregation of All-in-one PC/Printer Log” and “Message Output to Event Log” in the “Systemwalker Desktop Keeper Reference Manual”.

---

## **B.1.2 Determine user information of all-in-one PC/printer**

---

This section describes the methods of determining the user information of an all-in-one PC/printer.

Since the mechanisms for managing user information are different in each all-in-one PC/printer, the following management methods are available:

- Perform management through the user ID set in the all-in-one PC/printer;
- Perform management through the Windows logon user name.

Please specify the employee number of users as the user ID set in the all-in-one PC/printer.

Please specify a unique user name for each user as the Windows logon user name.

## **B.1.3 Aggregation mechanism for usage status of each all-in-one PC/printer**

---

This section describes the statistical mechanism for the usage status of each all-in-one PC/printer.

The aggregation of each all-in-one PC/printer is mainly performed by using inherent information set in the all-in-one PC/printer.

## **B.1.4 Aggregation mechanism for usage status of all-in-one PC/printer of each user**

---

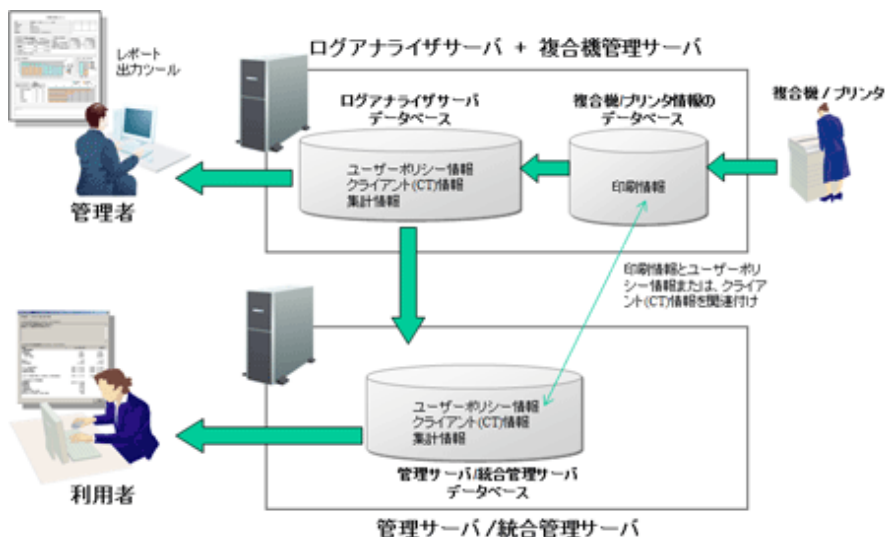
This section describes the aggregation mechanism for the usage status of an all-in-one/printer of each user.

User policy information or client (CT) information managed in the “management server/master management server database” of Systemwalker Desktop Keeper can be related to printing information so as to output the usage status of an all-in-one PC/printer of each user as a report, and notify the user about paper usage status.

The method of relation varies according to the method for managing user information.

- When managing through the user ID set in the all-in-one PC/printer:  
Establish a relation through the properties information “Employee ID” of the user policy or client (CT) information of Systemwalker Desktop Keeper.
- When managing through a Windows logon user name:  
Establish a relation through the attribute information “user name” of the user policy information of Systemwalker Desktop Keeper.

When outputting a report or notifying users, the statistic result will be displayed according to the attribute information “employee ID” of each user policy information or client (CT) information.



## B.1.5 Determine the method for relating printing information with Systemwalker Desktop Keeper information

This section describes the method for relating printing information with the information of Systemwalker Desktop Keeper.

- Use user policy information.

By setting an employee ID for user policy information, a relation with printing information can be achieved. The following are two methods for setting:

- Establish a relation through the [User Policy Setting] window of the management console.
- Set Employee ID for the user managed by Active Directory, and establish a relation by implementing Active Directory Linkage.
- Use client (CT) information.

Install the client (CT) of Systemwalker Desktop Patrol and the client (CT) of Systemwalker Desktop Keeper on the same computer. By setting “employee ID” during the installation of client (CT) of Systemwalker Desktop Patrol, relating with the printing information can be achieved.

Please refer to the following content to determine whether to use user policy information or client (CT) information.

- When it is expected to notify users on each client (CT) about the paper usage status, please use user policy information to establish the relation.  
Example: when one terminal has multiple users  
when one user uses multiple terminals
- When it is expected to notify every client (CT) about the paper usage status, please use CT information to establish the relation.  
Example: when one terminal is allocated to one person.
- When there is an all-in-one PC/printer managed by a Windows logon user name, please use user policy information to establish the relation.  
Example: when the all-in-one PC/printer with a user name has been set in the driver of the all-in-one PC/printer and the all-in-one PC/printer managed by Windows logon ID exist at the same time.

## B.2 Operating Environment



## Correspondent hardware/necessary software

- Please consult the manufacturer of the printer as stated in the software specification for correspondent hardware/necessary software.

## B.3 Restrictions and Considerations

---

- After the job log on the management server of the all-in-one PC/printer has been counted in the log analyzer, the registration of the job log into the all-in-one/printer management server during the aggregation period will be delayed, and the log will be excluded from the aggregation target.
- The paper cost output in the report is only the result obtained by multiplying the volume of paper usage with the price of one piece of paper during the aggregation period. Therefore, it is an approximate value instead of accurate cost of paper usage.
- The CO<sub>2</sub> emission output in the report is only the result obtained by multiplying the total volume of paper usage after being converted to A4 size with the CO<sub>2</sub> emission of one piece of paper during the aggregation period. Therefore, it is an approximate value instead of accurate CO<sub>2</sub> emission.
- If one user uses multiple client (CT)/Windows logon user names, when relating the printing information with the information of Systemwalker Desktop Keeper, client (CT)/Windows logon user names must be in the same group. If they are not in the same group, the number of pages being used will be counted repeatedly in multiple groups.
- The “Department” or “Department Name” group specified in the setting of [“B.4.6 Relate printing information with Systemwalker Desktop Keeper information”](#) and must not repeat with all groups. When repeated groups are specified, a relation cannot be established.
- For the “Unknown affiliation” group in the list of groups and the “User of unknown affiliation” in the list of users, a report is output only for the user that has printing actions. Therefore, users without printing actions will not be output to the “Unknown affiliation” group in the list of groups and the “User of unknown affiliation” in the list of users. In addition, the month without printing action of unknown affiliation will not be output to the group list and user list.
- In the setting of [“B.4.6 Relate printing information with Systemwalker Desktop Keeper information”](#), the volume of paper used when user that is not related with client (CT) and user uses the all-in-one PC/printer is only taken as the aggregation target of report when the v outputs the report. When the department management outputs a report, it will not be taken as the aggregation target.
- When [Manage under the group that is not configured] has been set in [System Settings]-[ Set group that is not configured] of the Server Settings Tool, client (CT) will be managed as “root” group instead of “non-configured” group in report output tool.
- When establishing a relation with user policy information according to [“B.4.6 Relate printing information with Systemwalker Desktop Keeper information”](#), if the Windows Logon user name of the user information is consistent with the employee ID of other users, the volume of paper used by other user will be displayed as the volume of paper used by the Windows logon user name.
- Because the data of the all-in-one PC/printer counted according to a Windows logon user name cannot relate to the volume of paper printed previously set by [“B.4.6 Relate printing information with Systemwalker Desktop Keeper information”](#), it might be output as a user of unknown affiliation.
- Regarding to the data of the all-in-one PC/printer counted according to the Windows logon user name, when the user information of Systemwalker Desktop Keeper set by [“B.4.6 Relate printing information with Systemwalker Desktop Keeper information”](#) contains Windows logon user names that are same in domain account and the local account, and the employee IDs set respectively are different, the data of the all-in-one PC/printer counted by the Windows logon ID will not become the aggregation target.

## B.4 Installation

---

### B.4.1 Confirm the log analyzer server has been constructed

---

A Systemwalker Desktop Keeper log analyzer server should be constructed. For the method of construction, please refer to “Construct log analyzer server” in the “Systemwalker Desktop Keeper Installation Guide”.

## **B.4.2 Confirm the environment of report output tool has been constructed**

The report output tool must be installed on the PC of system administrator that outputs report, and server settings and batch user settings should be performed.

For the method of construction, please refer to “Construct the environment for report output” in the “Systemwalker Desktop Keeper Installation Guide”.

## **B.4.3 Construct the environment of all-in-one/printer management server**

The management server of the all-in-one PC/printer should be installed on the computer installed with the log analyzer server.

Please consult the manufacturer of printer as stated in the software specification for the method of construction.

## **B.4.4 Register log analyzer server information on the management server of 3-level system**

In the case of a 3-level system, log analyzer server information is registered on the management server.

For details, please refer to “Set log analyzer server environment on management server/master management server” in the “Systemwalker Desktop Keeper Installation Guide”.

## **B.4.5 Set import time**

Set the startup time for importing from the all-in-one/printer to the log analyzer server as well as from the log analyzer server to the management server/master management server.

The initial value of startup time is shown below. No setting is required when starting from the following startup time without changes:

- Startup time for importing from all-in-one PC/printer to log analyzer server: 2:00 everyday;
- Startup time for importing from log analyzer server to management server/master management server: 3:00 everyday;



### **Note**

#### **Time sequence of import**

Please set the startup time for importing from the log analyzer server to the management server/master management server to a time after the import from the all-in-one/printer to the log analyzer server has completed.

- Import from the all-in-one/printer to the log analyzer server  
Implement the following steps on the log analyzer server.
- For environment excluding Windows Server 2008
  1. Select [All programs]-[Accessories]-[System tools]-[Tasks] from the [Start] menu to start the Task Scheduler.
  2. Open the properties of the following task.
  3. [DTKTaskRegist-PrinterCount]
  4. Select the [Schedule] tab.
  5. Change startup time (YY:MM), and click the [OK] button (please do not change anything apart from the startup time).
  6. Close the task scheduler.
- For Windows Server 2008 environment
  1. Select [All programs]-[Accessories]-[System tools]-[Task Scheduler] from the [Start] menu to start the Task Scheduler.
  2. Open the properties of the following task.

3. [DTKTaskRegist-PrinterCount]
4. Select the [Trigger] button and click [Edit].
5. Change the startup time (YY:SS) and click the [OK] button (please do not change anything apart from the startup time).
6. Click the [OK] button and close Properties.
7. Close the Task Scheduler.

- Importing from the log analyzer server to the management server/master management server

Implement the following steps on the management server/master management server

- For an environment excluding Windows Server 2008

1. Select [All programs]-[Accessories]-[System tools]-[Task] from the [Start] menu to start the Task Scheduler.
2. Open the properties of the following task.
3. [DTKTaskRegist-DtkPrinterBatch]
4. Select the [Schedule] tab..
5. Change the startup time (YY:MM), and click the [OK] button (please do not change anything apart from the startup time).
6. Close the Task Scheduler.

- For a Windows Server 2008 environment

1. Select [All programs]-[Accessories]-[System tools]-[Task Scheduler] from the [Start] menu to start the Task Scheduler.
2. Open the properties of the following task.
3. [DTKTaskRegist-DtkPrinterBatch]
4. Select the [Trigger] button and click [Edit].
5. Change the startup time (YY:SS) and click the [OK] button (please do not change anything apart from the startup time).
6. Click the [OK] button and close Properties.
7. Close the Task Scheduler.

## B.4.6 Relate printing information with Systemwalker Desktop Keeper information

---

This section describes the method for relating printing information with the information of Systemwalker Desktop Keeper.

### When relating with user policy information

- When establishing a relation through the [User Policy Setting] window of the Management Console

Please add user in the [User Policy Setting] window of the Management Console. Set [User Name], [Employee ID] and [Department name] when adding.

**[User name]:** Windows logon user name of the user

- **[Employee ID]:** Employee ID of the user;

**[Department Name]:** CT group name to which the user belongs.

For the setting method of user policy information, please refer to “Register user”.

- When establishing a relation by linking with Active Directory

1. Please specify [Employee ID] and [Department] of User Properties on Active Directory to the following values.

**[Employee ID]:** the employee ID of user;

**[Department]:** CT group name to which the user belongs.

Please use dsmod user command for setting. For details of command, please refer to the manual of Microsoft.

Properties specified in the dsmod user command are shown as follows:

[Employee ID]: empid

[Department]: dept

2. Please implement Active Directory Linkage.

### When relating the CT information

1. Install Systemwalker Desktop Patrol CT under the environment in which Systemwalker Desktop Keeper CT is installed.
2. Please specify Employee ID of the user in [Employee ID] during the installation of Systemwalker Desktop Patrol CT.

## B.4.7 Set user details (name and target)

---

By setting the details of every employee ID, name and target can be displayed when reporting the paper usage status of the all-in-one PC/printer and notifying client (CT) about the paper usage status.

1. Create an all-in-one PC/printer user information setting file (DTKPrinter\_PrintUserMaster.csv) and save it to the management server.

For details of the all-in-one PC/printer user information setting file, please refer to “All-in-one/printer user information setting file” in “Systemwalker Desktop Keeper Reference Manual”.

Saving location

For environment excluding Windows Server® 2008

```
C:\Documents and Settings\All Users\Application Data\Fujitsu\Systemwalker Desktop Keeper
```

For Windows Server® 2008 environment

```
C:\ProgramData\Fujitsu\Systemwalker Desktop Keeper
```

If no setting has been made, it will run according to the following setting:

- No name will be displayed (employee ID will be displayed) in the paper usage report and notification of paper usage status of the all-in-one/printer.
- Target of each user is the quantity of paper used in last month.

# Index

	[Numbers]		
3-level System Structure.....	372	Create Auditing Material.....	312
		creation in Management Console.....	362
	[A]	CSV files .....	135
Active Directory.....	108	CT Environment.....	396
Add/Delete Management Server.....	372	CT group .....	124
Add/Move/Delete CT.....	208	CT Group Policy.....	196
adding a new Master Management Server.....	367	CT Information/User Information.....	189
Adding to E-mail Software.....	8	CT list .....	52
Add or Remove Programs.....	405	CT Operation Log Window.....	279
Administrator Notification.....	412		[D]
Aggregate.....	257	Database .....	163
Aggregate by Objectives.....	256	Database of Management Server.....	442
Aggregation Result.....	256,262	Department Administrator.....	131
All Logs .....	15	Department Administrator Information.....	139
Allocate collectively .....	135	Department administrator information of CT group.....	140
Application Startup Log.....	479	Detailed Result.....	262
Application Startup Prohibition .....	12	Detail sheet.....	324
Application Startup Prohibition.....	462	Details of Number.....	253
Application Startup Prohibition Log.....	481	Device Configuration Change Log .....	20
Application Termination Log.....	480	Device Configuration Change Log.....	486
Apply Policy .....	38	Display the Number in Graph.....	252
Audit Operations on Client (CT) via Log Viewer.....	263		[E]
	[B]	E-mail control mode.....	405
Before Operation .....	1	E-mail File Attachment Prohibition.....	464
	[C]	E-mail Sending Log.....	18,484
changed to collective management on Master Management Server.....	365	E-mail Sending Suspension Log.....	485
Change of IP Address/Computer Name of Management Server/ Master Management Server.....	413	Encrypted Files .....	8
Change Operating Environment.....	362	Environment can be used.....	313
changing the existing Management Server to Master Management Server.....	370	Export CT information/User information.....	224
Character code that can be processed .....	4	Export Utility .....	5
collective management in each Management Server.....	366	External Application Log.....	512
Collective Management of User Policy.....	4		[F]
Command Operation Log .....	19	File Export .....	5
Communication Information of Management Server.....	437	File Export Log .....	15
Comprehensive Analysis Report.....	336	File Export Log.....	491
Comprehensive diagnosis sheet.....	341	File Export Prohibition .....	10
Conditions for Aggregation /Report Output .....	175	File Export Prohibition.....	454
Conditions of Using Web Console.....	247	File export status .....	515
Configuration Change Log.....	294,513	File Operation Log .....	22
Configuration Change Log List.....	299	File Operation Log.....	503
Configuration Information Tree .....	108	File operation status .....	515
Considerations for Preparing Operating Environment .....	27	File Reading Prohibition.....	457
Content of Comprehensive Analysis Report.....	340	File Trace Function of Log Viewer .....	25
Content of Information Disclosure Analysis Report.....	321	Flow of Operation .....	1
Content of Printing Volume Auditing Report.....	347	Flow of Preparing Operating Environment.....	46
Content of Terminal Usage Analysis Report.....	331	FTP Operation Log .....	21
Contents of Analysis Report of Violation Operation.....	336	FTP Operation Log.....	498
Control Client (CT).....	229	FTP Operation Prohibition Log.....	499
Control Services of Client (CT).....	230	FTP Server Connection Prohibition .....	13
Control the Processes of Client (CT).....	233	FTP Server Connection Prohibition.....	470
			[G]
		General Functions .....	2



Settings of [File Export Prohibition] Tab .....	64	What is Report Output Tool.....	313
Settings of [File Operational Process] Tab .....	81	Window Title Log.....	482
Settings of [File Operation Extension] Tab .....	85	Window Title Obtaining Log .....	17
Settings of [FTP Server Connection Prohibition] Tab.....	98	Worst Ranking of Violations.....	256
Settings of [Log Filtering Condition] Tab .....	90		
Settings of [Logon Prohibition] Tab .....	77		
Settings of [Log Switches] Tab.....	61		
Settings of [Other Settings] Tab .....	100		
Settings of [Printing Prohibition] Tab .....	75		
Settings of [Screen Capture Condition] Tab .....	92		
Settings of [URL Access Prohibition] Tab .....	96		
Settings of [Web Upload and Download Prohibition] Tab .....	99		
Specified USB Device.....	377		
Start Log Analyzer.....	247		
Start Log Viewer.....	263		
Start Management Console .....	49		
Start Report Output Tool.....	314		
Summary sheet.....	322		
System Structure from 2-level to 3-level.....	366		
Systemwalker Desktop Patrol.....	114		
[T]			
Target group sheet.....	326		
Target Group Sheet.....	343		
Terminal Operation Settings window.....	404		
Terminal Usage Analysis Report.....	327		
The status of applications and E-mails .....	516		
The violation status .....	515		
trace file.....	307		
Trace File Operation.....	299		
tracing file.....	307		
tracing result of file operation.....	307		
Transmission Schedule on Management Server .....	152		
Trend of Client (CT) Operation.....	238		
[U]			
Update/Move/Delete User.....	214		
URL Access Prohibition .....	13		
URL Access Prohibition.....	468		
USB devices permitted to be used.....	388		
User group .....	128		
User Group Policy.....	202		
Use Systemwalker Desktop Patrol Configuration Information Import Command .....	115		
[V]			
viewing logs.....	477		
View Logs.....	275		
View logs.....	478		
Violation Analysis Report.....	331		
[W]			
Web access status .....	517		
Web Download Prohibition.....	472		
Web Operation Log .....	20		
Web Operation Log.....	495		
Web Operation Prohibition Log.....	496		
Web Upload and Download Operation Prohibition .....	13		