

FUJITSU Software

Systemwalker Desktop Keeper

A decorative horizontal band with a red-to-dark-red gradient. It features abstract, glowing white and red lines that swirl and intersect, creating a sense of motion and depth.

User's Guide for Administrator

Windows

B1WD-3254-04ENZ0(00)
July 2015

Preface

Purpose of This Guide

This guide describes how to use the following product:

- Systemwalker Desktop Keeper V15.1.0

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(R) Windows
- General knowledge of the Internet
- General knowledge of VMware View(TM) (when installing client (CT) in the VMware View(TM) environment)
- General knowledge of Citrix XenDesktop(TM) (when installing client (CT) in the VMware View(TM) environment)
- General knowledge of Google Android(TM) (when installing the smart device (agent) (Android))
- General knowledge of iOS (when installing the smart device (agent) (iOS))

Structure of This Guide

The structure of this guide is as follows:

[Chapter 1 Before Operation](#)

This chapter describes the entire flow of operation and the notes for functions.

[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](#)

This chapter describes the methods for changing policies through management console

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

This chapter describes the methods for capturing abnormal points in log through the status window or log analyzer.

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

This chapter describes the methods for viewing logs.

[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 Release Information	This guide describes the additional features and incompatibility information of Systemwalker Desktop Keeper.
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 for 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 Systemwalker Desktop Keeper Export Utility.
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" menu of the Systemwalker Desktop Keeper Export Utility.

Symbols used in this guide

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

Symbols Used in Commands

This subsection describes the symbols used in examples of commands.

Meaning of symbols

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

Abbreviations

The manual uses abbreviations of the following products.

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 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	SEV13.2.0
Systemwalker Desktop Keeper V14g (14.2.0)	V14.2.0
Systemwalker Desktop Keeper V15.1.0	V15.1.0
Microsoft(R) Internet Explorer(R) 6.0 Windows(R) Internet Explorer(R) 7 Windows(R) Internet Explorer(R) 8 Windows(R) Internet Explorer(R) 9	Internet Explorer(R)

Product Name	Abbreviation
Windows(R) Internet Explorer(R) 10 Windows(R) Internet Explorer(R) 11	

The manual uses abbreviations of the following operation systems.

OS	Abbreviation
Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials	Windows Server(R) 2012 R2
Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Essentials Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials	Windows Server(R) 2012
Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows(R) Small Business Server 2011 Essentials	Windows Server(R) 2008 (*1)
Microsoft(R) Windows Server(R) 2003, Standard Edition Microsoft(R) Windows Server(R) 2003, Enterprise Edition Microsoft(R) Windows Server(R) 2003, Standard x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition	Windows Server(R) 2003 (*1)
Microsoft(R) Windows(R) 2000 Professional operating system Microsoft(R) Windows(R) 2000 Server operating system Microsoft(R) Windows(R) 2000 Advanced Server operating system	Windows(R) 2000
Microsoft(R) Windows NT(R) Server Version 4.0 Microsoft(R) Windows NT(R) Workstation Version 4.0	Windows NT(R)
Microsoft(R) Windows(R) XP Professional Microsoft(R) Windows(R) XP Home Edition	Windows(R) XP (*1)
Windows Vista(R) Home Basic Windows Vista(R) Home Premium Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate	Windows Vista(R) (*1)
Windows(R) 8.1 Enterprise Windows(R) 8.1 Pro Windows(R) 8.1	Windows(R) 8.1 (*1)

OS	Abbreviation
Windows(R) 8 Enterprise Windows(R) 8 Pro Windows(R) 8	Windows(R) 8 (*1)
Windows(R) 7 Ultimate Windows(R) 7 Enterprise Windows(R) 7 Professional Windows(R) 7 Home Premium	Windows(R) 7 (*1)
Microsoft(R) Windows(R) Millennium Edition	Windows(R) ME
Microsoft(R) Windows(R) 98 Second Edition	Windows(R) 98
Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 Foundation Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Essentials Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Foundation Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Essentials Microsoft(R) Windows Server(R) 2008 Foundation Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows(R) Small Business Server 2011 Essentials Microsoft(R) Windows Server(R) 2003, Standard Edition Microsoft(R) Windows Server(R) 2003, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003, Standard x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Microsoft(R) Windows(R) 2000 Professional operating system Microsoft(R) Windows(R) 2000 Server operating system Microsoft(R) Windows(R) 2000 Advanced Server operating system Microsoft(R) Windows(R) XP Professional Microsoft(R) Windows(R) XP Home Edition Windows Vista(R) Home Basic Windows Vista(R) Home Premium Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate Windows(R) 7 Ultimate Windows(R) 7 Enterprise Windows(R) 7 Professional Windows(R) 7 Home Premium Windows(R) 8 Enterprise Windows(R) 8 Pro Windows(R) 8 Windows(R) 8.1 Enterprise Windows(R) 8.1 Pro Windows(R) 8.1	Windows

OS	Abbreviation
Microsoft(R) Windows(R) Millennium Edition Microsoft(R) Windows(R) 98 Second Edition	
Android(TM) 3.0 - Android(TM) 5.0	Android
iOS 5.0 - iOS 8.1	iOS

*1: For commands and file saving locations, especially when they are differentially noted under the 64-bit edition, the abbreviations are as follows:

- Windows Server(R) 2008 64-bit Edition
- Windows Server(R) 2008 R2
- Windows Server(R) 2003 x64 Edition
- Windows Server(R) 2003 R2 x64 Edition
- Windows(R) XP 64-bit Edition
- Windows Vista(R) 64-bit Edition
- Windows(R) 7 64-bit Edition
- Windows(R) 8 64-bit Edition
- Windows(R) 8.1 64-bit Edition

Export Management Regulations

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

General Restriction

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

(These functions are available in Japanese version only.)

Prohibition Function

- Encryption Function in File Export
- Encryption Function in E-mail Attachment
- E-mail Attachment Prohibition Function
- E-mail Recipient Address Confirmation 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, pay attention to the following points:

- For character code, replace Shift-JIS with local character code (character code that corresponds to the code page on OS).
- 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, pay attention.

The following versions do not exist, 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 V13.2.1
- Systemwalker Desktop Keeper Base Edition V13.3.0
- Systemwalker Desktop Keeper Standard Edition V12.0L10
- 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)
- Systemwalker Desktop Keeper V14g (14.3.0)
- Systemwalker Desktop Keeper V14g (14.3.1)
- Systemwalker Desktop Keeper V15.0.0
- Systemwalker Desktop Keeper V15.0.1

For example, when it is described as "V13.3.0 or later", since V13.3.0 does not exist, replace it with "V14.2.0 or later". In addition, when it is described as "V14.0.0 or earlier", 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.

Android is a registered trademark or trademark of Google Inc.

Bluetooth is a registered trademark of Bluetooth SIG and is licensed to Fujitsu.

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

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

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

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

Screenshots are used according to the guidelines of Microsoft Corporation

July 2015

Revision History
July 2015, First Edition

Copyright 2005 - 2015 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.....	8
1.2.3 About Installation of Client (CT) of Management (Master Management) Server.....	8
1.2.4 About Windows Vista(R) 64-Bit Edition, Windows(R) 7 64-Bit Edition, Windows Server(R) 2008 64-Bit Edition, Windows Server(R) 2008 R2 Edition, Windows(R) 8 64-Bit Edition, and Windows Server(R) 2012.....	9
1.2.5 Smart Device (Agent).....	9
1.2.6 Export Utility.....	11
1.2.7 About USB Device Individual Identification Function.....	14
1.2.8 File Export Prohibition.....	14
1.2.9 Printing Prohibition.....	16
1.2.10 Logon prohibition.....	17
1.2.11 Application Startup Prohibition	17
1.2.12 URL Access Prohibition.....	17
1.2.13 FTP Server Connection Prohibition.....	17
1.2.14 Web Upload and Download Operation Prohibition.....	18
1.2.15 Clipboard Operation Prohibition.....	18
1.2.16 Wi-Fi Connection Prohibition (Smart Device).....	19
1.2.17 Application Usage Prohibition (Smart Device).....	19
1.2.18 All Logs (for Clients (CT)).....	19
1.2.19 File Export Log.....	20
1.2.20 Printing Operation Log.....	20
1.2.21 Window Title Obtaining Log.....	22
1.2.22 E-mail Sending Log.....	23
1.2.23 Command Operation Log.....	24
1.2.24 Device Configuration Change Log.....	25
1.2.25 PrintScreen Key Operation Log.....	26
1.2.26 Web Operation Log.....	26
1.2.27 FTP Operation Log.....	27
1.2.28 Clipboard Operation Log.....	27
1.2.29 File Operation Log.....	28
1.2.30 Logon/Logoff Log.....	31
1.2.31 Screen Capture.....	32
1.2.32 Web Access Log (Smart Device).....	32
1.2.33 Wi-Fi Connection Log (Smart Device).....	32
1.2.34 Application Usage Log (Smart Device).....	32
1.2.35 Application Configuration Change Log (Smart Device).....	32
1.2.36 Incoming/Outgoing Calls Log (Smart Device).....	32
1.2.37 Bluetooth Connection Log (Smart Device).....	33
1.2.38 Bluetooth Connection Prohibition (Smart Device).....	33
1.2.39 SIM Card Mount/Unmount Log (Smart Device).....	33
1.2.40 SD Card Mount/Unmount Log (Smart Device).....	33
1.2.41 About Collection of Logs for Investigation of Client (CT).....	33
1.2.42 About File Trace Function of Log Viewer.....	33
1.2.43 About Viewing Operation Logs of the Remote Connection Source and Target in Log Viewer.....	33
1.2.44 Administrator Notification Feature.....	34
1.2.45 IPv6 Support.....	34
1.2.46 Windows Store Apps in Windows(R) 8 or Windows Server(R) 2012 or Later.....	35
1.2.47 Dialog Boxes in Windows(R) 8 and Windows Server(R) 2012 or Later.....	36
1.2.48 Portable Device and Imaging Device Control.....	36
1.2.49 Log Viewing Database.....	36
1.2.50 User Operation Log Search Feature.....	36

Chapter 2 Prepare Operating Environment.....	38
2.1 Considerations for Preparing Operating Environment.....	38
2.1.1 What is Policy.....	38
2.1.2 How to Apply Policy.....	48
2.2 Flow of Preparing Operating Environment.....	55
2.3 Start Management Console.....	58
2.4 Set Initial Value of Policy.....	69
2.4.1 Perform Terminal Initial Settings.....	69
2.4.1.1 Log Collection Operation (Windows).....	70
2.4.1.2 File Operation.....	73
2.4.1.3 Extension.....	78
2.4.1.4 Window Title Filter.....	80
2.4.1.5 Window Title Screen Capture.....	82
2.4.1.6 Logon.....	85
2.4.1.7 Application.....	86
2.4.1.8 File Export/Read.....	88
2.4.1.9 Print/PrintScreen.....	98
2.4.1.10 Eco Monitoring.....	100
2.4.1.11 Internet.....	101
2.4.1.12 Web Upload/Download.....	103
2.4.1.13 FTP Server Connection.....	106
2.4.1.14 Clipboard.....	107
2.4.1.15 Send Log.....	108
2.4.1.16 Log Collection Operation (Android).....	110
2.4.1.17 Wi-Fi Connection.....	111
2.4.1.18 Bluetooth Connection.....	112
2.4.1.19 Application (Android).....	113
2.4.1.20 Device Functionality.....	115
2.4.1.21 Application (iOS).....	117
2.4.1.22 iCloud.....	118
2.4.1.23 Security and Privacy.....	119
2.4.1.24 Content Ratings.....	120
2.4.2 Perform Terminal Operation Settings.....	121
2.5 Create Configuration Information Tree.....	131
2.5.1 Import Information from Active Directory.....	131
2.5.2 Import Information from Systemwalker Desktop Patrol	137
2.5.3 Create through Management Console.....	146
2.6 Allocate Department Administrator.....	152
2.6.1 Export Department Administrator Information through Management Console.....	157
2.7 Preparations for Log Aggregation.....	159
2.7.1 Prepare for Using Status Window.....	159
2.7.2 Prepare for Using Log Analyzer.....	168
2.7.2.1 Schedule Log Transmission.....	168
2.7.2.1.1 Set Log Obtaining Period on Management Server.....	168
2.7.2.1.2 Setting Data Transfer Time on the Management Server.....	170
2.7.2.1.3 Setting Data Import Time on the Log Analyzer Server.....	172
2.7.2.2 Set Conditions for Aggregation/Report Output.....	174
2.7.2.2.1 Set Ranking Display Number.....	177
2.7.2.2.2 Set Screening Condition.....	178
2.7.2.2.3 Set Items Excluded From Aggregation Target.....	181
2.7.2.2.4 Set Other Conditions.....	184
2.7.2.2.5 Select Log Analyzer Server.....	186
Chapter 3 Set Policy in Management Console.....	188
3.1 Search CT Information/User Information.....	188
3.2 Modify Group Policy.....	196
3.2.1 Modify CT Group Policy.....	196

3.2.2 Modify User Group Policy.....	199
3.3 Allocate CT/User to Group.....	204
3.3.1 Add/Move/Delete CT.....	204
3.3.2 Register a User.....	207
3.3.3 Update/Move/Delete User.....	210
3.4 Modify CT Policy/User Policy.....	212
3.4.1 Modify CT Policy.....	212
3.4.2 Modify User Policy.....	216
3.5 Export CT information/User information.....	217
3.6 Control Client (CT).....	223
3.6.1 Control Services of Client (CT).....	223
3.6.2 Control the Processes of Client (CT).....	225
3.7 Controlling Smart Device (Agent).....	228
3.7.1 Controlling Smart Device (Agent) Remotely.....	228
3.7.2 Checking Remote Control Status.....	230
3.7.3 Controlling Smart Device when Password Entry Fails.....	233
Chapter 4 Check Trend of Client (CT) Operation.....	237
4.1 Check the Trend in Status Window.....	238
4.1.1 Display Status Window.....	238
4.1.2 Confirm Result of Log Aggregation.....	240
4.2 Check the Trend in Log Analyzer.....	244
4.2.1 Start Log Analyzer.....	245
4.2.2 Diagnose Risk of Information Disclosure.....	248
4.2.2.1 Display the Result of aggregation by Operation.....	248
4.2.2.2 Display the Ranking of Violations.....	253
4.2.2.3 Specify a Past Date to Display Aggregation Result.....	253
4.2.3 Aggregate by Objectives.....	253
Chapter 5 Audit Operations on Client (CT) via Log Viewer.....	261
5.1 Start Log Viewer.....	261
5.2 View Logs.....	271
5.2.1 View Logs in the CT Operation Log Window.....	275
5.2.2 View Logs in the User Operation Log Window.....	292
5.2.3 View Logs in the Configuration Change Log Window.....	300
5.3 Trace File Operation.....	305
5.4 Search CT Information in Log Viewer.....	313
5.5 Search User Information in the Log Viewer.....	317
Chapter 6 Create Auditing Material.....	320
6.1 How to Make Flexible Use of Report Output Tool.....	320
6.2 Start Report Output Tool.....	322
6.3 Information Disclosure Analysis Report.....	323
6.3.1 Output Information Disclosure Analysis Report.....	323
6.3.2 Content of Information Disclosure Analysis Report.....	329
6.4 Terminal Usage Analysis Report.....	335
6.4.1 Output Terminal Usage Analysis Report.....	335
6.4.2 Content of Terminal Usage Analysis Report.....	338
6.5 Violation Analysis Report.....	338
6.5.1 Output Violation Analysis Report.....	339
6.5.2 Contents of Analysis Report of Violation Operation.....	342
6.6 Comprehensive Analysis Report.....	342
6.6.1 Output Comprehensive Analysis Report.....	343
6.6.2 Content of Comprehensive Analysis Report.....	345
6.7 Printing Volume Auditing Report.....	348
6.7.1 Output Printing Volume Auditing Report.....	349
6.7.2 Content of Printing Volume Auditing Report.....	351
6.8 Set Report Output Schedule.....	360

Chapter 7 Change Operating Environment.....	364
7.1 Change Import Method of Configuration Information.....	364
7.2 Change Management Method of User Information.....	367
7.3 Change System Structure from 2-level to 3-level.....	369
7.4 Add/Delete Management Server in 3-level System Structure.....	373
7.5 Export Files to Specified USB Device Only.....	377
7.5.1 Operation example.....	378
7.5.2 Register USB device.....	384
7.5.3 Set USB devices permitted to be used in policy setting.....	394
7.5.4 Register USB device information using CSV file.....	397
7.5.5 Export registered USB device information as CSV file.....	398
7.5.6 Modify the registered USB device information.....	399
7.6 Modify Period to Save Logs.....	400
7.7 Change CT Environment.....	400
7.7.1 Change Management Server/Master Management Server To Be Connected.....	400
7.7.2 Change Operation Settings of Client (CT).....	405
7.7.3 Replace Client (CT).....	410
7.8 Change Management Console Environment.....	411
7.9 Change Management Server Environment.....	411
7.9.1 Start Server Settings Tool.....	412
7.9.2 Change Password of Initial Administrator.....	415
7.9.3 Modify Administrator Notification.....	415
7.9.4 Change System Environment with the Change of IP Address/Computer Name of Management Server/Master Management Server.....	416
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.....	440
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.....	443
7.12 Change Log Analyzer Environment.....	443
7.12.1 Transfer Log Analyzer Server.....	443
7.12.2 Modify IP Address/Port Number of Log Analyzer Server.....	445
7.12.3 Change the Data Transfer Task on the Management Server.....	446
7.12.4 Change the Data Import Task on the Log Analyzer Server.....	450
7.13 Change the Smart Device Relay Server Environment.....	455
7.13.1 Change the Connection Destination (Master) Management Server.....	455
7.13.2 Change the Smart Device Relay Server IP Address.....	455
7.13.3 Install and Add Systemwalker Desktop Patrol.....	456
Chapter 8 Policies That Can be Set.....	457
8.1 Set the Policies of Prohibition Function.....	457
8.1.1 File Export Prohibition.....	457
8.1.2 File Reading Prohibition.....	459
8.1.3 Printing Prohibition.....	461
8.1.4 Logon Prohibition.....	463
8.1.5 Application Startup Prohibition.....	464
8.1.6 PrintScreen Key Prohibition.....	466
8.1.7 URL Access Prohibition.....	467
8.1.8 FTP Server Connection Prohibition.....	469
8.1.9 Web Upload Prohibition.....	471
8.1.10 Web Download Prohibition.....	472
8.1.11 Clipboard Operation Prohibition.....	474
8.1.12 Wi-Fi Connection Prohibition (Smart Device).....	475
8.1.13 Bluetooth Connection Prohibition (Smart Device).....	476
8.1.14 Application Usage Prohibition (Smart Device).....	476
8.1.15 Device Functionality (iOS Device).....	477

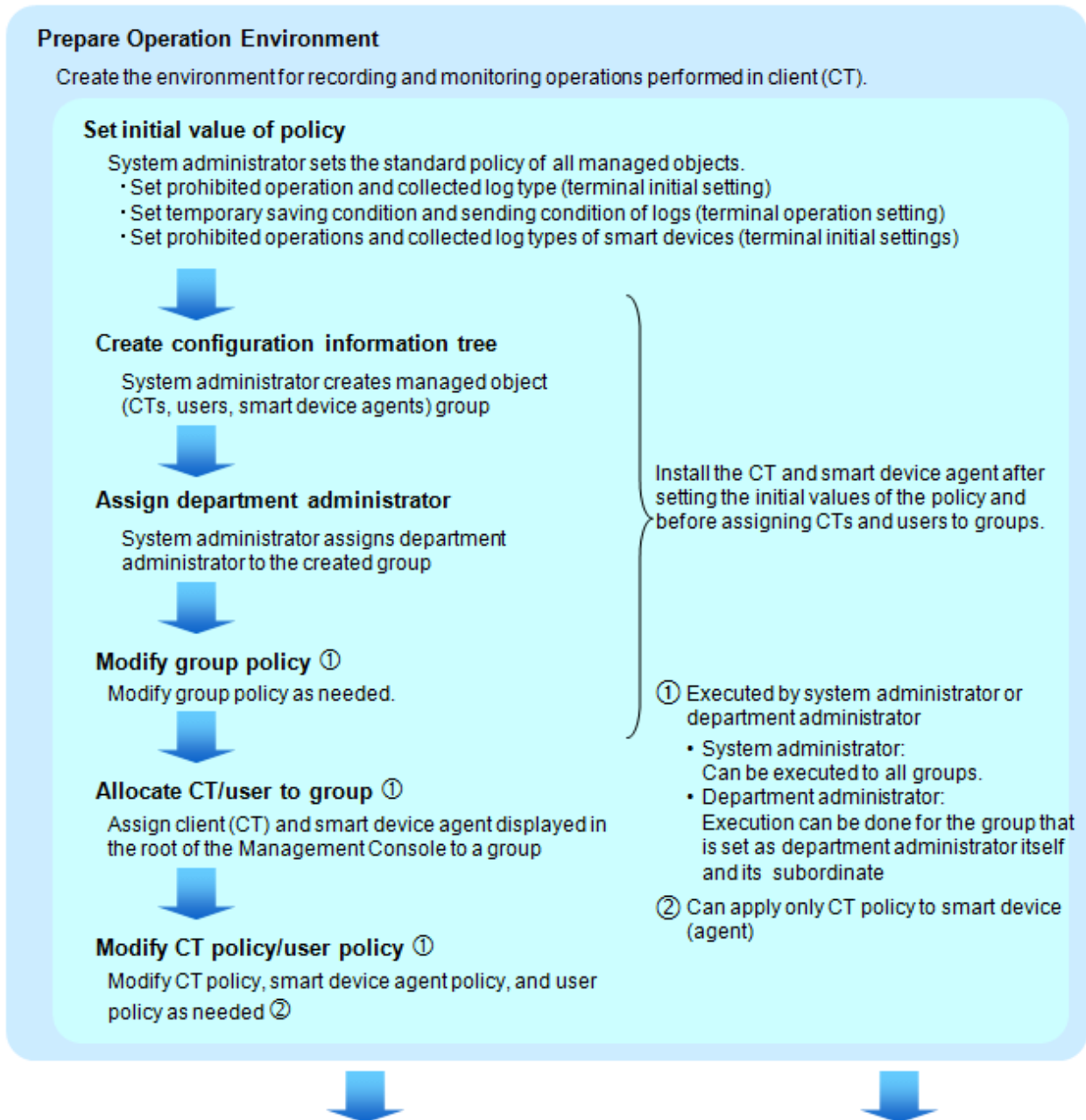
8.1.16 Applications (iOS Device).....	478
8.1.17 iCloud (iOS).....	479
8.1.18 Security and Privacy (iOS).....	480
8.1.19 Content Ratings (iOS).....	480
8.2 Policy Settings of Record Function.....	481
8.2.1 Application Startup Log.....	484
8.2.2 Application Termination Log.....	485
8.2.3 Application Startup Prohibition Log.....	486
8.2.4 Window Title Obtaining Log.....	486
8.2.5 E-mail Sending Log.....	488
8.2.6 Device Configuration Change Log.....	490
8.2.7 Printing Operation Log.....	493
8.2.8 Printing Prohibition Log.....	494
8.2.9 Logon Prohibition Log.....	495
8.2.10 File Export Log.....	495
8.2.11 PrintScreen Key Operation Log.....	497
8.2.12 PrintScreen Key Prohibition Log.....	498
8.2.13 Web Operation Log.....	499
8.2.14 Web Operation Prohibition Log.....	500
8.2.15 FTP Operation Log.....	502
8.2.16 FTP Operation Prohibition Log.....	503
8.2.17 Clipboard Operation Log.....	504
8.2.18 Clipboard Operation Prohibition Log.....	505
8.2.19 File Operation Log.....	506
8.2.20 Logon/Logoff Log.....	512
8.2.21 Linkage Application Log.....	516
8.2.22 Configuration Change Log.....	517
8.2.23 Wi-Fi Connection Log (Smart Device).....	518
8.2.24 Wi-Fi Connection Prohibition Log (Smart Device).....	519
8.2.25 Bluetooth Connection Log (Smart Device).....	520
8.2.26 Bluetooth Connection Prohibition Log (Smart Device).....	520
8.2.27 Application Usage Log (Smart Device).....	521
8.2.28 Application Usage Prohibition Log (Smart Device).....	522
8.2.29 Web Access Log (Smart Device).....	523
8.2.30 SD Card Mount/Unmount Log (Smart Device).....	524
8.2.31 SIM Card Mount/Unmount Log (Smart Device).....	526
8.2.32 Incoming/Outgoing Calls Log (Smart Device).....	526
8.2.33 Application Configuration Change Log (Smart Device).....	527
Appendix A List of Aggregation Objectives.....	529

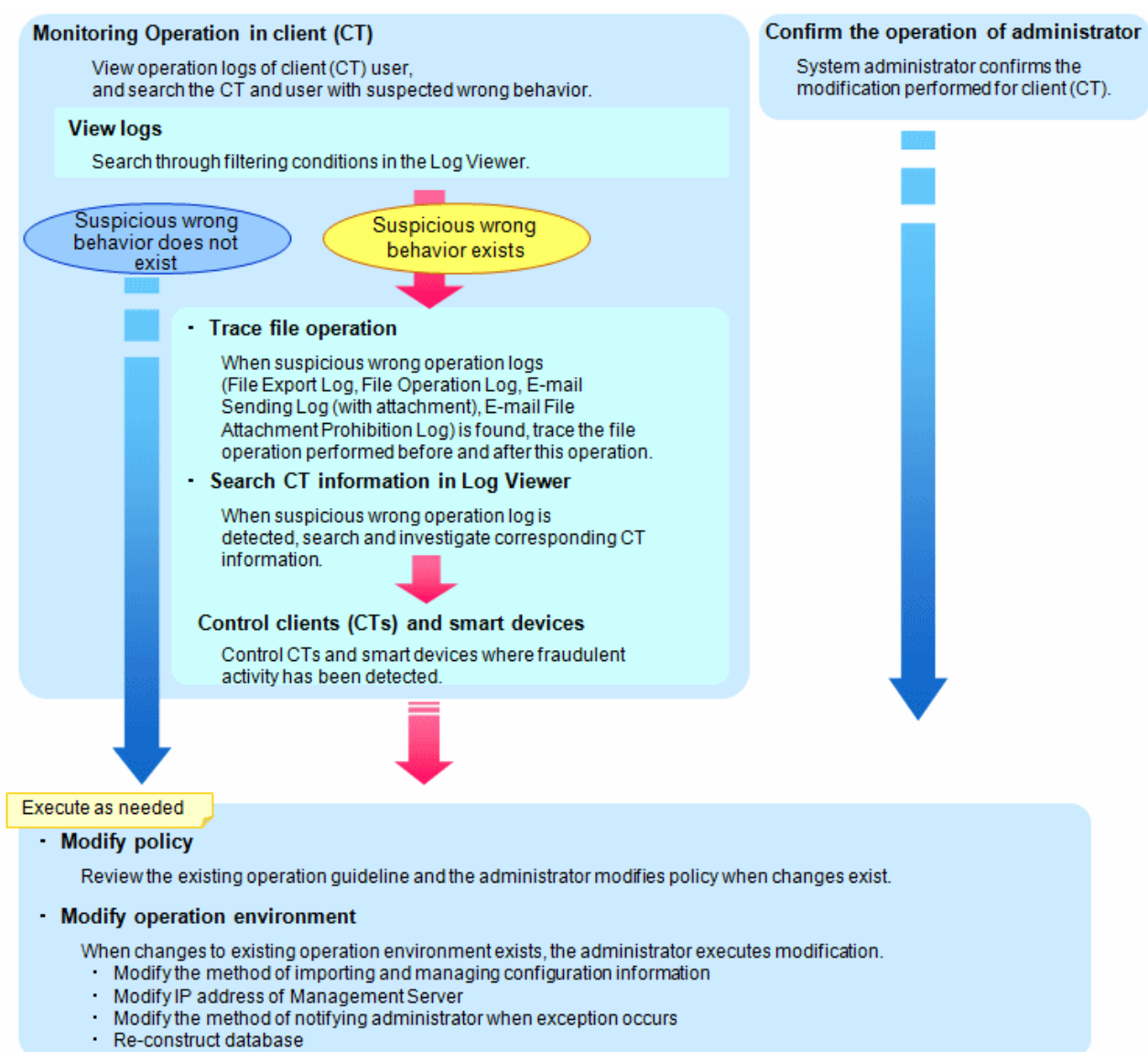
Chapter 1 Before Operation

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

This chapter provides notes relating to Systemwalker Desktop Keeper features.

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(R) 2008, the email 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:
This does not apply when email is sent from Microsoft(R) Outlook(R) 2007, Microsoft(R) Outlook(R) 2010, or Microsoft(R) Outlook(R) 2013.
- 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.
- When multiple users are logged on, messages displayed during process control and service control will be sent to a specific user only. The display conditions are as follows:
 - When there is a locally logged-on user, messages will be displayed to that user.
 - When there is no locally logged-on user, messages will be displayed to one of the remotely logged-on users.
- The policy status when multiple users are logged on is shown in the table below.

With smart devices (Android and iOS devices), only one user is logged on, so operation conforms to the CT policy.

"Multiple users logged on" means that at least two active users are logged on. For example, both local and remote users are logged on or at least two remote users are logged on. This does not apply to multiple local users logged on through switching, because in this case there will be only one active user.

Function		Valid Policy
Log (recording function)	Application startup/termination	User policy.
	Window title obtaining log	User policy.
	E-mail sending	CT policy.
	E-mail sending interruption	CT policy.
	Command operation	User policy.
	Device configuration change	(*1)
	Printing operation	User policy.
	File export	User policy.
	PrintScreen key operation	User policy.
	Web operation	User policy.
	FTP operation	User policy.
	File operation	CT policy.
	Logon/Logoff	CT policy.
	Clipboard operation	User policy.
	Linkage application	User policy.
	Web access log (Android device)	CT policy
	SD card mount/unmount log (Android device)	CT policy
	SIM card mount/unmount log (Android device)	CT policy
	Wi-Fi connection log (Android device)	CT policy
	Bluetooth connection log (Android device)	CT policy
Incoming/outgoing calls log (Android device)	CT policy	
Application usage log (Android device)	CT policy	
Application configuration change log (Android device)	CT policy	
Prohibition function	Application startup prohibition	User policy.
	Printing prohibition	User policy.
	PrintScreen key prohibition	User policy.

	Function	Valid Policy
	Logon prohibition	CT policy.
	E-mail attachment prohibition	CT policy.
	File export prohibition	(*2)
	File reading prohibition	(*2)
	URL access prohibition	User policy.
	FTP server connection prohibition	User policy.
	Web download operation prohibition	User policy.
	Web upload operation prohibition	User policy.
	Clipboard operation prohibition	User policy.
	Wi-Fi access prohibition (Android device)	CT policy
	Bluetooth connection prohibition (Android device)	CT policy
	Application usage prohibition (Android device)	CT policy
	Device Functionality usage (iOS device)	CT policy
	Application usage (iOS device)	CT policy
	iCloud usage (iOS device)	CT policy
	Security and privacy settings (iOS device)	CT policy
	Content Ratings settings (iOS device)	CT policy

*1: The policy status for the device configuration change log depends on the settings in the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window.

- When operating according to the CT policy
 - When **Allow to use all USB devices registered in Management Server** is **Yes**
- When operating according to the user policy
 - When **Allow to use all USB devices registered in Management Server** is **No**

In addition, the device configuration change log, which records the mounting of USB devices, operates according to the CT policy.

*2: The policy status for file export prohibition and file reading prohibition depends on the policy setting in **File export/read**.

- When operating according to the CT policy
 - When **Export using File Export Utility** is **Not Allowed**
 - When Permission switch of all USB registered in Management Server in the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window is **Yes**
- When operating according to the User policy
 - When Export using File Export Utility is **Allowed** and Access Settings in the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window is as follows:
 - **Reading and writing are limited to File Export Utility** is selected
 - **Writing is limited to File Export Utility** is selected
 - When Permission switch of all USB registered in Management Server in the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window is **No**
- When operating according to both the CT policy and user policy
 - User policy setting
 - When **Export using File Export Utility** is **Allowed** and **Permission switch of all USB registered in Management Server** in the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window is **Yes**

When the above policy is used, startup of Export Utility operation is determined according to the user policy, and actual export is determined according to the CT policy.

Example: When the CT policy prohibits the export of removable media, you can start Export Utility. However, the CT policy prohibits export, so you cannot export a file.

- When the OS of the client (CT) is Windows Vista(R), Windows Server(R) 2008, Windows(R) 7 Windows(R) 8, or Windows Server(R) 2012 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, do not click the **Back** button on the browser. If this button is used, errors may occur and it may not display properly.
- 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.
- In some cases the same log is sent by the client (CT) and smart device (agent) (Android) and stored in the Management Server. If this happens, the same log is displayed multiple times in the Log Viewer.
- If you have logged on using the built-in Administrator account of the operating systems below, use Internet Explorer(R) in the Desktop application on Web Console. Internet Explorer(R) from Windows Store apps is not supported.
 - Windows(R) 8 Pro
 - Windows(R) 8 Enterprise
 - Windows(R) 8.1 Pro
 - Windows(R) 8.1 Enterprise
 - Microsoft(R) Windows Server(R) 2012 Datacenter
 - Microsoft(R) Windows Server(R) 2012 Standard
 - Microsoft(R) Windows Server(R) 2012 Essentials
 - Microsoft(R) Windows Server(R) 2012 Foundation
 - Microsoft(R) Windows Server(R) 2012 R2 Datacenter
 - Microsoft(R) Windows Server(R) 2012 R2 Standard
 - Microsoft(R) Windows Server(R) 2012 R2 Essentials
 - Microsoft(R) Windows Server(R) 2012 R2 Foundation
- Communication between the Management Server or Master Management Server and a client (CT) is encrypted. Therefore, there are restrictions on unencrypted communications, such as communication with a client (CT) of V14.3.1 or earlier to which the communication encryption update has not been applied.
 - You must apply the urgent updates that were released in and after September 2014 to clients of V13.3.0 to V14.3.1, or upgrade to V15.1.
 - You cannot use clients of V13.2.1 or earlier. Upgrade to V15.1.0.
 - After you upgrade the Management Server to V15.1.0, the clients that you can fresh install are V15.0.0 and V15. 1.0.
- After logging on using a Microsoft account, the Microsoft account information is stored in the user name and domain name of the log. For example, if the Microsoft account is "fujitsu.tarou@example.com", the user name will show "fujitsu.tarou" and the domain name will show "example.com".

However, if you switch from an existing account to a Microsoft one, the existing account information may be stored in the user name and domain name of the log until the operating system is restarted.
- The log user name recorded is the one used for logon. The user name used for domain logon is neither case- nor width-sensitive, so the user name recorded may differ from the one used during registration.

Policies that can be set on client (CT) and smart device (agent)

The Management Console allows setting all policies for clients (CTs) and smart devices (agents), but which ones will take effect depend on the device. If a policy is set but does not take effect on a specific device, the recording feature or prohibition feature will not operate.

	Policy	Device		
		Client (CT)	Smart device (agent) (Android)	Smart device (agent) (iOS)
Log (recording feature)	Application startup	Y	N	N
	Application termination	Y	N	N
	Window title obtaining	Y	N	N
	E-Mail Sending/E-mail sending interruption	Y	N	N
	Command operation	Y	N	N
	Device configuration change	Y	N	N
	Printing operation	Y	N	N
	File export	Y	N	N
	PrintScreen key operation	Y	N	N
	Web operation	Y	N	N
	FTP operation	Y	N	N
	File operation	Y	N	N
	Logon,Logoff	Y	N	N
	Clipboard operation	Y	N	N
	Linkage application	Y	N	N
	Web access	N	Y	N
	SD card mount/unmount	N	Y	N
	SIM card mount/unmount	N	Y	N
	Wi-Fi connection	N	Y	N
	Bluetooth connection	N	Y	N
	Incoming/outgoing calls	N	Y	N
Application usage	N	Y	N	
Application configuration change	N	Y	N	
Prohibition feature	File access control	Y	N	N
	Application startup prohibition	Y	N	N
	Print prohibition	Y	N	N
	PrintScreen key prohibition	Y	N	N
	Logon prohibition	Y	N	N
	Attachment prohibition	Y	N	N
	URL access prohibition	Y	N	N
	FTP operation prohibition	Y	N	N
	Web operation prohibition	Y	N	N
	Clipboard operation prohibition	Y	N	N
	Wi-Fi connection prohibition	N	Y	N
	Bluetooth connection prohibition	N	Y	N
Application usage prohibition	N	Y	N	

Policy		Device		
		Client (CT)	Smart device (agent) (Android)	Smart device (agent) (iOS)
	Device Functionality usage	N	N	Y
	Application usage	N	N	Y
	iCloud usage	N	N	Y
	Security and privacy settings	N	N	Y
	Content Ratings settings	N	N	Y

Y: The recording and prohibition features operate when this is set as a policy on Management Console.

N: The recording and prohibition features do not operate even when this is set as a policy on Management Console.

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 "?".

Support for Unicode characters in clients (CTs) and smart devices (agents)

Operation logs and prohibition logs collected by a client (CT) or smart device (agent) are stored using Unicode characters.

Any collected application log that cannot handle Unicode characters may be recorded as "?".

If the export source file or folder name contains Unicode characters when Export Utility exports a file or folder to a destination listed below, you cannot specify that file or folder as the export source.

In addition, if the export destination file or folder name contains Unicode characters, you cannot specify that file or folder as the export destination.

- Export to a DVD or CD
- Encryption export to a destination other than a DVD or CD

Support for Unicode characters in Management Console

Entry and display operations in Management Console use Unicode characters.

However, if you have specified **ShiftJIS** for **Encoding for I/O files** in Server Settings Tool, any Unicode characters in an input file will not be displayed properly. If an output file contains Unicode characters, they will be converted to "?".

Support for Unicode characters in the Log Viewer

Entry and display operations in the Log Viewer use Unicode characters.

However, if you have specified **ShiftJIS** for **Encoding for I/O files** in Server Settings Tool, Unicode characters in the output file will be converted to "?".

Support for Unicode characters in other tools

- Commands provided by Systemwalker Desktop Keeper and server-based tools such as Server Settings Tool do not support entry or display of Unicode characters.

When the user name used for logon to Windows contains Unicode characters

- Do not use the following tools and commands that are provided by Systemwalker Desktop Keeper because they may not operate properly:
 - Tools and commands that are installed in the Management Server or Master Management Server

- Tools and commands that are installed in Smart Device Relay Server
- The Policy Application Tool
- You cannot perform encryption export to a DVD or CD by using the Export Utility.

Halfwidth and fullwidth characters and character count handled by Systemwalker Desktop Keeper

In Systemwalker Desktop Keeper, halfwidth character, fullwidth character, and character count are defined as follows:

- Halfwidth character: A character with an ASCII code in the range 0x20 to 0x7E
Space
Symbols: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~
Numeric characters: 0-9
Alphabetic characters: A-Z, a-z
- Fullwidth characters: Characters other than halfwidth characters
Halfwidth katakana characters (the width that is generally used) are treated as fullwidth characters.
- Character count: Each halfwidth character is counted as 1 character.
Each UTF-16 2-byte fullwidth character is counted as 1 character.
Each surrogate pair character uses 4 bytes to represent 1 character, so it is counted as 2 characters.
Each combining character uses n bytes to represent 1 character, so it is counted as n/2 or less characters, depending on the combining character.

Operating system updates after installation of Systemwalker Desktop Keeper

After upgrading to Windows(R) 8.1, it may temporarily not be possible to write to a CD or DVD.
If this happens, restart the operating system.

1.2.2 About Collective Management of User Policy

When communication between the Master Management Server and the Management Server is disabled due to network problems in the following case, you can connect Management Console to the Management Server and temporarily change the user policy:

- Server Settings Tool was used to configure the settings so that the Master Management Server centrally manages user information.

However, when communication between the Master Management Server and the Management Server resumes and Management Console that is connected to the Master Management Server is used to again update the user policy, the content that was set in the Management Server is overwritten.

When you restart the Management Server service, all the following information is overwritten by the Master Management Server settings:

- Administrator information
- User policy information and user group policy information
- User department configuration
- Department administrator information set for User Group

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. Refer to Section 1.2.48, "[1.2.45 IPv6 Support](#)" for the values displayed in IPv6.
- 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(R) 64-Bit Edition, Windows(R) 7 64-Bit Edition, Windows Server(R) 2008 64-Bit Edition, Windows Server(R) 2008 R2 Edition, Windows(R) 8 64-Bit Edition, and Windows Server(R) 2012

- In the **Get/Control Process List** function of the Management Console, when the client (CT) is Windows Vista(R) 64-bit edition, Windows(R) 7 64-bit edition, Windows Server(R) 2008 64-bit edition, Windows Server(R) 2008 R2 edition, Windows(R) 8 64-bit edition, or Windows Server(R) 2012, the process list of 64-bit application cannot be viewed. Also, the processes cannot be terminated.

1.2.5 Smart Device (Agent)

Common to Android and iOS

- Only CT policies can be applied to smart devices (agents).
- Data is transferred periodically between smart devices (agents) and the Management Server. Therefore, it is advisable to subscribe to a fixed price packet communication plan. Refer to "[Timing of communication between a smart device \(agent\) and the Management Server](#)" for details on communication timing and transferred data.
- Smart devices (agents) do not support DTKCTEntry.csv (automatic distribution file during CT registration) for automatic distribution during CT registration. All smart devices (agents) are placed directly under the root during registration.
- The table below lists the timing of communication between a smart device (agent) and the Management Server. Even if you update the policy for a smart device (agent) and click **Update Immediately** on Management Console, the updated policy will not be applied to the smart device (agent) until the time indicated below.

Timing of communication between a smart device (agent) and the Management Server

Timing	Description of communication	
	Smart device (agent) to Management Server	Management Server to smart device (agent)
Android		
When the smart device (agent) is started (*3)	Device information Accumulated operation logs Accumulated prohibition logs	Policy information
Every 8 hours (*1)	Accumulated operation logs (*2)	-
Every hour (*1)	Accumulated prohibition logs (*2) Remote control request confirmation (*4)	-
Once per day at a set time (12:00 to 13:00)	Device information (*2)	Policy information
When Sync now is clicked on the smart device (agent)	Device information Accumulated operation logs Accumulated prohibition logs	Policy information

Timing	Description of communication	
	Smart device (agent) to Management Server	Management Server to smart device (agent)
	Remote control request confirmation (*4)	
iOS		
When the relay server is started	Device information	-
Every 24 hours after the relay server is started	Device information	-

*1: The smart device (agent) startup time is used as the reference point.

*2: If the communication status or other reason prevents data transfer, retry is performed when communication is enabled. In addition, communication is attempted as soon as Wi-Fi is enabled. If both the retry and the attempt fail, data will be transferred at the timing described below.

*3: This timing applies if **Synchronize when starting up** is selected in the smart device (agent) settings window (the smart device (agent) starts when the smart device starts up)

*4: A remote control request confirmation is a communication that periodically asks if a remote control request has been made to smart device (agent).

If a remote control request has been made, the smart device (agent) sends the device information and also sends a communication to obtain policy information.

Android

- The user can use a standard application (for example, settings) that changes the smart device environment to uninstall a smart device (agent), as follows:
 - Set a client management password and ensure that **Select device administrators > Desktop Keeper Client** cannot be cleared.
- Under the following condition, the user can forcibly stop the smart device (agent) or delete data:
 - **Select device administrators > Desktop Keeper Client** is cleared on the smart device

Follow the procedure below:

- Configure operation to prevent smart device (agent) data from being deleted and the smart device (agent) from being forcibly stopped.
- Set a client management password and ensure that **Select device administrators > Desktop Keeper Client** cannot be cleared (supported in Android 4.0 and later).
- Operation in the multi-user environment of Android 4.2 or later is not supported.



Note

The Smart Device Relay Server and the smart device (agent) communicate periodically. Therefore, follow the procedure below so that connection is not closed during sleep when communication happens via Wi-Fi:

- Tap **Settings > Wireless & networks > Wi-Fi settings > Advanced > Wi-Fi sleep policy**, and select **Never**.
The setting may be found in a different location depending on the model. Refer to the manual for your model for details.

This setting may affect battery time.

If you do not configure this setting, the smart device (agent) may not be able to receive any remote control requests.

You do not need to configure this setting for communication with Smart Device Relay Server via a 3G line.

iOS

- The wipe information following a failure of the prescribed number of retries to clear the screen lock on a smart device (agent) (iOS) is not sent to Smart Device Relay Server. Therefore, you cannot confirm a wipe on Management Console.

- If **Content Ratings** is set for an iOS device, region settings different from **Ratings region** in the iOS device may not take effect. Configure the setting to suit the **Ratings region** setting in the iOS device.

1.2.6 Export Utility

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)
DVD/CD		More than 1.5 times of the capacity of files that are actually exported	More than 2.5 times of the capacity of files that are actually exported
Except DVD/CD	When it is not system drive (Note 2)	Not required	Same capacity as that of files that are actually exported
	When it is system drive	Same capacity as that of files that are actually exported	More than 2 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.
- When exporting a write-protected folder in the OS later than Windows Vista(R) 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

- 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(R) 7 Ultimate
- Windows(R) 7 Enterprise
- Windows(R) 7 Professional
- Windows(R) 7 Home Premium
- Windows Vista(R) Home Basic
- Windows Vista(R) Home Premium

- Windows Vista(R) Business
- Windows Vista(R) Enterprise
- Windows Vista(R) Ultimate
- Windows(R) 8 Enterprise
- Windows(R) 8 Pro
- Windows(R) 8.1 Enterprise
- Windows(R) 8.1 Pro

Export Files to DVD-R/RW

- Windows(R) 7 Ultimate
 - Windows(R) 7 Enterprise
 - Windows(R) 7 Professional
 - Windows(R) 7 Home Premium
 - Windows Vista(R) Home Basic
 - Windows Vista(R) Home Premium
 - Windows Vista(R) Business
 - Windows Vista(R) Enterprise
 - Windows Vista(R) Ultimate
 - Windows(R) 8 Enterprise
 - Windows(R) 8 Pro
 - Windows(R) 8.1 Enterprise
 - Windows(R) 8.1 Pro
- 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, 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, 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	Windows Vista(R)	Y	Y	Y	Y	N	N	N	N	N
	Windows(R) 7	Y	Y	Y	Y	N	N	N	N	N
	Windows(R) 8	Y	Y	Y	Y	N	N	N	N	N
Erase	Windows Vista(R)	N	Y	N	Y	N	N	N	N	N
	Windows(R) 7	N	Y	N	Y	N	N	N	N	N
	Windows(R) 8	N	Y	N	Y	N	N	N	N	N
Export prohibition		Y	Y	Y	Y	Y	Y	Y	Y	Y

Y: Supported

N: 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

- Blu-ray and HD DVD are not supported.
- 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. 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, 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).
- When performing DVD/CD writing by using the DVD/CD export function of the Export Utility, 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.

USB device prohibition

If using the USB device prohibition feature to allow only specified USB devices to be used, test operations with the USB device beforehand.

1.2.7 About USB Device Individual Identification Function

- 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/read**, the USB device individual identification function for Windows 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 Windows 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, register by using the information of the USB device in the unlocked state.
- 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, 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 Windows 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/read** of Management Console, the drive letter of the drive under writing prohibition cannot be set. Therefore, when setting the writing prohibition function, 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, access the excluded folder through the UNC path.
- A maximum of 50 excluded folders or 500 characters for all 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, 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, 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
- In Citrix XenDesktop and Citrix XenApp, the mapped drive is the network drive. Reading and writing prohibitions for the network drive can be set, but the excluded folder for network drive access prohibition setting will not be applied.

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)
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 Windows 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, 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, delete again after canceling DVD/CD/BD writing or reading prohibition.
- When you enable DVD and CD writing prohibition in Windows Explorer and then apply the policy, the drive will be hidden as of the next logon.
If you immediately update the policy and cancel the prohibition setting for the DVD or CD drive for which reading prohibition was set, the drive will be visible as of the next logon.
- If you have selected **Use** for the USB Device Individual Identification Function in a previous version and then upgrade to V15.1.0, DVD and CD devices will also be identified individually in V15.1.0. As a result, Export Utility will not be able to write to DVD or CD devices until you register DVD and CD devices connected via USB as allowed devices.
If you want to select **Use** for the USB Device Individual Identification Function and use a DVD or CD device, register the DVD or CD device as an allowed device. DVD and CD devices that are not connected via USB cannot be registered as allowed devices, so writing to those devices is not possible.

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, 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 Windows Explorer is disabled. In this case, 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).
- Printing is performed in Windows(R) Internet Explorer(R) 10 or Windows(R) Internet Explorer(R) 11 (including Windows(R) Internet Explorer(R) 11 Enterprise mode)
- When Microsoft(R) Word is under printing prohibition, two same logs will be collected at one printing operation.
- When UAC (user account control) of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012 is disabled, printing prohibition cannot be performed. The **Print** on the right-click menu of the Windows 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

- 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
- Application startup prohibition can be set per process. Therefore, if a common process will run multiple applications, such as Java applications and Windows Store apps for Windows(R) 8 or Windows Server(R) 2012 or later, you cannot set startup prohibition per application. You can prohibit startup of all Java applications and Windows Store apps by setting startup prohibition for the common process.

1.2.12 URL Access Prohibition

- This function cannot be run in a Web browser that is not Internet Explorer(R).
- This function must be run in Windows(R) Internet Explorer(R) 7 or higher.
- Running the prohibition function will activate the Internet Explorer(R) 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 only one tab is open in Internet Explorer(R) when access to a prohibited URL is attempted, Internet Explorer(R) will be forced to close.
If multiple tabs are open in Internet Explorer(R), only the tab that tried to access 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(R), 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.
- If you access an FTP server from Internet Explorer in an environment where Internet Explorer(R) 11 is installed, the FTP server connection prohibition feature will not operate.
- In Windows Vista(R) or later, when a user without administrator authority runs an application as the administrator and operates the FTP server connection prohibition feature, prohibition logs will not be recorded. In addition, no prohibition message will be displayed.

1.2.14 Web Upload and Download Operation Prohibition

- This function must be run in Windows(R) Internet Explorer(R) 7 or higher.
- File uploading and downloading through ActiveX and plug-in cannot be prohibited.
- When a file is opened and run directly in Internet Explorer(R), the Web upload and download prohibition function will run.
- When the Web page component displayed in Internet Explorer(R) is saved as image, the Web upload and download prohibition function will not be run.
- When the entire Web page displayed in Internet Explorer(R) 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(R) Internet Explorer(R) 9 or later is used, the blank page (about: blank) will be displayed under the following conditions. When the blank page is displayed, 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(R) Internet Explorer(R) 9 or later.
- In an OS later than Windows Vista(R), 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.
- In Windows(R) Internet Explorer(R) 11, you can specify host names or IP addresses as the allowed sites for the web upload prohibition feature and web download prohibition feature.
If you specify allowed sites that contain the URL, web upload and web download will not be allowed.

1.2.15 Clipboard Operation Prohibition

- Clipboard operation prohibition applies in the following cases:
 - When the remote desktop connection is used to establish a remote connection
 - When Citrix Receiver is used to connect to Citrix Xen App or Citrix Xen Desktop
 - When VMWare View Client or VMWare vSphere Client is used to connect to VMware (Horizon) View or VMware vSphere
- 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 halfwidth characters (1024 fullwidth characters). If the size is larger than 2048 bytes, the excess 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(R) 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(R) WORD or Microsoft(R) Excel is used in the virtual or physical environment, clipboard operations can be performed within the Microsoft(R) WORD or Microsoft(R) 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 Wi-Fi Connection Prohibition (Smart Device)

- If you select **Enable connection of registered access points** as the Wi-Fi connection prohibition policy, you must register at least one access point. Be sure to enter the correct BSSID of each access point to be registered. If you do not register any access point, or if you register an access point with an incorrect BSSID, the smart device may no longer be able to communicate with the server.

1.2.17 Application Usage Prohibition (Smart Device)

- This feature does not operate for widgets that are displayed in the home window.
- Use of applications for which a package name was registered is prohibited.

1.2.18 All Logs (for Clients (CT))

- 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(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012, 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(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012, 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.

1.2.19 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.

1.2.20 Printing Operation Log

- When a shared printer connects to the server defined as a Windows printing server in Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012 for printing, the name resolution of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 64-bit edition, or Windows Server(R) 2012 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(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 64-bit edition, or Windows Server(R) 2012 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(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 64-bit edition, or Windows Server(R) 2012. One of the two logs records the name of the PC that performs printing operation changes to the name of the printing server.
- 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.
- If you select **Monitor printing of local printer only** for **Set printing monitoring mode**, select **Yes** for the printing operation log in the CT policy settings window to obtain the printing operation log. Even if a user policy exists, the printing operation log will not be browsed.
 - In order to collect printing operation log, Port 139 must be opened. When a personal firewall is used, 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, 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(R) 7
 - Windows Vista(R)
 - Windows Server(R) 2008
 - Windows(R) 8
 - Windows Server(R) 2012
 - To collect the printing operation log that records the printing through a network printer, the **File and Printer Sharing for Microsoft Network** check box must be selected in the network connection properties of the Control Panel. When the computer has multiple LAN cards, check all the LAN cards that perform printing via network.
 - 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(R) Office Document Image Write and Adobe PDF) that does not print on paper will be recorded as print log.
- Operations of document writers that do not print on paper (such as Microsoft(R) Office Document Image Writer and Adobe PDF), may be recorded as print logs.
- A client (CT) can monitor up to 512 printers. If you have registered more than 512 printers, logs will not be obtained for printing operations at the excess printers.
- Sometimes printing operations are performed while multiple users (domain user and local user) are logged on under the same user name to a client (CT). In this case, the domain portion of the printing operation log may show the domain name (computer name) of the user who has not performed printing.

1.2.21 Window Title Obtaining Log

- A window title obtaining log is collected when a window becomes active.
- A log may not be collected if a window becomes active while the screen saver is running.
- 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(R) 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.

1.2.22 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, set each SMTP port number to the same one.
- The Web mail and groupware that do not use SMTP communication protocol cannot be monitored. However, when you send email from Microsoft(R) Outlook(R) 2007 or a later version of Outlook, email sending logs are collected even if the protocol is not SMTP (no logs are recorded for sending of items other than emails, such as those by the Microsoft(R) Outlook(R) Text Messaging feature (SMS) and FAX sending feature).
- When Microsoft(R) Outlook(R) 2003 or an earlier version of Outlook is being used and 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.
However, these restrictions do not apply when you send emails from Microsoft(R) Outlook(R) 2007 or a later version of Outlook.
- When Microsoft(R) Outlook(R) 2003 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, do not set **Auto select encoding for E-mail sending** in Microsoft(R) Outlook(R) 2003.
However, these restrictions do not apply when you send emails from Microsoft(R) Outlook(R) 2007 or a later version of Outlook.
- 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)
However, these restrictions do not apply when you send emails from Microsoft(R) Outlook(R) 2007 or a later version of Outlook.
- The maximum size of all information collected in E-mail sending logs is 2048 halfwidth characters (1024 fullwidth characters). If the information exceeds this size, information items will continue to be deleted in the sequence described below until the size is within 2048 halfwidth characters (1024 fullwidth characters).
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 halfwidth characters (50 fullwidth characters).
 2. The recipient address (Bcc) will be truncated to 500 halfwidth characters (250 fullwidth characters).
 3. The recipient address (Cc) will be truncated to 500 halfwidth characters (250 fullwidth characters).
 4. The recipient address (To) will be truncated to 500 halfwidth characters (250 fullwidth characters).
 5. The E-mail subject will be truncated to 100 halfwidth characters (50 fullwidth characters).
 6. The attachment name will be truncated to 300 halfwidth characters (150 fullwidth characters).
- An email address that does not conform to RFC-5321 may be cut off when it is recorded. The same applies to the address portion of the original storage email.
- 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.
However, when you send emails from Microsoft(R) Outlook(R) 2007 or a later version of Outlook, email sending logs can be collected immediately even if you do not restart the client (CT).
- 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.
- The Systemwalker Desktop Keeper add-on has been added in Microsoft(R) Outlook(R) 2007 and later versions of Outlook. Do not disable or delete this add-on, because doing so will cause Outlook to be terminated by force. If multiple users have logged on to the PC, Outlook may be terminated by force not just for the user who disabled or deleted the add-on but for all users.

- If you attach a file with a long name to an email in Microsoft(R) Outlook(R), the name of the attachment may be shortened when it is recorded. For example, when Microsoft(R) Outlook(R) attaches a file, it changes the file name portion (preceding the extension) so that the total number of characters including the extension is 255. Therefore, the maximum length of the file name to be recorded as the email sending log is also 255 characters (regardless of whether the characters are halfwidth or fullwidth). Microsoft(R) Outlook(R) 2013 shortens the names even further and sometimes appends "..." to the file name. When a file name is shortened in this way, the file cannot be traced.
- A maximum of 1023 characters (halfwidth and fullwidth) is recorded for each of the following: email attachment prohibition log, email sending log (sent after confirmation), email sending interruption log, warning address (or list of warning addresses if there are multiple applicable warning addresses), and attachment name (or list of attachment names if there are multiple names). Any portion beyond 1023 characters is discarded. In addition, if there are multiple attachments, one email attachment prohibition log is created per attachment. However, if the list of attachments exceeds 1023 characters, no logs will be recorded for the excess attachment names. Moreover, the last file name may be cut off when it is recorded.
- If you specify a sender other than the prescribed account when sending email from Microsoft(R) Outlook(R) 2007, the sender recorded in the email sending log is the email address of the prescribed account.

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.
- When you send emails from Microsoft(R) Outlook(R) 2007 or a later version of Outlook and you store the original email, the file extension when you retrieve the original email from Log Viewer will be msg. Microsoft(R) Outlook(R) must have been installed on the PC before you can view the original emails.
- Emails that you send from Microsoft(R) Outlook(R) 2007 or a later version of Outlook and whose original you stored are displayed in draft format.

Email sending log

- Unencrypted storage takes effect after it is set on Management Console. Emails that have already been stored remain encrypted. Even if you enable encryption, original emails that were stored without being encrypted remain unencrypted.

1.2.23 Command Operation Log

- A command log is collected only when **Command Prompt** is started in Windows. 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, even if you start **Command Prompt** in Windows, a command log will not be collected for the following:
 - 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 "x" button, the command log 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 log 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 log is collected, date and time will be inserted immediately before 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 sometimes not be inserted immediately before the input command depending on 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

```
--[2013/09/05 13:37:19]--

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

- If the command for displaying the window again is input, logs will be collected twice at one output. (Example: "append" command)
- If you start the command prompt from the Quick Access Menu in Windows(R) 8 or later, a command log cannot be collected.

1.2.24 Device Configuration Change Log

- When UAC is enabled in Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012, 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.
- When auto-mapping mounts a USB device in a virtual operating system, the USB device appears to be the network drive. In this case, you can control the USB device by using reading and writing prohibitions for the network drive. You cannot use the Individual Identification Function for control.
- To obtain device configuration change logs for a device that was mounted by auto-mapping, assign the device to a drive. In this case, the obtained server name and shared name may be blank.

Connecting a USB device in Xen Desktop 5.6 or later

In Xen Desktop 5.6 or later, recognition and operation of a USB device depend on how the device is connected.

Connection method	Identification by OS	Management Console	CT	
		USB device registration	Prohibition feature	Log retrieval feature
USB redirect	Removable Device	Can be registered as a USB device	Reading prohibition Removable: Y DVD/CD: - Network: N	File export log Y: (can obtain as removable)

Connection method	Identification by OS	Management Console	CT	
		USB device registration	Prohibition feature	Log retrieval feature
			Reading prohibition Removable: Y DVD/CD: - Network: N USB Device Individual Identification Function: Y	Device configuration change log Y: (can obtain as removable)
Auto-mapping	Network (*1, *2)	Cannot be registered	Reading prohibition Removable: N DVD/CD: - Network: Y Reading prohibition Removable: N DVD/CD: - Network: Y USB Device Individual Identification Function: N	File export log Y: (can obtain as network) Device configuration change log OS Can obtain by mounting auto-mapping drive to drive

Y: Operates normally, N: Cannot operate, -: Not an operation target, OS: Operation depends on the operating system

*1: A USB device is recognized as a network drive (\\serverName\sharedName).

*2: Operation depends on the operating system.

When the virtual operating system is Windows Vista(R) or later: Not mapped to the drive letter.

1.2.25 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.

1.2.26 Web Operation Log

- This function must be run in Windows(R) Internet Explorer(R) 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(R), 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(R) 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(R) 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.

1.2.27 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(R) 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.
- If you access an FTP server from Internet Explorer in an environment where Internet Explorer(R) 11 is installed, no FTP operation log will be obtained.
- In Windows Vista(R) or later, when a user without administrator authority runs Internet Explorer(R) as the administrator and operates the FTP operation log feature, the related operation logs will not be recorded.

1.2.28 Clipboard Operation Log

- A clipboard operation log is collected in the following cases:
 - When the remote desktop connection is used to establish a remote connection
 - When Citrix Receiver is used to connect to Citrix Xen App or Citrix Xen Desktop
 - When VMWare View Client or VMWare vSphere Client is used to connect to VMware (Horizon) View or VMware vSphere
- 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 halfwidth characters (1024 fullwidth characters). 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 Windows 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(R) 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(R) WORD or Microsoft(R) Excel is used in the virtual or physical environment, the clipboard operation can be performed within Microsoft(R) WORD or Microsoft(R) 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.

1.2.29 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(R) or Windows Explorer will not be collected.
- When the OS is Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012, 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 you use the TEMP or TMP user environment variable in Windows Explorer to create a file, "Create" logs will not be collected.
- When Excel file operation logs are collected, "View" logs are created even under the following conditions:
 - Excel containing a link to another sheet is reference, and
 - There is no link destination file
- When you use WordPad to update a docx file in Windows(R) 8 or Windows Server(R) 2012, an "Update" log may not be output.
- When you run the "Save as" operation, "Save as", "Create", and "Update" logs may be collected.

Notes on operations that generate a large volume of logs

- When you shut down or restart immediately after an operation that generates a large volume of logs (*1), some logs generated before the restart may not be collected.
When you perform such an operation, wait a while before performing shutdown processing.

- After an operation that generates a large volume of logs, Systemwalker Desktop Keeper processes may temporarily experience high load.

This is not an issue if the high load is temporary, but if it occurs periodically, take measures such as removing folders for which a large volume of logs are likely to be created.

*1: For example: Operations such as batch copy and deletion of folders that contain several tens of thousands of files

Regular file operations that use batch processing

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 "[8.2.19 File Operation Log](#)".
 - Windows Explorer
 - Notepad
 - Wordpad
 - Microsoft(R) Word (2003, 2007, 2010, and 2013)
 - Microsoft(R) Excel (2003, 2007, 2010, and 2013)
 - Microsoft(R) PowerPoint(R) (2003, 2007, 2010, and 2013)
 - Commands in the Command Prompt window (COPY, XCOPY, MOVE, DEL, ERASE, RD, REN and MD)

However, pay attention to the following items.

- The "Update" operations (such as Save As and Replace) of Microsoft(R) Word are collected as the log of **Create** operation.
- In Microsoft(R) Word, Excel, and PowerPoint, the "Create" operation may be collected as an "Update" log (Microsoft(R) Office 2013).
- Same as Windows Explorer and XCOPY, for a process registered in the **File operation**, 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 "[8.2.19 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 "Move" operation is performed in the above software or commands, "Copy" and "Create" (move source) logs may be collected.
- 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 halfwidth characters (129 fullwidth characters) 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(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012, 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 collected logs will be the "Update" log of the copy destination file or move destination file, the "Delete" log of the move source, and the "Rename" log of the copy source file and copy destination file, or the move source file and move destination file, if the same drive is used.
- Under virtual environment, the file name of physical drive of drive mapping may contain extra information sometime [\\Device\{PicaDriveRedirector}].
Example: [\\Client\F\$\Customer\CustomerInformation.xls] will be obtained as [\\Device\{PicaDriveRedirector}\Client\F\$\Customer\CustomerInformation.xls].
- In a virtual environment, when you operate a file from the command prompt, 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]
- In a virtualization environment, operation logs may not be obtained for files that have a size of 0 bytes.
- In a virtualization environment, superfluous "Create" logs may be obtained when you perform file operations.
- In a virtualization environment, folder operation logs may not be obtained.
- When you perform file operations in Microsoft(R) Office, operation logs may be obtained for the temporary files (such as .dll, .dat, and .lnk) that are created by the operating system.
- When you use Microsoft(R) PowerPoint and save all pages in an image format (such as jpg or tif), a separate image file is output for each page. However, a "Save as" log is recorded only for the page image file for which you specified the file name in the **Save as** dialog box. The file operation logs for the other pages are recorded as "Create" logs.
- When you operate (such as update or rename) a file after creating it, a "Create" log may not be output.

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**. 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.
- An operation log cannot be collected when you directly save data in Internet storage.

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 "8.2.19 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.
 - When you delete a file from the network drive (including access via a UNC path) in Windows(R) 8 or Windows Server(R) 2012, a "Delete" log may not be output.

When you move a file from the network drive (including the access time in a UNC path) in Windows(R) 8 or Windows Server(R) 2012, the "Move" log may be output as a "Copy" log.

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 halfwidth characters (130 fullwidth characters), the exclusion setting will be invalid and the file operation log will be collected.
 - However, if the path is 260 halfwidth characters (130 fullwidth characters) and the 260th character is "\", the setting will be valid.
- When the path of excluded target in Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, or Windows Server(R) 2012 contains dedicated Unicode characters, it will not become the target for exclusion.

1.2.30 Logon/Logoff Log

- The logoff 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(R) or Windows(R) 7, the logoff logs of all logon users at the time when power of a PC is cut off by force will be recorded.
- When you perform shutdown before logging on while the fast startup feature is enabled in Windows(R) 8, a PC suspension log rather than a PC shutdown log may be obtained. In addition, the next time that the operating system is started, a PC recovery log rather than a PC startup log may be obtained. The transfer target information file and CT operation parameter information file update operations, the CT policy request operation, and the self version upgrade check that are normally performed when a PC starts may not work. To ensure that these operations are performed properly, restart the operating system instead of shutting down.
- When our unique feature is used to monitor increases in the number of sessions, a session increase triggers the creation of a logon log. This log is not created in conjunction with the security auditing log in the event log.

- The only trigger (operation) for creation of the logon and logoff logs is an interactive logon operation to Windows.

1.2.31 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.

1.2.32 Web Access Log (Smart Device)

- This feature does not operate in any web browser other than the standard Android browser (Android Browser). Therefore, operation should preferably also use such features as application usage prohibition to ensure that a browser other than the standard Android browser cannot be used.
- If you delete the standard Android browser (Android Browser), you cannot obtain an access history up to the time of deletion. Therefore, operation should preferably also use such features as application usage prohibition so that a tool that can delete the web access history cannot be used.
- If you perform page operations for which no access history is added, such as tapping the back or forward button in the standard Android browser (Android Browser), no logs will be obtained.

1.2.33 Wi-Fi Connection Log (Smart Device)

- At operation of an application that changes the Wi-Fi connection status, such as applications that automatically determine the connection status and automatically switch the connection to the Wi-Fi access point, a Wi-Fi connection log may be recorded at unexpected timing.
- A log is not obtained at disconnection.

1.2.34 Application Usage Log (Smart Device)

- This feature does not operate for widgets that are displayed in the home window.
- If application usage logs are to be collected and you run multiple applications within a short period, logs may be collected only for the application that you used last.
- Home app (window that is displayed when you click the home button) logs are not obtained.
- If you start a specific application, return to the home app, and then start the same application again, logs will not be obtained. In this case, the number of logs is just the one log for that application.

1.2.35 Application Configuration Change Log (Smart Device)

- An application configuration change log is not recorded when you uninstall a smart device (agent) (Android).
- An uninstallation log may be obtained when you update a smart device (agent) (Android).

1.2.36 Incoming/Outgoing Calls Log (Smart Device)

- This feature does not operate outside the standard Android telephone applications and telephone directory applications (such as Skype and Line).
- Operation should preferably also use application usage prohibition so that telephone applications other than the standard Android telephone applications and telephone directory applications cannot be used.
- This feature does not support simultaneous communication on multiple lines as provided by, for example, call waiting and multi-way calling.

1.2.37 Bluetooth Connection Log (Smart Device)

- A log is collected when pairing with a Bluetooth device is completed.

1.2.38 Bluetooth Connection Prohibition (Smart Device)

- This feature prohibits pairing with a Bluetooth device and forcibly cancels pairing with a device that has already been paired.

1.2.39 SIM Card Mount/Unmount Log (Smart Device)

- When you add or change a SIM card, a log of the device model number, issue date, telephone number, model number, SIM card mount/unmount status, and serial number is obtained.
- When you delete a SIM card, no serial number log is obtained.

1.2.40 SD Card Mount/Unmount Log (Smart Device)

- When you add or change an SD card, a log of the device model number, issue date, telephone number, model number, total capacity, and used capacity is obtained.
- When you delete an SD card, no total capacity or used capacity log is obtained.
- Due to restrictions of the Android operating system, the total capacity and used capacity obtained for the SD card mount log may relate to internal storage and not for external storage (SD card).

1.2.41 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.

1.2.42 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 with certain software products or commands, 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. 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 Windows 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.

1.2.43 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, 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.

1.2.44 Administrator Notification Feature

- The administrator is not notified when a prohibited operation is detected on a smart device (agent), or a change to smart device (agent) information is detected.
- You must set the email subject on each Management Server.

1.2.45 IPv6 Support

Descriptions and notes specific to the IPv6 format are as follows:

- IPv6 states that address values should be separated into 16-bit portions with a colon (:) and written in hexadecimal notation.

Example: 2001:0db8:0000:0000:0000:0000:9abc

- The notation can be abbreviated.

Example: 2001:0db8:0000:0000:0000:0000:9abc = 2001:db8::9abc

- Special notation (loopback address)

Example:

- IPv4: 127.0.0.1

- IPv6: 0::1 and ::1

- URL notation (addresses enclosed in square brackets "[]" can be accessed)

Example: `http://[2001:218:2001:3000::181]/`

- IPv6 address shared folder specification

When specifying a shared folder, change ":" to "-" and append ".ipv6-literal.net".

Example: `\\2001-db8--1.ipv6-literal.net\shared`

You can also use an abbreviated RFC 5952-compliant format.



Note

- When using IPv6 to communicate with Log Analyzer Server, you must specify a resolvable host name and not an IPv6 address.
- Do not use link-local addresses. Behavior is not guaranteed if link-local addresses are used.
- You cannot use IPv4-mapped addresses.

1.2.46 Windows Store Apps in Windows(R) 8 or Windows Server(R) 2012 or Later

The following recording and prohibition features of the client (CT) do not operate in Windows Store apps for Windows(R) 8 or Windows Server(R) 2012 or later:

Recording features

- Web upload log
- FTP operation (upload/download)
- Clipboard operation log
- Printed page count

Use the policy to configure collection of the application startup log, application termination log, and window title obtaining log as backup operations for restricted features.

Refer to "[2.4.1.1 Log Collection Operation \(Windows\)](#)" for details on how to set the policy.

Prohibition features

- Print prohibition
- FTP server connection prohibition
- Web upload prohibition
- Clipboard operation prohibition

Use the policy to set Windows Store apps in the startup prohibition application as backup operations for restricted features.

Refer to "[2.4.1.7 Application](#)" for details on how to set the policy.

- Application startup prohibition can be set per process. Therefore, if a common process will run multiple applications, such as Windows Store apps, you cannot set startup prohibition per application. You can prohibit startup of all Windows Store apps by setting startup prohibition for the common process.
- The application startup log and application termination log are obtained per process. Therefore, if a common process will run multiple applications, such as Windows Store apps, you cannot identify the application from the startup log and termination log. Also use the window title obtaining log to identify the application.
- The application termination log is obtained per process. Depending on how a Windows Store app is terminated, only the window may close, without the process terminating. In this case, the application termination log will not be obtained because the application is running in the background.

1.2.47 Dialog Boxes in Windows(R) 8 and Windows Server(R) 2012 or Later

If, while the Start window is displayed, a Windows Store app starts and is displayed in the foreground, message dialog boxes for previously opened desktop applications will be displayed in the background. Similarly, the self version upgrade dialog box and the operation prohibition dialog boxes on a client (CT) may thus also be hidden behind the Start window or a Windows Store app.

1.2.48 Portable Device and Imaging Device Control

- A portable device or imaging device is a device that the Windows operating system displays as such in Device Manager. Typical examples include digital cameras, IC recorders, and image scanners.
- If you prohibit the connection of portable devices and imaging devices, you can connect only USB-connected devices. Connection of all devices that use the IEEE1394 interface or other means for connection is prohibited. Even devices that connect via USB may not be allowed to connect if they incorporate multiple functions, as exemplified by multifunction printers. Some smart phones and other devices are multifunctional composite devices and their connection may not be allowed.
You can check if connection of a device is allowed by viewing the USB device logon window on Management Console and verifying if the device is recognized as WPD or is actually allowed in the policy settings.
- If you uninstall a client (CT) while the connection of portable devices and imaging devices remains prohibited in the policy settings, the connection state may continue to show that connection is prohibited. In this case, connect the device and then select **Enable** in Device Manager.

1.2.49 Log Viewing Database

- When Management Servers are in a 3-level structure and you perform a log search on both the Master Management Server and a downstream Management Server, restore the management information of the Master Management Server in the Log Viewing Database. Restore log data by restoring the log information that was separately obtained by the Master Management Server and the downstream Management Server.
- Log information and administrator information obtained in older versions can also be browsed by restoring it to the Log Viewing Database.
- When restoring log information backed up on a Master Management Server in a 3-level structure to the Log Viewing Database, the Master Management Server IP address that is displayed in the CT operation log window becomes the Management Server IP address used when building the Log Viewing Database. Also, the downstream Management Server IP address will be displayed as "0.0.0.0".
- When restoring log information backed up on a downstream Management Server in a 3-level structure or Management Server in a 2-level structure to the Log Viewing Database, the Management Server IP address that is displayed in the CT operation log window becomes the Management Server IP address used when building the Log Viewing Database.
- The department administrator can also browse the Log Viewing Database. The groups that can be browsed in the Log Viewing Database are displayed in accordance with the department administrator permission settings that were registered in the restored management information.
- Before browsing the configuration change log of a downstream Management Server in a 3-level structure, restore the downstream Management Server management information to be browsed. In this case, the configuration change log, CT operation log, and user operation log search only the information in the downstream Management Server.

1.2.50 User Operation Log Search Feature

- A search of the user operation log is performed on the Log Viewing Database. Therefore, restore management information and log information to the Log Viewing Database before performing the search.
- The user operation log is easier to search if you create a user policy definition and user layer configuration. Another approach is to use the Link with Active Directory feature and Link with Systemwalker Desktop Patrol feature to define a user policy and user layer configuration.
- When Management Servers are in a 3-level structure, centrally manage user information on the Master Management Server. In addition, restore Master Management Server management information in the Log Viewing Database.
- Assume that you have an environment where Management Servers are in a 3-level structure and a user policy is created on each Management Server. In this case, even if you restore the Master Management Server management information, a large volume of user

information that has been logged by downstream Management Servers will be displayed for the **Other users** group in the user operation log search window.

- If you delete client (CT) information from management information, you cannot search for operation logs for that client (CT) even in the user operation log. But you can search for clients (CTs) in the **Deleted CT** group, even if the settings are configured to not display deleted clients (CTs).
- If you select a user to be searched for and no user name or domain name has been recorded for that user in the log, a halfwidth single-byte space will be displayed as the user name. In this case, clicking that space will enable you to search the logs of a user for whom no user name has been recorded.
- If you perform a file trace when searching the user operation log, you can search only the operation logs in clients (CTs) that have recorded the trace source logs. You cannot perform a file trace across multiple clients (CTs).
- There is no feature for searching or displaying the operation logs for such operations as setting the policy in the **User Policy Settings** window on Management Console or performing searches in the Log Viewing Database in Log Viewer.
- Even if the department tree pane in the user operation log search window shows violation logs for that department and client (CT), the department name and client (CT) name are not displayed in red.

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) and smart device (agent) 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 smart device (agent) and collecting logs, the following three operation policies must be determined and the determined contents should be set in Systemwalker Desktop Keeper. Note that if you are using a personal smart device for business use, the following three operation policies must be determined for the personal device and company-owned device respectively.

- Determine the allowed operations, unallowed (prohibited) operations and log collection operations when the PC and smart device are being used.

The determined contents will be set as "Terminal Initial Settings".

If you are using a personal smart device for business use, determine allowed operations, unallowed (prohibited) operations, and log collection operations for the personal device and company-owned device respectively. Only one set of settings can be configured for **Terminal Initial Settings**, so configure these settings for either the company-owned device or the personal device.

- For a PC, determine how to send the saved logs to the server.

The determined contents will be set as "Terminal Operation Settings".

The company-owned device and the personal device must use the same settings because only one set of settings can be configured for **Terminal Operation Settings**.

- Determine how to manage PC, PC users (Users), and smart devices in the Group.

The managed group will be set as configuration information tree. (User group cannot manage the smart device.)

Group smart devices by "company-owned" and "personal", and set the policies for company-owned devices and personal devices respectively.

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 and smart device (Android device and iOS device) are being used.

Contents can be set in policy.

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

Setting Prohibited Operations (PC)

The operations that can be prohibited by installing the client (CT) on the PC include those shown below. These policies are set in the Management Console by the system administrator or department administrator.

- File Export Prohibition

File and folder export in drive, network drive, removable drive or DVD/CD can be prohibited conditionally.

According to the set condition, "File Export Utility" can be used to export files and folders from the prohibited drive.

Refer to *Systemwalker Desktop Keeper User's Guide for Client* for "File Export Utility".

- Reading Prohibition

Reading of data on the removable drive, network drive or DVD/CD can be prohibited.

- Printing Prohibition

Printing by non-specified applications can be prohibited.

- PrintScreen Key Prohibition

The use of PrintScreen key for collecting the hard copy of screen 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

Logon with the user name that belongs to a set group can be prohibited. The groups that can be prohibited are as follows:

- Microsoft account

- Application Startup Prohibition

Startup of the specified applications can be prohibited.

- URL Access Prohibition

Access to the unauthorized URL can be prohibited.

- FTP Server Connection Prohibition

Connection to the non-specified FTP server can be prohibited.

- Web Upload and Download Prohibition

Upload and download to and from unauthorized websites can be prohibited.

- Clipboard Operation Prohibition

Information transfer from the virtual environment to the physical environment or from the physical environment to the virtual environment via clipboard can be prohibited.

Setting Log Collection Operation (PC)

The operations that can collect logs by installing the client (CT) on the PC include those shown below. These policies are set in the Management Console by the system administrator or department administrator.

- Application startup log
- Application termination log
- Application startup prohibition log
- Window title obtaining log
- E-mail sending log
- 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
- Linkage log

Setting operations to be prohibited (Android device)

The operations that can be prohibited by installing the smart device (agent) (Android) on the Android device include those shown below. These policies are set in the Management Console by the system administrator or department administrator.

- **Wi-Fi connection prohibition**
Connection to the Wi-Fi access point set as a policy can be allowed or prohibited.
- **Bluetooth connection prohibition**
Pairing with the Bluetooth device set as a policy can be allowed or prohibited.
- **Application usage prohibition**
Use of application set as a policy can be allowed or prohibited.

Setting operations to collect logs (Android device)

The operations that can collect logs by installing the smart device (agent) (Android) on the Android device include those shown below. These policies are set in the Management Console by the system administrator or department administrator.

- **Wi-Fi connection log**
- **Bluetooth connection log**
- **Application usage log**
- **Web access log**
- **SD card mount/unmount log**
- **SIM card mount/unmount log**
- **Incoming/outgoing calls log**
- **Application configuration change log**

Setting operations to be prohibited (iOS device)

The operations that can be prohibited by installing the smart device (agent) (iOS) on the iOS device include those shown below. These policies are set in the Management Console by the system administrator or department administrator.

- Device feature usage
Device feature usage, such as use of camera, screen capture, and Siri, set as a policy can be allowed or prohibited.
- Application usage
Use of application such as YouTube, iTunes Store, and Safari set as a policy can be allowed or prohibited.
- iCloud usage
iCloud usage such as backup to iCloud and document sync set as a policy can be allowed or prohibited.
- Security and privacy settings
Data transfer to Apple, forced encryption backup and similar can be set as a policy.
- Content ratings settings
Viewing of contents (movies, TV programs, Apps) can be set as a policy.

Policy Settings Targets

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

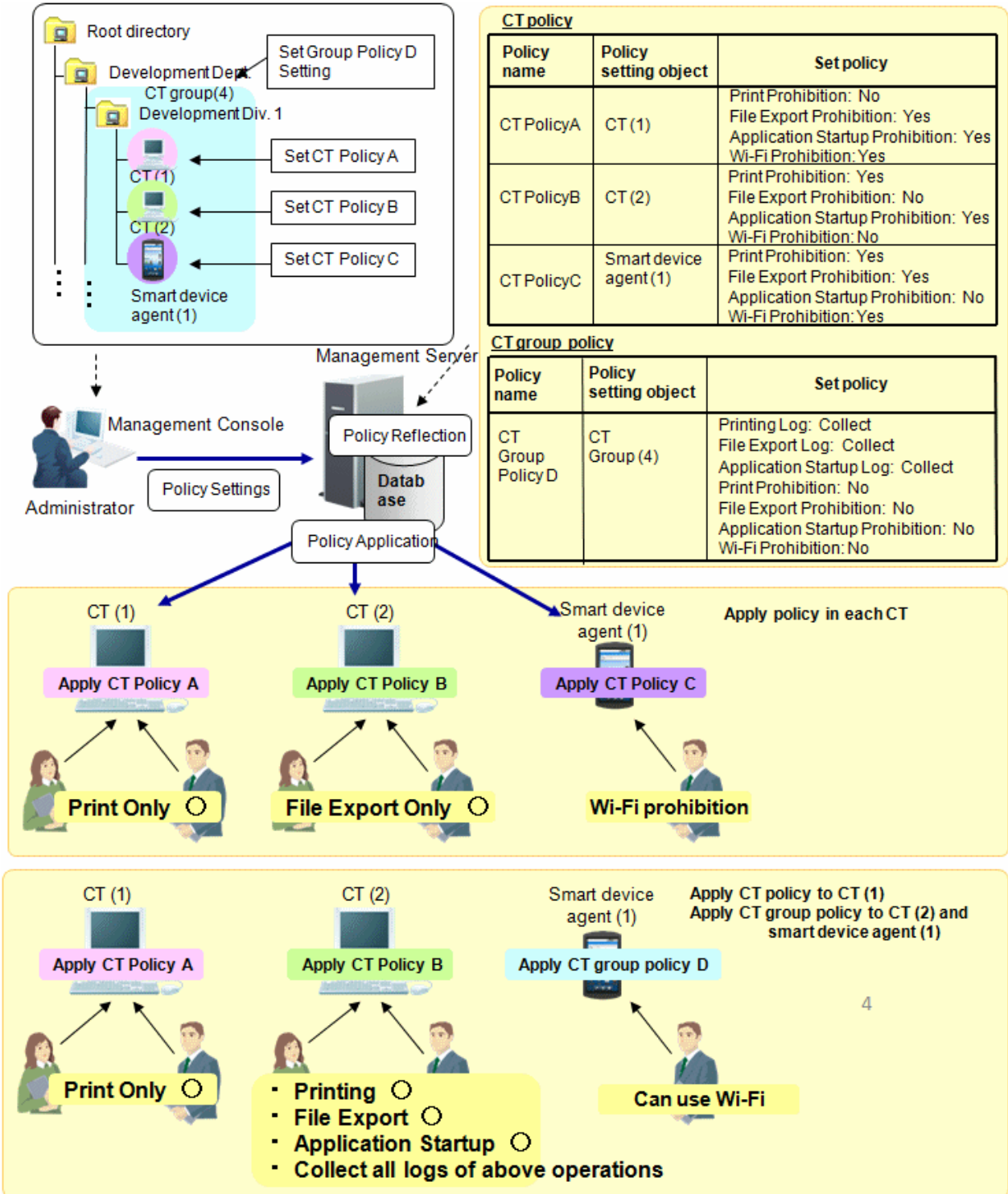
The policy set for the "client (CT)" and "smart device (agent)" is called "CT policy".

When setting policy for the "User", it is called "User Policy". The "user policy" cannot be set for the "smart device (agent)".

Settings for Client (CT) and smart device (agent)

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

In addition, the clients (CTs) and smart devices (agents) can be grouped by department or purpose, and the policy set for the group is called a 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), smart device (agent), and CT group through the Management Console.

The following policies can be set for each client (CT) and smart device (agent).

Settings for both the client (CT) (such as print prohibition and file export prohibition) and smart device (agent) (such as Wi-Fi prohibition and Bluetooth connection prohibition) can be configured for one CT policy.

If the CT policy is applied to the client (CT), the settings for the client (CT) will be enabled, and likewise if the CT policy is applied to the smart device (agent), the settings for the smart device (agent) will be enabled.

- CT (1) Printing only.

Printing prohibition: No (Enabled)
File export prohibition: Yes (Enabled)
Application startup prohibition: Yes (Enabled)
Wi-Fi connection prohibition: Yes (Disabled)

- CT (2) File export only.

Printing prohibition: Yes (Enabled)
File export prohibition: No (Enabled)
Application startup prohibition: Yes (Enabled)
Wi-Fi connection prohibition: No (Disabled)

- Wi-Fi cannot be used on the smart device (1).

Application usage prohibition: No (Disabled)
Wi-Fi connection prohibition: Yes (Enabled)

Group the clients (CTs) and smart devices (agents) and set the group policy to allow printing, file export, and application startup, and also collect all the logs.

CT policy will be applied to each client and smart device (agent) immediately or at the next startup. After policy has been applied, the client (CT) and smart device (agent) 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.
- Wi-Fi usage is prohibited on the smart device agent (1).

When the CT policy is applied to CT (1), and the CT group policy is applied to CT (2) and smart agent (1)

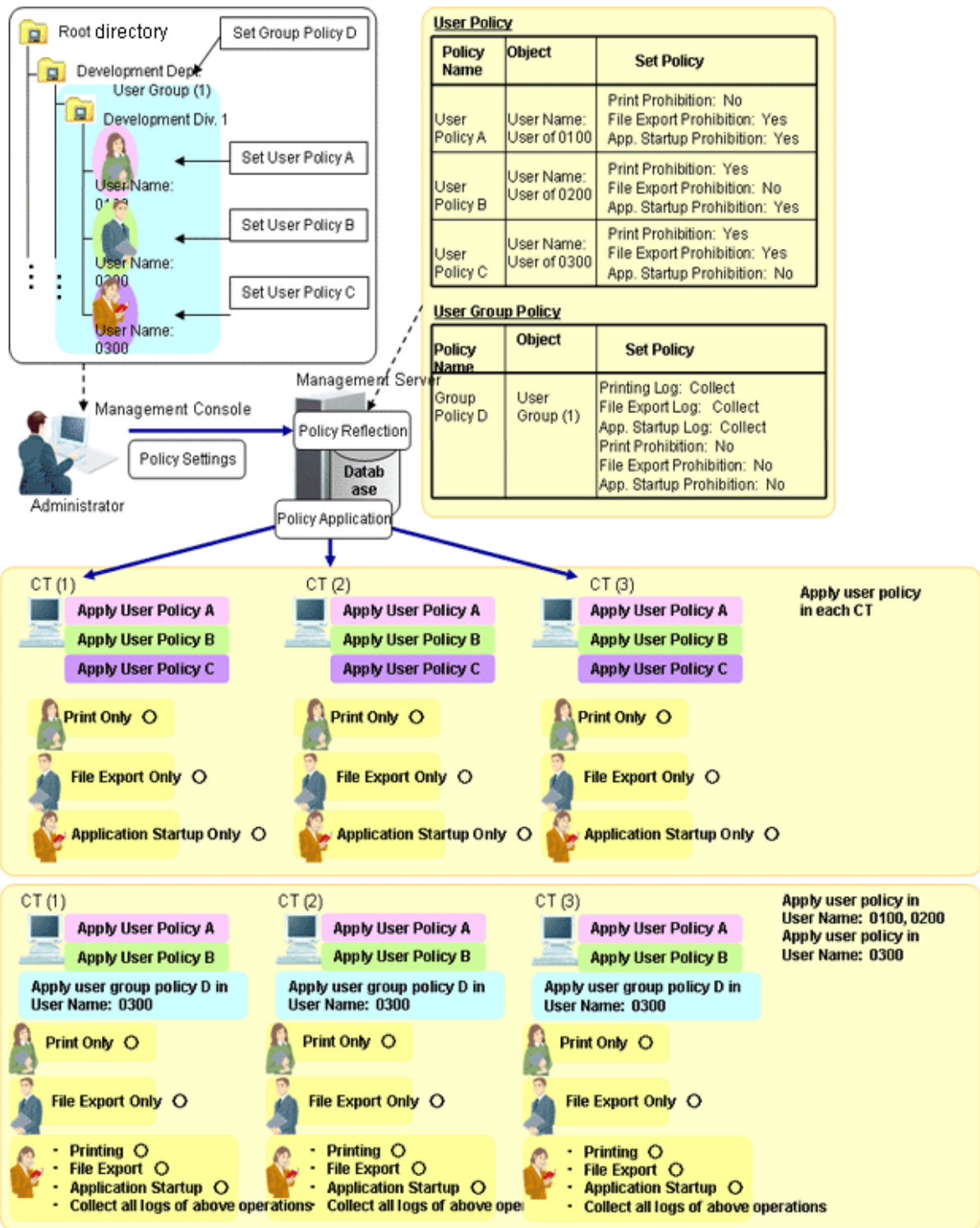
- CT (1) No matter who operates, only printing is allowed .
- CT (2) No matter who operates, printing, file export, application startup can be performed, and the logs of each operation will be collected.
- Wi-Fi usage is allowed on the smart device agent (1).

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.

Note that the user policy and user group policy cannot be set for the smart device (agent).



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
		Client (CT)	Smart device (agent) (Android)	Smart device (agent) (iOS)	Client (CT)
Prohibition Function	File export prohibition	Y	N	N	Y
	Reading prohibition	Y	N	N	Y
	Printing prohibition	Y	N	N	Y
	PrintScreen key prohibition	Y	N	N	Y
	Logon prohibition	Y	N	N	N (Note)
	Application startup prohibition	Y	N	N	Y
	E-mail attachment prohibition	Y	N	N	Y
	URL access prohibition	Y	N	N	Y
	FTP server connection prohibition	Y	N	N	Y
	Web upload and download prohibition	Y	N	N	Y
	Clipboard operation prohibition	Y	N	N	Y
	Wi-Fi connection prohibition	N	Y	N	N

Settings Items		CT Policy			User Policy
		Client (CT)	Smart device (agent) (Android)	Smart device (agent) (iOS)	Client (CT)
	Bluetooth connection prohibition	N	Y	N	N
	Application usage prohibition	N	Y	N	N
	Device feature usage	N	N	Y	N
	Application usage	N	N	Y	N
	iCloud usage	N	N	Y	N
	Security and privacy settings	N	N	Y	N
	Content ratings settings	N	N	Y	N
Record Function	Application startup log	Y	N	N	Y
	Application termination log	Y	N	N	Y
	Application startup prohibition log	Y	N	N	Y
	Window title obtaining log	Y	N	N	Y
	E-mail sending log	Y	N	N	Y
	E-mail sending interruption log	Y	N	N	Y
	E-mail attachment prohibition log	Y	N	N	Y
	Command log	Y	N	N	Y
	Device configuration change log	Y	N	N	Y
	Printing operation log	Y	N	N	Y
	Printing prohibition log	Y	N	N	Y
	Logon prohibition log	Y	N	N	N (Note)
	File export log	Y	N	N	Y
	PrintScreen key operation log	Y	N	N	Y
	PrintScreen key prohibition log	Y	N	N	Y
	Web operation log	Y	N	N	Y
	Web operation prohibition log	Y	N	N	Y
	FTP operation log	Y	N	N	Y
	FTP operation prohibition log	Y	N	N	Y
	Clipboard operation	Y	N	N	Y
	Clipboard operation prohibition log	Y	N	N	Y
	File operation log	Y	N	N	N (Note)
	Logon/Logoff log	Y	N	N	N (Note)
	Linkage log	Y	N	N	N (Note)
	Screen capture	Y	N	N	Y
	Wi-Fi connection log	N	Y	N	N
Wi-Fi connection prohibition log	N	Y	N	N	
Bluetooth connection log	N	Y	N	N	

Settings Items		CT Policy			User Policy
		Client (CT)	Smart device (agent) (Android)	Smart device (agent) (iOS)	Client (CT)
	Bluetooth connection prohibition log	N	Y	N	N
	Application usage log	N	Y	N	N
	Application usage prohibition log	N	Y	N	N
	Web access log	N	Y	N	N
	SD card mount/unmount log	N	Y	N	N
	SIM card mount/unmount log	N	Y	N	N
	Incoming/outgoing calls log	N	Y	N	N
	Application configuration change log	N	Y	N	N

Y: can be set

N: 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

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. 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	
		At normal startup (Logon to Windows after OS has started)	When starting in safe mode or the safe mode with network (Note 2) (Note 3)
OS Startup Mode			Windows Vista(R) Windows(R) 7 Windows Server(R) 2008 Windows(R) 8 Windows Server(R) 2012
Prohibition Function	File export prohibition	Y	Y
	Printing prohibition	Y	N
	PrintScreen key prohibition	Y	Y
	Logon prohibition	Y	Y
	Application startup prohibition	Y	Y
	E-mail attachment prohibition	Y	N
	URL access prohibition	Y	Y
	FTP server connection prohibition	Y	Y
Web upload and download prohibition	Y	Y	

Form of operation		When recording the operations of the client (CT) of Systemwalker Desktop Keeper	
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 2) (Note 3)
			Windows Vista(R) Windows(R) 7 Windows Server(R) 2008 Windows(R) 8 Windows Server(R) 2012
	Clipboard prohibition	Y	Y
Record Function	Application startup log	Y	Y
	Application termination log	Y	Y
	Application startup prohibition log	Y	Y
	Window title obtaining log	Y	Y
	Window title obtaining log (with URL)	Y	Y
	E-mail sending log	Y	N
	E-mail sending interruption log	Y	Y
	E-mail attachment prohibition log	Y	N
	Command log	Y	Y
	Device configuration change log	Y	Y
	Printing operation log	Y	N
	Printing prohibition log	Y	N
	Logon prohibition log	Y	Y
	File export log	Y	Y
	PrintScreen key operation log	Y	Y
	PrintScreen key prohibition log	Y	Y
	Web operation log	Y	Y
	Web upload prohibition log	Y	Y
	Web download prohibition log	Y	Y
	FTP operation log	Y	Y
	FTP operation prohibition log	Y	Y
	Clipboard operation log	Y	Y
	Clipboard operation prohibition log	Y	Y
	File operation log	Y	Y
	Logon/Logoff log	Y	Y (Note 1)
	Linkage log	Y	Y
Screen capture	Y	Y	

Y: Valid

N: Invalid.

Note 1: PC sleep logs and PC restoration logs are not collected.

Note 2: 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 3: 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.

Setting policy on personal devices

For personal devices for business use, protection of the owner's privacy and business data integrity must both be achieved. Determine the policy based on the example shown below:

1. Do not retrieve the operation logs

From the perspective of privacy protection, retrieval of the operation logs from personal devices should be avoided.

Ensure that the operation logs are "not retrieved" for the settings on personal devices.

2. Avoid unnecessary prohibition settings

Personal devices can be used for private use also, and therefore care should be taken for setting prohibition features.

Set prohibition features carefully so that the devices in private use will not be affected.

3. Manage applications to be used for business

Use the feature to prohibit application usage outside business hours to restrict the business application usage on personal devices to within business hours only. By prohibiting the use of business applications during private time, information leakage can be prevented.

4. Prohibit the use of applications that trigger off information leakage

Create a blacklist of applications which clearly should not be used (because they may trigger information leakage) on personal devices also, and prohibit the use of such applications. By prohibiting the use of applications on devices that can also be used for business, information leakage can be prevented.

Note that, for Android devices on which Systemwalker Desktop Patrol V15.1 or later is installed, personal devices can be identified as such by referring to Systemwalker Desktop Patrol. Refer to the *Systemwalker Desktop Patrol Operation Guide: for Administrators* for details.

2.1.2 How to Apply Policy

Timing for Policy Update

The timing for policy updates is as follows:

- CT Policy

Client (CT)

- When connection is established with the Master Management Server or Management Server for the first time after the client (CT) operating system is started
- 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.

Smart device (agent)

- When **Sync now** is selected on the smart device (agent)
- When the smart device (agent) is started
(When **Synchronize when starting up** is selected in the smart device (agent) settings window)
- When automatic synchronization with the Management Server is executed (once per day between 12:00 and 13:00)

- User Policy

Client (CT)

- 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.

Smart device (agent)

The user policy cannot be applied to the smart device (agent).

Point

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 every day.

In a situation where the client (CT) and Management Server are offline, and a user to whom the user policy is set is logged on, the user policy previously applied to the CT will be applied. For the CT to which the user policy of the logged-on user has never been applied, the CT policy will be applied.

Policy Change

The situation determines which policy will be valid for which operation that is performed by the system administrator (department administrator), client (CT), and smart device (agent) user.

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

To confirm the set policies, start the Management Console.

After the CT group to which the client (CT) and smart device (agent) to be confirmed belong has been selected in the CT group tree, if the client (CT) and smart device (agent) are selected from the CT list, the CT policy will be displayed in the policy list.

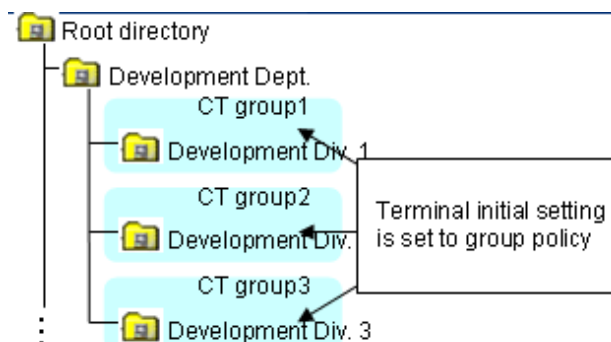
Select the **User Policy Settings** from the **User Settings** menu. After the user group to which the user expected to be confirmed belongs has been selected from in the displayed window, if a user is selected from the user list, the user policy will be displayed in the policy list.

Relationship between CT Group Policy and CT Policy

1. Create a group.

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

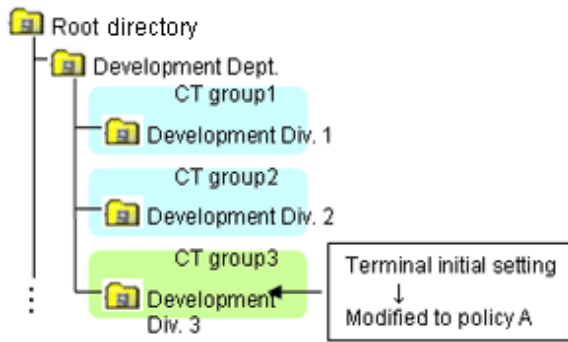
But in case of a three-level structure, when creating a CT group in the subordinate Management Server under the Master Management Server by connecting to the Master Management Server, the policy that has been set in the Master Management Server will be set for this CT group.



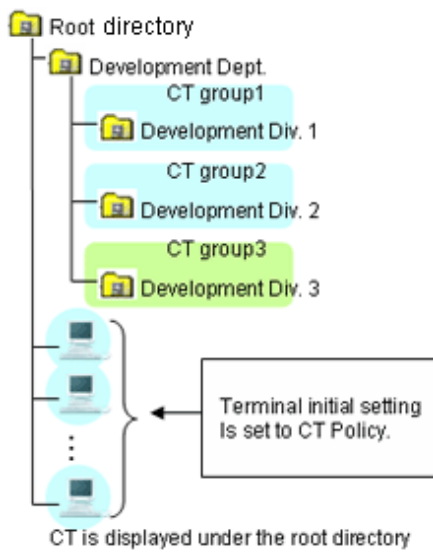
2. Modify the group policy as needed.

The group policy will be modified as follows:

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

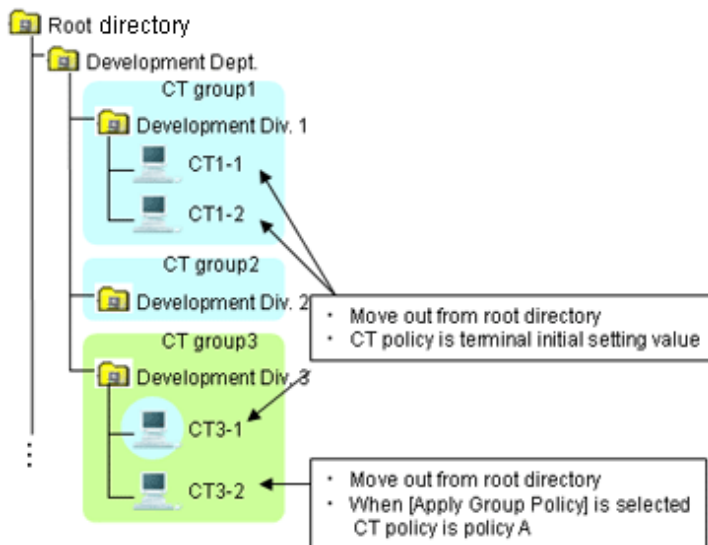


3. After the CT is installed and the client (CT) has communicated with the Management Server, the terminal initial settings value will be set as CT policy.



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

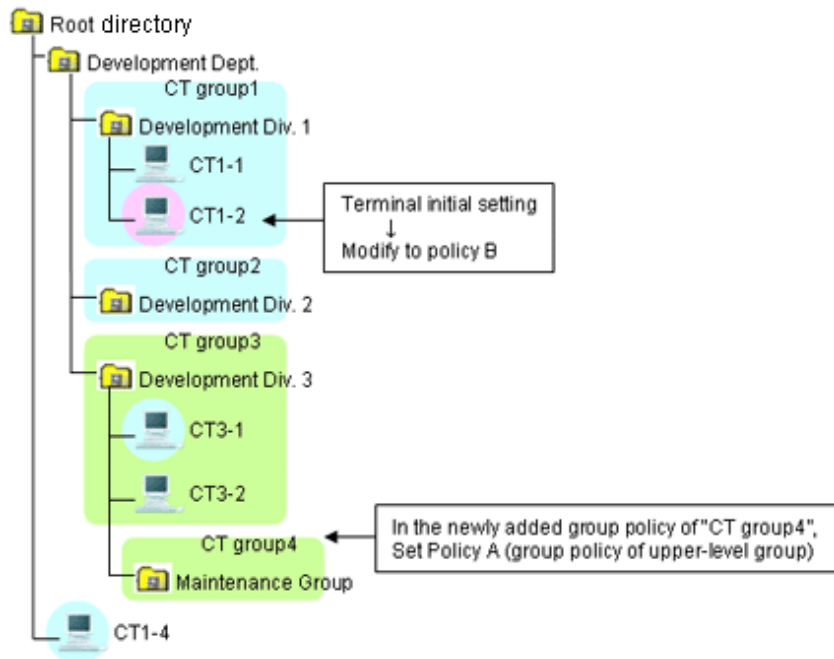
In the CT policy of the client (CT) that is directly moved out from the Root directory, the value of terminal initial settings is set. In the policy of the client (CT) for which "Apply Group Policy" check box is selected, the group policy of moving destination will be set.



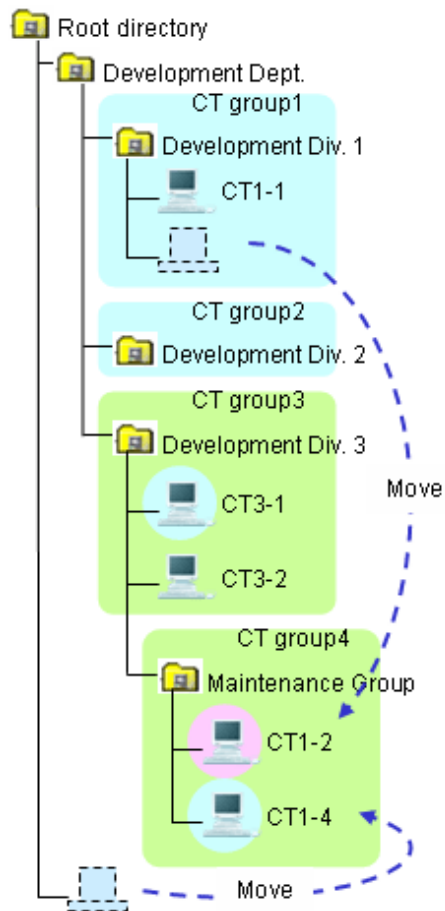
5. Create a sub-group.

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".

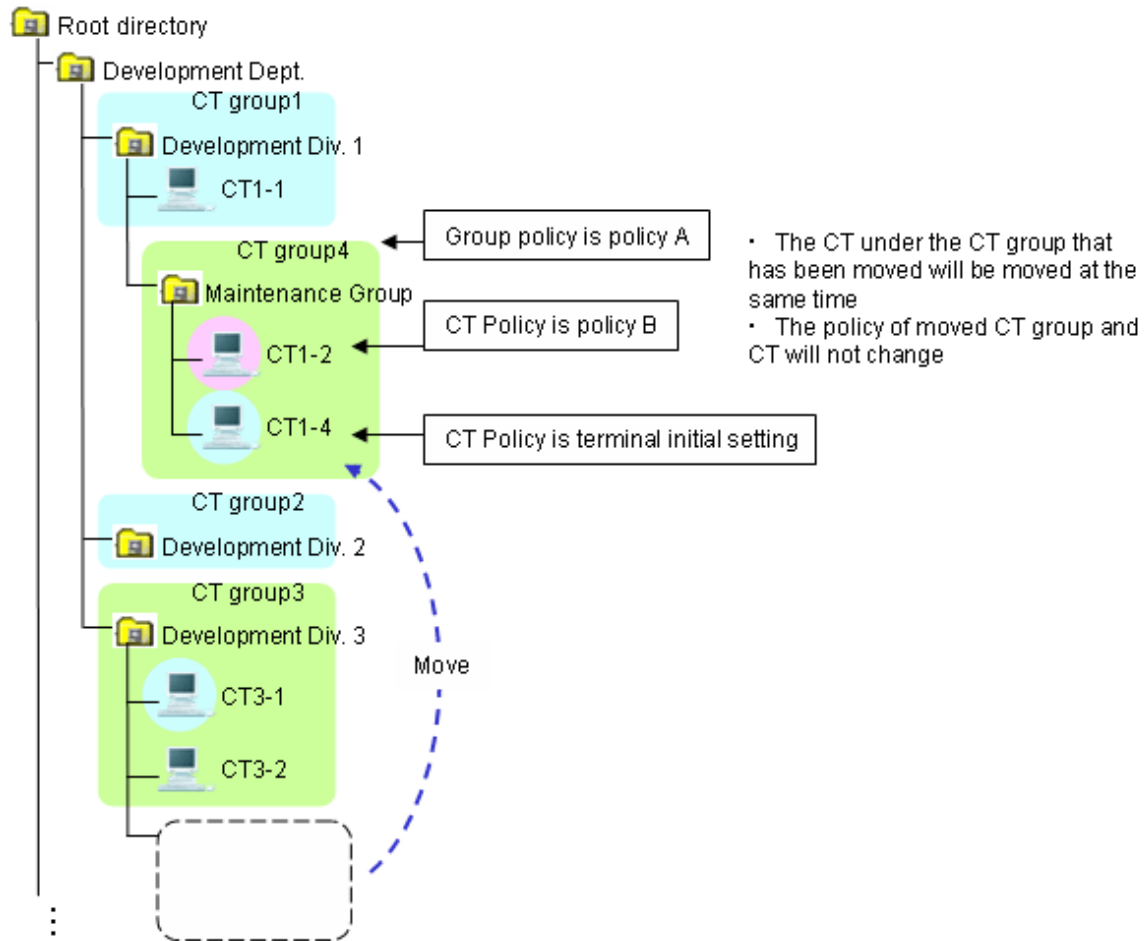


6. Move a CT.



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" check box 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 user policy will not be applied to the smart device (agent).)

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.

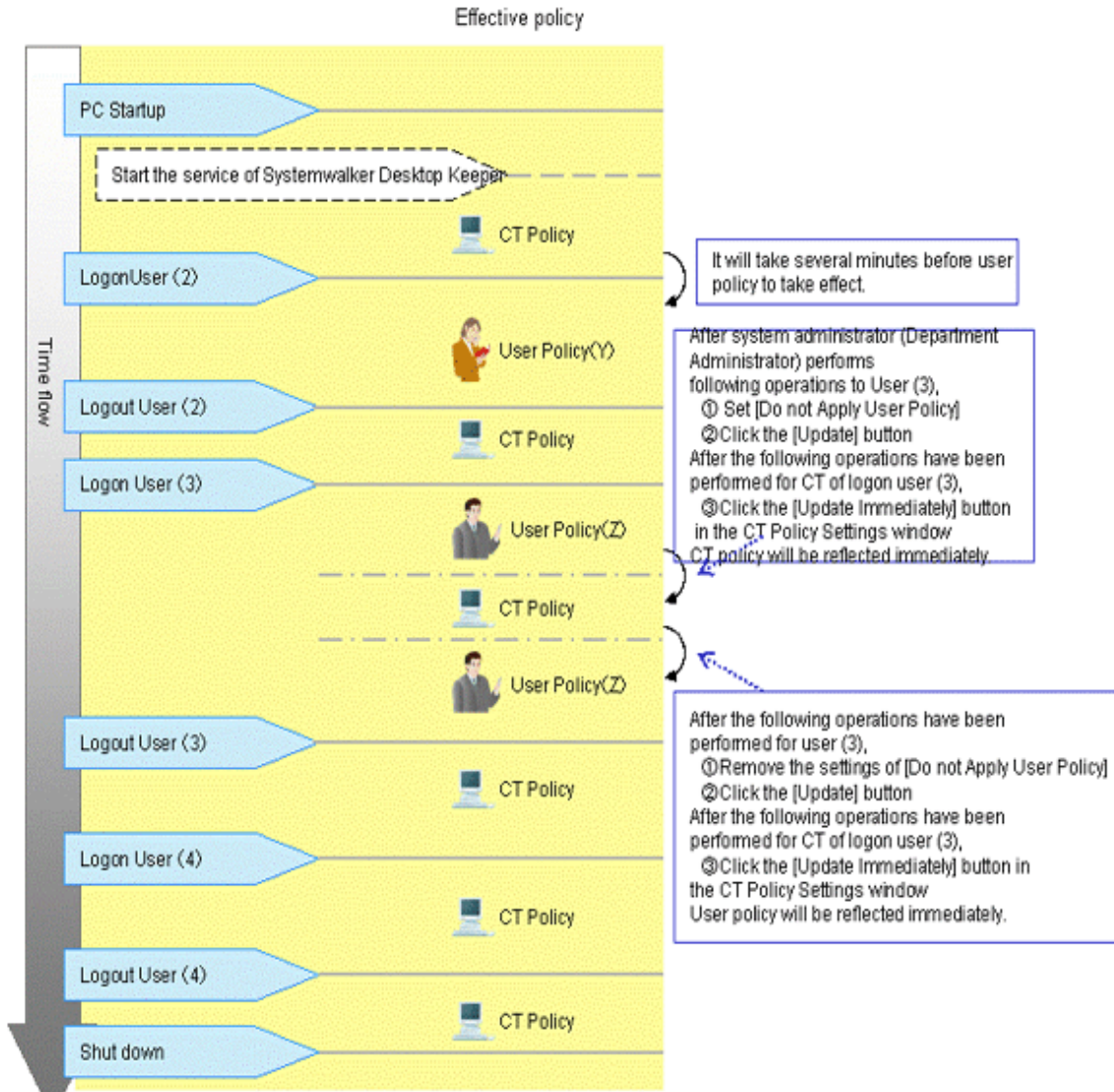
Select three users out of the five from "User (1) to User (5)" to register to the Management Server.
 After the user is registered, set the user policy of "User (1)" to "User (3)" as follows:

User Name	User Policy
User (1)	Policy X

User Name	User Policy
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.

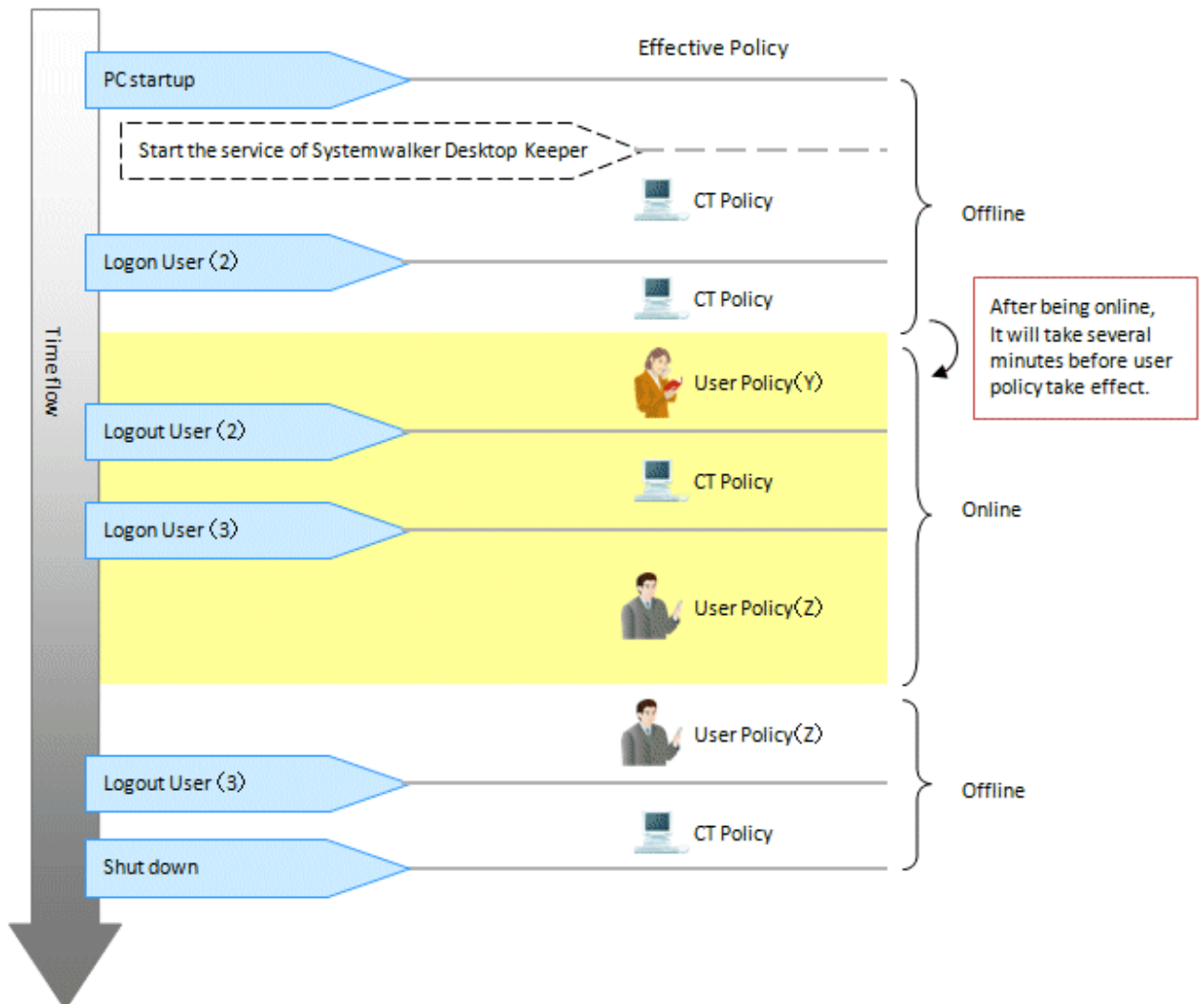
d) Then for the client (CT) to which the User (3) logs on, click **Update Immediately** in the CT policy settings window after the Management Console has been started.
User policy (Policy Z) is updated immediately.

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.

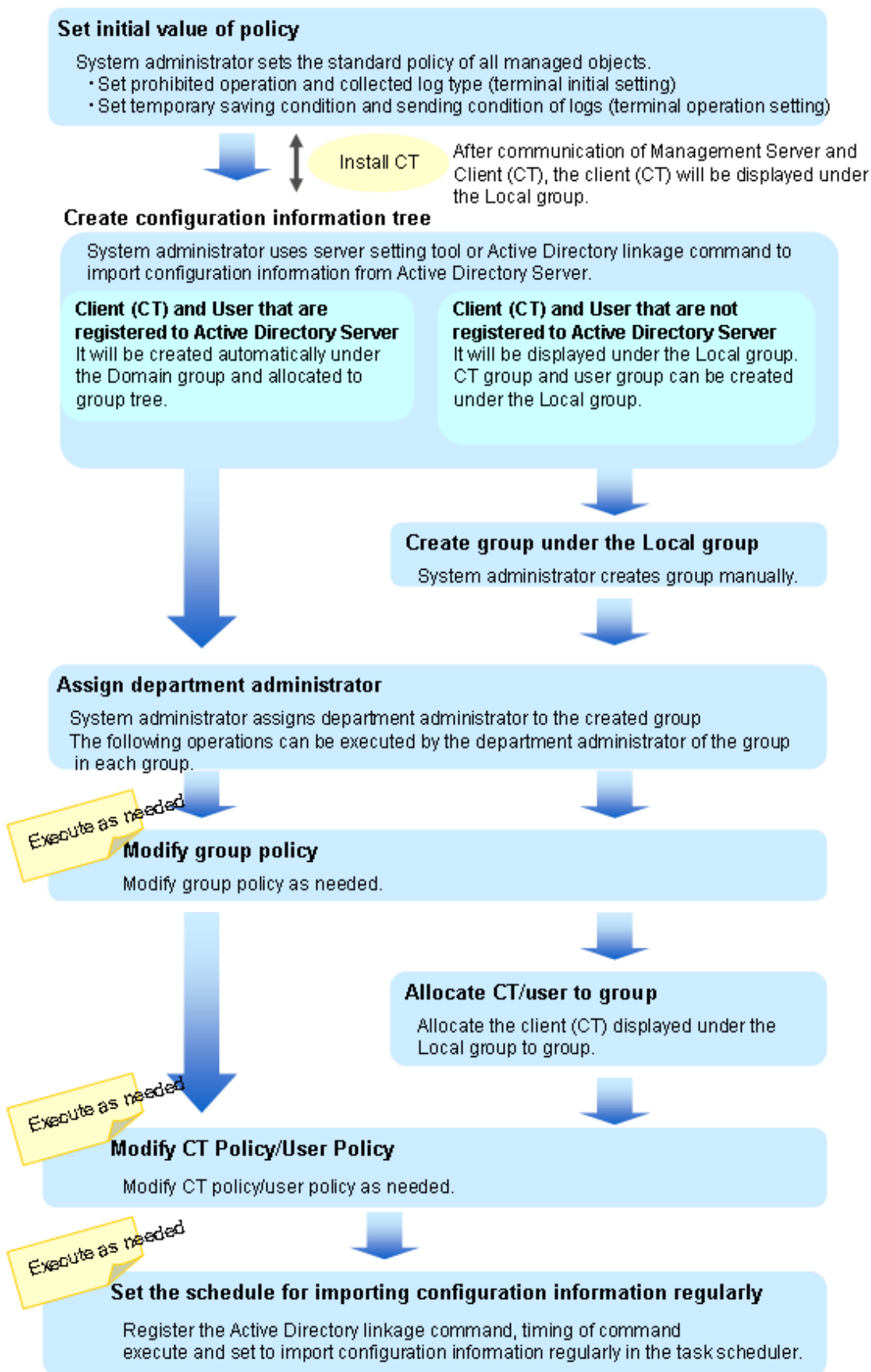
2.2 Flow of Preparing Operating Environment

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

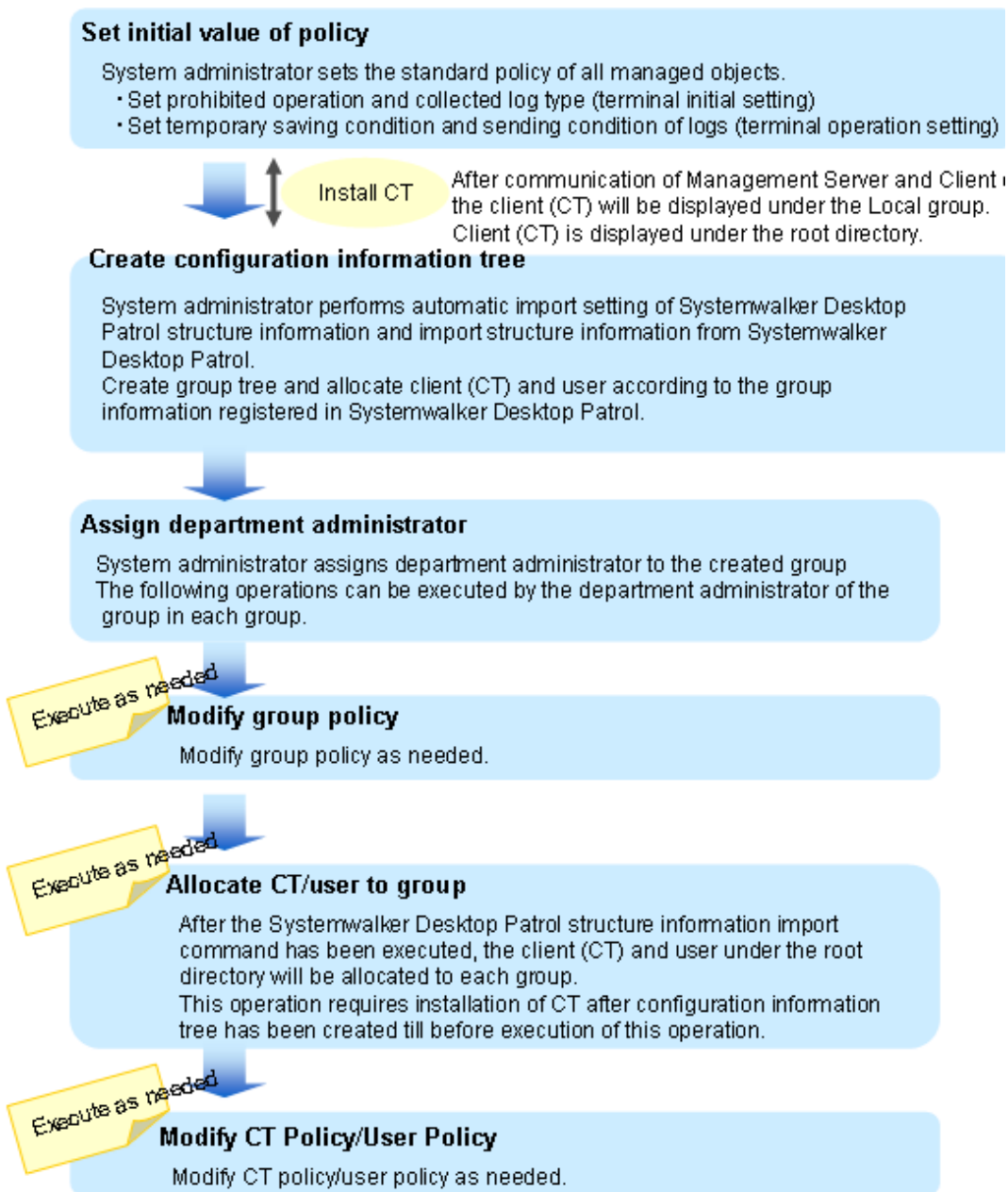
The flow varies upon the method of creating configuration information tree.

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

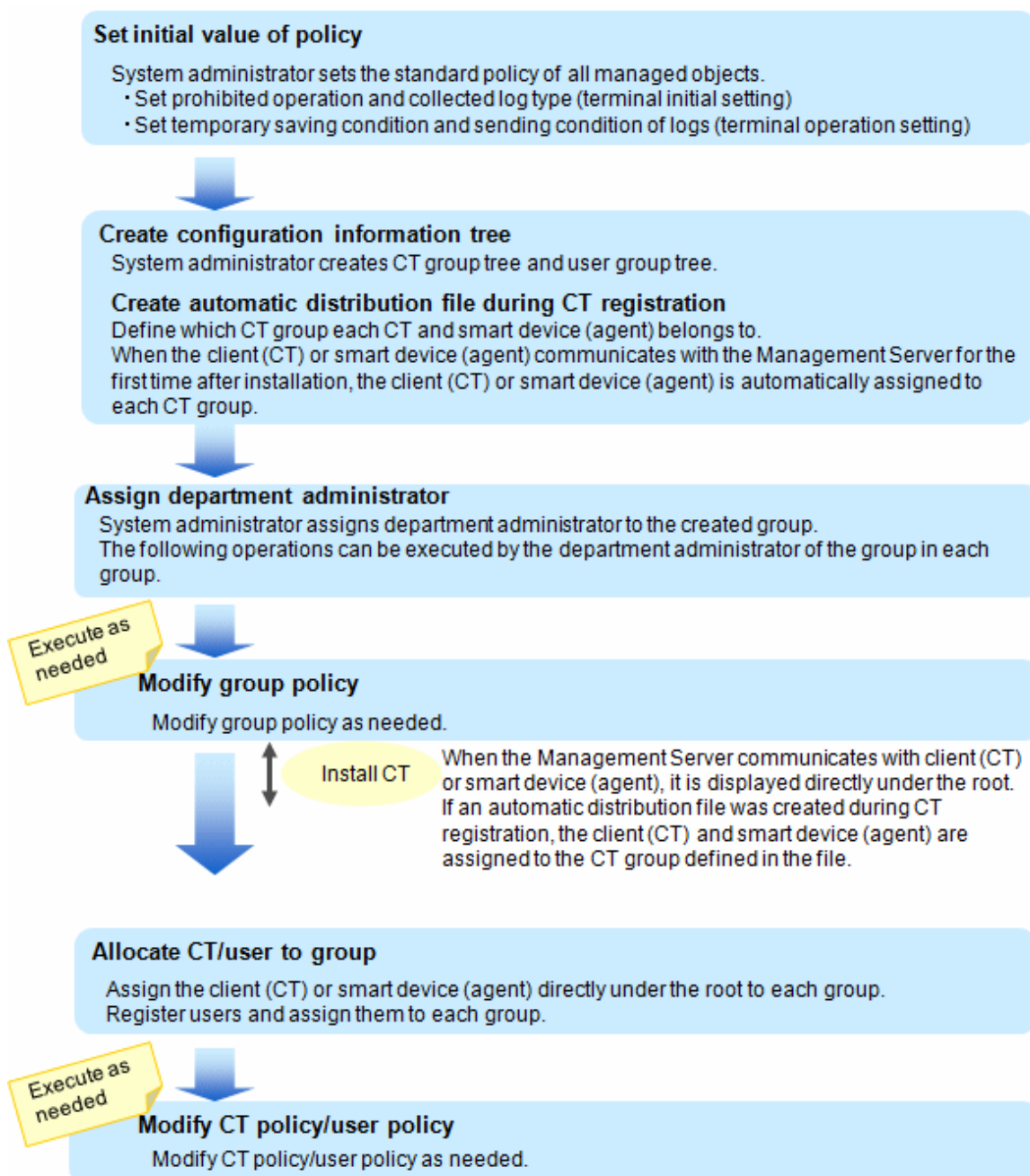
When importing configuration information from active directory



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, 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 (with the total number of clients (CTs) and smart devices (agents) being around 2,000 or more), 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 **Start > Systemwalker Desktop Keeper > Management Console > Management Console** 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.

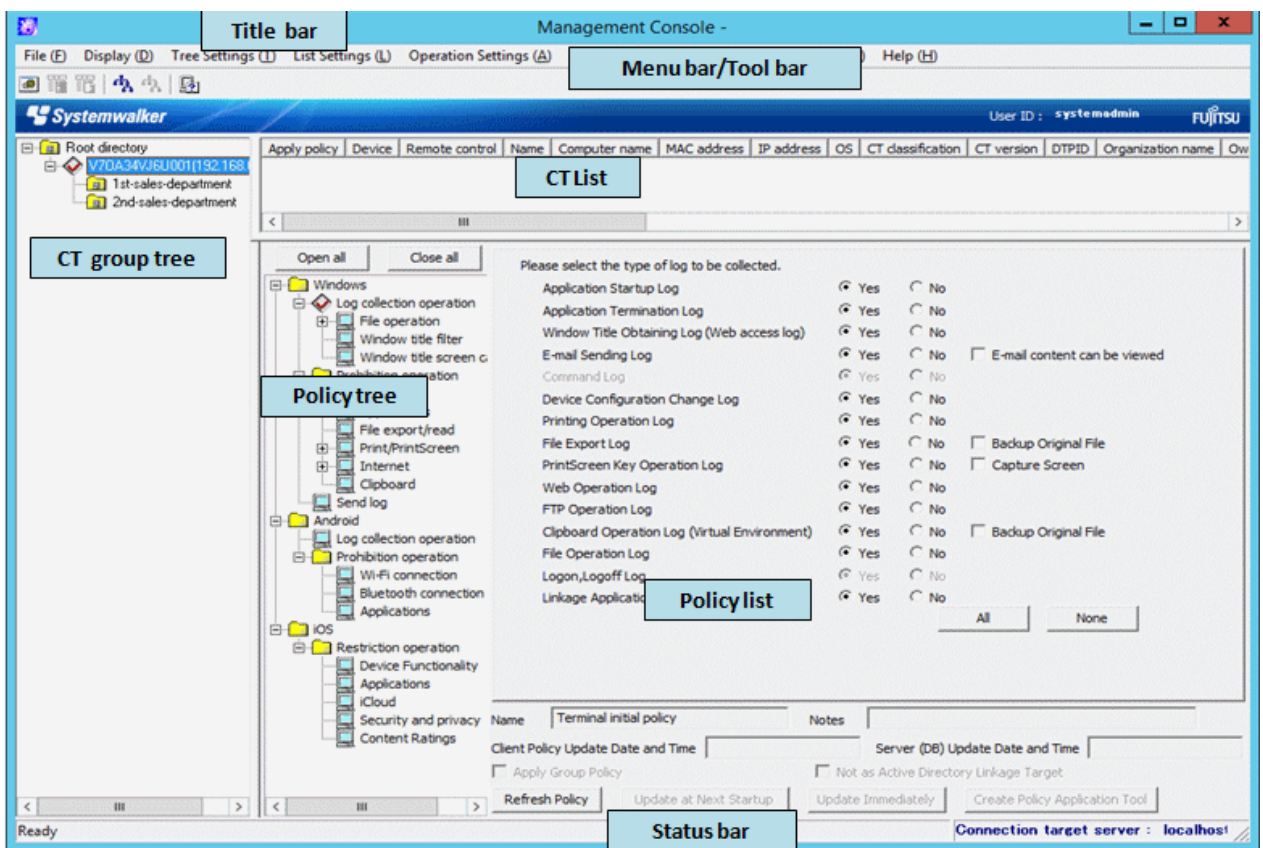
The login method of the system administrator is the same as that of a department administrator.

- **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. 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.



The following 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.
	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	
	Client (CT)	Smart device (agent)
Apply policy	This shows the policy applied.	

Item Name	Description	
	Client (CT)	Smart device (agent)
	<ul style="list-style-type: none"> - CT: The CT policy is applied. - Group: The CT group policy is applied. 	
Device	This is displayed as PC ..	This is displayed as Smart device .
Remote control	Blank	The latest remote control status is displayed. Refer to " 3.7.2 Checking Remote Control Status " for details on the displayed status.
Name	<p>The computer name is displayed as the default value.</p> <p>After the client (CT) has been installed, even if the computer name is modified, the name will remain unchanged.</p>	<p>The default value is displayed in the name format in which the following three strings are concatenated:</p> <ul style="list-style-type: none"> - Phone number, or model name (for devices with no phone numbers) (*2) (*3) - The user ID set when the smart device (agent) was installed (*4) - Sequential number (0001-9999) <p>Example 1: 080xxxxxxxxx_SAMPLEUSER_0001</p> <p>Example 2: T-01C_SAMPLEUSER_0001</p>
	To change the name, refer to " Modify CT Policy " and change it in the window (CT policy settings window) displayed immediately after the Management Console is started.	
Computer name	This refers to the computer name of the client (CT).	This is the model name of the smart device (agent). (*3)
MAC address	This refers to the MAC address of the client (CT).	This is the MAC address of the smart device (agent).
IP address (*1)	This refers to the IP address of the client (CT).	This is the IP address of the smart device (agent).
OS	Operating system name of the client (CT).	This is the OS name of the smart device (agent).
CT classification	This is displayed as SE . (SE is displayed for Standard Edition V13.3.0 or earlier, while a blank is displayed for Base Edition.)	This is displayed as SE .
CT version	This refers to the version of installed Systemwalker Desktop Keeper client (CT) and smart device (agent). In addition, refer to "CT Version" of <i>Systemwalker Desktop Keeper Reference Manual</i> for correspondence of Version/Edition of product.	
DTPID	<p>This refers to "User ID (+) PC Name" of Systemwalker Desktop Patrol client (CT).</p> <p>It indicates the client (CT) of Systemwalker Desktop Keeper and the client (CT) of Systemwalker Desktop</p>	Blank

Item Name	Description	
	Client (CT)	Smart device (agent)
	Patrol are installed in the same computer.	
Organization name	This refers to the organization name set in the OS of the client (CT).	Blank
Owner name	This refers to the owner name set in the OS of the client (CT).	Blank
Subnet mask	This refers to the subnet mask.	This is the subnet mask of the smart device (agent).
Link with Active Directory	Whether the client (CT) imports information by linking with Active Directory can be displayed. - When using the Link with Active Directory to import information: (Blank) - When using a method other than the Link with Active Directory to import information: Non-target	Blank
Network participation status	This is the network participation status of the client (CT). - Domain: The client (CT) belongs to a domain. - Group: The client (CT) does not belong to a domain.	Blank
Affiliated domain name	The name of the domain to which the client (CT) belongs. When Network Participation Status is Group , the group name will be displayed.	Blank
Last logon date and time	At startup, 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. - Send CT policy - Send user policy The date and time are displayed or updated in the following case: - When a policy is synchronized between the Master Management Server or Management Server and the client (once per day between 0:30 and 1:30)	This is the final date and time when the Master Management Server or Management Server sent a CT policy to a smart device (agent). The date and time are displayed or updated in the following cases: - When Sync now is selected on the smart device (agent) - When automatic synchronization between the Master Management Server or Management Server and the smart device (agent) is performed (once per day between 12:00 and 13:00)
Date and time of client policy update	This refers to the final date and Time when the Master Management Server or Management Server sends CT Policy to the client (CT).	

Item Name	Description	
	Client (CT)	Smart device (agent)
	<p>it will be displayed or updated in following cases:</p> <ul style="list-style-type: none"> - When the client (CT) added to the CT list is restarted and starts to communicate with the Master Management Server or Management Server. - When the CT policy is reflected in the client (CT) after clicking Update Immediately button of the Management Server. - When a policy is synchronized between the Master Management Server or Management Server and the client (once per day between 0:30 and 1:30) 	
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 smart device (agent) and reflects to the database (including immediate update).	
Notes	<p>This refers to the information entered when the policy of the client (CT) and smart device (agent) is reflected.</p> <p>Refer to "Modify CT Policy" during modification.</p>	
Trace conditions	<p>This refers to the settings that are traced and collected in the client (CT).</p> <ul style="list-style-type: none"> - Summary: Collect the summary of content traced by the client (CT). - Details: The details traced by the client (CT) are collected by levels. - Blank: When the trace content is not collected or the client (CT) is V12.0. 	Blank
DTP version	This is the version of Systemwalker Desktop Patrol CT installed in PC.	Blank
Virtual PC	<p>When installing the client (CT) in the virtual environment, it is displayed as follows:</p> <ul style="list-style-type: none"> - (Main): When it is the master image of the virtual PC. -: When it is the virtual PC. 	Blank

*1: If you disable the dual stack, the disabled IP address may continue to be displayed for a while.

*2: The model name can be checked using the following:

- Tap **Settings > About phone** and check **Model number**.

The procedure to view the model name may be different, however, depending on the operating system and device type.

*3: Only the first 15 characters are set for the model name.

*4: For the smart device (agent) (iOS), the user ID will not be set for the name.

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

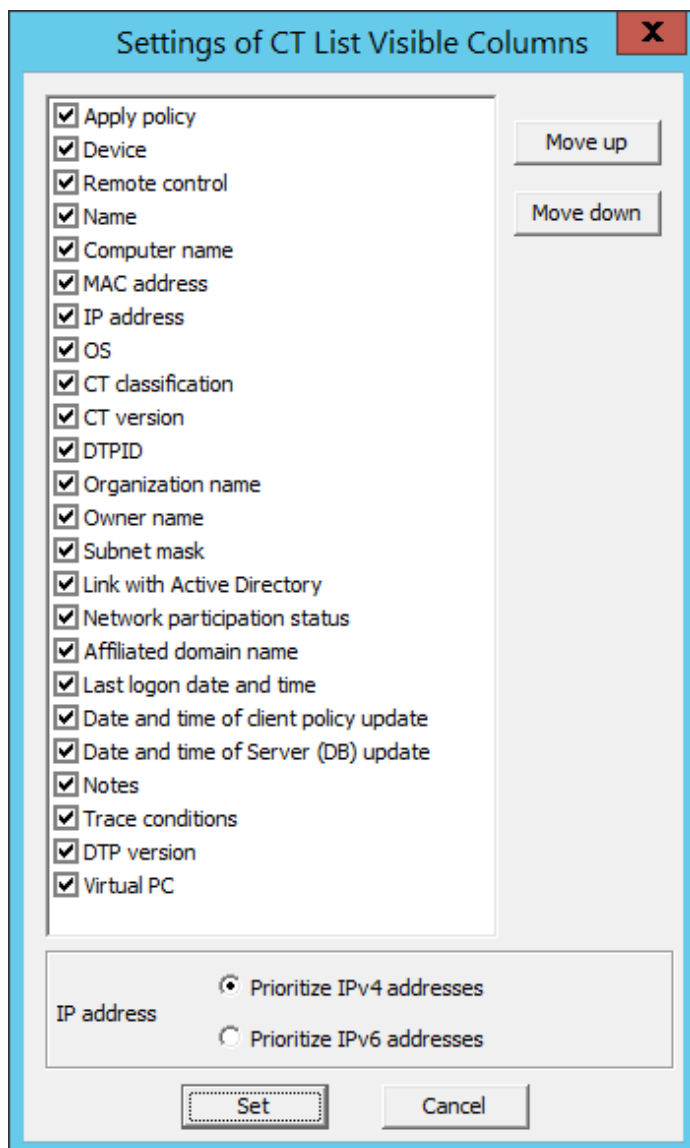
- When confirmation is performed by the CT,
Select a CT from the CT list. At the moment, the CT policy will be updated.
- When updating information for all CTs,
Select **Refresh Tree (All Servers)** from the **Tree Settings** menu.
- When updating information of all subordinate CTs in the selected Management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



- a. Select the check box displayed in the CT list.
- b. Select the item that requires modification of display sequence by clicking the **Move Up** or **Move Down** button.

c. For IP address, select one of the following:

- **Prioritize IPv4 addresses:** IPv4 addresses will be displayed in an IPv4/IPv6 dual-stack environment, and IPv6 addresses will be displayed in an IPv6 address-only environment.

- **Prioritize IPv6 addresses:** IPv6 addresses will be displayed in an IPv4/IPv6 dual-stack environment, and IPv4 addresses will be displayed in an IPv4 address-only environment.

Refer to "[1.2.45 IPv6 Support](#)" for details on the values displayed in IPv6.

d. 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.

Policy tree

Policies are grouped by category and displayed in a hierarchy.

Selecting a policy in the policy tree switches the windows in the policy list.

Policy List

This displays the policies that have been set.

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).

Menu Bar		Toolbar	Function Summary
	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.
Tree 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 check box 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 check box 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.

Menu Bar		Toolbar	Function Summary	
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 Management Server	-	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 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

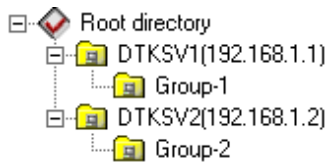
After the "Display Server" check box of "Tree Settings" is selected in the Management Console connected to Master Management Server, the computer name and IP address of the connected Master Management Server and Management Server will be displayed, and the CT group will be displayed on each server.

As the server is always displayed during Active Directory Linkage, the selection of **Display Server** check box cannot be cancelled.

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



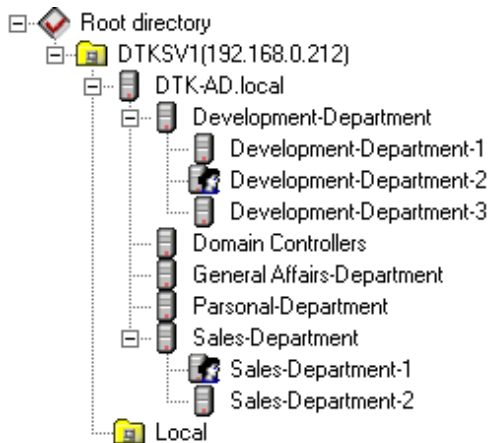
When Display Server is selected (when Active Directory Linkage is not performed)



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



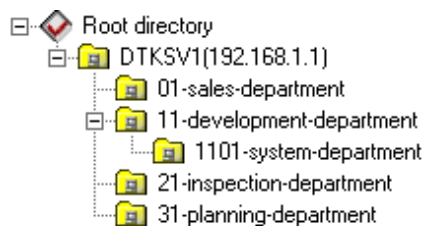
Display "Deleted CT" group

After **Tree Settings > Display Server** of the Management Console is selected, the "Deleted CT" group (when the **Display Server** check box is not selected, the **Display "Deleted" Group** check box cannot be selected.) will be displayed when **Display "Deleted" Group** of **Tree Settings** is selected.

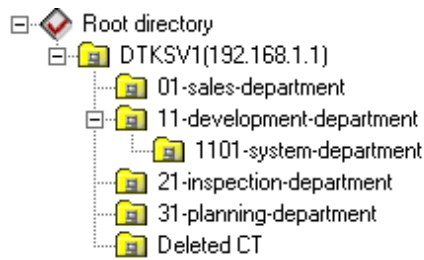
The following is an example when Active Directory Linkage is not performed.

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) and smart device (agent) operation and collected logs in the terminal initial settings.

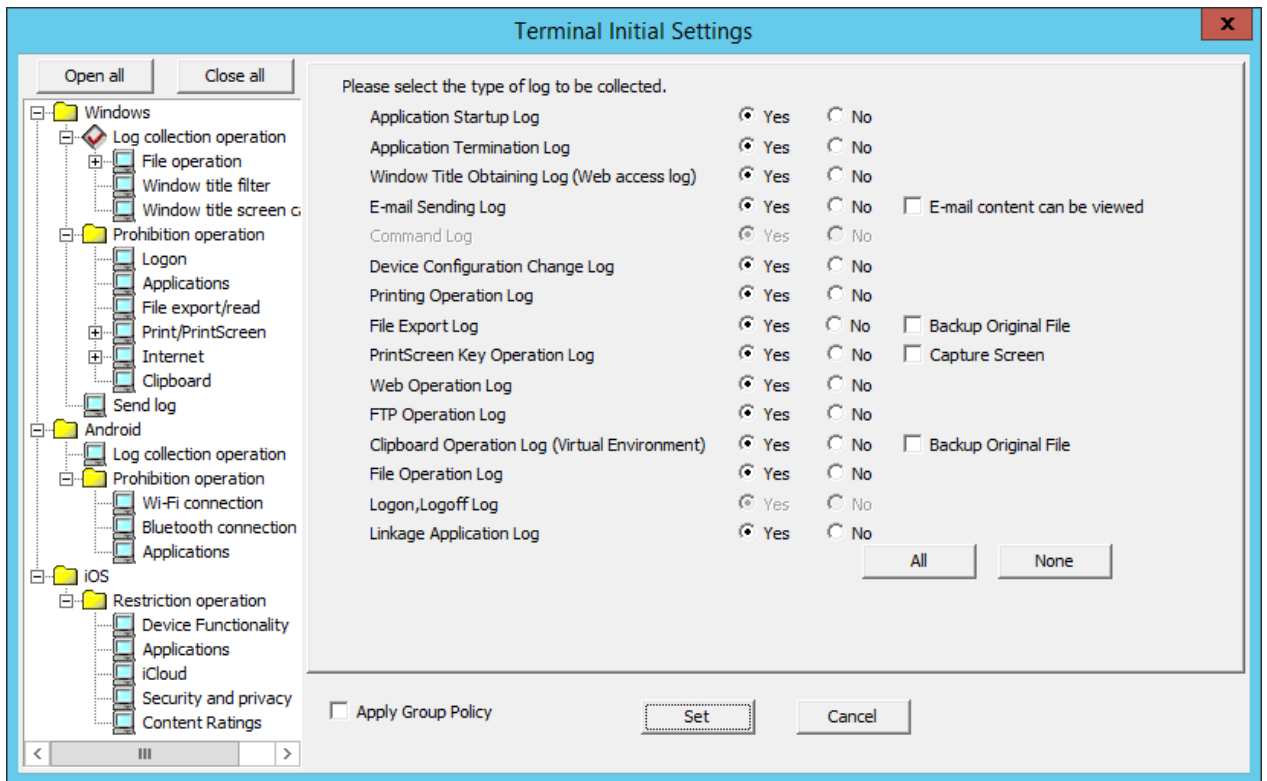
In a 3-level system structure, perform terminal initial settings in each the Management Server. Even if the terminal initial settings is performed in the Master Management Server, it cannot be reflected to a Management Server.

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: (Initial Value) 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 each policy, click the **Set** button.
Select a policy to be set from the tree.

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.

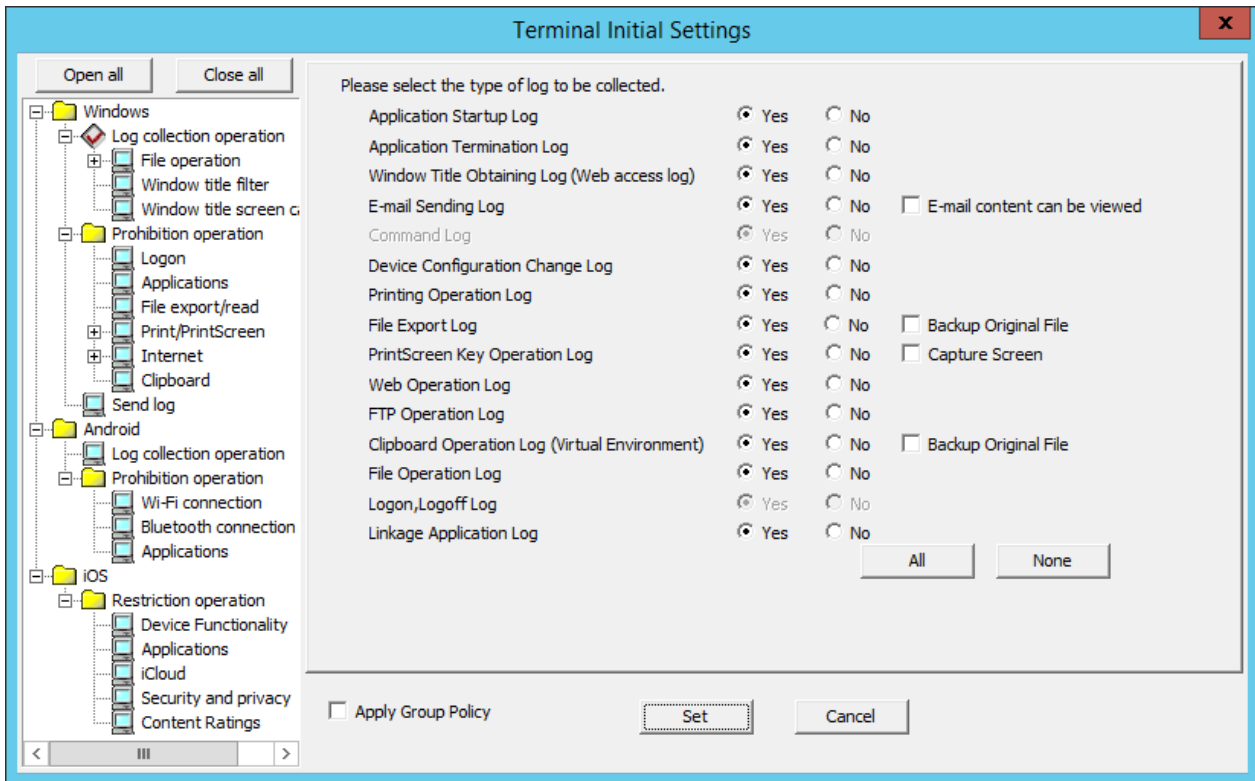
Refer to "[Modify CT Policy](#)" or "[3.4.2 Modify User Policy](#)" for the policy reflection operation.

The following section describes the settings for each policy.

2.4.1.1 Log Collection Operation (Windows)

Specify the type of the log to be collected on the client (CT) in **Windows > Log collection operation**. When it is set to "Yes", the operation logs in the client (CT) will be collected.

The settings to be specified in **Windows > Log collection operation** are described below.



Item Name	Description
Application Startup Log	Application startup logs will be collected. Initial Value: Yes is selected. (*1)
Application Termination Log	Application termination logs will be collected. Initial Value: Yes is selected. (*1)
Window Title Obtaining Log(Web access log)	Window title logs at startup of window application will be collected. Initial Value: Yes is selected. (*1)
E-mail Sending Log	E-mail sending logs will be collected. Initial Value: Yes is selected. (*1)
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: (Initial Value) 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.
Device Configuration Change Log	Device configuration change logs will be collected. Initial Value: Yes is selected. (*1)
Printing Operation Log	Printing logs will be collected. Initial Value: Yes is selected. (*1) When "Yes" is selected, input can be performed in the following policy: - Eco monitoring
File Export Log	Logs during file export with File Export Utility will be collected. Initial Value: Yes is selected. (*1)
Backup Original File	This can be set when the File Export Utility option is "Yes".

Item Name	Description
	<p>When it is selected: The original file of the file exported by File Export Utility will be backed up.</p> <p>When it is not selected: (Initial Value) The original file of the file exported by File Export Utility will not be backed up.</p>
PrintScreen Key Operation Log	<p>PrintScreen key operation logs will be collected. This can be set when the Disabling PrintScreen Key of Print/PrintScreen is "No". Initial Value: Yes is selected. (*1)</p>
Capture Screen	<p>This can be set when PrintScreen Key Operation Log is "Yes".</p> <p>When it is selected: The screen capture at the time point when PrintScreen key operation logs are collected will be recorded.</p> <p>When it is not selected: (Initial Value) The screen capture at the time point when PrintScreen key operation logs are collected will not be recorded.</p>
Web Operation Log	<p>The following log will be collected:</p> <ul style="list-style-type: none"> - Web download log <p>Initial Value: Yes is selected. (1*)</p>
FTP Operation Log	<p>The following logs will be collected:</p> <ul style="list-style-type: none"> - FTP upload log - FTP download log <p>Initial Value: Yes is selected. (*1)</p>
Clipboard Operation Log(Virtual Environment)	<p>Clipboard operation logs will be collected. This can be set when Do not prohibit is selected for Clipboard > Prohibition of clipboard operation between different environments. - Initial Value: Yes is selected. (*1)</p>
Backup Original File	<p>This can be set when the Clipboard Operation Log (Virtual Environment) is set to "Yes".</p> <p>When it is selected: The information (text, image, file path) copied via clipboard can be backed up as original file.</p> <p>When it is not selected: (Initial Value) The information (text, image, file path) copied via clipboard will not be backed up as original file.</p>
File Operation Log	<p>File operation logs will be collected. Initial Value: Yes is selected. (*1)</p> <p>When "Yes" is selected, input can be performed in the following policies:</p> <ul style="list-style-type: none"> - File operation - Extension
Logon,Logoff Log	<p>The following logs will be collected:</p> <ul style="list-style-type: none"> - Logon log - Logoff log - PC startup log - PC shutdown log

Item Name	Description
	<ul style="list-style-type: none"> - PC sleep log - PC restoration log - PC connection log - PC disconnection log <p>Initial Value: "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>Linkage application logs will be collected.</p> <p>Initial Value: Yes is selected. (*1)</p>
All	Select to collect all logs.
None	Select not to collect all logs.

*1: If the client (CT) was installed using custom installation, **No** is selected by default.



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 server is set to **Yes**, the printing operation log can be collected.

2.4.1.2 File Operation

The screening conditions for obtaining file operation logs can be set in **File operation**. 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.

The items in **File operation** can be set when **Yes** is selected in **Windows > Log collection operation > File Operation Log**.

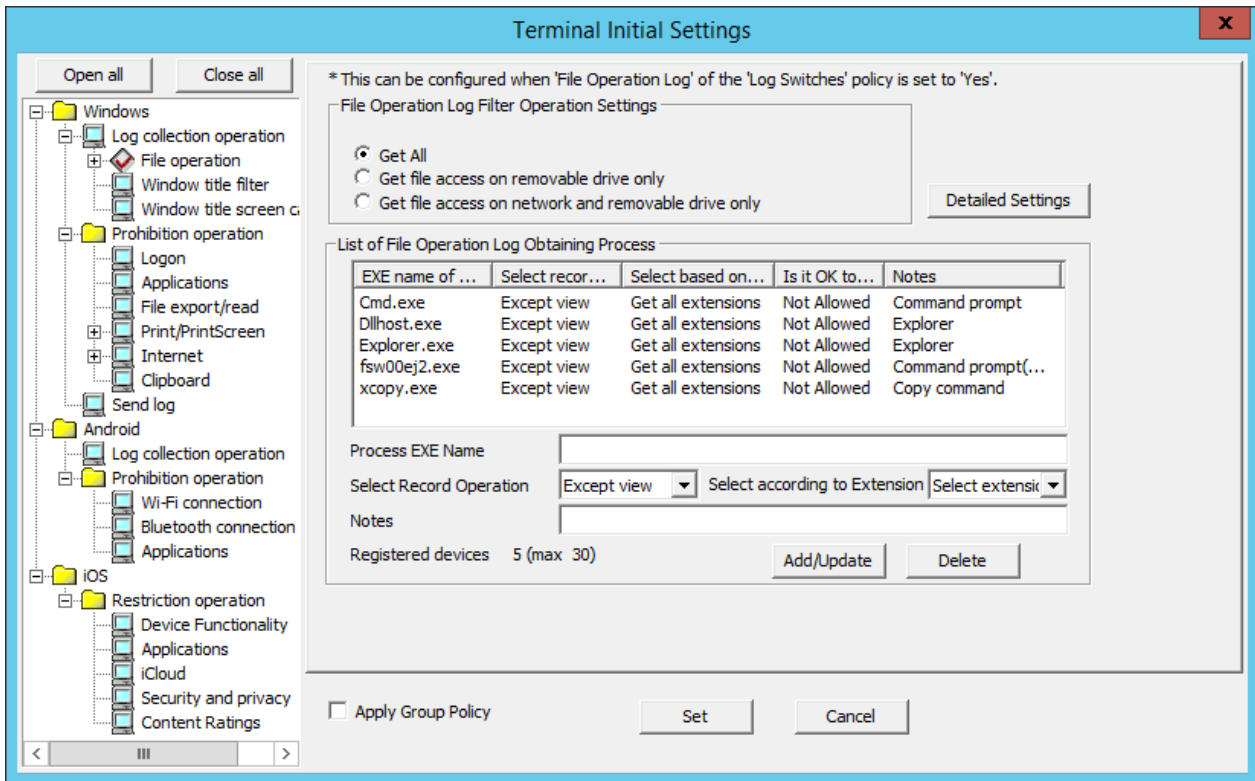


Note

Do not register the software with many disk accesses.

Since the output of a large amount of logs will cause insufficient database capacity, 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, register after confirming the performance and OS operation state on the test machine.



Initial Value Displayed in [List of File Operation log ObtainingProcess]

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
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 (Initial Value)	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 File Operation Process - Detailed Settings window will be displayed. Set the folder in which the file operation logs are not collected.

Item Name	Description
	(This item cannot be set if No is selected in Windows > Log collection operation > File Operation Log.)

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. Initial Value: "Initial Value Displayed in [List of File Operation log ObtainingProcess]" 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. (Alphabetic characters are not case-sensitive) In addition, ".com", ".exe", or ".bin" can be entered in the extension of a process. However, if double-byte characters or the following symbols are used, error will occur. " \ " / " " : " * " ? " " " " < " > " " Initial Value: 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 (Initial Value) 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. - 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: - exe - dll - ini - tmp - lnk - inf - Select extension (Initial Value) This is selected when collecting only the necessary file operation log. The operations of entering extensions in Extension will be recorded. * 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.
Notes	Enter the memo information of process name. Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). Initial Value: Not Specified.

Item Name	Description
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
Add/Update	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.
Delete	Delete the selected information of List of File Operation Log Obtaining Processes .

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**.

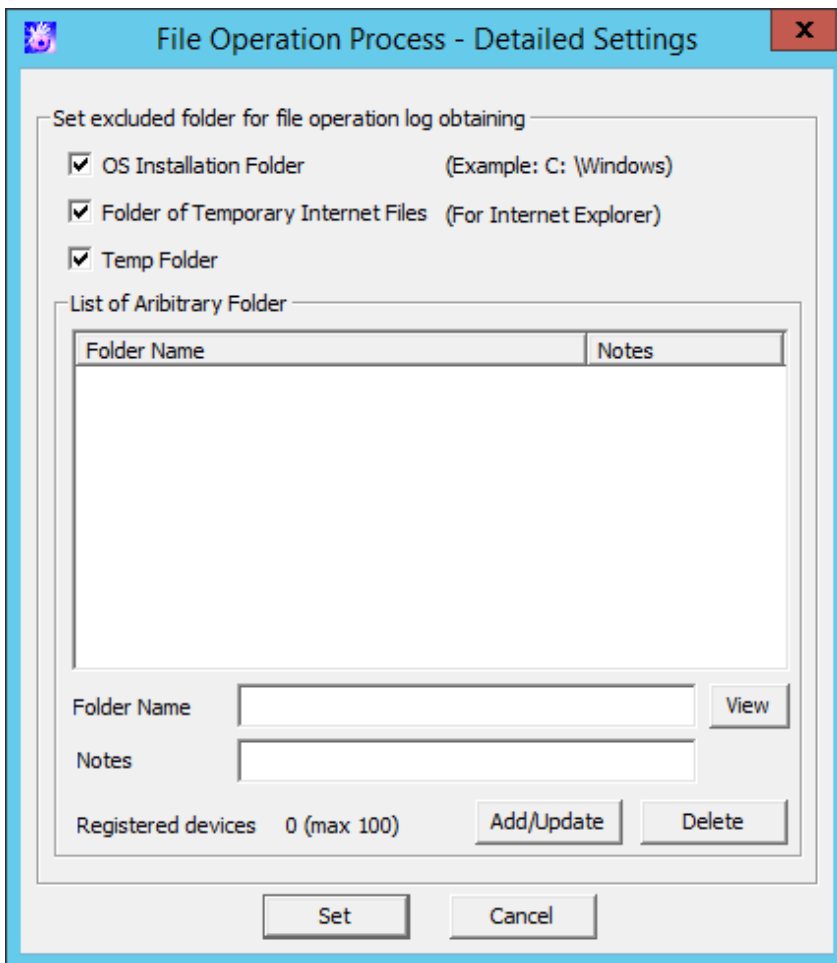
- **Select Record Operation**
- **Select according to Extension**
- **Notes**

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 check box 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. (Initial Value): Selected (*)
Folder of Temporary Internet Files	Select this check box when accessing the files on the folder of Temporary Internet Files, but when the file operation logs are not to be obtained. (Initial Value): Selected (*)
Temp Folder	Select this check box 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"> - The folder specified according to the user environment variable TEMP and TMP. - The folder a specified according to the system environment variable TEMP and TMP. (Initial Value): 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. Specify up to 254 halfwidth (127 fullwidth) characters. However, the file name cannot contain any of the following symbols: : * ? " < >

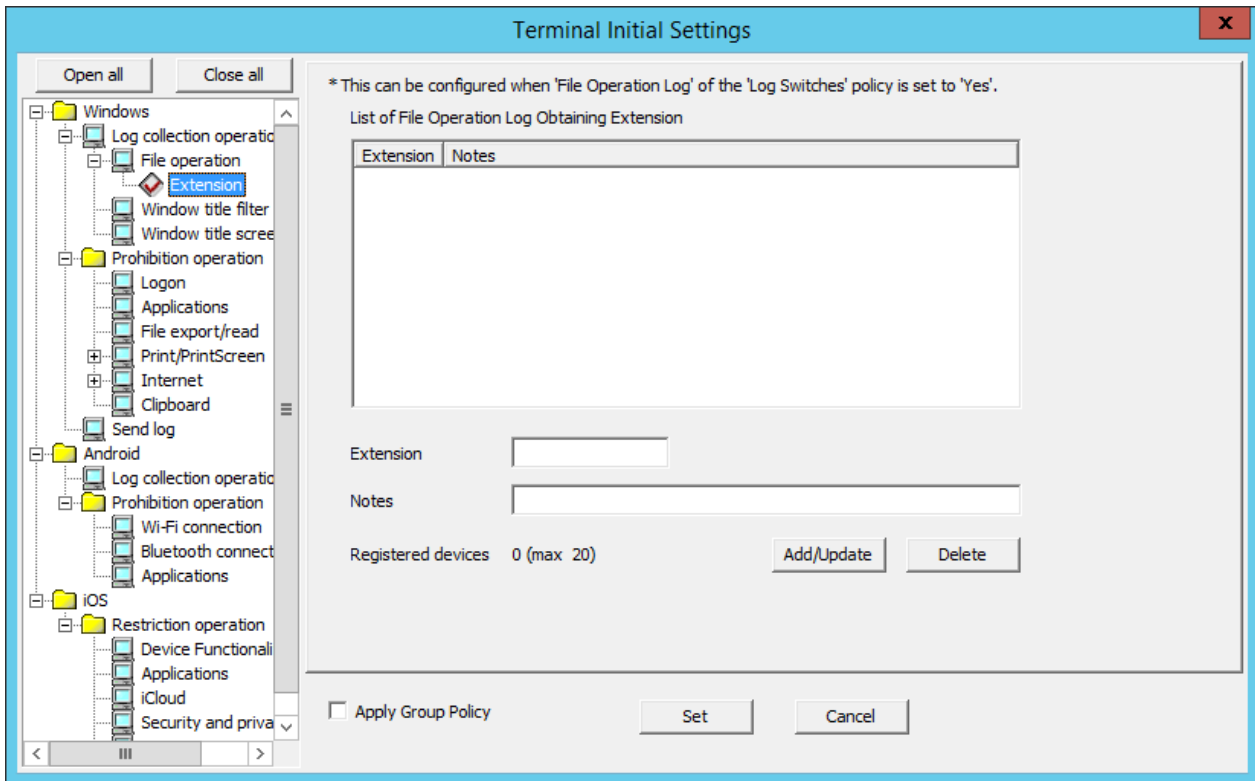
Item Name	Description
	<p>It is not case-sensitive. A maximum of 100 folder names can be registered.</p> <p>Specify the folder by adding "\" or "/" after the drive's name + colon (:), Specifying the drive name only is also allowed ("D" etc.). When only the drive's name is specified, the file operation 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"> - 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. - 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. <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, register "d:\data.tmp".</p> <p>Initial Value: Not Specified.</p>
Notes	<p>Enter the memo information, etc. Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). Initial Value: 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, enter the full path in Folder Name.</p>
Registered devices	<p>The number of registered cases and the maximum number of registrations possible are displayed.</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 Arbitrary Folder, and click the Delete button.</p>
Set	<p>Confirm the input content and return to the previous window.</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.

2.4.1.3 Extension

For the file (extension) accessed by the process set in **File operation**, when the file operation log is collected, the extension can be set in **Extension**.

The items in **Extension** can be set when **Yes** is selected in **Windows > Log collection operation > File Operation Log**.



Item Name	Description
List of File Operation Log Obtaining Extension	Display the extension of the registered and obtained file operation log. 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 File operation , the log of that process will not be collected. Initial Value: Not Specified.
Extension	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.) Up to 16 single-byte characters (Alphabetic characters are not case-sensitive) can be entered. Only halfwidth alphanumeric characters, halfwidth symbols (except for the symbols mentioned below), and spaces can be entered (however, spaces cannot be specified at the beginning or the end). Error will occur if the following symbols are used. "\ " / " : " * " ? " " " < " > " " . " If the wildcard (*) is used, "*" should be put at the beginning or at the end of the extension. <ul style="list-style-type: none"> - When forward matching is specified. Enter "Extension". Example: xl* - When backward matching is specified Enter "Extension". Example: *ls The wildcard "*" cannot be entered in other locations. In addition, the wildcard "*" cannot be entered alone Enter it in combination with characters. Initial Value: Not Specified.
Notes	Enter the extension and memo information. Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). Initial Value: Not Specified.

Item Name	Description
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
Add/Update	Add the entered information to the list. Up to 20 cases can be registered. In addition, the modified information should be set.
Delete	Delete the information selected in the List of File Operation Log Obtaining Processes .

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.

2.4.1.4 Window Title Filter

The conditions for collecting the window title obtaining log can be set in **Window title filter**.

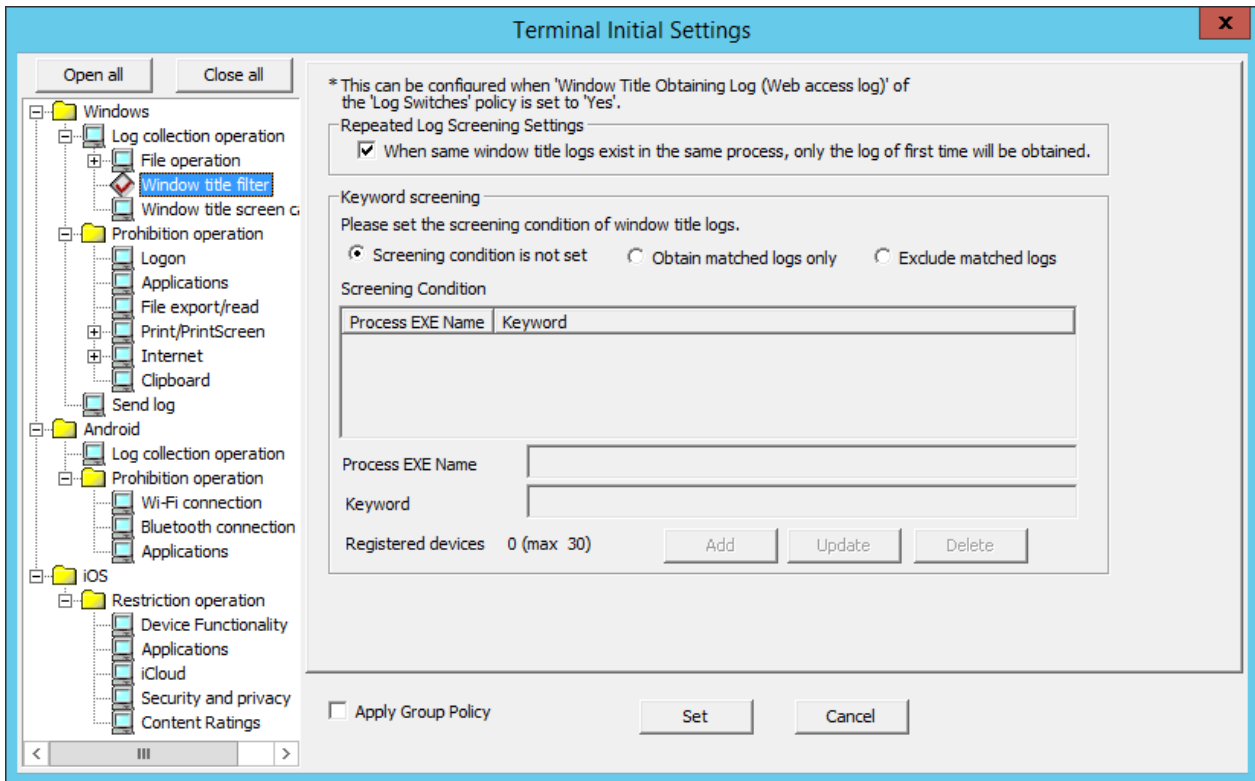
Though a large number of window title obtaining logs can be collected in order to record all operations on the PC, there will be many repeated logs. Therefore, to avoid collecting the repeated logs, the filtering condition should be set.

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.

Window title filter can be set when **Yes** is selected in **Windows > Log collection operation > Window Title Obtaining Log(Web access log)**.

The following describes the settings in **Window title filter**.



Repeated Log Screening Setting

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

Keyword screening

Item Name	Description
Screening condition is not set (Initial Value)	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. Initial Value: 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. (Alphabetic characters are not case-sensitive) Spaces can only be used in-between characters. ".com", ".exe", or ".bin" can be entered in the extension of process.

Item Name	Description
	<p>Error will occur if the following symbols are used. "\" "/" "." "*" "?" "" "<" ">" " "</p> <p>When it is not specified, logs of all processes will be collected (or excluded). Initial Value: Not Specified.</p>
Keyword	<p>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.</p> <p>Example:</p> <ul style="list-style-type: none"> - Save as - Print <p>Specify up to 254 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). (Alphabetic characters are not case-sensitive)</p> <p>When Keyword is not specified, all window title obtaining logs of processes specified in Process EXE Name will be collected (will not be collected). Initial Value: Not Specified.</p>
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
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.

2.4.1.5 Window Title Screen Capture

The condition of collecting the screen capture can be set in **Window title screen capture**.

Set conditions in this setting to capture the window title screen at the same time as the window title obtaining the log that matches the conditions set in **Window title filter** is collected.

Window title screen capture can be set when **Yes** is selected in **Windows > Log collection operation > Window Title Obtaining Log(Web access log)**.

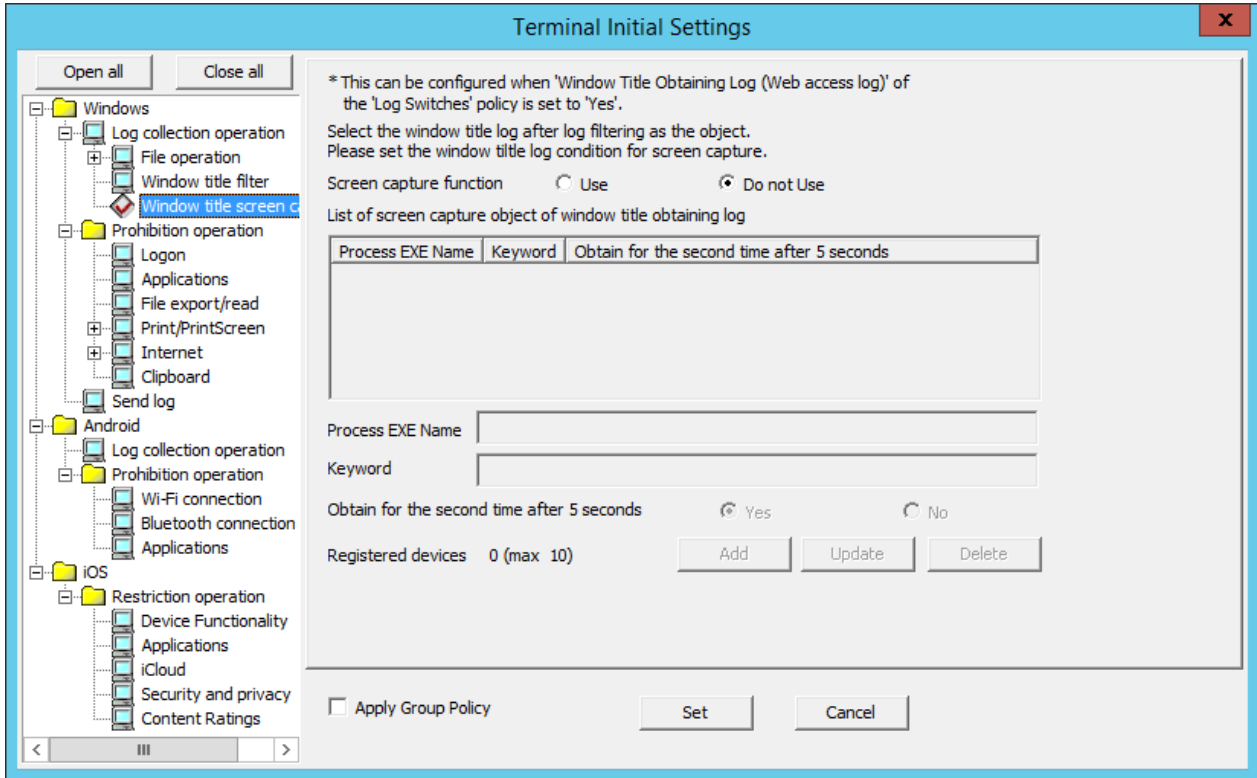
The settings related to screen capture can be performed in the **Terminal Operation Settings** window (Settings item: **Attached data condition settings**). Refer to "2.4.2 Perform Terminal Operation Settings" for details.

 **Note**

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, regularly confirm the capacity and backup and delete.

The following describes the settings in the **Window title screen capture**.



Item Name	Description
<p>Screen capture function</p>	<p>Select whether to obtain screen capture.</p> <ul style="list-style-type: none"> - Use Obtain screen capture. - Do not Use (Initial Value) Do not obtain screen capture.
<p>List of screen capture object of window title obtaining log</p>	<p>The conditions for obtaining screen capture are displayed in a list.</p> <p>Initial Value: Not Specified.</p>
<p>Process EXE Name</p>	<p>Enter the EXE name of screen capture.</p> <p>Up to 254 single-byte characters (127 double-byte characters) can be entered. Alphabetic characters are not case-sensitive.</p> <p>".com", ".exe", or ".bin" can be input in the process extension.</p> <p>Error will occur if the following symbols are used.</p> <p>"\ " / " : " * " ? " " " < " > " "</p> <p>When the EXE name of process is set to blank, logs of all process will be collected (excluded).</p> <p>Initial Value: Not Specified.</p>

Item Name	Description
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"> - Save as - Print <p>Specify up to 254 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). (Alphabetic characters are not case-sensitive)</p> <p>When the EXE name of process is entered in the EXE Name of Process, make sure to input in Keyword.</p> <p>Initial Value: 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, select Yes.</p> <ul style="list-style-type: none"> - Yes Obtain screen capture for the second time after 5 seconds. - No Obtain screen capture once only. <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>
Registered devices	<p>The number of registered cases and the maximum number of registrations possible are displayed.</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 **Window title screen capture** and **Window title filter** 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.

2.4.1.6 Logon

The group prohibited from logon can be set in **Logon**. 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:

- Microsoft account

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:

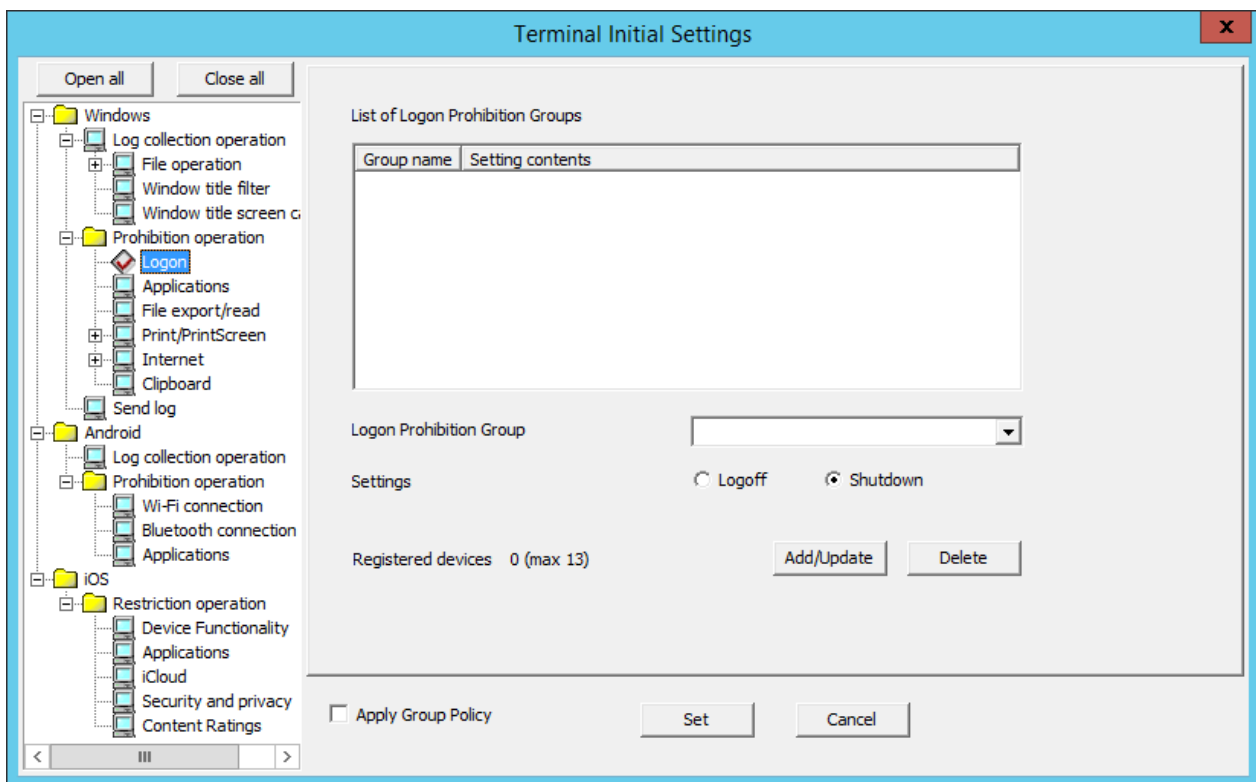
- The user name entered during logon to the Windows PC belongs to multiple groups.
- Logon prohibition is set for any one group in the multiple groups to which the user name belongs.

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 **Logon**.

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

The following section describes the settings of **Logon**.



Item Name	Description
List of Logon Prohibition Groups	The set logon prohibition group will be displayed. Initial Value: Not specified.
Logon Prohibition Group	Select the logon prohibition group from the pull-down menu. Refer to Windows manual for the details of each group. Initial Value: Not specified.
Settings	When prohibiting the target group from logon, the processing in the client (CT) can be specified. - Logoff Logoff by force. Under Windows Server(R) 2008, set Logoff when users with User authority are not expected to use.

Item Name	Description
	<p>- Shutdown (Initial Value) Shutdown by force. However, under Windows Server(R) 2008, the User authority cannot shut down the computer.</p> <p>The time from logon prohibition being detected from the client (CT) to logoff or shutdown can be set in the "Terminal Operation Settings". Refer to "2.4.2 Perform Terminal Operation Settings" for "Terminal Operation Settings".</p>
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
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.

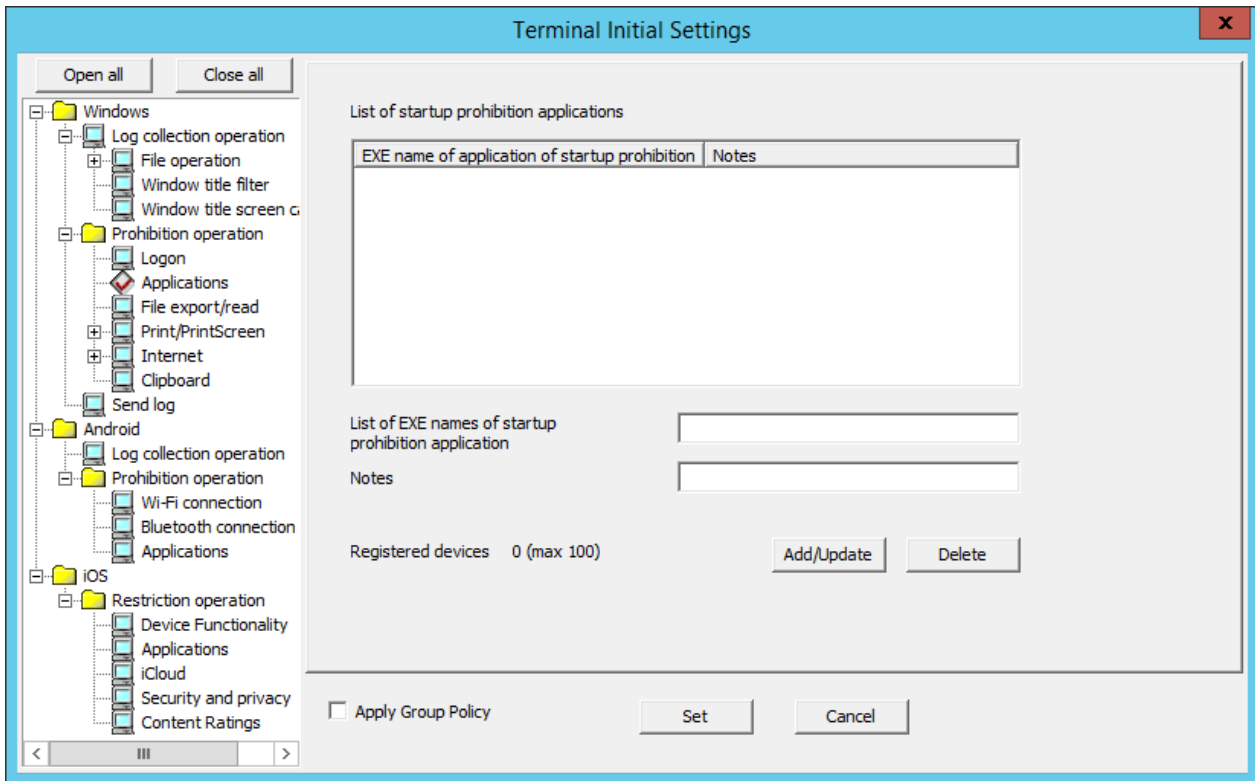
When deleting information

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

2.4.1.7 Application

In **Application**, 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 **Application**.



Item Name	Description
List of startup prohibition applications	The set EXE name of the application prohibited from startup will be displayed. Initial Value: 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(R) Excel) Up to 254 single-byte characters (127 double-byte characters) can be entered. (Alphabetic characters are not case-sensitive) However, error will occur if the following symbols are used. " \ " / " : " * " ? " " " < " > " " Initial Value: Not specified.
Notes	Enter the application name and memo information. Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). Initial Value: No specified.
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
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.

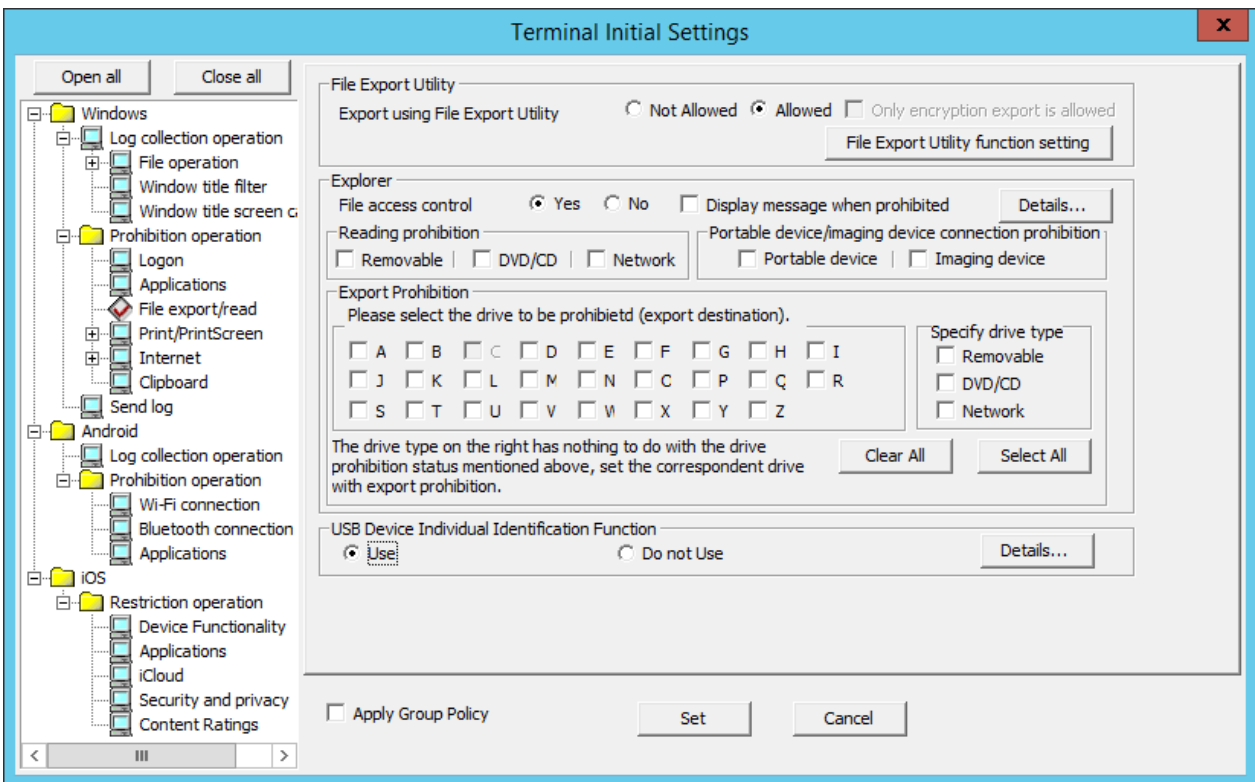
2.4.1.8 File Export/Read

In **File export/read**, 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 **File export/read**.




File Export Utility

Item Name		Description
Export using File Export Utility	Not Allowed (Initial Value)	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.
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	<p>Reading Prohibition and Export Prohibition can be set.</p> <p>The Display message when prohibition check box can be selected when this item is selected. After it is selected, messages will be displayed when the prohibition operation is performed.</p>
	No (Initial Value)	<p>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.</p> <p>When this item is selected, Reading Prohibition and Export Prohibition cannot be set.</p>
Display message when prohibited		<p>After setting this item, the following message will be displayed when inserting the prohibited device into the client (CT).</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>[S105-ERR001]Accessing to this drive is prohibited by system administrator. (Drive: G)</p> </div> <p>The above message is output when a violation regarding an added drive is recorded in the device configuration change log.</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>[S105-ERR002]Accessing to this drive is prohibited by system administrator. (Drive: Y-E DATA USB-FDU USB Device)</p> </div> <p>The above message is output when Violation regarding an added USB device is recorded in the device configuration change log for USB devices.</p> <p>Initial Value: Not selected</p> <p>Refer to "8.2.6 Device Configuration Change Log" for "Violation" of device configuration change log.</p>
Details		<p>Settings can be performed when the File Access Control is "Yes".</p> <p>The File access control - Detailed Settings window will be displayed. (Set the conditions of folders excluded from network drive access prohibition)</p>
Reading Prohibition		Set the targets for reading prohibition.
	Removable	<p>Reading of the following devices that are identified as drive letter are prohibited.</p> <p>Initial Value: Not selected</p> <ul style="list-style-type: none"> - Floppy disk - External hard disk (removable hard disks such as USB, IEEE1394, PCMCIA connection) - MO - USB memory <p>Compact flash memory</p>
	DVD/CD	<p>Reading of DVD/CD is prohibited.</p> <p>Initial Value: Not selected</p>
	Network	<p>Reading of network drive is prohibited.</p> <p>Initial Value: Not selected</p>

Item Name		Description	
Portable device/imaging device connection prohibition		Prohibits connection of portable devices and imaging devices.	
	Portable device	Prohibits connection of portable devices. Default value: Not selected.	
	Imaging device	Prohibits connection of imaging devices. Default value: Not selected.	
Export Prohibition		Set the targets for exporting prohibition.	
	Please select the drive to be prohibited(export destination).	<p>Select the drive that is the target for export prohibition. Initial Value: All are not selected</p> <p>The drive that becomes the prohibited target by specifying the drive letter should satisfy all the following conditions. 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"> - Drive identified as a drive letter in the PC. - Drive apart from the network drive. <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> Note</p> <hr style="border-top: 1px dotted orange;"/> <p>About network drive</p> <p>The network drive cannot be prohibited by specifying the drive letter. Prohibit it by selecting the Network check box.</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. Initial Value: Not selected</p> <ul style="list-style-type: none"> - Floppy disk - External hard disk (removable hard disks connected by such as USB, IEEE1394, PCMCIA connection) - MO - USB memory - Compact flash memory
		DVD/CD	<p>Export to DVD/CD is prohibited. Initial Value: Not selected</p>
		Network	<p>Export to network drive is prohibited. Initial Value: Not selected</p>
	Clear All		Clear all the selections for the settings of the prohibited drive (export destination) and Specify drive type .
Select All		Select all for the settings of the prohibited drive (export destination) and Specify drive type .	

 **Note**

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

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 USB devices registered in the USB Device Registration window of the Management Control.</p> <p>Refer to "7.5.2 Register USB device" of "7.5 Export Files to Specified USB Device Only" for the method of adding USB devices.</p>
Do not Use Initial Value	<p>When exporting files and folders using File Export Utility, follow the policies set in File Export Utility.</p> <p>In addition, the writing and reading with Explorer, etc. should follow the policies set in Explorer.</p>
Details	<p>The File Export Prohibition - USB Device Individual Identification Function - Detailed Settings window will be displayed.</p> <p>(Set the access condition for the administrator to use the allowed USB device, as well as adding and deleting the allowed USB device.)</p>

File Export Utility function setting window

The conditions of using File Export Utility can be set.

File Export Prohibition - File Export Utility function setting

Settings of File Export Utility function

- Unable to start the format function
- Display only removable device and DVD/CD as export destination
- Enter the reason for export

Set the date on which File Export Utility can be started

- Limit period for use
 / / ~ / / (YYYY/MM/DD)
- Limit time for use
 : ~ : (HH:mm)

The day of a week on which it can be used

Sun Mon Tue Wed Thu Fri Sat The day of a week that is not selected has nothing to do with the above setting Unable to use.

Date and Time Confirmation Method

Inquire Management Server

Date and time when CT is used

Detailed Settings of Encryption Export

Password length

Minimum number of characters

Maximum number of characters

Decryption Restriction

- Number of Password Attempts
- Number of days to decrypt

Extension of encrypted file

exe Specify an extension

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"> - Format Drive - Erase CD-RW/DVD-RW <p>When it is not selected: (Initial Value) 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: (Initial Value) During file export, all export destinations will be displayed.</p>
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: (Initial Value) 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: - 1st, January, 2000 ~ 31st, December, 2037</p> <p>When it is not selected: (Initial Value): 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: (Initial Value): 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. (Initial Value): All are selected.</p>
Date and Time Confirmation Method	<p>Inquire Management Server (Initial Value):</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"> - 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. - Unable to start when it is unable to obtain (Initial Value): The File Export Utility cannot be started.
	<p>Date and Time when CT is used</p> <p>The date and time when the File Export Utility can be started is based on the date and time of the CT.</p>

File access control - Detailed Settings window

File Access Control - Detailed Settings

Set excluded folder for network drive access prohibition

Folder Name	Notes

Folder Name View

Notes

Add/Update Delete

Number of registrations 0 items (maximum 50 items)
 Number of registered characters 0 Characters (maximum 500 characters)
 *The number of characters is calculated based on halfwidth characters

Set Cancel

Item Name	Description
Set excluded folder for network drive access prohibition	The folder excluded from network drive access prohibition can be set.
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:) Specify up to 260 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). The following characters cannot be specified: "/", ":", "*", "?", " ", "<", ">", " " In addition, "\" cannot be specified at the end of path. Initial Value: No specification Refer to " 1.2.45 IPv6 Support " for details on specifying an IPv6 address.
View	The dialog for selecting the excluded folder can be displayed.
Notes	Enter the information such as memo. Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). Initial Value: No specification
Number of registrations	The number of registered cases displayed in the list and the maximum number of registrations possible are displayed. A maximum of 50 cases can be registered.

Item Name	Description
Number of registered characters	The number of characters that can be used for the folder name is limited to a maximum of 500 halfwidth (250 fullwidth) characters. The number of characters used for the registered folder names is converted to halfwidth characters and displayed.
Add/Update	Add an excluded folder. Up to 50 cases can be added. In addition, all folder paths cannot exceed 500 halfwidth (250 fullwidth) characters 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 previous window.
Cancel	Do not save the settings and close the window.

File Export Prohibition - USB Device Individual Identification Function - 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. If the Management Server and client (CT) cannot communicate, USB devices that have been used in the past can be used. No: (Initial Value) Whether each USB device can be used or not can be set.
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.

Item Name	Description
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 Reading and writing are limited to File Export Utility check box and the Writing is limited to File Export Utility check box. When neither is selected, the registered USB devices can be read and written using File Export Utility and Explorer, etc. (Not File Export Utility).
Reading and writing are limited to File Export Utility	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.
Writing is limited to File Export Utility	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 .
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
Add Device	The File Export Prohibition - Detailed Settings of USB Device Individual Identification Function - Select USB device 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.

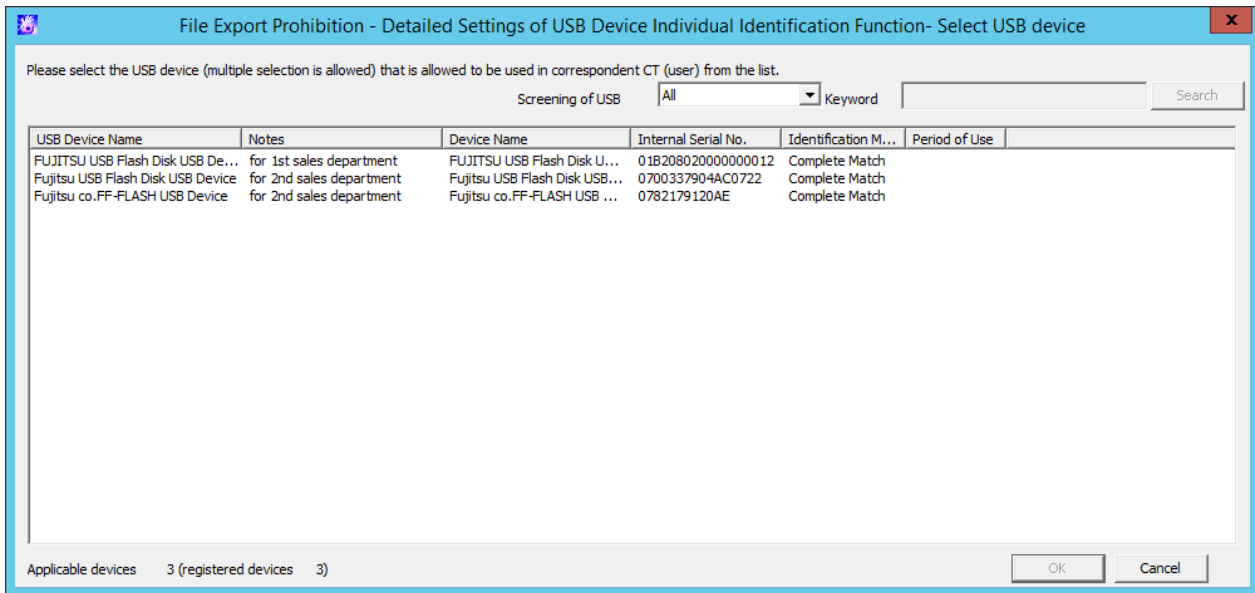
When adding an available USB device

Click the **Add Device** button.

File Export Prohibition - Detailed Settings of USB Device Individual Identification Function - Select 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 - USB Device Individual Identification Function - Detailed Settings window](#).



Item name	Description
Screening of USB	<p>The USB devices to be displayed in List of USB Devices can be filtered. Select from the following:</p> <ul style="list-style-type: none"> - All (default value) Displays all USB devices. - USB Device Name Searches the string entered in Keyword for partial matches, and displays USB devices. - Device Name Displays the string entered in Keyword in partial matches. - Internal Serial No. Displays the string entered in Keyword in partial matches. - Identification Method Displays the string entered in Keyword in partial matches. The strings that can be entered are as follows: <ul style="list-style-type: none"> - Complete Match - Product Match - Serial No. Match - Not Available <p>Notes Displays the string entered in Keyword in partial matches.</p>
Keyword	<p>Specifies the search conditions for the USB devices to be displayed.</p> <p>Specify up to 128 halfwidth and fullwidth characters.</p>
Search	<p>Performs USB device search using the conditions specified in Screening of USB Device and Keyword.</p>

 **Note**

Depending on the type of portable device/imaging device, the communication mode may be automatically set during connection to the PC, or you may be able to select it from the menu. Either of the following connections will be established but the configured **Access Settings** may not be enabled depending on the communication mode.

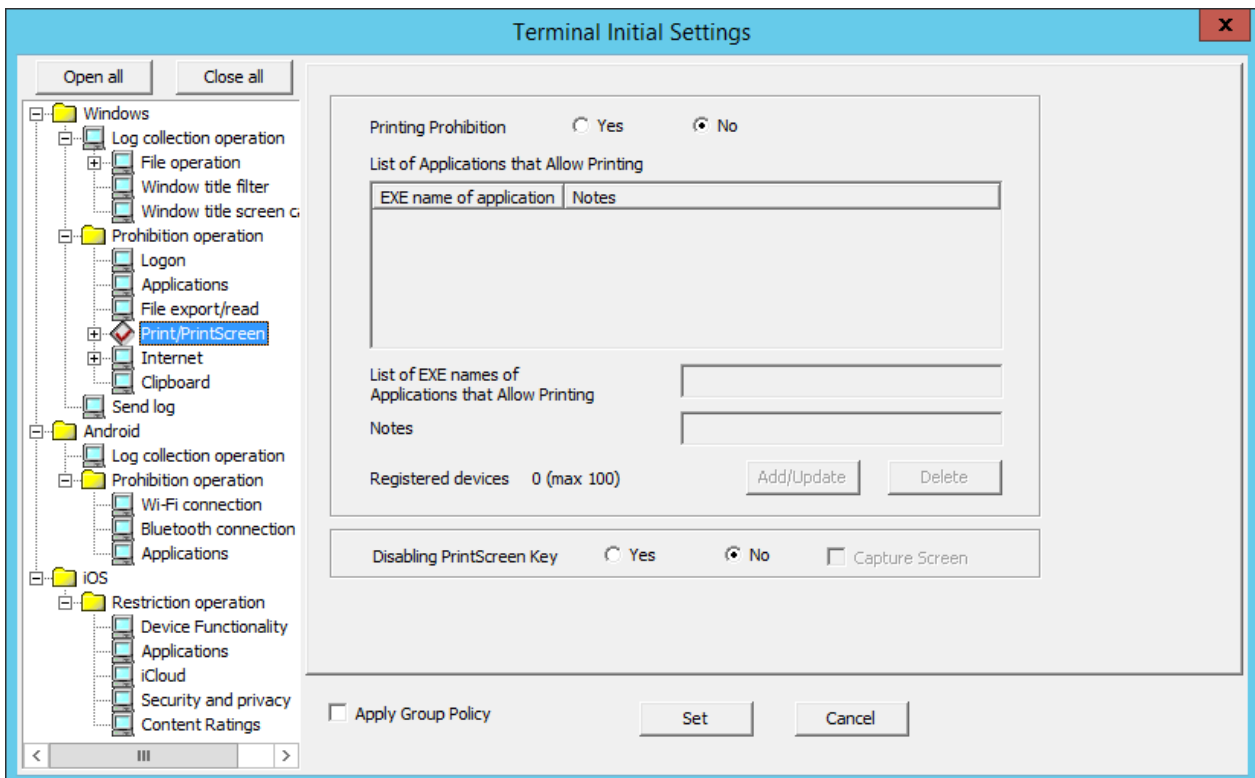
Recognition method	Access behavior
Drive letter assigned	Normally, the drive type for portable devices/imaging devices is recognized as Removable , and the device behaves according to Read-only or Read and Write set in the access settings configured in the Detailed Settings window. If the drive type for the inserted portable device/imaging device is recognized as DVD/CD , the device will behave as configured in the Reading prohibition > DVD/CD setting or Export Prohibition > Specify drive type > DVD/CD settings.
Drive letter not assigned	If connection is allowed, the device will behave according to Read and Write irrespective of the access settings. Whether the data can actually be written depends on the specification of the device connected. If, for example, a digital camera is connected, image data can be viewed and deleted but generally cannot be written. Data cannot be written from the File Export Utility because no drive letter is assigned.

If dedicated software provided by the device manufacturer is used for communication, read prohibition may not be enabled.

2.4.1.9 Print/PrintScreen

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 **Print/PrintScreen**.

The following section describes the settings of **Print/PrintScreen**.



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 (Initial Value)	Printing is not prohibited.
List of Applications that Allow Printing		The set EXE Name of Application that Allow Printing will be displayed. Initial Value: 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(R) Excel) Up to 254 single-byte characters (127 double-byte characters) can be entered. (Alphabetic characters are not case-sensitive.) However, if the following symbols are used, error will occur. " \ " / " " : " * " ? " " " " < " > " " Initial Value: No specification will be made.
Notes		Enter the application name and memo information. Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). Initial Value: No specification will be made.
Registered devices		The number of registered cases and the maximum number of registrations possible are displayed.
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.
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 Windows > Log collection operation 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.

2.4.1.10 Eco Monitoring

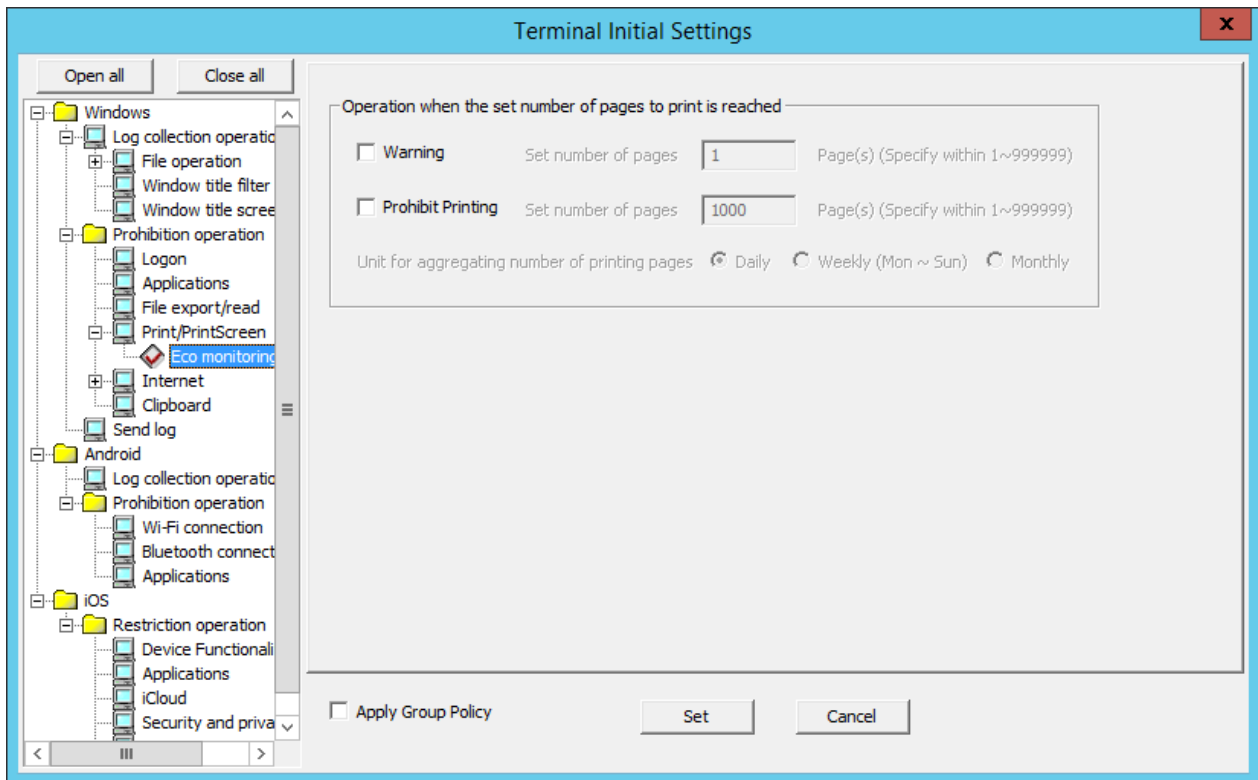
By monitoring the printed pages, the conditions can be set in **Eco monitoring** to reduce unnecessary printing.

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 **Windows > Log collection operation**, 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 **Eco monitoring** will be processed as CT policy.



Operations when the set number of pages to print is reached

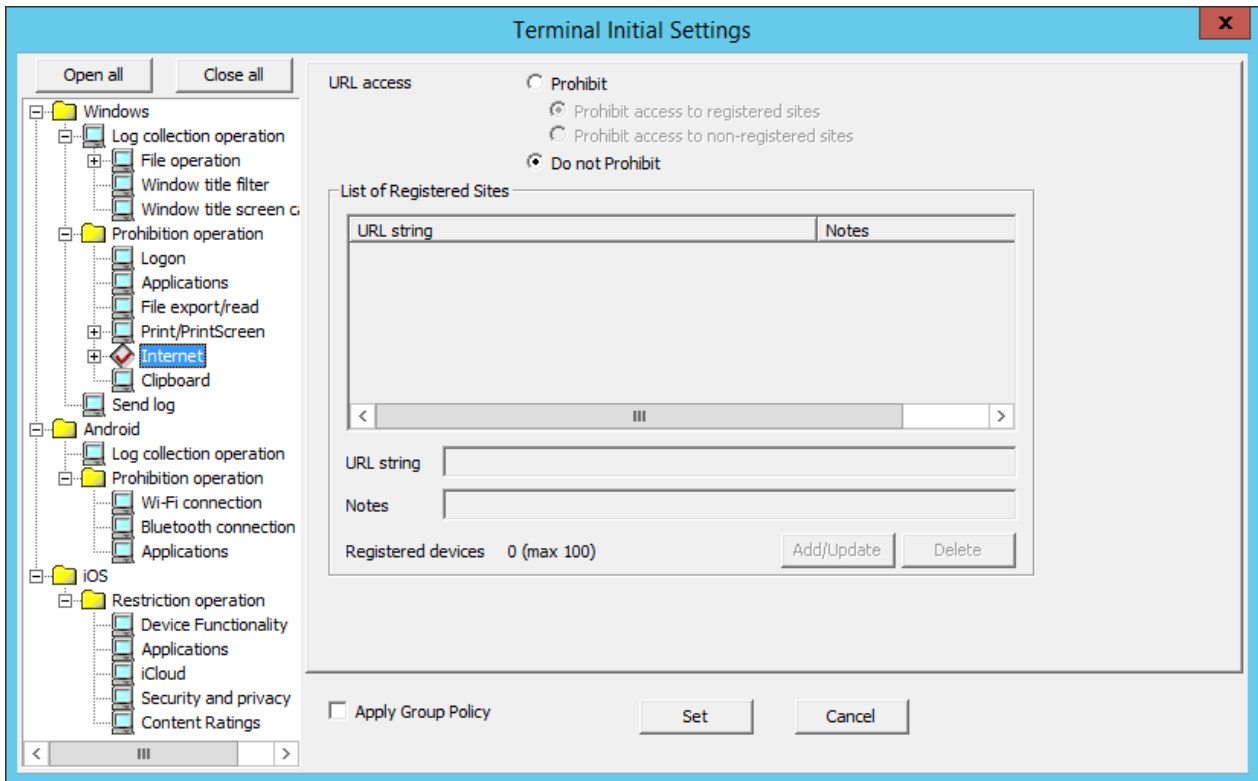
Item Name	Instruction
Warning (*)	<ul style="list-style-type: none"> - When this is selected: When the set number of printed pages is reached, the warning message will be displayed. It will be recorded as a printing operation log. The actions of a document writer (Microsoft(R) Office Document Image Writer, Adobe PDF, etc.) that does not print on paper will be counted as printed pages. - 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.

Item Name		Instruction
		<ul style="list-style-type: none"> - When this is not selected (Initial Value): Though the printing pages can be counted, the messages cannot be displayed.
Prohibit Printing (*)		<ul style="list-style-type: none"> - 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 Print/PrintScreen cannot print. The printing for a document writer (Microsoft(R) 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. <ul style="list-style-type: none"> - Set number of pages: the set scope of the number of pages that triggers printing prohibition is 1-999999. The initial value is 1000. - When this is not selected: (Initial Value) Though the printing pages will be counted, the printing will not be prohibited.
Unit for aggregating number of printed pages	Daily (Initial Value)	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,
input the set number of pages in **Warning** =< the set number of pages in **Prohibit Printing**.

2.4.1.11 Internet

The URL prohibited from being accessed can be set in **Internet**.

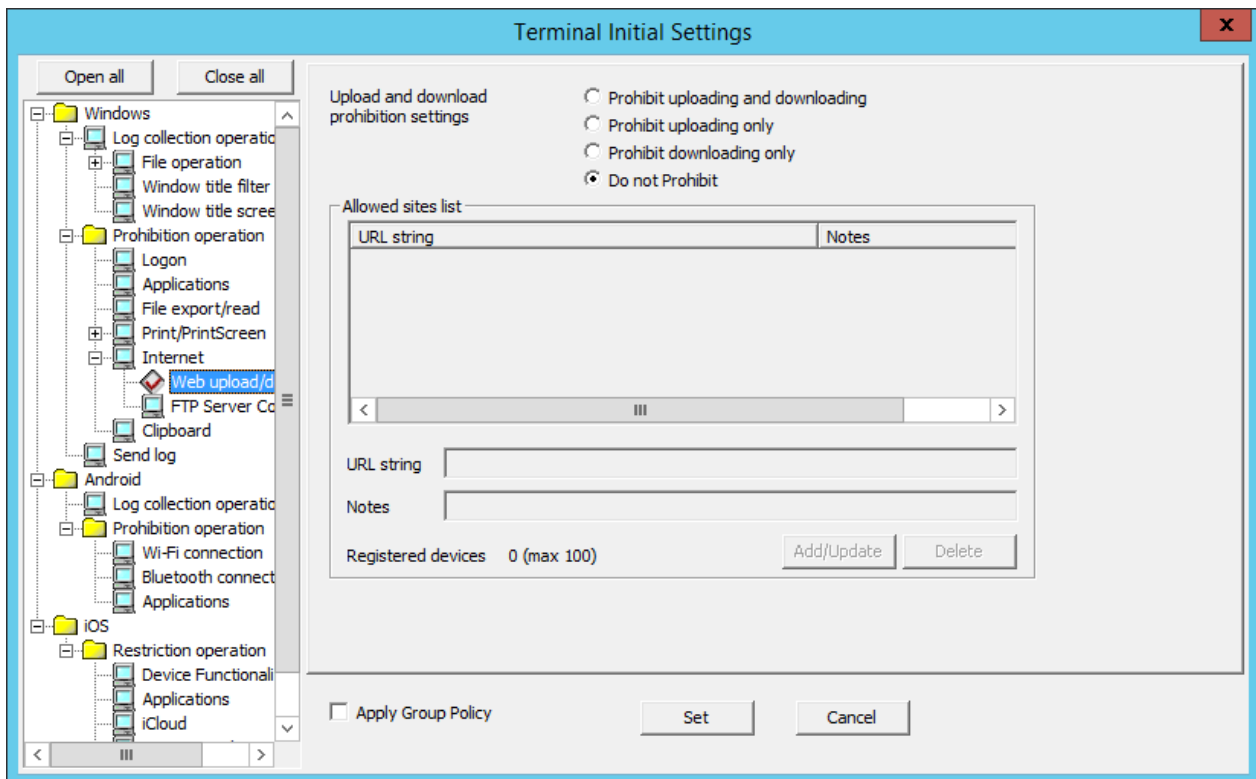


Item Name		Description
URL access	Prohibit	Access to URL is prohibited.
	Prohibit access to registered sites	Access to the URL specified in List of Registered Sites is prohibited.
	Prohibit access to non-registered sites	Access to the URL other than the one specified in the List of Registered Sites is prohibited.
	Do not Prohibit (Initial Value)	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. Initial Value: 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 1] When fujitsu.com is set in the URL string , the following address will be prohibited or allowed. http://www.fujitsu.com/global/ [Example 2] If "10.10.10.10" is prohibited in the settings in URL string , the following will be prohibited. http://10.10.10.10 The following will not be prohibited even if the IP address for jp.fujitsu.com is "10.10.10.10". http://jp.fujitsu.com If you want to prohibit "http://jp.fujitsu.com", the strings included in prohibited URLs, such as "jp.fujitsu.com", must be specified. Up to 254 single-byte alphanumeric characters and symbols can be entered (Alphabetic characters are not case-sensitive)

Item Name	Description
	<p>The valid symbols of URL are as follows: "" "" "." "-" "_" "(" " " _ ":" "% " "+"</p> <p>Halfwidth katakana, control characters, and spaces cannot be specified.</p> <p>A multi-byte character domain name cannot be used.</p> <p>Up to 100 cases can be registered.</p> <p>Refer to "1.2.45 IPv6 Support" for details on IPv6 addresses.</p> <p>Initial Value: Not Specified.</p>
Notes	<p>Enter the information such as the memo of URL.</p> <p>Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters).</p> <p>Initial Value: Not Specified.</p>
Registered devices	<p>The number of registered cases and the maximum number of registrations possible are displayed.</p>
Add/Update	<p>URL will be added.</p> <p>Up to 100 cases can be added.</p> <p>After modifying Notes the lines selected in List of Registered Sites, the information can be updated (The URL string cannot be updated.)</p>
Delete	<p>The lines selected in List of Registered Sites will be deleted.</p>

2.4.1.12 Web Upload/Download

The Web upload and download operations permitted by the administrator can be set in **Web upload/download**.



Item Name	Description
Upload and download	<p>Prohibit uploading and downloading</p> <p>- Client (CT) for V14.2.0 or later</p>

Item Name	Description
prohibition settings	Prohibits uploading and downloading from websites other than those specified in Allowed sites list. <ul style="list-style-type: none"> - Client (CT) for V14.1.0 Prohibits downloading from websites other than those specified in Allowed sites list. Uploading will not be prohibited for any website. <ul style="list-style-type: none"> - Client (CT) for versions other than the above Neither uploading nor downloading will be prohibited for any website.
	Prohibit uploading only <ul style="list-style-type: none"> - Client (CT) for V14.3.0 or later Prohibits uploading from websites other than those specified in Allowed sites list. Downloading will not be prohibited for any website. <ul style="list-style-type: none"> - Client (CT) for V14.2.0 Prohibits uploading and downloading from websites other than those specified in Allowed sites list. <ul style="list-style-type: none"> - Client (CT) for V14.1.0 Prohibits downloading from websites other than those specified in Allowed sites list. Uploading will not be prohibited for any website. <ul style="list-style-type: none"> - Client (CT) for versions other than the above Neither uploading nor downloading will be prohibited for any website.
	Prohibit downloading only <ul style="list-style-type: none"> - Client (CT) for V14.3.0 or later Prohibits downloading from websites other than those specified in Allowed sites list. Uploading will not be prohibited for any website. <ul style="list-style-type: none"> - Client (CT) for V14.2.0 Prohibits uploading and downloading from websites other than those specified in Allowed sites list. <ul style="list-style-type: none"> - Client (CT) for V14.1.0 Prohibits downloading from websites other than those specified in Allowed sites list. Uploading will not be prohibited for any website. <ul style="list-style-type: none"> - Client (CT) for versions other than the above Neither uploading nor downloading will be prohibited for any website.
	Do not Prohibit (Default value) <p>Uploading and downloading from any website are allowed.</p>
Allowed sites list	URLs of the websites for which uploading and downloading are allowed, and notes about these URLs are displayed. <p>Up to 100 URLs can be registered.</p> <p>Default value: No value is displayed.</p>
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. <p>[Example 1] When fujitsu.com is set in the URL string, all the following addresses are permitted.</p> <p>http://www.fujitsu.com/global/</p>

Item Name	Description
	<p>Example 2: If "10.10.10.10" is specified in URL string, the following will be allowed. http://10.10.10.10 (Allowed)</p> <p>The following will be prohibited if the IP address for jp.fujitsu.com is "10.10.10.10": http://jp.fujitsu.com (Not allowed)</p> <p>Example 3: If "/desktopkeeper" is specified in URL string, the following will be allowed. http://www.soft.fujitsu.com/desktopkeeper/ (Allowed) http://jp.fujitsu.com (Not allowed)</p> <p>Up to 254 single-byte alphanumeric characters and symbols can be entered. (Alphabetic characters are not case-sensitive) The valid characters of URL are as follows: "" ". " - ") " (" _ " : " / " + " ["] "</p> <p>A multi-byte character domain name cannot be used. Up to 100 cases can be registered. To specify an IPv6 address, enclose the address in []. Example: http://[2001:db8::1]</p> <p>To set the path part only, "/" must be specified at the beginning. Example: /desktopkeeper</p> <p>Initial Value: Not Specified.</p>
Notes	<p>Enter the memo information of the URL that allows upload and download. Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters). Initial Value: Not Specified.</p>
Registered devices	<p>The number of registered cases and the maximum number of registrations are displayed.</p>
Add/Update	<p>The URL of the Web site that allows upload and download will be added. Up to 100 cases can be added.</p> <p>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.).</p>
Delete	<p>The lines selected in the List of sites allow uploading and downloading will be deleted.</p>



Note

Client (CT) for V14.1.0 and V14.2.0 when the path part is included in the URLs set for the allowed sites

In V14.3.0 or later (Master) Management Server/Management Console, the path part can be included in the URLs set for the allowed sites. (Example: jp.fujitsu.com/solutions)

If operation is performed with a policy in which the path part is included in the URLs set for the allowed sites. However, uploading and downloading to and from the allowed sites will not be allowed on the client (CT) for V14.1.0 and V14.2.0. In this case, specify the host name part of the URL ("jp.fujitsu.com" in "jp.fujitsu.com/solutions") as the URL of the allowed site.

Example:

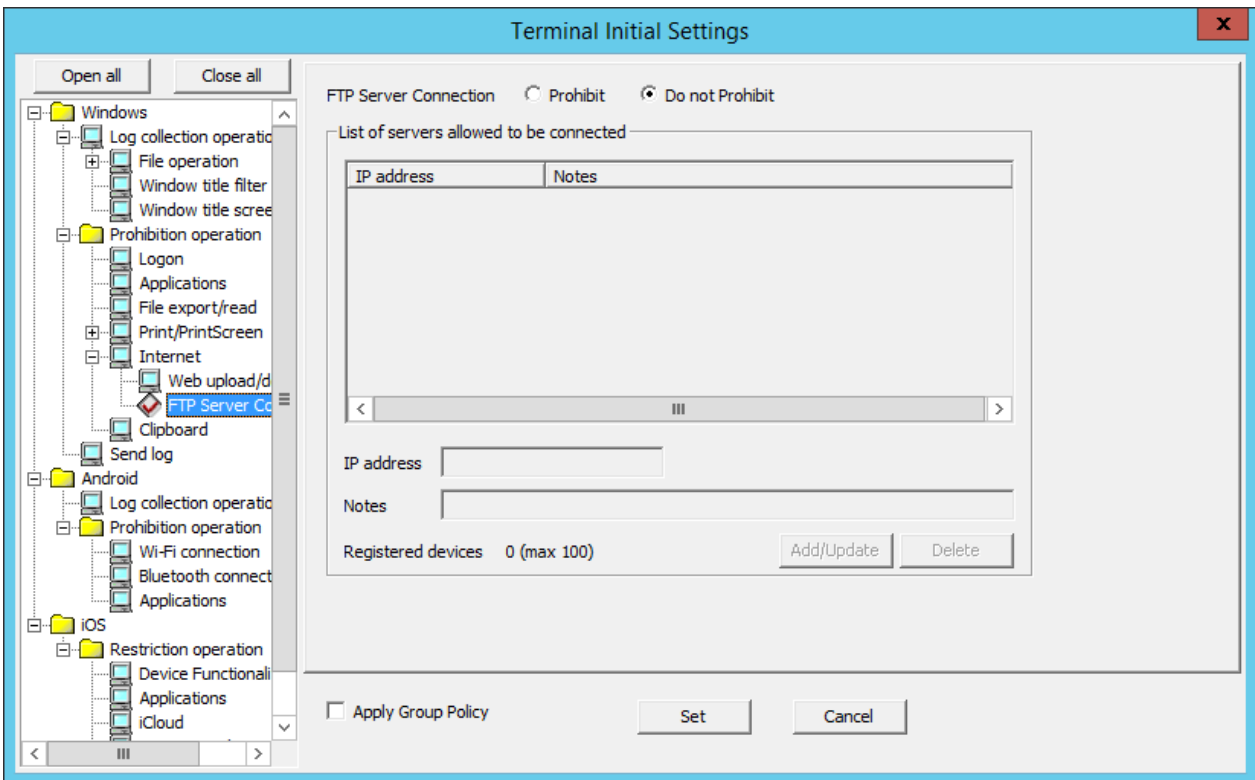
Upload and download prohibition settings: Settings other than **Do not Prohibit**

URL of the allowed site set: jp.fujitsu.com/solutions

- If the URL of the website accessed is "http://jp.fujitsu.com/download.html"
 - Client (CT) for V14.3.0 or later: Would determine that it is not an allowed site.
 - Client (CT) for V14.1.0 and V14.2.0: Would determine that it is not an allowed site.
- If the URL of the website accessed is "http://jp.fujitsu.com/solutions/download.html"
 - Client (CT) for V14.3.0 or later: Would determine that it is an allowed site.
 - Client (CT) for V14.1.0 and V14.2.0: Would determine that it is not an allowed site.

2.4.1.13 FTP Server Connection

Prohibition of the connection to the FTP server which is not permitted by the administrator can be set in **FTP Server Connection**. To prohibit the connection to FTP server from Internet Explorer(R), set in **Internet**.

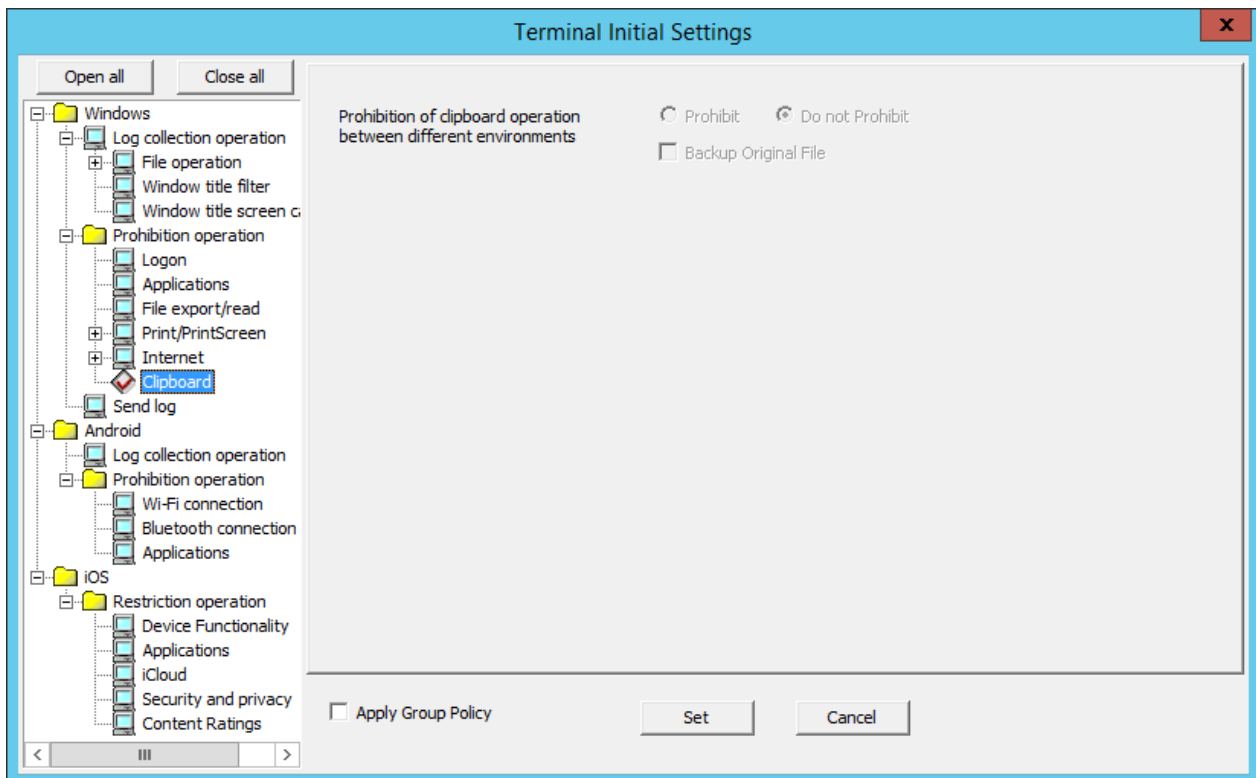


Item Name		Description
FTP Server Connection	Prohibit	Prohibit the access to the servers that is not specified in the List of servers allowed to be connected .
	Do not Prohibit (Initial Value)	Any FTP server can be connected.
List of servers allowed to be connected		The IP address of FTP server allowed to be connected and the memo related to the server to be connected are displayed. Initial Value: Not Displayed.
IP address		Enter the IP address (IPv4/IPv6 format) of the server to be connected. For IPv4 addresses, specify up to 45 halfwidth numeric characters and periods. For IPv6 addresses, specify up to 45 halfwidth hexadecimal characters and colons. Up to 100 cases can be registered.

Item Name	Description
	Refer to " 1.2.45 IPv6 Support " for details on registration with IPv6 addresses. Initial Value: 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. Initial Value: Not Specified.
Number of registrations	The number of registered cases and the maximum number of registrations possible are displayed.
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.

2.4.1.14 Clipboard

The clipboard operation prohibition can be set in **Clipboard**.



Item Name	Description
Prohibition of clipboard operation between different environments	When the Clipboard Operation Log (Virtual Environment) option in Windows > Log collection operation 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.

Item Name	Description
Backup Original File	<p>When the option of Prohibition of clipboard operation between different environments is Prohibit, the item can be set.</p> <p>When this is selected: The information (text, image) copied from the clipboard will be backed up as the original file.</p> <p>When this is not selected: (Initial Value) The information (text, image) copied from the clipboard will not be backed up as the original file.</p>

2.4.1.15 Send Log

The method of sending operation logs from the client (CT) to the Management Server can be set in **Send log**. The sent logs are operation logs, prohibition logs and attached data.



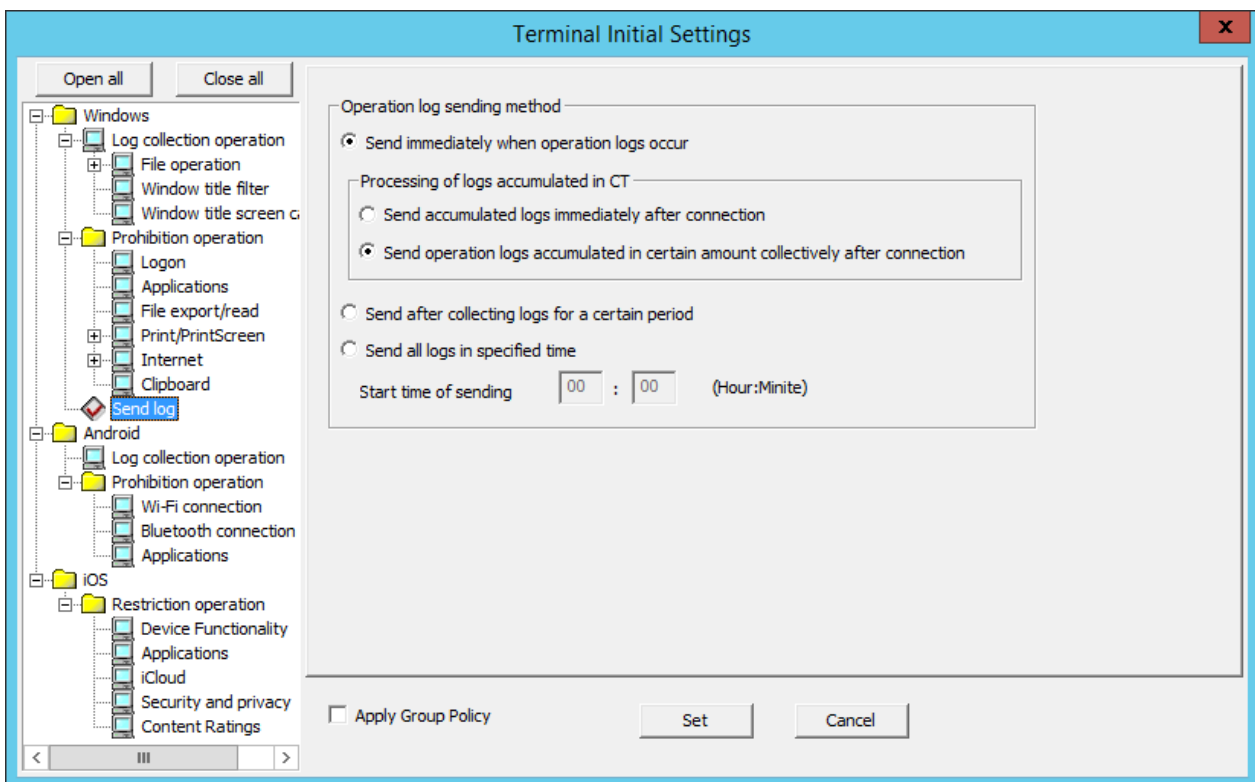
Note

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

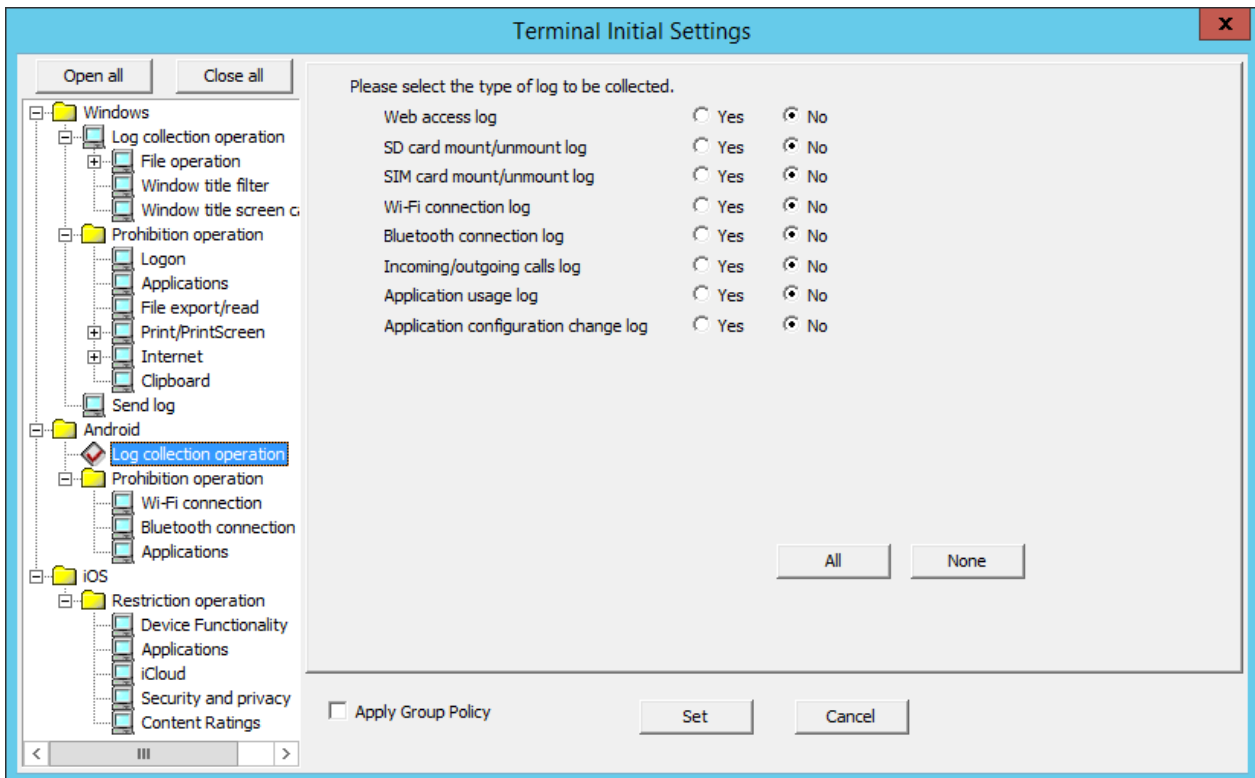
Item Name	Description
Send immediately when operation logs occur (Initial Value)	Logs will be sent to the server immediately when they are generated.
Processing of logs accumulated in CT	<p>Set the method of sending the logs accumulated in the client (CT) due to reasons such as a mobile application immediately when the network connects to the server.</p> <p>If operation logs are generated, they will be accumulated at the time, and sent to the server every 10 seconds. Violation logs, on the other hand, are sent when they are generated. When connecting to the network, operation logs accumulated during disconnection from the network are sent from the client (CT) to the server every 10 seconds from the time of connection (the communication with the Management Server or Master Management Server is started). Accumulated violation logs are sent every 0.5 seconds per log. The number of accumulated logs to be sent at one time is set in Maximum number of logs can be sent at one time in the Terminal Operation Settings window. Refer to "2.4.2 Perform Terminal Operation Settings" for details.</p> <p>If operation logs are generated, they will be accumulated at the time, and then sent to the server in a regular interval. Violation logs, on the other hand, are sent when they are generated. When connecting to the network, a certain number of operation logs accumulated during disconnection from the network are sent from the client (CT) to the server at a regular interval from the time of connection (the communication with the Management Server or Master Management Server is started). Accumulated violation logs are sent every 0.5 seconds per log. The amount of accumulated logs to be sent at one time and the interval for sending are set in the Terminal Operation Settings window. Refer to "2.4.2 Perform Terminal Operation Settings" for details.</p>
Send accumulated logs immediately after connection	
Send operation logs accumulated in certain amount collectively after connection	
Send after collecting logs for a certain period	The same behavior as when Send immediately when operation logs occur > Send operation logs accumulated in certain amount collectively after connection is selected.
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"> - The number of clients (CT number of sets): 1000 - Number of daily logs: 1000 - Time required for log sending: About 15 minutes at most <p>Example 2</p> <ul style="list-style-type: none"> - The number of clients (CT number of sets): 2000 - Number of daily logs: 1000 - Time required for log sending: About 30 minutes at most

Item Name	Description
	The number of logs to be sent at one time and the interval for sending are set in the Terminal Operation Settings window. Refer to " 2.4.2 Perform Terminal Operation Settings " for details.

2.4.1.16 Log Collection Operation (Android)

In **Android > Log collection operation**, specify whether to collect each log type. Select **Yes**, and the operation logs for the smart device (agent) will be collected.

The following describes the settings configured in **Android > Log collection operation**.

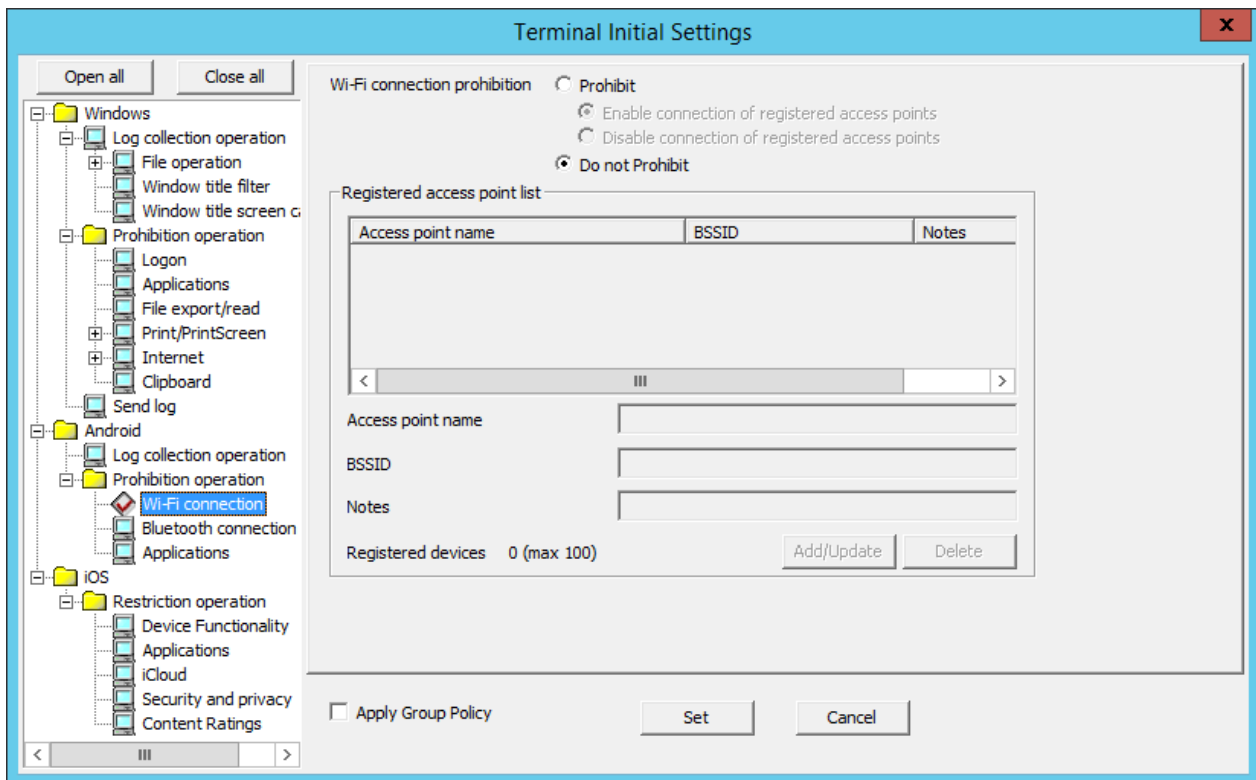


Item name	Description
Web access log	Logs accessed from standard browsers will be collected. Default value: No is selected.
SD card mount/unmount log	SD card mount/unmount logs will be collected. Default value: No is selected.
SIM card mount/unmount log	SIM card mount/unmount logs will be collected. Default value: No is selected.
Wi-Fi connection log	Wi-Fi connection/disconnection logs will be collected. Default value: No is selected.
Bluetooth connection log	Bluetooth connection/disconnection logs will be collected. Default value: No is selected.
Incoming/outgoing calls log	Phone numbers will be collected from the phone call history, and if the numbers are registered in the phonebook, then the names of those associated with the numbers will also be collected. Default value: No is selected.
Application usage log	Logs for applications used will be collected.

Item name	Description
	Default value: No is selected.
Application configuration change log	Application configuration change (install/uninstall) logs will be collected. Default value: No is selected.

2.4.1.17 Wi-Fi Connection

In **Wi-Fi connection**, specify the BSSID for the access point to prohibit Wi-Fi use.

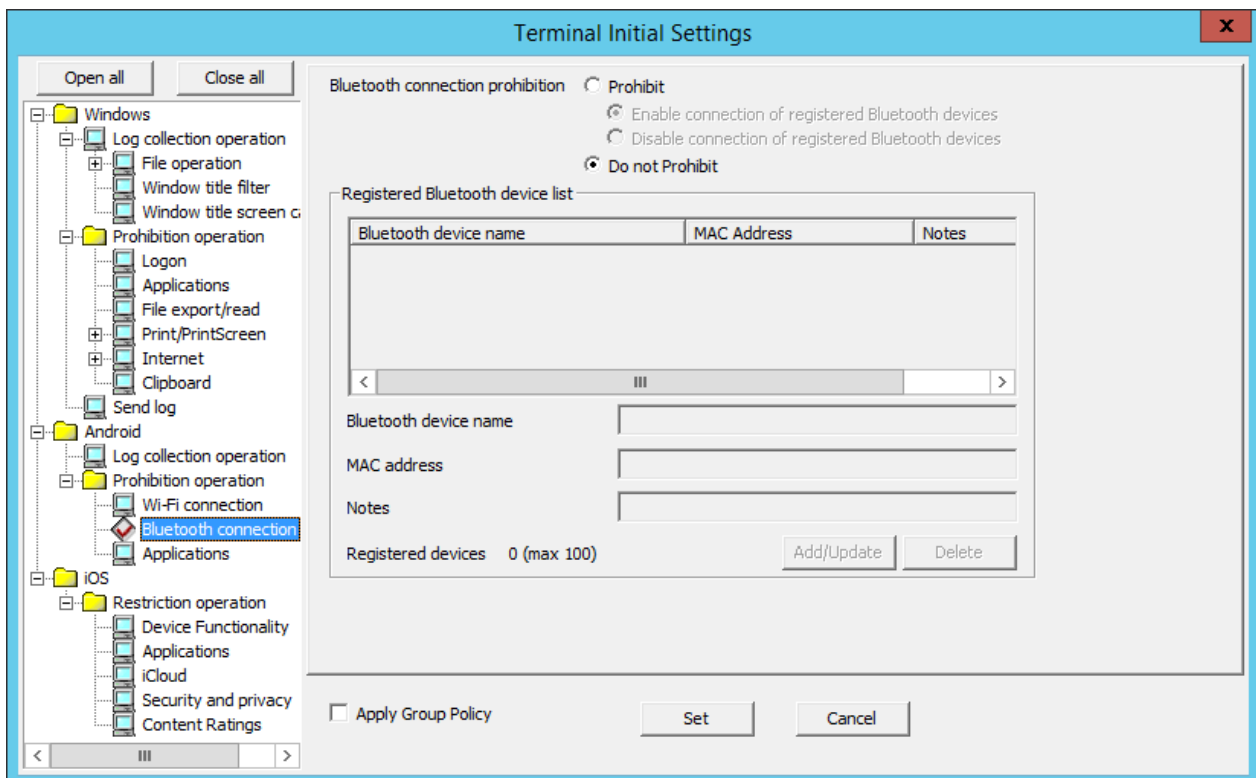


Item name	Description	
Wi-Fi connection prohibition	Prohibit	Prohibits connection to the access points specified in Registered access point list .
	Enable connection of registered access points	Enables connection to the access points specified in Registered access point list .
	Disable connection of registered access points	Disables connection to the access points specified in Registered access point list .
	Do not Prohibit (Default value)	Connection to any access point is possible.
Registered access point list	Displays the access point name, BSSID, and notes for the access points to which connection will be enabled or disabled. Default value: No value is displayed.	
Access point name	Enter the access point name. Specify up to 254 halfwidth (127 fullwidth) characters. Up to 100 names can be registered.	

Item name	Description
	Default value: No value is displayed.
BSSID	Enter the access point Basic Service Set Identifier (BSSID). The characters that can be entered comply with the BSSID convention. Enter the BSSID in the "XX:XX:XX:XX:XX:XX" or "XX-XX-XX-XX-XX-XX" format. ("X" denotes a halfwidth alphanumeric character while ":" and "-" denote halfwidth colon and halfwidth hyphen respectively.) (Example: 02:E0:32:33:A3:C0) Default value: No value is displayed.
Notes	Enter information such as notes on the access points to which connection is allowed. Specify up to 128 halfwidth (64 fullwidth) characters. Default value: No value is specified.
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
Add/Update	Adds access points to which connection will be allowed. Information will be updated when Access point name and Notes for the row selected in Registered access point list are changed. A new access point will be added when BSSID is changed.
Delete	Deletes the row selected in Registered access point list .

2.4.1.18 Bluetooth Connection

In **Bluetooth connection**, set the MAC address for Bluetooth devices on which Bluetooth use will be prohibited.

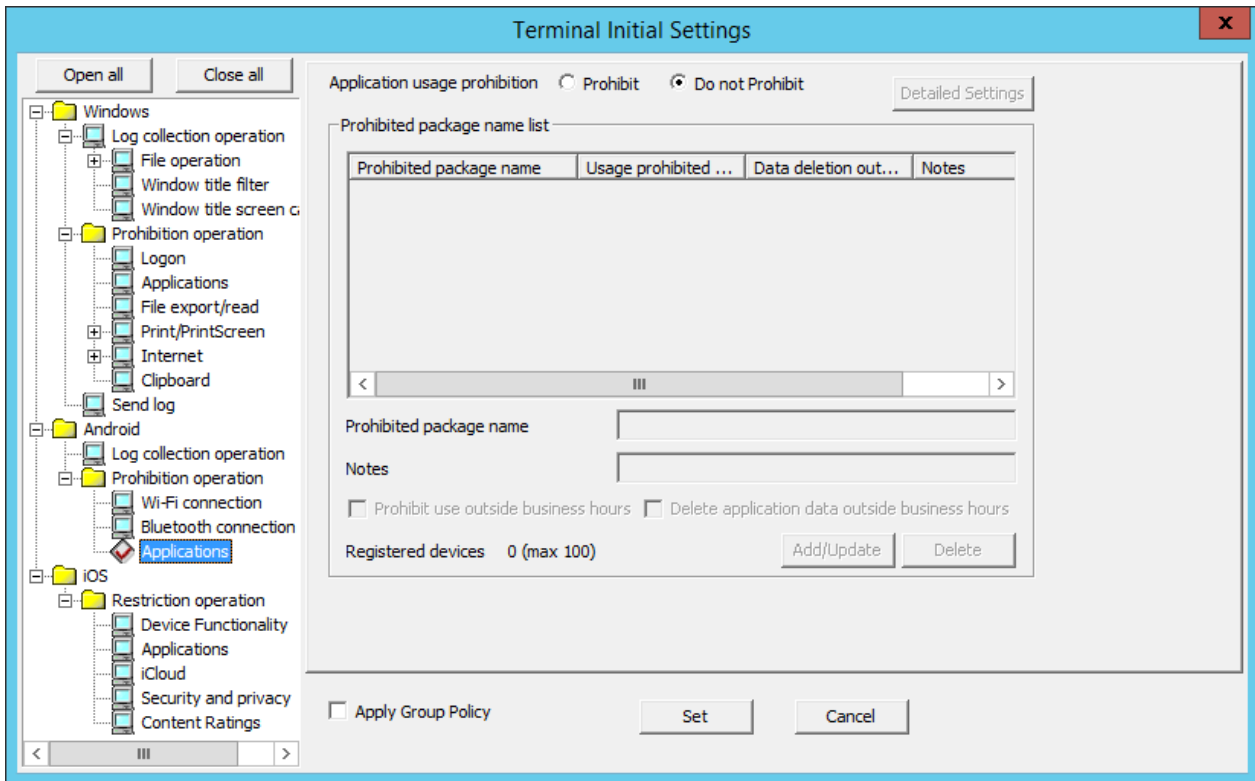


Item name		Description
Bluetooth connection prohibition	Prohibit	Prohibits connection to the Bluetooth devices specified in Registered Bluetooth device list .
	Enable connection of registered Bluetooth devices	Enables connection to the Bluetooth devices specified in Registered Bluetooth device list .
	Disable connection of registered Bluetooth devices	Disables connection to the Bluetooth devices specified in Registered Bluetooth device list .
	Do not Prohibit (Default value)	Connection to any Bluetooth device is possible.
Registered Bluetooth device list		Displays the Bluetooth device name, MAC address, and notes for the Bluetooth devices to which connection will be enabled or disabled. Default value: No value is displayed.
Bluetooth device name		Enter the Bluetooth device name. Specify up to 254 halfwidth (127 fullwidth) characters. Spaces can only be specified in-between characters. Up to 100 Bluetooth device names can be registered. Default value: No value is displayed. Control characters cannot be specified.
MAC address		Enter the MAC addresses for uniquely identifying Bluetooth devices. The characters that can be entered comply with the MAC address convention. Enter the MAC address in the "XX:XX:XX:XX:XX:XX" or "XX-XX-XX-XX-XX-XX" format. ("X" denotes a halfwidth alphanumeric character while ":" and "-" denote halfwidth colon and halfwidth hyphen respectively.) (Example: 02:E0:32:33:A3:C0) Default value: No value is displayed.
Notes		Enter information such as notes on the Bluetooth devices registered. Specify up to 128 halfwidth (64 fullwidth) characters. Default value: No value is specified.
Registered devices		The number of registered cases and the maximum number of registrations possible are displayed.
Add/Update		Adds Bluetooth devices to which connection will be allowed. Information will be updated when Bluetooth device name and Notes for the row selected in Registered Bluetooth device list are changed. A new Bluetooth device will be added when MAC address is changed.
Delete		Deletes the row selected in Registered Bluetooth device list .

2.4.1.19 Application (Android)

In **Android > Application**, set the package name for prohibited applications.

You can also set whether to prohibit use of specified applications outside business hours only, and whether to delete application data outside business hours, and so on.



Item name		Description
Application usage prohibition	Prohibit	Prohibits use of packages specified in Prohibited package name list .
	Do not Prohibit (Default value)	Any package can be used.
Prohibited package name list		Displays the package name and notes for the package to be prohibited. Default value: No value is displayed.
Prohibited package name		Enter the package name. The characters that can be entered comply with the package name convention. Entering of the extension (apk) is optional. Specify up to 254 halfwidth (127 fullwidth) characters. Spaces can only be specified in-between characters. Up to 100 package names can be registered. Default value: No value is displayed. Control characters cannot be used.
Notes		Enter information such as notes on the packages. Specify up to 128 halfwidth (64 fullwidth) characters. Default value: No value is specified.
Registered devices		The number of registered cases and the maximum number of registrations possible are displayed.
Prohibit use outside business hours		Select this to prohibit the use of specified packages outside business hours. Default value: Not selected. Refer to " 2.4.2 Perform Terminal Operation Settings " for details on the use outside business hours.
Delete application data outside business hours		Select this to delete the data of specified packages outside business hours. If packages for which this item is selected are installed, the following message will be output when outside business hours. This message will be output only once outside business hours. Until data deletion is completed, other operations cannot be performed.

Item name	Description
	<p>[AA10-WRN004]</p> <p>System administrator prohibits the use of the application outside business hours so the data will be deleted.</p> <p>Tap 'OK'. If the application screen appears, tap 'Clear data' to delete the data. The data in the following folders are deleted automatically:</p> <ul style="list-style-type: none"> - Folders used by the application - Any folders specified by system administrator <p>Default value: Not selected.</p> <p>Refer to "2.4.2 Perform Terminal Operation Settings" for details on the use outside business hours.</p>
detailed Settings	<p>Click this to delete data on external storage devices such as SD cards. When this item is clicked, the Application Usage Prohibition - Advanced Settings window will be displayed, and you will be able to specify a folder for the external storage on the Android device.</p> <p>The rule for entering the folder name is as follows:</p> <ul style="list-style-type: none"> - The folder name that can be entered complies with the folder path convention for Linux. - There is no specific character that cannot be used for the folder name. - Specify an absolute path (only a path starting with "/" can be entered) for the folder name. (*1) - The maximum length of the folder name that can be entered is 254 halfwidth (127 fullwidth) characters. - The maximum length of the note that can be entered is 128 halfwidth (64 fullwidth) characters. - The name is not case-sensitive.
Add/Update	<p>Adds or updates the packages to be prohibited.</p> <p>Information will be updated when Notes for the row selected in Prohibited package name list is changed. A new package will be added when Prohibited package name list is changed.</p>
Delete	<p>Deletes the row selected in Prohibited package name list.</p>

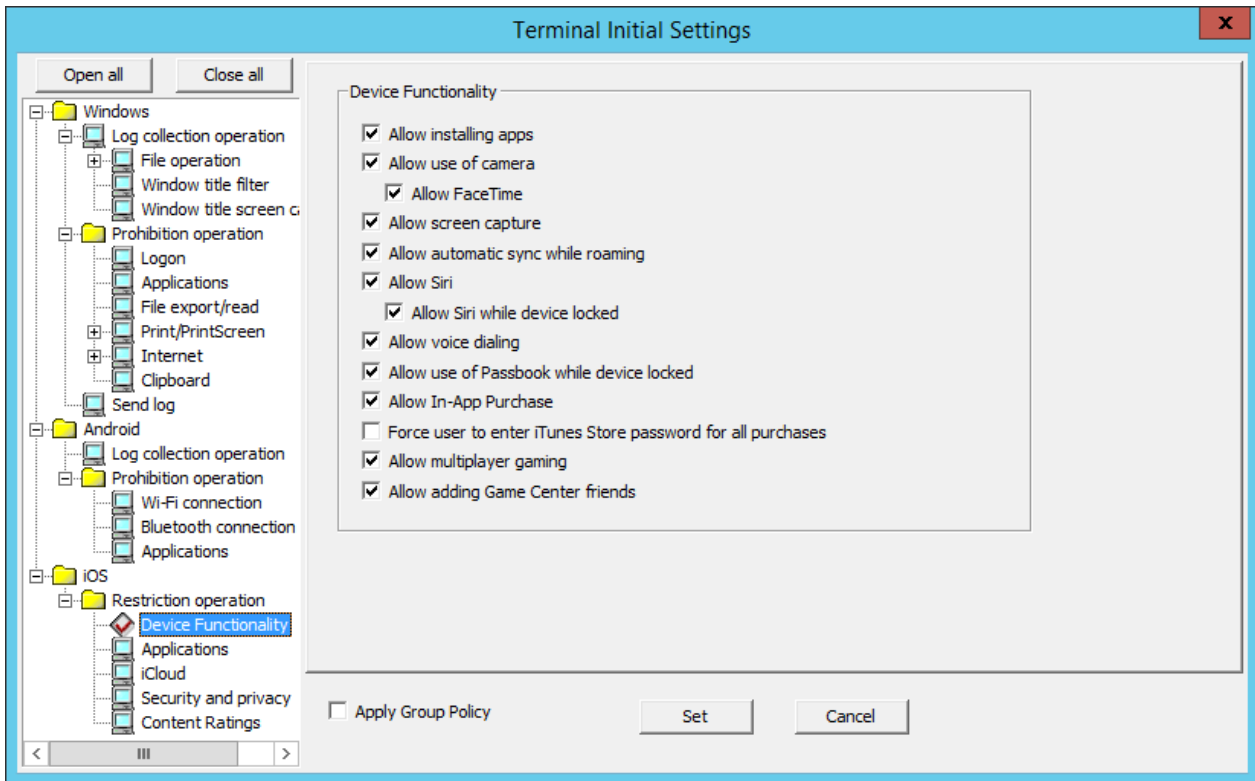
*1: The absolute path here means the absolute path from the SD cards.

An example is shown below.

- To delete files and folders under "/mnt/sdcard/temp/private":
Specify "/temp/private".
- To delete files and folders under "/mnt/external_sd/gyomu1/important":
Specify "/gyomu1/important".

2.4.1.20 Device Functionality

In **Device Functionality**, set the prohibition feature for iOS devices.

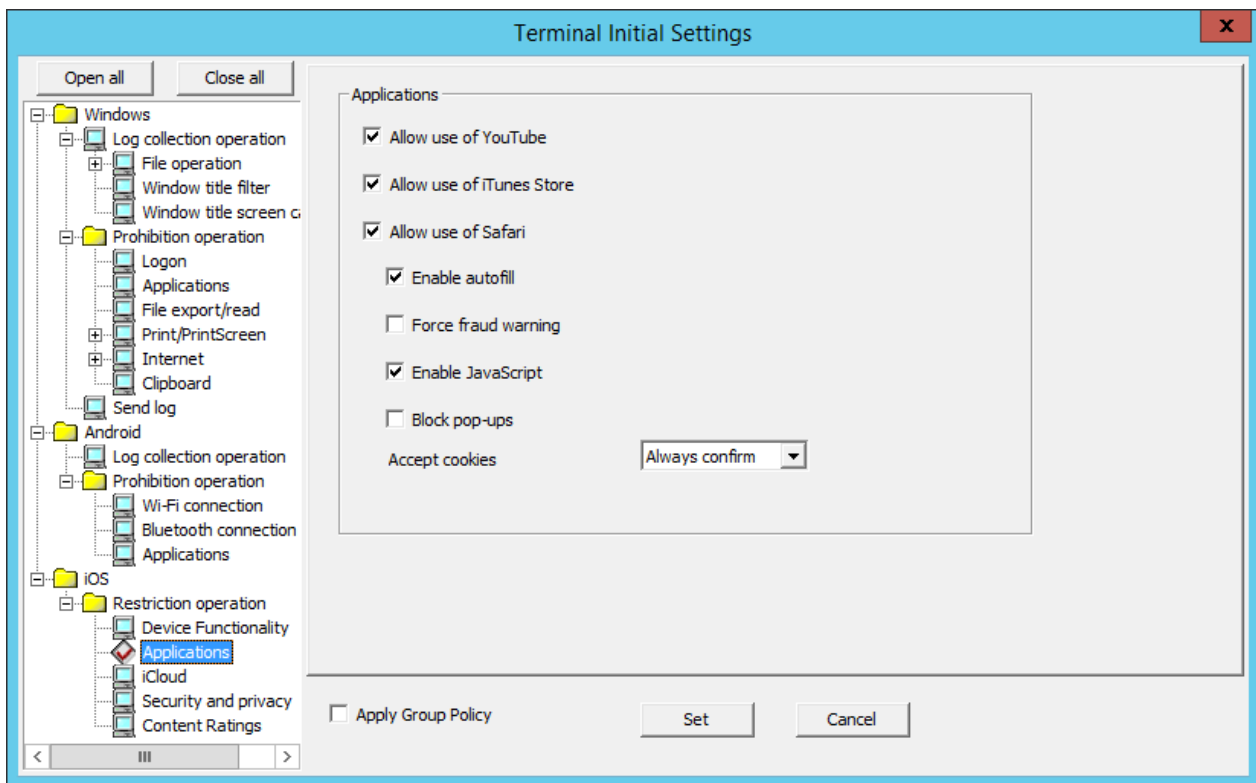


Item name	Description
Allow installation of apps	Specify whether to allow installation of applications. To prohibit it, clear this item. Default value: Selected.
Allow use of camera	Specify whether to allow use of the camera. To prohibit it, clear this item. Default value: Selected.
Allow FaceTime	Specify whether to allow FaceTime. To prohibit it, clear this item. Default value: Selected.
Allow screen capture	Specify whether to allow screen capture. To prohibit it, clear this item. Default value: Selected.
Allow automatic sync while roaming	Specify whether to allow automatic synchronization during roaming. To prohibit it, clear this item. Default value: Selected.
Allow Siri	Specify whether to allow Siri. To prohibit it, clear this item. Default value: Selected.
Allow Siri while device locked	Specify whether to allow Siri when the device is locked. To prohibit it, clear this item. Default value: Selected.
Allow voice dialing	Specify whether to allow voice dialing. To prohibit it, clear this item. Default value: Selected.
Allow use of Passbook while device locked	Specify whether to allow Passbook when the device is locked. To prohibit it, clear this item. Default value: Selected.

Item name	Description
Allow In-App Purchase	Specify whether to allow in-app purchases. To prohibit it, clear this item. Default value: Selected.
Force user to enter iTunes Store password for a purchases	Specify whether to force the user to enter iTunes Store password before any purchase. To force it, select this item. Default value: Not selected.
Allow multiplayer gaming	Specify whether to allow multiplayer gaming. To prohibit it, clear this item. Default value: Selected.
Allow adding Game Center friends	Specify whether to allow Game Center friends to be added. To prohibit it, clear this item. Default value: Selected.

2.4.1.21 Application (iOS)

In **iOS > Application**, set the prohibition feature for iOS applications.

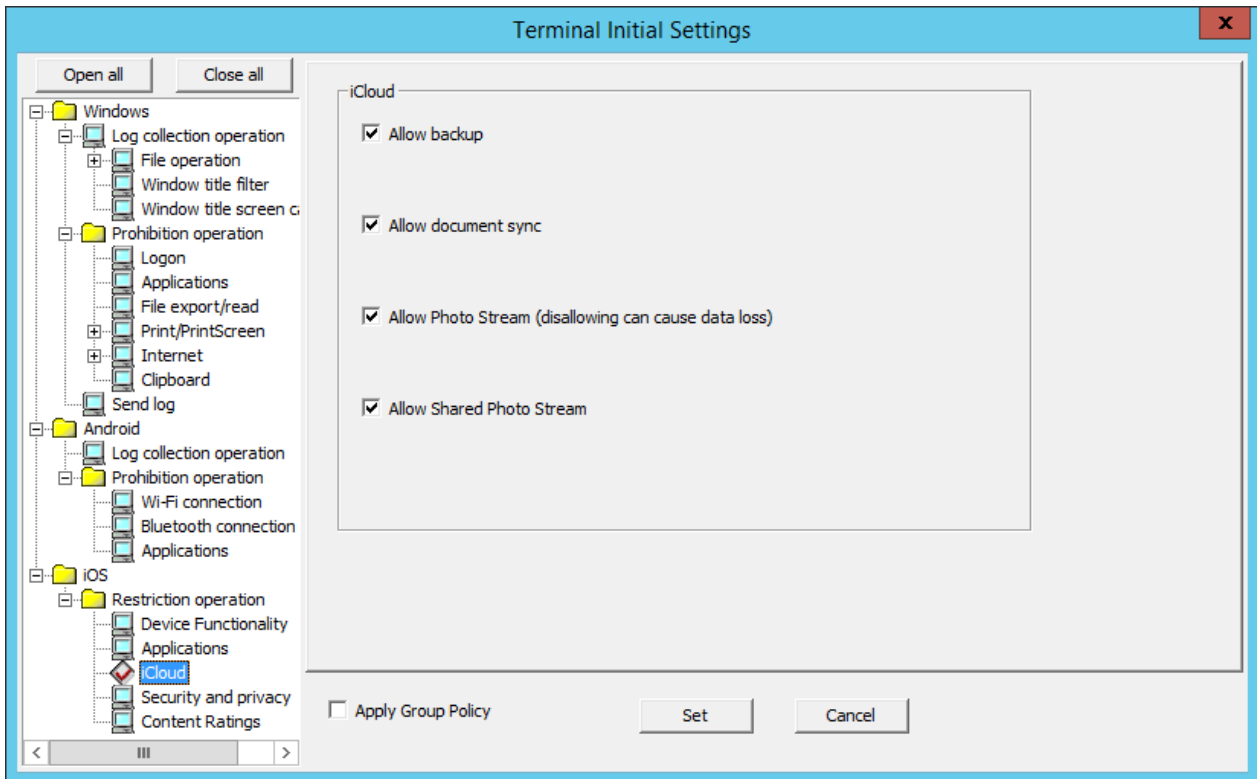


Item name	Description
Allow use of YouTube	Specify whether to allow use of YouTube. To prohibit it, clear this item. Default value: Selected.
Allow use of iTunes Store	Specify whether to allow use of the iTunes Store. To prohibit it, clear this item. Default value: Selected.
Allow use of Safari	Specify whether to allow use of Safari. To prohibit it, clear this item. Default value: Selected.

Item name	Description
Enable autofill	Specify whether to enable autofill. To disable it, clear this item. Default value: Selected.
Force fraud warning	Specify whether to allow access to suspicious websites. To prohibit it, clear this item. Default value: Not selected.
Enable JavaScript	Specify whether to enable JavaScript. To disable it, clear this item. Default value: Selected.
Block pop-ups	Specify whether to enable pop-ups. To disable it, clear this item. Default value: Not selected.
Accept cookies	Select from the menu to specify whether to enable cookies. <ul style="list-style-type: none"> - No Disables cookies. - From visited sites Disables cookies from websites other than those directly accessed. - Always confirm (Default value) Enables cookies.

2.4.1.22 iCloud

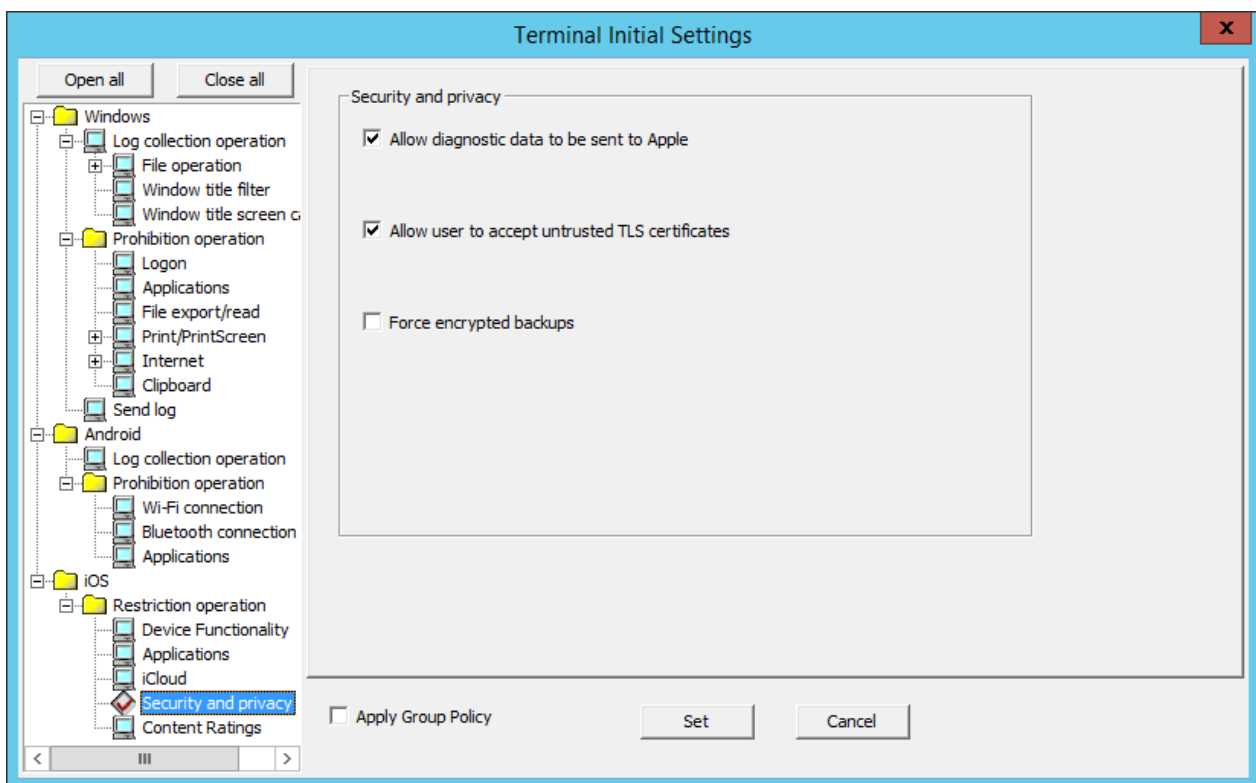
In **iCloud**, set the iCloud prohibition feature for iOS.



Item name	Description
Allow backup	Specify whether to allow backup to iCloud. To prohibit it, clear this item. Default value: Selected.
Allow document sync	Specify whether to allow document synchronization. To prohibit it, clear this item. Default value: Selected.
Allow Photo Stream (disallowing can cause data loss)	Specify whether to allow Photo Stream. To prohibit it, clear this item. Default value: Selected.
Allow Shared Photo Stream	Specify whether to allow shared Photo Stream. To prohibit it, clear this item. Default value: Selected.

2.4.1.23 Security and Privacy

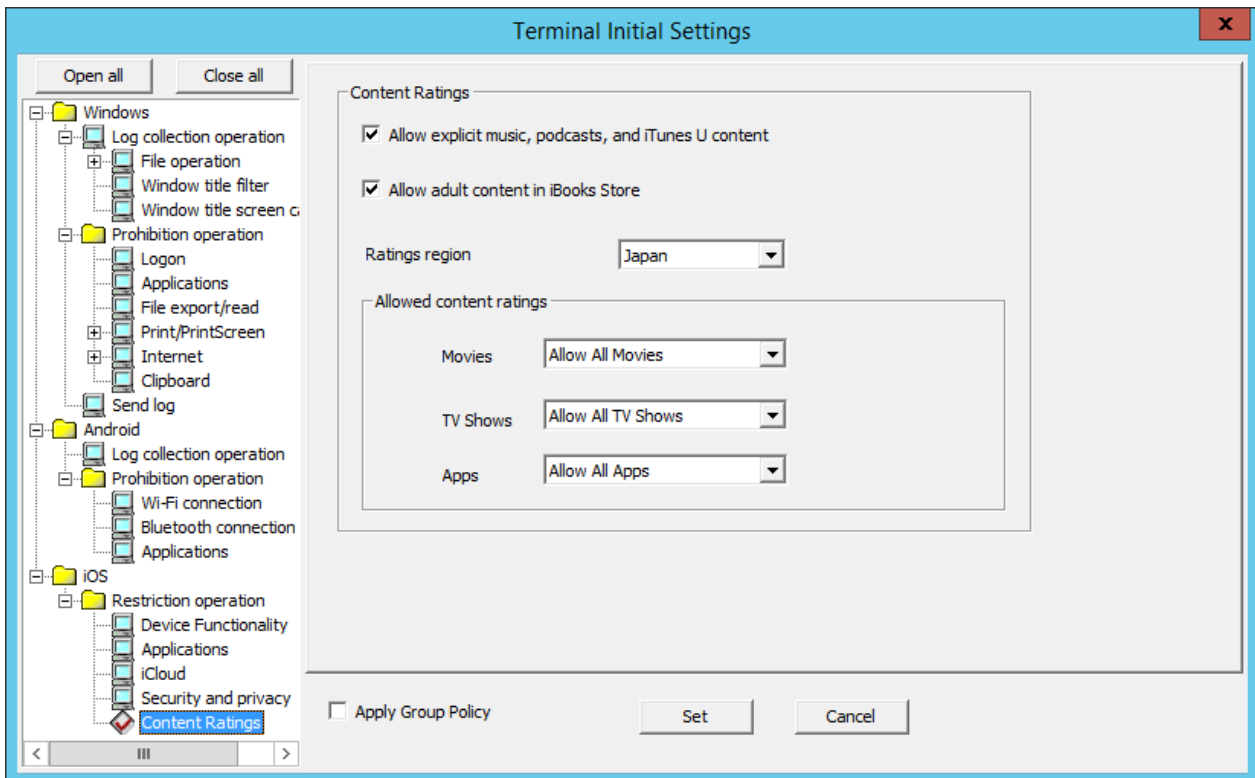
In **Security and privacy**, configure settings for sending data to Apple and security settings.




Item name	Description
Allow diagnostic data to be sent to Apple	Specify whether to allow diagnostic data to be sent to Apple. To prohibit it, clear this item. Default value: Selected.
Allow users to accept untrusted TLS certificates	Specify whether to allow untrusted TLS certificates to be accepted. To prohibit it, clear this item. Default value: Selected.
Forced encrypted backups	Specify whether to forcibly encrypt backups. To encrypt backups, clear this item. Default value: Not selected.

2.4.1.24 Content Ratings

In **Content Ratings**, specify the content that can be viewed depending on the ratings.



Item name	Description
Allow explicit music, Podcasts, and iTunes U content	Specify whether to allow explicit music, Podcasts, and iTunes U content. To prohibit it, clear this item. Default value: Selected.
Allow adult content in iBooks Store	Specify whether to allow adult content in iBooks Store. To prohibit it, clear this item. Default value: Selected.
Ratings region	Select the appropriate ratings region from the menu. <ul style="list-style-type: none"> - U.S. - Australia - Canada - Germany - France - Ireland - Japan (Default value) - New Zealand - U.K.

Item name	Description
	 Note <hr style="border-top: 1px dotted orange;"/> <p>If Content Ratings is set for an iOS device, region settings different from Ratings region in the iOS device may not take effect. Configure the setting to suit the Ratings region setting in the iOS device.</p> <hr style="border-top: 1px dotted orange;"/>
Allowed content ratings	Configure the content prohibition settings to suit the ratings for the region selected in Ratings region .
	<p>Movies</p> <p>Select the movie ratings from the menu.</p> <ul style="list-style-type: none"> - Do not allow movies Prohibits movies. - Allow All movies (Default value) Allows all movies. <p>Other selection items vary depending on the region selected in Ratings region. Configure settings in accordance with the ratings for respective regions.</p>
	<p>TV Shows</p> <p>Select the TV show ratings from the menu.</p> <ul style="list-style-type: none"> - Do not allow TV programs Prohibits TV programs. - Allow All TV programs (Default value) Allows all TV programs. <p>Other selection items vary depending on the region selected in Ratings region. Configure settings in accordance with the ratings for respective regions.</p>
	<p>Apps</p> <p>Select the application ratings from the menu.</p> <ul style="list-style-type: none"> - Do not allow Apps Prohibits applications. - Allow All Apps (Default value) Allows all applications. - 4+ Allows applications with 4+ ratings only. - 9+ Allows applications with up to 9+ ratings. - 12+ Allows applications with up to 12+ ratings. - 17+ Allows applications with up to 17+ ratings. <p>Selection items are common to all regions.</p>

2.4.2 Perform Terminal Operation Settings

Perform the client (CT) operation settings (settings of conditions relating to attached data and method of log sending) and smart device (agent) operation settings. 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 timing for the smart device (agent) operation settings to be reflected on the smart device (agent)

- Android

The timing for the smart device (agent) operation settings to be reflected on the smart device (agent) is as follows:

- When the smart device (agent) is started
- Once per day at a set time (between 12:00 and 13:00)
- When **Sync now** is selected on the smart device (agent)

- iOS

Operation settings are reflected in the profile at the following timing:

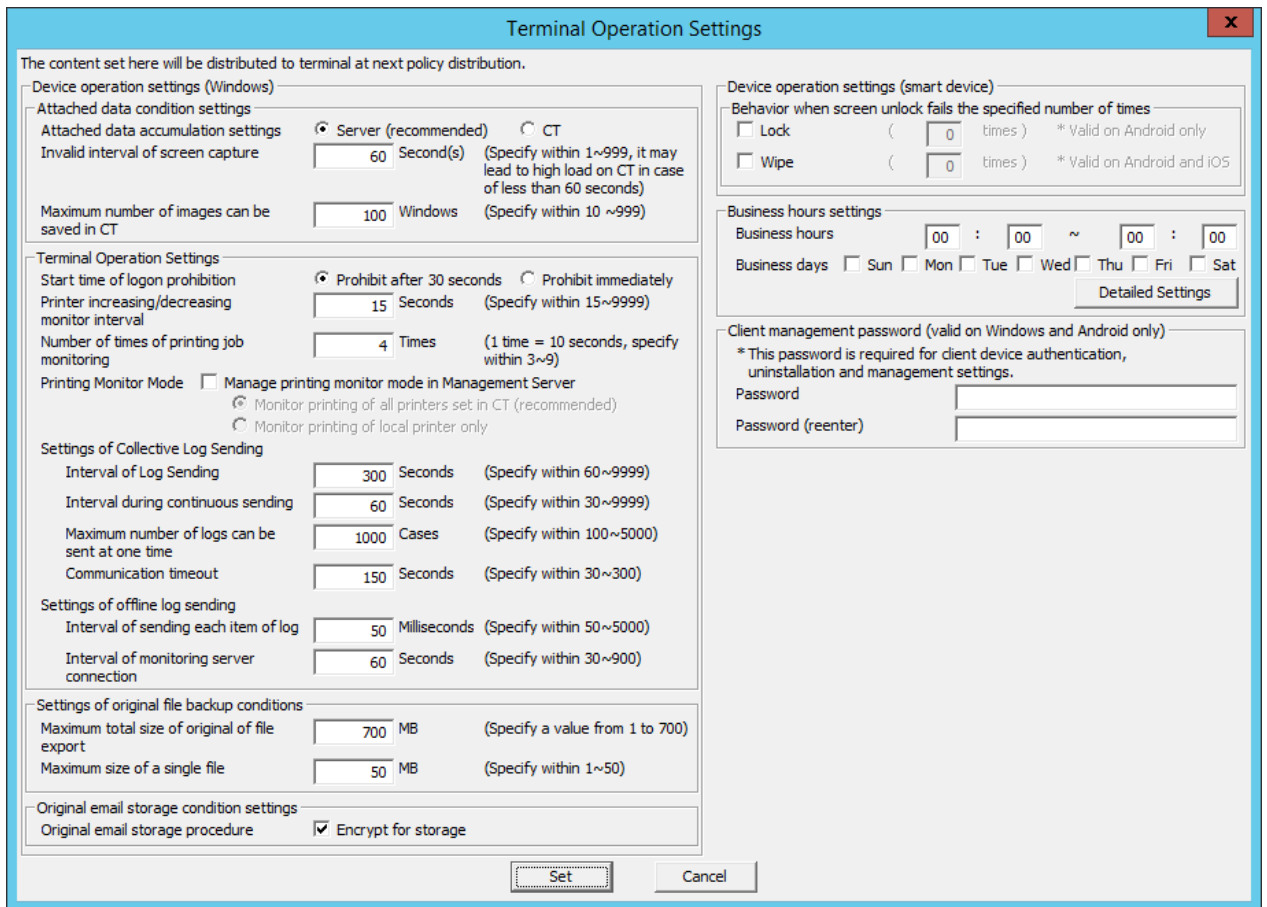
- When a target device is selected in the Management Console, and **Update Immediately** is clicked
 - When a target device is selected in the Management Console, and **Update at Next Startup** is clicked
-

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	<p>Specify the location for saving the attached data (screen capture, original file backup in file export).</p> <ul style="list-style-type: none"> - Server (recommended) Save the attached data in the Management Server. - 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). 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, add the user of viewing data in the security settings of save folder. 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. 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>The initial value is Server (Recommended).</p>

Item Name	Description
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), 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"> - Prohibition after 30 seconds Logoff or shutdown 30 seconds after the logon prohibition is detected. - Prohibit immediately Logoff or shutdown immediately after the logon prohibition is detected. <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. 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> <p>Increase this value when file names and total number of pages are incorrect in the collected log.</p>
Printing Monitor Mode	<p>Select the mode of printing in the client (CT).</p> <ul style="list-style-type: none"> - 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. - 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.

Item Name	Description	
	<ul style="list-style-type: none"> - Monitor printing of all printers set in CT (recommended) The printing mode becomes Monitor printing of all printers on this CT (recommended) - onitor printing of local printers only The printing mode becomes "Monitor the printing of local printers only". <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 Send log of CT policy is set.</p> <ul style="list-style-type: none"> - When Send immediately when operation logs occur and Send operation logs accumulated in certain collectively after connection are selected. - When Send after collecting logs for a certain period and Send operation logs accumulated in certain collectively after connection are selected.
	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 Send log of CT policy is set.</p> <ul style="list-style-type: none"> - When Send immediately when operation logs occur and Send operation logs accumulated in certain collectively after connection are selected. - When Send after collecting logs for a certain period and Send operation logs accumulated in certain collectively after connection are selected.
	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 Send log of CT policy is set.</p> <ul style="list-style-type: none"> - When Send immediately when operation logs occur and Send operation logs accumulated in certain collectively after connection are selected. - When Send after collecting logs for a certain period and Send operation logs accumulated in certain collectively after connection are selected.
	Communication Timeout	<p>Specify the timeout value (seconds) of connection between the CT and server when logs are sent collectively. 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>

Item Name		Description
		<p>The Communicate Timeout will be valid when any of the following options in Send log of CT policy is set.</p> <ul style="list-style-type: none"> - When Send immediately when operation logs occur and Send operation logs accumulated in certain collectively after connection are selected. - When Send after collecting logs for a certain period and Send operation logs accumulated in certain collectively after connection are selected.
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. 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 Send log of CT policy is set.</p> <ul style="list-style-type: none"> - When Send immediately when operation logs occur and Send accumulated logs immediately after connection are selected. - When Send immediately when operation logs occur and Send operation logs accumulated in certain collectively after connection are selected.
	Interval of monitoring server connection	<p>Specify the communication confirmation interval (seconds) of the server when logs are sent immediately. 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 Send log of CT policy is set.</p> <ul style="list-style-type: none"> - When Send immediately when operation logs occur and Send accumulated logs immediately after connection are selected. - When Send immediately when operation logs occur and Send operation logs accumulated in certain collectively after connection are selected.

Note

About sending command operation log to server

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

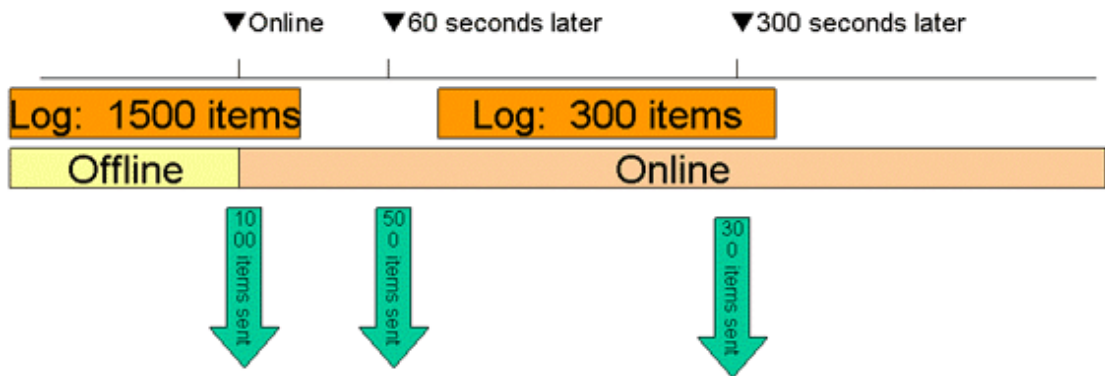
Settings of Collective Log Sending

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, 300 logs will be sent 300 seconds after 500 logs are sent.

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).

Original email storage condition settings

Item name	Description
Original email storage procedure	Specify whether to encrypt emails during storage. - Encrypt for storage is cleared Emails will be stored without being encrypted. Encrypt for storage is selected Emails will be encrypted and then stored. By default, Encrypt for storage is selected.

Point

Viewing emails stored without being encrypted

Emails stored without being encrypted can be viewed by directly referencing the file stored in the folder set in **Server settings tool > Folder/CT self version upgrade settings > E-mail content saving target**

Note

Original email storage procedure

Even if the **Encrypt for storage** setting is changed, the emails stored before the change will not be affected by the new setting.

After operation is performed with **Encrypt for storage** selected (emails are encrypted and then stored), if you clear **Encrypt for storage** (emails are stored without being encrypted), the new setting will be effective for emails stored after the change. The emails stored before the change will not be affected and will remain encrypted.

Similarly, if **Encrypt for storage** is cleared (emails are stored without being encrypted) and you then select it (emails are encrypted and then stored), the emails stored before the change will not change and will remain unencrypted.

Device operation settings (smart device) > Behavior when screen unlock fails the specified number of times

This setting will be applied to the smart device operation settings.

Refer to "[3.7.3 Controlling Smart Device when Password Entry Fails](#)" for details.

Business hours settings

This setting will be applied to the smart device operation settings.

Refer to "[2.4.1.19 Application \(Android\)](#)" for details.

Item name	Description
Business hours	Specify the business start time and finish time in the following format: hhmm - hhmm - hh: Specify the hour using 00 - 23. - mm: Specify the minute using 00 - 59. Business hours settings are enabled when Business days is selected. The default value is "00:00 - 00:00".
Business days	Specify the business days by day of the week. Multiple days can be selected from the following days: Sun,Mon,Tue,Wed,Thu,Fri,Sat By default, no value is specified.
Advanced Settings	Click this item, and the The Business Hours Settings - Advanced Settings window will be displayed. Set exceptions for holidays and other business days.

Note

Use **Business days** and **Business hours** in combination.

If a combination of business days (Mon, Tue, Wed, Thurs, Fri) and business hours (09:00 - 17:30) is specified, business hours will be assumed to be "09:00 - 17:30, Monday - Friday".

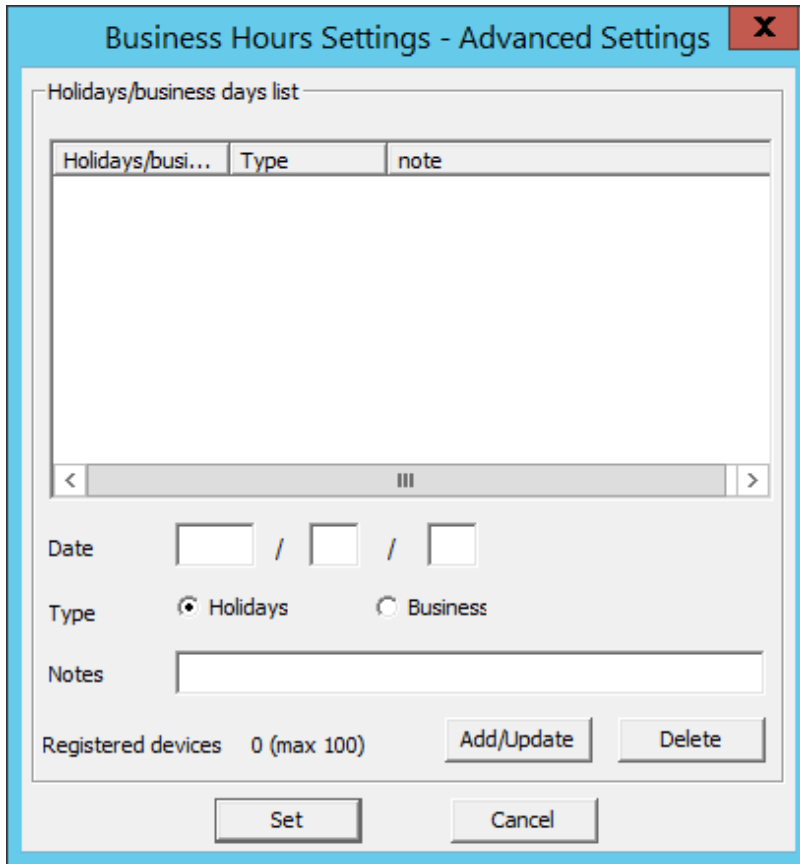
Even if 09:00 - 17:30 is set in **Business hours**, it will not be recognized if **Business days** is not selected.

Entering the business hours

- You can enter a start time that is later than the finish time.
In this case, operation will be performed assuming the business hours are set over two days.
Example: If "18:30 - 05:00" is specified, operation will be performed assuming the business hours run until 5 A.M. the next morning.
- You can enter a start time that is the same as the finish time.
In this case, operation will be performed assuming the business operates 24 hours a day.

The Business Hours Settings - Advanced Settings window

In the Business hours settings, set the exceptions for holidays and other business days.



Item name	Description
Holidays/business days list	Displays the list of exceptions for holidays and other business days. By default, no value is specified.
Date	Enter the dates to be set as exceptions for holidays and other business days. Dates from Jan. 1, 2000 to Dec. 31, 2037 can be entered using halfwidth numeric characters. By default, no value is specified.
Type	Specify whether to set the entered date as a holiday or business day.
Notes	Enter information regarding dates. Specify up to 128 halfwidth (64 fullwidth) characters.

Item name	Description
	By default, no value is specified.
Registered devices	The number of registered cases and the maximum number of registrations possible are displayed.
Add/Update	Adds the dates for exceptions for holidays and other business days. Up to 100 dates can be added. Information will be updated when Remarks for the row selected in Holidays/business days list is changed. Date cannot be updated.
Delete	Deletes the row selected in Holidays/business days list .
Set	Confirms the information entered, and returns to the previous screen.
Cancel	Closes the window without saving the settings.

Client management password

This setting will be applied to the client (CT) operation settings and smart device operation settings.

By setting the client management password, whether the password entered during the client (CT) installation matches the client management password will be checked when the client (CT) is registered on the Management Server. Once client deployment and version upgrade are completed, changing the password is recommended.

Also, entry of the password that was set will be required during uninstallation of the client (CT) and smart device (agent) (Android).

This password must be set on the Management Server and Master Management Server respectively.

The client management password set on the Master Management Server will be valid only for the client (CT) and smart device (agent) (Android) under the Master Management Server.

Note that when you are changing the connection destination Management Server or Master Management Server for the client (CT), use the same password as before.

Item name	Description
Password	Specify the password required for authentication, uninstallation and management settings for the client device during its registration. Specify up to 32 halfwidth alphanumeric characters and symbols, except for the following symbols: & < > \ " ~ ' ? : ^ You cannot enter halfwidth or fullwidth spaces, and halfwidth katakana. By default, no value is specified.
Password (reenter)	Reenter the password. The number and type of characters that can be entered are the same as those for Password . By default, no value is specified.

The client management password is valid on Windows and Android only. The password will not be valid on iOS.

If the client management password is set

If the client management password is set, operations on Windows will be as follows:

- Authentication will be performed during the registration of the client (CT) to the Management Server. Whether the password entered during the client (CT) installation matches the client management password will be checked, and if they do not match, the device will not be registered.
- Entry of the client management password will be required during the client (CT) uninstallation.

Also, operations on Android will be as follows:

- Entry of the password will be required during the smart device (agent) (Android) uninstallation.

If the client management password is not set

If the client management password is not set, operations on Windows will be as follows:

- Authentication will not be performed during the registration of the client (CT) to the Management Server.
- When uninstalling the client (CT), enter the password specified during installation.

Also, operations on Android will be as follows:

- A screen prompting password entry will be displayed during the smart device (agent) (Android) uninstallation but password entry will not be required.

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), smart device (agent), 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.

Refer to "OS" in the *Systemwalker Desktop Keeper User's Guide* for details on the operating system on which Systemwalker Desktop Keeper can import configuration information from the Active Directory server.

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.

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.

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 zero length or 41 halfwidth (21 fullwidth) characters or more.

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.

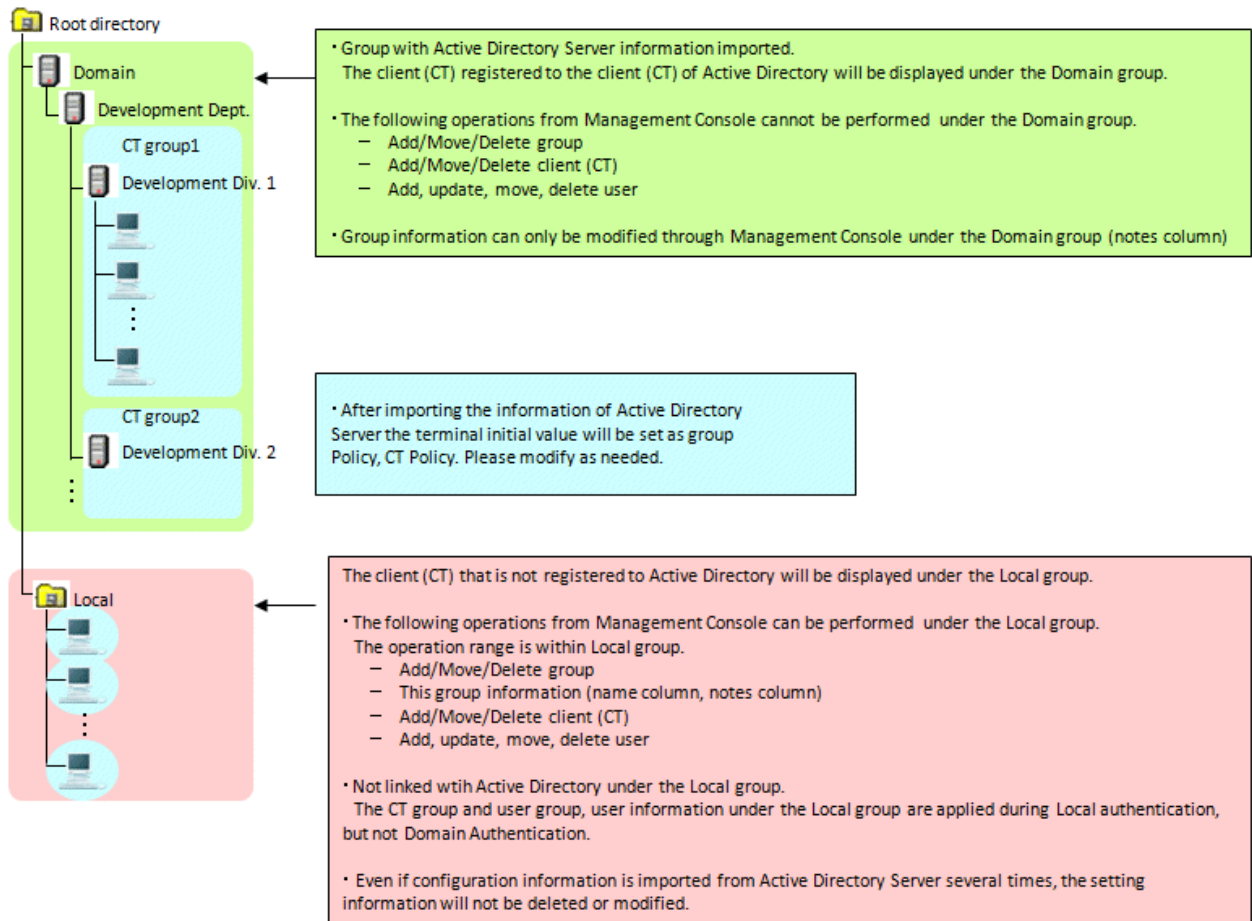
The information indicating that the data is being imported from Active Directory is displayed.

After the data is imported, the information indicating completed is displayed.

3. Click the **OK** button.

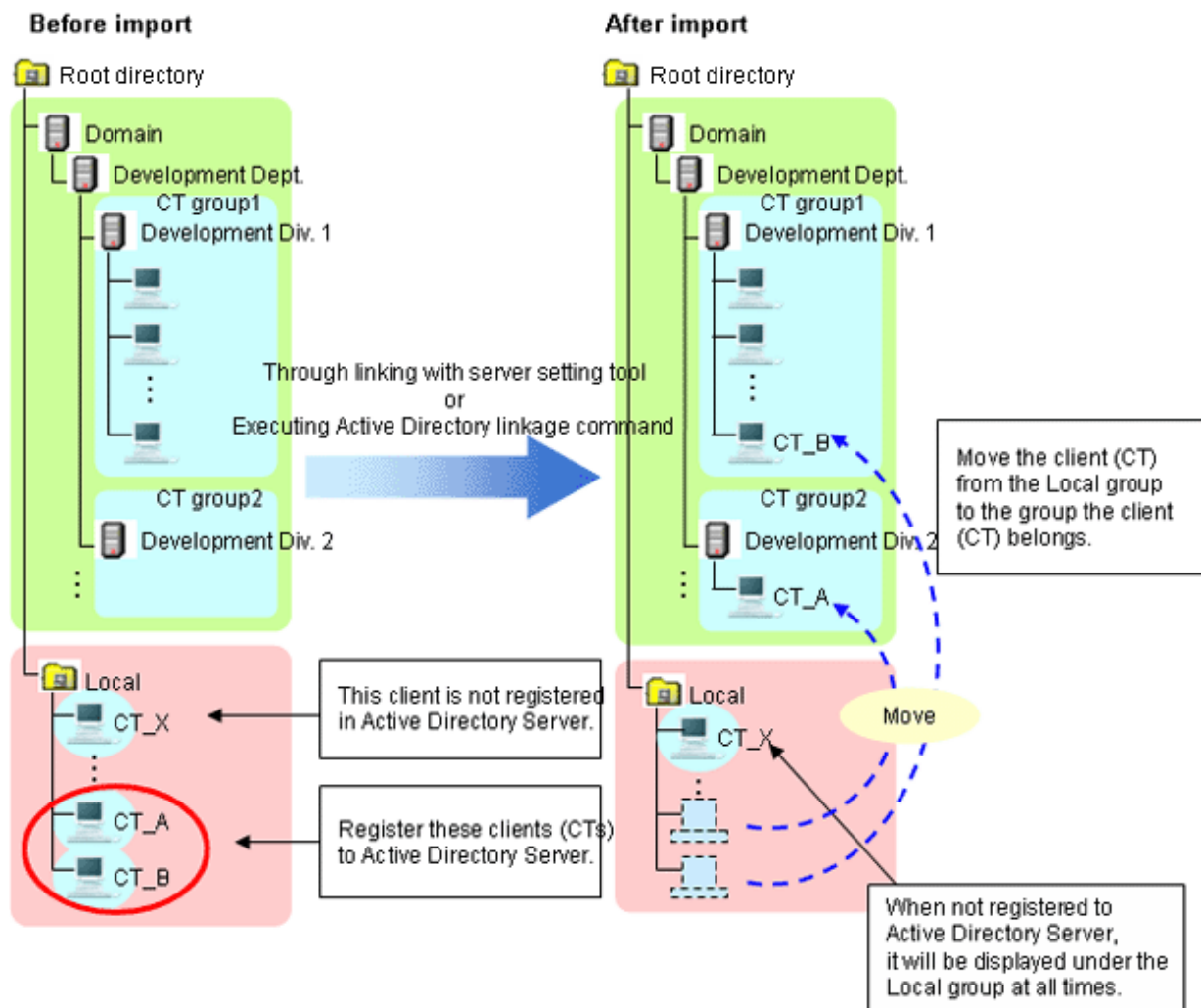
Display Configuration Information Tree

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, 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, 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)

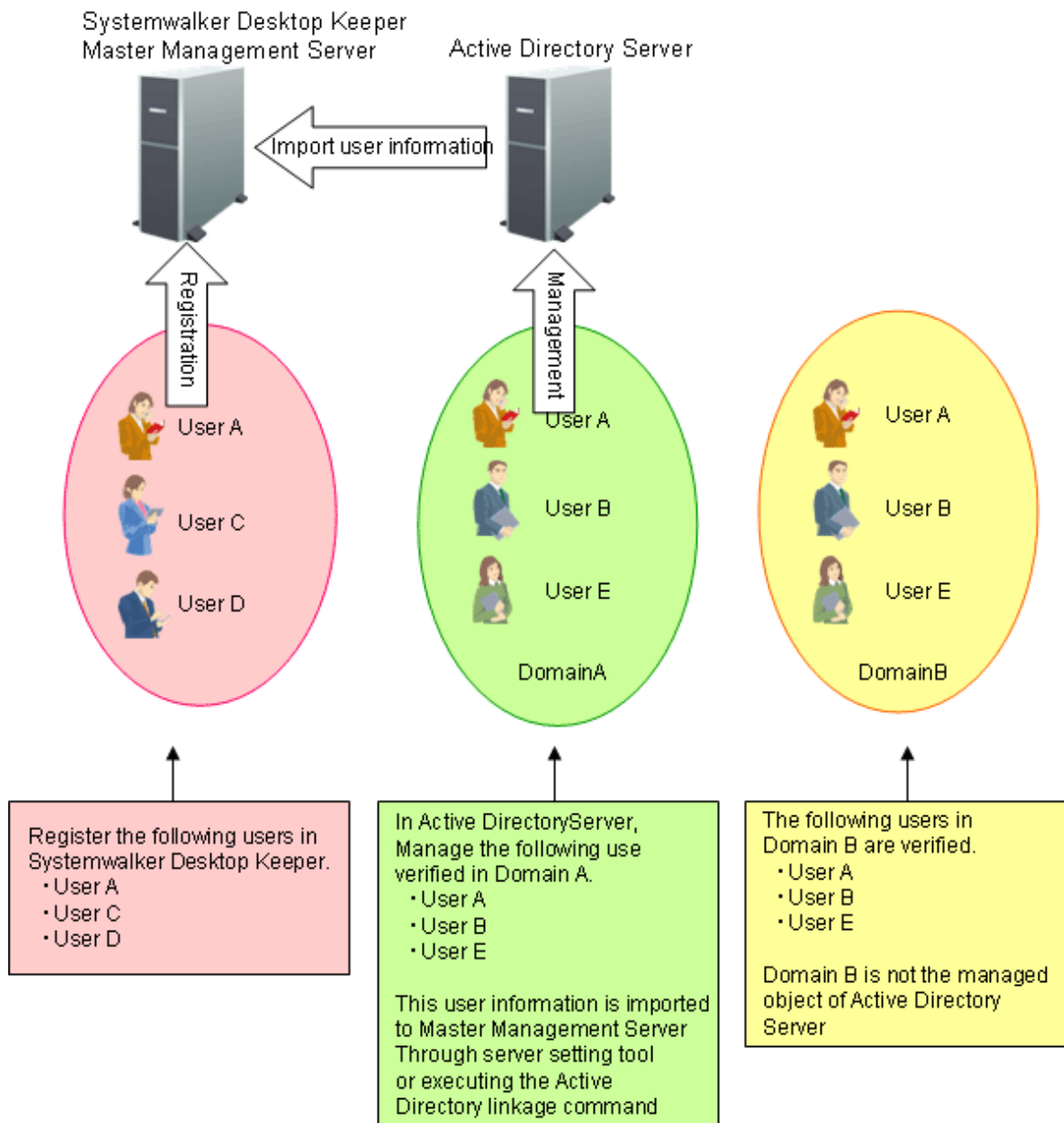
As a user will be created automatically when importing configuration information from the Active Directory Server, user policy should be used as well.

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.

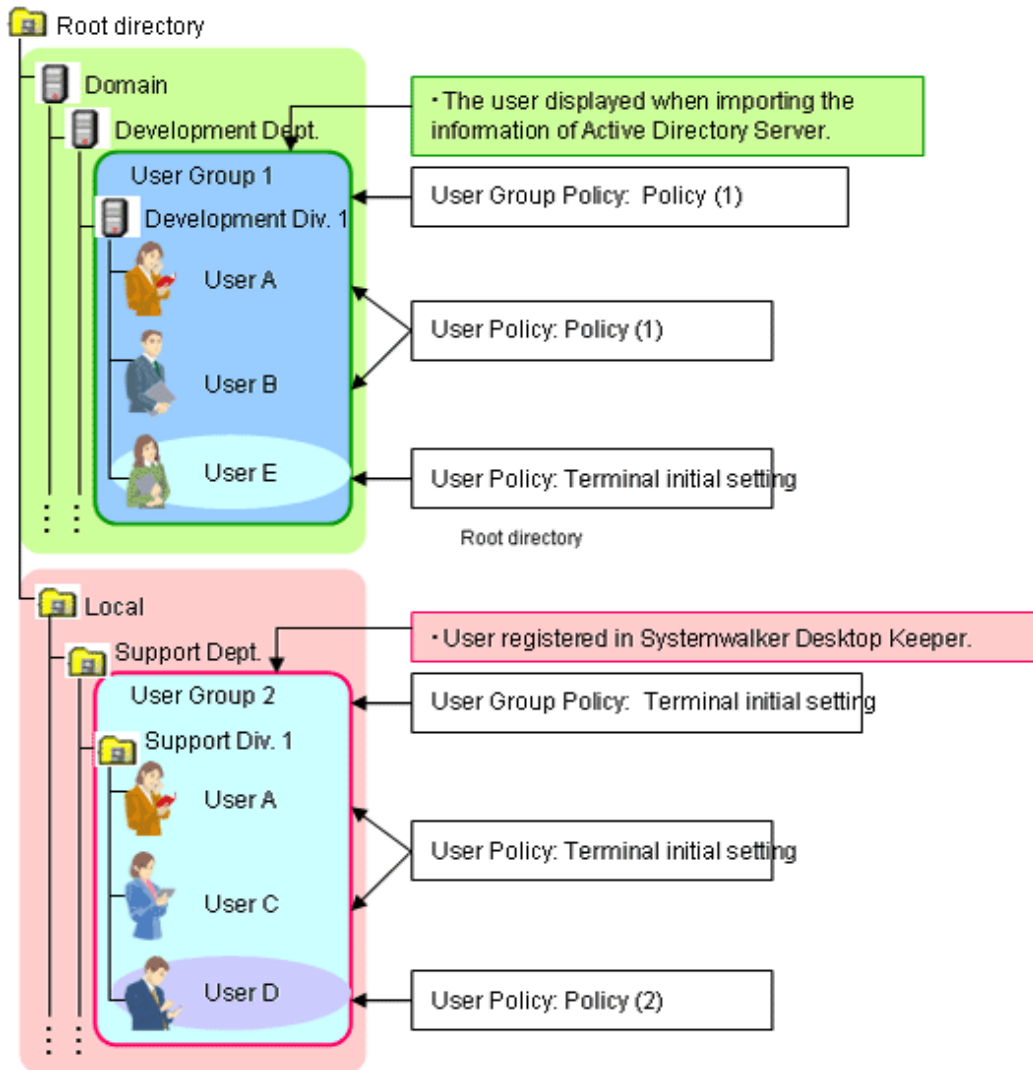
After the second and later Active Directory Linkage has completed, set the group policy of correspondent user group (OU) in the user policy of newly added user.

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, 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, 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, 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, refer to the manual of Systemwalker Desktop Patrol.

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 the 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, 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, 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, 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, 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. 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, 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, 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, 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, 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.

Add /U and /F options before executing the Systemwalker Desktop Patrol configuration information import command. For details, 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, 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, refer to "Information File of Discarded Folder" in *Systemwalker Desktop Keeper Reference Manual*.

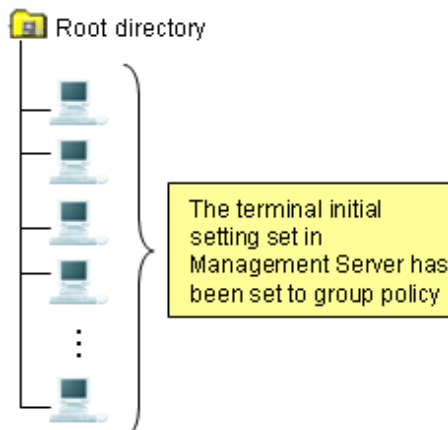
Information File of Discarded Folder is saved in the Management Server. However, it should also be saved in the Master Management Server if the managed the client (CT) exists under the Master Management Server.

Add the /E option before executing the Systemwalker Desktop Patrol configuration information import command. For details, refer to "DTKIMPDP.EXE (Systemwalker Desktop Patrol Configuration information Import)" in *Systemwalker Desktop Keeper Reference Manual*.

Display in Configuration Information Tree

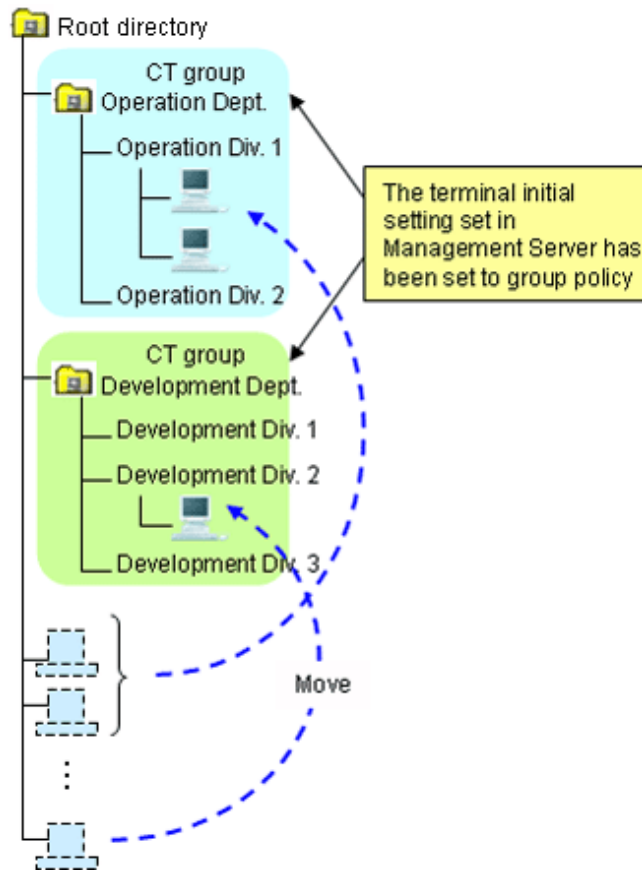
1. Install the CT of Systemwalker Desktop Keeper.

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).



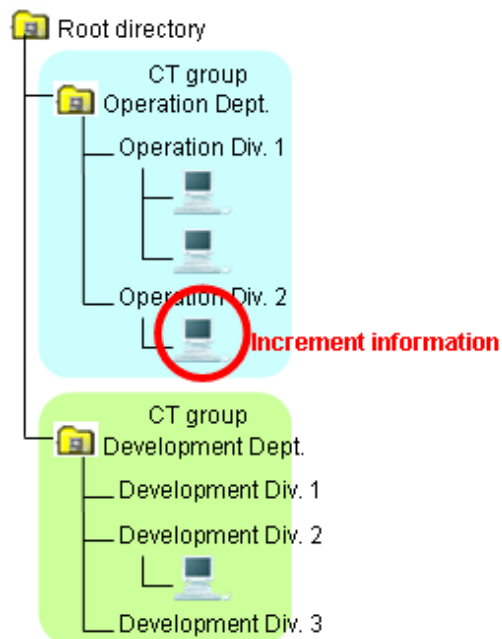
- Execute the Systemwalker Desktop Patrol configuration information import command (for the first time).

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, 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, 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 (20 fullwidth) characters, the first 40 single-byte (20 fullwidth) 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, refer to the manual of Systemwalker Desktop Patrol.

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 a File for Importing Configuration 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"> - Enter the file name with full path. Enter the path until the path of imported file with full path. - Select the View button. The Specify an Import File window is displayed. Select the imported file and click the Open button. <p>The maximum length of full path that can be entered is 218 halfwidth (109 fullwidth) characters. However, the following symbols are not allowed in a file name: \\, /, :, *, ?, ", <, >, .</p>
Result Log File	<p>Specify the file for outputting import operation result. As the extension will not be added automatically, specify an extension that can be determined easily, such as "KEKKA.TXT" through the following method.</p> <ul style="list-style-type: none"> - Enter the file name with full path. Enter with full path in the input field until the path of the output result log file. - 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. <p>The maximum length of full path that can be entered is 218 halfwidth (109 fullwidth) characters. However, the following symbols are not allowed in a file name: \\, /, :, *, ?, ", <, >, .</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"> - Add Add after the result log of last time. - Overwrite Overwrite the result log of last time.

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:

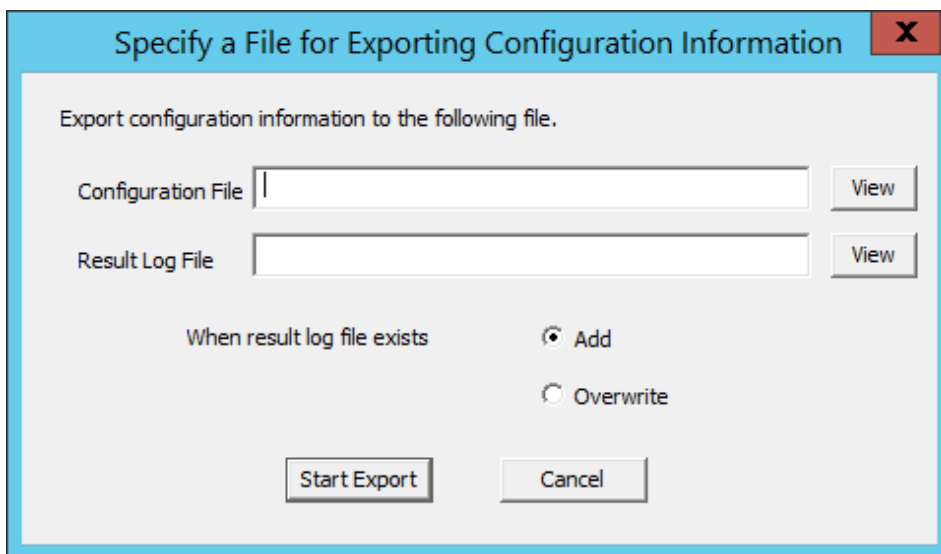
- When the client (CT) version of Systemwalker Desktop Keeper is V13.0.0 or later
- When there is information in **DTPID** in the CT list of Management Console

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 Configuration Information** window is displayed.



3. Click the **Start Output** button after entering the following information.

Item Name	Description
Configuration 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, specify an extension that can be determined easily such as "FILEA.CVS" through the following method.</p> <ul style="list-style-type: none"> - Enter the file name with the full path. Enter with the full path in the input field until the path of the output configuration information file. - 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. <p>The maximum length of full path that can be entered is 218 halfwidth (109 fullwidth) characters. However, the following symbols cannot be contained in a file name. Symbols cannot be used: \, /, :, *, ?, ", <, > and .</p>

Item Name	Description
Result Log File	<p>Specify the file for outputting import operation result. As the extension will not be added automatically, specify an extension that can be determined easily such as "KEKKA.LOG", through the following method.</p> <ul style="list-style-type: none"> - 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. - 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. <p>The maximum length of full path that can be entered is 218 halfwidth (109 fullwidth) characters. However, the following symbols are not allowed in a file name: \, /, :, *, ?, ", <, >, .</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"> - Add Add after the result log of last time. - Overwrite Overwrite the result log of last time.

4. Import configuration information in Systemwalker Desktop Patrol.

For the method of import, 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, execute in each Management Server.

Create a CT group

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. 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**
- Specify up to 40 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters).

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. Modify the policy as needed. For details regarding the modification of policy, 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. Delete the CT groups or CTs under it first. For detail on how to delete a CT, 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.

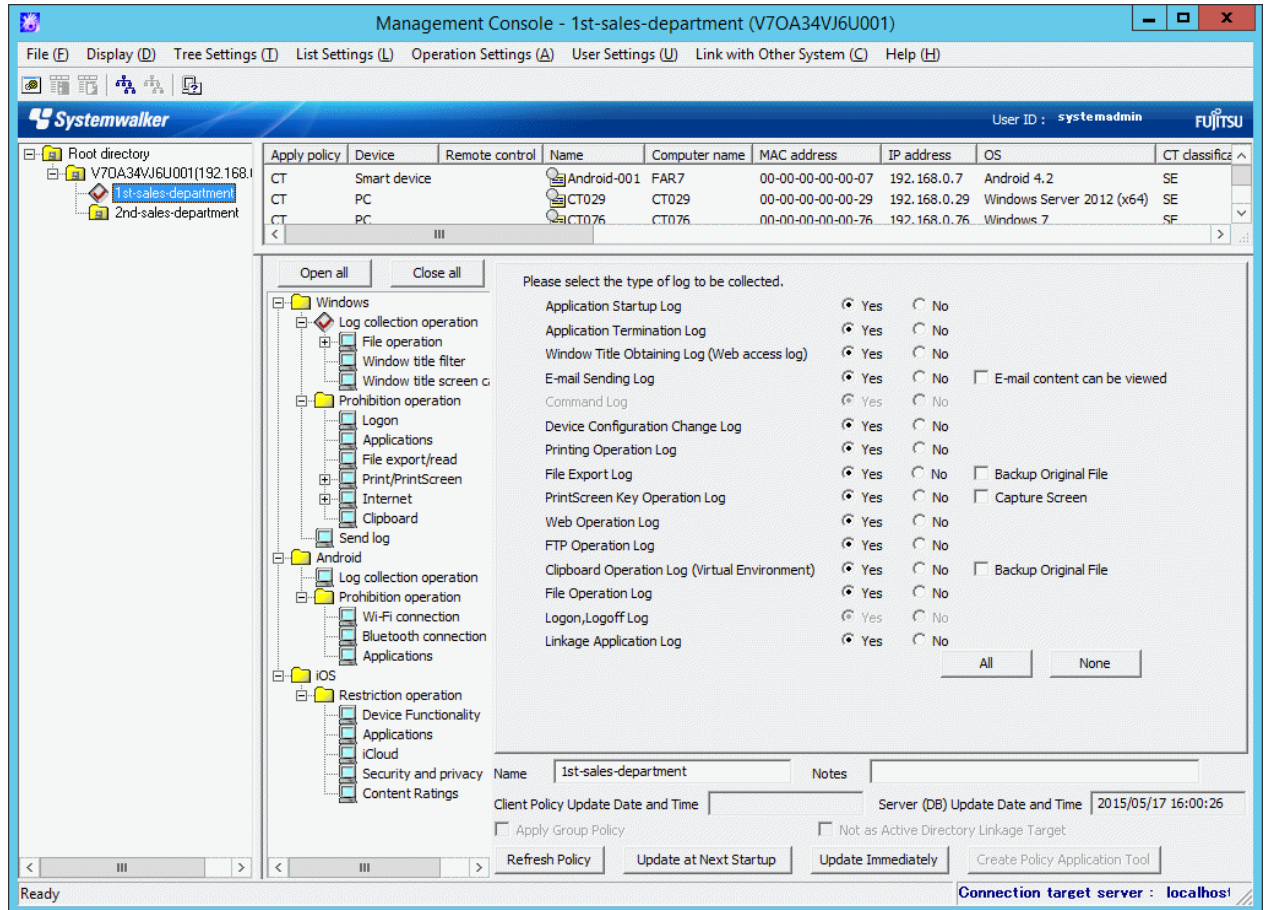
Modify group information

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.
Specify up to 40 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters).
 - **Notes:** Enter the notes relating to CT group.
Specify up to 127 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters).

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, 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, 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, refer to "Automatic Distribution File During CT Registration" of *Systemwalker Desktop Keeper Reference Manual*.

Location for saving

Windows Server(R) 2008 and Windows Server(R) 2012 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, the error will be displayed in trace file (fsw21sj0.log) of server service. At this time, 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.



Operate collective management of user policy through Master Management Server.

To manage user policy collectively, 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. Cancel the settings.

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

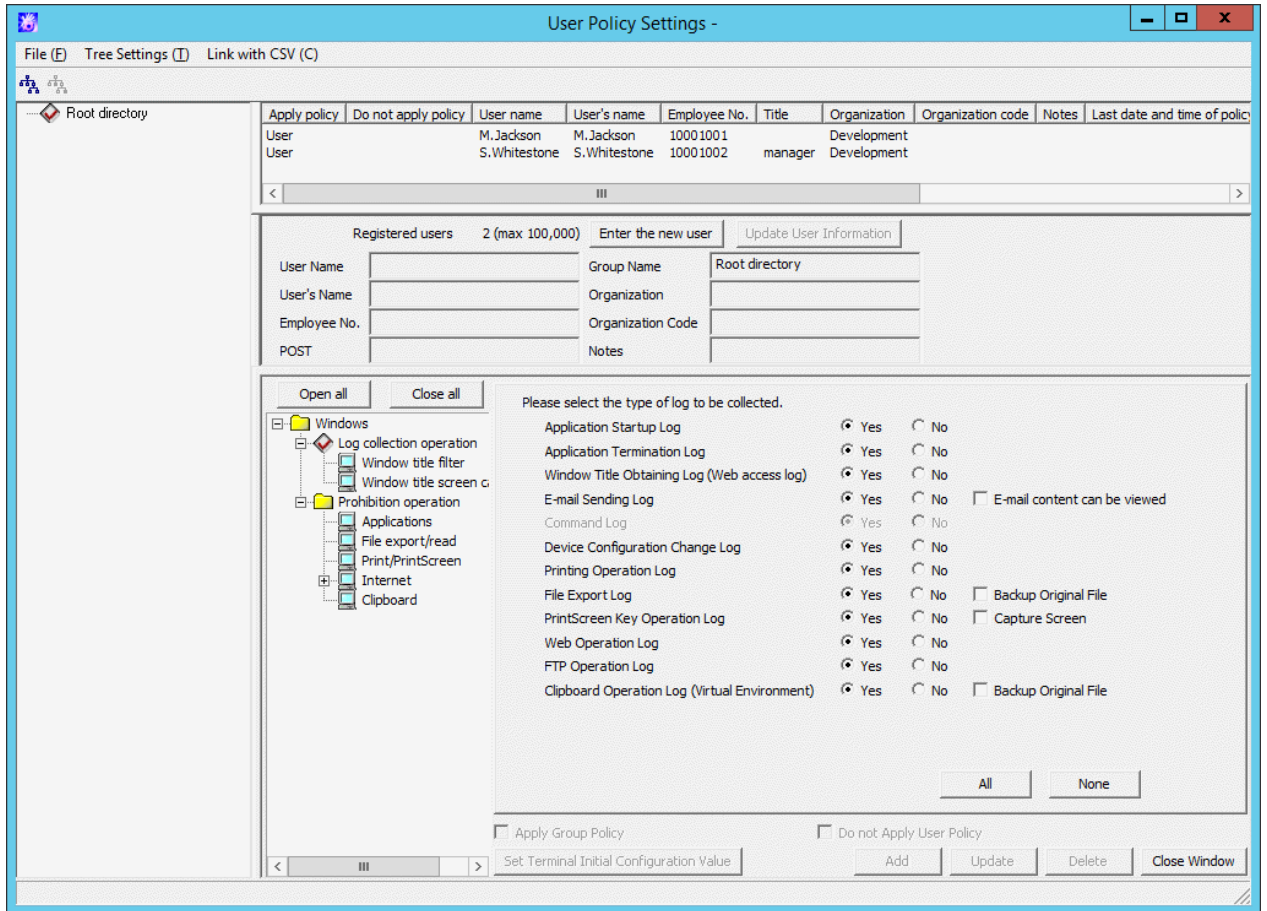
After a user group has been created, user policy can be set collectively for users in the user group.

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.

5. Enter the following information and click the **Add** button.

Group Name: Specify up to 40 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters).

The message that prompts structure update is output.

6. Click the **OK** button.

The group added in user group tree is displayed.

7. 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. Modify the policy as needed. For details regarding policy modification, 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. Delete the user group or user under it first. For details on how to delete a user, 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.
Specify up to 40 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters).
- **Notes:** Enter the notes relating to the user group.
Specify up to 128 bytes (can be a combination of fullwidth and halfwidth characters and symbols, kanji, hiragana and katakana characters).

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, 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 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, 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, set the department administrator in CT group in order to view logs.

As to the client (CT) and smart device (agent) 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) and smart device (agent) 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)

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), 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, 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, 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.

The department administrator set here is valid for all subordinate groups.

Select Group: Development

List of department administrators

User ID	User Name	Access authority	E-mail address
FujitsuHanako	(Develop Sec.) Fujitsu Ha...	(Department administrator) Management Co...	fujitsu.hanako@xx.xxxxx.com

< ||| >

Select Deselect

List of selected department administrators

User ID	User Name	Access authority	E-mail rec...	E-mail address
FujitsuTaro	(Develop Sec.) Fujitsu Taro	(Department administrator) Log Viewer and ...	<input checked="" type="checkbox"/>	fujitsu.taro@xx.xxxx

< ||| >

Register Cancel

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. 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.

The department administrator set here is valid for all subordinate groups.

Select Group: Development

List of department administrators

User ID	User Name	Access authority	E-mail address
FujitsuHanako	(Develop Sec.) Fujitsu Ha...	(Department administrator) Management Co...	fujitsu.hanako@xx.xxxxx.com

< ||| >

Select Deselect

List of selected department administrators

User ID	User Name	Access authority	E-mail rec...	E-mail address
FujitsuTaro	(Develop Sec.) Fujitsu Taro	(Department administrator) Log Viewer and ...	<input checked="" type="checkbox"/>	fujitsu.taro@xx.xxxx

< ||| >

Register Cancel

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. 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.

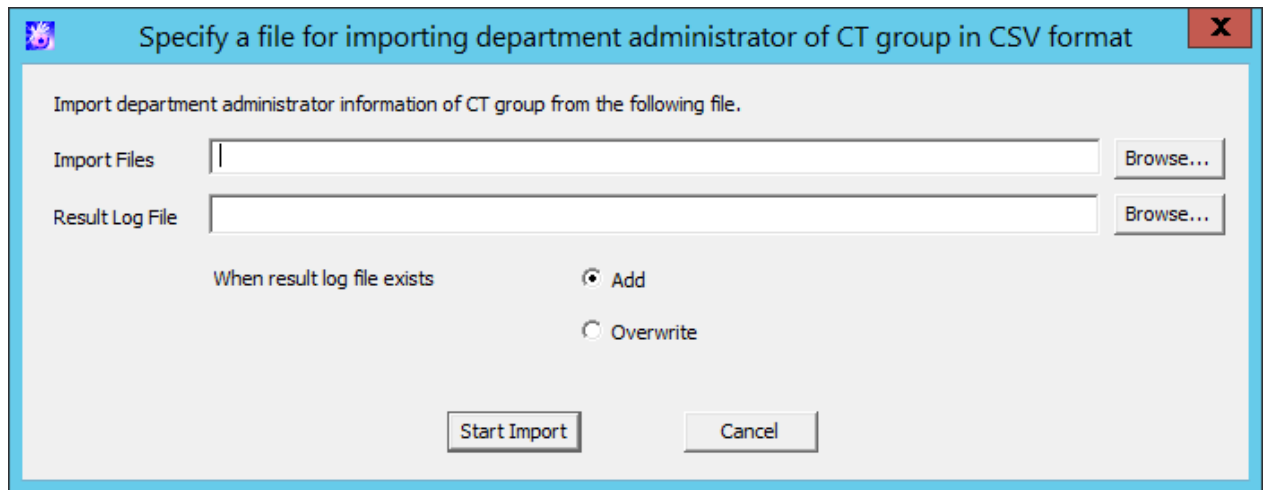
Allocate department administrator to CT group

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 in CSV format** window is displayed.



- **Import File** (required): Specify the CVS file with defined department administrator information with the full path. Specify up to 218 halfwidth (109 fullwidth) characters. However, the file name cannot contain any of the following symbols:
\\/: * ? " < > |
- **Result Log file** (required): Specify the file for saving operation result with full path. Specify up to 218 halfwidth (109 fullwidth) characters. However, the file name cannot contain any of the following symbols:
\\/: * ? " < > |
- **When result log file exists:** When a current result log file exists, 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**.

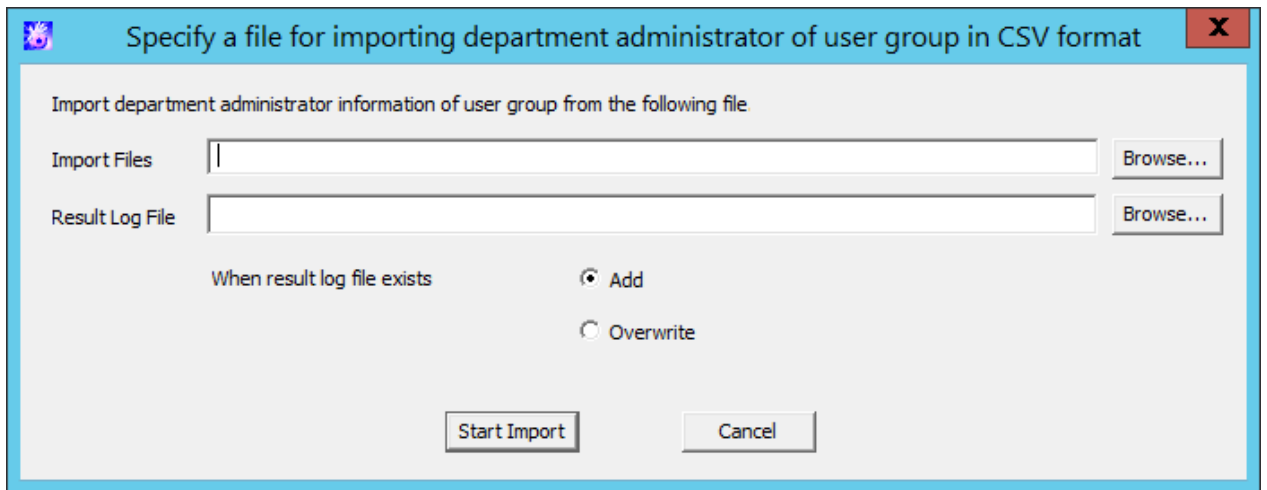
Use the user ID and password of the system administrator to logon.

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 in CSV format** window is displayed.



- **Import Files** (required): Specify the CVS file with defined department administrator information with the full path. Specify up to 218 halfwidth (109 fullwidth) characters. However, the file name cannot contain any of the following symbols: \ / : * ? " < > |
- **Result Log File** (required): Specify the file for saving operation result with full path. Specify up to 218 halfwidth (109 fullwidth) characters. However, the file name cannot contain any of the following symbols: \ / : * ? " < > |
- **When result log file exists**: When a current result log file exists, 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.

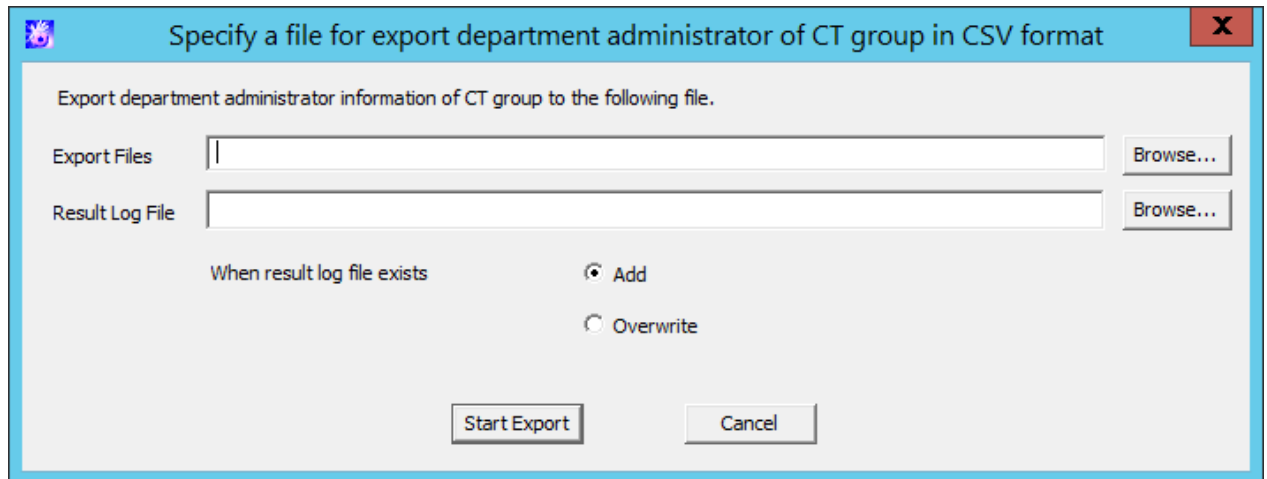
When the department administrator performs the export, all information of the department group and its subordinate groups can be exported. For groups that do not belong to a department, only **Group ID** and **Group Name** will be exported.

For details about exported content, 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.
Specify up to 218 halfwidth (109 fullwidth) characters. 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.
Specify up to 218 halfwidth (109 fullwidth) characters. However, the following symbols are not allowed in a file name:
" \ " / " " : " " * " " ? " " " " " < " " > " " | " .
 - **When result log file exists**: When the current result log file exists, 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 Export** button.
 4. A message appears after the operation. Click the **OK** button.

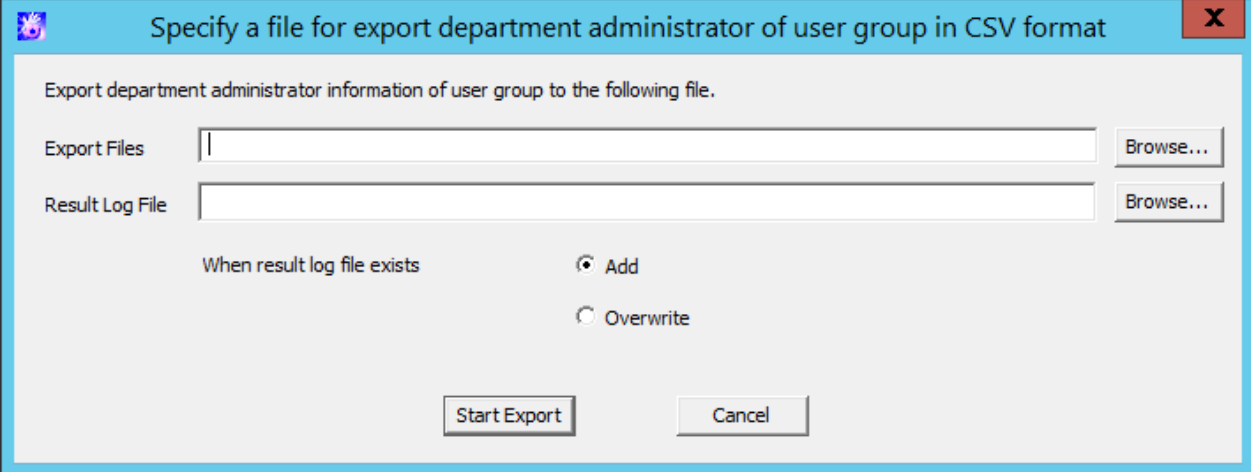
Export department administrator information of user group

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.
Specify up to 218 halfwidth (109 fullwidth) characters. 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.
Specify up to 218 halfwidth (109 fullwidth) characters. However, the following symbols are not allowed in a file name.
" \ " / " " : " * " " ? " " " " < " " > " " | " .
 - **When result log file exists**: When the current result log file exists, 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

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, set aggregation conditions in the Master Management Server. To know the state of the subordinate Management Server, set aggregation conditions in each Management Server.

1. Start Web Console with any of the following methods.

In a 2-level system structure, connect to the Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main 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, connect to (Master) Management Server respectively.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main 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

-

Refer to "[1.2.45 IPv6 Support](#)" for details on the IPv6 specification.

-

The **Login** window is displayed.

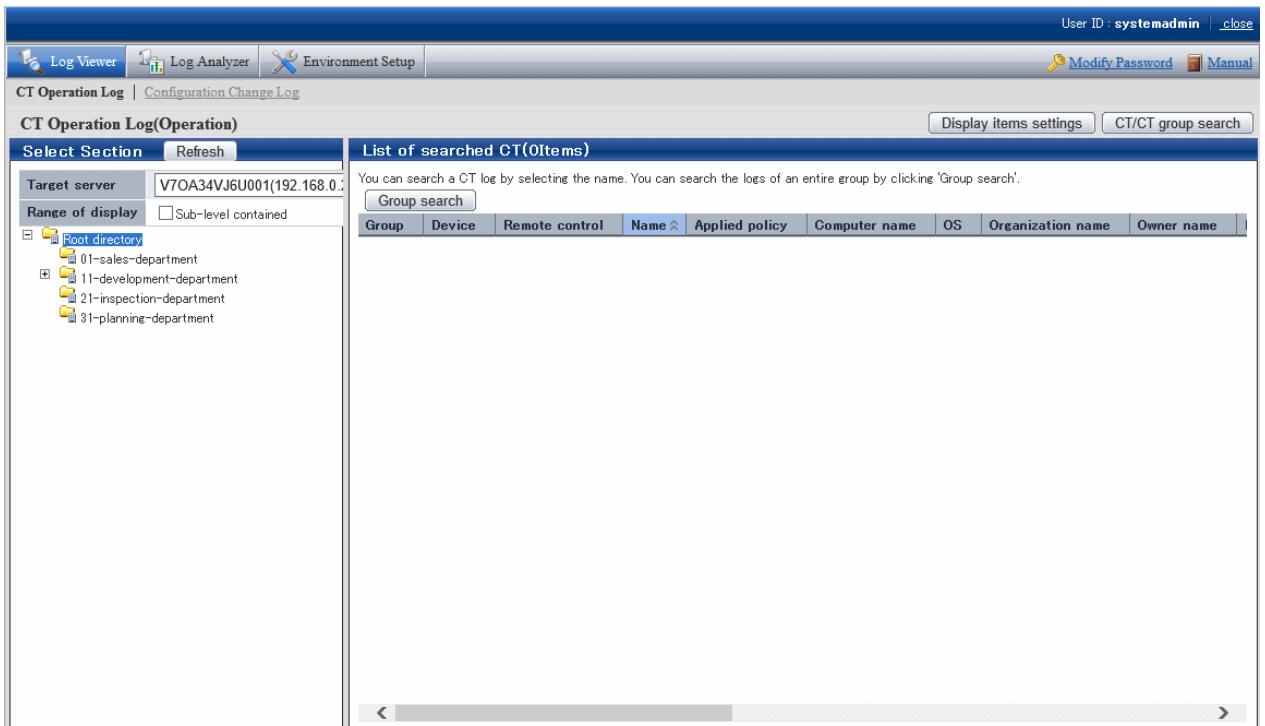
2. Enter the following information and click the **Login** button.

- **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, refer to "[Change password](#)".

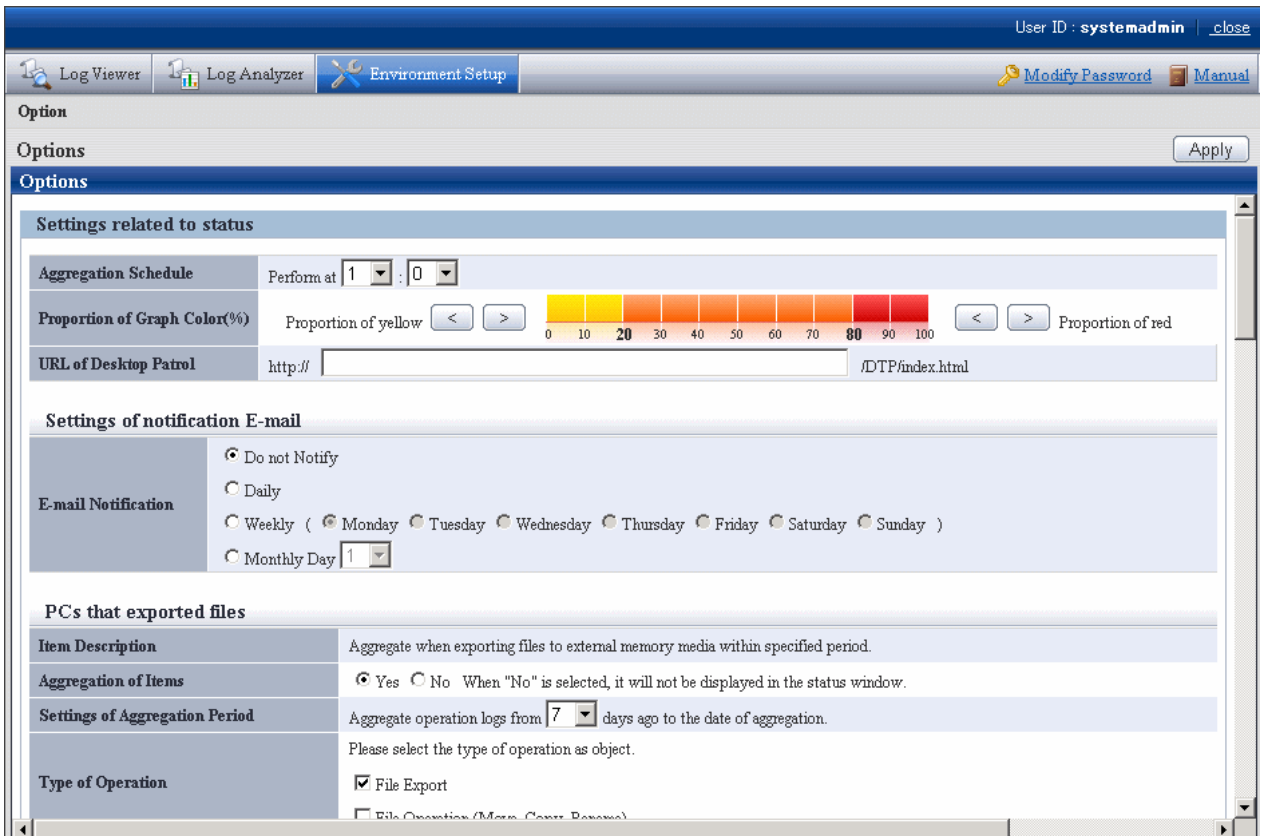
The status window is displayed.



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	<p>Set the time to start aggregation.</p> <ul style="list-style-type: none"> - Hour: Select by hour within the range of 0-23 - Minute: Select by minute within the range of 0-59 <p>Initial value: 1 hour 0 minute</p> <p> Note</p> <hr style="border-top: 1px dotted orange;"/> <p>Take the following points into consideration in the settings of an aggregation schedule:</p> <ul style="list-style-type: none"> - The aggregation process will cause a heavy load. Perform in the time frame with lower business load (at midnight, etc.). - Do not modify configuration information and environment setup during aggregation. The aggregation result may be displayed incorrectly. - Level Control Service must be started during the aggregation process. Do not overlap with the operation of stopping Level Control Service (backup, restoration, data transmission, etc.). <hr style="border-top: 1px dotted orange;"/>
Proportion of Graph Color(%)	<p>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%.</p> <p>Initial value: the threshold value of the yellow histogram is within 20% the threshold value of the red histogram is above 80%</p>
URL of Desktop Patrol	<p>Set it when assets management information of Systemwalker Desktop Patrol is displayed.</p> <p>Single-byte alphanumeric characters, "." and ":" can be specified.</p> <p>Initial value: not displayed</p>
Settings of notification E-mail	
E-mail Notification	<p>Set to notify the department administrator about the aggregation result by E-mail.</p> <ul style="list-style-type: none"> - Do not notify: Do not notify by E-mail. - Daily: notify by E-mail every day. - Weekly: Specify the day to notify by E-mail once a week. Set which day and whether to notify the aggregation result by E-mail on that day weekly. - 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. <p>Initial value: Do Not notify</p> <p>The following aggregation items are not notified by E-mail.</p> <ul style="list-style-type: none"> - PCs that blocked the use of prohibited USB device - PCs that blocked the use of prohibited account group - Devices that blocked the use of prohibited application - PCs that blocked prohibited printing - PCs that blocked the sending of email with prohibited attachment

Item Name	Description
	<p>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).</p> <p>E-mail is not sent in following cases:</p> <ul style="list-style-type: none"> - When there is no department administrator in the upper level group - When the recipient address of the department administrator is not set though department administrator has been set - When there is no error PC in the department managed by the department administrator - 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. Set an E-mail notification on each Management Server. - When aggregation process stops abnormally - When Level Control Service stops At this time, if aggregation process ends normally, E-mail notification will be performed after Level Control Service starts. <p>Also, 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>Specify up to 128 halfwidth (64 fullwidth) characters. The E-mail will be sent without any subject if the subject is omitted.</p> <p>Initial value: (blank)</p>
E-mail Text	<p>Set the body text of E-mail.</p> <p>Specify up to 512 halfwidth (256 fullwidth) characters.</p> <p>Initial value: (blank)</p> <p>The body text of notification is shown as follows.</p> <div style="border: 1px solid black; padding: 5px;"> <pre> The specified content in [E-mail Body Text] [Overview] Aggregation target department: [Counting information] (*1) PCs that exported files: PCs used out of working time: Pattern 1: PCs used out of working time: Pattern 2: PCs that performed suspicious access: PCs not connected for a long period: [Attachment information] (*2) ----- PCs that exported files 1: terminal name : : ----- PCs used out of working time: Pattern 1 1: terminal name : </pre> </div>

Item Name	Description
	<pre data-bbox="638 235 1085 448">: ----- : : (omitted) -- http://IP address DTK/index.html</pre> <p data-bbox="638 470 1404 593">*1: if over one correspondent terminal exists in items to be aggregated, they will be recorded. *2: when Attach is selected in List of Problem PCs, the correspondent terminal name will be displayed in each aggregation target item.</p> <p data-bbox="638 616 766 683"> Note</p> <hr data-bbox="638 683 1404 694"/> <p data-bbox="638 705 1085 728">About content recorded in E-mail body text</p> <p data-bbox="638 750 1404 840">The content notified by using the E-mail notification function is the aggregation result during the E-mail notification. After the next aggregation (once per day), the result may be inconsistent with that in the status window.</p> <hr data-bbox="638 851 1404 862"/>
List of Fault PCs	<p data-bbox="638 884 1332 907">Set whether to record the list of aggregated PCs in the E-mail body text.</p> <ul data-bbox="654 929 1404 1041" style="list-style-type: none"> - Not attach: Not to record the list of problem PCs. - Attach: Record the list of problem PCs. (Up to 1000 error PCs can be recorded.) <p data-bbox="638 1064 861 1086">Initial value: not attach</p>
PCs that exported files (all conditions are aggregated as AND conditions)	
Item Description	Description of the aggregated items.
Aggregation of Items	Set whether to display the aggregation result in the status window or not. Initial value: 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. Initial value: 7 days
Type of Operation	Select from file export, file operation (move, copy and rename) as the type of operation log of counting target. Multiple selection can be made. At least one must be selected. Initial value: File export
Settings of External Memory Media Type	Select from Removable, CD/DVD and Network as the drive type of external memory media. Multiple can be selected. At least one must be selected. Initial value: Removable
Filtering Settings	Set keyword contained in the file path of export source. By specifying the path of the shared folder as a keyword, aggregation can be performed when exporting files of specific shared server only. To specify multiple keywords, enter a single-byte space between each of them. Up to 10 keywords can be specified. As single-byte space is used as a separator, it cannot be used as a keyword. Specify up to 128 (halfwidth or fullwidth) characters, including delimiter characters. The alphabetic characters are case-insensitive. When specifying shared folder, specify as follows.

Item Name	Description
	\\server name\folder name \\IP address\folder name Initial value: (blank) Refer to " 1.2.45 IPv6 Support " for details on specifying IPv6 addresses.
PCs used out of working time (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. Initial value: Yes
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. Initial value: 7 days
Settings of Non-working Time	Define the time frame as "Non-working Time". <ul style="list-style-type: none"> - Day of a week: select which day to be set as non-working time. At least one must be selected. - 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 "-". Initial value: <ul style="list-style-type: none"> - Pattern 1 (supposed from Monday to Friday) <ul style="list-style-type: none"> - Day of the week: Monday, Tuesday, Wednesday, Thursday, Friday - Time: from 00:00 to 08:59 and 17:00 to 23:59 - Pattern 2 (supposed on weekend supposed) <ul style="list-style-type: none"> - Day of the week: Saturday, Sunday - Time: Not specified  Example <hr style="border-top: 1px dotted blue;"/> <p>Specification Example 1</p> <p>When aggregating PCs used at weekends</p> <ul style="list-style-type: none"> - Time: not specified - Day of the week: Saturday and Sunday are selected <p>Specification Example 2</p> <p>When aggregating PCs used during non-working time from Monday to Friday</p> <ul style="list-style-type: none"> - Time: 00:00 to 08:59 or 17:00 to 23:59 - Day of the week: Monday, Tuesday, Wednesday, Thursday, Friday selected <hr style="border-top: 1px dotted blue;"/> <p>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.</p>
PCs that performed suspicious access (all conditions are aggregated as AND conditions)	

Item Name	Description
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. Initial value: 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. Initial value: 7 days
Settings of Access Type	Set access type. <ul style="list-style-type: none"> - Start in safe mode: it is aggregated when the PC is started in safety mode. - Login with local user: in the environment where the domain is used, it is aggregated when logging in as local user. - Login with administrator authority: it is aggregated when logging in with administrator authority. Initial value: Start in safe mode
PCs not connected for a long period (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. Initial value: Yes
Aggregation period settings	Set the period with no connection. PCs that have not been connected for longer than the days set since the last connection (policy update) are aggregated. Number of days can be selected by the day from 1 to 366 days. Default value: 30 days
Smart devices not connected for a long period (Conditions are all aggregated as AND condition.)	
Item Description	Description of aggregation items.
Aggregation of items	Specify whether to aggregate or not. If you select not to aggregate, this item will not be displayed in the status window. Default value: Yes is selected.
Settings of Disconnection Period	Set the disconnection period. Mobile devices that have not been connected for longer than the days set since the last connection (policy update) are aggregated. Select by 1 day within 1-366. Initial value: 7 days
PCs that blocked the use of prohibited USB device PCs that blocked the use of prohibited account group Devices that blocked the use of prohibited application PCs that blocked prohibited printing PCs that blocked the sending of email 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. Initial value: 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. Initial value: 7 days

2.7.2 Prepare for Using Log Analyzer

This section explains the settings required for using the 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 four items must be set:

- Transmission target (Log Analyzer Server)
- Transmission source (Management Server)
- Log obtaining period
- **Data transfer**

When the transmission target and transmission source are being installed, set for transferring administrator information. For settings items, 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 **Start > Systemwalker Desktop Keeper > Server > Log Analyzer Settings Apps > Systemwalker Desktop Keeper > Log Analyzer Settings** and start the **Log Analyzer Server Settings** window.

2. Set the start date for log obtaining in **Log obtaining period** in the **Data Transfer Settings** tab.

Relationship between configuration value of log obtaining period and transferred logs

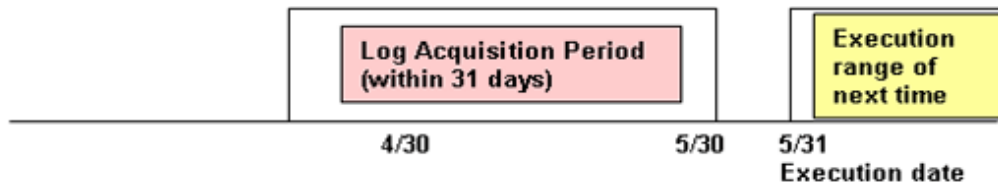
Log transmission considers logs of the days before the task operation day (the day of executing data transmission command) as its target. The log obtaining period, as the target date, is the date on which logs are registered to the Management Server, rather than the time when operation logs are generated 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.

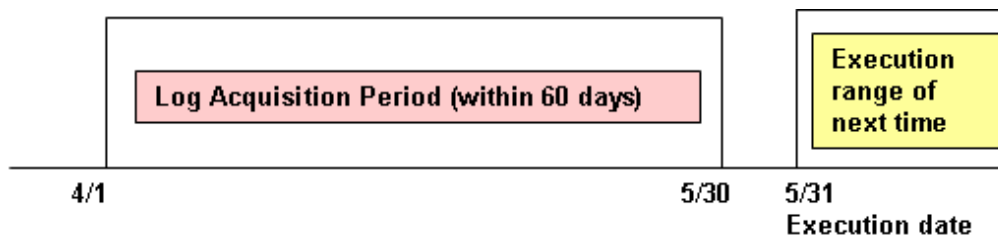
The following is the example of executing a task on May 31st.



- 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, 2013 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 Setting Data Transfer Time on the Management Server

Transfer logs and user information from the Management Server to the Log Analyzer Server.

Register data transfer tasks to the Log Analyzer Server to the Tasks feature of the operating system on which Management Server is running, and enable regular transfer of data. When transferring data to the Log Analyzer Server, 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

For the data transfer start time, specify the time of day during which fewer users are on the client (CT).

While the log data is being saved and sent during data transfer, the following services of Management Server will be stopped. Therefore, 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, do not transfer at the above time frame.

If any item other than the task start time has been changed in "7.12.3 Change the Data Transfer Task on the Management Server" and the start time settings are changed using this tool, the values set for all items other than the start time will revert to default values.

The following describes the settings procedures.

1. Click **Start > Systemwalker Desktop Keeper > Server > Log Analyzer settings**, or **Apps > Systemwalker Desktop Keeper > Log Analyzer settings**, to start the **Log Analyzer Server Settings** window.

The screenshot shows the 'Log Analyzer Server Settings' window with the 'Server Information Settings' tab selected. The window is organized into four main sections:

- Transmission destination (Log Analyzer Server):** Includes a text box for 'Log transmission destination shared folder (format: \\<ip address>\<folder>)' with a 'Folder (H)' label, and two text boxes for 'Windows account for connecting shared folder' labeled 'Account (A)' and 'Password (P)'.
- Transmission source (Management Server):** Includes a text box for 'Folder for temporary log storage (format: <drive>\<folder>)' with a 'Folder (T)' label, and two text boxes for 'Database user ID (ID with backup and restore permissions set using Server Settings Tool)' labeled 'User ID (C)' and 'Password (W)'.
- Log obtaining period:** Features two radio buttons. The first is 'In the latest 31 days (initial value)' and is selected. The second is 'Period designation' with a date dropdown set to '5/12/2015' and the text 'Period up to the day before the running'.
- Data transfer:** Includes three dropdown menus for 'Start time' (set to '0'), 'Hour' (set to '00'), and 'Minute'. Below are two text boxes for 'Windows account for data transfer' labeled 'Account (U)' and 'Password (V)'.

At the bottom right, there are two buttons: 'Set (S)' and 'Exit (E)'.

2. In **Data transfer** in **Data Transfer Settings**, specify the data transfer start time and the information for the Windows account that will implement the data transfer task.
In **Windows account for data transfer**, specify a user with administrator privileges.

Information

Data transfer 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. Execute the following command when it is expected to keep the command prompt window.

```
cmd /c TRANS.bat [Enter]
```

2.7.2.1.3 Setting Data Import Time on the Log Analyzer Server

Save logs and user information from the Management Server to the database of the Log Analyzer Server.

In the Tasks feature of the operating system on which Log Analyzer Server is running, register the tasks for importing data to the Log Analyzer Server and deleting tasks, and enable regular data storage in the database.

Once data import in to the Log Analyzer Server is executed, the imported logs are aggregated at the same time as the import of the log data, and the aggregation result will be updated.

At this time, the difference between the aggregation results before and after the data import will be output as a log.

- [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 2013/04/21 01:00:00 is output

Start

20130421 operation happening day 20130408 information disclosure (0, 0, 0, 0, 0) terminal use (0, 0, 20) violation operation (0, 0, 0, 0, 0) printing volume auditing (0)

20130421 operation happening day 20130409 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, 2013, 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).

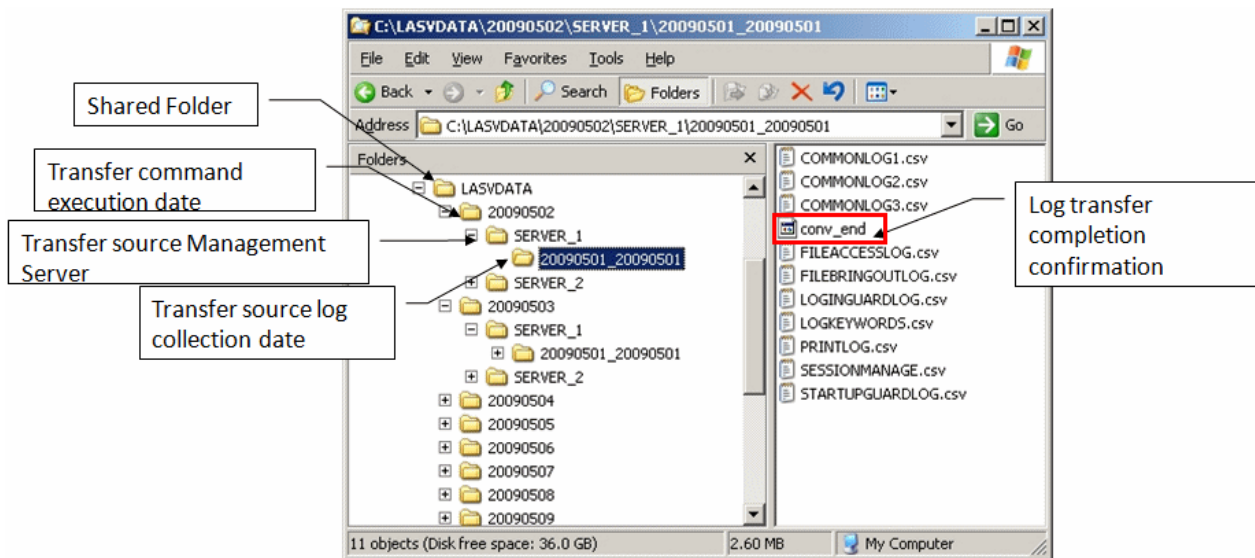
Note

To ensure disk capacity, 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, 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.

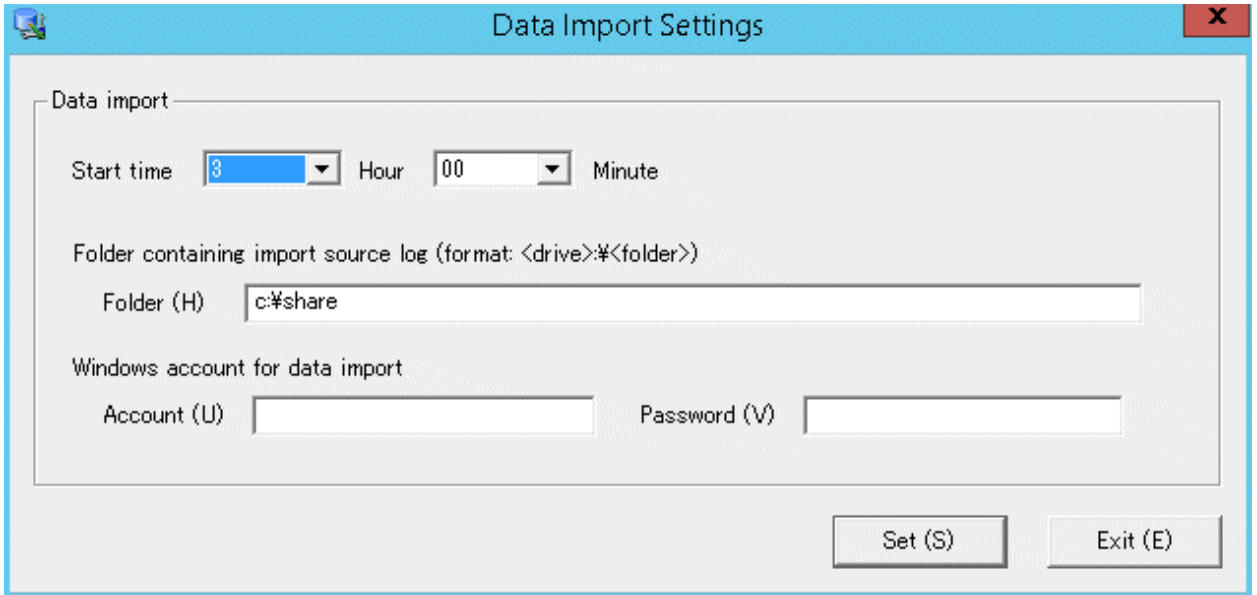
When "File for confirming the completion of log transmission (conv_end)" has been created in all "Folder of transmission source log collection day" in the "Transmission source Management Server name" folder under the "Transmission command execution day" folder in the above image, saving and deletion can be performed. Save and delete logs according to the "Transmission command execution day" folder unit.

If any item other than the task start time has been changed in "7.12.4 Change the Data Import Task on the Log Analyzer Server" and the start time settings are changed using this tool, the values set for all items other than the start time will revert to default values.

The following describes the settings procedure.

1. Log on to the Log Analyzer Server as the Log Analyzer user (the Windows account set during the Log Analyzer Server installation).

2. Select **Start > Systemwalker Desktop Keeper > Log Analyzer > Data Import Settings**, or **Apps > Systemwalker Desktop Keeper > Data Import Settings** to start the **Data Import Settings** window.



3. In the **Data Import Settings** window, set the start time for data import.

Item name		Description
Data import	Start time	This item is used to configure the settings to import data regularly. Specify the start time for data import. Set the start time of data import later than the data transfer start time so that the data import will start after execution of data transfer is finished.
	Account / Password	Specify the Windows account and its password used when constructing the database.

Information

Data can also be imported 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.



Note

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: Connect to the Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on the Management Server.
- Specify "http://host name or IP address of Management Server/DTK/index.html" in the address bar of the Brower.
When the port number of IIS is changed, specify as follows:
http://IP address: port number/DTK/index.html
Refer to "[1.2.45 IPv6 Support](#)" for details on the IPv6 specification.

In a 3-level system structure: Connect to the Master Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on the Master Management Server.
- Specify "http://host name or IP address of Master Management Server/DTK/index.html" in the address bar of the Brower.
When the port number of IIS is changed, specify as follows:
http://IP address: port number/DTK/index.html
Refer to "[1.2.45 IPv6 Support](#)" for details on the IPv6 specification.

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.

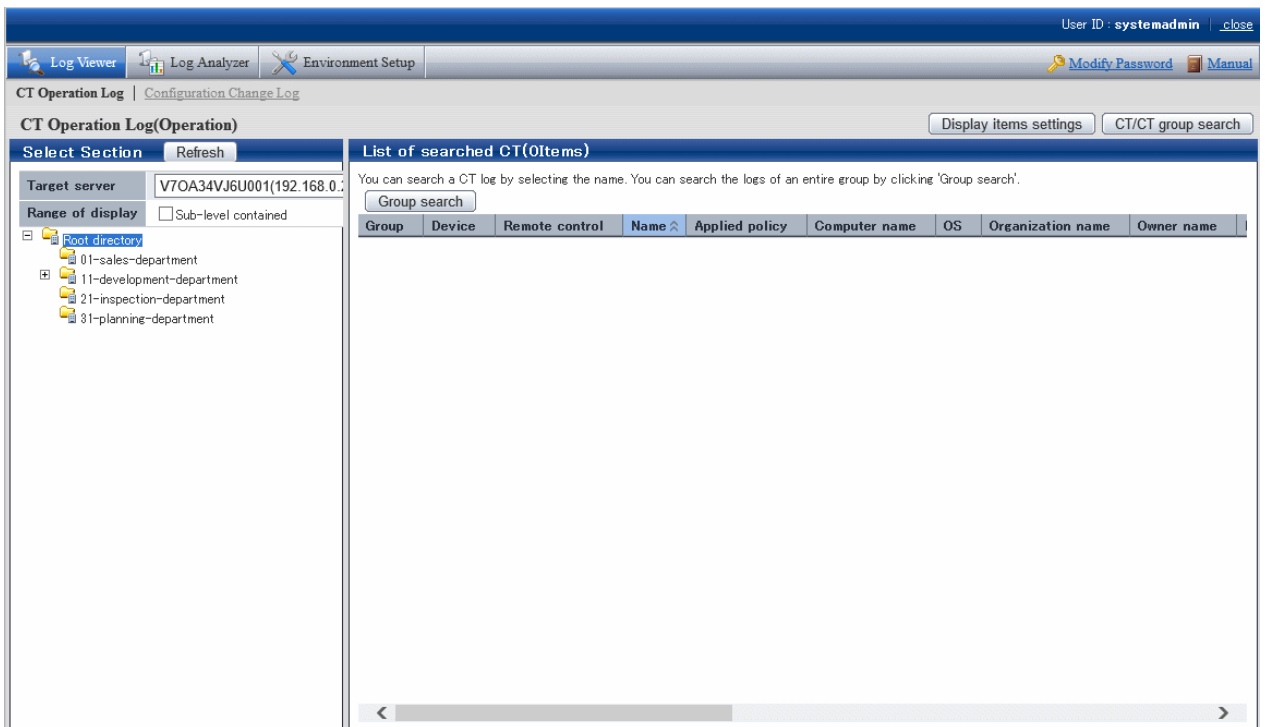
When using Log Analyzer, the system administrator with "Log Viewer" authority must be specified.

- **User ID**
- **Password**

It is recommended that the password be changed regularly. For details on how to do so, refer to "[Change password](#)".

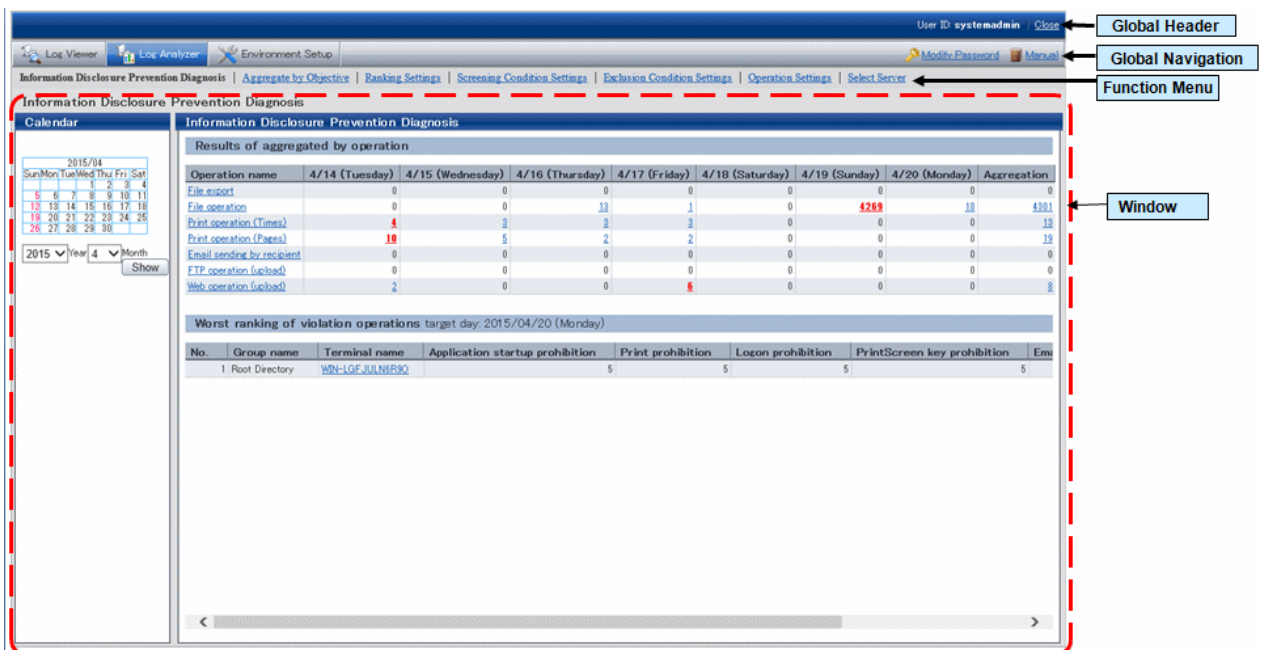
3. Click **Log Management** of Global Navigation in the displayed status window.

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.
- **Close:** 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, 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

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 [x] of the Brower, the warning 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).

Make sure to use **Logout** when closing the settings windows.

2.7.2.2.1 Set Ranking Display Number

Set the displayed number of the ranking number. The settings of the ranking display number will be displayed immediately after being modified.



Note

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)

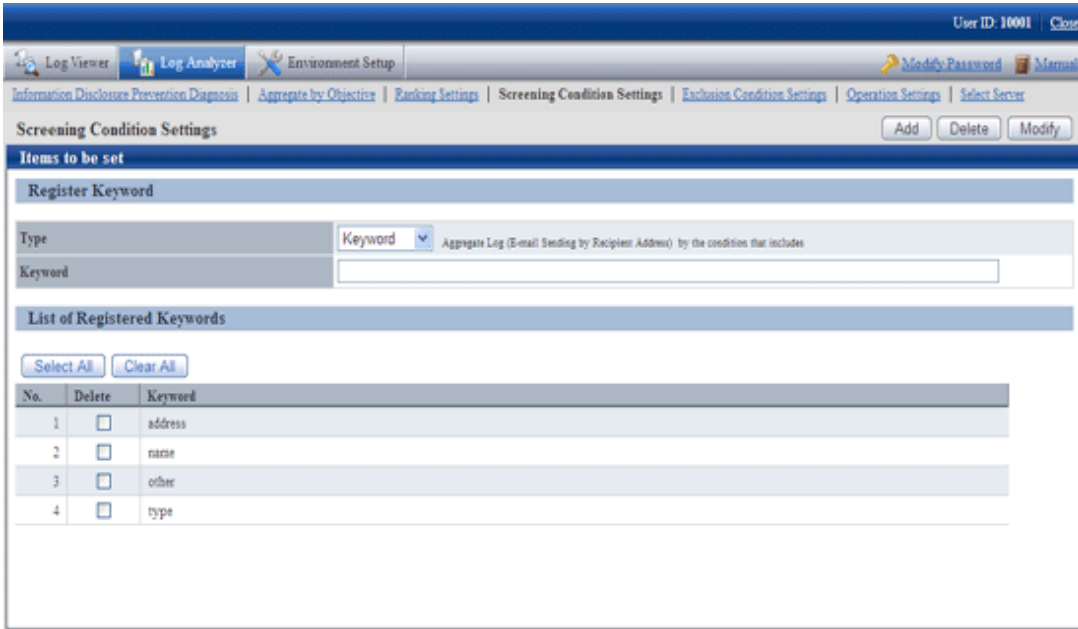
In order to apply the screening condition settings and aggregate before March 2, aggregation should not be performed again after the re-aggregation option of "DTTOOLEX.EXE (data transmission or deletion for the Log Analyzer Server)" has been executed.


 **Note**

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.  Note 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.

2. 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 40 fullwidth characters or Up to 80 halfwidth characters can be registered. However, the character string including ",", """, and halfwidth or fullwidth "_", "%" 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 FTP operation Web operation	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. Confirm how to record the logs.

For the keyword specified by the application, do not use capital single-byte letters and register it after modifying all of them to lowercase ones.

Up to 200 keywords not exceeding 4,000 halfwidth characters in total can be registered. Count any character that is not part of the Shift-JIS encoding as eight halfwidth characters.

3. Click the **Add** button.

Keywords are displayed in **List of Registered Keywords**.

4. 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, 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

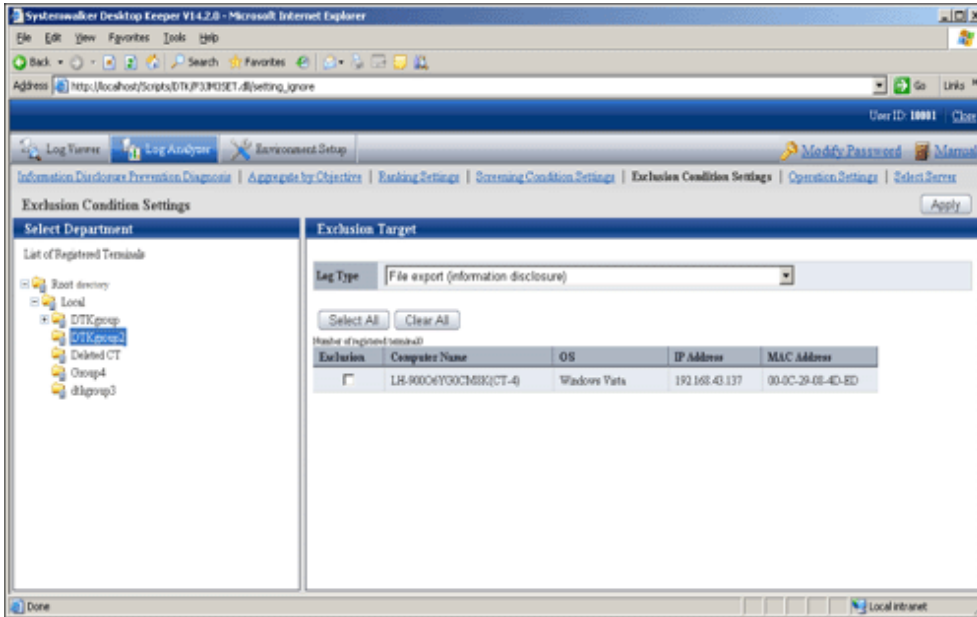
Do not modify conditions when moving logs or using Log Analyzer Server and Report Output Tool.


This may cause conflicts and errors in the aggregation result and diagnosis result or in the report output result.

About the smart device (agent) operation log

The smart device (agent) is displayed in the list but the smart device (agent) operation log is not aggregated in the Log Analyzer.

1. Select **Exclusion Condition Settings** of the function menu.
The following window is displayed.



Item Name	Description
<p>Select Department</p>	<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> Note</p> <p>.....</p> <p>About Not Configured group</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 directory" group instead of "Not Configured" group.</p> <p>.....</p> <ul style="list-style-type: none"> - Folder icon When a sub-folder exists, display/hide can be modified by clicking the icon. - 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.
<p>List of Registered Terminal</p>	<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>
<p>Exclusion Target</p>	<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"> - Number of Registered Terminals: This is the current number of terminals that are registered as excluded ones. - Exclude: This is selected when the item has become the excluded target.

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
FTP operation	Information disclosure analysis	FTP operation log (upload)
Web operation	Information disclosure analysis	Web operation log (upload)

- 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, 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

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. It is divided into two main sections: 'Information Disclosure Prevention Settings' and 'Eco auditing settings'.
Information Disclosure Prevention Settings:
 - 'Worst ranking of violation': Radio buttons for 'Display' (selected) and 'Not display'. Below are 'Ranking Display Number' (input field with '5') and 'Display in red' (input field with '10 items or more').
 - 'Set the day of a week to start weekly report': Radio buttons for Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday (selected).
 - 'Start the start date of monthly report': A dropdown menu showing '21' and the unit 'Day'.
 - 'Information Disclosure Prevention Diagnosis Operation': A checkbox for 'Desktop Log AnalyzerRun with compatibility'.
Eco auditing settings:
 - 'Settings of Start Month in a Year': A dropdown menu showing '4' and the unit 'Month'.
 - 'Printing volume auditing settings': Input fields for '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)), and '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"> - Display/Not Display the radio button. Select display/hide the ranking of violation operations displayed in the information disclosure prevention diagnosis window. - Ranking Display Number Specify a ranking display number within 1-99. - Display in red In the 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.
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 Settings of [Basic Information] tab in the Report Output Tool window.</p>

Item Name	Description
Start the start date of monthly report	<p>Specify the date as the start date of the monthly report.</p> <p>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> <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 Settings of [Basic Information] tab 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>
IP address display settings	<p>- Prioritize IPv4 addresses/Prioritize IPv6 addresses option button</p> <p>For a PC that has both an IPv4 address and IPv6 address, specify which is to be prioritized for display in the IP address field of the list of excluded PCs in the exclusion conditions setting window. The default setting is Prioritize IPv4 addresses.</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, specify the coefficient for calculating paper cost in RMB.</p> <p>Accurate to the second decimal place.</p>

Item Name	Description
	Value from 0.01 to 99.99 can be specified. The initial value is 0.60. In the printing volume auditing report, use this coefficient as the Paper cost equivalent to 1 page.
CO2 emission equivalent to 1 page (or 1 piece)	In the printing volume auditing 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. In the printing volume auditing report, use this coefficient as the CO2 emission equivalent to 1 page of printing paper.
Auditing Judgment Standard 1 Auditing Judgment Standard 2	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. 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. 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.

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

Do not select Log Analyzer Server when using Log Analyzer function and moving logs

This may cause conflicts and errors in the aggregation result.

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, 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. 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, 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), smart device (agent), 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

Follow the procedure below to search 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) and smart device (agent) to which the "Deleted CT" group belongs will also be searched.

The client (CT) and smart device (agent) 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.

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** check box of **Applied policy** should not be selected.

Search client (CT) and smart device (agent):

Specify the items of search condition.

Item Name	Description
Computer Name	Search according to the computer name or smart device (agent) model name of the client (CT). Results that partially match with the input conditions will be displayed. Up to 15 single-byte and double-byte characters can be entered.
IP Address	Search according to the IP address of the client (CT) or smart device (agent). The result of which the front part matches with the input conditions will be displayed.

Item Name	Description
	<p>For a dual stack network, search also for the IP address not displayed in the IP Address column in the CT list.</p> <p>If an IPv6 address is specified</p> <p>Specifying "0123:12" will include "123:12:", "123:12X.", and "123:12XX." in the result ("X" denotes a halfwidth numeric character). If conversion using RFC 5952 is possible, then specify the converted value.</p> <p>Example: If you entered "2001:db8:0:0:0:0:2:1", convert to "2001:db8::2:1" first, and then perform search.</p> <ul style="list-style-type: none"> - If an IPv4 address is specified <p>Specifying "10.1" will include "10.1.", "10.1X." and "10.1XX." in the result ("X" denotes a halfwidth numeric character).</p> <p>Enter in the format of "XXX.XXX.XXX.XXX".</p> <p>Example: 140.48.23.12</p> <p>For IPv4 addresses, specify up to 45 halfwidth numeric characters and periods. For IPv6 addresses, specify up to 45 halfwidth hexadecimal characters and colons.</p>
MAC Address	<p>Search according to the MAC address of the client (CT) or smart device (agent). The result that completely matches with the input conditions will be displayed.</p> <p>Enter in the format of "XX-XX-XX-XX-XX-XX". ("X" indicates one halfwidth alphanumeric character, and "-" is a halfwidth hyphen)</p> <p>Example: 02-E0-32-33-A3-C0</p>
Owner	<p>Search according to the owner set in the OS of the client (CT). Results that partially match with the input conditions will be displayed.</p> <p>Up to 93 single-byte and double-byte characters can be entered.</p>
CT Version	<p>Search according to the version of the client (CT) or smart device (agent) of the Systemwalker Desktop Keeper installed. Results that completely match with the input conditions will be displayed.</p> <p>Enter in the format of "X.X.X.X". ("X" indicates more than one halfwidth numeral characters, and "." is a halfwidth period)</p> <p>Example: 2.1.0.1</p> <p>Up to 15 halfwidth characters can be specified.</p>
Name/CT Group Name	<p>Search according to the name of the CT group, client (CT), or smart device (agent). Results that partially match with the input conditions will be displayed.</p> <p>Up to 40 single-byte and double-byte characters can be entered.</p>
DTPID	<p>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.</p> <p>Enter "<i>userId+pcName</i>" of the client (CT) of Systemwalker Desktop Patrol. (the plus sign must be halfwidth)</p> <p>Perform search with partial matching.</p> <p>Up to 41 halfwidth and fullwidth characters can be specified.</p>
Notes	<p>Search according to the notes entered when updating the client (CT) or smart device (agent) policy. Results that partially match with the input conditions will be displayed.</p> <p>Up to 128 single-byte and double-byte characters can be entered.</p>

Item Name		Description
Last Logon Date		The client (CT) and smart device (agent) communicate 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 halfwidth numeral character) Example: 20130701
Client Policy Update Date		Search according to the last date when the client (CT) or smart device (agent) obtained policy from the Master Management Server or Management. Enter in the format of "XXXXXXXX". ("X" indicates one halfwidth numeral character) Example: 20130922
Applied Policy	As Condition	When this check box is selected, the policy being applied to the client (CT) and smart device (agent) will be included in the search condition.
	CT	The search target is the client (CT) and smart device (agent) to which the CT policy is applied.
	Group	The search target is the client (CT) and smart device (agent) to which the CT group policy is applied.
Active Directory Linkage Target	As Condition	When this check box is selected, whether it is the client (CT) that imports information from Active Directory will be included in the search condition.
	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 check box 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.
Device	As Condition	Adds to the search condition PCs in which client (CT) is installed or smart devices in which smart device (agent) is installed.
	PC	Adds to the search condition PCs in which client (CT) is installed.
	Smart device	Adds to the search condition smart devices in which smart device (agent) is installed.
Remote control	As Condition	Adds to the search condition devices in which the remote control status is one of the selected values.
	Requesting	Adds to the search condition client (CT) and smart device (agent) that requested remote control.
	In progress	Adds to the search condition client (CT) and smart device (agent) on which remote control is in progress.
	Completed	Adds to the search condition client (CT) and smart device (agent) on which remote control has been completed.
	Not implemented	Adds to the search condition client (CT) and smart device (agent) on which remote control is not implemented.

Item Name	Description
Search	The search will be started and the results will be displayed.
Close Window	The entered search condition will be saved.

- 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**, refer to "[When modifying the displayed items and sequence](#)".

When double-clicking on the client (CT), smart device (agent) 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.

- 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 **x** 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.

Follow the procedure below to search:

- Start **Management Console**.
- Select **User Policy Settings** from the **User Settings** menu.
The **User Policy Settings** window is displayed.
- 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.

The screenshot shows the 'Management Console Search User/User Group' window. It features a search interface with the following elements:

- 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, with radio buttons for User and Group.
- Do not Apply User Policy:** As Condition, with radio buttons for Applied and Not Applied.
- Buttons:** Search, Close Window, and Select.
- Table:** A table with columns: Group name, Apply policy, Do not apply po..., User name/Gro..., User's name, Employee No., and Title. The table is currently empty.

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** check boxes 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 single-byte and double-byte characters can be entered. Alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified.
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 single-byte and double-byte characters can be entered. Alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified.
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 single-byte and double-byte characters can be entered. Alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified.
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 single-byte and double-byte characters can be entered. Alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified.
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 single-byte and double-byte characters can be entered. Alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified.
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 single-byte and double-byte characters can be entered. Alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified.
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 single-byte and double-byte characters can be entered. Alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified.
Applied Policy	As Condition	When this check box 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 check box 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.

6. Click the **Search** button.

The search results are displayed.

Group name	Apply policy	Do not apply policy	User name/Group name	User's name	Employee No.	Title	Org
System Development	User		FujitsuTaro	Fujitsu Taro			
System Development	User		FujitsuHanako	Fujitsu Hanako			

Search Result 2 Case(s)

When double-clicking on the user or user group that has been found, the **Management Console Search User/User Group** window will be displayed, and the correspondent user or user group will be in selected state. The **Management Console 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 **Management Console 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 x button at the top right of the **Management Console 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, all policies 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 items with modified settings.

Follow the procedure below to modify 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.

The screenshot shows the Management Console for the '1st-sales-department' group. The interface includes a menu bar, a toolbar, and a user ID of 'systemadmin'. The left pane shows a tree view with '1st-sales-department' selected. The main area displays a table of devices and a configuration panel for log collection settings.

Apply policy	Device	Remote control	Name	Computer name	MAC address	IP address	OS	CT classification
CT	Smart device		Android-001	FAR7	00-00-00-00-00-07	192.168.0.7	Android 4.2	SE
CT	PC		CT029	CT029	00-00-00-00-00-29	192.168.0.29	Windows Server 2012 (x64)	SE
CT	PC		CT076	CT076	00-00-00-00-00-76	192.168.0.76	Windows 7	SF

The configuration panel shows the following log collection settings:

- Application Startup Log: Yes No
- Application Termination Log: Yes No
- Window Title Obtaining Log (Web access log): Yes No
- E-mail Sending Log: Yes No E-mail content can be viewed
- Command Log: Yes No
- Device Configuration Change Log: Yes No
- Printing Operation Log: Yes No
- File Export Log: Yes No Backup Original File
- PrintScreen Key Operation Log: Yes No Capture Screen
- Web Operation Log: Yes No
- FTP Operation Log: Yes No
- Clipboard Operation Log (Virtual Environment): Yes No Backup Original File
- File Operation Log: Yes No
- Logon, Logoff Log: Yes No
- Linkage Application Log: Yes No

Buttons: All, None

Client Policy Update Date and Time: [] Server (DB) Update Date and Time: 2015/05/17 16:00:26

Apply Group Policy Not as Active Directory Linkage Target

Buttons: Refresh Policy, Update at Next Startup, Update Immediately, Create Policy Application Tool

Connection target server: localhost



In the following cases, 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

Select **Refresh Tree** from the **Tree Settings** menu to update.

3. Select the policy in the policy tree and modify it.

For description of policy setting items, 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**, 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

Each policy will be updated to the database, but it will not be updated to the client (CT) and smart device (agent) immediately. The timing with which the latest policy is reflected is shown below:

- Client (CT)
 - When communication is established with the server (either the Master Management Server or Management Server) to which the client (CT) will connect during the next startup of the client (CT)
- Smart device (agent)
 - When **Sync now** is clicked on the smart device (agent)
 - When automatic synchronization with the Management Server is executed (once a day between 12:00 and 13:00)

- When clicking the **Update Immediately** button

- Client (CT)

Each policy will be updated both in database and the running client (CT).

- The setting of **File export/read** 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 **Print/PrintScreen** 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 **Logon**, 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).

- Smart device (agent)

Each policy will be reflected on the database, but it will not be reflected on the smart device (agent) immediately. The timing with which the latest policy is reflected is shown below:

- When **Sync now** is clicked on the smart device (agent)
- When automatic synchronization with the Management Server is executed (between 12:00 and 13:00)

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, 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]

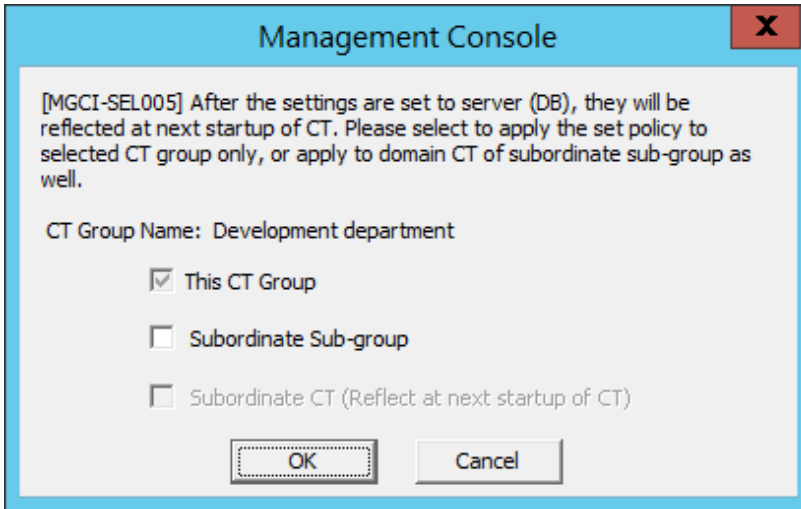
The timeout period for the connection of the client (CT) that is not connected to the Master Management Server or Management Server is 5 seconds for each client (CT). In addition, in spite of dependence on network environment, when performing **Update**

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) and smart device (agent) of the selected CT group. The **Name** and **Notes** of the subordinate client (CT) and smart device (agent) will not be overwritten. Selection can be performed when **Subordinate Sub-group** has been selected.

7. After **Name** or **Notes** has been modified, select **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), smart device (agent) or CT group policy to another client (CT), smart device (agent) or CT group.

After the copy of policy has been used, the same policy can be set at another client (CT), smart device (agent) or CT group.

Follow the procedure below:

1. Start **Management Console**.

2. Select the client (CT), smart device (agent) or CT group as the copy source.

- If client (CT) or smart device (agent) is selected

1. Select the CT group with the client (CT) or smart device (agent) registered as copy source from the CT group tree.

2. Select the client (CT) and smart device (agent) as the copy source from the CT list.

- If CT group is selected

1. Select the CT group as the copy source from the CT group tree.

3. Right-click the selected client (CT), smart device (agent) or CT group.

The pop-up menu is displayed.

4. Select **Copy Policy** from the displayed pop-up menu.

5. Select client (CT), smart device (agent) or CT group as the copy target.

- If client (CT) or smart device (agent) 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) or smart device (agent) as copy target from the CT list.

- If CT group is selected

1. Select the CT group tree as copy target from the CT group tree.

6. Right-click the selected client (CT), smart device (agent) or CT group.

The pop-up menu is displayed.

7. Select **Paste Policy** from the displayed pop-up menu.

The confirmation window for policy copying is displayed.

- If pasting to client (CT) or smart device (agent)

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.

- If 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, all policies 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 items with modified settings.

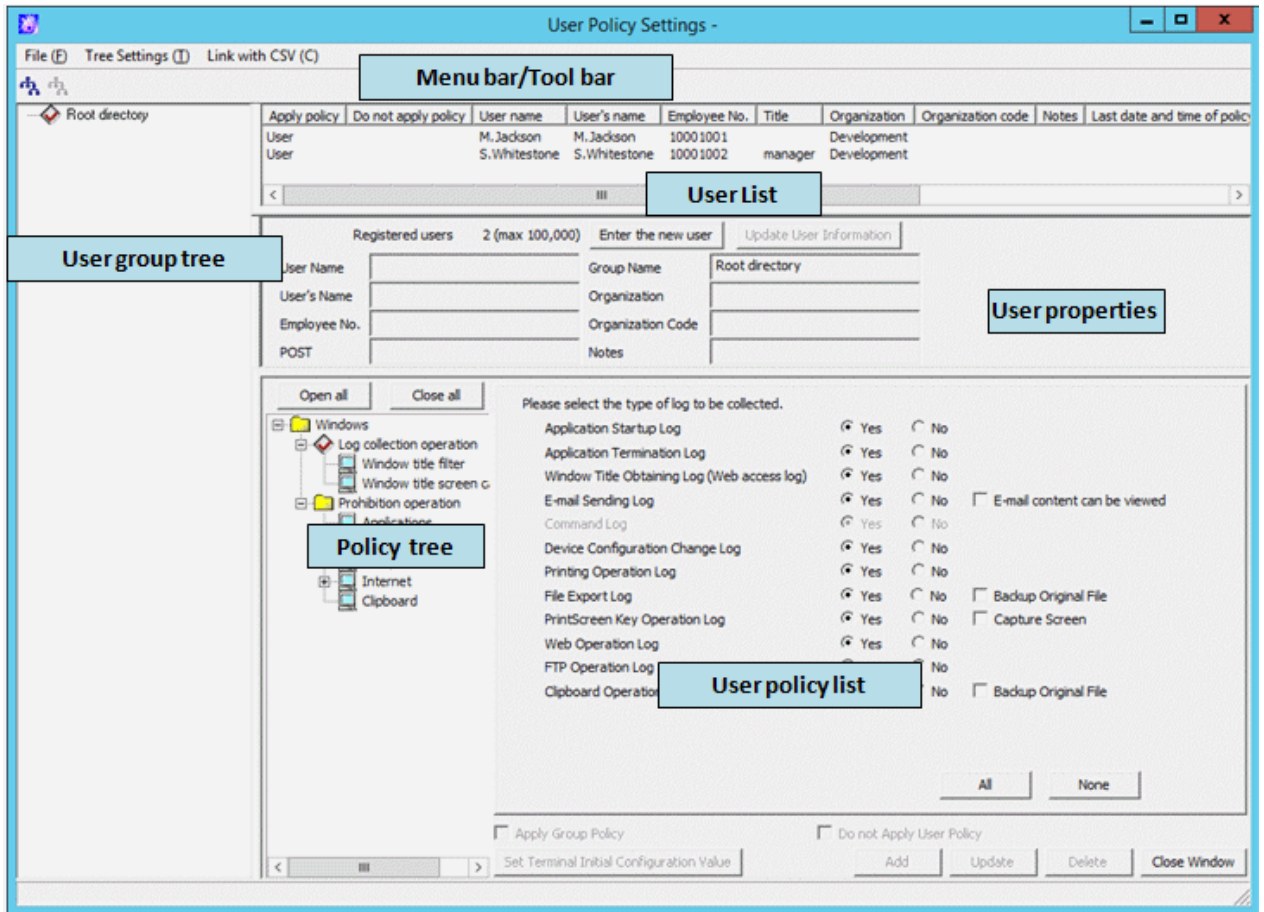
Follow the procedure below to modify a user group policy:

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, refer to "[Content Displayed in Window](#)".



3. Select the user group that requires policy modification from the user group tree.

4. Select the policy in the policy tree and modify it.

For description of policy setting items, 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.

Item Name	Displayed Content
	<ul style="list-style-type: none"> - User: Indicates the user policy has been set. - Group: Indicates the user group policy has been set.
Do not apply policy	<p>Whether the user policy is applied will be displayed.</p> <ul style="list-style-type: none"> - Not Applied: Indicates no user policy is applied. - (Blank): Indicates a user policy is applied.
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)	<p>Enter the user name for logging on Windows (different from the "Full Name" that can be set in user name).</p> <p>Up to 40 halfwidth (20 fullwidth) alphanumeric, kanji, hiragana and katakana characters, and symbols can be specified. Single-byte uppercase letters and single-byte lowercase letter will be recognized as the same character.</p> <p>However, errors will occur in the following cases:</p> <ul style="list-style-type: none"> - User name with a period "." only - User name with space only - User name that contains """/""\""[""]"";"" ""_"";""+""*""?""<"">""
User's Name	<p>Enter the name of the user that uses the user name.</p> <p>Up to 128 single-byte (64 double-byte) alphanumeric, kanji, hiragana and katakana characters, and symbols can be entered.</p>

Item Name	Input Content
Employee No.	Enter the employee number of the user that uses the user name. Up to 40 single-byte (20 double-byte) alphanumeric, kanji, hiragana and katakana characters, and symbols can be entered.
Title	Enter the title of the user that uses the user name. Up to 128 single-byte (64 double-byte) alphanumeric, kanji, hiragana and katakana characters, and symbols can be entered.
Group Name	Enter the group name of the user group. Up to 40 single-byte (20 double-byte) alphanumeric, kanji, hiragana and katakana characters, and symbols can be entered.
Organization	Enter the organization to which the user that uses the user name belongs. Up to 128 single-byte (64 double-byte) alphanumeric, kanji, hiragana and katakana characters, and symbols can be entered.
Organization Code	Enter the organization code to which the user that uses the user name belongs. Up to 40 single-byte (20 double-byte) alphanumeric, kanji, hiragana and katakana characters, and symbols can be entered.
Notes	Enter the notes of the user that uses the user name. Up to 128 single-byte (64 double-byte) alphanumeric, kanji, hiragana and katakana characters, and symbols 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, 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.
	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).

	Menu Bar	Tool Bar	Function Summary
	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 window. 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.

Follow the procedure below:

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.
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.
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) or smart device (agent) in the Management Console, a client (CT) needs to be installed on the PC that is a managed target, or an agent needs to be installed on the smart device. The following are two methods for allocating to the CT group of the client (CT) and smart device:

- Manually move the client (CT) and smart device (agent) under Root directory to a CT group
- Automatically allocate the client (CT) to a CT group using the automatic allocation file during CT registration



Once a CT is deleted from the Management Console, it no longer can be added, even if it is overwrite-installed. If this is the case, CT needs to be uninstalled and reinstalled or the re-register Client (CT) command needs to be executed. Refer to "Re-register Client (CT)" in the *Systemwalker Desktop Keeper Reference Manual* for details on the re-register Client (CT) command.

Manually move the client (CT) and smart device (agent) under root directory to a CT group

To add a new client (CT) and smart device (agent) in the CT group tree and CT list of the Management Console, install a CT on the PC that is the managed target, or agent on the smart device. Refer to "Install Client (CT)" in the *Systemwalker Desktop Keeper Installation Guide* for details on client (CT) installation. Refer to "Installing Smart Device (Agent) (Android)" or "Installing Smart Device (Agent) (iOS)" in the *Systemwalker Desktop Keeper Installation Guide* for details on smart device (agent) installation.

- For client (CT)

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, move it to the corresponding CT group.

- Smart device (agent)

The smart device (agent) will be added to the CT Group Tree and CT List during the initial synchronization with the Master Management Server or Management Server after installation. At this time, the smart device (agent) will be displayed directly under the root so move it to the corresponding CT Group.

Refer to "[Settings for Client \(CT\) and smart device \(agent\)](#)" for details on the mechanism of applying policy to the client (CT) and smart device (agent).

For the location where the client (CT) is displayed in the CT group tree, refer to "[Relationship between CT Group Policy and CT Policy](#)" or "[Display Configuration Information Tree](#)".

For details on how to move the client (CT), 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, refer to "[Create automatic distribution file during CT registration](#)".

Note

Smart device (agent) does not support the use of the automatic distribution file during CT registration for automatic distribution to the CT Group.

Only the client (CT) installed on the PC is the subject of the use of the automatic distribution file during CT registration for automatic distribution to the CT Group.

Note

For the following cases, update the information in the CT List to the latest version.

If either of the following conditions is satisfied, the information in the CT List for the Management Server under the Master Management Server displayed in the screen may not have been updated to the latest version.

- If the CT is added, moved, or deleted on the Management Server
- Link with Active Directory is executed, and the CT is added, moved, or deleted

To update the information to the latest version, click **Tree Settings > Refresh Tree**.

Note

Cause for the same CT being registered multiple times

When the same CT is registered multiple times under The Management Console, 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) or smart device (agent) displayed in the CT list to a CT group of the CT group tree.

The client (CT) or smart device (agent) displayed in the following locations can only be moved by the system administrator:

- Under Root directory
- Under domain group
- Under Local group

If using the Management Console connected to the Master Management Server in a system with a 3-level structure, moving across Management Servers is not possible.

When importing configuration information from Active Directory, for the moving of CT, refer to "[Display Configuration Information Tree](#)".

Follow the procedure below:

1. Start **Management Console**.
2. Select the CT group in which the client (CT) and smart device (agent) to be moved is registered, from the CT group tree.
3. Select the client (CT) and smart device (agent) to be moved from the CT list.

4. Move the client (CT) and smart device (agent) to the target CT group using drag and drop.

The client (CT) and smart device (agent) are 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 or smart device (agent) displayed in the CT list.

The client (CT) or smart device (agent) 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, refer to "[Display Configuration Information Tree](#)".

After a CT has been deleted, it will be moved to "Deleted CT" group

After a client (CT) or smart device (agent) has been deleted and the configuration information has been updated in the Management Console, it will no longer be displayed in the Management Console.

At this time, the client (CT) or smart device (agent) 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) or smart device (agent) 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) or smart device (agent) that has been moved to the "Deleted CT" group can be reused. In this case, move the client (CT) or smart device (agent) 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) or smart device (agent) 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) or smart device (agent) that belongs to the "Deleted CT" group has been deleted and the configuration has been updated, it 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) or smart device (agent) in the Management Console again, the CT in the target PC, or the agent in the smart device, needs to be uninstalled and re-installed. For installation of the client (CT), refer to "Install Client (CT)" of *Systemwalker Desktop Keeper Installation Guide*.

Refer to "Installing Smart Device (Agent) (Android)" or "Installing Smart Device (Agent) (iOS)" in the *Systemwalker Desktop Keeper Installation Guide* for details on smart device (agent) installation.

However, the client (CT) or smart device (agent) displayed in the Management Console after re-installation will be regarded as a CT that is different from the deleted one. Therefore, even it is displayed again, logs before deletion cannot be viewed in the Log Viewer.

Follow the procedure below:

1. Start **Management Console**.
2. From the CT group tree, select the CT group in which the client (CT) or smart device (agent) to be deleted is registered.
3. From the CT list, select and right-click the client (CT) or smart device (agent) to be deleted.

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) or smart device (agent) 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 client (CT) or smart device (agent) 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, refer to "[Display Configuration Information Tree](#)".



Point

When managing user policies collectively, operate from Master Management Server

In the Server Settings Tool, when user policies are collective management, 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, refer to "User Information" of *Systemwalker Desktop Keeper Reference Manual*.



Note

Set registration information correctly

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

Follow the procedure below:

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 policy 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 **Windows > Log collection operation** in the **User Policy Settings** window, the buttons for collecting these logs do not exist. When collecting the following logs, 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, 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

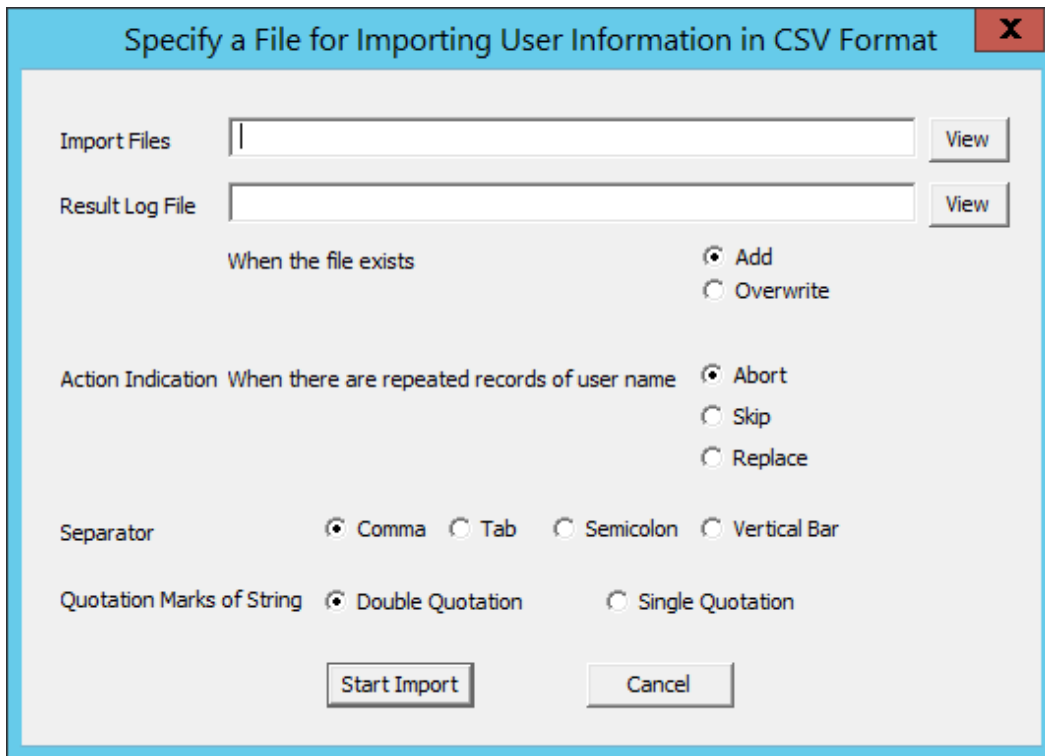
This section describes how to allocate users collectively using the CSV file.

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
<p>Import Files (Required)</p>	<p>Specify the created CSV file. The specification method is as follows:</p> <ul style="list-style-type: none"> - Enter the file name with full path - Enter the full path of a CSV file in the input field. - Enter by the View button <p>When the Specify an imported file window is displayed, click the Open button after the imported CSV file has been specified.</p> <p>The maximum length of the full path is 218 halfwidth characters (109 fullwidth characters). In addition, the following symbols cannot be used in a file name: "\"/":;*?"'""<">" "</p> <p>Refer to "User Information" in the <i>Systemwalker Desktop Keeper Reference Manual</i> for details on the specification of the CSV file for importing.</p>
<p>Result Log File (Required)</p>	<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"> - Enter the file name with full path - Enter the full path up to the output log file in the input field. - Enter by the View button - When the Specify result log file window is displayed, click the Open button after the output log file has been specified. <p>The maximum length of the full path is 218 halfwidth characters (109 fullwidth characters). In addition, the following symbols cannot be used in a file name: "\"/":;*?"'""<">" "</p>

Item Name	Description
When the file exists (Required)	In Specify result log file , select an output method when the log output file has already been specified: <ul style="list-style-type: none"> - Add Add operation log in case when the previous information still remains. - Overwrite Delete the remaining information and output the operation log to a new file.
Action Indication When there are repeated records of user name (Required)	Select one of the following operations if duplicate User Name exists when importing a CSV file: <ul style="list-style-type: none"> - Abort When there are duplicated User Name, suspend the import operation. The user information before suspension will be imported. - Skip Only the duplicated User Name will not be imported. Instead, user information of unduplicated User Name will be imported. - 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.
Separator (Required)	Select the separator that has been input when creating a CSV file. An error may occur in the case of wrong selection.
Quotation marks of String (Required)	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: <ul style="list-style-type: none"> - If a double quotation is used during the creation of a CSV file, but the single quotation is selected here, an error will occur. - 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.

An input example of the user information CSV import file is shown below:

```
'taro','Taro Fujitsu','100000','Department Manager','Administration Department','5555','Asset manager'
'hanako','Hanako Fujitsu','100001','Section Manager','Administration Department','5555',''
```

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, 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, refer to "[Register Users Collectively Using CSV File](#)".

Update through a window

Follow the procedure below:

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.
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

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)

Follow the procedure below:

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 using drag and 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.

Follow the procedure below:

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 a client (CT) or smart device (agent) that belongs to the "Deleted CT" group cannot be changed. The name and notes cannot be modified as well.

Follow the procedure below to modify a CT policy:

1. Start **Management Console**.
2. From the CT group tree, select the CT group to which the client (CT) or smart device (agent) that requires policy modification belongs.

The latest policy information is displayed.



In following cases, 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

Select **Refresh Tree** from the **Tree Settings** menu to update.

3. From the CT list, select the client (CT) or smart device (agent) that requires policy modification.
4. From the policy tree, select the policy and modify it.
Refer to "[2.4.1 Perform Terminal Initial Settings](#)" for details on policy setting items.
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, Katakana, or symbols can be entered.
- **Notes:** Up to 127 single-byte characters (63 double-byte characters) including alphanumeric characters, Chinese characters, Hiragana, Katakana, or symbols can be entered.

6. Click any of the following buttons to update policy to the CT.

- When clicking the **Update at Next Startup** button

Each policy will be updated to the database, but it will not be updated to the client (CT) or smart device (agent) immediately. The timing with which the latest policy is reflected is shown below:

- Client (CT)
 - When communication is established with the server (either the Master Management Server or Management Server) to which the client (CT) will connect during the next startup of the client (CT)
- Smart device (agent)
 - When **Sync now** is clicked on the smart device (agent)
 - When automatic synchronization with the Management Server is executed (between 12:00 and 13:00)
- When clicking the **Update Immediately** button

- Client (CT)

Each policy will be updated both in database and the running the client (CT).

- The setting of **File export/read** 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 **Print/PrintScreen** 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**, 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).

- Smart device (agent)
- Each policy will be reflected on the database, but it will not be reflected on the smart device (agent) immediately. The timing with which the latest policy is reflected is shown below:
 - When **Sync now** is clicked on the smart device (agent)
 - When automatic synchronization with the Management Server is executed (between 12:00 and 13:00)

Point

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) and smart device (agent)

Even if the CT policy is not applied to the client (CT) and smart device (agent), the group policy of the CT group to which the client (CT) and smart device (agent) belong can still be applied. At this time, select the **Apply Group Policy** check box to perform the policy update.

Select a CT group to collectively modify its subordinate client (CT) and smart device (agent) policies

When setting CT group policy, policy can also be set collectively for the subordinate client (CT) and smart device (agent) under the CT group. In this case, the configuration value of CT policy is the same as the value of CT group policy.

Refer to "[3.2.1 Modify CT Group Policy](#)" for details.

Copy CT Policy

The policy that has been set for the client (CT), smart device (agent) or CT group policy can be copied to another client (CT) and smart device (agent) or CT group.

Refer to "[Copy CT Group Policy or CT Policy](#)" for setting method.

Create Policy Application Tool

Note

Devices on which the policy application tool can be started

The policy application tool can be started on PCs on which clients (CT) are installed, but the tool cannot be started on smart devices on which smart devices (agent) are installed.

The tool that modifies the CT policy of the client (CT) that cannot connect to Management Server can be created.

Follow the procedure below:

1. Start **Management Console**.
2. Select the client (CT) to create the policy application tool.
3. Click the **Create Policy Application Tool** button.

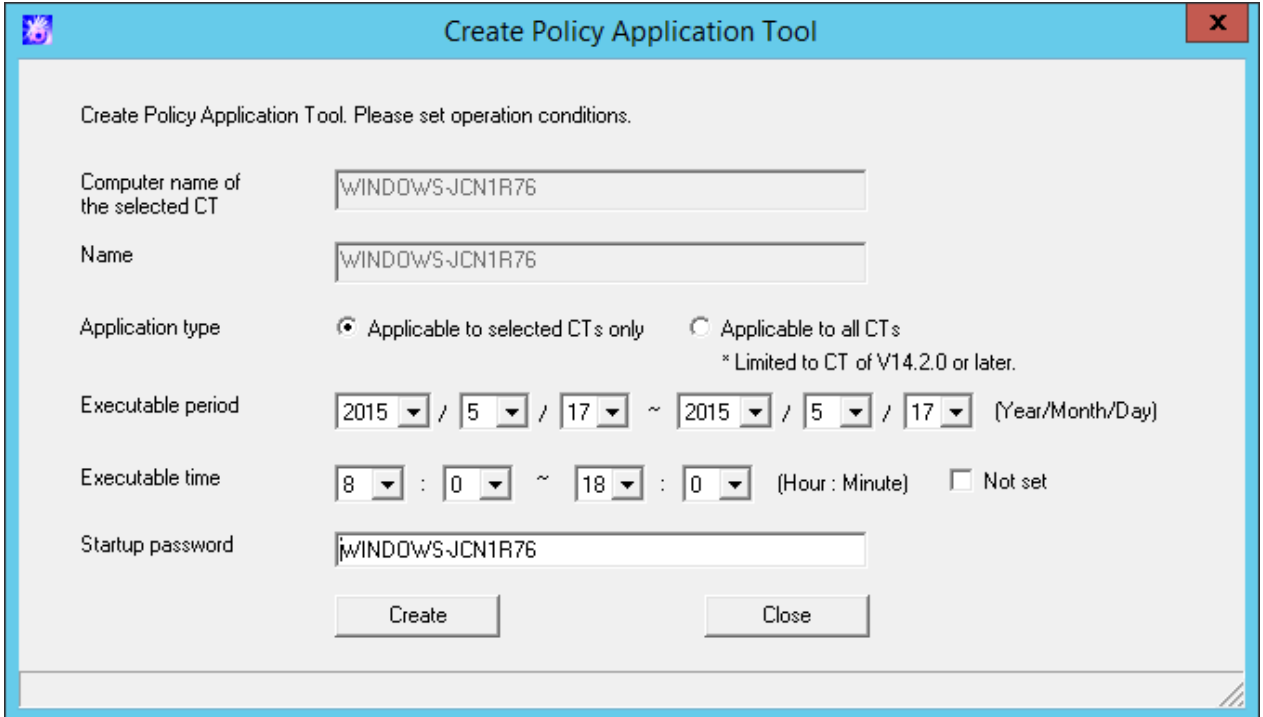
A window confirming whether to display the **Create Policy Application Tool** window will be displayed.

- Click **OK** to display the policy creation window, and click **Cancel** to cancel the policy creation.

Point

After **OK** is selected, a message indicating that the policy application tool is being created will be displayed in **Management Console**. During this period, the Management Console cannot be operated.

- 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"> - Applicable to selected CTs only Policy application tool can be executed in the selected client (CT) only. - Applicable to all CTs Policy application tool can be executed in all clients (CTs).
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

Item Name	Description
	Minute: 0-50 (in 10 mins) If Not set is ON, this setting will be invalid and only the period will be determined.
Startup password	Set the password entered when booting the policy application tool. <ul style="list-style-type: none"> - Up to 32 characters can be entered. - Only single-byte characters are allowed. - It is case sensitive. - The following symbols cannot be used: &, \, :, ?, ", ~, ^, ', <, >, , and single-byte space.

6. Click the **Create** button.
A window confirming whether to create the policy application tool will be displayed.
7. Select the **OK** button if there is no problem.
The **Browse For Folder** window is displayed. Select the destination for saving the policy application tool.
8. After the saving destination is selected, select the **OK** button.
A message confirming that the policy application tool has been output successfully will be displayed.
9. 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, 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

Follow the procedure below:

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. Select the policy in the policy tree and modify it.

The user specific policy can be set. For description of policy setting items, refer to "[2.4.1 Perform Terminal Initial Settings](#)".

- When setting the value of the **Terminal Initial Settings** window, click the **Set Terminal Initial Configuration Value** button. For the **Terminal Initial Settings** window, refer to "[2.4.1 Perform Terminal Initial Settings](#)".
- When applying the user group policy of the user group to which the user belongs, select the **Apply Group Policy** check box. (This is also applicable when multiple users are selected.)
- To temporarily cancel the application of user policy and apply the CT policy, select the **Disable User Policy** check box. To apply the user policy again, 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

Follow the procedure below:

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, refer to "[2.4.1 Perform Terminal Initial Settings](#)".

4. From the policy tree, select the policy and modify it.

For description of policy setting items, 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.

Refer to "[3.2.2 Modify User Group Policy](#)" for details.

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.

Refer to "[Copy User Group Policy or User Policy](#)" for details.

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.

Note

The CT information that belongs to the "Deleted CT" group cannot be exported to CSV files.

Follow the procedure below:

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"> - Enter a file name with full path Enter the full path of imported CSV file in the input field. - 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. <p>The length of the full path should be within 218 halfwidth characters (109 fullwidth characters). The following symbols are not allowed in a file name: " \ / : ; * ? " ' " < " > " "</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</p>

Item Name	Description
	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 V14.2.0 format. For item names of the exported CSV file and exported information, refer to "CT Information" of <i>Systemwalker Desktop Keeper Reference Manual</i> .

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, 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.

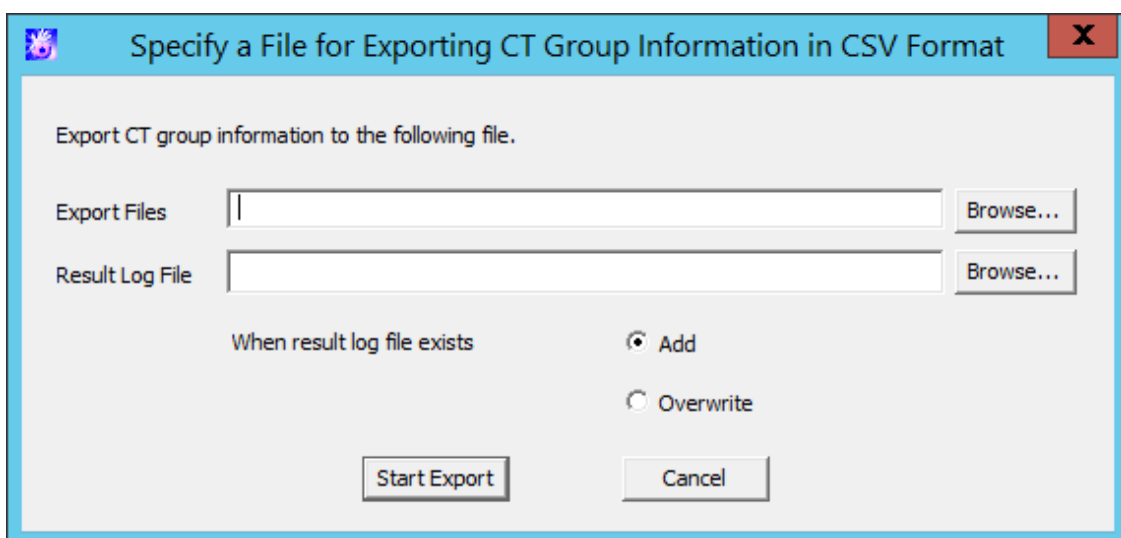
When CT group information is exported from the Management Console that connects to the Master Management Server, the group information of the CT under the Master Management Server will be exported.

When linking with Active Directory, only the information of the Local group can be exported.

Follow the procedure below:

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 halfwidth characters (109 fullwidth characters). The following symbols are not allowed in a file name: "\"/\"/:\"*\"?\"\"\"\"<\">\" \" - When it is not Windows Vista(R), Windows(R) 7, Windows Server(R) 2008, Windows(R) 8 or Windows Server(R) 2012 Initial Value: [OS Installation Drive]\Documents and Settings\Logon User Name\My Documents\DTKCTEntry.csv - When it is Windows Vista(R), Windows(R) 7, Windows Server(R) 2008, Windows(R) 8 or Windows Server(R) 2012 Initial Value: [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. Specify the full path using up to 218 halfwidth characters (109 fullwidth characters). However the following symbols are not allowed in a file name: "\"/\"/:\"*\"?\"\"\"\"<\">\" \" - When it is not Windows Vista(R), Windows(R) 7, Windows Server(R) 2008, Windows(R) 8 or Windows Server(R) 2012 Initial Value: [OS Installation Drive]\Documents and Settings\Logon User Name\My Documents\DTKCTEntry.log - When it is Windows Vista(R), Windows(R) 7, Windows Server(R) 2008, Windows(R) 8 or Windows Server(R) 2012 Initial Value: [OS Installation Drive]\User\Logon User Name \Documents \DTKCTEntry.log
When result log file exists	When the original result log file exists, 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, 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.

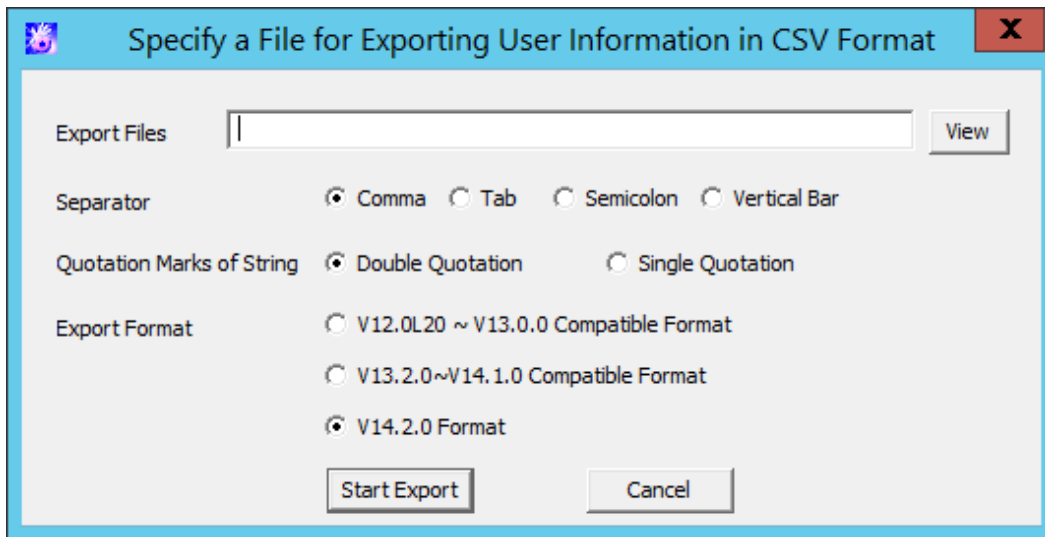
Follow the procedure below:

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"> - Enter a file name with full path Enter the full path of imported CSV file in the input field. - Enter by clicking the Browse 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. <p>The length of the full path should be within 218 halfwidth characters (109 fullwidth characters). The following symbols are not allowed in a file name: " \ / : * ? " " < " > " " "</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. <p>V12.0L20 ~ V13.0.0 Compatible Format: Export in the format that is same as V13.0.0 or earlier.</p> <p>V13.2.0 - V14.1.0 Compatible Format: Export in V13.2.0 format.</p> <p>V14.2.0 Format: Export in V14.2.0 format.</p> <p>For the item name of the exported CSV file and exported information, refer to "User Information" of <i>Systemwalker Desktop Keeper Reference Manual</i>.</p>

The CSV file is exported.

Among the exported items, if there is a character that is identical to the one selected in **Quotation Marks of String**, 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, click the **OK** button.

Note

The user information CSV output file is used for verifying registered user information and policy settings information.

The CSV file output here cannot be used to register using the feature described in "Register Users Collectively Using CSV File" in "3.3.2 Register a User". This is because there are too many items in the output CSV file.

Refer to "Output CSV files for use" in "User Information" in the *Systemwalker Desktop Keeper Reference Manual* for details on the output format for the user information CSV output file.

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, refer to "Upgrading the client (CT)" 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.

Follow the procedure below to export the file:

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.

CT Group Name: Development department

Export the IP address of subordinate CT to the following file.

Export Files Browse...

Result Log File Browse...

When result log file exists Add Overwrite

Start Export Cancel

- **Export Files** (Required): Specify the CSV file for exporting IP address with full path.

Specify the full path using up to 218 halfwidth characters (109 fullwidth characters). 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.

Specify the full path using up to 218 halfwidth characters (109 fullwidth characters). However the following symbols are not allowed in a file name.

\\\"/\"/:\"*\"?\"\"\"\"<\">\"|\"

- **When result log file exists:** When the original result log file exists, 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, 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.



Changing the service status and ending processes for the smart device (agent)

Changing the service status and ending processes for the smart device (agent) cannot be controlled from the Management Console.

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).

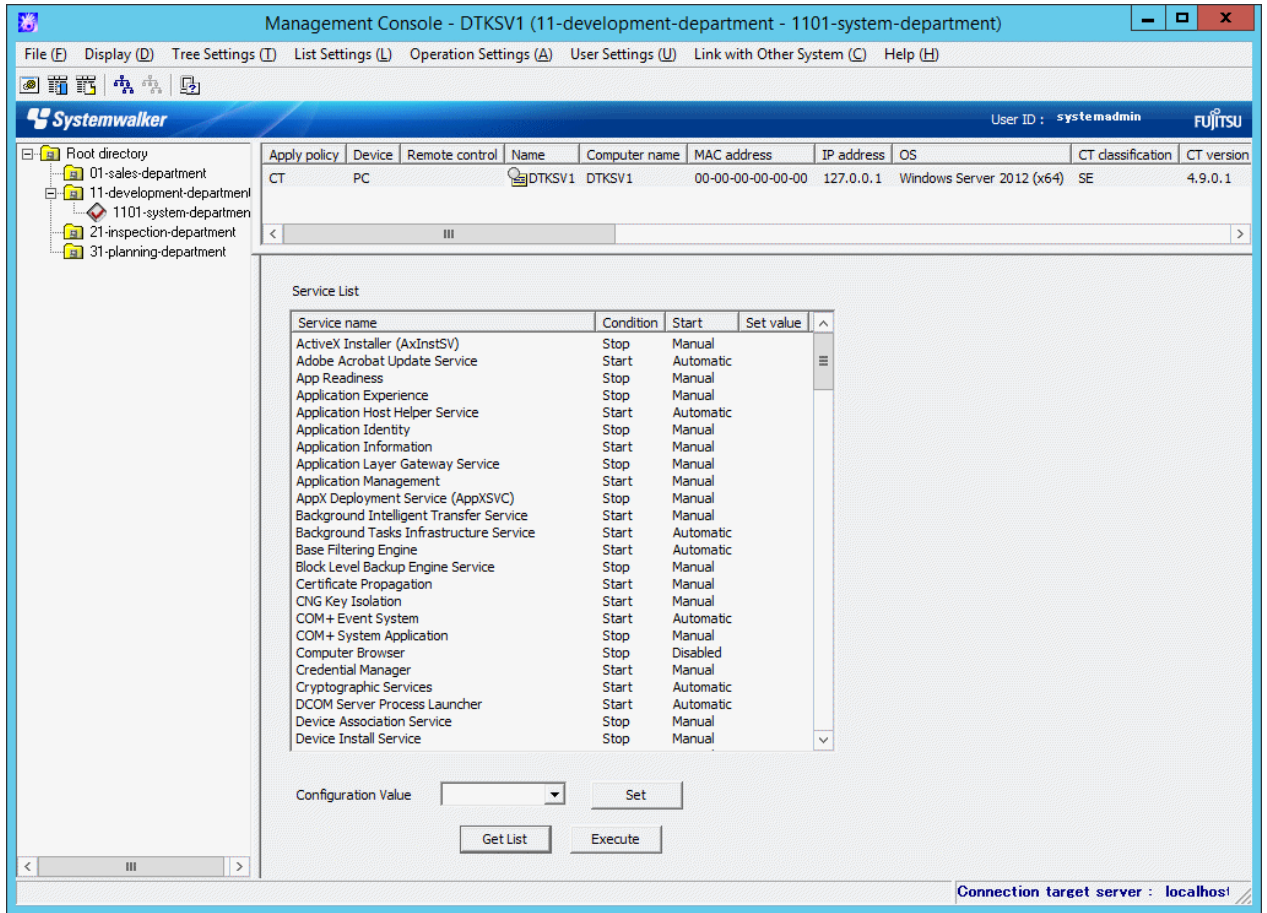
Follow the procedure below to view the service list:

1. Start the **Management Console**.
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.



Note

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.

Follow the procedure below to control services:

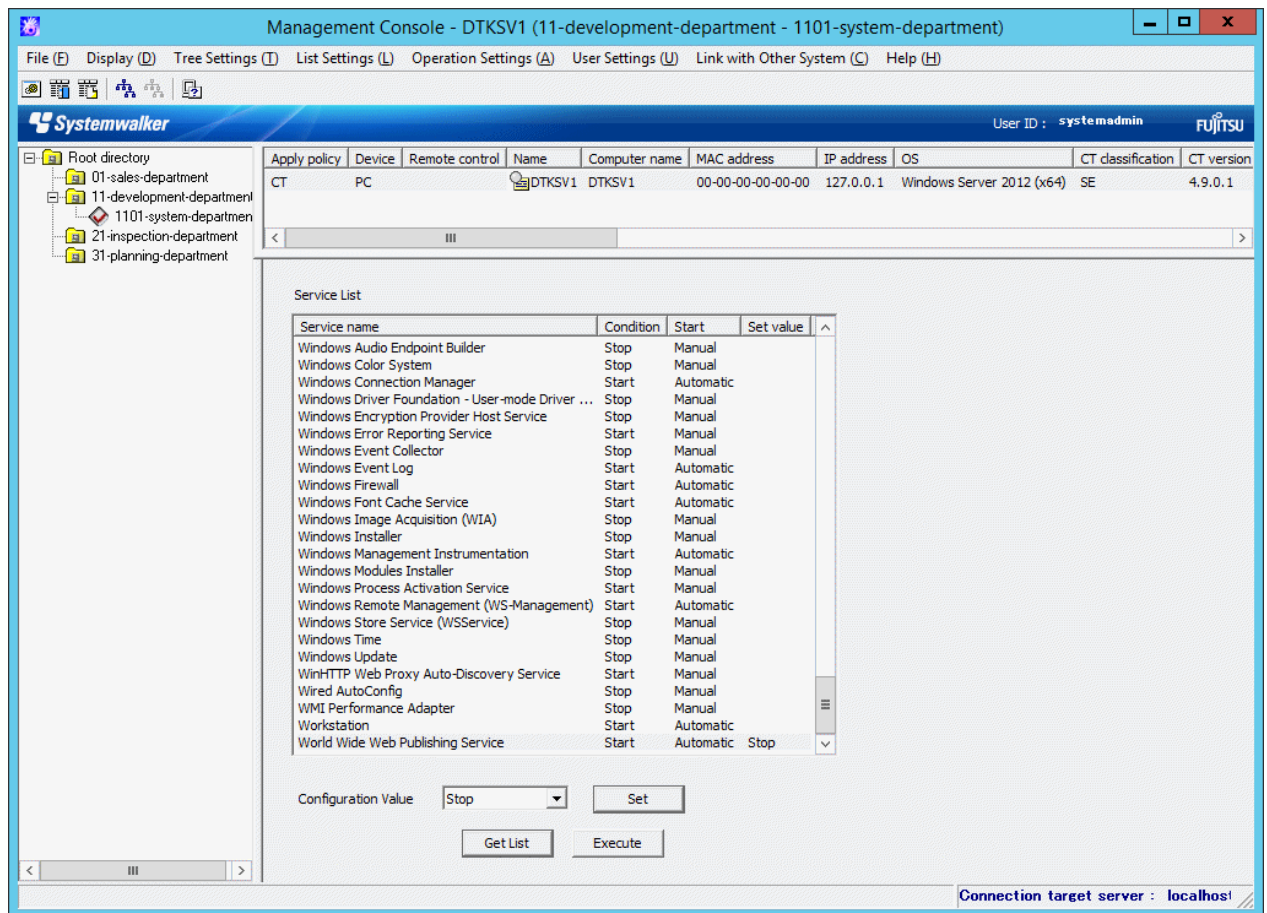
1. Start the **Management Console**.

- From the CT group tree, select the CT group to which the client (CT) with service control has been registered.
- From the CT list, select the client (CT) for service control, and select **Get/Control Service List** from the **Display** menu.
- Click the **Get List** button.

The list of services registered in the selected client (CT) is displayed.

- Select the lines to modify status from **Service List**.
- 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.



- 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(R) 64-bit Edition, Windows(R) 7 64-bit Edition, Windows Server(R) 2008 64-bit Edition, Windows Server(R) 2008 R2, Windows(R) 8 64-bit Edition and Windows Server(R) 2012, the processes running in 64-bit cannot be viewed.

- Part of the processes relating to Windows systems cannot be viewed.
Example:

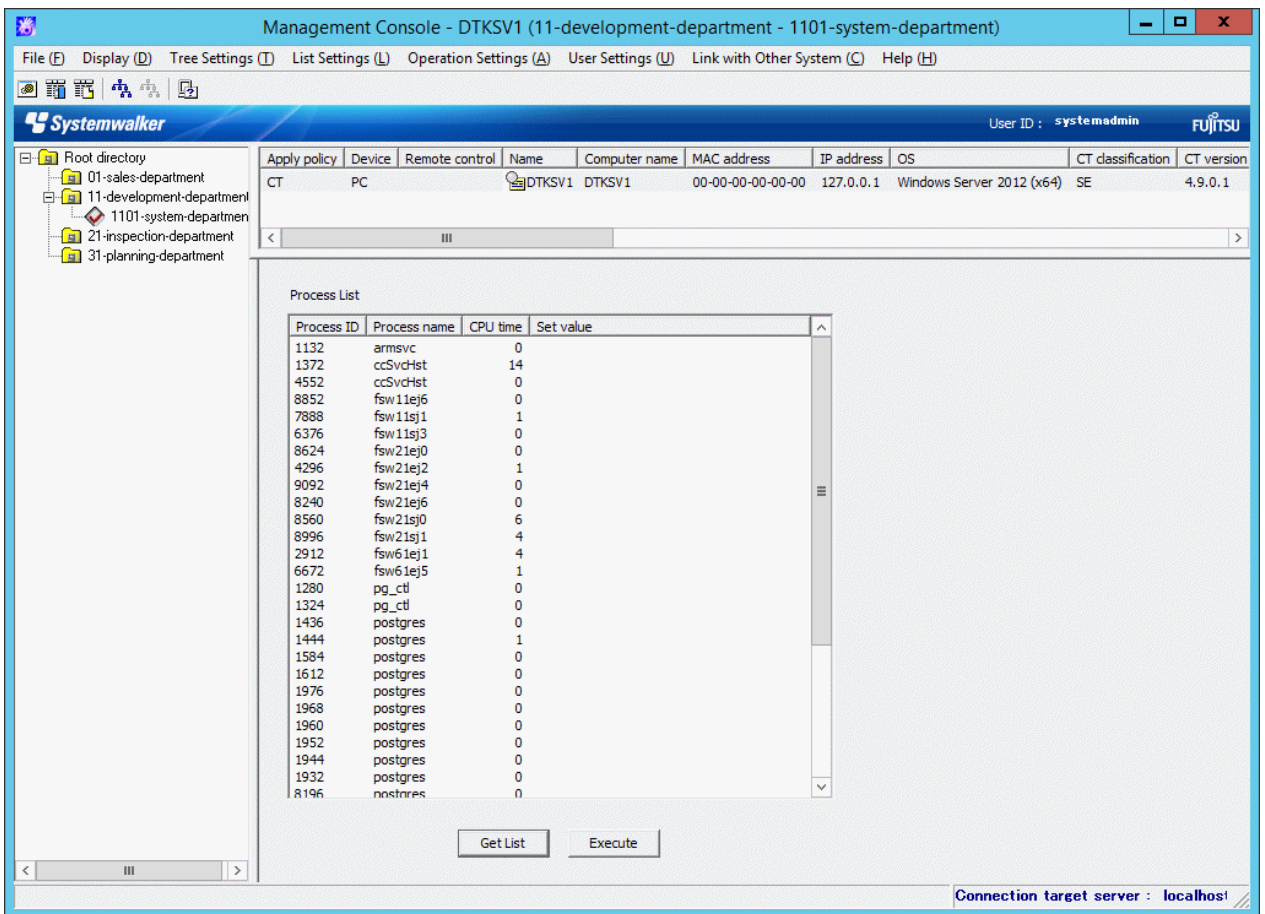
- System Idle process
- system



Follow the procedure below to view the process list:

1. Start **Management Console**.
2. From the CT group tree, select the CT group to which the client (CT) for viewing process list has been registered.
From the CT list, select the client (CT) for viewing process list, and select **Get/Control Process List** from the **Display** menu.
3. 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).



Note

View Processes

- In case of Windows Vista(R) 64-bit Edition, Windows(R) 7 64-bit Edition, Windows Server(R) 2008 64-bit Edition, Windows Server(R) 2008 R2, Windows(R) 8 64-bit Edition and Windows Server(R) 2012, 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(R) 64-bit Edition, Windows(R) 7 64-bit Edition, Windows Server(R) 2008 64-bit Edition, Windows Server(R) 2008 R2, Windows(R) 8 64-bit Edition and Windows Server(R) 2012, processes cannot be terminated.

Messages output when multiple users are logged on concurrently

When multiple users are logged on concurrently, the messages output during control of processes and services will only be output to specific users. The conditions under which these messages will be output are shown below:

- If there are users who are logged on locally, the message(s) will be output to these users
 - If there is no user who is logged on locally, then the message(s) will be output to only one of the users who are logged on remotely
-

Follow the procedure below to control processes:

1. Start **Management Console**.
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**.

6. Double-click the selected line.

End is displayed in **Set value**.

The screenshot shows the Systemwalker Management Console interface. The title bar reads "Management Console - DTKSV1 (11-development-department - 1101-system-department)". The menu bar includes "File (F)", "Display (D)", "Tree Settings (T)", "List Settings (L)", "Operation Settings (A)", "User Settings (U)", "Link with Other System (C)", and "Help (H)". The user ID is "systemadmin" and the logo "FUJITSU" is visible. On the left, a tree view shows a hierarchy of departments: "01-sales-department", "11-development-department", "1101-system-department", "21-inspection-department", and "31-planning-department". The main area displays a table with columns: "Apply policy", "Device", "Remote control", "Name", "Computer name", "MAC address", "IP address", "OS", "CT classification", and "CT version". The table contains one row: "CT", "PC", "DTKSV1", "DTKSV1", "00-00-00-00-00-00", "127.0.0.1", "Windows Server 2012 (x64)", "SE", and "4.9.0.1". Below this is a "Process List" table with columns: "Process ID", "Process name", "CPU time", and "Set value". The "Process List" table contains the following data:

Process ID	Process name	CPU time	Set value
1132	armsvc	0	
1372	ccSvcHst	14	
4552	ccSvcHst	0	
8852	fsw11ej6	0	End
7888	fsw11ej1	1	
6376	fsw11ej3	0	
8624	fsw21ej0	0	
4296	fsw21ej2	1	
9092	fsw21ej4	0	
8240	fsw21ej6	0	
8560	fsw21ej0	6	
8996	fsw21ej1	4	
2912	fsw61ej1	4	
6672	fsw61ej5	1	
1280	pg_ctl	0	
1324	pg_ctl	0	
1436	postgres	0	
1444	postgres	1	
1584	postgres	0	
1612	postgres	0	
1976	postgres	0	
1968	postgres	0	
1960	postgres	0	
1952	postgres	0	
1944	postgres	0	
1932	postgres	0	
8196	postgres	0	

At the bottom of the process list, there are two buttons: "Get List" and "Execute". The status bar at the bottom right shows "Connection target server : localhost".

7. Click the **Execute** button.

The End of process will be updated to the client (CT).

3.7 Controlling Smart Device (Agent)

The system administrator must control operation to prevent improper use of smart devices that users may have lost.

3.7.1 Controlling Smart Device (Agent) Remotely

This section describes how to control smart device (agent) remotely.



Note

Remote control wipe

Remote control wipe restores the smart device to its factory settings, and therefore it will not be possible to manage it until the smart device (agent) is reinstalled.

Reflecting policies (Android)

Remote control works as a client-side operation (Pull type) that obtains policies from the smart device. Unlike the server-side operation (Push type) which distributes policies from the server, therefore, policies are not reflected in real time.

Once remote control is executed, it will take up to one hour before its application to the smart device takes place.

If you are using Wi-Fi to connect to the server, however, it may take longer, depending on the conditions of the network connection. In this case, remote control will be applied at the time when Wi-Fi communication becomes available.

Phonebook application (Android)

Phonebook applications store information such as history in their unique storage areas, and therefore some of its data cannot be accessed from other applications.

History for such applications cannot be deleted even with remote control data deletion.

Remote control wipe, however, erases data completely, and even history will be deleted.

Deleting the web access history (Android)

By deleting the web access history, the information listed in **History** and **Bookmark** will be deleted, but the URL on the browser cannot be deleted. If multiple tabs are opened, the URLs on these tabs cannot be deleted.

Behaviors when multiple remote operations are requested (Android)

If multiple remote operations are requested for a single smart device, the smart device (agent) will receive these requests collectively when it is synchronized with the relay server. Execution normally starts in order of wipe, data deletion, and lock (*), and therefore if wipe is included in multiple remote operations, the smart device may be initialized before remote control operations other than wipe is executed. If smart device (agent) is reinstalled on this smart device, remote control that has not been executed may be executed after it becomes synchronized with the relay server.

*: The execution order may change depending on the status of the smart device.

Remote control on personal devices

Remote control can be executed even on personal devices in business uses when they are lost.



If remote control is executed correctly, a warning message will be displayed on the smart device (agent).

On a device on which multiple remote control operations are executed, multiple warning messages will be displayed.

The order displayed on the device may differ from the actual remote control execution order.

Follow the procedure below to control a smart device:

1. Start the **Management Console**.
2. From the CT List, right-click the smart device on which remote control will be executed, and click **Remote control**.

In Android, the **Show status**, **Lock** or **Unlock**, **Wipe**, and **Delete data** items will be displayed.

In iOS, the **Show status**, **Lock**, **Wipe**, and **Clear passcode** items will be displayed.

The following describes each menu item:

Menu name	Description
Show status	Displays the execution status of remote control. Refer to " 3.7.2 Checking Remote Control Status " for details.
Lock	Locks the smart device. In Android, operation will not be possible during lock even when the operator unlocks the device because the screen will be locked again immediately. In iOS, the screen will be in locked-state during lock. The screen can be unlocked by entering a password.
Unlock	Reverts the locked smart device to its previous state. This item is displayed instead of Lock after the device is successfully locked. This item is enabled for Android only.
Wipe	Restores the smart device to its factory settings. After executing this operation, it will not be possible to manage the smart device until the smart device (agent) is reinstalled.
Delete data	Deletes data stored on the smart device. This menu is enabled for Android only.

Menu name	Description
	<p>The target data is as follows:</p> <ul style="list-style-type: none"> - Phonebook: Android-standard phonebook data Includes favorite and often-used contact details - SD card: Data in SD cards - Call history: Incoming and outgoing data history - SMS message: Sent, received, drafted, and failed messages - Standard browser: Browsing history and bookmarks
Clear passcode	<p>Clears the passcode set for iOS. This item is enabled for iOS only.</p>

- The **Lock, Unlock, Wipe, Delete data, Clear passcode** items display a confirmation message. Click **Yes** to execute the operations. Once executed, the operations cannot be canceled.

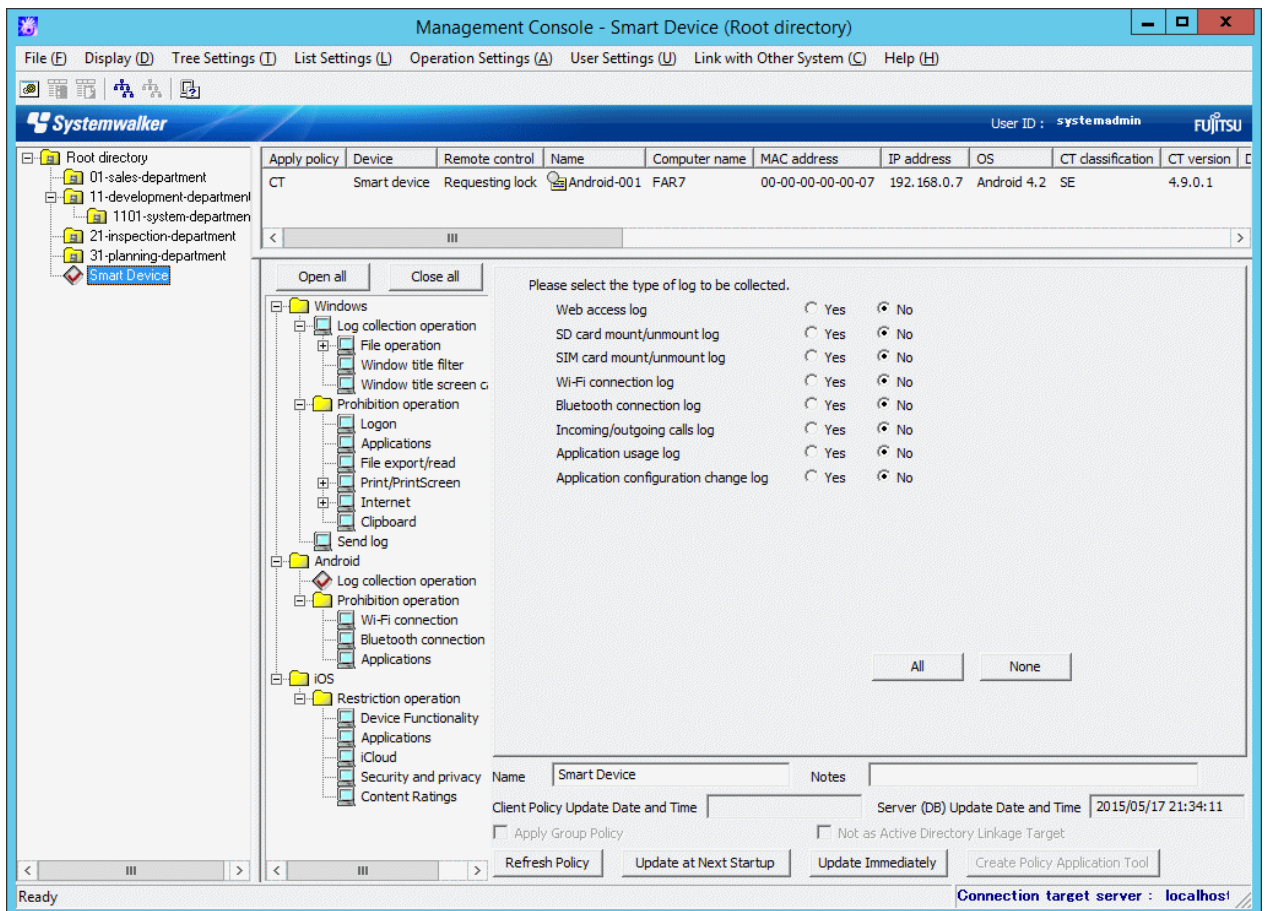
3.7.2 Checking Remote Control Status

The system administrator can check the execution status of remote control.

Checking the latest status

Follow the procedure below:

- Start the **Management Console**.
- From the CT List, select the smart device for which the execution status of remote control is to be checked.



The latest remote control status will be displayed in **Remote control** in the CT List.

The statuses below will be displayed depending on the remote control operation processed.

If multiple remote control operations are executed, the status of the remote control operation executed last will be displayed. Even if lock or wipe was executed after a failed unlock operation, the status of the last remote control operation will be displayed.

Remote control operation	Status
Lock/Unlock	<ul style="list-style-type: none"> - Requesting lock - Locking - Lock completed - Requesting unlock - Unlock completed
Delete data	<ul style="list-style-type: none"> - Requesting data deletion - Deleting data - Data deletion completed
Wipe	<ul style="list-style-type: none"> - Requesting wipe - Wiping - Wipe completed
Clear passcode	<ul style="list-style-type: none"> - Requesting passcode clear - Clearing passcode - Passcode clear completed
Not implemented	Blank

For any operation other than the one with a blank in **Remote control**, the execution status of remote control can be checked. Refer to "[Checking detailed status](#)" for details.

The timing with which the remote control status is reflected

The timing with which the following remote control status is reflected in **Remote control** is shown below:

- Requesting ...: When remote operations are set in the Management Console
- ...ing: When the smart device (agent) obtains policy (*1)
- ... completed: When the log for successful remote control on the smart device (agent) is received by the Smart Device Relay Server, and stored in the database (*1)

*1: The CT List in the Management Console needs to be refreshed. Refer to "[CT List](#)" for details.

Note

Even if the remote control operation is successful, the old status may remain if communication between the Management Server, Smart Device Relay Server, and smart device (agent) fails. If this happens, execute remote control again, or clear the displayed status (refer to "[Clearing the displayed status](#)" for details).

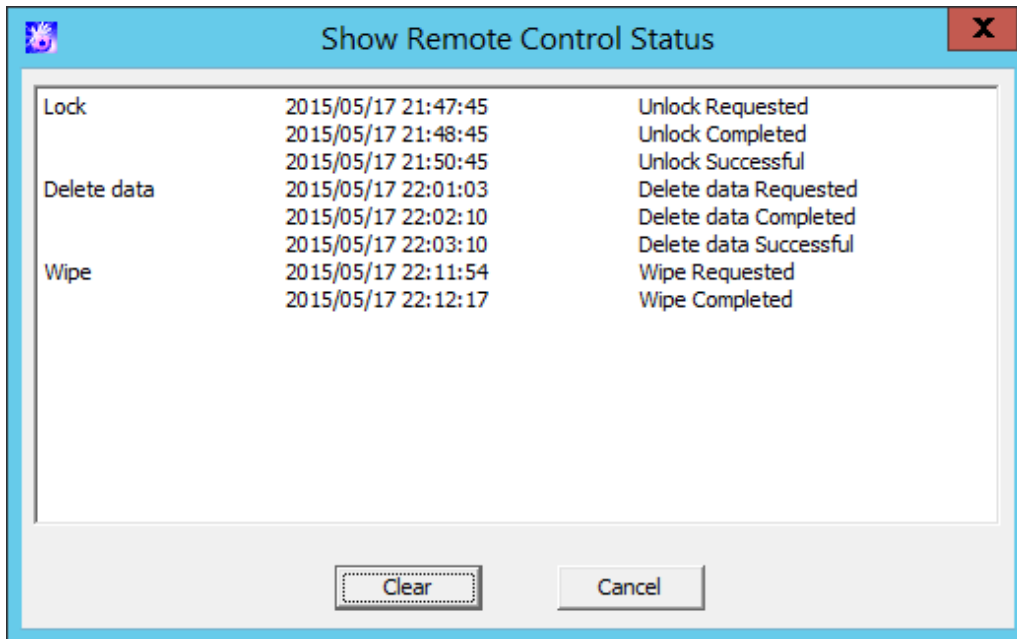
Checking detailed status

Follow the procedure below:

1. Start the **Management Console**.

- From the CT List, right-click the smart device on which remote control status will be checked, and click **Remote control > Show status**.

The **Show Remote Control Status** window will be displayed.



Clearing the displayed status

Once remote control is executed, the execution datetime will be displayed until the status is cleared.

If remote operation on the smart device has completed, click **Clear** to clear the status (the status in **Remote control** in the CT List will also be cleared).

The status cannot be cleared while a remote control operation is in progress. Clicking **Clear** while a remote control operation is in progress outputs the following message:

[MGFW-ERR011] Cannot clear the displayed status of remote control processing because it is in progress. Clear the displayed status after all remote control processing is completed.

Messages displayed in the Show Remote Control Status window

Depending on the remote control operation processed, various messages are displayed in the **Show Remote Control Status** window.

The messages displayed are shown below:

List of messages displayed:

Remote control operation	Message text
Lock/Unlock	YYYY/MM/DD hh:mm:ss Lock Requested
	YYYY/MM/DD hh:mm:ss Lock Completed
	YYYY/MM/DD hh:mm:ss Lock Successful
	YYYY/MM/DD hh:mm:ss Lock Failed
	YYYY/MM/DD hh:mm:ss Unlock Requested
	YYYY/MM/DD hh:mm:ss Unlock Completed
	YYYY/MM/DD hh:mm:ss Unlock Successful
	YYYY/MM/DD hh:mm:ss Unlock Failed
Wipe	YYYY/MM/DD hh:mm:ss Wipe Requested
	YYYY/MM/DD hh:mm:ss Wipe Completed

Remote control operation	Message text
Delete data	YYYY/MM/DD hh:mm:ss Delete data Requested
	YYYY/MM/DD hh:mm:ss Delete data Completed
	YYYY/MM/DD hh:mm:ss Delete data Successful
	YYYY/MM/DD hh:mm:ss Delete data Failed
Clear passcode	YYYY/MM/DD hh:mm:ss Clear passcode Requested
	YYYY/MM/DD hh:mm:ss Clear passcode Completed
	YYYY/MM/DD hh:mm:ss Clear passcode Successful
	YYYY/MM/DD hh:mm:ss Clear passcode Failed

Message text and meaning:

Message text	Meaning
Lock Requested	Displays the time the system administrator requested lock.
Lock Completed	Displays the time the smart device received the lock request.
Lock Successful	Displays the time the smart device executed lock (execution was successful).
Lock Failed	Displays the time the smart device failed to lock (execution failed, and retry will be performed).
Unlock Requested	Displays the time the system administrator requested unlock.
Unlock Completed	Displays the time the smart device received the unlock request.
Unlock Successful	Displays the time the smart device executed unlock (execution was successful).
Unlock Failed	Displays the time the smart device failed to unlock (execution failed, and retry will be performed).
Wipe Requested	Displays the time the system administrator requested wipe.
Wipe Completed	Displays the time the smart device received the wipe request. After wipe is executed, it will not be possible to manage the smart device, and therefore the execution result will not be displayed.
Delete data Requested	Displays the time the system administrator requested data deletion.
Delete data Completed	Displays the time the smart device received the data deletion request.
Delete data Successful	Displays the time the smart device executed data deletion (execution was successful).
Delete data Failed	Displays the time the smart device failed the data deletion (execution failed, and retry will be performed).
Clear passcode Requested	Displays the time the system administrator requested passcode clearing.
Clear passcode Completed	Displays the time the smart device received the passcode clearing request.
Clear passcode Successful	Displays the time the smart device executed passcode clearing (execution was successful).
Clear passcode Failed	Displays the time the smart device failed to clear the passcode (execution failed, and retry will be performed).

3.7.3 Controlling Smart Device when Password Entry Fails

Settings can be configured in advance so that lock and wipe can be executed even if the screen unlock password is incorrectly specified for the specified number of times.



Minimum length of Android passwords

The minimum length of Android passwords can be specified.

Failure to enter the password is detected when a password longer than the minimum length is entered and still failed.

The minimum length depends on device type, operating system, and installed applications.

Entering password when unlocking the screen

This setting does not force you to enter password for unlocking the screen.

Locking the smart device

Once the smart device is locked, lock will be repeatedly executed every time the password is entered incorrectly until it is successfully unlocked or wipe is executed.

Management for entering the Android password

If Android itself fails to unlock for a certain number of times, a message will be output. If this happens, you will not be able to enter password for a certain period of time.

The timing with which Android outputs the message and the period of time during which entering of the password will be prohibited depend on device type.

Checking the smart device behavior in advance

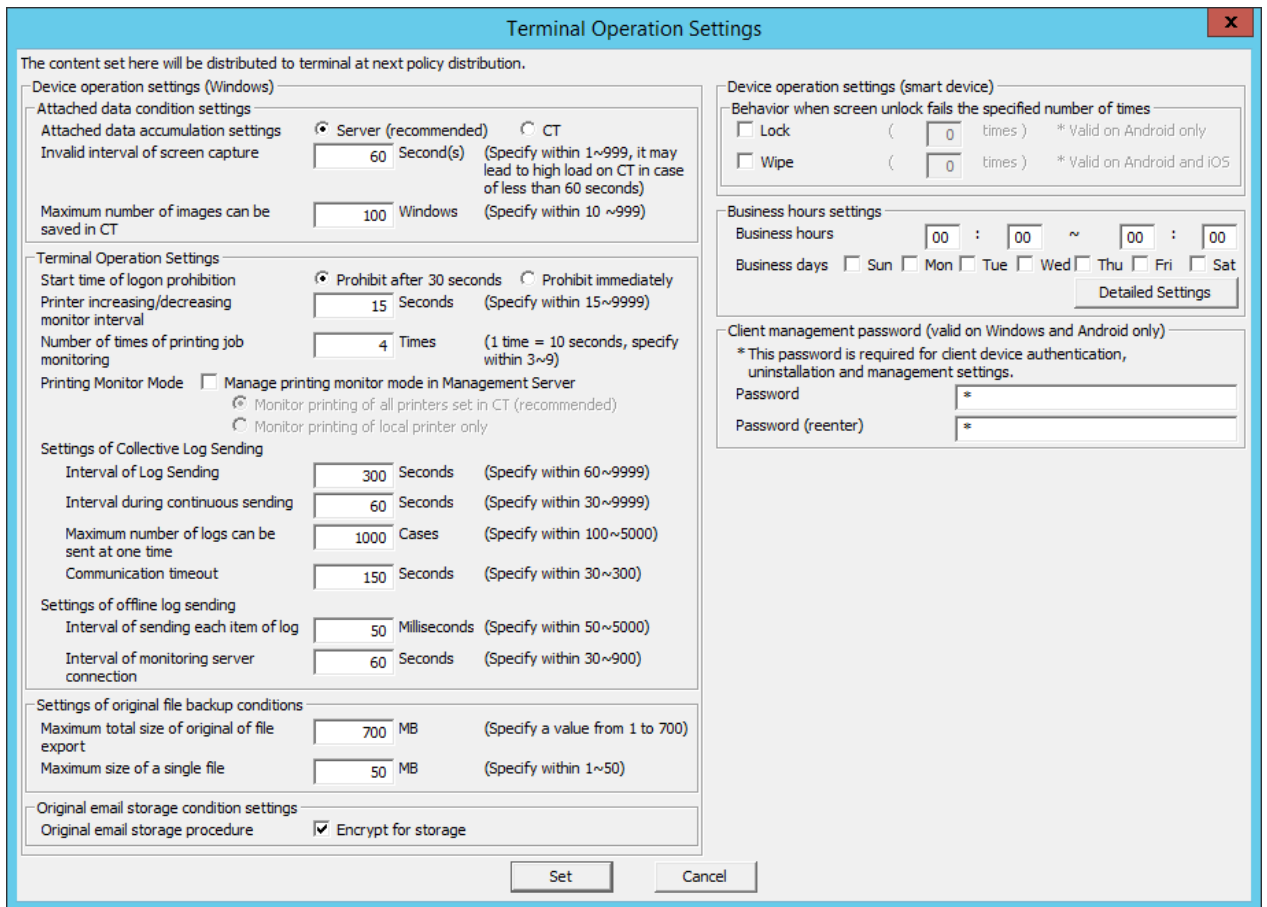
Some smart devices cannot detect unlock failures, and as a result lock and wipe operations may fail. Check the smart device behavior in advance.

Follow the procedure below:

1. Start the **Management Console**.

2. Click **Operation Settings > Terminal Operation Settings**.

The **Terminal Operation Settings** window will be displayed.



3. Enter the following information, and click **Set**.

Device operation settings (smart device) > Behavior when screen unlock fails the specified number of times

Configure whether to execute lock and wipe when screen unlock on the smart device fails the specified number of times consecutively.

Item name	Description
Lock	Select this to lock the smart device when screen unlock on the smart device fails the specified number of times consecutively. A number between 4 and 10 can be specified for the number of times. The lock feature is enabled for Android only. By default, this item is not selected.
Wipe	Select this to execute wipe on the smart device when screen unlock on the smart device fails the specified number of times consecutively. A number between 4 and 10 can be specified for the number of times. Note that, if Lock is selected, a value greater than the number of times specified for Lock must be specified for this item. The wipe feature is enabled for Android and iOS. By default, this item is not selected.

For example, if both **Lock** and **Wipe** are selected, and 5 and 7 are set for the number of times, respectively:

- Lock will be executed if screen unlock on the smart device fails 5 consecutive times.
- If the unlock request fails, lock will be executed again.

- If the above operations are repeated, wipe will be executed when screen unlock fails for the seventh time.

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 or smart devices will be displayed.

- PCs that exported files
- PCs used out of working time
- PCs that performed suspicious access
- PCs not connected for a long period
- Smart devices not connected for a long period
- PCs that blocked the use of prohibited USB device
- PCs that blocked the use of prohibited account group
- Devices (*1) that blocked the use of prohibited application
- PCs that blocked prohibited printing
- PCs that blocked the sending of email with prohibited attachment

*1: Includes both PCs and smart devices.

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 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.

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

Refer to "4.2.3 Aggregate by Objectives" for details.



Note

Notes relating to the start of Web Console

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.

Notes when Windows(R) Internet Explorer(R) 10 or later is used

The upper part of the displayed characters will be missing when Windows(R) Internet Explorer(R) 10 or later is used for display.

4.1 Check the Trend in Status Window



Note

Do not modify configuration information while browsing the Status Window

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: Connect to the Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on 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: Connect to the Management (Master Management) Server. To display the result of aggregation in every Management Server, connect to each Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on 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

Refer to "1.2.45 IPv6 Support" for details on the IPv6 specification.

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, 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

- **Aggregation Target 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.



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, view the information after the next aggregation.

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. View it after the aggregation has finished.

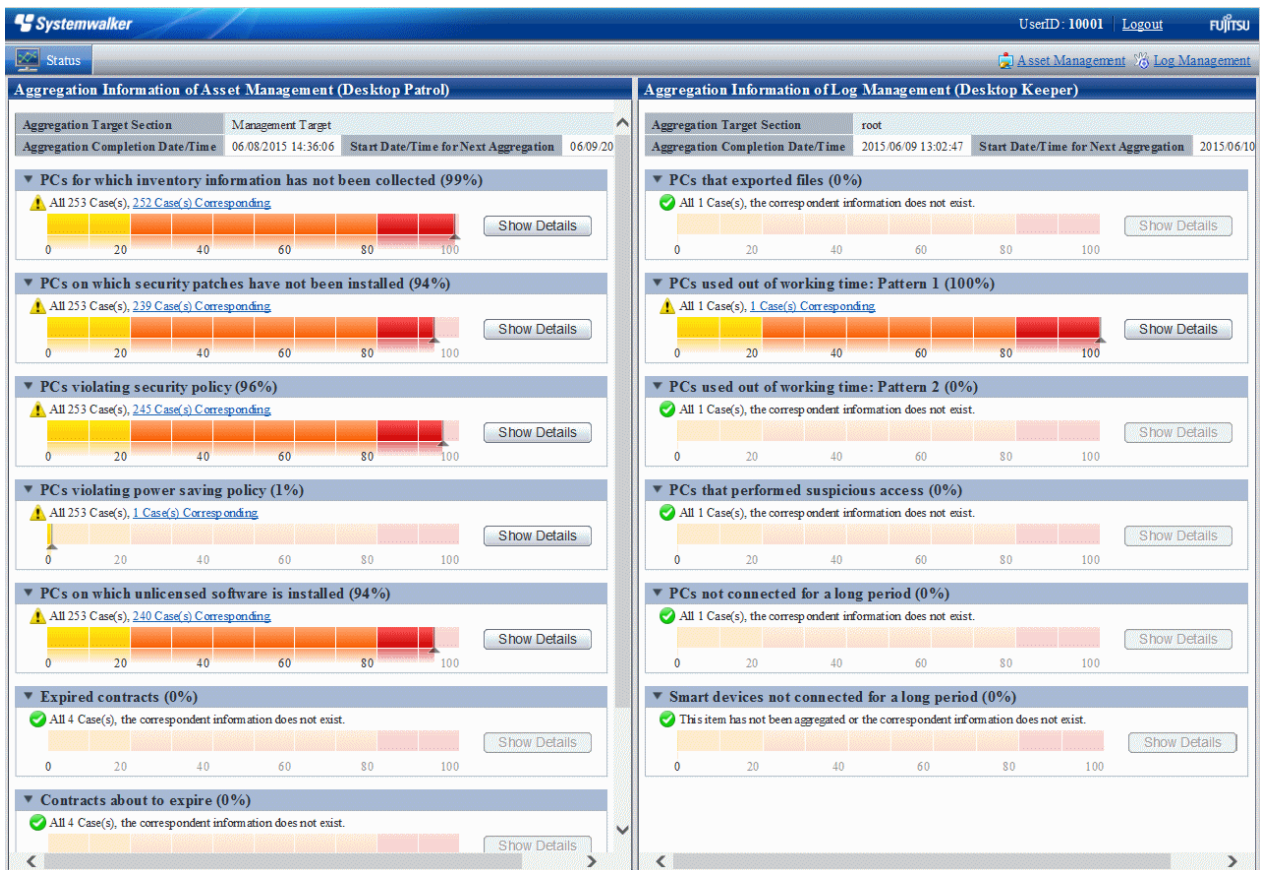
Confirm the event log of Management (Master Management) Server

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, 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. 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:

- PCs that 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.

- PCs 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.

- PCs that 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.

- PCs not connected for a long period

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.

- Smart devices not connected for a long period

Number of smart devices that have not been connected for a long period or in which the client feature might have been uninstalled. The period in which the device has not been connected is added as a condition of aggregation for policy distribution status of Systemwalker Desktop Keeper.

- PCs that blocked the use of prohibited USB device

The number of PCs on which the use of prohibited USB memory (*1) has been blocked is displayed.

For the log of violation (*2) to the category of device configuration change log, aggregation is performed after the condition of aggregation period has been added.

*1: Includes removable devices, CD/DVD, portable devices, and USB devices recognized as imaging devices.

*2: 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.

- PCs that 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.

- Devices that blocked the use of prohibited application

The number of devices (PCs and smart devices) on which the startup of prohibited application has been blocked is displayed.

For application startup prohibition log (*1) and application usage prohibition log (*2), aggregation is performed after the condition of aggregation period has been added.

*1: The startup of an application that is specified in the "Application Startup Prohibition" policy will be recorded as a violation.

*2: The attempt to use applications specified in the application usage prohibition policy will be recorded as a violation.

- PCs that 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.

- PCs that blocked the sending of email 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.

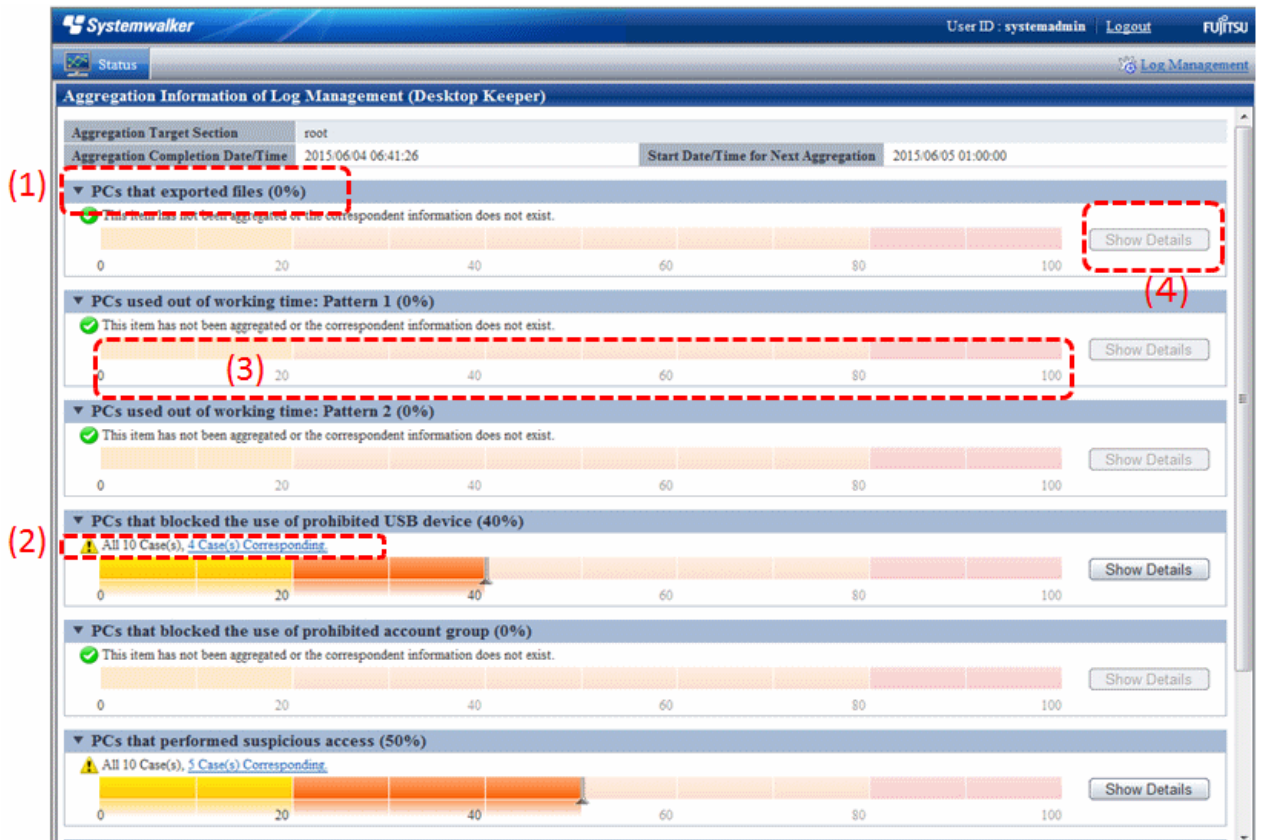
* Sending of an E-mail with the prohibited attachment specified in the "E-mail Sending" policy will be recorded as a violation.

The system administrator can set whether to show/hide each item.

For details on setting these items, 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. 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.

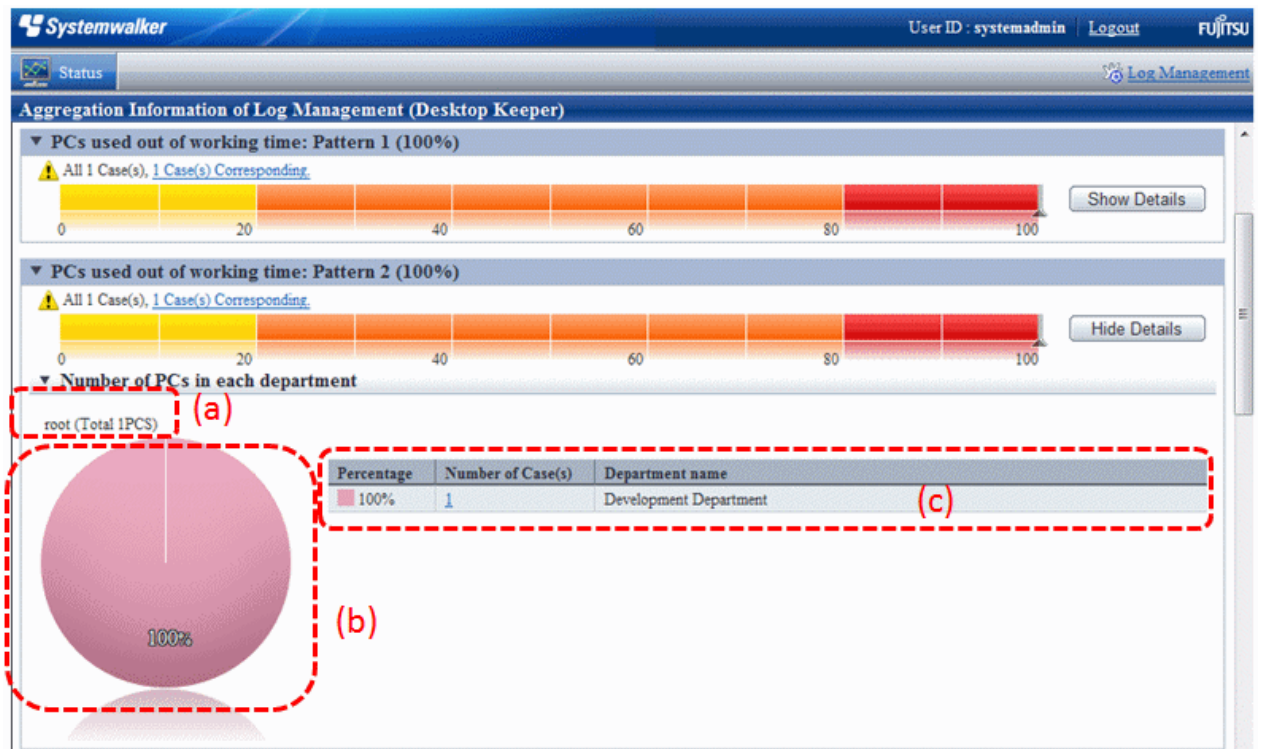
⚠: This is displayed when the correspondent number is more than 1.

(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. 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.

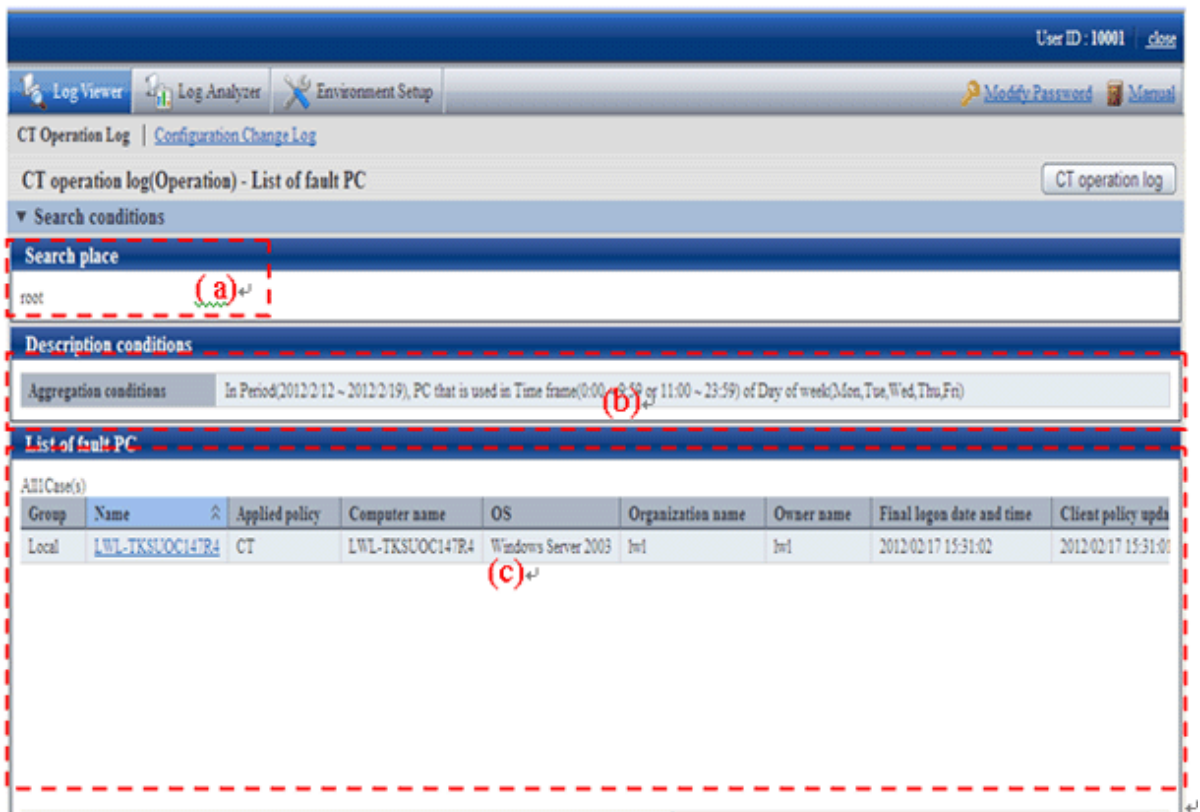
After clicking the department name, the target department, pie chart and ranking table will be changed to the information under the selected department.

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, 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, refer to "[5.2.1 View Logs in the 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 directory" group instead of the "Not Configured" group.

About the smart device (agent) operation log

The smart device (agent) operation log is not aggregated.

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(R) Internet Explorer(R) 6.0 (ServicePack1)
 - Windows(R) Internet Explorer(R) 7
 - Windows(R) Internet Explorer(R) 8
 - Windows(R) Internet Explorer(R) 9
 - Windows(R) Internet Explorer(R) 10
 - Windows(R) Internet Explorer(R) 11

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: Connect to the Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on 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: Connect to the Master Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu** or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on 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

Refer to "[1.2.45 IPv6 Support](#)" for details on the IPv6 specification.

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.

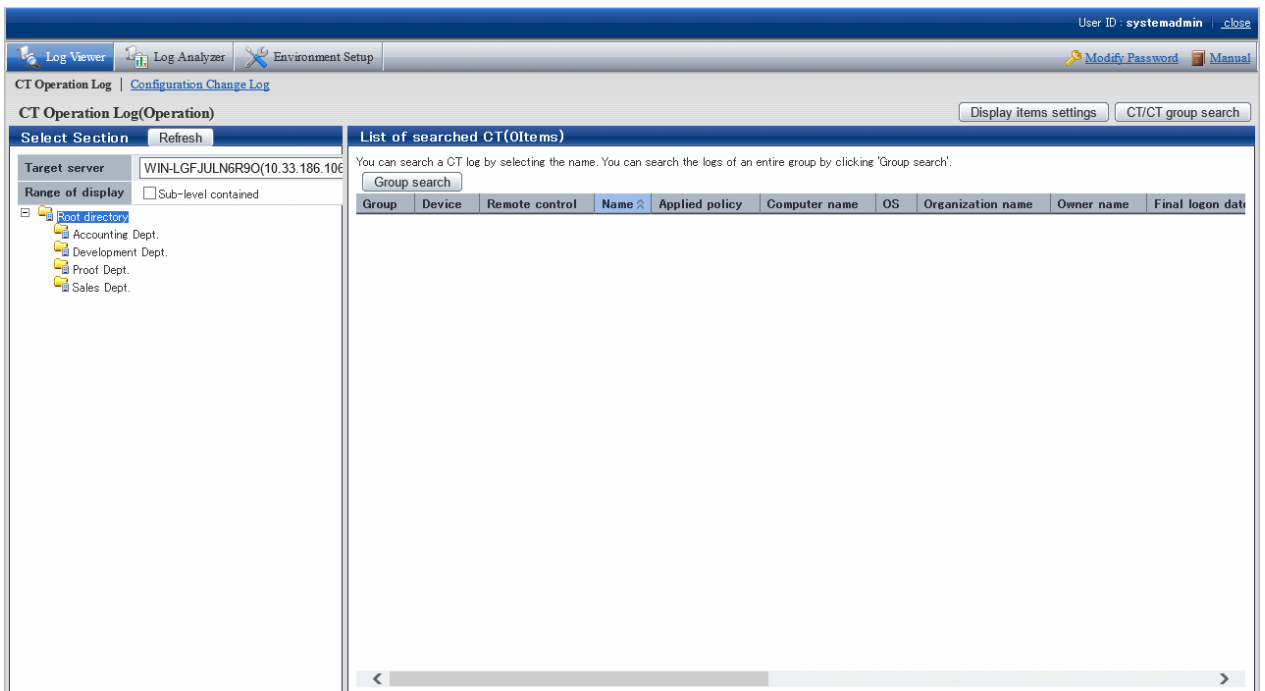
When Systemwalker Desktop Patrol is linking with a single sign on, the input of the User ID is case-sensitive.

- **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, refer to "[Change password](#)".

The Status Window is displayed.

3. Click **Log Management** of Global Navigation.

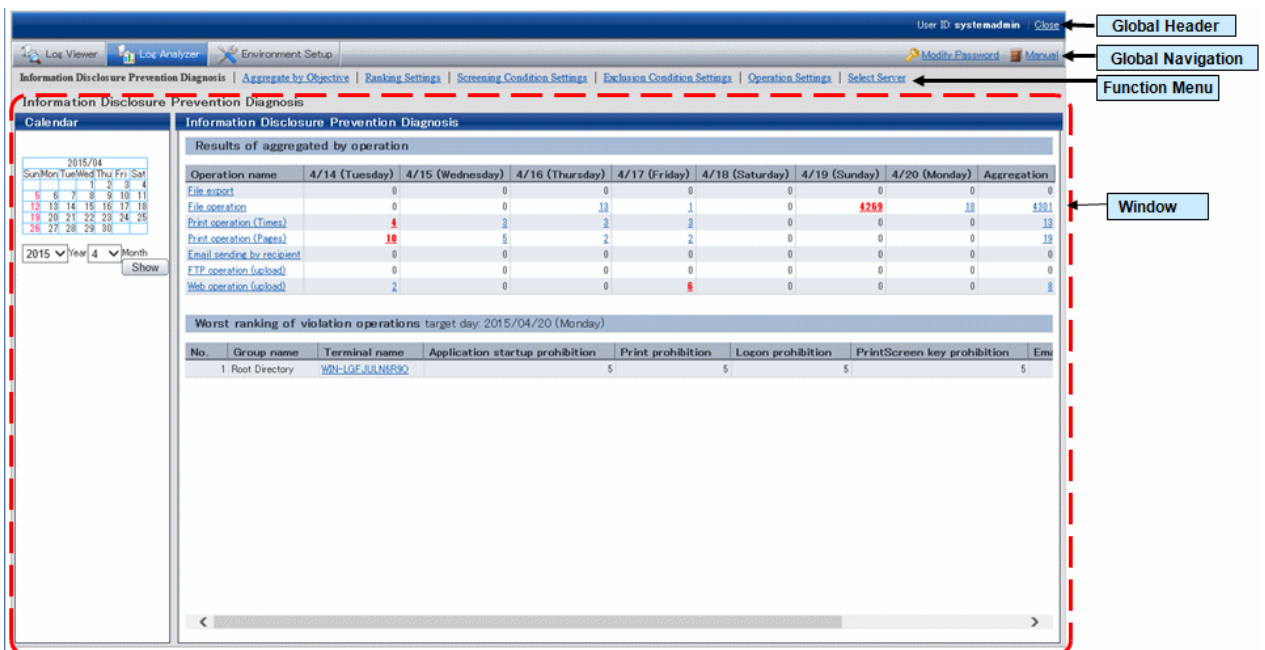
Log Viewer is started and the **CT Operation Log** window is displayed.



4. Click **Log Analyzer** of Global Navigation.

The **Information Disclosure Prevention Diagnosis** window is displayed.

In addition, in a system with multiple Log Analyzer servers, 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, 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, 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 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 servers 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

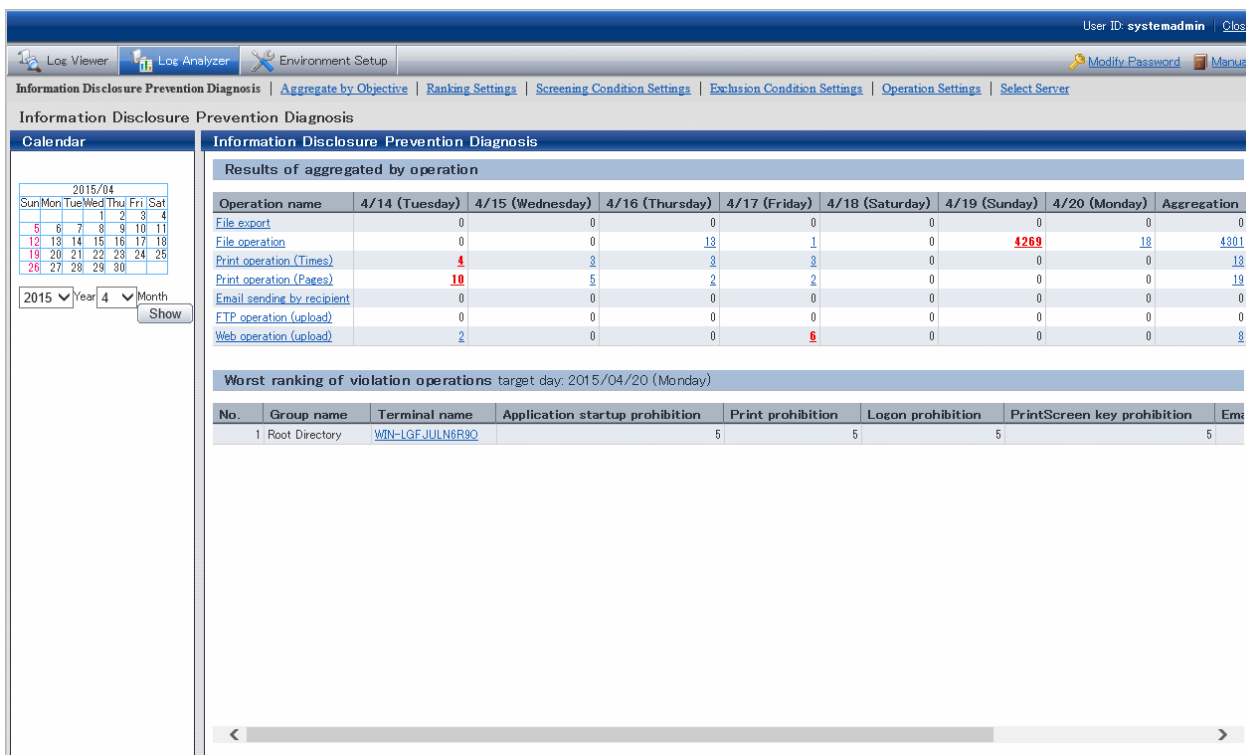
When a connection to the Log Analyzer server cannot be made due to the stop of the server and interruption of the network, depending on the environment and number of servers, it may take several minutes before the window is displayed.

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), E-mail sending operation, FTP operation (upload), Web operation (upload) as well as the total number of operations within recent 7 days.
- **Worst ranking of Violation operations:** 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.



The screenshot displays the 'Information Disclosure Prevention Diagnosis' window. On the left is a calendar for April 2015. The main area shows a table titled 'Results of aggregated by operation' with columns for dates from 4/14 to 4/20 and an 'Aggregation' column. The table lists operations such as 'File export', 'File operation', 'Print operation (Times)', 'Print operation (Pages)', 'Email sending by recipient', 'FTP operation (upload)', and 'Web operation (upload)'. Below this table, it shows the 'Worst ranking of violation operations' for the target day 2015/04/20 (Monday), with a table listing violations like 'Root Directory'.



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, 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.
- FTP operation log (upload)
The number of file uploads to the FTP server is aggregated.
- Web operation log (upload)
The number of file uploads to the web site is aggregated.

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. Make sure to apply this setting.

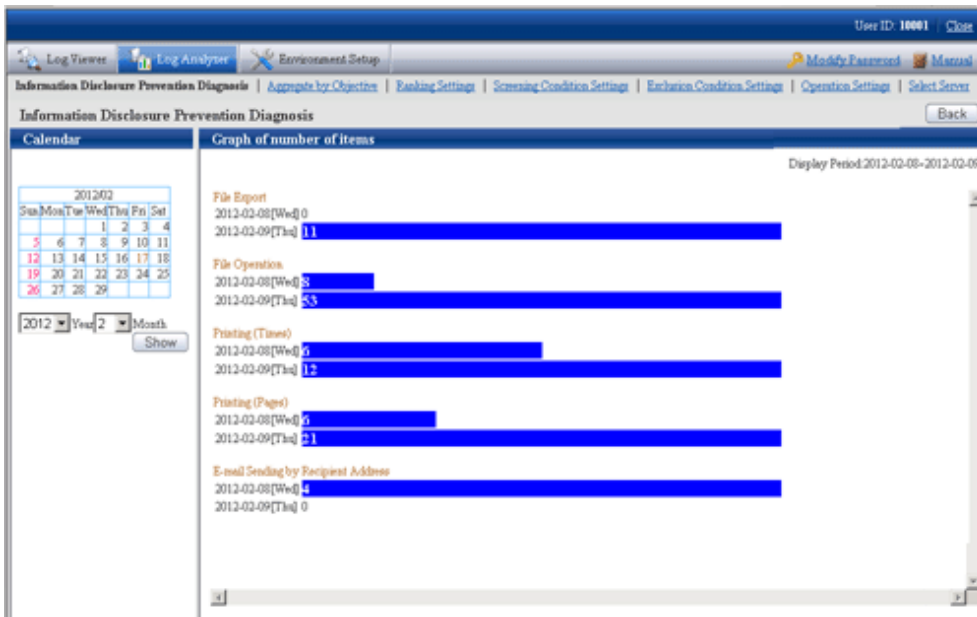
Display the Number in Graph

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).

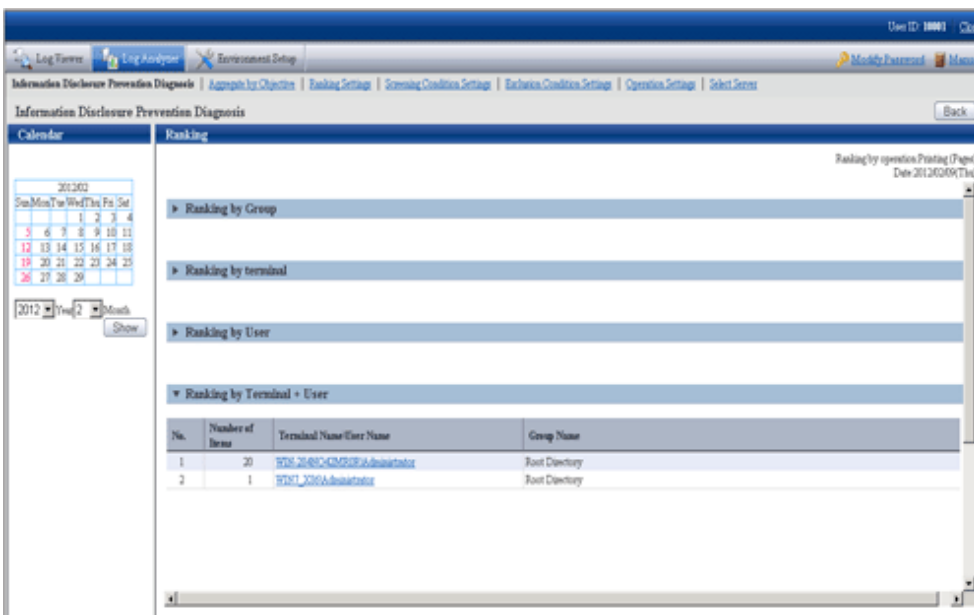
The procedure is as follows:

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 up to 1024 halfwidth characters (512 fullwidth characters).

In the CT group tree of Management Console, the **Group Name** of client (CT) exists under the root directly is displayed as "Root directory".

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)".

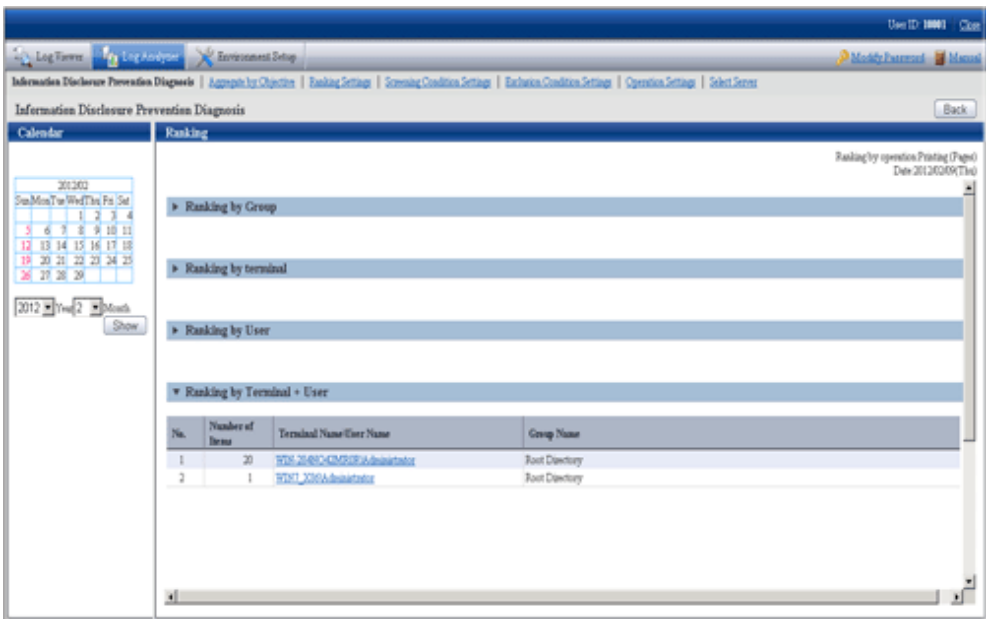
[Example] BLONO (Fujitsu Taro)

In ranking by terminal + user name, it will be displayed in form of "Computer Name (Name) + user name".

[Example] BLONO (Fujitsu Taro) + Administrator

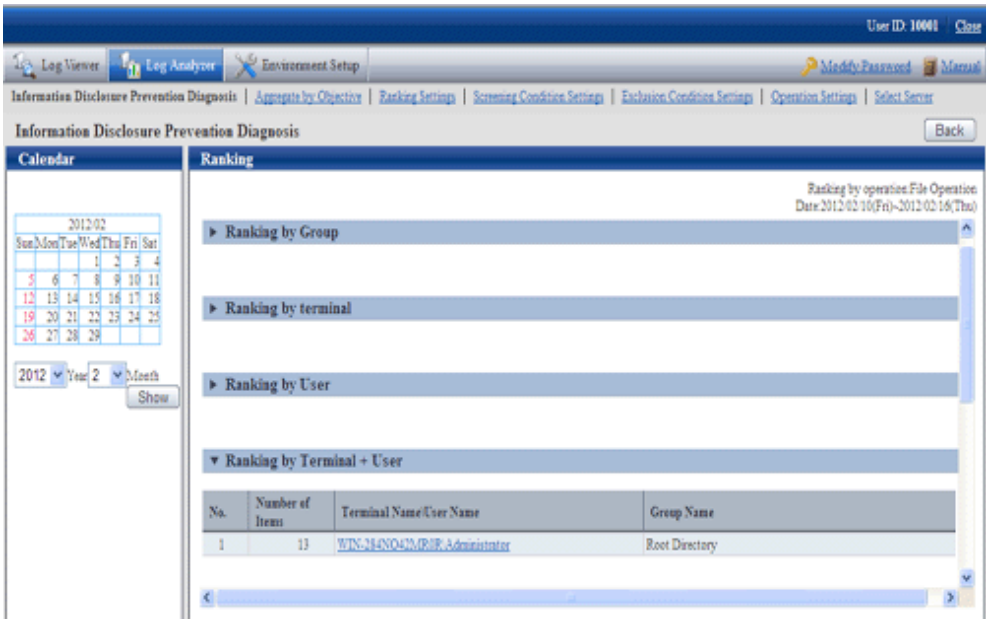
When clicking the number on the date column

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" check box 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 directory**, **Local** and **Deleted CT** in ranking by group cannot be switched to the Log Viewer window as well.

4.2.2.2 Display the Ranking of Violations

In the 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, 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 April 2015. The main area displays a table titled 'Results of aggregated by operation' with columns for dates from 4/14 to 4/20 and an 'Aggregation' column. The table lists various operations and their counts for each day. Below this is a section for 'Worst ranking of violation operations' with a table listing the top violations.

Operation name	4/14 (Tuesday)	4/15 (Wednesday)	4/16 (Thursday)	4/17 (Friday)	4/18 (Saturday)	4/19 (Sunday)	4/20 (Monday)	Aggregation
File export	0	0	0	0	0	0	0	0
File operation	0	0	0	13	0	0	18	4301
Print operation (Times)	4	3	3	3	0	0	0	13
Print operation (Pages)	10	5	2	2	0	0	0	19
Email sending by recipient	0	0	0	0	0	0	0	0
FTP operation (upload)	0	0	0	0	0	0	0	0
Web operation (upload)	2	0	0	6	0	0	0	8

No.	Group name	Terminal name	Application startup prohibition	Print prohibition	Logon prohibition	PrintScreen key prohibition	Em...
1	Root Directory	WIN-LGF-JULN6R9Q	5	5	5	5	

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(R) Internet Explorer(R) 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 the Management Server without using a proxy according to the following procedure.

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.

During the Count by Purpose operation, "Audit Success" and "Audit Failure" may be recorded in the event log (security)

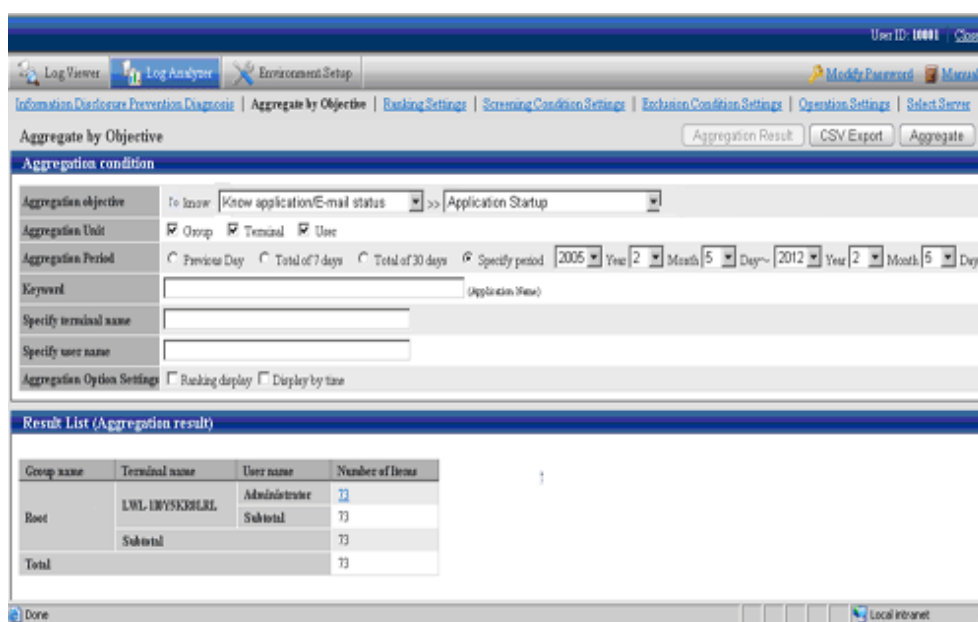
The "Audit Success" and "Audit Failure" statuses may be output as below to the event log (security) on the Log Analyzer Server during the Count by Purpose operation, but there is no impact to the operation.

- Audit Success
 - Event ID: 4648
 - Event ID: 4634
 - Event ID: 4624
 - Event ID: 4672
 - Audit Failure
 - Event ID: 4776
-

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.

2. In **Aggregation objective**, select an aggregation objective and its sub-menu.

Aggregation Objective	Sub-menu of Aggregation Objective	Content
To know Violation operation status	Application Startup Prohibition	Aggregate the number corresponding to application startup prohibition.
	Printing Prohibition	Aggregate the number corresponding to printing prohibition.
	Logon Prohibition	Aggregate the number corresponding to logon prohibition.
	PrintScreen key Prohibition	Aggregate the number corresponding to PrintScreen key prohibition.
	E-mail Attachment Prohibition	Aggregate the number corresponding to E-mail attachment prohibition.
To know File export status	File Export	Aggregate the number of file export.
	File Export (by drive)	Aggregate the number of file export by the type of target drive as export destination.
To know File operation status	File Operation	Aggregate the number of file operation.
	File Operation (Remote)	Aggregate the number of file operation on network.
	File Operation (Removable)	Aggregate the number of file operation on removable media.

Aggregation Objective	Sub-menu of Aggregation Objective	Content
To know Application/ E-mail status	Application Startup	Aggregate the number of application startup.
	E-Mail Sending by Recipient Address	Aggregate the number of E-mail sending,
To know Printing operation status	Printing Operation (times)	Aggregate the number of printing.
	Printing Operation (Number of Pages)	Aggregate the total number of printed pages.
To know Web access status	Window Title with URL Obtaining	Aggregate the number of internet access.
	Window Title with URL (by site) Obtaining	Aggregate the number of Internet access by site.
To know Information disclosure status	File Export	Filter logs according to filtering condition/exclusion condition and aggregate the number of file export for external media.
	File Operation	Filter logs according to filtering condition/exclusion condition and aggregate the number of file operation for external media.
	Printing Operation (Times)	Filter logs according to filtering condition/exclusion condition and aggregate the number of printing.
	Printing Operation (Number of Pages)	Filter logs according to filtering condition/exclusion condition and aggregate the total number of printed pages.
	E-mail Sending by Recipient Address	Filter logs according to filtering condition/exclusion condition and aggregate the number of E-mail sending.
	FTP operation (upload)	Filter logs according to filtering condition/exclusion condition and aggregate the number of FTP uploads.
	Web operation (upload)	Filter logs according to filtering condition/exclusion condition and aggregate the number of Web uploads.

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"> - Group: Aggregate in the unit of the CT group - Terminal: Aggregate in the unit of computer name (*). *) It is displayed in the CT list of the Management Console. - User: Aggregate in the unit of user name. <p>When multiple units are selected, the relationship between units is in sequence of Group > Terminal > 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																											

Item Name	Description																																																																																																																																																										
Aggregation Period	<p>Specify the collection date for logs to be aggregated.</p> <ul style="list-style-type: none"> - Previous Day: Aggregate the logs 1 day before the execution of aggregation by objectives. - Total of 7 days: Aggregate the logs in the last week (7 days till the last day). - Total of 30 days: Aggregate the logs in last 30 days (30 days till the last day). - Specify period: Aggregate the logs in any time period. Set the start date and end date. The period can be specified is from Jan. 1, 2004 to Dec. 31, 2024. <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. Aggregate by weeks and set appropriate value in aggregation period.</p>																																																																																																																																																										
Keyword	<p>Specify the keyword for search during aggregation.</p> <p>Specify up to 50 characters (no distinction between halfwidth and fullwidth). Aggregate the logs that partially match with the specified keyword. Valid keyword varies with aggregation objectives. Refer to "Appendix A List of Aggregation Objectives" for details.</p>																																																																																																																																																										
Specify terminal name	<p>Aggregate the logs that contain the specified computer name (partially match). Specify up to 60 characters (no distinction between halfwidth and fullwidth).</p>																																																																																																																																																										
Specify user name	<p>Aggregate the logs that contain the specified user name (partially match). Specify up to 40 characters (no distinction between halfwidth and fullwidth).</p>																																																																																																																																																										
Aggregation Option Settings	<p>Specify the display format of the aggregation result.</p> <ul style="list-style-type: none"> - 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. <table border="1" data-bbox="518 1301 821 1543"> <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-XYWIN-AF</td> <td>6</td> <td>5</td> </tr> <tr> <td>WIN-24NO42</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"> - 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. <table border="1" data-bbox="518 1724 1121 1910"> <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>Energy area</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>Area</td> <td>15</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>Control Group</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> <td>15</td> </tr> <tr> <td>Control Group</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>Control Group</td> <td>1</td> <td>12</td> <td>2</td> <td>2</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>Control</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>Ad Group</td> <td>1</td> <td>7</td> <td>2</td> <td>2</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>Control</td> <td>1</td> <td>2</td> <td>22</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>Control</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> </tr> <tr> <td>Control</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>Control</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>Control</td> <td>1</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> <td>2</td> </tr> </tbody> </table> <p>The above image shows correspondent data exists at 3pm, 4pm, 5pm, 6pm, 8pm 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-XYWIN-AF	6	5	WIN-24NO42	4	6	LWL-TKSUO	2	7	Time	#1	#2	#3	#4	#5	#6	#7	#8	#9	Energy area	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	Area	15	2	2	2	2	2	2	2	2	Control Group	2	2	2	2	15	15	15	15	15	Control Group	2	2	2	2	2	2	2	2	2	Control Group	1	12	2	2	1	1	1	1	1	Control	1	2	2	2	2	2	2	2	2	Ad Group	1	7	2	2	1	1	1	1	1	Control	1	2	22	2	2	2	2	2	2	Control	1	2	2	2	1	1	1	1	1	Control	1	2	2	2	2	2	2	2	2	Control	1	2	2	2	2	2	2	2	2	Control	1	2	2	2	2	2	2	2	2
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-XYWIN-AF	6	5																																																																																																																																																									
WIN-24NO42	4	6																																																																																																																																																									
LWL-TKSUO	2	7																																																																																																																																																									
Time	#1	#2	#3	#4	#5	#6	#7	#8	#9																																																																																																																																																		
Energy area	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																																																																																																																																																		
Area	15	2	2	2	2	2	2	2	2																																																																																																																																																		
Control Group	2	2	2	2	15	15	15	15	15																																																																																																																																																		
Control Group	2	2	2	2	2	2	2	2	2																																																																																																																																																		
Control Group	1	12	2	2	1	1	1	1	1																																																																																																																																																		
Control	1	2	2	2	2	2	2	2	2																																																																																																																																																		
Ad Group	1	7	2	2	1	1	1	1	1																																																																																																																																																		
Control	1	2	22	2	2	2	2	2	2																																																																																																																																																		
Control	1	2	2	2	1	1	1	1	1																																																																																																																																																		
Control	1	2	2	2	2	2	2	2	2																																																																																																																																																		
Control	1	2	2	2	2	2	2	2	2																																																																																																																																																		
Control	1	2	2	2	2	2	2	2	2																																																																																																																																																		

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:

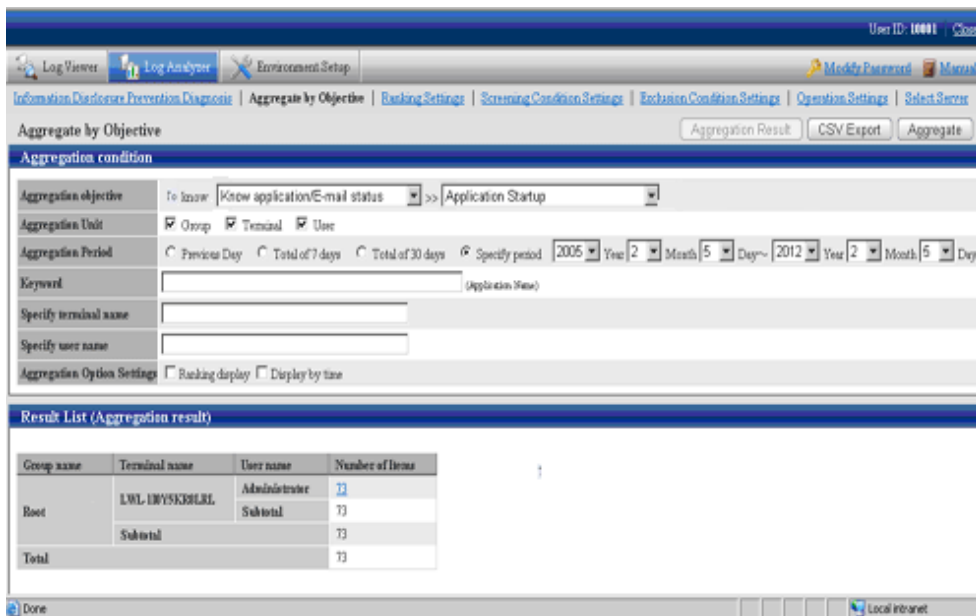
Aggregation function may be in use by another user. Do you want to continue?

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, 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 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, 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

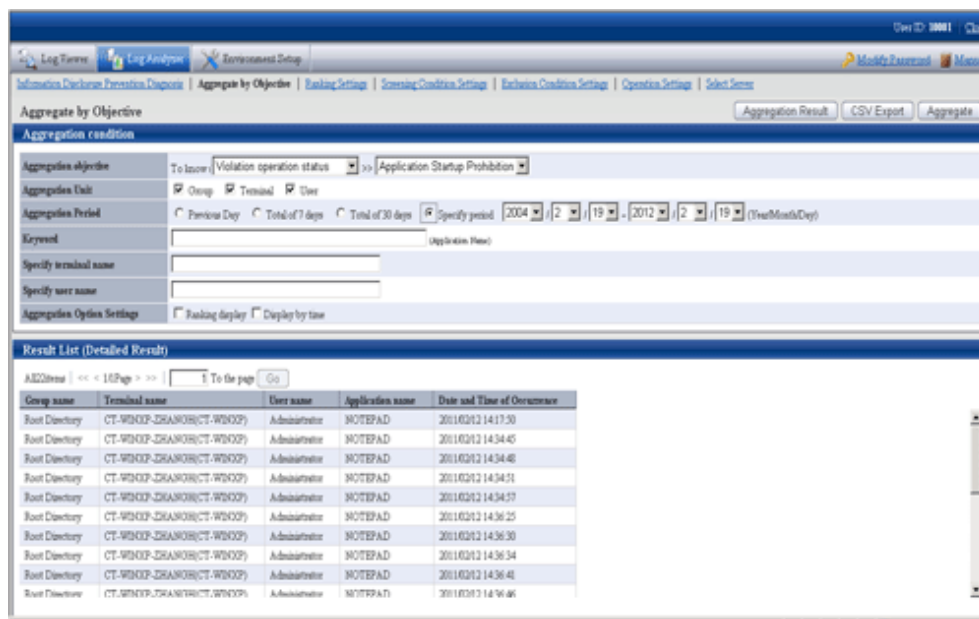
Detailed Result

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, refine the aggregation unit and reduce the aggregation period before detailed displayed.

In the process of aggregation or cancellation of aggregation, 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. Refer to "[Appendix A List of Aggregation Objectives](#)" for details.

To return to the aggregation result, 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(R) Office Excel data.

The character encoding for the CSV file must match the setting on the import source Management Server of the Log Analyzer Server being referenced (encoding setting for the I/O files of the Server Settings Tool). However, if the encoding setting is changed on the Management Server, the change will not be reflected to the CSV file until the import to the Log Analyzer Server is complete.

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(R) 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 client (CT) and smart device (agent) users will be saved on the server as various logs. The system administrator or department administrator confirms operation content of CT and smart device (agent) 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) and smart device (agent) 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 smart device (agent) users 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

Do not start multiple web consoles on one PC.

Notes on displaying the web console on Windows(R) Internet Explorer(R) 10 or later

When you display the web console on Windows(R) Internet Explorer(R) 10 or later, the top of the characters will be missing.

Start Log Viewer

1. Start the web console through any of the following methods:

In a 2-level structure: Connect to the Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu**, or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on 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: Connect to the Master Management Server.

- Select **Start > Systemwalker Desktop Keeper > Server > Desktop Keeper Main Menu**, or **Apps > Systemwalker Desktop Keeper > Desktop Keeper Main Menu** on 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

Refer to "[1.2.45 IPv6 Support](#)" for details on the IPv6 specification.

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.

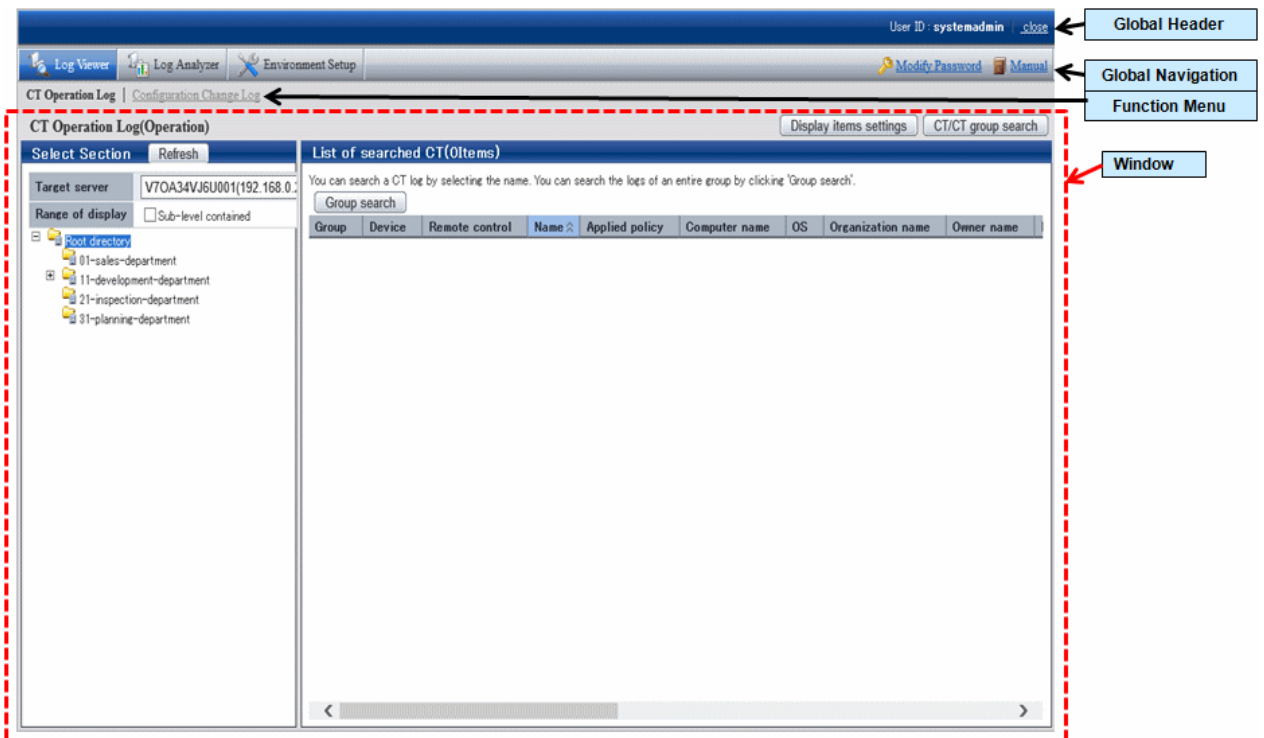
- **User ID:** set in the **Administrator Information Settings** window of the Server Settings Tool.
- **Password:** set in the **Administrator information settings** window of the Server Settings Tool
It is recommended to change the password regularly. For details on how to do so, refer to "[Change 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. (Refer to "[Change password](#)" for how to change password)
- Manual: Display the manual.

Function Menu







- CT Operation Log: Search and display CT Operation Logs.
- User operation log: Searches and displays user 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. 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), smart device (agent), and CT group under Management Server is not known.
- **Select Section:** "Local" of 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 check box is selected, the selected CT group and all its subordinate CTs will be displayed in **List of searched CT**
If the check box 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) or smart device (agent) that generates violation logs will be displayed in **List of searched CT**. When the client (CT) or smart device (agent) 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) or smart device (agent) that generates violation logs.
When this item is not selected, clients (CTs) and smart devices (agents) 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.

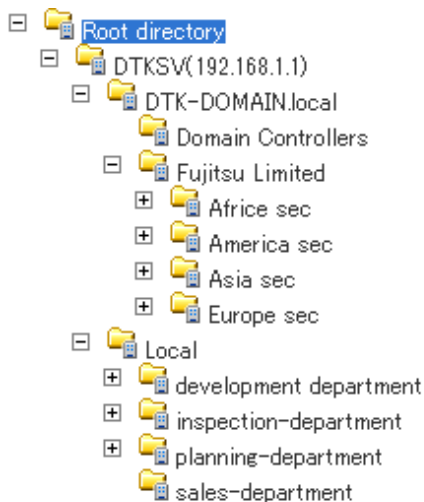
User logs on to Log Viewer	Displayed icon	Meaning of icon
System administrator		All groups will be displayed with identical icons when the system administrator logs on to the Log Viewer. This indicates the group in which " Display the group or client (CT) and smart device (agent) that have generated violation logs in red " is not set; or no violation log has been generated though settings have been performed.
		This indicates the group in which " Display the group or client (CT) and smart device (agent) that have generated violation logs in red " 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.

User logs on to Log Viewer	Displayed icon	Meaning of icon
		This indicates the group in which "Display the group or client (CT) and smart device (agent) that have generated violation logs in red" 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 clients (CTs) and smart devices (agents) that belong to the selected group are displayed. The item to be displayed can be selected. For the method, 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 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	
	Client (CT)	Smart device (agent)
Name (*1)	The name that can be added to client (CT), initial value is the computer name.	This is a name that can be given to a smart device (agent). The initial value is a telephone number, or a model name if the telephone number cannot be obtained.
	When modifying, refer to " Modify CT Policy ". Name cannot be set to an item not displayed.	
Group (*1)	This is the group to which the client (CT) and smart device (agent) belong.	
Device	A client (CT) is displayed as PC .	A smart device is displayed as Smart device .
Remote control	Blank	An overview of the remote control status is displayed. - Implement: Remote control is implemented. Refer to " 3.7.2 Checking Remote Control Status " for details. Blank: Remote control is not implemented.
Applied policy (*1)	This is the policy that is applied. CT: CT policy is applied. Group: CT group policy is applied.	
Computer name (*1)	This is the computer name of client (CT).	This is the model name of the smart device (agent).
MAC address	This is the MAC address of client (CT).	This is the MAC address of the smart device (agent).
IP address (*2)	This is the IP address of client (CT)	This is the IP address of the smart device (agent).
OS (*1)	This is the OS name of client (CT).	This is the OS name of the smart device (agent).
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)	This is displayed as SE .
CT version	This is the version of the client (CT) and smart device (agent) of Systemwalker Desktop Keeper that is installed. In addition, for correspondence of product version/edition, refer to "CT version" of <i>Systemwalker Desktop Keeper Reference Manual</i> .	
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.	Blank
Organization name (*1)	This is the organization name set in the OS of client (CT).	Blank
Owner name (*1)	This is the owner name set in the OS of client (CT).	Blank

Item Name	Description	
	Client (CT)	Smart device (agent)
Subnet mask	This is the subnet mask of the client (CT) and smart device (agent).	
Active Directory Linkage	<p>This shows whether the client imports information by Active Directory Linkage.</p> <ul style="list-style-type: none"> - 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 	Blank
Network participation conditions	<p>This is network participation situation of the client (CT).</p> <ul style="list-style-type: none"> - Domain: The client (CT) belongs to domain. - Group: The client (CT) does not belong to domain. 	Blank
Domain name	<p>This is the name of domain to which the client belongs. The group name will be displayed when Network Participation is Group.</p>	This is the model name of the smart device (agent).
Final logon date and time (*1)	<p>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,</p> <ul style="list-style-type: none"> - Send CT policy. - Send user policy. <p>The date and time are displayed or updated in the following case:</p> <ul style="list-style-type: none"> - When a policy is synchronized between the Master Management Server or Management Server and the client (once per day between 0:30 and 1:30) 	<p>This is the final date and time when the Master Management Server or Management Server sent a CT policy to a smart device (agent).</p> <p>The date and time are displayed or updated in the following cases:</p> <ul style="list-style-type: none"> - When Sync now is selected on the smart device (agent) - When automatic synchronization between the Master Management Server or Management Server and the smart device (agent) (12:00 to 13:00) is performed.
Client policy update date and time (*1)	<p>This is the final date and time when the Master Management Server or Management Server sends CT policy to the client (CT). It is displayed or updated in the following cases:</p> <ul style="list-style-type: none"> - 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; - When CT policy is reflected on the client (CT) after the Update Immediately button on the Management Console is clicked. 	

Item Name	Description	
	Client (CT)	Smart device (agent)
	- When a policy is synchronized between the Master Management Server or Management Server and the client (once per day between 0:30 and 1:30)	
Server (DB) update date and time (*1)	This is the latest date and time when the Management Server or Master Management Server updates the policy of the client (CT) and smart device (agent) and reflects it to the database (including immediate update).	
Note	This is the information input when updating the policy of the client (CT) and smart device (agent). When it needs to be modified, refer to " Modify CT Policy ".	
DTP version	This is the version of Systemwalker Desktop Patrol Client installed in PC.	Blank
Trace status	This is the setting of trace collection in client (CT). <ul style="list-style-type: none"> - Summary: Collect the trace of the client (CT) at summary level. - Details: Collect the trace of the client (CT) at detail level. - Blank: Do not collect the trace of the client (CT), or the client (CT) is V12.0. 	Blank
Occurrence date and time of violation log (*1)	This is the date and time when violation logs are collected on the client (CT) and smart device (agent).	
Management Server	The computer name of the management server to which the client and smart device (agent) belong.	
Virtual PC	The following icons will be displayed if the client (CT) is installed in a virtual environment: <ul style="list-style-type: none"> - -(Main): Master image of virtual PC - -: Virtual PC 	Blank

*1: Items displayed as initial value.

*2: If you disable the dual stack, the disabled IP address may continue to be displayed for a while.

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) and smart device (agent), 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 **Display items settings** window is displayed.

2. Scroll the window and 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) and smart device (agent) that belong 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) and smart device (agent) that have 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 you select the CT group that is displayed in red, the rows of the client (CT) and smart device (agent) where violation logs occurred will be displayed in red in **List of searched CT**.

After you click the **Select CT** button, the column of the client (CT) and smart device (agent) where violation logs 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 **Display items settings** window is displayed.

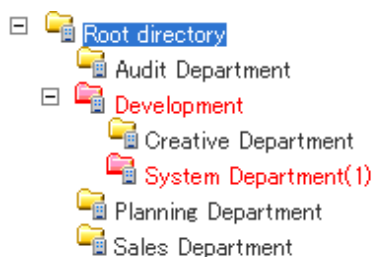
2. Scroll the window and display **Violation CT display settings**.

The item descriptions for **Violation CT display settings** are as follows:

Item Name	Description
Display violation CT	<p>Set the group to which the client (CT) and smart device (agent) that have generated violation logs belong 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"> - Display Display the group to which the client (CT) and smart device (agent) that have generated violation logs belong and the number of clients (CTs) and smart devices (agents) that have generated violation logs in red. - Not display Do not display the clients (CTs) that have generated a violation log in red even if they exist. <p>Initial value: Not display is select.</p>
Violation range of display	<p>Set whether to display the situation in which the client (CT) and smart device (agent) that have generated violation logs exist in a certain range of time prior to the startup date of Log Viewer in red.</p> <p>Setting can be performed when Display is selected from the Display violation CT window.</p> <ul style="list-style-type: none"> - This day

Item Name	Description
	<ul style="list-style-type: none"> - If violation logs generate on the date of starting Log Viewer, display the client (CT), smart device (agent), and CT group in red. - Within yesterday Display the client (CT), smart device (agent), 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, 2013, the client (CT), smart device (agent), and CT group that have generated violation logs on Feb. 9, 2013 and Feb. 10, 2013 will be displayed in red. - Within one week Display the client (CT), smart device (agent), 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), smart device (agent), and CT group that have generated violation logs from last Monday to the day of startup in red. - Within this month Display the client (CT), smart device (agent), 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, 2013, display the client (CT), smart device (agent), and CT group that have generated violation logs from Feb 1 to 10, 2013 in red. - Within the specified date Display the client (CT), smart device (agent), and CT group that have generated violation logs from the specified day to the date of starting Log Viewer in red.
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), smart device (agent), and CT group that have generated violation logs from the specified day to the date of starting Log Viewer in red.</p>

3. Set each item and click the **Set** button.



Change the database to be viewed

Select the database to view operation logs.

1. Click the **Display items settings** button in the **CT Operation Log** window.

The **Display items settings** window is displayed.

2. Scroll the window and display **Viewing database settings**.

The item descriptions for **Viewing database settings** are as follows:

Item Name	Description
Viewing database settings	Set the database to be viewed by Log Viewer

Item Name	Description
	<ul style="list-style-type: none"> - Operation database The operation database is viewed by Log Viewer. - Log viewing database The log viewing database is viewed by Log Viewer. <p>Initial value: Select Operation database.</p>

3. Select the database to be viewed and click the **Set** button.



Note

Log Viewing Database

If you have not created the log viewing database and have not restored log data, you cannot set **Log viewing database**.

Administrators and department administrators for whom **Log Viewer > view backup log** is selected in **Detailed Authority** in the **Administrator Information Settings** window of the Server Settings Tool can browse the Log Viewing Database.

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 **Display items settings** window is displayed.

2. Scroll the window and display **Log search settings**.

The item descriptions for **Log search settings** are as follows:

Item Name	Description
Log search of connection source terminal and connection target terminal	<p>Set the search range of operation log.</p> <ul style="list-style-type: none"> - Logs of the specified terminal are searched only Search operation logs of specified terminals only. - Logs of connection source terminal and connection target terminal of the specified terminal are also searched Search operation logs including connection source terminal and connection target terminal of specified terminal. <p>Initial value: Logs of the specified terminal are searched only is selected</p>

3. Select the operation log search range and click the **Set** button.

Change the IP address display settings

In an IPv4/IPv6 dual-stack environment, set whether to prioritize IPv4 addresses or IPv6 addresses as the IP addresses to be displayed in the Log Viewer.

1. Click **Display items settings** in the **CT Operating Log** window.

The **Display items settings** window is displayed.

2. Scroll the window and display **IP address display settings for CT**.

The item descriptions for **IP address display settings for CT** are as follows:

Item Name	Description
IP address	Set which IP addresses are to be given priority.

Item Name	Description
	<ul style="list-style-type: none"> - Prioritize IPv4 addresses In an IPv4/IPv6 dual-stack environment, IPv4 addresses are displayed. In an IPv6 address-only environment, IPv6 addresses are displayed. - Prioritize IPv6 addresses In an IPv4/IPv6 dual-stack environment, IPv6 addresses are displayed. In an IPv4 address-only environment, IPv4 addresses are displayed. <p>Initial value: Prioritize IPv4 addresses is selected.</p>

3. Select the IP address type to be prioritized and click **Set**.

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**.

Types of log that 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, 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, refer to "5.2.1 View Logs in the CT Operation Log Window", "5.2.3 View Logs in the Configuration Change Log Window".

View logs in the [CT Operation Log] window

Types of log that can be viewed	Log description	
	Client (CT)	Smart device (agent)
Application Startup Log	This is the log when starting an application in the client (CT). When linking with Citrix XenApp, the application startup operation performed in Citrix XenApp client will be recorded.	-
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.	-
Application Startup Prohibition Log	This is the log when starting a prohibited application in client (CT). It is displayed in red in Log Switches .	-
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.	This is the log collected when the following operations are performed on a smart device (agent): <ul style="list-style-type: none"> - An application is used. - A prohibited application is used (*1). - The web is accessed. *1: Displayed in red in List of logs
E-mail Sending Log	This is the log when E-mails have been sent in the client.	-
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 .	This is the log collected when the following operations are performed on a smart device (agent): <ul style="list-style-type: none"> - Wi-Fi connection is made to an access point. - Wi-Fi connection is made to a prohibited access point (*2). - A pairing with a Bluetooth device is established. - A pairing with a Bluetooth device for which pairing is prohibited is established (*2). - An SD card is mounted/unmounted. - A SIM card is mounted/unmounted.

Types of log that can be viewed	Log description	
	Client (CT)	Smart device (agent)
		*2: Displayed in red in List of logs
Printing Operation Log	<p>This is the log when Printing operation has been performed in the client (CT).</p> <p>When linking with Citrix XenApp, the printing performed in the Citrix XenApp Client will be recorded.</p> <p>A printing log will be recorded in both the Citrix XenApp Server and Citrix XenApp Client when printing is performed via a virtual printer.</p>	-
Printing Prohibition Log	<p>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)</p>	-
Logon Prohibition Log	<p>This is the log when logging on with a prohibited group in the client (CT). It is displayed in red in List of logs.</p>	-
File Export Log	<p>This is the log when exporting files with the File Export Utility in client (CT).</p>	-
PrintScreen Key Operation Log	<p>This is the log when operating the PrintScreen key in the client (CT).</p> <p>When linking with Citrix XenApp, PrintScreen operations performed in the Citrix XenApp Client will be recorded.</p>	-
PrintScreen Key Prohibition Log	<p>This is the log when the prohibited PrintScreen key is used in the client (CT). It is displayed in red in List of logs.</p>	-
Web Operation Log	<p>This is the log when the following operation is performed in client (CT):</p> <ul style="list-style-type: none"> - Upload to Web sites. - Download from Web sites. <p>When linking with Citrix XenApp, Web operations performed in the Citrix XenApp Client will be recorded.</p>	-
Web Operation Prohibition Log	<p>This is the log when the following operation is performed in the client (CT). It is displayed in red in List of logs.</p> <ul style="list-style-type: none"> - Access to prohibited URL. - Upload to the prohibited URL. - Download from the prohibited URL. 	-
FTP Operation Log	<p>This is the log when the following operation is performed in client (CT):</p> <ul style="list-style-type: none"> - Upload files to FTP server - Download files from FTP server 	-

Types of log that can be viewed	Log description	
	Client (CT)	Smart device (agent)
	When linking with Citrix XenApp, FTP operations performed in the Citrix XenApp Client will be recorded.	
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 .	-
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.	-
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 .	-
File Operation Log	This is the log when a file operation is performed in the client (CT).	-
Logon/Logoff	This is the log when the following operations are performed in the client (CT): <ul style="list-style-type: none"> - Logon - Logoff - PC startup - PC shut-down - PC sleep - PC recovery - PC connection - PC disconnection 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.	-
Linkage Application Log	This is the log of applications linked with the client (CT). For information about linking another application to the client (CT), refer to "Link with Other Products" in <i>Systemwalker Desktop Keeper Operation User's Guide</i> .	-
Incoming/outgoing calls log	-	This is the log of telephone numbers of incoming and outgoing calls used by a

Types of log that can be viewed	Log description	
	Client (CT)	Smart device (agent)
		standard Android telephone on a smart device (agent).
Application configuration change log	-	This log is collected when an application is installed or uninstalled on a smart device (agent).

Point

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.). Policy setting is not required for the purpose of log collection.

The following 4 types of logs can be viewed in the **Configuration Change Log** window of the Log Viewer:

- **Terminal Settings:** Record of modified client (CT) and smart device (agent) policy.
- **Level composition settings:** Record of modification of CT group tree such as moving a CT and smart device (agent) 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, execute the DTKSTCV.EXE (export configuration change log) command, and view the logs after exporting them as CSV files. 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 the 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. To change the database whose operation logs will be browsed, select the desired database.
Refer to "[Change the database to be viewed](#)" for details.
3. Set the following items in **Select Section**
 - Select the Management Server that manages the client (CT) and smart device (agent) from **Target server**.

- In **Range of display > Sub-level contained**, select whether to display only the clients (CTs) and smart devices (agents) directly under the selected group, or all clients (CTs) and smart devices (agents).
 - In **Range settings > The violation CT is displayed only**, select whether to display only the clients (CTs) and smart devices (agents) for which violation logs are generated, or all clients (CTs).
4. From the CT group tree of **Select Section**, select the CT group to which the client (CT) and smart device (agent) for viewing logs belong.

Logs on the client (CT) and smart device (agent) 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) and smart devices (agents) 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) and smart devices (agents) belonging to local groups during Active Directory Linkage.
- When selecting CT group: Logs can be searched and viewed on all clients (CTs) and smart devices (agents) 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) and smart devices (agents) belonging to the CT group will be displayed in **List of searched CT**.

The screenshot shows the Log Viewer application interface. On the left, the 'Select Section' pane shows a tree view of the organization structure, including 'Root directory', 'Audit Department', 'Development', 'Creative Department', 'System Department', 'Planning Department', and 'Sales Department'. The 'System Department' is selected. The 'Range of display' section has 'Sub-level contained' checked. The 'Range settings' section has 'The violation CT is displayed only' checked. The main pane displays a table titled 'List of searched CT(3Items)'. The table has columns: Group, Device, Remote control, Name, Applied policy, Computer name, OS, Organization name, and Owner. Three rows are listed, all with red text indicating violation logs: 'System Department PC WINDOWS-AM8TT36 CT WINDOWS-AM8TT36 Windows 8.1 FWEST Windows', 'System Department PC WINDOWS-ELG1IAS CT WINDOWS-ELG1IAS Windows 8.1 FWEST Windows', and 'System Department PC WINDOWS-JCN1R76 CT WINDOWS-JCN1R76 Windows Server 2012 (x64) FWEST Windows'. An 'Activate Windows' watermark is visible at the bottom right of the application window.

The client (CT), smart device (agent), and CT groups with violation logs will be displayed in red. Refer to "[Display the group or client \(CT\) and smart device \(agent\) that have generated violation logs in red](#)" for details.



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, 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.

5. Perform any of the following operations according to the purpose of viewing CT Operation Logs:

- View logs by client (CT) and smart device (agent)
Click **Name** of client (CT) and smart device (agent) for viewing logs in **List of searched CT**.
- View client (CT) and smart device (agent) logs within the selected range in CT group tree
Click the **Group search** button in **List of searched CT**.

The **CT Operation Log(Operation) - Log search** window is displayed.

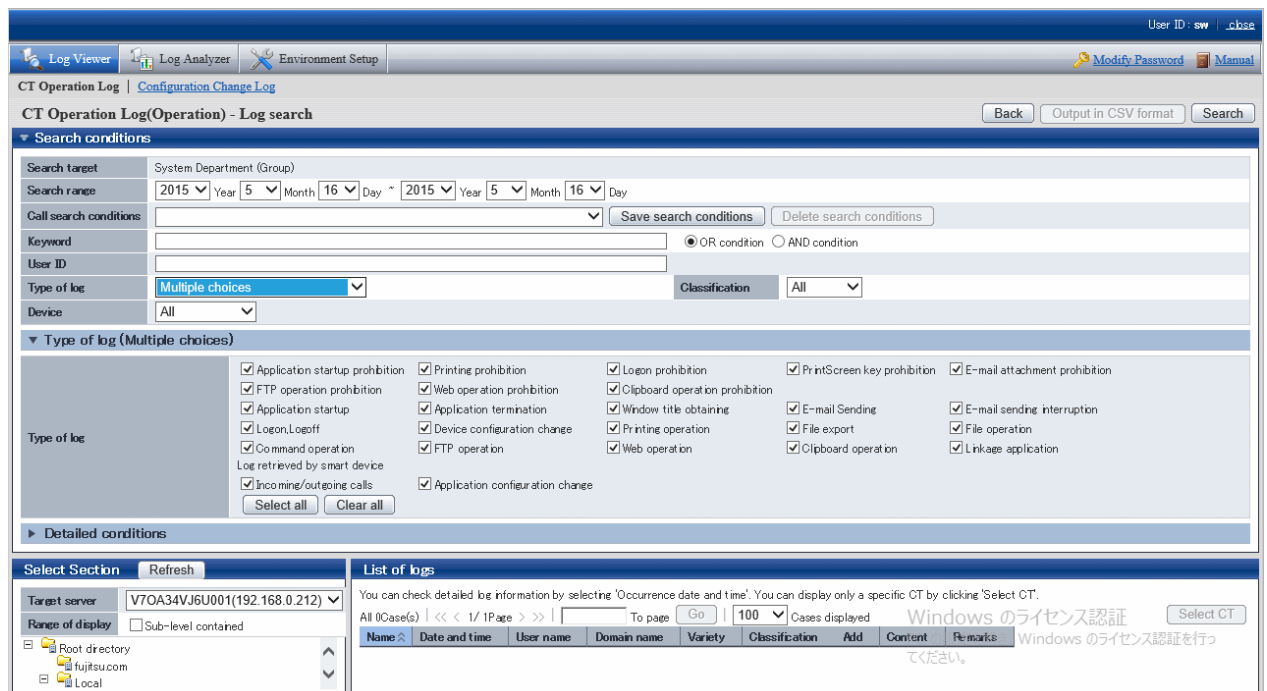
Search conditions, **Type of log (Multiple choices)** and **Detailed conditions** can be opened or closed.

After clicking **Search conditions**, **Type of log (Multiple choices)** and **Detailed conditions** (rightward triangle symbol), the **Search conditions** window will be opened.

After clicking ▼**Search conditions**, ▼**Type of log (Multiple choices)** and ▼**Detailed conditions**, the **Search conditions** window will be closed.

 **Note**

In case of Microsoft(R) Internet Explorer(R) 6.0, if the scroll bar cannot be displayed for conforming log list when unfolding "Detailed conditions", check if "Log Type (Multiple choices)" and "Detailed conditions" are in folded status.



6. Set **Search conditions**

Click **Detailed conditions** to set detailed conditions such as drive type and log collection time, etc.

Item Name	Description
Search target	<p>The name of the client (CT) or smart device (agent) in which the search logs are collected or the CT group name will be displayed.</p> <p>The name or group name will be followed by "(CT)" or "(Group)".</p>
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"> - Start date <ul style="list-style-type: none"> _ Sep 2013: 1 Sep. 2013 is assumed to be specified. __ 2013: 1 Jan. 2013 is assumed to be specified. _(Day)_(Month)_(Year): Start searching from the earliest saved log. 15_ 2013: Specification error 15 Sep. __: Specification error <p>If no end month or day is specified, search till the end of the specified year (Dec 31).</p> <p>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"> - End date <ul style="list-style-type: none"> _ Sep 2013: 30 Sep. 2013 is assumed to be specified. __ 2013: 31 Dec 2013 is assumed to be specified. _(Day)_(Month)_(Year): Search till the last saved log. _ 15, 2013: Specification error 15 Sep _ : Specification error <p>If the specified year is omitted, the specified month and day should be omitted.</p> <p>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:</p> <p>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"> - Saving method <p>Set the search conditions to be saved; the conditions out of Search range can be saved.</p> <p>After the setting has completed, click the Save search conditions button. The window for saving the search conditions is displayed.</p> <p>To save again, select Save as and click the Register button. Each administrator can save up to 10 conditions. If 10 search conditions have already been saved, to save another, delete the oldest and register the new search condition.</p> <p>Up to 128 halfwidth and fullwidth characters can be entered as the search condition name.</p> <p>If desired to update search conditions, select Update and click the Register button.</p> - Deletion method <p>To delete a search condition, select a search condition name, and click the Delete search conditions button.</p>
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>

Item Name	Description
	<p>Enter up to 128 halfwidth and fullwidth characters.</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</p> <p>The contents set as keyword varies with different log types. Refer to the content column and notes column of "Display Content" of "8.2.1 Application Startup Log" and "8.2.22 Configuration Change Log" for details.</p>
User ID	Search according to user name. Only one user name can be entered.
Type of log	Search by log type. When two or more log types are set as the search condition, select Multiple Selection . The Type of log (Multiple Selection) right under it will be opened, select the corresponding log type.
Classification	<p>The operations 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.</p> <p>When selecting the The violation CT is displayed only check box of Range settings and clicking the Group Search button: Violation is displayed.</p>
Device	<p>Search by device type.</p> <p>To search only client (CT) logs, select PC. To search only smart device (agent) logs, select Smart device. Selecting All sets PC and Smart device, and all device logs will be searched.</p>

Type of log (Multiple choices)

Item Name	Descriptions
Type of log	<p>Select the type of log to be displayed in List of logs. Refer to "Types of log that can be viewed" for information about log types.</p> <p>Select All : Select all log types. Clear All : Cancel the selection of all log types Initial State: All are selected.</p>

Detailed Conditions

Item Name	Descriptions
Type of drive	<p>Search according to the type of drive.</p> <p>Drive type becomes a valid condition when setting the following items in Type of log.</p> <ul style="list-style-type: none"> - All - File Operation - File Export <p>The following four types can be specified and multiple specifications at the same time are allowed:</p> <ul style="list-style-type: none"> - Removable: The following media identified as a drive letter: <ul style="list-style-type: none"> - Floppy disk - External hard disk (removable hard disk connection via USB, IEEE 1394 or PCMCIA, etc.) - MO

Item Name	Descriptions
	<ul style="list-style-type: none"> - USB memory - Compact flash memory - Remote: Network drive - CD/DVD: CD/DVD drive - Fixed: PC fixed drive. <p>Relationship between settings of Type of log and Type of drive and searched log:</p> <ul style="list-style-type: none"> - 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"> - A) When creating a new file, file creation target - B) When updating, location of updated file - C) When viewing, location of viewed file - D) When deleting, location of deleted file - E) When renaming, location of the file before renaming - F) When renaming, location of the file after renaming - G) When copying, location of the copy source file - H) When copying, file copy destination - I) When moving, location of the move source file - J) When moving, file moving destination - 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
Time	<ul style="list-style-type: none"> - Not specified: Time is not included in search condition. - Specify range: The range of time for log collection is specified as search condition. <ul style="list-style-type: none"> - If "a:00~b:59" is input, search with the condition of time range from a:00:00 to b:59:59. - If "a:00~-:59" is input, search with the condition of time range from a:00:00 to 23:59:59. - If "-:00~b:59" is input, search with the condition of time range from 0:00:00 to b:59:59. <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"> - 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. - Select all: Select all check boxes in Specify time. - Clear all: Cancel all selected check boxes in Specify time. <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>

Item Name	Descriptions
	<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>

7. Click the **Search** button.



Note

If you specify a large number of CTs or a long search period in the search conditions, the following message may be displayed:

```
[LWSV-SEL003] A search may not be possible due to the large amount of data targeted for search.
Continue processing?
```

If the conditions do not need to be reviewed, continue with processing.

If the search takes a long time, a timeout may occur. Alternatively, if there is a large number of search results, the search may be canceled and one of the following messages may be displayed:

```
[LWSV-ERR015] Processing will be canceled because the number of log items will exceed %d. Review
the conditions.
```

```
[LWSV-ERR011] Processing will be canceled because the number of log data items (%d) was exceeded.
Review the conditions.
```

In this case, refine the search conditions before performing the search again.

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

View logs by CT or smart device (agent)

The CT operation log corresponding to the client (CT) will be displayed in **List of logs**.

View logs of client (CT) and smart device (agent) under the selected range in CT group tree

CT operation logs of all clients (CTs) and smart devices (agents) 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**.

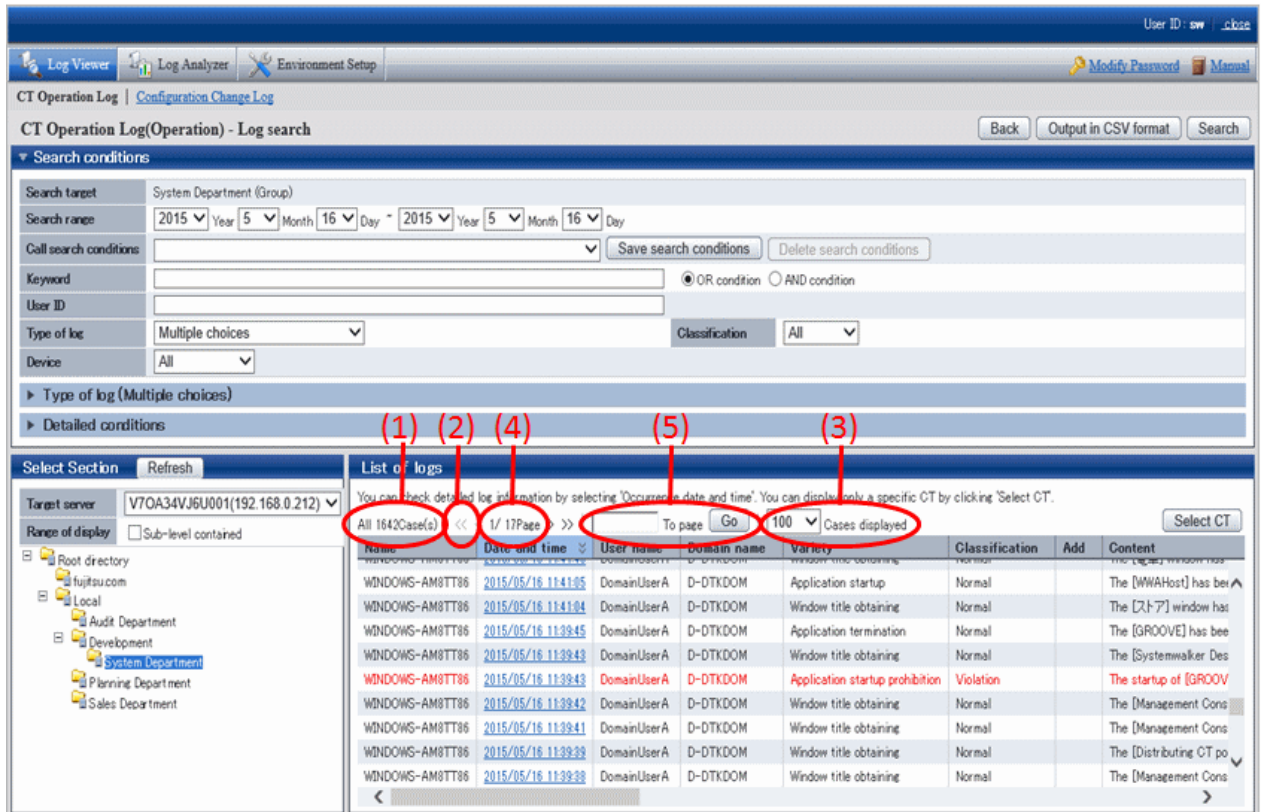
The screenshot shows the Log Analyzer interface. The top navigation bar includes 'Log Viewer', 'Log Analyzer', and 'Environment Setup'. The main title is 'CT Operation Log (Operation) - Log search'. Below this, there are search filters for 'Search target' (System Department (Group)), 'Search range' (2015 Year 5 Month 16 Day), and 'Call search conditions'. The 'List of logs' section shows a table of log entries with columns: Name, Date and time, User name, Domain name, Variety, Classification, Add, and Content. One entry is highlighted in red, indicating a violation.

Name	Date and time	User name	Domain name	Variety	Classification	Add	Content
WINDOWS-AM8TT86	2015/05/16 11:41:05	DomainUserA	D-DTKDOM	Application startup	Normal		The [WWAHost] has be...
WINDOWS-AM8TT86	2015/05/16 11:41:04	DomainUserA	D-DTKDOM	Window title obtaining	Normal		The [ソフトウェア] window has
WINDOWS-AM8TT86	2015/05/16 11:39:45	DomainUserA	D-DTKDOM	Application termination	Normal		The [GROOVE] has bee
WINDOWS-AM8TT86	2015/05/16 11:39:43	DomainUserA	D-DTKDOM	Window title obtaining	Normal		The [Systemwalker Des
WINDOWS-AM8TT86	2015/05/16 11:39:43	DomainUserA	D-DTKDOM	Application startup prohibition	Violation		The startup of [GROOV
WINDOWS-AM8TT86	2015/05/16 11:39:42	DomainUserA	D-DTKDOM	Window title obtaining	Normal		The [Management Cons
WINDOWS-AM8TT86	2015/05/16 11:39:41	DomainUserA	D-DTKDOM	Window title obtaining	Normal		The [Management Cons
WINDOWS-AM8TT86	2015/05/16 11:39:39	DomainUserA	D-DTKDOM	Window title obtaining	Normal		The [Distributing CT po
WINDOWS-AM8TT86	2015/05/16 11:39:38	DomainUserA	D-DTKDOM	Window title obtaining	Normal		The [Management Cons

The client (CT), smart device (agent), and CT group that have generated violation logs will be displayed in red. Refer to "Display the group or client (CT) and smart device (agent) that have generated violation logs in red" for details.

- b. When clicking **Name** of the client (CT) and smart device (agent) to view logs, only the CT operation log of the correspondent client (CT) and smart device (agent) will be displayed.

When clicking **Number of violation logs** of the client (CT) and smart device (agent) to view logs, only the violation log of the correspondent client (CT) and smart device (agent) 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.).

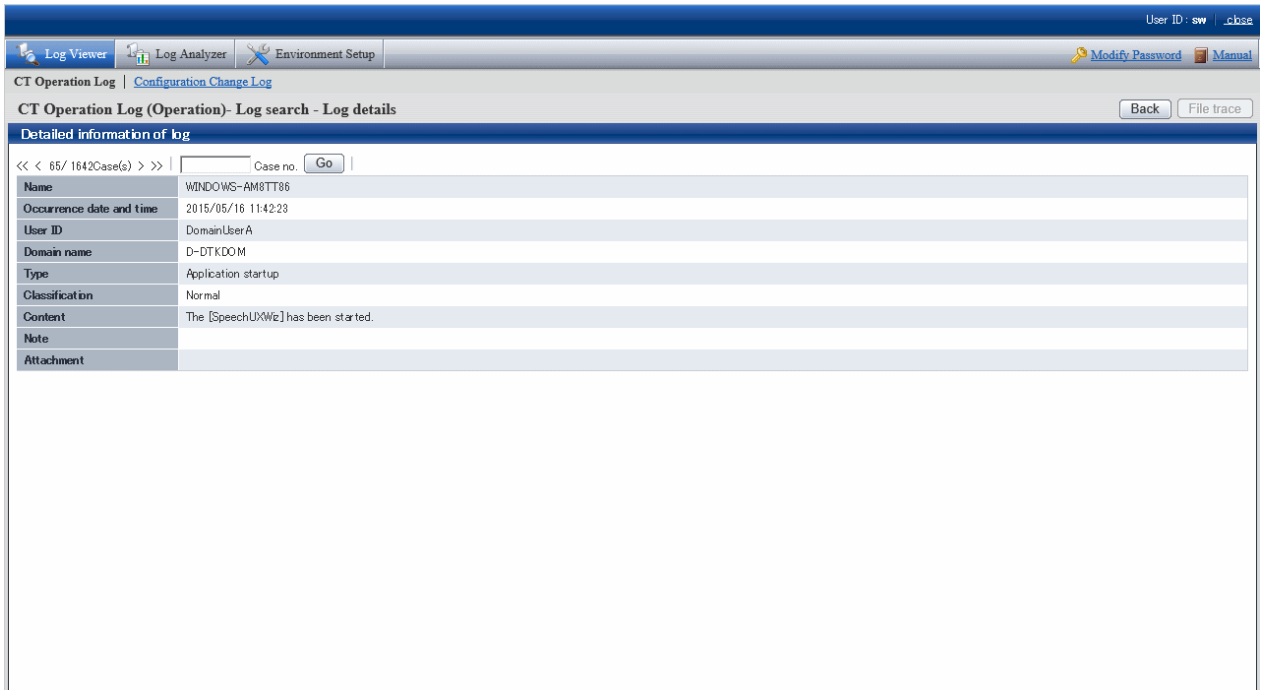
Item Name	Description	
	Client (CT)	Smart device (agent)
Name	This is the name that can be attached to the client (CT). Its initial value is the computer name. When modifying, refer to " Modify CT Policy ".	This is a name that can be given to a smart device (agent). Its initial value is a telephone number, or a model name if the telephone number cannot be obtained.
Date and time	This is the date and time when logs are collected in the client (CT) and smart device (agent).	
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),	This is the telephone number of a smart device (agent), or blank if the telephone number cannot be obtained.

Item Name	Description	
	Client (CT)	Smart device (agent)
	<p>the user name will be displayed as "System" when the following operation logs are collected:</p> <ul style="list-style-type: none"> - File operation log - E-mail sending log - E-mail attachment prohibition log <p>If a user logs on using a Microsoft account, up to 40 halfwidth characters (20 fullwidth characters) from the start of the Microsoft account information preceding @ will be displayed.</p> <p>For example, if the Microsoft account is "fujitsu.tarou@example.com", then "fujitsu.tarou" will be displayed as the user name.</p>	
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(R) 98 or Windows(R) 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"> - File operation log - E-mail sending log - E-mail attachment prohibition log <p>If a user logs on using a Microsoft account, the Microsoft account information will be displayed.</p> <p>For example, if the Microsoft account is "fujitsu.tarou@example.com", then "example.com" will be displayed as the domain name.</p>	This is the model name of the smart device (agent).
variety	<p>This is the type of the log. This line will be displayed in red when the following prohibition logs are collected:</p> <ul style="list-style-type: none"> - Application startup prohibition log - E-mail attachment Prohibition log - Device configuration change log (*1) - Printing prohibition log - Logon prohibition log - PrintScreen Key prohibition Log - URL access prohibition 	<ul style="list-style-type: none"> - Wi-Fi connection prohibition log - Bluetooth connection prohibition log - Application usage prohibition log

Item Name	Description	
	Client (CT)	Smart device (agent)
	<ul style="list-style-type: none"> - Web upload prohibition log - Web download prohibition log - FTP server connection prohibition log - Clipboard operation prohibition log - Linkage application log (*1) <p>*1: When the classification is Violation</p>	
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"> - This is displayed as 1 or 2 when the captured screen is the obtained window title log. <ul style="list-style-type: none"> - 1: when the captured screen is the obtained window 1. - 2: when the captured screen is the obtained window 2 - Displayed as 1 when the policy for obtaining screen capture is set in PrintScreen key prohibition log". - 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. <p>Displayed as 1 when the policy that allows viewing of E-mail content is set in E-mail sending log.</p>	
Content	<p>This is the content of the log</p> <p>Perform the following operations to confirm all contents:</p> <ul style="list-style-type: none"> - Click the Date and time of log display in List of logs, and confirm it in the Log Details window. - Confirm that the log is exported as a CSV file. Refer to "Export contents displayed in [List of logs] to CSV file" for a method of export to a CSV file. <p>Up to 519 halfwidth characters (259 fullwidth characters) 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"> - Logs are collected in the client (CT), the OS of which is Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 or Windows Server(R) 2012. - PC system of Log Viewer is Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 or Windows Server(R) 2012. <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 "&#xA;AAAA;", AAAA is a hexadecimal code with 4 or 5 digits.</p>	
Remarks	<p>This is the notes of the logs.</p>	

8. Click **Date and time** of the displayed log.

The **CT operation log(Operation) - Log search - Log details** window is displayed.



Item Name	Description	
	Client (CT)	Smart device (agent)
Name	For the name that can be attached to the client (CT), the initial value is the computer name. When modifying, refer to " Modify CT Policy ".	A name that can be given to a smart device (agent). The initial value is a telephone number, or a model name if the telephone number cannot be obtained.
Occurrence date and time	This is the date and time when logs are collected from the client (CT) and smart device (agent).	
User name	This is the user name entered when logging on the client (CT). 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: <ul style="list-style-type: none"> - File operation log - E-mail sending log - E-mail attachment prohibition log If a user logs on using a Microsoft account, up to 40 halfwidth characters (20 fullwidth characters) from the start of the Microsoft account information preceding @ will be displayed. For example, if the Microsoft account is "fujitsu.tarou@example.com", then "fujitsu.tarou" will be displayed as the user name.	This is the telephone number of a smart device (agent), or blank if the telephone number cannot be obtained.

Item Name	Description	
	Client (CT)	Smart device (agent)
Domain name	<p>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(R) 98 or Windows(R) 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 client (CT) when the following operation logs are collected:</p> <ul style="list-style-type: none"> - File operation log - E-mail sending log - E-mail attachment prohibition log <p>If a user logs on using a Microsoft account, the Microsoft account information will be displayed.</p> <p>For example, if the Microsoft account is "fujitsu.tarou@example.com", then "example.com" will be displayed as the domain name.</p>	<p>This is the model name of the smart device (agent).</p>
Type	<p>This is the type of the log. This line will be displayed in red when the following prohibition logs are collected:</p>	
	<ul style="list-style-type: none"> - Application startup prohibition log - E-mail attachment prohibition log - Device configuration change log (*1) - Printing prohibition log - Logon prohibition log - PrintScreen key prohibition log - URL access prohibition - Web upload prohibition log - Web download prohibition log - FTP server connection prohibition log - Clipboard operation prohibition log - Linkage application log (*1) <p>*1: When the classification is Violation</p>	<ul style="list-style-type: none"> - Wi-Fi connection prohibition log - Bluetooth connection prohibition log - Application usage prohibition log
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>	
Content	<p>This is the content of the log</p> <p>Up to 519 halfwidth characters (259 fullwidth characters) 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>	

Item Name	Description	
	Client (CT)	Smart device (agent)
	<ul style="list-style-type: none"> - Logs are collected in the client (CT), the OS of which is Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 or Windows Server(R) 2012. - PC system of Log Viewer is Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 or Windows Server(R) 2012. - 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 "&#xA;A;A;A;", A;A;A;A is a hexadecimal code with 4 or 5 digits). 	
Note (Note 1)	This is the notes of the logs.	
Attachment (Note 1)	<p>The displayed information is as follows:</p> <ul style="list-style-type: none"> - If the captured screen is the obtained window title log <ul style="list-style-type: none"> - Picture 1 - Picture 1, Picture 2 - When the captured screen is the obtained PrintScreen key prohibition log <ul style="list-style-type: none"> - Picture 1 - When the original backup policy is set in file export log <ul style="list-style-type: none"> - File name (display the backup file name) - When original file is backed up in linkage application log <ul style="list-style-type: none"> - Original file - When the policy that allows viewing of E-mail content is set in E-mail sending log <ul style="list-style-type: none"> - E-mail Content - In case of clipboard operation log" or clipboard operation prohibition log <ul style="list-style-type: none"> - The data copied via clipboard is text: Details - The data copied via clipboard is image: Picture - The data copied via clipboard is file: Details 	
Session ID (Note 2)	This is the ID indicating the command execute in command prompt of client (CT) and the result of command execution	
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** check box 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** check box 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](#).

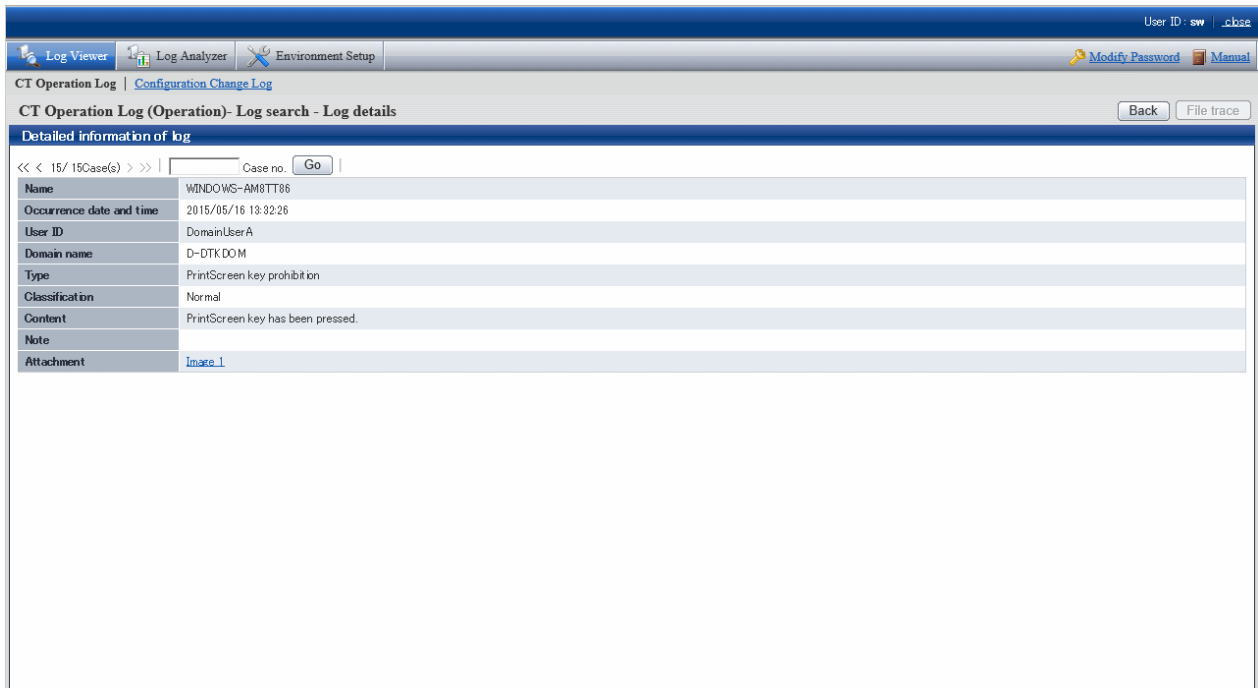
View/Save screen capture data

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.

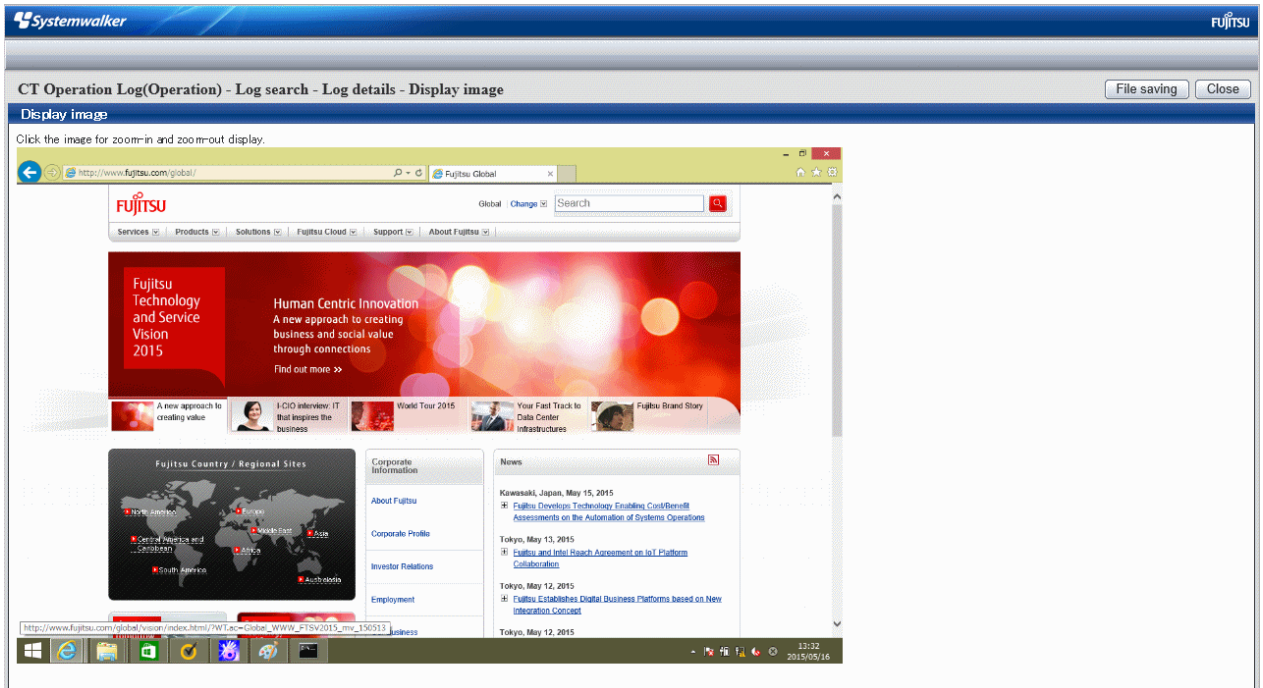


The screenshot shows the 'Log Viewer' application interface. The main window title is 'CT Operation Log (Operation) - Log search - Log details'. Below the title bar, there are navigation tabs for 'Log Viewer', 'Log Analyzer', and 'Environment Setup'. The current view is 'Detailed information of log'. A search bar shows '15/15Case(s)' and a 'Go' button. The log entry details are as follows:

Name	WINDOWS-AM8TT86
Occurrence date and time	2015/05/16 13:32:26
User ID	DomainUserA
Domain name	D-DTK DOM
Type	PrintScreen key prohibition
Classification	Normal
Content	PrintScreen key has been pressed.
Note	
Attachment	Image_1

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, 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. Confirm the settings and modify them according to the execution situation. For the confirmation of **Terminal Operation Settings**, 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"

Example: PC382686-20131215203412-1.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 tabs for 'Log Viewer', 'Log Analyzer', and 'Environment Setup'. The main window title is 'CT Operation Log (Operation) - Log search - Log details'. Below the title bar, there is a search bar with '1/ 1348Case(s)' and a 'Go' button. The main content area displays a table of log details:

Name	WINDOWS-AM8TT86
Occurrence date and time	2015/05/16 13:39:04
User ID	DomainUserA
Domain name	D-DTKDOM
Type	File export
Classification	Normal
Content	Take [D:\Customer.ledger.docx] as [F:\Customer.ledger.docx], through [Plain text], exporting to [F:] has been performed. Drive type: [Removable]
Note	Volumes: [], Size(byte) [2,521,919], Device name: [BUFFALO USB Flash Disk USB Device], Internal serial No.: [01B20802000000012]
Attachment	Customer.ledger.docx

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. 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"
Example: PC382686-20131226132137.wmf
- The original file backup name of E-mail sending log: "CT name" + "-" + "Log occurrence date and time (yyyymmddhhmss)" + "." + "Extension"
Example: PC382686-20131226132137.eml
- The original file backup name of clipboard operation log and clipboard operation prohibition log: "CT name" + "-" + "Log occurrence date and time (yyyymmddhhmss)" + "." + "Extension"
Example:
In case of text or file: PC382686-20131226132137.txt
In case of image: PC382686-20131226132137.png



Note

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, 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. Confirm the settings and modify them according to the execution situation. For the confirmation of **Terminal Operation Settings**, 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. Select the desired option.

For the item name and description of an exported CSV file, refer to "Log List" of *Systemwalker Desktop Keeper Reference Manual*.

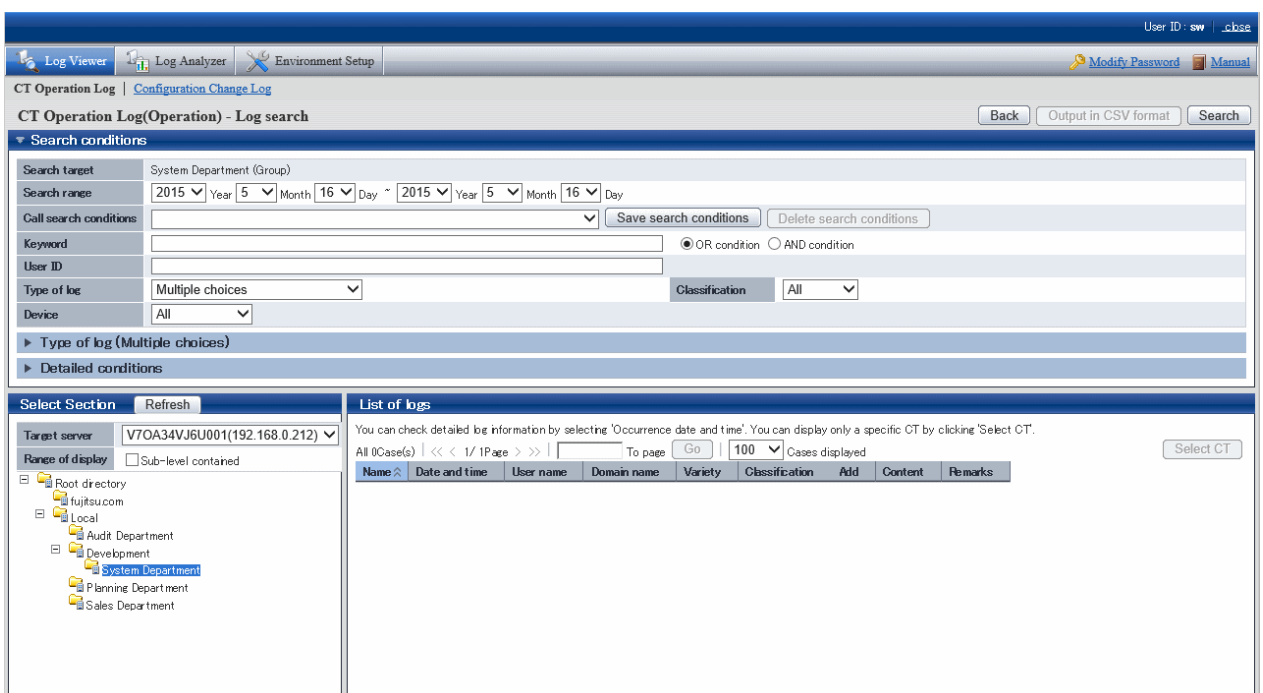
When file download is not successful

When the download of CSV file, original file backup and command operation file is not successful, refer to "Preparation of Using Web Browser in PC" of *Systemwalker Desktop Keeper Installation Guide* to modify the settings of Internet Explorer(R).

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**.



The screenshot shows the Log Viewer application interface. The top navigation bar includes 'Log Viewer', 'Log Analyzer', and 'Environment Setup'. The main window title is 'CT Operation Log | Configuration Change Log'. Below the title, there are buttons for 'Back', 'Output in CSV format', and 'Search'. The 'Search conditions' section is expanded, showing search criteria for 'System Department (Group)', '2015 Year 5 Month 16 Day', and '2015 Year 5 Month 16 Day'. There are also fields for 'Keyword', 'User ID', 'Type of log' (set to 'Multiple choices'), and 'Device' (set to 'All'). The 'List of logs' section is visible, showing a table with columns: Name, Date and time, User name, Domain name, Variety, Classification, Add, Content, and Remarks. The table currently displays 'All 0Case(s)'. A 'Select CT' button is located to the right of the table.

3. The asset information of Systemwalker Desktop Patrol will be displayed in other windows.

5.2.2 View Logs in the User Operation Log Window

In the **User operation log** window, you can search and browse logs by user. This section describes how to browse logs in the **User operation log** window.

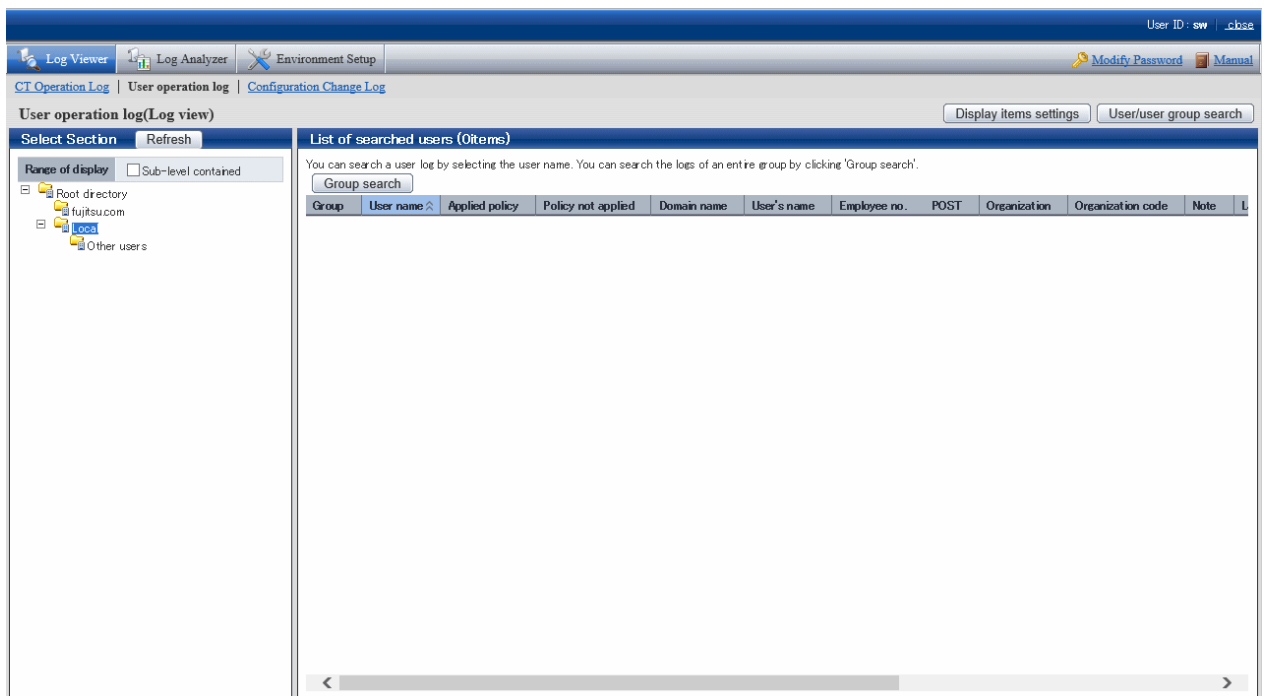
The procedure is as follows:

1. Start the Log Viewer and click **Display items settings**.

The **Display items settings** window is displayed.

2. Select **Log Viewing Database** as the database for browsing operation logs.
Refer to "[Change the database to be viewed](#)" for details on operation.
3. In the menu, click **User operation log**.
The **User operation log** window is displayed.
4. In **Select Section**, select the search target groups.
In **Range of display > Sub-level contained**, select whether to display all users or just the users directly under the selected group.
Selecting **Root directory** searches for all users.
Selecting a group searches for all users in that group.
If a log for a user who is not registered in the user policy has been recorded, the user name retrieved from that log is displayed as a user in the **Other users** group.

List of searched users displays a list of the users who belong to the selected group.



The following table describes the items that are displayed in **List of searched users**:

Item name	Description
Group	This is the name of the group to which the user belongs.
User name	This is the user name entered at logon. Clicking a user name displays the log search window for that user.
Applied policy	This is the applied policy. <ul style="list-style-type: none"> - User: User policy is applied. - Group: User group policy is applied. Nothing is displayed for users in the Other users group.
Policy not applied	If the settings are configured not to apply a policy, Do not apply is displayed. Nothing is displayed if a policy has been applied and the user is in the Other users group.
Domain name	If the user has been registered in the user policy and was created through linkage with Active Directory, the domain address registered in the Active Directory linkage settings of the Server Settings Tool is displayed.

Item name	Description
	If the user has been registered in the user policy and is in Local group, Local is displayed. If the user is in the Other users group, Local is displayed.
User's name	The value set in the User Policy Settings window of the Management Console is displayed. Nothing is displayed for users in the Other users group.
Employee no.	The value set in the User Policy Settings window of Management Console is displayed. Nothing is displayed for users in the Other users group.
POST	The value set in the User Policy Settings window of Management Console is displayed. Nothing is displayed for users in the Other users group.
Organization	The value set in the User Policy Settings window of Management Console is displayed. Nothing is displayed for users in the Other users group.
Organization code	The value set in the User Policy Settings window of Management Console is displayed. Nothing is displayed for users in the Other users group.
Note	The value set in the User Policy Settings window of Management Console is displayed. Nothing is displayed for users in the Other users group.
Last policy acquisition date and time	This is the date and time at which the latest policy was set. Nothing is displayed for users in the Other users group.
Server (DB) update date and time	This is the final date and time at which the Management Server or Master Management Server updated the client (CT) and smart device (agent) policy and updated it in the database (including immediate update). Nothing is displayed for users in the Other users group.
Registration datetime	This is the date and time at which the user was registered. Nothing is displayed for users in the Other users group.

Point

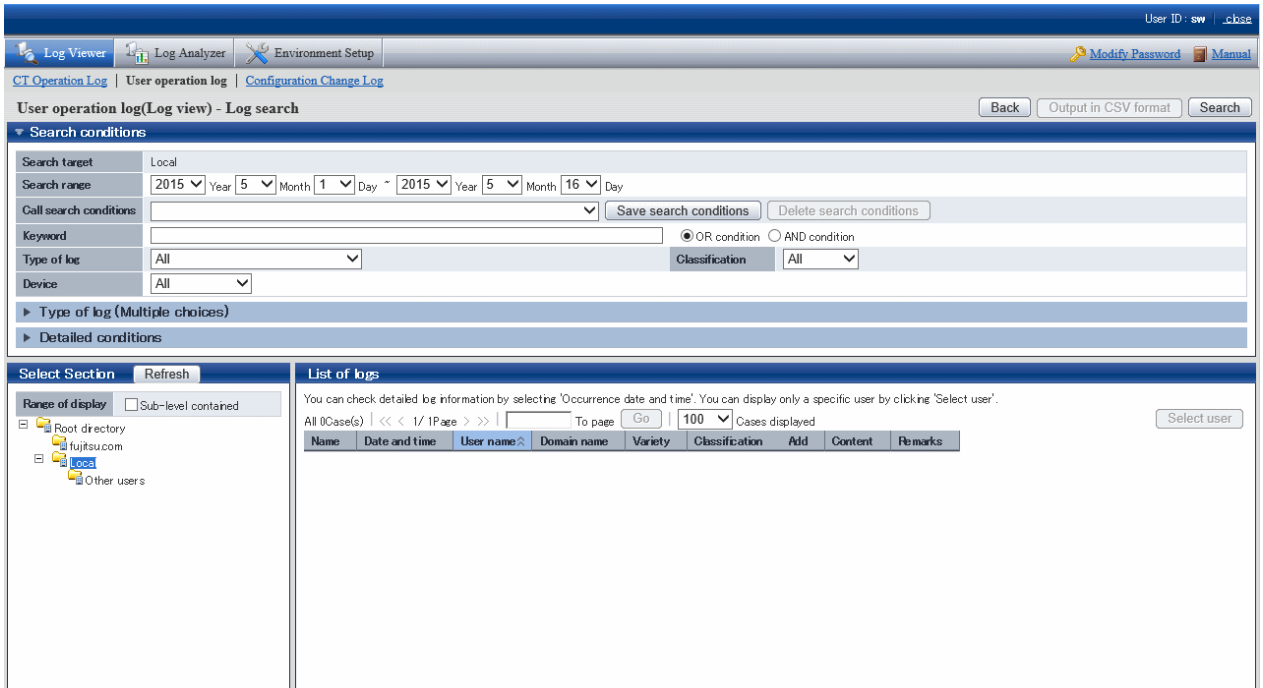
To change the items displayed in **List of searched users**, display the **Display items settings** window by clicking **Display items settings**, and then change the items in **Display settings for list of searched users**.

The procedure is the same as that for **Display settings for list of searched CTs**. Refer to "[Set visible columns in \[List of searched CT\]](#)" for details.

5. Perform one of the following operations according to the purpose of browsing the user operation logs:

- Browse logs by user
In **List of searched users**, click **User name** of the user whose logs you want to browse.
- Browse the logs of users in the range selected in the group tree
In **List of searched users**, click **Group search**.

The **User operation log(Log view) - Log search** window is displayed.



You can open and close the **Search conditions**, **Type of log (Multiple choices)**, and **Detailed conditions** panes.

Clicking **User operation log(Log view) - Log search**, **Type of log (Multiple choices)**, or **Detailed conditions** (the expand icon) opens the search conditions.

Clicking **User operation log(Log view) - Log search**, **Type of log (Multiple choices)**, or **Detailed conditions** closes the search condition pane.

6. Set **User operation log(Log view) - Log search**.

To set detailed conditions such as the drive type and log collection time, click **Detailed conditions**.

Item name	Description
Search target	The selected search target is displayed. The user name or group name will be followed by "(User)" or "(Group)".
Search range	Searches a specified time range. If you do not specify the start time and end time of Search range , all search periods may be searched. If you do not specify any start month or date, the search will start from the beginning of the specified year (January 1). If you do not specify any start date, the search will start from the beginning of the specified month (the first day). - Start date 2013 9 -: September 1, 2013 is assumed to have been specified. 2013 - -: January 1, 2013 is assumed to have been specified. - Year -Month- Day : Search from the earliest saved log. 2013 - 15: Invalid date - 9 15: Invalid date If you do not specify any end month or date, the search will end at the end of the specified year (December 31). If you do not specify any end date, the search will end at the end of the specified month (the last day). - End date 2013 9 -: September 30, 2013 is assumed to have been specified.

Item name	Description
	<p>2013 - -: December 31, 2013 is assumed to have been specified.</p> <p>-Year - Month _Day: Search up to the last saved log.</p> <p>2013 - 15: Invalid date</p> <p>- 9 15: Invalid date</p> <p>If you omit the year, you must omit the month and day.</p> <p>If you omit the month, you must omit the day.</p> <p>The date on which you display the User operation log(Log view) - Log search window is displayed as the initial value for both the start date and end date.</p>
Call search conditions	<p>Invokes saved search conditions.</p> <p>The methods for saving or deleting search conditions are as follows:</p> <ul style="list-style-type: none"> - Saving <p>Set a search condition to be saved. You can save conditions that are not included in Search range.</p> <p>After setting conditions, click Save search conditions. The window for saving search conditions is displayed.</p> <p>To save search conditions for the first time, click Save as > Register. Each administrator can save up to 10 search conditions. If 10 search conditions have already been saved, to save another, delete the oldest and register the new search condition.</p> <p>Up to 128 halfwidth and fullwidth characters can be entered as the search condition name.</p> <p>To update a search condition, click Update > Register.</p> - Deleting <p>To delete a search condition, select the search condition name and click Delete search conditions.</p>
Keyword	<p>Searches according to log keyword. When specifying multiple keywords, enter a halfwidth or fullwidth space between keywords.</p> <p>If you specify OR condition, the search will be an OR search using more than one of the multiple keywords that you specified. If you specify AND condition, the search will be an AND search using all the multiple keywords that you specified.</p> <p>If you specify multiple keywords, select the OR condition or AND condition.</p> <p>Content enclosed within square brackets [] in information that is displayed in the content column and notes column of logs can be set as a keyword.</p> <p>The content that you can set as a keyword depends on the log type. Refer to the content and note under "Displayed content" in "8.2.1 Application Startup Log" to "8.2.22 Configuration Change Log".</p>
Type of log	<p>Searches a selected log type.</p> <p>To specify multiple log types in the search conditions, select Multiple choices. The Type of log (Multiple choices) pane opens directly below. Select the desired log types.</p>
Classification	<p>You can select allowed operations or unallowed operations in the policy settings. To search allowed operations, select Normal. To search unallowed operations, select Violation. Selecting All is equivalent to selecting Normal and Violation.</p>
Device	<p>Searches according to the selected device type. To search only client (CT) logs, select PC. To search only smart device (agent) logs, select Smart device. Selecting All sets PC and Smart device, and all device logs will be searched.</p>

Type of log (Multiple choices)

The screenshot shows the 'User operation log(Log view) - Log search' interface. Under the 'Type of log (Multiple choices)' section, there is a grid of checkboxes for various log types. The 'Select all' button is highlighted, indicating that all log types are currently selected.

Item name	Description
Type of log	<p>Select the types of log to be displayed in List of logs. Refer to "Types of log that can be viewed" for details on log types.</p> <p>Select all: Selects all log types.</p> <p>Clear all: Clears all log types.</p> <p>Initial value: All log types are selected.</p>

Detailed conditions

The screenshot shows the 'Detailed conditions' section of the log search interface. It includes options to filter by drive type, time, and day of the week. The 'Specify time' section shows a grid of checkboxes for each hour of the day, with 'Select all' and 'Clear all' buttons.

Item name	Description
Drive type	<p>Searches according to drive type. The drive type condition is enabled when you specify any of the following items in Type of log:</p> <ul style="list-style-type: none"> - All - File operation - File export <p>The following drive types can be specified - specify one or more:</p> <ul style="list-style-type: none"> - Removable: The following media identified by a drive letter: <ul style="list-style-type: none"> - Floppy disk - External hard disk (removable hard disk connected via USB, IEEE1394, PCMCIA, etc.) - MO - USB memory - Compact flash memory - Remote: Network drive - CD/DVD: CD/DVD drive - Fixed: PC fixed drive <p>Relationship between searched logs and the settings for Type of log and Drive type</p> <ul style="list-style-type: none"> - If you specify File operation in Type of log, the logs for which Drive type (removable, remote, CD/DVD, fixed) is specified as the following locations A) to J) are displayed as search results: <ul style="list-style-type: none"> - A) When creating: File creation destination - B) When updating: Location of the updated file - C) When viewing: Location of the viewed file - D) When deleting: Location of the deleted file - E) When renaming: Location of the file before renaming - F) When renaming: Location of the file after renaming - G) When copying: Location of the copy source file - H) When copying: File copy destination - I) When moving: Location of the move source file - J) When moving: File move destination - If you specify File export in Type of log, the logs for which Drive type (removable, remote, CD/DVD, fixed) is specified as the file export destination are displayed as search results.
Time	<ul style="list-style-type: none"> - Not specified: Time is not included in the search conditions. - Specify range: Specifies a log collection time range in search conditions. <ul style="list-style-type: none"> - If you enter "a:00 to b:59", the search will use the time range a:00:00 to b:59:59 as a condition. - If you enter "a:00 to -:59", the search will use the time range a:00:00 to 23:59:59 as a condition. - If you enter "-:00 to b:59", the search will use the time range 00:00:00 to b:59:59 as a condition.

Item name	Description
	<p>If you enter both a and b, a must be equal to or less than b. If you specify two time ranges, an overlap does not pose any problem. If you specify "-" in the start time, "0" is assumed to have been specified. If you specify "-" in the end time, "23" is assumed to have been specified. The initial value contains "-" in all items (no condition has been set).</p> <ul style="list-style-type: none"> - Specify time: To specify the time at which a log was collected as a search condition, select the desired time. If you select more than one time, the search will be an OR search where at least one of the times selected must match. If you do not select any time, all times are assumed to have been selected. - Select all: Selects all check boxes in Specify time. - Clear all: Clears all check boxes in Specify time. <p>If you specify Day of the week together with this condition, the search will be an AND search using all conditions.</p>
Day of the week	<p>Select all: Selects all check boxes in Day of the week.</p> <p>Clear all: Clears all check boxes in Day of the week.</p> <p>Day of the week check box: To specify the day of the week on which a log was collected as a search condition, select the desired day of the week. If you select multiple days of the week, the search will be an OR search using at least one day of the week. If you do not select any day of the week, all days of the week are assumed to have been selected.</p> <p>If you specify Time together with this condition, the search will be an AND search using all conditions.</p>

7. Click **Search**.



Note

If you specify a large number of users or a long search period in the search conditions, the following message may be displayed:

```
[LWSV-SEL003] A search may not be possible due to the large amount of data targeted for search.
Continue processing?
```

If the conditions do not need to be reviewed, continue processing.

If the search takes a long time, a timeout may occur. Alternatively, if there is a large number of search results, the search may be canceled and one of the following messages may be displayed:

```
[LVSY-ERR015] Processing will be canceled because the number of log items will exceed %d. Review
the conditions.
```

```
[LWSV-ERR011] Processing will be canceled because the number of log data items (%d) was exceeded.
Review the conditions.
```

In this case, refine the search conditions before performing the search again.

Examples of refining search conditions:

- Reducing the search time
- Reducing the number of users set as the search target
- Setting a search keyword

The search results are displayed in **List of logs**.

The screenshot shows the Log Viewer application interface. The top navigation bar includes 'Log Viewer', 'Log Analyzer', and 'Environment Setup'. The main window title is 'User operation log(Log view) - Log search'. Below the title bar, there are search filters for 'Search target' (Root directory), 'Search range' (2015 Year 5 Month 1 Day to 2015 Year 5 Month 16 Day), 'Keyword' (Domain), 'Type of log' (Multiple choices), and 'Device' (All). The 'List of logs' section displays a table with columns: Name, Date and time, User name, Domain name, Variety, Classification, Add, Content, and Res. The table contains three rows of log entries.

Name	Date and time	User name	Domain name	Variety	Classification	Add	Content	Res
WINDOWS-AM8TT86	2015/05/16 11:30:00	DomainUserA	D-DTKDOM	Logon	Normal		Logged on. Authentication target: [D-DTKDOM]	Con
WINDOWS-AM8TT86	2015/05/16 11:22:57	Domain_UserA	D-DTKDOM	Logon	Normal		Logged on. Authentication target: [D-DTKDOM]	Con
WINDOWS-AM8TT86	2015/05/16 11:13:17	domainuserB	D-DTKDOM	Logon	Normal		Logged on. Authentication target: [D-DTKDOM]	Con

The search results data that is displayed in **List of logs** is arranged in ascending user name order and ascending date and time. To view logs by client (CT), click **Name** to sort them.

You can view a list of logs of a particular user by clicking **Select user** and selecting the user. Alternatively, you can view a list of logs of all users.

The content that is displayed in **List of logs** and the procedure for operating it are the same as those for **List of logs** in the **CT Operating Log** window. Refer to "5.2.1 View Logs in the CT Operation Log Window" for details.

5.2.3 View Logs in the Configuration Change Log Window

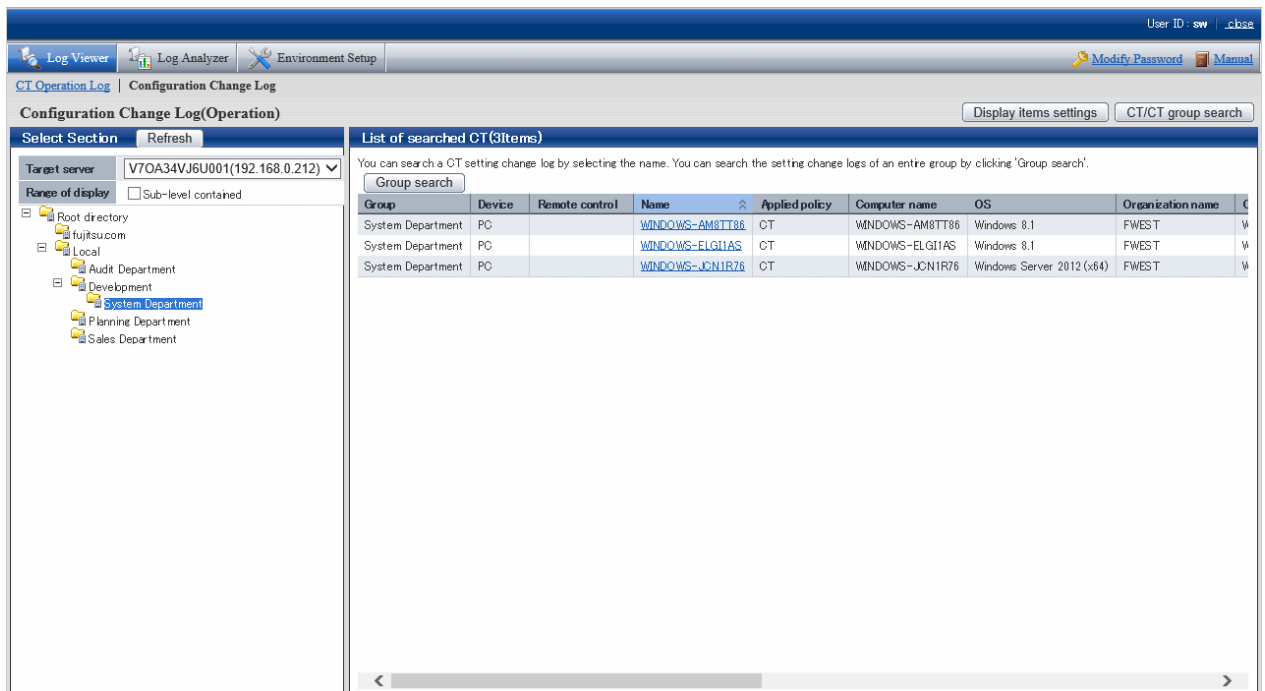
This department describes how to display **Configuration Change Log List** and how to view logs when modifying configuration information of client (CT) in the Management Console.

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. In **Select section > Target server**, select the Management Server that manages the clients (CTs) and smart devices (agents). In **Range of display > Sub-level contained**, select whether to display only the clients (CTs) and smart devices (agents) directly under the selected group, or all clients (CTs) and smart devices (agents).
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 and Terminal Operation Settings set in Management Server:

- a. Select the **Root directory** displayed in CT group tree of **Select Section**.
If **All** is specified in **Target server**, select a server.
The client (CT) and smart device (agent) are displayed in the **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 or smart device (agent):

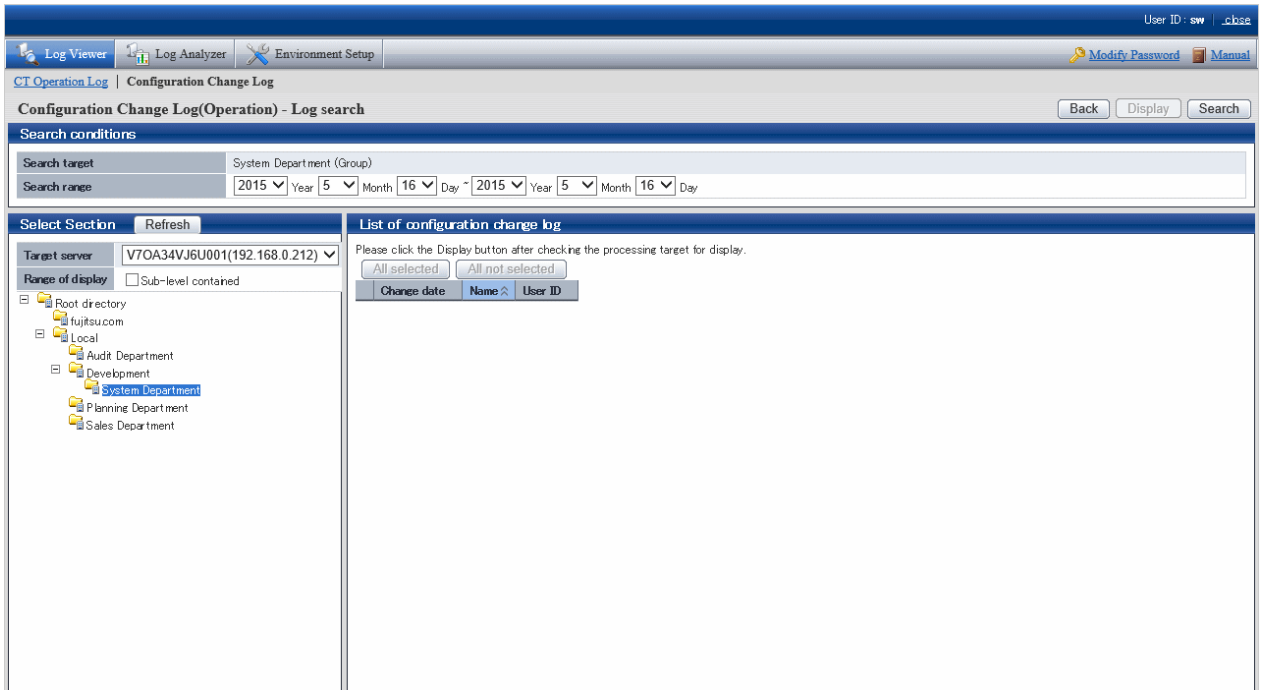
- a. Select the CT group to which the client (CT) and smart device (agent) for viewing logs belong from the CT group tree of **Select Section**.
The client (CT) and smart device (agent) that belong to the CT group are displayed in **List of searched CT**.

View configuration change log of CT group and its subordinate client (CT) and smart device (agent):

- 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) and smart device (agent) for viewing logs.

The **Configuration change log(Operation) - Log Search** window is displayed.

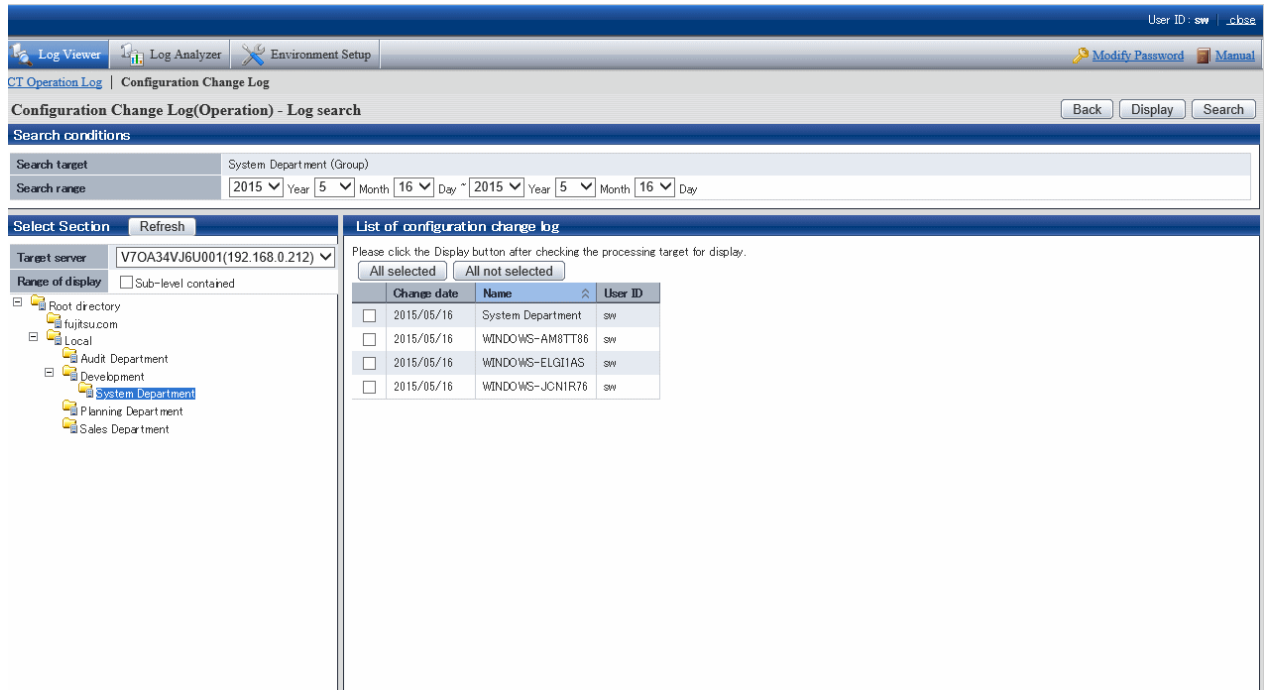


5. Set Search Conditions.

Item Name	Description
<p>Search range</p>	<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"> - Start date <ul style="list-style-type: none"> _ Sep 2013: 1 Sep. 2013 is assumed to be specified. __ 2013: 1 Jan. 2013 is assumed to be specified. _(Day)_(Month)_(Year): Start searching from the earliest saved log. 15_ 2013: Specification error 15 Sep. __: Specification error - End date <ul style="list-style-type: none"> _ Sep 2013: 30 Sep. 2013 is assumed to be specified. __ 2013: 31 Dec 2013 is assumed to be specified. _(Day)_(Month)_(Year): Search till the last saved log. _ 15, 2013: Specification error 15 Sep _ : Specification error <p>If the specified year is omitted, the specified month and day should be omitted.</p> <p>If the specified month is omitted, the specified day should be omitted.</p>

6. Click the **Search** button.

The search result is displayed in **List of configuration change log**.



The information will be sorted after clicking the following items (e.g. Date of change, Name or User ID).

Item Name	Description	
	Client (CT)	Smart device (agent)
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.	This is a name that can be given to a smart device (agent). Its initial value is a telephone number, or a model name if the telephone number cannot be obtained.
	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.	

- 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.

Item Name	Description	
	Client (CT)	Smart device (agent)
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.	This is a name that can be given to a smart device (agent). Its initial value is a telephone number, or a model name if the telephone number cannot be obtained.
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"> - Terminal settings: Records of modifying CT and smart device (agent) policy. - Level composition settings: Records of modifying CT group tree such as moving CTs, smart devices (agents), etc. - Services Control: Records of service control in the client (CT). - Process Control: Records of process control in the client (CT). 	
Content	This is the content of the configuration change log. The displayed content should be within 259 halfwidth characters (127 fullwidth characters). To confirm all contents, export to CSV file. For details on how to export to CSV files, 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** check box 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. Select the desired option.

For the item name and a description of the exported CSV file, 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, refer to "Preparation of Using Web Browser in PC" of *Systemwalker Desktop Keeper Installation Guide* to modify the settings of Internet Explorer(R).

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 (Web upload or download)

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 section 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, 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.

Point

You can perform a file trace even when searching the user operation log of a user who browses the Log Viewing Database.

The file trace feature is used in the same way as the CT operation log.

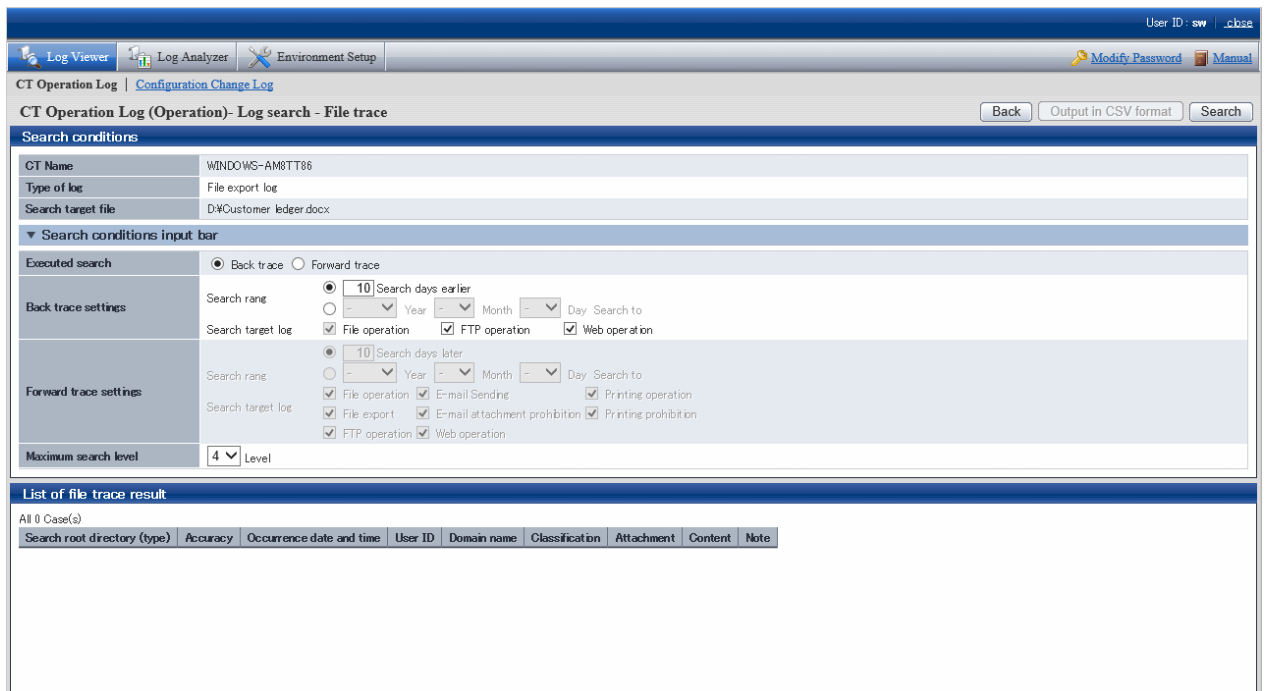
The range of a user operation log file trace is the user name and client (CT) for which the logs that were set as the trace target have been obtained. If there are multiple user names in a client (CT), you cannot perform a trace across multiple user names.

The description below describes how to perform a file trace using the CT operation log file trace feature, but the procedure is the same for the user operation log file trace feature.

1. Start Log Viewer.
2. 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, refer to "[5.2.1 View Logs in the CT Operation Log Window](#)".

3. 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	Back trace 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

Item Name	Description
	<p>Operation Log and export operations of File Export Log. This is used while investigating previous file operations.</p> <p>Forward trace 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>
<p>Search range</p>	<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"> - Period (Days) <ul style="list-style-type: none"> - "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". - Date <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> <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"> - The search range can be specified to "Jan 1, 2004 ~ Dec 31, 2024". - 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. - 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. - In case of both back trace and forward trace, it is unable to specify the date of generating operation log specified as tracing target. - Start date <ul style="list-style-type: none"> _ Sep 2013: 1 Sep. 2013 is assumed to be specified. __ 2013: 1 Jan. 2013 is assumed to be specified. _(Day)_(Month)_(Year): Start searching from the earliest saved log. 15_ 2013: Specification error 15 Sep. __: Specification error - End date <ul style="list-style-type: none"> _ Sep 2013: 30 Sep. 2013 is assumed to be specified. __ 2013: 31 Dec 2013 is assumed to be specified. _(Day)_(Month)_(Year): Search till the last saved log. _ 15, 2013: Specification error 15 Sep _ : Specification error

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.
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.

The screenshot shows the Log Analyzer interface. The top menu includes Log Viewer, Log Analyzer, and Environment Setup. The main window title is "CT Operation Log (Operation)- Log search - File trace". Below the title bar, there are buttons for "Back", "Output in CSV format", and "Search".

Search conditions

CT Name: WINDOWS-AM8TT86
Type of log: File export log
Search target file: D:\Customer ledger.docx

Search conditions input bar

Executed search: Back trace Forward trace

Back trace settings

Search range: 10 Search days earlier
Search target log: File operation FTP operation Web operation

Forward trace settings

Search range: 10 Search days later
Search target log: File operation E-mail Sending Printing operation
 File export E-mail attachment prohibition Printing prohibition
 FTP operation Web operation

Maximum search level: 4 Level

List of file trace result

All 3 Case(s)

Search root directory (type)	Accuracy	Occurrence date and time	User ID	Domain name	Classification	Attachment	Content
File export log	0	2015/05/16 13:36:08	DomainUserA	D-DTKDOM	Normal	1	Take [D:\Customer ledger.docx] as [F:\Customer ledger.docx] through [Plain text], exporting to [F:]
[Source file(Customer ledger.docx)]	0	2015/05/16 13:36:08	DomainUserA	D-DTKDOM	Normal	1	Take [D:\Customer ledger.docx] as [F:\Customer ledger.docx] through [Plain text], exporting to [F:]
[File operation log(Rename)]	A	2015/05/16 13:35:55	DomainUserA	D-DTKDOM	Normal		Operation: [Rename], Source file name: [D:\2MB.docx], Drive type: [Fixed], Target file name: [D:\Cus-

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)

Item Name	Description
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, refer to " View attached data ".
Content	Display the content of the log.
Notes	Display the notes of the log.

When there are more than 1,000 search results, a message indicating that search processing was canceled will be displayed and only the first 1,000 search results will 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)

The screenshot shows the Log Analyzer interface with the following search conditions:

- CT Name: WINDOWS-AM8TT86
- Type of log: File export log
- Search target file: D:\Customer ledger.docx
- Executed search: Back trace (selected)
- Back trace settings: Search range: 10 Search days earlier; Search target log: File operation, FTP operation, Web operation (checked)
- Forward trace settings: Search range: 10 Search days later; Search target log: File operation, E-mail Sending, Printing operation, File export, E-mail at attachment prohibition, Printing prohibition, FTP operation, Web operation (checked)
- Maximum search level: 1 Level

The search results table is as follows:

Search root directory (type)	Accuracy	Occurrence date and time	User ID	Domain name	Classification	Attachment	Content
File export log	0	2015/05/16 13:35:08	DomainUserA	D-DTKDOM	Normal	1	Take [D:\Customer ledger.docx] as [F:\Customer ledger.docx], through [Plain text], exporting to [F:]
[Source file(Customer ledger.docx)]	0	2015/05/16 13:35:08	DomainUserA	D-DTKDOM	Normal	1	Take [D:\Customer ledger.docx] as [F:\Customer ledger.docx], through [Plain text], exporting to [F:]
[File operation log(Rename)]	A	2015/05/16 13:35:55	DomainUserA	D-DTKDOM	Normal		Operation: [Rename], Source file name: [D:\2MB.docx], Drive type: [Fixed], Target file name: [D:\Cus

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]

Information of [Search Route (Type)]	Information of [Content]
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:\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. At the top, there are tabs for 'Log Viewer', 'Log Analyzer', and 'Environment Settings'. The 'Log Analyzer' tab is active, showing 'CT operation log' and 'Configuration Change Log'. Below this, there are buttons for 'Back', 'Output in CSV format', and 'Search'. The 'Search conditions' section includes a table with 'CT Name' (LWL-TKSUOC147R4), 'Type of log' (File export log), and 'Search target file' (C:\LA_worksettings.csv). Below this is a 'Search conditions input bar' with 'Executed search' set to 'Forward trace'. It includes 'Back trace settings' and 'Forward trace settings' with various search range and target log options. At the bottom, the 'List of file trace result' section shows a table with 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

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]
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. Select the desired option.

For item name and description of an exported CSV file, 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. 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, refer to "Preparation of Using Web Browser in PC" of *Systemwalker Desktop Keeper Installation Guide* to modify the settings of Internet Explorer(R)

5.4 Search CT Information in Log Viewer

This department describes how to search the client (CT), smart device (agent), and CT group.

When the "Deleted CT" group is displayed in the CT group tree of **Select Department** domain, the client (CT) and smart device (agent) that belong to the "Deleted CT" group will also be searched.

The client (CT) and smart device (agent) 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 directory** 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.

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** check box of **Applied policy** should not be selected.

Search Client (CT) and Smart Device (Agent):

Specify the items of search condition.

Item Name	Description
Computer name	Search according to the computer name of the client (CT) and smart device (agent). Results that partially match the input conditions will be displayed. Up to 15 characters (7 fullwidth characters) can be entered.
IP address	Search according to the IP address of the client (CT) and smart device (agent). Results of which the front part matches the input conditions will be displayed. Note that, for a dual stack network, search also for the IP address that is not displayed in the IP Address column in the CT list. Enter up to 45 halfwidth characters.

Item Name	Description
	<ul style="list-style-type: none"> - When an IPv6 address is entered When searching with "0123:12", the result will include "123:12:", "123:12X.", and "123:12XX.". ("X" indicates one halfwidth numeral character, and ":" indicates one halfwidth colon.) Note that, if conversion using RF5952 is possible, convert first before performing search. Example: If you entered "2001:db8:0:0:0:2:1", convert to "2001:db8::2:1" first, and then perform search. - When an IPv4 address is entered When searching with "10.1", the result will include "10.1.", "10.1X." and "10.1XX.". ("X" indicates one halfwidth numeral character, and "." indicates one halfwidth period.) Enter in the format of "XXX.XXX.XXX.XXX". Example: 140.48.23.12
MAC address	<p>Search according to the MAC address of the client (CT) and smart device (agent). Results that completely match the input conditions will be displayed.</p> <p>Enter in the format of "XX-XX-XX-XX-XX-XX". ("X" indicates one halfwidth alphanumeric character, and "-" indicates one halfwidth hyphen.)</p> <p>Example: 02-E0-32-33-A3-C0</p>
Owner name	<p>Search according to the owner set in the OS of client (CT). Results that partially match the input conditions will be displayed.</p> <p>Up to 93 halfwidth characters (46 fullwidth characters) can be entered.</p>
CT Version	<p>Search according to the version of the client (CT) and smart device (agent) of the Systemwalker Desktop Keeper installed. Results that completely match the input conditions will be displayed.</p> <p>Enter in the format of "X.X.X.X". ("X" indicates more than one halfwidth numeral character, and "." indicates a halfwidth period.)</p> <p>Example: 2.1.0.1</p>
Name/CT group name	<p>Search according to the name of the CT group or smart device (agent) and client (CT). Results that partially match the input conditions will be displayed.</p> <p>Up to 40 halfwidth characters (20 fullwidth characters) can be entered.</p>
DTPID	<p>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. (The "+" character is a halfwidth plus.)</p> <p>Perform search with partially matching.</p>
Notes	<p>Search according to the notes entered when updating the client (CT) and smart device (agent) policy. Results that partially matches the input conditions will be displayed.</p> <p>Up to 128 halfwidth characters (64 fullwidth characters) can be entered.</p>
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>A smart device (agent) on which you have performed automatic synchronization or clicked Sync now communicates with the Master Management Server or Management Server. You can search according to the date and time at which the communication was 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>

Item Name	Description
	<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"> - Start date <ul style="list-style-type: none"> _ Sep 2013: 1 Sep. 2013 is assumed to be specified. __ 2013: 1 Jan. 2013 is assumed to be specified. _(Day)_(Month)_(Year): Start searching from the earliest saved log. 15_ 2013: Specification error 15 Sep. __: Specification error - End date <ul style="list-style-type: none"> _ Sep 2013: 30 Sep. 2013 is assumed to be specified. __ 2013: 31 Dec 2013 is assumed to be specified. _(Day)_(Month)_(Year): Search till the last saved log. _ 15, 2013: Specification error 15 Sep _ : Specification error <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) and smart device (agent) obtain 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). 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> <ul style="list-style-type: none"> - Start date <ul style="list-style-type: none"> _ Sep 2013: 1 Sep. 2013 is assumed to be specified. __ 2013: 1 Jan. 2013 is assumed to be specified. _(Day)_(Month)_(Year): Start searching from the earliest saved log. 15_ 2013: Specification error 15 Sep. __: Specification error - End date <ul style="list-style-type: none"> _ Sep 2013: 30 Sep. 2013 is assumed to be specified. __ 2013: 31 Dec 2013 is assumed to be specified. _(Day)_(Month)_(Year): Search till the last saved log. _ 15, 2013: Specification error 15 Sep _ : Specification error <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>

Item Name		Description
Applied policy	As conditions	When this check box is selected, the policy being applied to the client (CT) and smart device (agent) will be included in the search condition.
	CT	The search targets are the client (CT) and smart device (agent) to which the CT policy is applied.
	Group	The search targets are the client (CT) and smart device (agent) to which the CT group policy is applied.
Active Directory Linkage target	As conditions	When this check box 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	As conditions	When this check box 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.
	Master image	This refers to the client (CT) installed in the master image of a virtual PC.
Device	As conditions	When this check box is selected, the environment where the client (CT) and smart device (agent) are installed will be included in the search condition.
	PC	This refers to the client (CT) installed in a PC.
	Smart device	This refers to the smart device (agent) installed in a smart device.
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

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, refer to "[Set visible columns in \[List of searched CT\]](#)".

After clicking **Name** of a searched client (CT), smart device (agent), 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.

5.5 Search User Information in the Log Viewer

This section describes how to search for users and user groups.

If the **Other users** group is displayed in the user group tree in the **Select Section** pane, users who belong to the **Other users** group are also searched.

Users in the **Other users** group are displayed as **Other users in Group** in **List of search users**.

1. Start the Log Viewer.
2. In the user group tree, select **Root directory > Local > Domain name** or **User Group** as the search target.
3. Click **User/user group search**.

The **User/user group search** window is displayed.

4. Enter the following information as the search conditions:

The search will be an AND search using all conditions.

Search a user group

Specify only **User name/user group name** and **Notes**. At this time, **As conditions** in **Applied policy** and **As conditions** in **Policy not applied** must not have been selected.

Search a user

Specify search condition items.

Item name	Description
User name/user group name	Search by user name or user group name. Results that partially match the input conditions will also be displayed. Up to 40 halfwidth and fullwidth characters can be entered.
User's name	Search by the user's name. Results that partially match the input conditions will also be displayed. Up to 128 halfwidth and fullwidth characters can be entered.
Employee no.	Search by the employee no. of the user. Results that partially match the input conditions will also be displayed. Up to 40 halfwidth and fullwidth characters can be entered.

Item name		Description
POST		Search by the post of the user. Results that partially match the input conditions will also be displayed. Up to 128 halfwidth and fullwidth characters can be entered.
Organization		Search by the organization of the user. Results that partially match the input conditions will also be displayed. Up to 128 halfwidth and fullwidth characters can be entered.
Organazation code		Search by the organization code of the user. Results that partially match the input conditions will also be displayed. Up to 40 halfwidth and fullwidth characters can be entered.
Notes		Search by the notes you entered when reflecting the user/user group policy. Results that partially match the input conditions will also be displayed. Up to 128 halfwidth and fullwidth characters can be entered.
Applied policy	As conditions	When this option is selected, the policy applied to the user is included in the search conditions.
	User	The search target is users to which the user policy has been applied.
	Group	The search target is users to which the user group policy has been applied.
Policy not applied	As conditions	When this option is selected, the setting indicating whether to apply the policy to a user is included in the search conditions.
	Apply	The search target is users to which the policy is to be applied.
	Do not apply	The search target is users to which the policy is not to be applied.
Search		Starts a search and displays the results.
Cancel		Saves the entered search conditions.



Note

Attention is required with fullwidth characters

If you use fullwidth characters for the following items, it is possible to enter a string that exceeds the upper limit but an error will occur during the search:

- **User name/user group name**
- **User's name**
- **Employee no.**
- **POST**
- **Organization**
- **Organazation code**
- **Notes**

5. Click **Search**.

The search results are displayed in **List of searched users**.

The displayed items are the ones that you selected in the **Display items settings** window. Refer to "[Set visible columns in \[List of searched CT\]](#)" for details on the **Display items settings** window.

When you click **User name** for the searched user or user group, the **Log search** window is displayed, with the relevant user group selected in the configuration information tree.

The entered search conditions are saved while you are logged on. However, they are cleared if you change your password or update to the latest information.

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 the 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 the 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 the 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, 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 the 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 directory" group instead of the "Not Configured" group.

About smart device (agent) operation log

The smart device (agent) operation log is not aggregated.

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(R) 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, prepare an environment that satisfies all the following conditions:

- The Report Output Tool has been installed in the PC that outputs report.
- Microsoft(R) Excel of any of the following versions has been installed in the PC that outputs report:
 - Microsoft(R) Office Excel 2007 (32-bit Edition)
 - Microsoft(R) Office Excel 2010 (32-bit Edition)
 - Microsoft(R) Office Excel 2013 (32-bit Edition)
- 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. 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 **Start > Systemwalker Desktop Keeper > Log Analyzer > Report Output Tool** or **Apps > Systemwalker Desktop Keeper > Report Output Tool**.

The login window is displayed.

Item Name	Description
Management Server	A list of Master Management Servers or Management Servers registered to the Log Analyzer Server is displayed in the menu. Select the Master Management Server or Management Server for which the login user ID is set from the menu.
User ID	It is user ID of the system administrator or department administrator.
Password	Specify the password of user ID entered in User ID .

The information moved from the Management Server to the 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, 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 or server name 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
- FTP operation (upload) log
- Web operation (upload) log

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.

The screenshot shows the 'Report Output Tool' window with the following configuration:

- User ID: systemadmin
- Management Server: 192.168.17.66
- Basic Information | Option | Log Information | Object Group
- Report title (T): Information Disclosure Analysis Report
- Created by (N): systemadmin
- Analysis period:
 - Daily report (D) Year: 2015 Month: 6 Day: 3
 - Weekly report (W) Year: 2015 Month: 5 Day: 24 In one week from this day
 - Monthly report (M) Year: 2015 Month: 4 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)

- User ID: This is the login user ID.
 - Management Server: This is the IP address or server name 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.

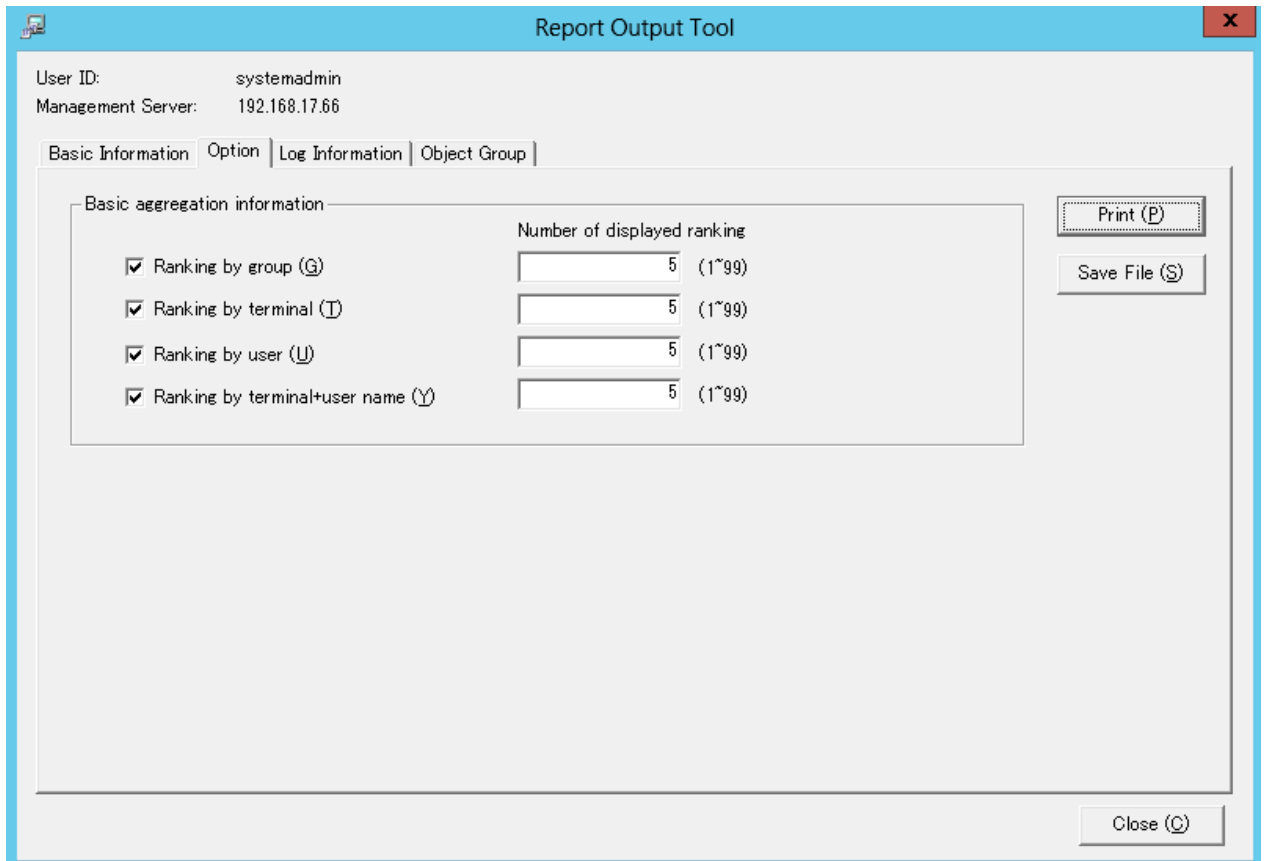
Settings of [Basic Information] tab

Set the following items.

Input Item		Content
Report title		Specify the report title using up to 64 halfwidth characters or 32 fullwidth characters.
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.
	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.



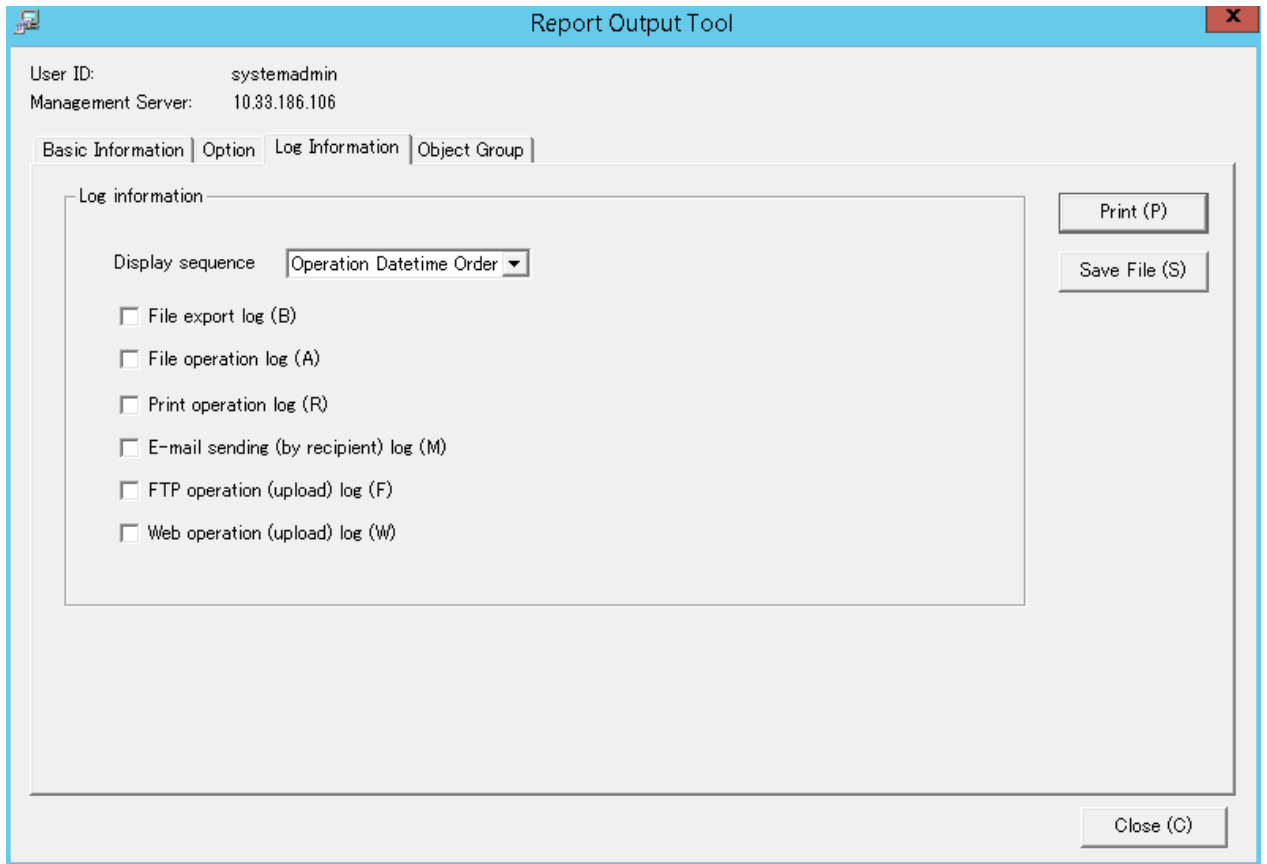
Select the ranking items to be output to report.

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 ranking based on number of cases.
Ranking by terminal	Display the result of aggregation by terminal with the ranking based on number of cases.
Ranking by user	Display the result of aggregation by user name with the 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 ranking based on number of cases. Even if the same user name appears in different terminals, it will be processed separately.

Settings of [Log Information] tab

Set the following items.

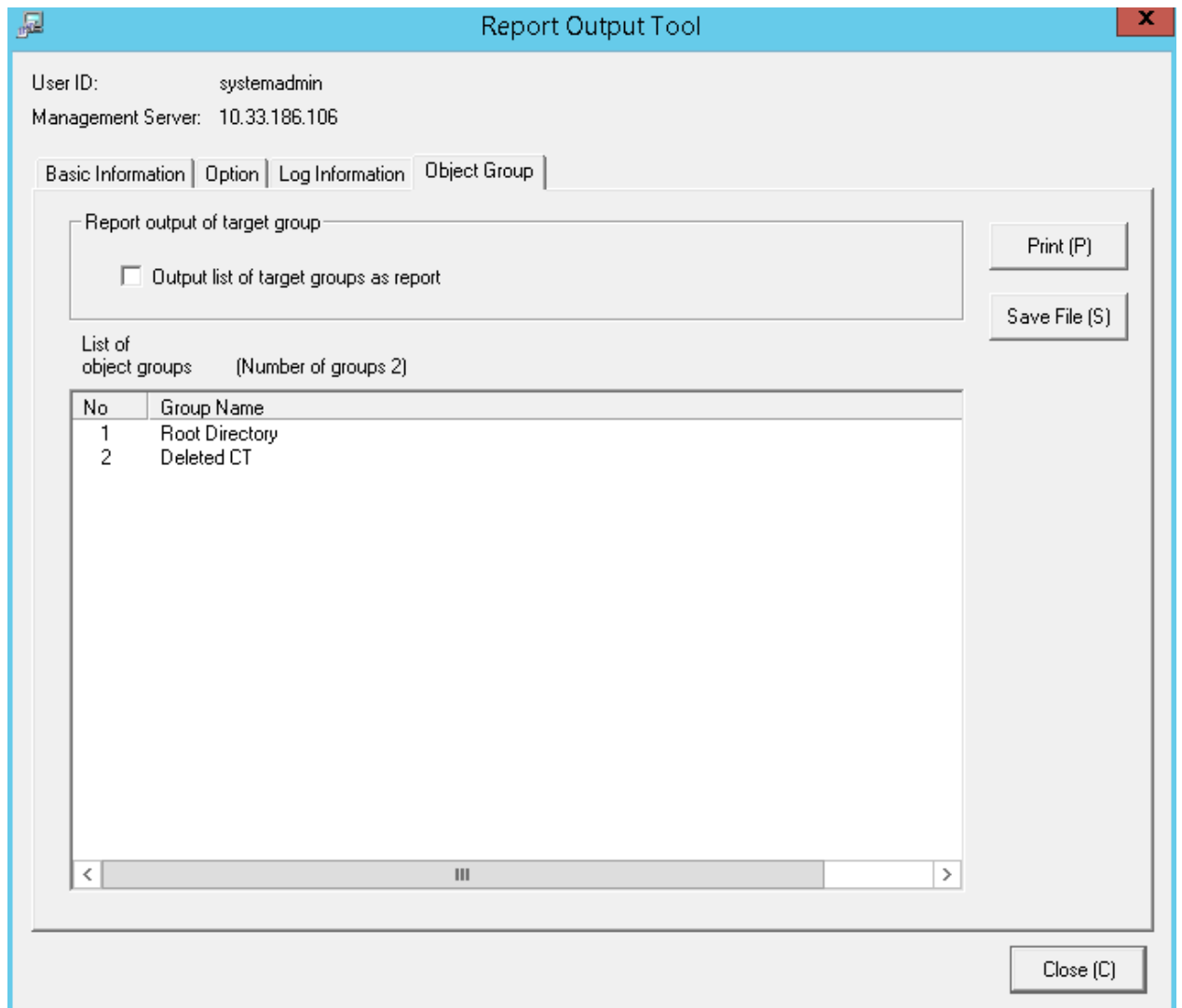


Select when outputting the logs used in the aggregation of ranking. All items are selected in default.
The Information disclosure analysis report is a single file output in CSV format.

Item Name	Description
Display sequence	Select the log display sequence from one of the following: - Operation Datetime Order - Group + Device + User Order The default value is Operation Datetime Order .
File export log	Output file export log as a separate file.
File operation log	Output file operation log as a separate file.
Print operation log	Output printing log as a separate file.
E-mail sending (by recipient) log	Output logs of e-mail sending by recipient address as a separate file.
FTP operation (upload) log	Outputs the FTP operation (upload) log as a separate file.
Web operation (upload) log	Outputs the Web operation (upload) log as a separate file.

Settings of [Object Group] tab

Set the following items.



Item Name	Description
Report output of target group Output list of target groups as report	<ul style="list-style-type: none"> - When it is selected: Output List of object to report. - When it is not selected (Initial Value): Do not output List of object to report.
List of object groups	<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

Do not operate Microsoft(R) Excel in the process of report output

Do not perform the **New** and **Open** operation of Microsoft(R) Excel file during the report output process, as report output may not be performed normally.

In addition, confirm whether Microsoft(R) Excel was started correctly before the report output. When Microsoft(R) 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 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.



Save the output report to a safe place

The output report may contain personal information and system configuration information. 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
E-mail Sending Log by Recipient Address	Leak_Log_Mailsend_YYYYMMDD.csv
FTP operation (upload)	Leak_Log_FTPUpload_YYYYMMDD.csv
Web operation (upload)	Leak_Log_WebUpload_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.

Also when the number of data items exceeds 50,000, the excess items will be output to a new file, with a unique sequential number enclosed by parentheses appended to the file name.

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)	
	Details (FTP operation uploads)	
	Details (Web operation uploads)	
Object Group Sheet	Object 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(R) Excel and service pack being used.

Summary Sheet

(1) Information Disclosure Analysis Report

Object	(2)	Managed Object *View object group sheet			
Number of object PCs	(3)	109 Set(s)			
Created by	(4)	systemadmin			
Created on	(5)	2015/05/13			
Analysis period	(6)	2015/03/21 ~2015/04/20			

				(7)	

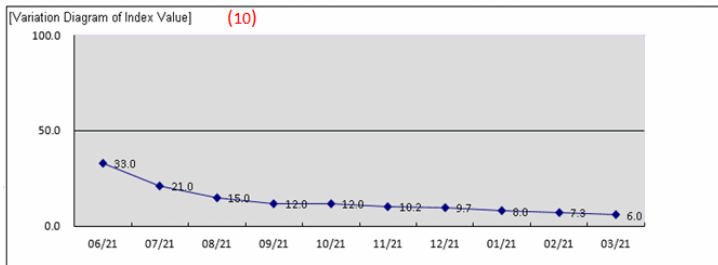
[Diagnosis Information] (8)

Index Value	6.0 %
-------------	-------

[Proportion of Number of items] (9)

Number of all items	41,696
Number of safe items	39,212
Number of dangerous items	2,484

Legend:
 □ Number of safe items
 □ Number of dangerous items



[Diagnosis Comment] (11)
 [Information disclosure analysis]
 Improved comparing with the last time. Improved in the long term.

[Variation of Number of items by Operation] (12)

	File export	File operation	Number of printing operations	Pages of printing operations	Email sending by recipient	FTP operation (upload)	Web operation (upload)
2015/03/21	0	0	0	0	0	0	0
2015/03/22	0	0	0	0	0	0	0
2015/03/23	0	0	0	0	0	0	0
2015/03/24	0	1	8	15	12	15	12
2015/03/25	6	0	43	89	19	89	19
2015/03/26	9	34	211	234	34	234	34
2015/03/27	1	82	34	47	22	47	22
2015/03/28	0	0	0	0	15	0	15
2015/03/29	0	0	0	0	0	0	0
2015/03/30	0	0	0	0	0	0	0
2015/03/31	0	15	12	18	34	18	34
2015/04/01	4	67	134	154	32	154	32
2015/04/02	3	88	24	48	19	48	19
2015/04/03	0	0	55	74	18	74	18
2015/04/04	0	0	0	0	0	0	0
2015/04/05	4	0	0	0	0	0	0
2015/04/06	1	45	45	88	76	88	76
2015/04/07	1	16	122	222	83	222	83
2015/04/08	2	9	112	176	89	176	89
2015/04/09	3	1	34	47	16	47	16
2015/04/10	7	18	21	45	28	45	28
2015/04/11	0	0	0	0	0	0	0
2015/04/12	0	0	0	0	0	0	0
2015/04/13	0	5	19	32	36	32	36
2015/04/14	2	2	29	32	29	32	32
2015/04/15	15	216	37	48	22	48	22
2015/04/16	1	12	68	78	26	78	26
2015/04/17	2	26	59	69	29	69	29
2015/04/18	0	0	0	0	0	0	0
2015/04/19	0	0	0	0	0	0	0
2015/04/20	0	8	59	129	76	129	76
Aggregation	51	640	1126	1640	657	1640	657

(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) + number of FTP operations (upload) + number of Web operations (upload)

[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.

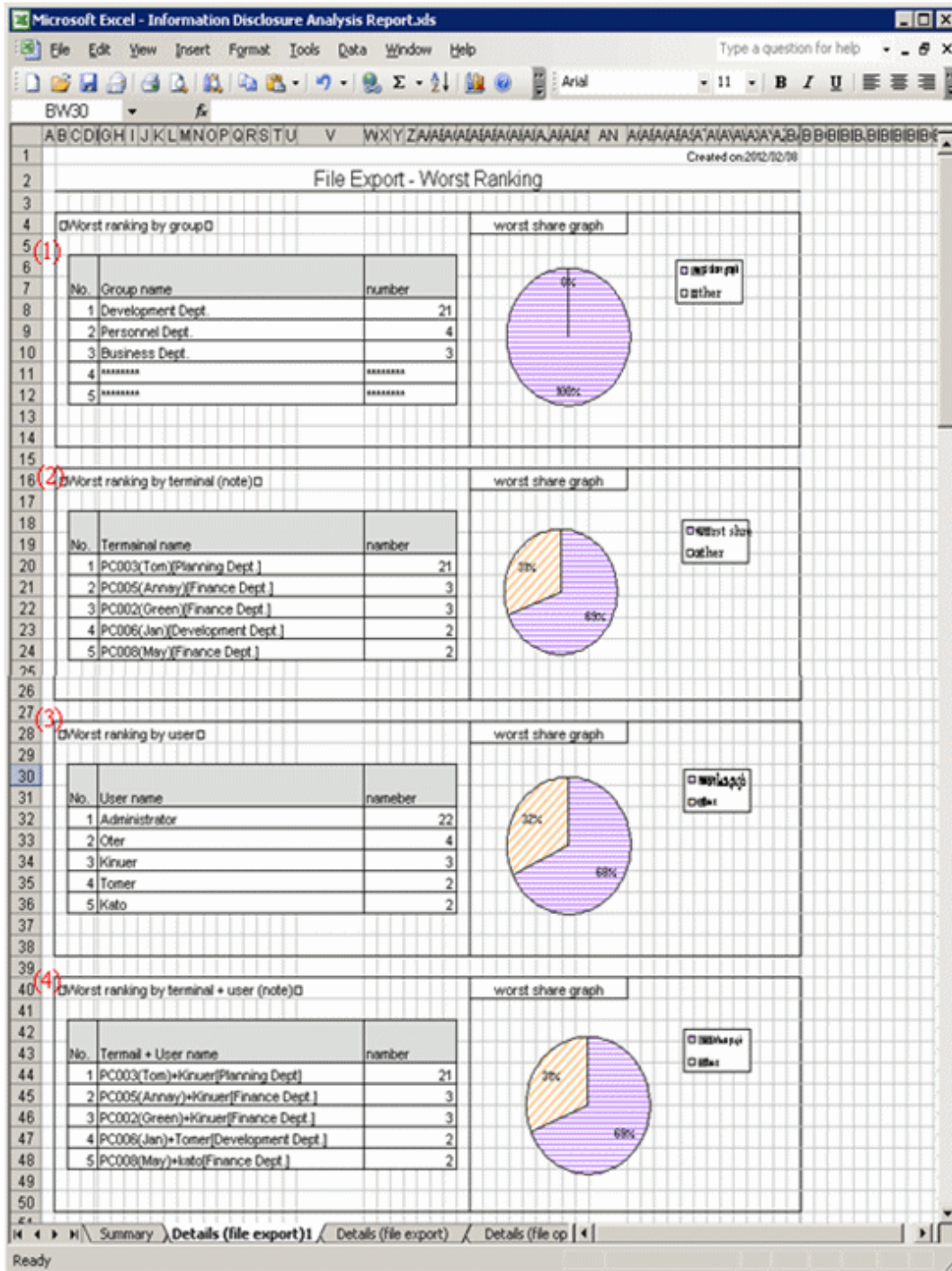
In addition, the maximum number of operation cases within the period is displayed in red character in each operation log.

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 halfwidth characters (256 fullwidth characters) can be displayed in the contents of each item in ranking table.



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) 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 ranking share graph.

(2) 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 ranking share graph.

(3) 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 ranking share graph.

(4) 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 ranking 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]

Object Group Sheet

The department information that has been analyzed will be output.

The screenshot shows an Excel spreadsheet titled "Information Disclosure Analysis Report.xls". The active sheet is "Object group". The table contains the following data:

(1) Object Group	
(2) No	(3) 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) Object 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 halfwidth characters (256 fullwidth characters) can be displayed in the content of each item in object 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. At the top, it displays 'User ID: systemadmin' and 'Management Server: 192.168.17.66'. Below this are four tabs: 'Basic Information', 'Option', 'Log Information', and 'Object Group'. The 'Basic Information' tab is active, showing a 'Report title (T)' field with 'Terminal Usage Analysis Report' and a 'Created by (N)' field with 'systemadmin'. To the right of these fields are 'Print (P)' and 'Save File (S)' buttons. The 'Analysis period' section has three radio button options: 'Daily report (D)' (selected) with Year 2015, Month 6, Day 3; 'Weekly report (W)' with Year 2015, Month 5, Day 24, and the note 'In one week from this day'; and 'Monthly report (M)' with Year 2015, Month 4, and the note 'In one month from this day'. A note below states 'The start date of weekly report and monthly report can be modified in Web Console.' The 'Index value' section has two input fields: 'Difference value compared with the last time (B)' with '10' and '% (1~99)', and 'Long-term difference (L)' with '5' and '% (1~99)'. A 'Close (C)' button is at the bottom right.

2. Set the items of each tab.

The settings of each tab will be saved in the 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

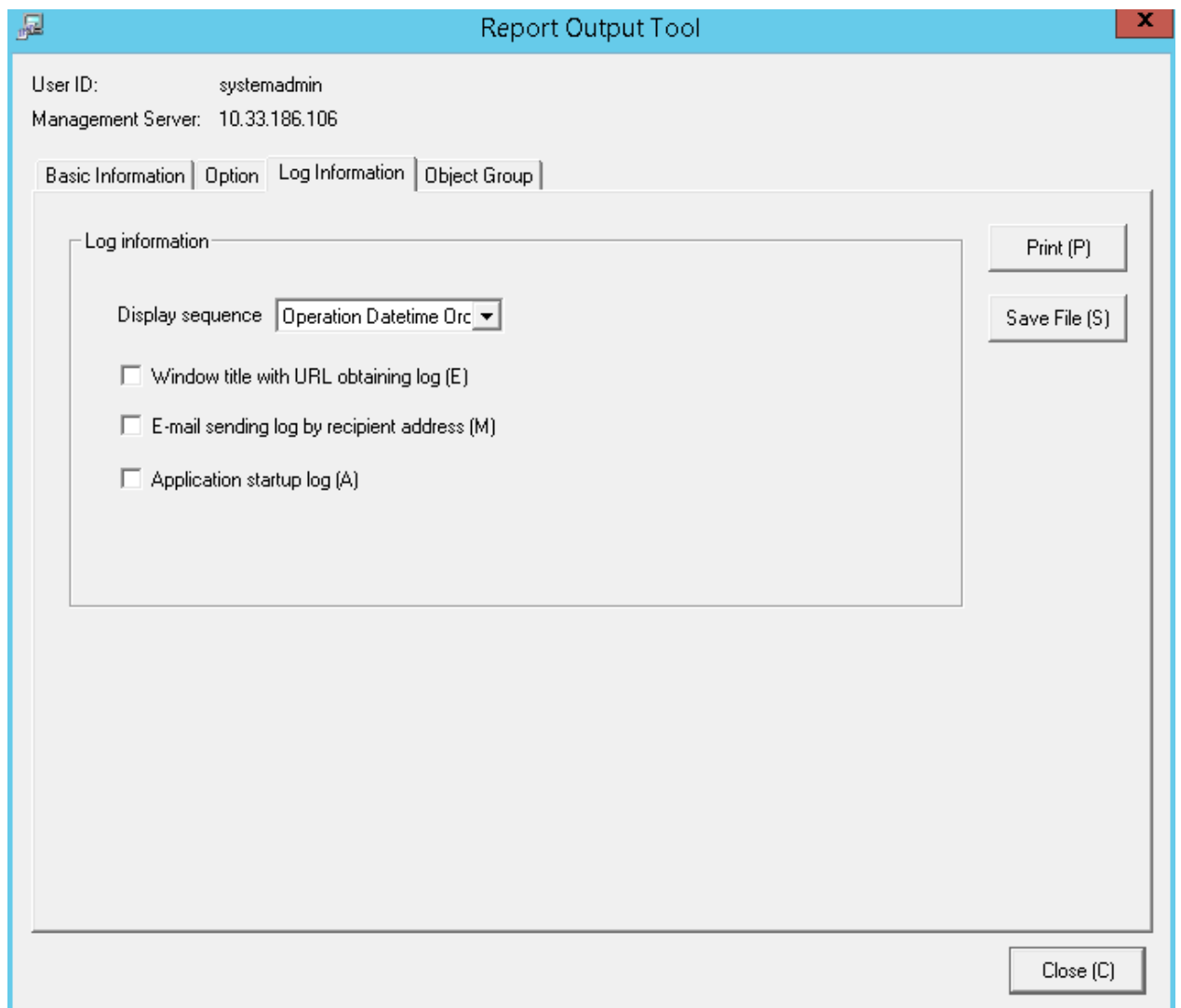
The settings of the **Basic Information** tab can be applied to the output of the Information disclosure analysis report. Refer to "[Settings of \[Basic Information\] tab](#)".

Settings of [Option] tab

The settings of the **Option** tab can be applied to the output of the Information disclosure analysis report. Refer to "[Settings of \[Option\] tab](#)".

Settings of [Log Information] tab

Set the following items.



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
Display sequence	Select the log display sequence from one of the following: - Operation Datetime Order - Group + Device + User Order The default value is Operation Datetime Order .

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 [Object Group] tab

Set whether the **Object Group List** can be output to report.

The settings of this tab can be applied to the output of the Information disclosure analysis report. Refer to "[Settings of \[Object Group\] tab](#)".

3. Click the **Print** or **Save File** button.

Note

Do not operate Microsoft(R) Excel in the process of report output

Do not perform the **New** and **Open** operation of Microsoft(R) Excel file in the report output process, as report output may not be performed normally.

In addition, confirm whether Microsoft(R) Excel was started correctly before doing the report output. When Microsoft(R) 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

Save the output report to a safe place.

The output report may contain personal information and system configuration information. 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
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.

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)	
Object Group Sheet	Object 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(R) 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.

Refer to "[Summary Sheet](#)", "[Detail Sheet](#)", "[Object Group Sheet](#)" for output format.

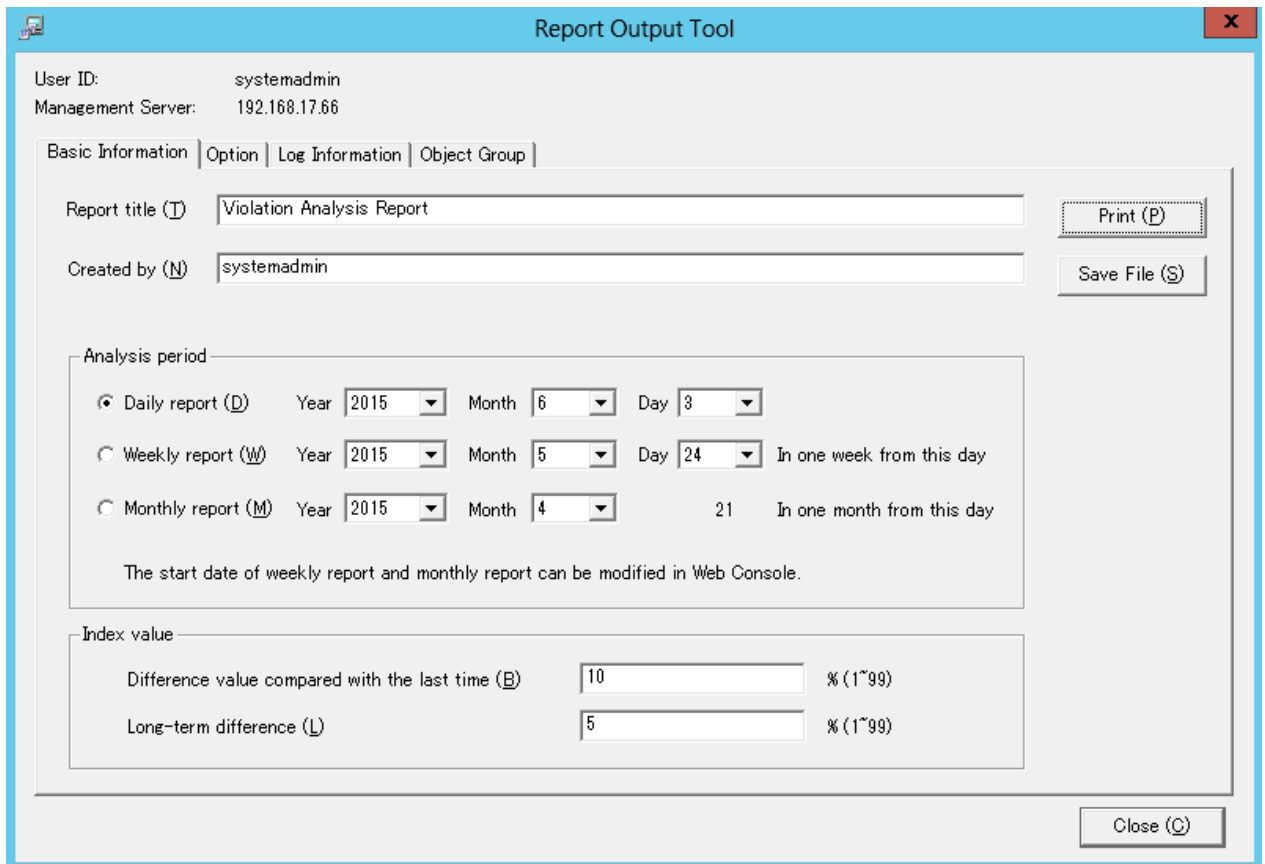
6.5 Violation Analysis Report

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: systemadmin
- Management Server: 192.168.17.66
- Basic Information tab is selected.
- Report title (T): Violation Analysis Report
- Created by (N): systemadmin
- Analysis period:
 - Daily report (D): Year 2015, Month 6, Day 3
 - Weekly report (W): Year 2015, Month 5, Day 24. In one week from this day
 - Monthly report (M): Year 2015, Month 4, 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

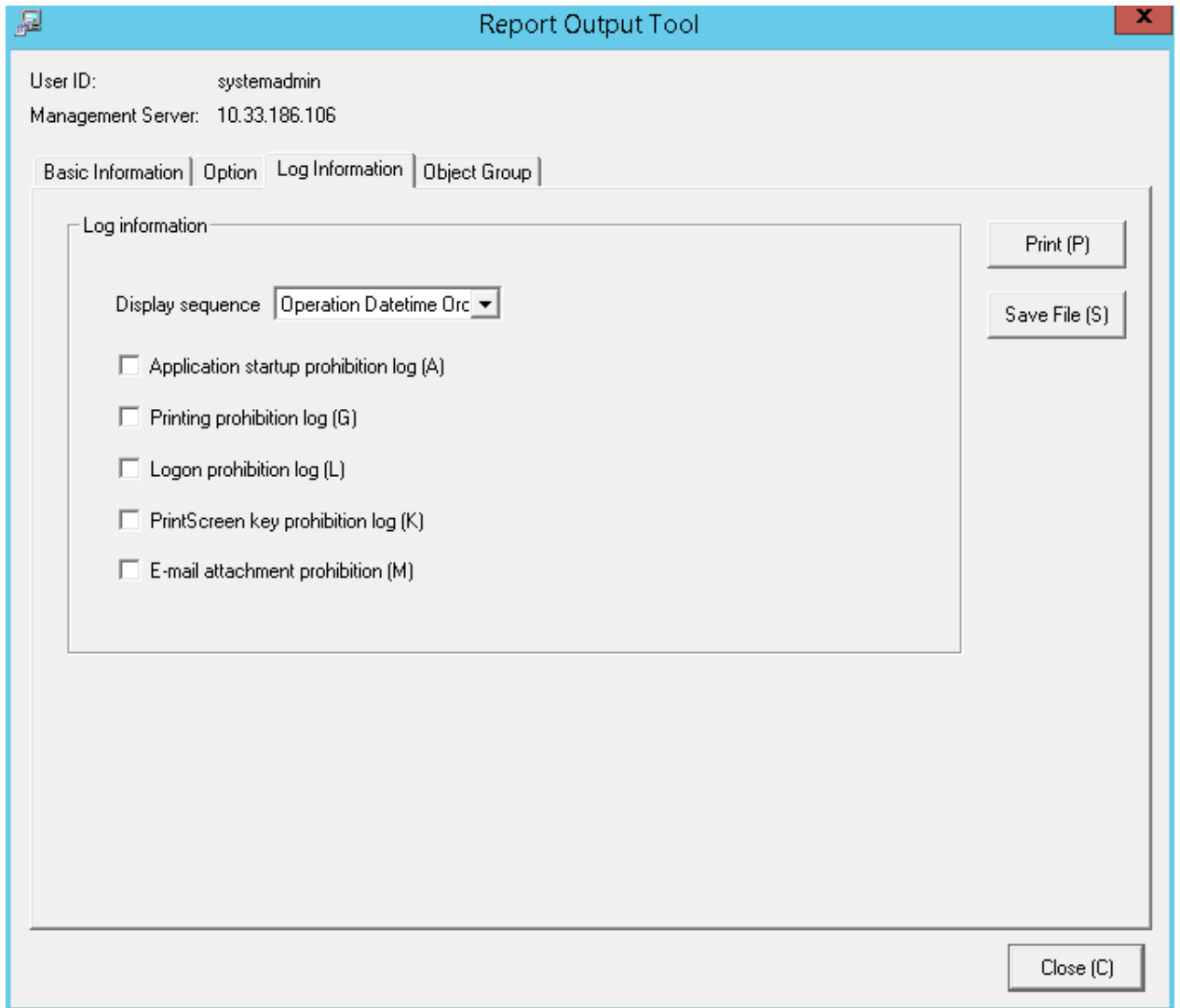
The settings of **Basic Information** tab can be applied to the output of information disclosure analysis report. Refer to "[Settings of \[Basic Information\] tab](#)".

Settings of [Option] tab

The settings of **Option** tab can be applied to the output of information disclosure analysis report. Refer to "[Settings of \[Option\] tab](#)".

Settings of [Log Information] tab

Set the following items.



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
Display sequence	Select the log display sequence from one of the following: - Operation Datetime Order - Group + Device + User Order The default value is Operation Datetime Order .
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 can be applied to the output of the information disclosure analysis report. Refer to "[Settings of \[Object Group\] tab](#)".

3. Click the **Print** or **Save File** button.

Note

Do not operate Microsoft(R) Excel in the process of report output

Do not perform the **New** and **Open** operation of Microsoft(R) Excel file in the report output process, as report output may not be performed normally sometimes.

In addition, confirm whether Microsoft(R) Excel was started correctly before the report output. When Microsoft(R) 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

Save the output report to a safe place

The output report may contain personal information and system configuration information. 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.

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)	
Object Group Sheet	Object 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(R) 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

Refer to "[Summary Sheet](#)", "[Detail Sheet](#)", "[Object 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 configuration:

- User ID: systemadmin
- Management Server: 192.168.17.66
- Basic Information tab selected
- Report title (T): Comprehensive Analysis Report
- Created by (N): systemadmin
- Analysis period:
 - Daily report (D): Year 2015, Month 6, Day 3
 - Weekly report (W): Year 2015, Month 5, Day 24. In one week from this day
 - Monthly report (M): Year 2015, Month 4, 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 in each tab.

The settings of each tab will be saved in the 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.

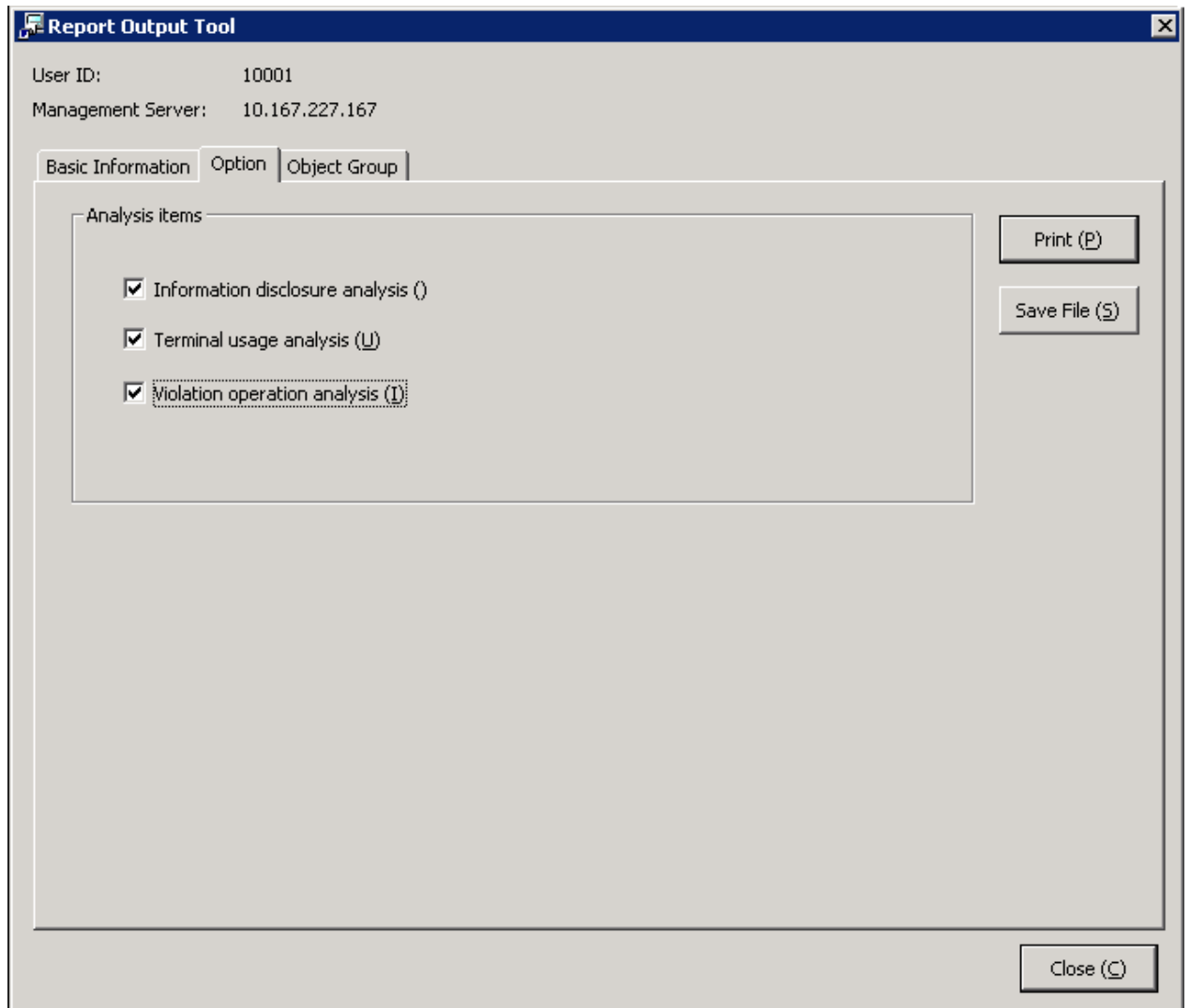
Settings of the [Basic Information] tab

The settings of the basic information tab can be applied to the output of the information disclosure analysis report. Refer to "[Settings of \[Basic Information\] tab](#)".

Settings of the [Option] tab

Select analysis items.

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. Refer to "[Settings of \[Object Group\] tab](#)".

3. Click the **Print** or **Save File** button.

Note

Do not operate Microsoft(R) Excel in the process of report output

Do not perform the **New** and **Open** operation of Microsoft(R) Excel file during the report output process, as the report output may not be performed normally.

In addition, confirm whether Microsoft(R) Excel was started correctly before the report output. When Microsoft(R) 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

Save the output report to a safe place

The output report may contain personal information and system configuration information. 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(R) Excel and service pack being used.

Comprehensive diagnosis sheet

(1) Comprehensive Analysis Report

Object	(2)	Managed Object *View object group sheet
Number of object PCs	(3)	109 Set(s)
Created by	(4)	systemadmin
Created on	(5)	2015/05/13
Analysis period	(6)	2015/03/21 ~2015/04/20

	(7)	
--	-----	--

[Information Disclosure Prevention] (8)

Index Value	6.0 %
-------------	-------

Number of all items	41,696
Number of safe items	38,212
Number of dangerous items	2,484

Order	Group name	File export	File operation	Number of printing operations	Email sending by recipient	FTP operation (upload)	Web operation (upload)	Aggregation
1	Planning Dept.	10	143	356	154	154	356	1,173
2	Development Dept.	29	21	531	2	3	521	1,107
3	Management Dept.	28	210	34	256	256	34	818
4	Sales Dept. 1	1	211	31	190	150	31	614
5	Sales Dept. 2	10	85	134	54	54	134	531

[Terminal Usage Status] (9)

Index Value	11.7 %
-------------	--------

Number of all items	161,087
Number of safe items	142,291
Number of dangerous items	18,796

Order	Group name	Window title with URL obtained	Email sending by recipient	Application startup	Aggregation
1	Planning Dept.	1,045	32	11,084	12,161
2	Development Dept.	1,274	48	429	1,751
3	Management Dept.	1,238	10	109	1,357
4	Sales Dept. 1	648	108	182	938
5	Sales Dept. 2	348	125	125	598

[Violation Status] (10)

Index Value	0.1 %
-------------	-------

Number of all items	202,952
Number of safe items	202,783
Number of dangerous items	169

Order	Group name	Application startup prohibition	Print prohibition	Logon prohibition	PrintScreen key prohibition	Attachment prohibition	Aggregation
1	Planning Dept.	22	12	12	4	5	55
2	Development Dept.	15	12	5	4	2	38
3	Management Dept.	24	0	4	5	1	34
4	Sales Dept. 1	1	15	0	0	1	17
5	Sales Dept. 2	3	0	1	0	12	16

[Diagnosis Comment] (11)
 [Information disclosure analysis] Improved comparing with the last time Improved in the long term.
 [Terminal usage analysis] Improved comparing with the last time Improved in the long term.
 [Violation analysis] Improved comparing with the last time Improved in the long term.

(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, refer to "[Summary Sheet](#)".

Object Group Sheet

The department information that has been analyzed will be output.

(1) Object Group	
(2) No	(3) 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) Object 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 halfwidth characters (256 fullwidth characters) can be displayed in the content of each item in object 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 the 'Report Output Tool' window with the following details:

- User ID:** 10001
- Management Server:** 10.167.143.226
- Basic Information tab:**
 - Report title (T):** Printing Volume Auditing Report
 - Created by (N):** admin
 - Monitoring period:** Year 2012, Month 1, In one month starting from the first day
- Buttons:** Print (P), Save File (S), Close (C)

- User ID: The login user ID.
 - Management Server: IP address or server name 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. Specify up to 64 bytes (can be a combination of fullwidth characters and halfwidth alphanumeric characters and symbols). Initial value: "Printing Volume Auditing report".
Created by	Specify the creator of report. Specify up to 40 bytes (can be a combination of fullwidth characters and

Input Item	Content
	halfwidth alphanumeric characters and symbols). 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 whether to output **List of object** to report.

The settings of this tab can be applied to the output of Information disclosure analysis report. Refer to "[Settings of \[Object Group\] tab](#)".

3. Click the **Print** or **Save File** button.



Note

Do not operate Microsoft(R) Excel in the process of report output

Do not perform the **New** and **Open** operation of the Microsoft(R) Excel file in the report output process, as report output may not be performed normally.

In addition, confirm whether Microsoft(R) Excel was started correctly before the report output. When Microsoft(R) 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

Save the output report to a safe place

The output report may contain personal information and system configuration information. 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.
	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.
Object Group Sheet	Object Group	Output the information of report auditing object group.

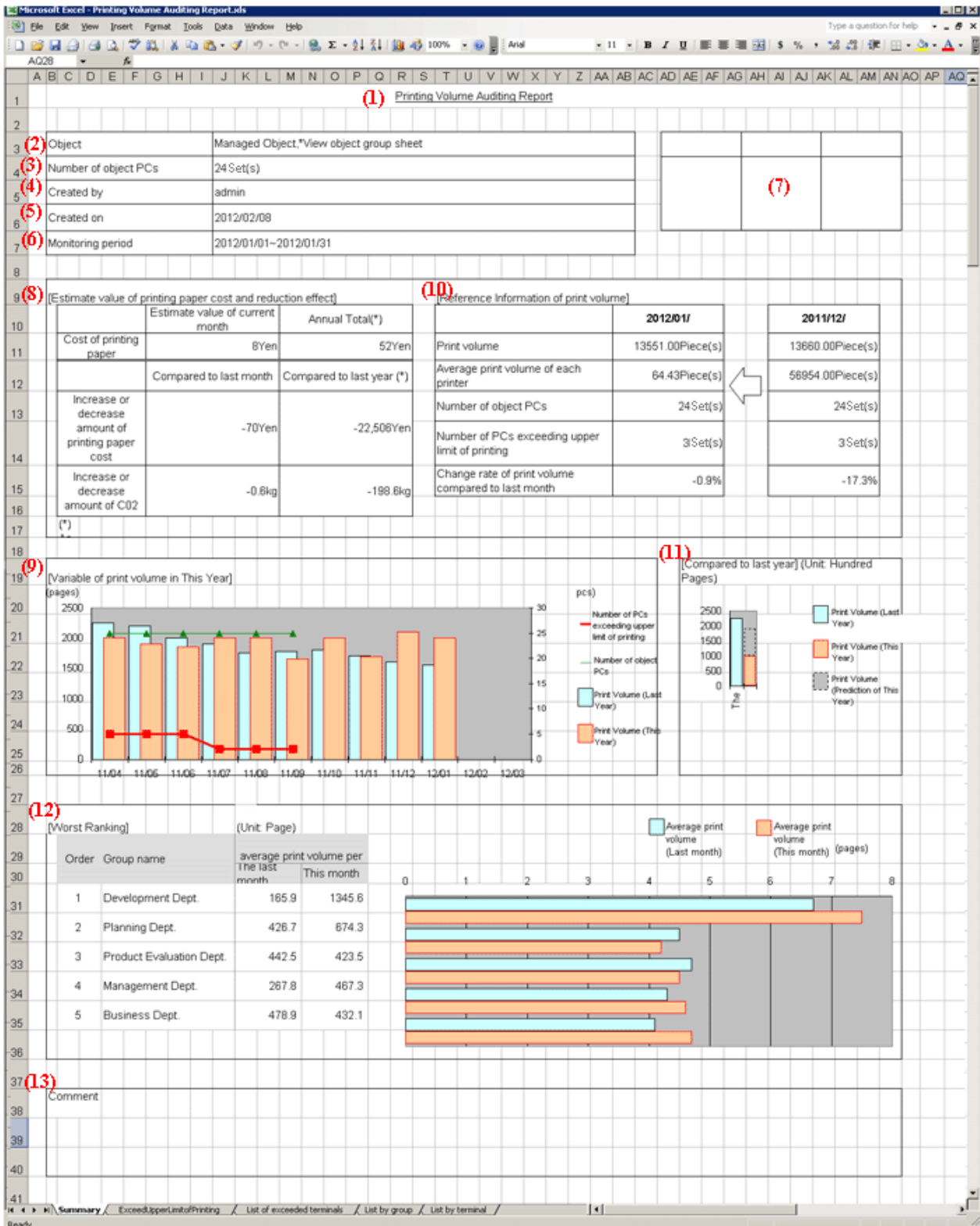
The layouts of the generated report file and printing result may vary depending on the version of Microsoft(R) Excel and service pack being used.

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 the Log Analyzer of each Web Console. Modify the settings in Web Console to modify these values. For details, refer to "[2.7.2.2.4 Set Other Conditions](#)".

Summary Sheet: Summary



(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", 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.

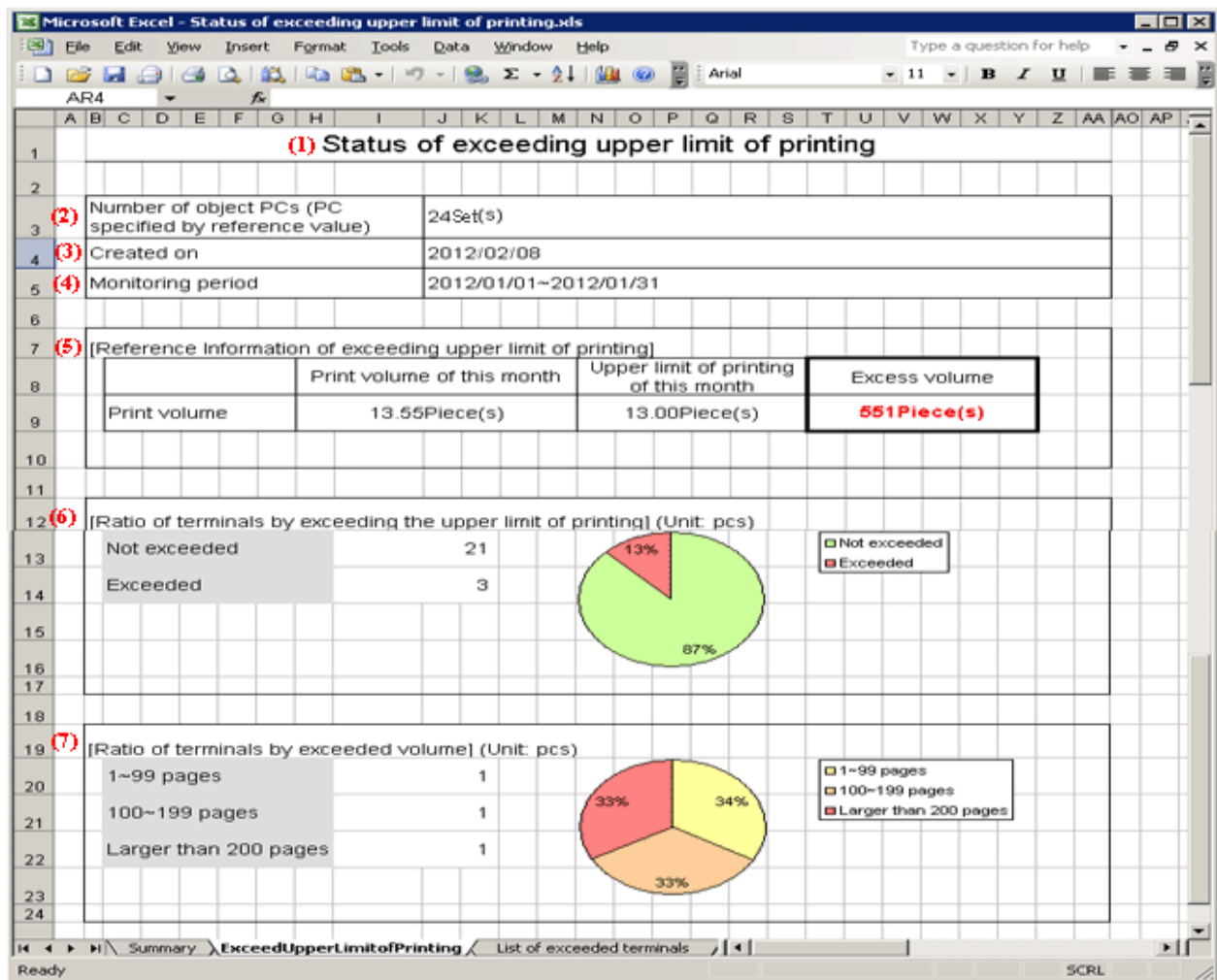
- The predicted value is the value obtained by multiplying the monthly average value of print volume by number of the remaining number of months.

(12) 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.

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, refer to "2.4.1.10 Eco Monitoring".

(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 the 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	1,345	27	186	808
▲	2	Development Dept.	CT010(Lindar)	1195	1000	195	32	224	972
▲	3	Development Dept.	CT011(Green)	595	500	95	16	112	488

(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 the 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.

Daily = (upper limit of printing of this month * (number of the remaining months of this year+1) - print volume of this month) / (number of the remaining days of this year)

Weekly= (upper limit of printing of this month * (number of the remaining months+1) - print volume of this month) / (number of the remaining days of this year) *7

Monthly= (upper limit of printing of this month * (number of the remaining months+1) - print volume of this month) / (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

(1) Print volume Monitor Report [By Group List]							
(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	Root Division	1	344	266.9	1	344	500
2	Operation Dept.	2	1234	493	3	1234	1500
3	Operation Dept./Operation Div. 1	3	1681.7	560.6	3	1682	2000
4	Operation Dept./Operation Div. 2	2	956	478	8	667	1000
5	Development Dept.	2	1245	622.5	2	1245	2000
6	Planning Dept.	5	888	177.6	5	789	1000
7	Management Dept.	2	902	451	2	902	1000
8	Finance Dept.	2	838	419	2	890	1000
9	Product Evaluation Dept.	2	834	417	2	834	1000
10	Business Dept.	2	554	277	2	504	1000

(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

(2) No.	(3) Group name	(4) Computer name	(5) Print volume of this month (pages)	(6) Upper limit of printing of this month (pages)	Object: Managed Object
1	Root Directory	CT00(Tom)	344	500	
2	Operation Dept.	CT002(Pollog)	486	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(Ang)	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)	400	500	
16	Planning Dept.	CT016(Maj)	484	500	
17	Management Dept.	CT017(Frag)	400	500	
18	Management Dept.	CT018(Sckg)	430	500	
19	Finance Dept.	CT019(Bwly)	435	500	
20	Finance Dept.	CT020(Dary)	400	500	
21	Product Evaluation Dept.	CT021(Ang)	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 (-).

Object Group Sheet: Object Group

Created on:2012/02/08		
(1) Print volume Monitor Report [Object Group]		
(2) No.	(3) Group name	Object Managed Object
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 object 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. Do not register the batch file that uses batch commands or batch commands more than once in Task Schedule.



Note

In Windows Vista(R), Windows(R) 7 and Windows(R) 8

In the environment of Windows Vista(R), Windows(R) 7 and Windows(R) 8, when operating in the command prompt, open the command prompt through **Execute as Administrator**.

The procedure is as follows:

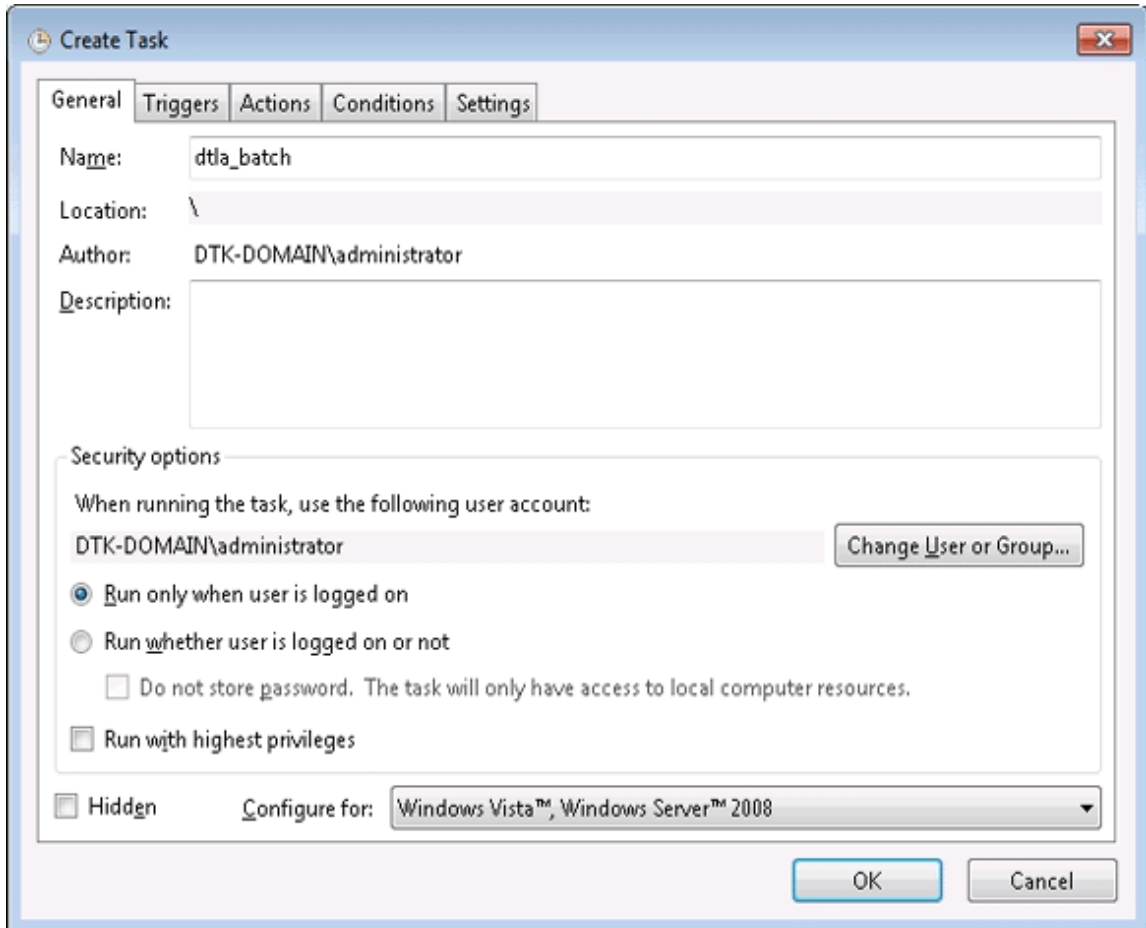
1. Record report output commands in batch file according to the output report.
For details of report output commands, refer to "DTLA_REPORT_BATCH.EXE (report output)" in *Systemwalker Desktop Keeper Reference Manual*.
 - Specify command name or output target folder with full path.
 - When space is contained in the path, enclose it with " (double quotes).
 - When outputting multiple reports, arrange and record commands.

Batch file description example:

```
"dtkl nstal /Dir\LogAnalyzer\ReportTool\DTLA_report_batch.exe" -t leak -s monthly -f c:\work  
"dtkl nstal /Dir\LogAnalyzer\ReportTool\DTLA_report_batch.exe" -t cmuse -s weekly -f c:\work  
"dtkl nstal /Dir\LogAnalyzer\ReportTool\DTLA_report_batch.exe" -t summary -s daily -f c:\work
```

2. Register the batch files to Task Schedule.

a. Start Task Scheduler and select the **General** tab.



b. Set the following information.

- **When running the task, use the following user account:** Specify the user account of Windows. Specify the logon user account when setting batch users.
- **Run only when user is logged on:** This item must be selected. If not, batch commands may not run normally.
- **Run with highest privileges:** Select the check box.

c. 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

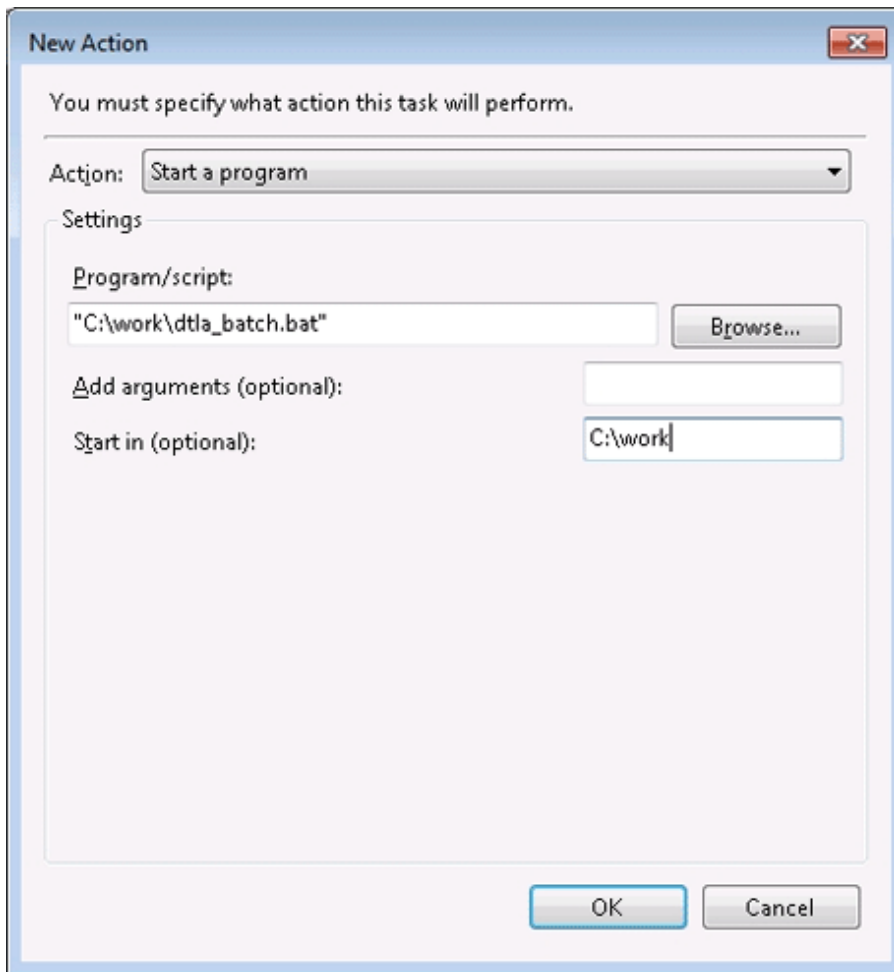
Expire: 2/11/2012 9:21:05 PM Synchronize across time zones

Enabled

OK Cancel

d. Set the start schedule for batch command files and click the **OK** button.

e. Select the **Actions** tab and click the **New** button.



f. 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, enclose it with " (double quotes).
- **Start in (optional):** Specify the folder that contains execution files with full path. Do not enclose the path with " (double quotes).

g. 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.



Notes if updates have been applied

If updates have been applied, check the instruction(s) attached to the updates and ensure that no issues should be noted before changing the operating environment, and perform the tasks accordingly.

To stop services during the operating environment change, you must exit all Management Consoles

During connection to the Management Console, the Management Server or Master Management Server determines whether the source address for the connection is correct.

For this reason, you must exit all Management Consoles before restarting the services of the Management Server or Master Management Server, and then reconnect afterwards.

Connection will fail if you attempt to connect to the Management Server without exiting the Management Console. If this happens, exit the Management Console and reconnect.

Exiting the Management Console will take the amount of time specified in the setting below:

Server settings tool > Management Server settings > Timeout value of communication between servers

7.1 Change Import Method of Configuration Information

When changing to import by linking with Active Directory from manual creation in Management Console

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. 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 shall be the same.

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).

Encoding for I/O files

ShiftJIS UTF-8

3. Select **Execute Active Directory linkage** in **Active Directory Linkage**.
Refer to "Perform System Settings" of *Systemwalker Desktop Keeper Installation Guide* for details on other setting items.
4. Click the **Set** button.

- Click the **Active Directory linkage settings** button of the **Server Settings Tool** window.

The **Active Directory Linkage Settings** window is displayed

Set domain controller viewed by Management Server.

Domain list

Computer name	Domain name	NetBIOS ...	Perform L...	User ID	Update da...	Registration date a...
ADSERVER	fujitsu.com	ADSV	Perform	administrator	2015/05/13 17:32:51	2015/05/13 17:32:51

Computer name:

Domain name: NetBIOS:

Execute linkage:

User Name:

Password (first entry): Already set

Password (re-entry):

Number of registrations 1 items (max 1 items)

- Set the linked Active Directory server information and click the **Add** button.
Refer to "Linking with Active Directory" of *Systemwalker Desktop Keeper Installation Guide* for details on setting items.
- 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, refer to "[2.5.1 Import Information from Active Directory](#)".
The configuration information is imported.
Move the existing group tree to the Local group.
- 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, refer to "[3.4.2 Modify User Policy](#)".
- Start the service.

When import through linking with Active Directory is cancelled

- Stop the service of the server.
- Start the Server Settings Tool and click the **System settings** button.
The **System Settings** window is displayed.
- Select the **Not execute Active Directory linkage** and click the **Set** button in **Active Directory Linkage**.
- 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.

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 on command, 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.

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 shall be the same.

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	<input checked="" type="radio"/> Use	<input type="radio"/> Not use
- Owner	<input checked="" type="radio"/> Use	<input type="radio"/> Not use
- OS Type	<input checked="" type="radio"/> Use	<input type="radio"/> 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).

Encoding for I/O files

ShiftJIS UTF-8

- 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.

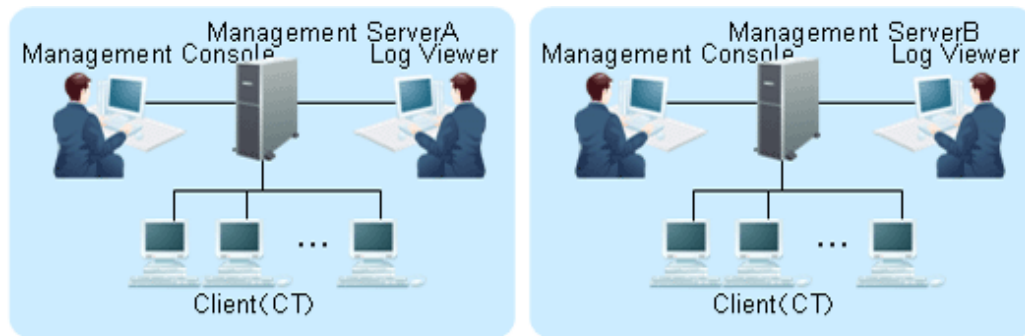
The transferred user information will be managed in the Management Console connected to each Management Server.

7.3 Change System Structure from 2-level to 3-level

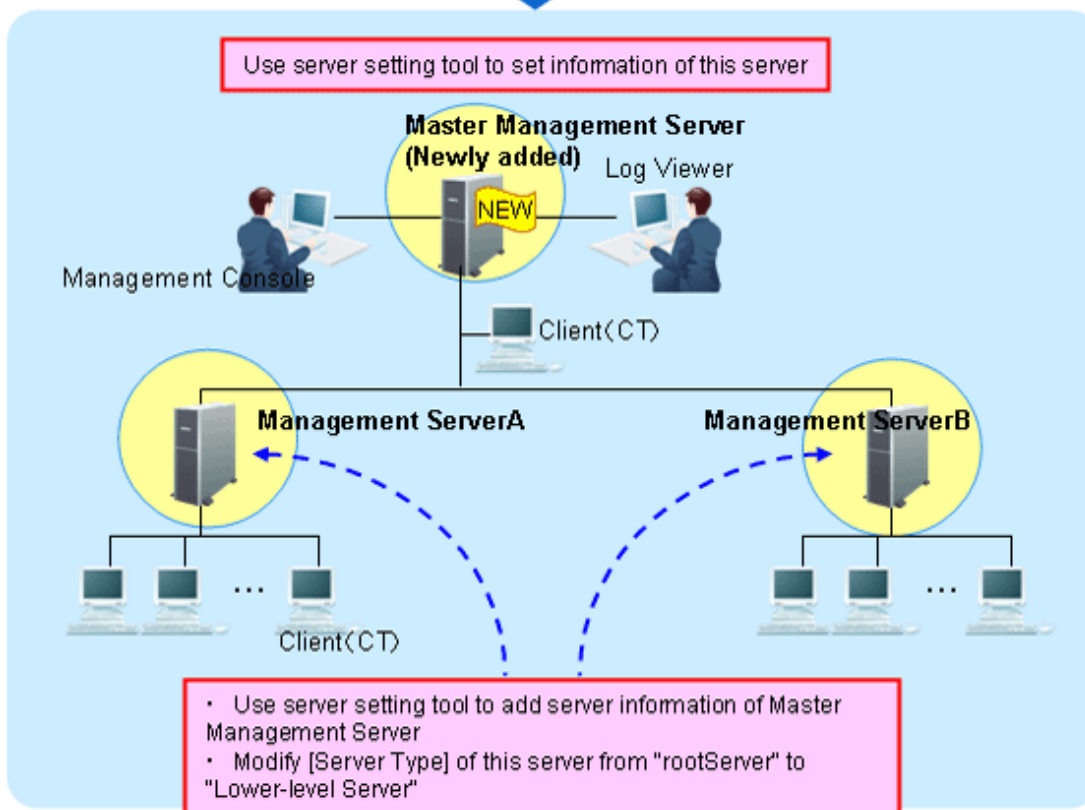
This section describes the following two methods for changing the system structure from 2-level to 3-level:

- 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, 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. For Link with Active Directory and centralized management of user information, match the settings in **Set data linkage method** in the **System settings** window for the Server Settings Tool on the Management Server with the settings on the Master Management Server.

- Set the following information in the **Server Information Settings** window of the Server Settings Tool on the Management Server.

Perform settings related to server.
 For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
 For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
 Lowercases of node name will be changed to uppercases before registration.
 In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

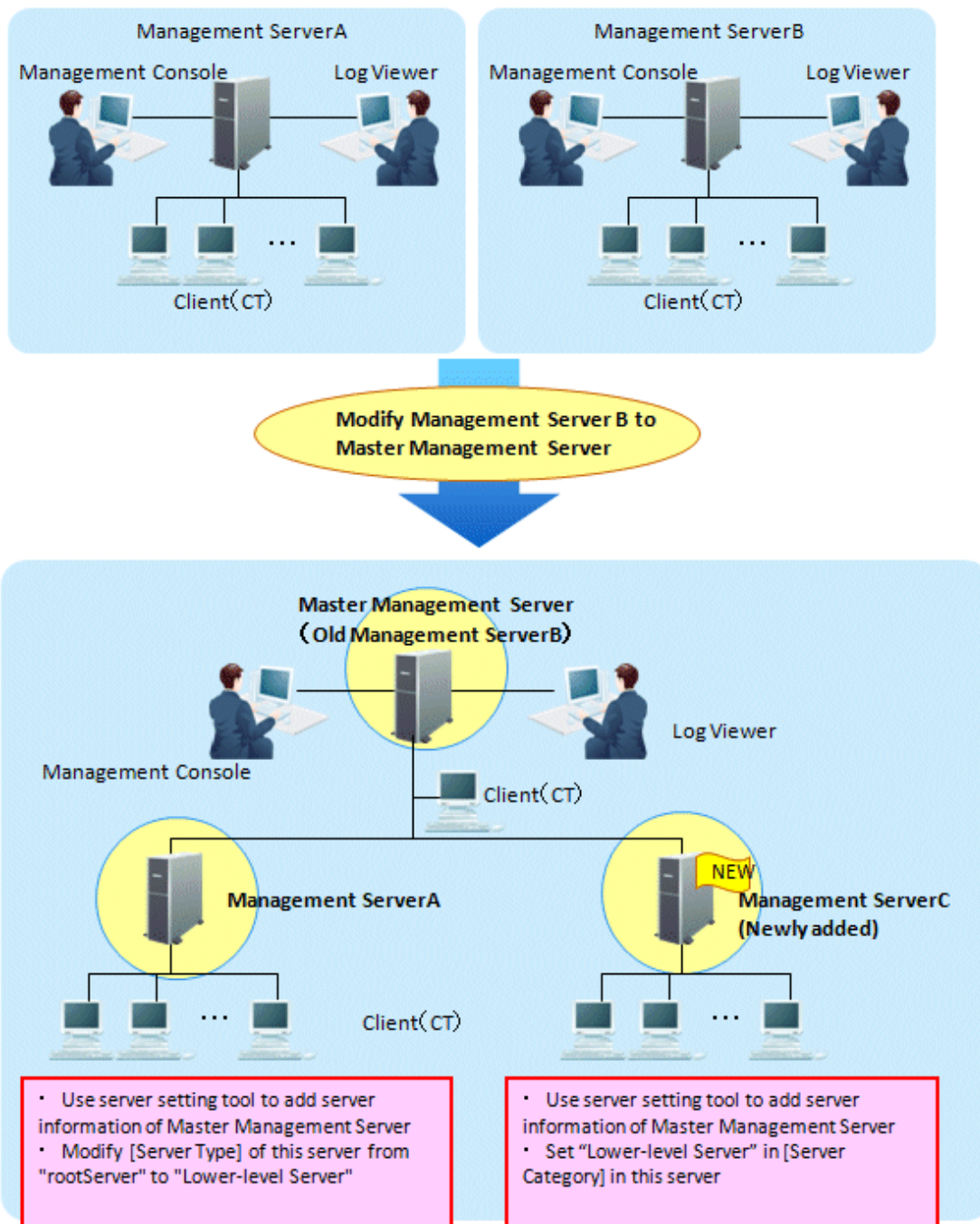
Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...
Own node	V70A34VJ6U001	V70A34VJ6U001	133.162.24.230	root server	2015/05/17 14:10:14	2015/05/13 17:18:04

Node type: Node name: Server IP address or server name:
 Computer name: Server classification:

Number of regist 1 items (maximum 255 items)

- Change the **Server classification** of this server from "Root Server" to "Sub-Level Server".
 - Add the information of the Master Management Server.
 For details, refer to "Set Server Information" of *Systemwalker Desktop Keeper Installation Guide*.
- Start the level control service and server service of the Master Management Server.
 - 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.
 - When the client (CT) directly under the Master Management Server is connected, any of the following operations can be performed:
 - Install a new client (CT) in the PC.
 Refer to "Install client (CT)" of *Systemwalker Desktop Keeper Installation Guide* for installation method.
 - Change the existing client (CT) environment.
 For information on how to do so, refer to "[7.7.1 Change Management Server/Master Management Server To Be Connected](#)".
 - 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, 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, 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 Server**. 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.
2. 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, refer to "Set Server Information" of *Systemwalker Desktop Keeper Installation Guide*.

3. For Link with Active Directory and centralized management of user information, match the settings in **Set data linkage method** in the **System settings** window for the Server Settings Tool on the Management Server with the settings on the Master Management Server.
4. Construct a new Management Server C.
For information on how to do so, refer to "Installation" of *Systemwalker Desktop Keeper Installation Guide*.
Set the following information in the **Server Information Settings** window of the Server Settings Tool.

Perform settings related to server.
For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
Lowercases of node name will be changed to uppercases before registration.
In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...

Node type: Node name: Server IP address or server name:
Computer name: Server classification:

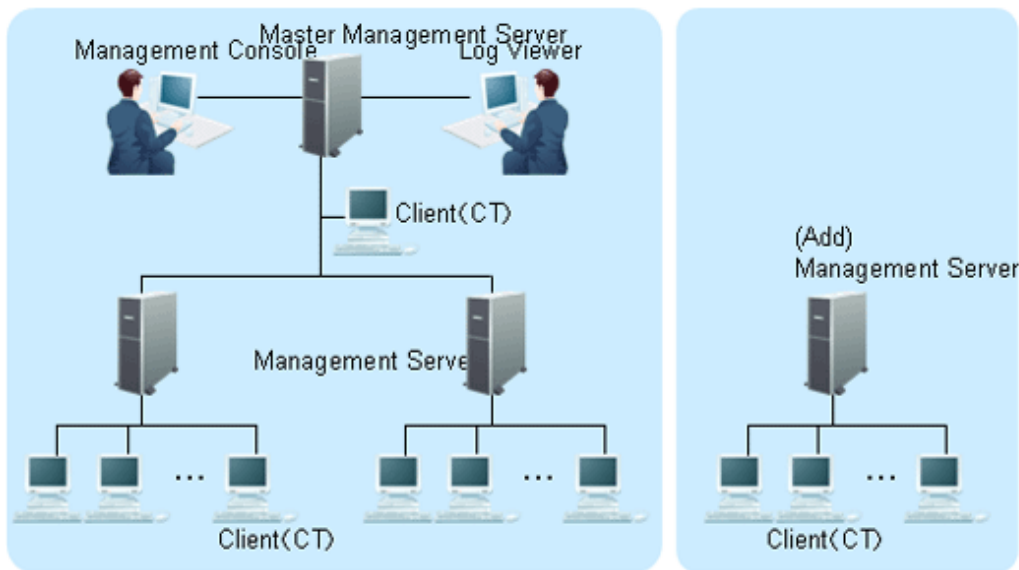
Number of regist 0 items (maximum 255 items)

- Add the information of the Master Management Server.
For details on how to do so, refer to "Set Server Information" of *Systemwalker Desktop Keeper Installation Guide*.
 - Set the **Server classification** of this server to "Sub-Level Server".
5. Start the level control service and server service of the Master Management Server.
 6. 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.
 7. When the client (CT) directly under the Master Management Server is connected, any of the following operations can be performed:
 - Install a new client (CT) in the PC.
For information on how to do so, refer to "Install client (CT)" of *Systemwalker Desktop Keeper Installation Guide*.
 - Change the existing client (CT) environment.
For information on how to do so, refer to "7.7.1 Change Management Server/Master Management Server To Be Connected".

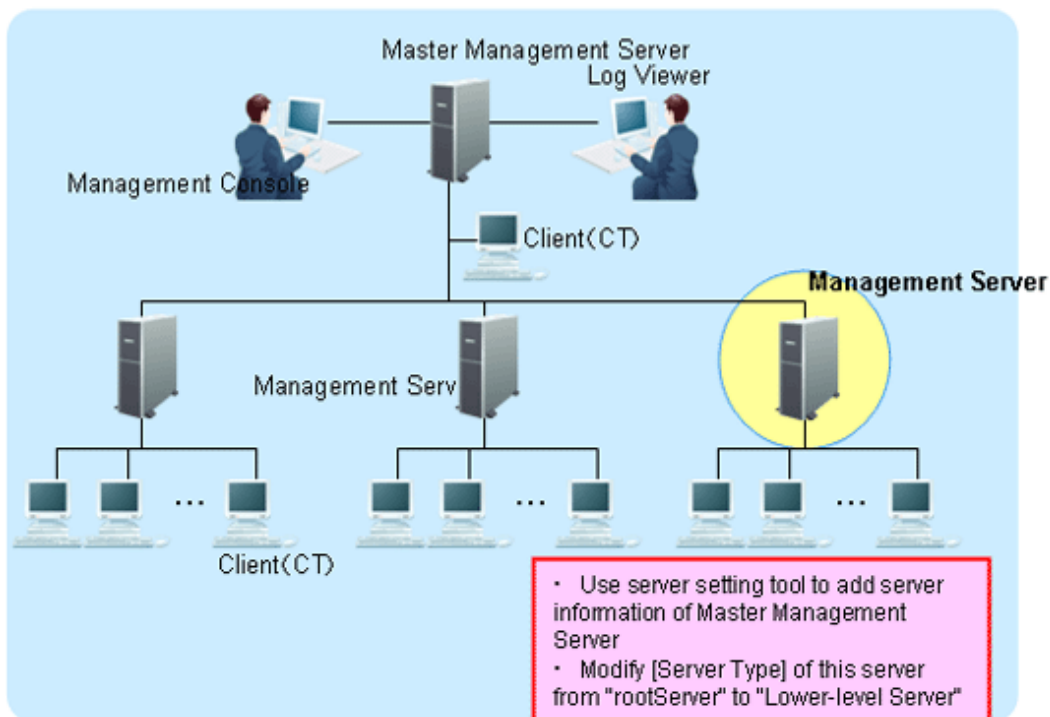
7.4 Add/Delete Management Server in 3-level System Structure

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.

Refer to "DTKTBLCV.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.
3. For Link with Active Directory and centralized management of user information, match the settings in **Set data linkage method** in the **System settings** window for the Server Settings Tool on the Management Server with the settings on the Master Management Server.

- Set the following information in the **Server Information Settings** window of the Server Settings Tool in the added Management Server.

Perform settings related to server.
 For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
 For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
 Lowercases of node name will be changed to uppercases before registration.
 In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...
Own node	V70A34VJ6U001	V70A34VJ6U001	133.162.24.230	root server	2015/05/17 14:14:11	2015/05/13 17:18:04

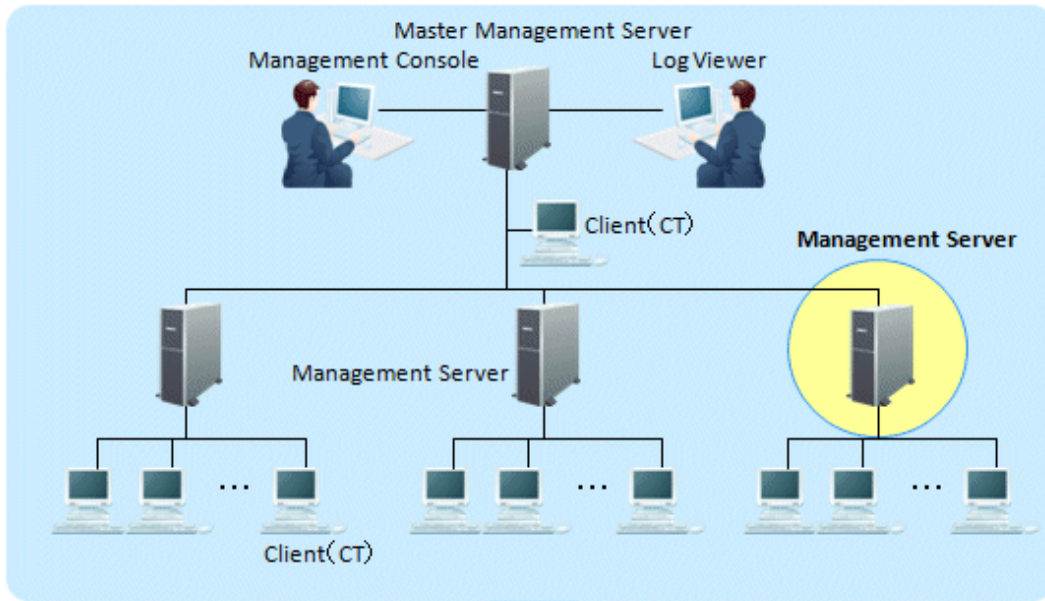
Node type: Node name: Server IP address or server name:
 Computer name: Server classification:

Number of regist 1 items (maximum 255 items)

- Modify the **Server classification** of this server from "Root Server" to "Sub-Level Server".
 - Add the information of the Master Management Server.
 For details on how to do so, 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.

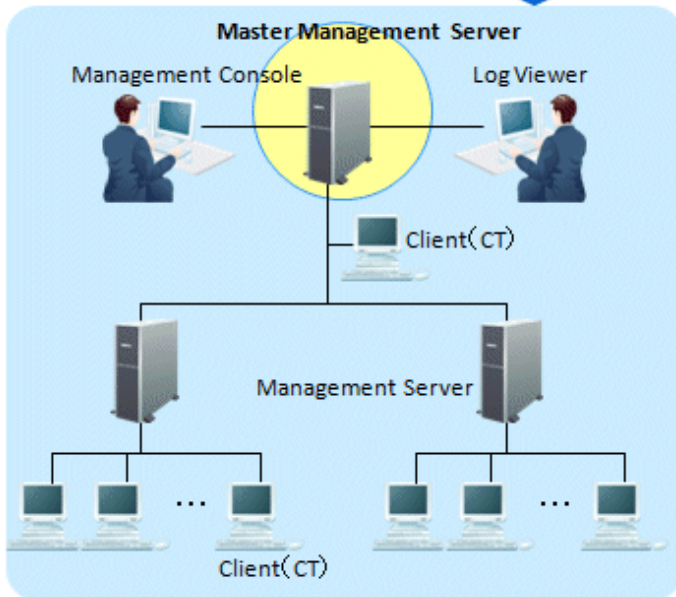
Delete Management Server

When the server information of the Master Management Server is deleted in the Management Server, 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, 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.

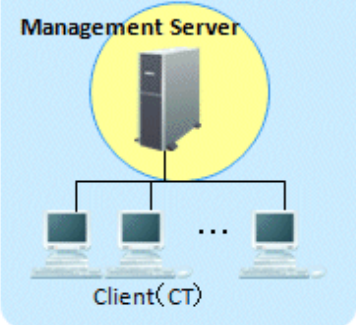


Use server setting tool, delete the server information of Management Server

Separate Management Server

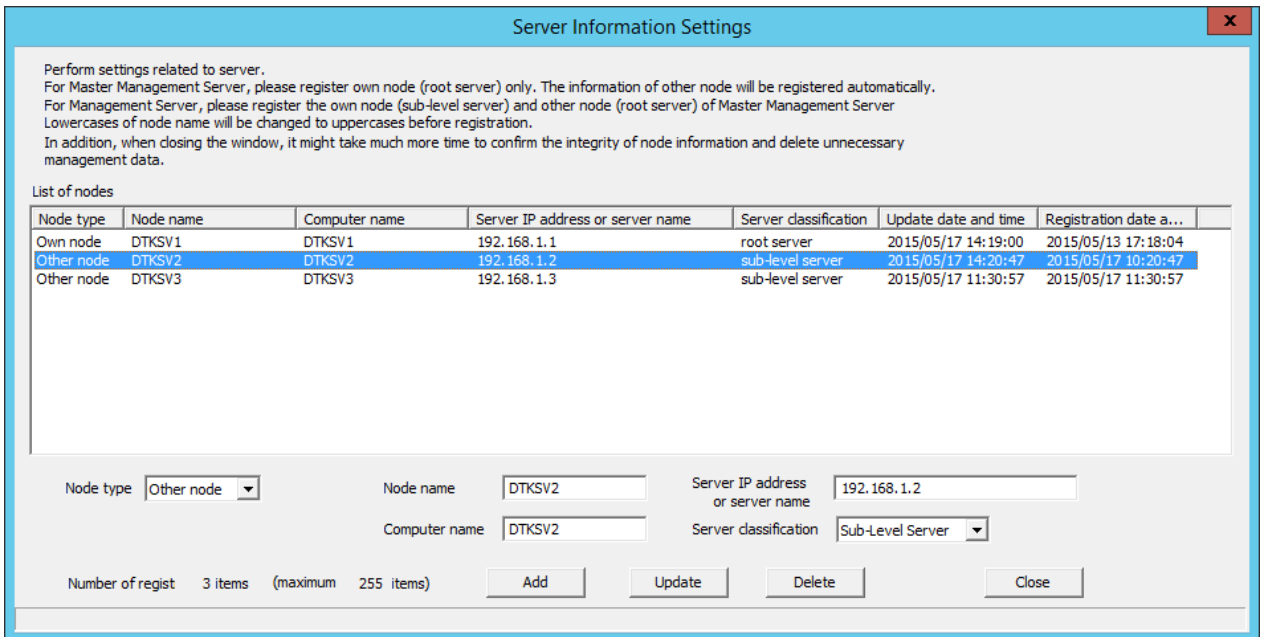


Use server setting tool, delete the server information of Master Management Server

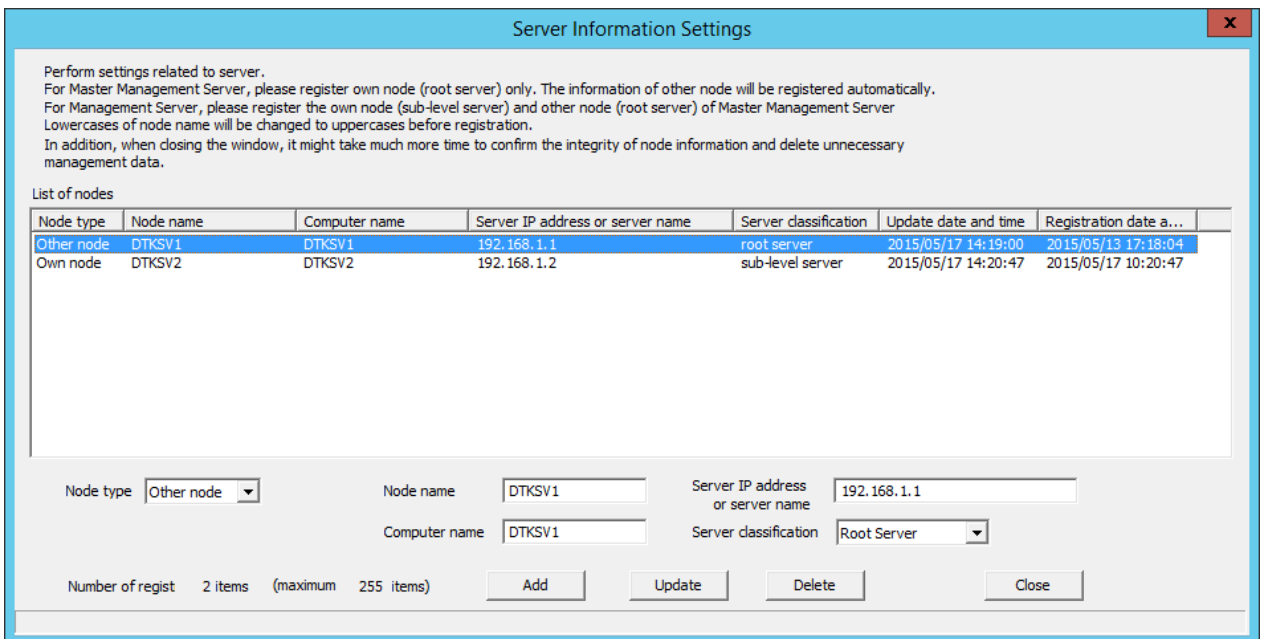


1. Stop the level control service and server service of the Master Management Server and separated Management Server.

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

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.

Refer to "[7.5.2 Register USB device](#)" and "[7.5.3 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, CD/DVD, portable devices, and imaging 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, refer to "[7.5.2 Register USB device](#)" and "[7.5.4 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, refer to "[7.5.5 Export registered USB device information as CSV file](#)" and "[7.5.6 Modify the registered USB device information](#)".



Point

Conditions of Individual Identification Function of USB Device can be set.

When the **File export/read** is set to the following patterns, the **Individual Identification Function of USB Device** can be set.

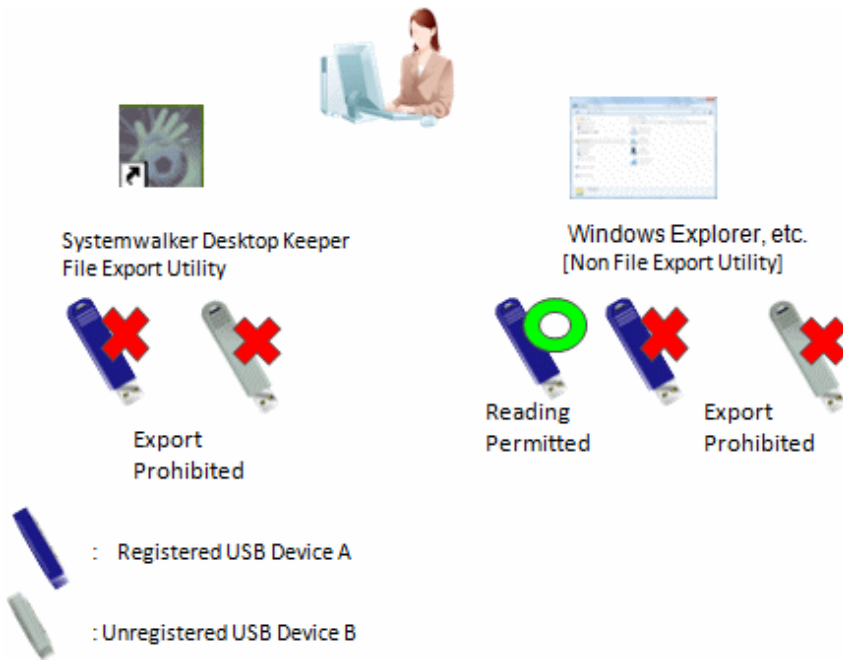
- Pattern 1
 - When **Export using File Export Utility** is set to **Yes**
 - Pattern 2
 - When **File Access Control** is set to **Yes**
 - When **Read Prohibition** is set to **Removable**, Or
 - When **Specify Drive Type** is set to **Removable**
-

7.5.1 Operation example

This describes the operation example when the file export and reading are performed using only the USB devices that are permitted by the administrator.

Operation 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, refer to "[Policy setting of operation example 1](#)".

Operation 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.



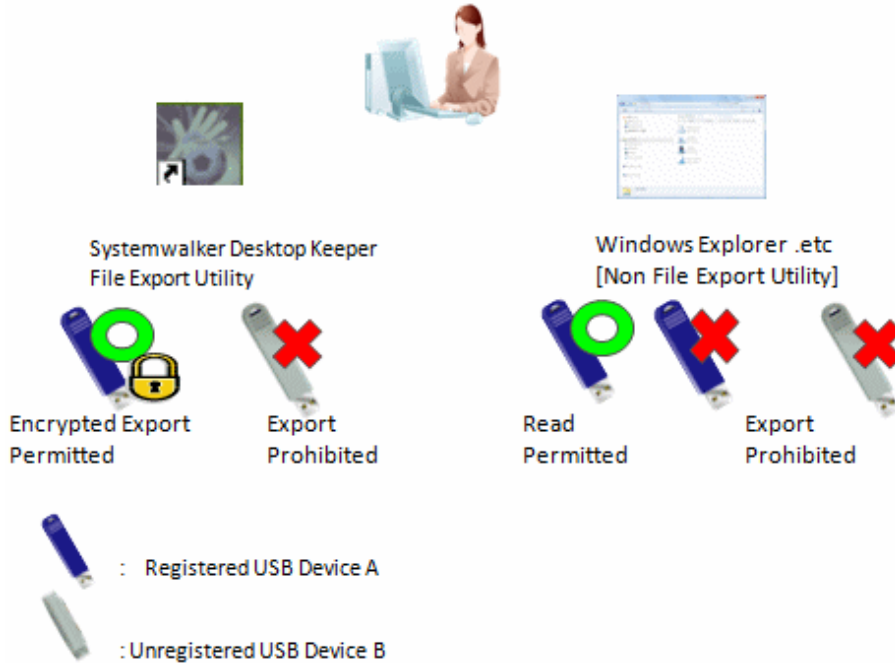
This application can be achieved through the following settings.

File export is allowed only after encryption using the Export Utility. Exporting and reading using Explorer (Not Export Utility) are prohibited.

Refer to "[Policy setting of operation example 2](#)" for policy setting.

Operation 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.

Refer to "[Policy setting of operation example 3](#)" for policy setting.

Operation example 4: Exporting freely using Windows 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 operation 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, set File Export Utility and export files through File Export Utility.



This application can be achieved through the following settings.

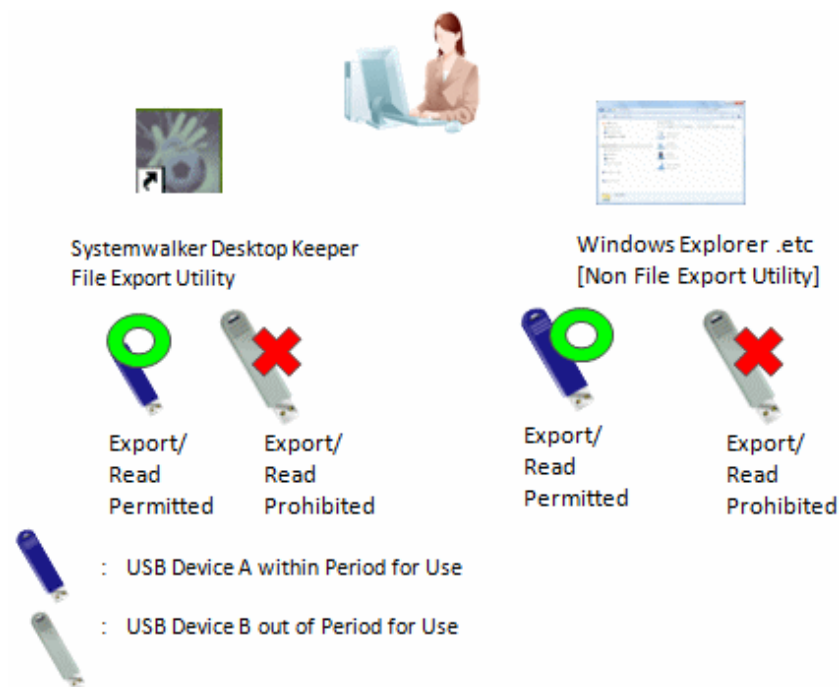
Export and reading by Explorer (Not Export Utility) are permitted.

*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.

Refer to "[Policy setting of operation example 4](#)" for policy setting.

Operation 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.



This application can be achieved through the following settings.

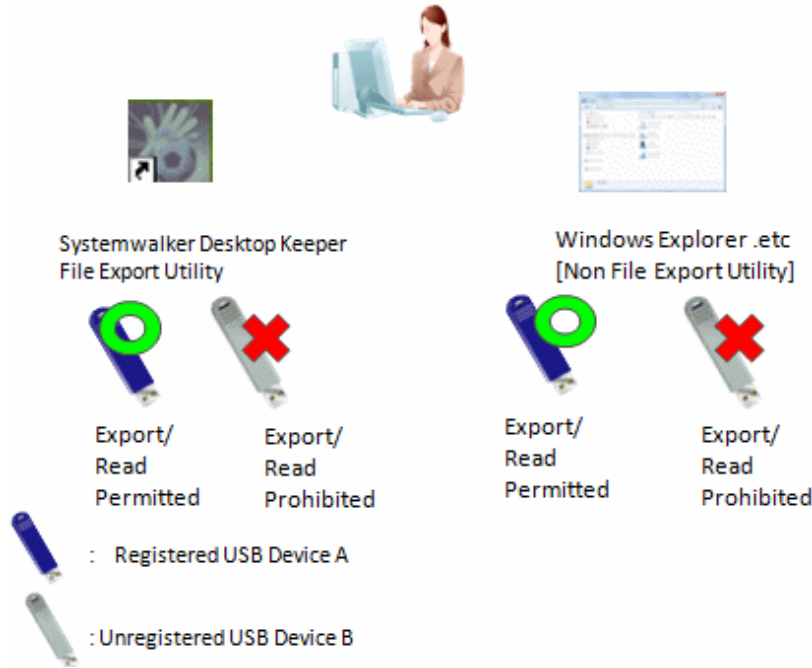
Set the period for use of the USB device, and permit exporting and reading.

Note: It can also be limited to use by File Export Utility only or set to read only.

For policy setting, refer to "[Policy setting of operation example 5](#)".

Operation 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.



This application can be achieved through the following settings.

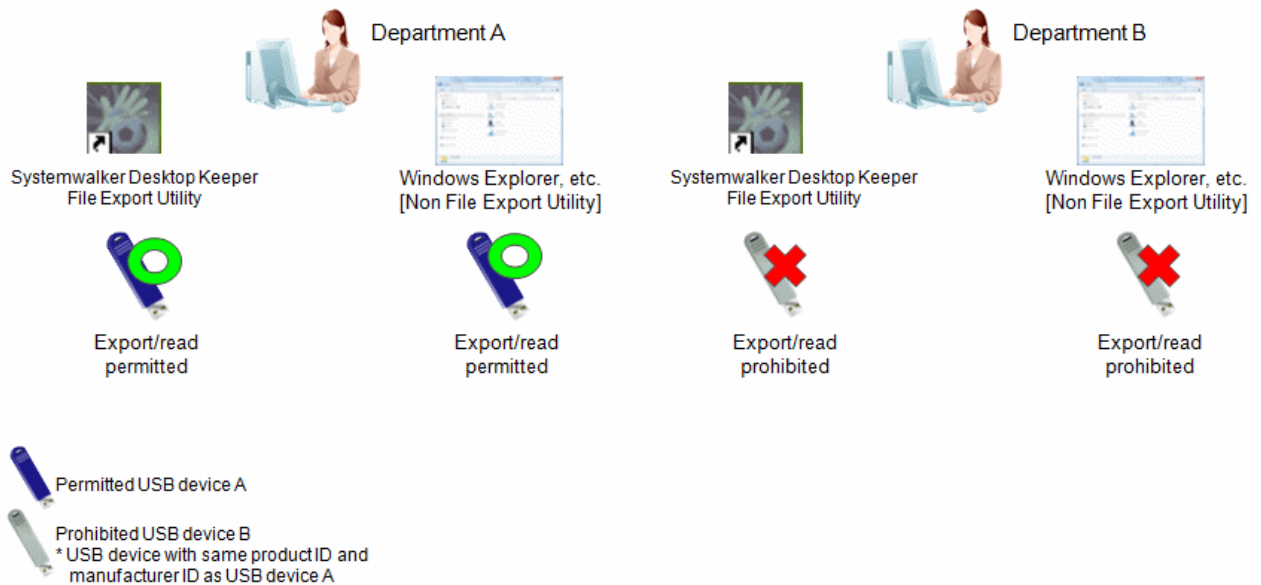
Permit the use of all USB devices registered on the Management Server/ Master Management Server, and permit exporting and reading.

It can also be limited to use by File Export Utility only or set to read only.

Refer to "[Policy setting of operation example 6](#)" for policy setting.

Operation example 7: Prohibit only some of a large number of USB devices (USB devices with the same product ID and manufacturer ID)

This example assumes that the USB devices have the same product ID and manufacturer ID, and that only some of them should be prohibited for use by a certain department.



This operation can be achieved through the following settings.

In the **USB Device Registration** window, register "USB device A" in **Product Match** and "USB device B" as **Not Available**. When the registration is performed, the product ID and manufacturer ID of "USB device A" and "USB device B" will become the same. For the group policy for "Section A", permit the use, export, and read of all USB devices registered in the Management Server. For "Section B", specify "USB device B" as its group policy.

Refer to "[Policy setting of operation example 7](#)" for details on policy settings.

Operation example 8: Enabling only the permitted digital cameras

This example assumes that the USB devices have the same product ID and manufacturer ID, and only some of them should be prohibited for use by a certain department.

In this example, the use of digital cameras is prohibited, in addition to the operation example 4. This will enable only permitted digital cameras to be used, and other digital cameras, scanners, digital voice recorders or similar will be prohibited.

Note that settings for read/write permission are not available for portable devices or imaging devices. Also, there is no operation exclusively designed for Export Utility.



This operation can be achieved with the following settings.

Exporting and reading using Windows Explorer or similar (other than Export Utility) will also be authorized. Settings related to Export Utility are optional.

Refer to "[Policy setting of operation example 8](#)" for details on policy settings.

7.5.2 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.
Portable device/imaging device	Identify the device itself as the USB device that can be registered and the inserted memory media cannot be identified separately.
USB DVD/CD-R/RW Device	Identify the device itself as the USB device that can be registered and the inserted DVD/CD media cannot be identified separately.

USB devices can be registered using different identification methods.

For example, a USB device can be registered using **Complete Match** and **Product Match**.

The following identification methods can be used for USB device registration:

- **Complete Match** and **Product Match**
- **Complete Match** and **Not Available**
- **Serial No. Match** and **Product Match**
- **Serial No. Match** and **Not Available**
- **Product Match** and **Not Available**

To determine the availability of USB devices in the Management Server, check if USB devices are registered in the following order of priority:

Complete Match -> Serial No. Match -> Product Match -> Not Available

If it is determined that USB devices were registered using multiple identification methods, the date of the last connection, name of the last user, and name of the last computer that used will always be updated for all matching USB devices.

Additionally, if the **Deadline of USB Device Use** settings are configured, the deadline for USB device use will be configured according to the rule in the table below:

USB device registration method	Expiry status of USB device use	USB device whose deadline for use will be updated
Registration using Complete Match and Product Match	If the deadline for USB devices registered using Complete Match is expired.	USB devices in Product Match will be updated.
	If the deadline for USB devices registered using Product Match is expired.	USB devices in Complete Match and Product Match will be updated.
	If neither deadline is expired.	USB devices in Complete Match and Product Match will be updated.
Registration using Serial No. Match and Product Match	If the deadline for USB devices registered using Serial No. Match is expired.	USB devices in Product Match will be updated.
	If the deadline for USB devices registered using Product Match is expired.	USB devices in Serial No. Match and Product Match will be updated.
	If neither deadline is expired.	USB devices in Serial No. Match and Product Match will be updated.
Registration using Product Match and Not Available (*1)	If the deadline for USB devices registered using Product Match is expired.	Deadline will not be updated.
	If the deadline for USB devices registered using Not Available is expired.	USB devices in Product Match and Not Available will be updated.
	If neither deadline is expired.	USB devices in Product Match and Not Available will be updated.

*1: Same as registration using **Complete Match** and **Not Available** or **Serial No. Match** and **Not Available**. Refer to the columns "Expiry status of USB device use" and "USB device whose deadline for use will be updated" for **Complete Match** or **Serial No. Match** for the description for **Product Match**.

The device information registered can be distributed as the CT policy or user policy.

Menu bar in the USB device registration window

This section describes the menu bar in the **USB device registration** window.

Menu bar		Feature overview
File	Close	Closes the window.
Operation Settings	USB Device Operation Settings	Configures the USB device operation settings.
Link with CSV	Import Settings Content	Displays the Specify a File for Importing USB Device Information window. Use this option to migrate the USB device information to another Management Server.
	Export Settings Content	Displays the Specify a File for Exporting USB Device Information window. Use this option to configure and export the CSV export conditions for the USB device information.

Configuring the USB device operation settings

Follow the procedure below to configure the USB device operation settings.

1. Start the **Management Console**.

2. Click **Operation Settings > USB Device Registration**.

The **USB Device Registration** window is displayed.

3. Click **Operation Settings > USB Device Operation Settings**.

The **USB Device Operation Settings** window is displayed.

Item name	Description		
Set Deadline of USB Device Use	Deadline for USB device use.		
<table border="1"> <tr> <td data-bbox="261 277 304 322"></td> <td data-bbox="304 277 647 322">Not set (default)</td> </tr> </table>		Not set (default)	Sets that USB devices can be used any time.
	Not set (default)		
<table border="1"> <tr> <td data-bbox="261 322 304 501"></td> <td data-bbox="304 322 647 501">Set</td> </tr> </table>		Set	Sets the deadline until which USB devices can be used. Specify an extension period (in days) after the deadline for USB device use is expired. A value from 1 to 999 can be specified.
	Set		
<table border="1"> <tr> <td data-bbox="261 501 304 712"></td> <td data-bbox="304 501 647 712">Period for use will be reset automatically by default during USB device connection</td> </tr> </table>		Period for use will be reset automatically by default during USB device connection	Specify whether to automatically extend the deadline for USB device use when it is expired. The number of days specified in Set > Initial Value will be added as the extended period. The deadline set for use can be extended by selecting this item and then using USB devices.
	Period for use will be reset automatically by default during USB device connection		

4. Click **Set**.

 **Note**

Notes on the timing in which the deadline for USB device use is updated

The deadline for use is reset when communication with the Management Server is established. If communication with the Management Server cannot be established, the deadline will be reset the next time communication is established.

 **Point**

Device use deadline can be batch updated.

Follow the procedure below to batch update USB device deadlines:

1. In **Set Deadline of USB Device Use**, select **Not set**, and then select **Set**.
The device use deadline will be cleared in batch.
2. In **Set Deadline of USB Device Use**, select **Set** and enter an initial value, and then click **Set**.

Register

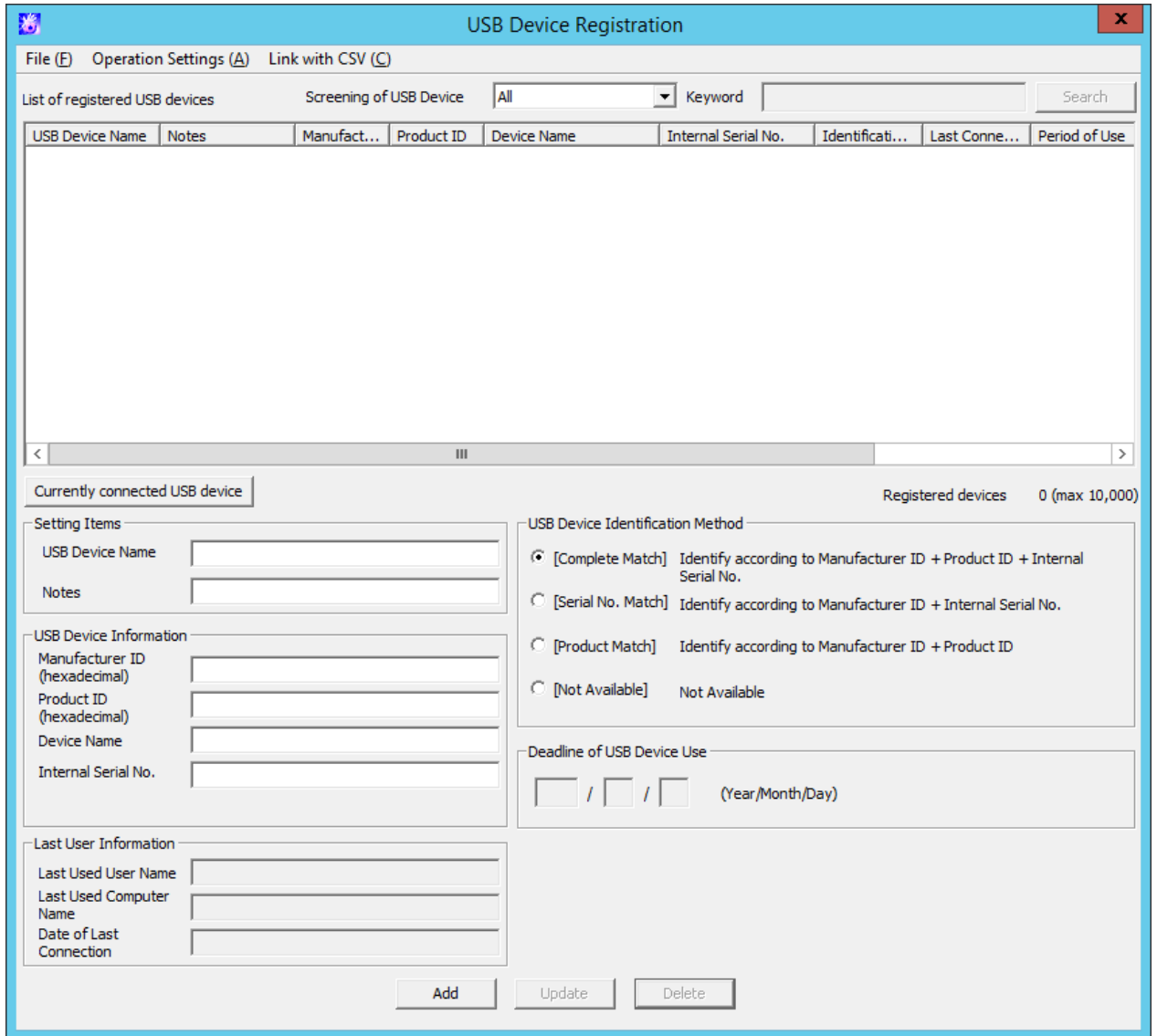
Register one by one in the **Register USB Device** window. One USB device will be registered as one item.

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
Screening of USB Device	<p>Screen the USB devices displayed in the List of registered USB devices. The following items can be selected:</p> <ul style="list-style-type: none"> - Within period for use Display the USB devices within period for use. This can be used when the Settings of Period for Using USB Device is performed. - 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. - All Display all USB devices.

Item Name	Description
	<ul style="list-style-type: none"> - USB device name Search the character string entered in Keyword with partially match and display the USB device. - Manufacturer ID Search the character string entered in Keyword with complete match and display the USB device. Enter the keyword in hexadecimal digit. - Product ID Search the character string entered in Keyword with complete match and display the USB device. Enter the Keywords in hexadecimal digit. - Device name Display the character string input in Keyword with partially match. - Internal serial number Display the character string input in Keyword with partially match. - 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"> - Complete match - Product match - Serial number match - Not available - Last used user name Display the character string entered in Keyword with partially match. - Last used computer name Display the character string entered in Keyword with partially match. - Notes Display the character string entered in Keyword with partially match.
Keyword	Specify the search condition of displayed USB device. Up to 128 halfwidth and fullwidth characters can be specified.
Search	Perform the USB device search according to the conditions specified in USB Device Screening and Keyword .
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"> - USB device name Display the device name of USB device. - Notes Display the notes of USB device. - Manufacturer ID Display the manufacturer ID of USB device.

Item Name		Description
		<ul style="list-style-type: none"> - Product ID Display the product ID of USB device. - Device name Display the device name of USB device. - Internal serial number Display the internal serial number of USB device. - Identification method Display the identification method of USB device. - Last connection date Display the date of last used USB device. - Period for use Display the period for use of permitted USB device of use. - Last used user name Display the user name that uses USB device at last. - Last used computer name Display the computer name that uses USB device at last.
Currently connected USB device		Displays the USB Device Registration - Currently Connected USB Devices window , where the USB device can be selected from a list of USB devices connected to the PC.
Setting Item	USB Device Name	<p>Up to 80 single-byte characters (40 double-byte characters) can be entered. However, the following characters cannot be entered:</p> <ul style="list-style-type: none"> - Control code - 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.) <p>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:</p> <ul style="list-style-type: none"> - Control code
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, enter the following items:</p> <ul style="list-style-type: none"> - Manufacturer ID Four hexadecimal digits can be entered. - Product ID Four hexadecimal digits can be entered. - Device name Up to 80 single-byte characters (40 double-byte characters) can be entered. However, the following characters cannot be entered. <ul style="list-style-type: none"> - Control code - Internal serial number Up to 64 single-byte characters (32 double-byte characters) can be entered.

Item Name		Description
Last User Information	Last Used User Name Last Used Computer Name Date of Last Connection	Display the information of the last user of USB device.
USB Device Identification Method		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 USB Device Identification Method 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 No. match	Identify according to manufacturer ID + internal serial number. In USB Device Identification Method , 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"> - Though it can be used at any time, only registration is implemented at present. - It becomes idle resource temporarily without any user. - The corresponding USB device is lost. In the List of registered USB Devices , all items of this line will be displayed in gray.
Deadline of USB Device Use		When Set Deadline of USB Device Use is selected in the USB Device Operation Settings , set the period for use of the USB device. Only the single-byte digits can be entered, and the input scope is as follow. <ul style="list-style-type: none"> - Year: 2000-2037 - Month: 1-12 - Day: 1-31
Add		Register a USB device. Up to 10,000 devices can be registered.
Update		Update USB device information.
Delete		Delete a registered USB device.

* It is recommended to confirm that the registration is performed before/after authentication in advance.

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.

Note

Note on the deadline of USB device use

When determining available devices in the **USB Device Registration** window, the deadline of USB device use will be compared with the system date of the PC on which the Management Console is run. If the system date of the Management Console is not accurate, you may find some USB devices available (or unavailable) unexpectedly.

3. Insert the USB device that requires registration into the PC of Management Console.
4. Click the **Currently connected USB device** button.

The information of the inserted USB device is displayed in the [USB Device Registration - Currently Connected USB Devices window](#).

Point

USB device with lock function

When using a USB device with a lock function, click the **Get USB Device Information** button after unlocking.

5. Select **USB Device Identification Method**.
6. Enter **USB Device Name** and **Notes**.

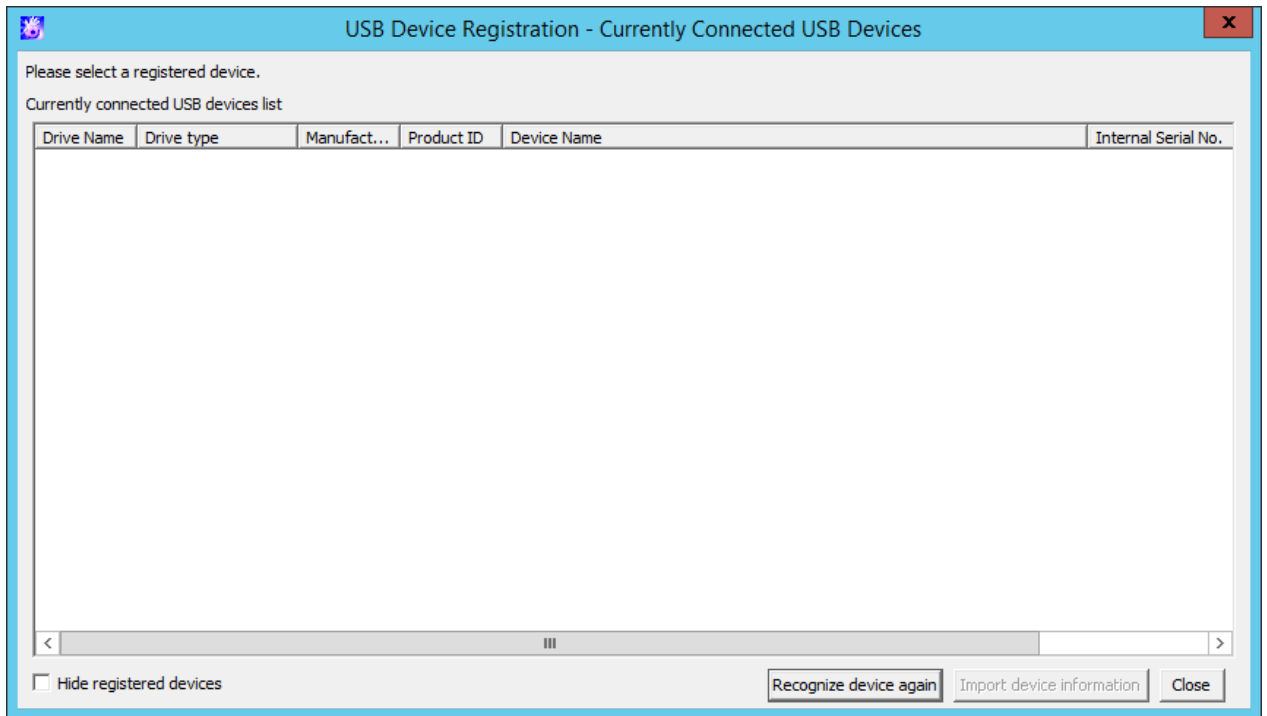
In the case of a 3-level structure, the registration information will be saved on the Master Management Server; in the case of a 2-level structure, the registration information will be saved on Management Server and the information of multiple subordinating departments will co-exist. Therefore, when 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.

7. click the **Add** button.

The registration content is displayed in **List of registered USB devices**.

USB Device Registration - Currently Connected USB Devices window

From the list of USB devices connected to the PC, select the USB device to be registered.



Item name	Description
Currently connected USB devices list	List of USB devices connected to the PC. Clicking a column header sorts the list by the values in that column.
Drive Name	Drive letter assigned to the USB device, from A: to Z:. For portable devices and imaging devices, a blank will be displayed.
Drive type	For devices to which a drive letter was assigned, Removable or DVD/CD will be displayed. For portable devices and imaging devices, WPD (Windows Portable Device) will be displayed.
Manufacturer ID	USB device manufacturer ID, displayed in hexadecimal notation.
Product ID	USB device product ID, displayed in hexadecimal notation.
Device Name	USB device name.
Internal Serial No.	USB device internal serial number. For devices without internal serial number, a blank will be displayed.
Hide registered devices	If you select this item, the devices already registered in the USB device registration window will not be displayed.
Recognize device again	Information about the USB device connected to the PC is retrieved again, and Currently connected USB devices list displayed will be updated.
Import device information	Information about the USB device selected in Currently connected USB devices list will be set for each input field in USB Device Information in the USB Device Registration window.
Close	Closes the window.

Point

The settings for **Hide registered devices** will remain enabled even when the Management Console is restarted. Also, the settings are configured per PC so they will remain enabled when other administrators log on.

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, 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**.

7.5.3 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 [7.5.1 Operation example](#) including policy setting from operation example 1 to operation example 7.

Policy setting of operation example 1

In **File export/read**, 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 operation example 2

In **File export/read**, 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 operation example 3

In **File export/read**, set as follows:

- **File Export Utilit**
 - 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 operation example 4

In **File export/read**, 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 operation 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 **File export/read**, set as follows:

- **Individual Identification Function of USB Device**
 - Select **Use**.
 - Select the permitted access settings of use in **File Export Prohibition- Individual Identification Function of USB Device-Detailed Settings** window.

Policy setting of operation example 6

In **File export/read**, 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 Prohibition- Individual Identification Function of USB Device-Detailed Settings** and select the permitted access settings of use.
 - 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.

Policy setting of operation example 7

Set the following policy to the CT group policy (user group policy) for "Section A".

In **File export/read**, set as follows:

- **USB Device Individual Identification Function**
 - Select **Use**.
 - In the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window, set **Allow to use all USB devices registered in Management Server** to **Yes**, and select the access settings for permitted use.

Set the following policy to the group policy for "Section B".

In **File export/read**, set as follows:

- **USB Device Individual Identification Function**
 - Select **Use**.
 - Specify USB devices that, in the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window, have **Identification Method** set to **Not Available**.

Policy setting of operation example 8

This is the setting for allowing only some digital cameras to be used and prohibiting the use of all other digital cameras, scanners and similar.

In **File export/read**, set as follows:

- **File Export Utility**
 - In **Export using File Export Utility**, select **Allowed**.
 - Select **Only encryption export is allowed**.
- **Windows Explorer**
 - In **File access control**, select **Yes**.

- In **Export Prohibition > Specify drive type**, select **Removable**.
- In **Portable device/imaging device connection prohibition**, select **Portable device**.
- In **Portable device/imaging device connection prohibition**, select **Imaging device**.
- **USB Device Individual Identification Function**
 - Select **Use**.
 - In the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window, add the digital cameras allowed to **List of Available USB Devices** and select **Read and Write**. Do not select any of the check boxes under it.

Point

Prohibiting USB device use for a specific client (CT) or user under "Section A"

As in operation example 7, follow the procedure below to set the policy for prohibiting USB device use for a specific client (CT) or user in "Section A".

1. Select the client (CT) or user for which the policy will be set.
2. In **File export/read**, set as follows:
 - **USB Device Individual Identification Function**
 - Select **Use**.
 - Specify USB devices that, in the **File Export Prohibition - USB Device Individual Identification Function - Detailed Settings** window, have **Identification Method** set to **Not Available**.

Click **Update at Next Startup** or **Update Immediately** to set the policy.

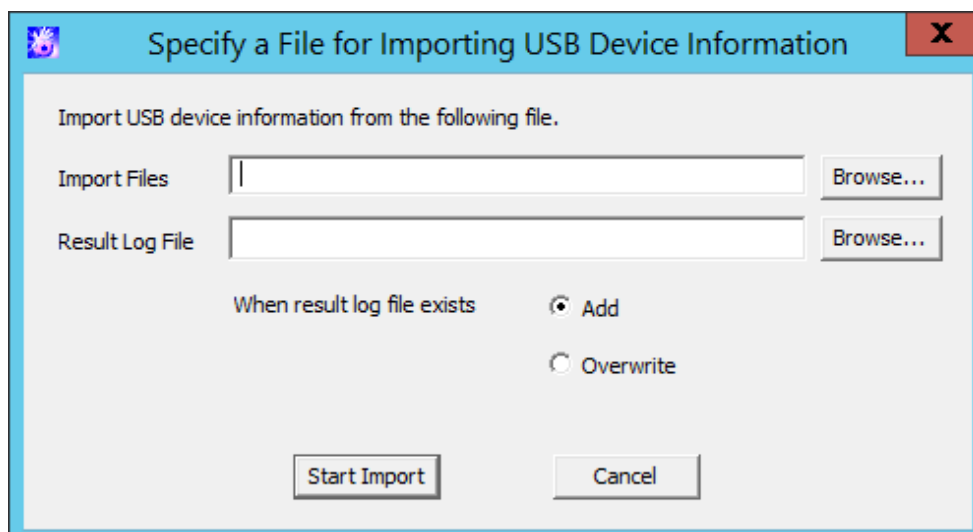
CT policy will be reflected when the client (CT) is started. User policy will be reflected at logon.

Policy will also be reflected at immediate update.

7.5.4 Register USB device information using CSV file

1. Create USB device list file.
For details on the USB device list file, 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.
Specify up to 218 halfwidth characters (109 fullwidth characters), except for the following symbols in the file name: \ / : * ? " < > |
- **Result Log file** (Required): specify and save the file of execution results with full path.
Specify up to 218 halfwidth characters (109 fullwidth characters), except for the following symbols in the file name: \ / : * ? " < > |
- **When result log file exists:** 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.

4. Set the above-mentioned information and click the **Start Import** button.

The **Display Import Status of USB Device Information** window is displayed.

5. After the import of the USB device information has completed, "Registration Completed" will be displayed in **Process Status**. Click the **OK** button.

7.5.5 Export registered USB device information as CSV file

1. Start **Management Console** and the **USB Device Registration** window is displayed.

2. Click the **File Export** button.

The **Specify a File for Exporting USB Device Information** window is displayed.



- **Export File** (Required): specify the CSV file for exporting USB device information with full path.
Specify up to 218 halfwidth characters (109 fullwidth characters), except for the following symbols in the file name: \ / : * ? " < > |
- **Result Log File** (Required): specify the file for exporting execution results with full path.
Specify up to 218 halfwidth characters (109 fullwidth characters), except for the following symbols in the file name: \ / : * ? " < > |
- **When result log file exists:** 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.

7.5.6 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, refer to "[7.5.5 Export registered USB device information as CSV file](#)".
2. Modify the contents of the CSV file if needed.

Enter the CSV file as text file to edit. After editing with software such as Microsoft(R) 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 on the CSV file, 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. Do not modify the item apart from the USB device name, notes or identification method.

Delete USB device information

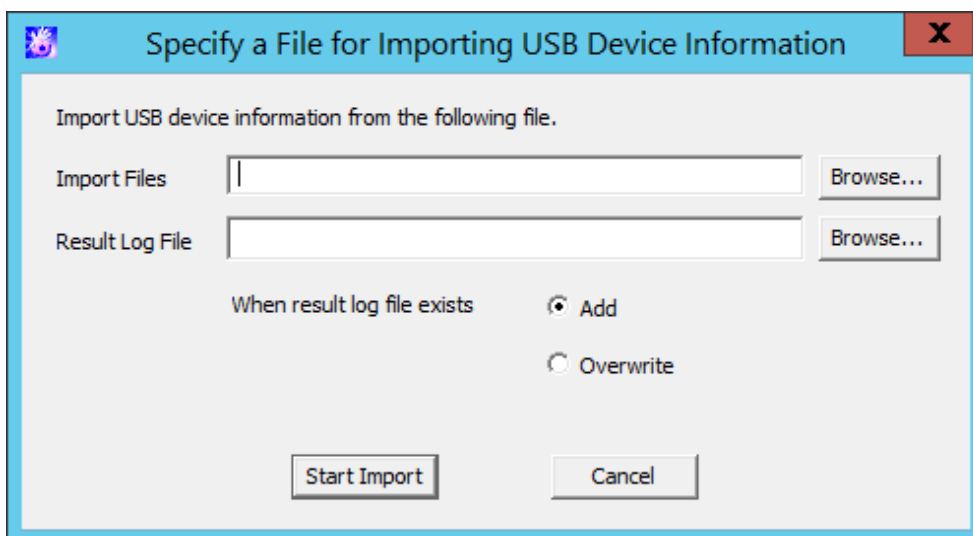
- a. Specify "D" in the first item (process flag).
- b. Confirm that the second item (GUID) is specified.

Move USB device information to another Management Server.

When modifying the USB device information registered on the moved Management Server, 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 a File for Importing USB Device Information** window is displayed.



- **Import File** (Required): specify the USB device list file with full path.
Specify up to 218 halfwidth characters (109 fullwidth characters), except for the following symbols in the file name: \ / : * ? " < > |
 - **Result Log File** (Required): specify and save the file of execution results with full path.
Specify up to 218 halfwidth characters (109 fullwidth characters), except for the following symbols in the file name: \ / : * ? " < > |
 - **When result log file exists**: 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.
5. Set the above-mentioned information and click the Start Import button.
- The **USB Device Information Import Status Display** window is displayed.
6. After the import of USB device information import has completed, "Registration Completed" will be displayed in **Process Status**. Click the **OK** button.



Note

The CSV file used for import cannot be used again.

The CSV file used for import cannot be used again. To modify the CSV file as modify USB device information, perform the operation again using CSV file import in Step 1.

7.6 Modify Period to Save Logs

The log saving period and timing for log backup, etc., are usually the information set at the system design/installation. However, after regular backup of the collected logs has been started, the log amount may exceed the expected amount that requires a change of settings. In this case, the balance between the log saving period and amount of collected log can be obtained by modifying the log saving period.

The following are two change methods:

- 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, refer to "Determine How to Use Logs" of *Systemwalker Desktop Keeper Installation Guide*.

For details on setting items of the backup tool, commands to be used, change procedures, etc., refer to "Backup User Asset" of *Systemwalker Desktop Keeper Installation Guide*.

7.7 Change CT Environment

This section describes how to change the 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).



Note

Use the same client management password for the Management Server and Master Management Server.

When changing the connection destination Management Server or Master Management Server for the client (CT), use the same client management password as before.

Change IP address using files in Management Server

This section describes how to change IP address in Management Server.



Note

Windows(R) 8 Fast Startup feature

Assume that you are using Windows(R) 8, the Fast Startup feature is enabled, and you shut down before you have logged on. In this case, the transfer target information file and CT operation parameter information file update operations, the CT policy request operation, and the self version upgrade check that are normally performed when a PC starts may not work. To ensure that these operations are performed properly, restart the operating system instead of shutting down.

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 on the procedure, 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 on the procedure, 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, 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, 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 on the information file to be moved, refer to "Information File To Be Moved" of *Systemwalker Desktop Keeper Reference Manual*.

Location for saving

Under Windows Server(R) 2008 or Windows Server(R) 2012 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 Windows Server(R) 2008 or Windows Server(R) 2012 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.

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 on the information file to be moved, refer to "Information File To Be Moved" of *Systemwalker Desktop Keeper Reference Manual*.

Location for Saving

Under Windows Server(R) 2008 or Windows Server(R) 2012 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 Windows Server(R) 2008 or Windows Server(R) 2012 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.
Refer to "Information File To Be Moved" of *Systemwalker Desktop Keeper Reference Manual* for details on the information file to be moved.

Location for Saving

Under Windows Server(R) 2008 or Windows Server(R) 2012 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 Windows Server(R) 2008 or Windows Server(R) 2012 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 on the information file to be moved, refer to "Information File To Be Moved" of *Systemwalker Desktop Keeper Reference Manual*.

Location for Saving

Under Windows Server(R) 2008 or Windows Server(R) 2012 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 Windows Server(R) 2008 or Windows Server(R) 2012 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., change the settings through maintenance commands.

Change IP address using commands in client (CT).



Note

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, 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.

```
fswl1ej7.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).

```
fswl1ej7.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.

- 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).

- Restart the client (CT).

The change status of the Management Server to be connected can be confirmed according to the following.

- Start the Management Console that connects to the (Master) Management Server of moving source or the moving target.
- 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.
- 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

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	

Change Method		Items that can be modified	Version of Client (CT) that can be modified
		<ul style="list-style-type: none"> - Confirmation message of recipient address during E-mail sending 	V14.2.0 or later
		<ul style="list-style-type: none"> - IP address of backup Management Server - Size of result log file - Size of prohibition log file - Size of error log file - Number of days to save error log - Size of trace log file - Printing monitoring mode (*) - E-mail control mode <ul style="list-style-type: none"> - Port number for E-mail sending monitoring - Monitoring mode of E-mail attachment prohibition - Port number for communication of E-mail attachment prohibition - Port number 2 for communication of E-mail attachment prohibition - Run immediately after logon 	V14.2.0 or later
	Change in Terminal Operation Settings window	<ul style="list-style-type: none"> - Printing monitoring mode 	All versions
Change in Client (CT)	Change in Add or Remove Programs	<ul style="list-style-type: none"> - Printing monitoring mode - E-mail control mode <ul style="list-style-type: none"> - Port number for E-mail sending monitoring - Monitoring mode of E-mail attachment prohibition - Port number for communication of E-mail attachment prohibition - Port number 2 for communication of E-mail attachment prohibition 	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



Note

Windows(R) 8 Fast Startup feature

Assume that you are using Windows(R) 8, the Fast Startup feature is enabled, and you shut down before you have logged on. In this case, the transfer target information file and CT operation parameter information file update operations, the CT policy request operation, and

the self version upgrade check that are normally performed when a PC starts may not work. To ensure that these operations are performed properly, restart the operating system instead of shutting down.

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 on information file of CT operating parameter, refer to "Information File of CT Operating Parameter" of *Systemwalker Desktop Keeper Reference Manual*.

Location for Saving

Under Windows Server(R) 2008 or Windows Server(R) 2012 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 Windows Server(R) 2008 or Windows Server(R) 2012 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.

Setting Item	Timing of Reflecting the Set Value
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, 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

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.

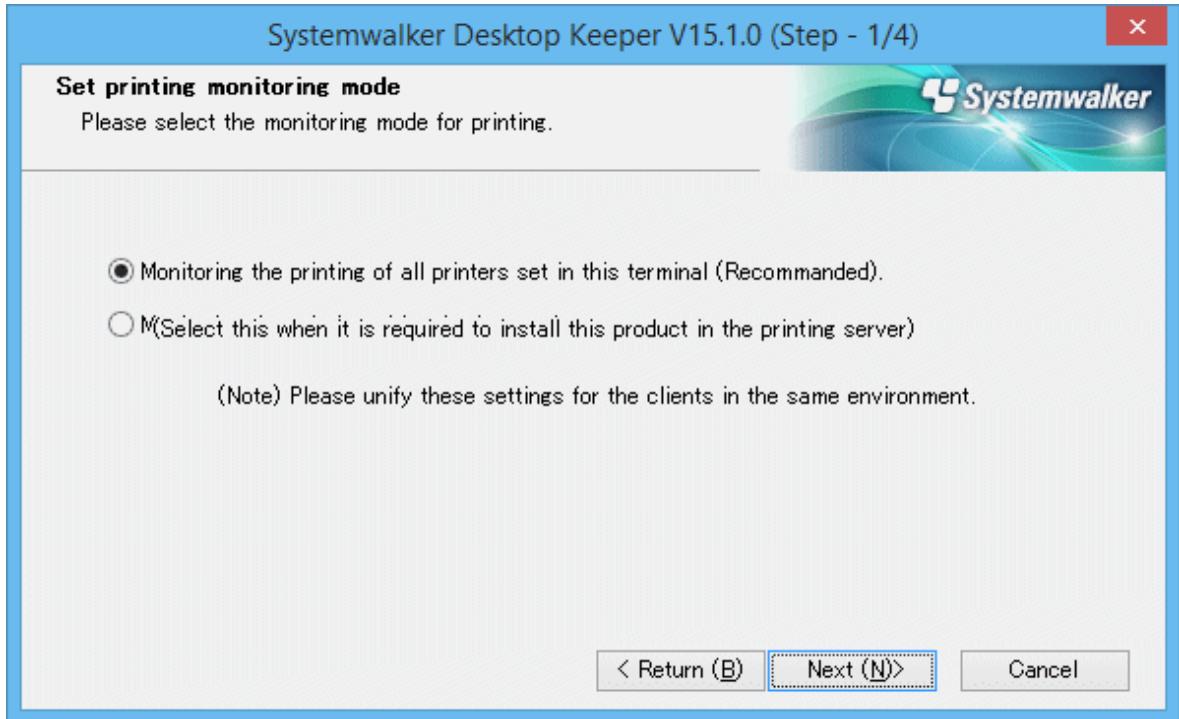
When the **Printing Monitoring Mode** is also set in the information file of CT operating parameter, the configuration value of the information file of the CT operating parameter will be reflected.

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 on the configuration value, 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**.

The screenshot shows a configuration window titled "Systemwalker Desktop Keeper V15.1.0 (Step - 2/4)". The main heading is "Set E-mail Control Mode" with a sub-instruction: "Please enter the information related to e-mail sending and e-mail file attachment prohibition." The window is divided into two sections: "E-mail Sending" and "E-mail 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

At the bottom, there are three buttons: "< Return (B)", "Next (N)>" (which is highlighted with a dashed border), and "Cancel".

For details on the configuration value, 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), 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. Start **Server settings tool**.

Refer to "7.9.1 Start Server Settings Tool" for details.
 2. Select **Stop Service** from the **Service** menu of the **Server Settings Tool** window.
 3. The confirmation window for stopping service is displayed. Click the **OK** button.
 4. Click the **System Settings** button.

The System Settings window is displayed.
 5. 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**.
 6. Click the **Set** button.
 7. Select **Start Service** from the **Service** menu of the **Server Settings Tool** window.
 8. The confirmation window for starting service is displayed. Click the **OK** button.
- Settings of the terminal to install the client.
 1. 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 server 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 server 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 server name when changing the (Master) Management Server to be connected, 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 **Welcome** window is displayed.
4. Select **Modify** and click the **Next** button.
The **Enter the server information** window is displayed.
5. Change the server name or IP address.

When Adding New Server Name or IP Address

- a. Set **Sever 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 Server Name or IP Address

- a. Select the "Sever name or IP address of connected (Master) Management Server: Port number being used" to be deleted.
- b. Click the **Remove** button.

When Changing the Server Name or IP Address that has been Set

- a. Select the "Sever name or IP address of connected (Master) Management Server: Port number being used" to be modified.
 - b. Click the **Remove** button.
 - c. Set the **Sever 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, 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

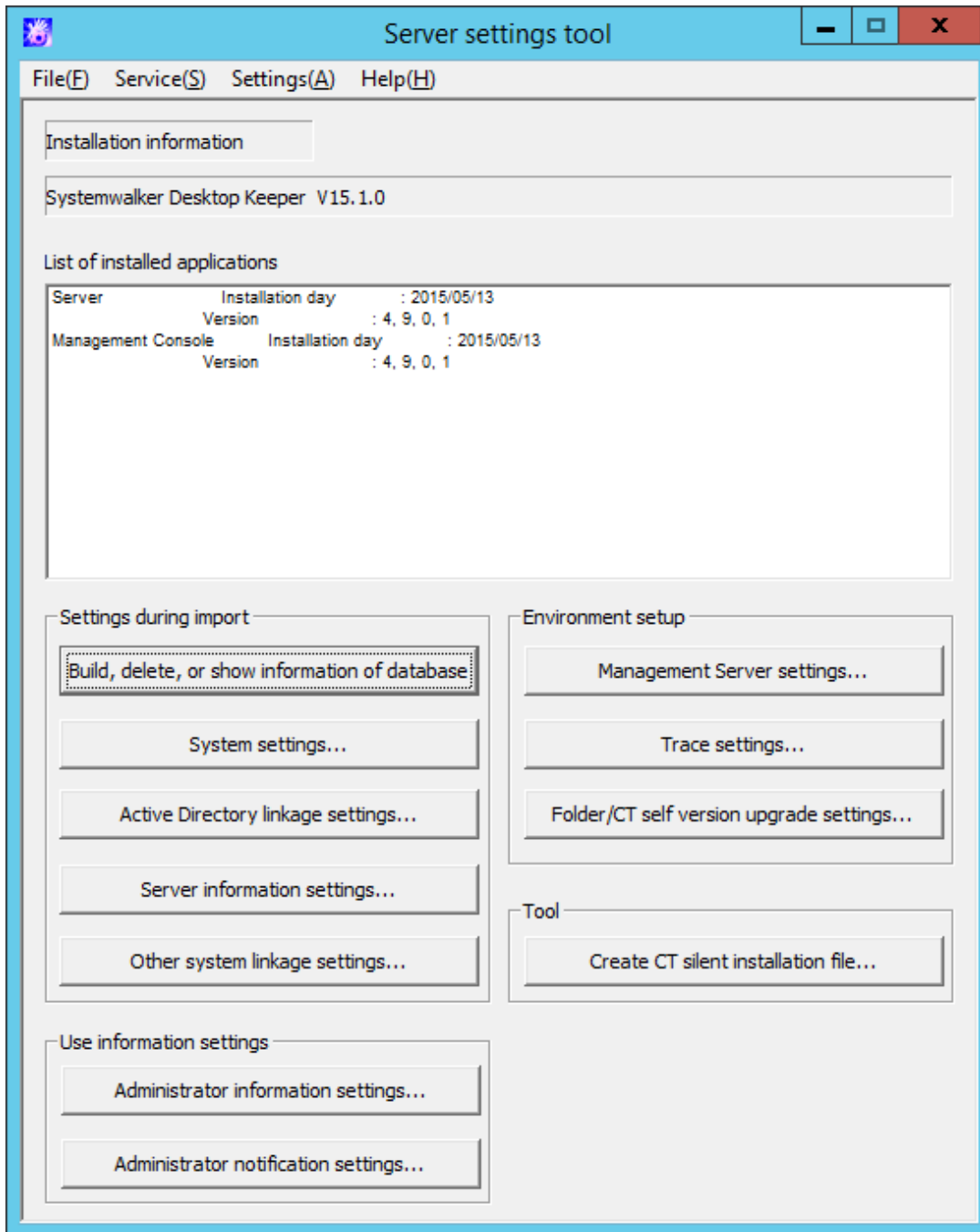
Start Server Settings Tool

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 **Systemwalker Desktop Keeper > Server > Server Settings Tool** from the **Start** menu or **Apps > Systemwalker Desktop Keeper > Server settings tool**.
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 changed after the installation of Management Server and Master Management Server.

It is recommended to change the password regularly. For information on how to do so, 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".

- 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 Tool** window.

Item Name	Description
Installation information	The version of installed product will be displayed.
List of installed applications	The installation date and version of installation application of each Systemwalker Desktop Keeper will be displayed. - Installed application The following applications will be displayed when they are installed.

Item Name		Description
		<ul style="list-style-type: none"> - Management Server/Master Management Server (Name displayed: Server) - Management Console (Name displayed: Management Console) - Installation date (The installation date will be displayed in the format of mm/dd/yyyy) - Version of installed application
Settings during import	Build, delete, or show information of database	Displays the Build, delete, or show information of database window. Construct, delete, and show information of the database used in the Master Management Server and Management Server.
	System settings...	Display the System Settings window. Set all operations of the Master Management Server and Management Server.
	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"> - Authentication user of Management Console, Log Viewer, Backup Tool, Restoration Tool and Report Output Tool - Department administrator - Authority given to the above mentioned registrants
	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.

Menu Bar		Function Summary	
	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.	
	Change Password	Change the password of the initial administrator. Specify up to 32 halfwidth alphanumeric characters and symbols, except for spaces and the following symbols: & < > \ " ~ ' ? : ^	
	Trace Server Settings Tool	OFF	Do not collect the trace of Server Settings Tool.
		Summary	Collect the trace of Server Settings Tool at summary level.
Details		Collect the trace of Server Settings Tool at detail level.	
Help	Online Help	Display the HTML manual.	
	Version Information	Display the copyright information and version information.	

7.9.2 Change Password of Initial Administrator

This section describes how to change the password of the initial administrator.

1. Start **Server Settings Tool**.
2. Select **Change Password** from the **Settings** menu.
The **Change Password** window is displayed.
3. Enter the old password in "Old password" and enter the changed password in "New password".
 - Specify the password with no more than 32 single-byte alphanumeric characters and symbols.
 - The following symbols cannot be specified: & < > | \ " ~ ' ? : ^
 - The single-byte space cannot be entered.
4. Click the **Set** button.

7.9.3 Modify Administrator Notification

In the **Administrator Notification Settings** window, set the method of notifying events that occur in the client (CT) and database (E-mail notification, event log writing) to the administrator during installation.

However, when it is necessary to modify the configuration value corresponding to the operation status, the change can be performed after the operation has started.

For information on how to make such changes, refer to "Administrator Notification Settings" of *Systemwalker Desktop Keeper Installation Guide*.

Administrator Notification Settings window

Administrator Notification Settings

Perform the settings related to notification administrator when detecting the violation operation.

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
Linage 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 (5~20)
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"/> 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, 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, 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, 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.

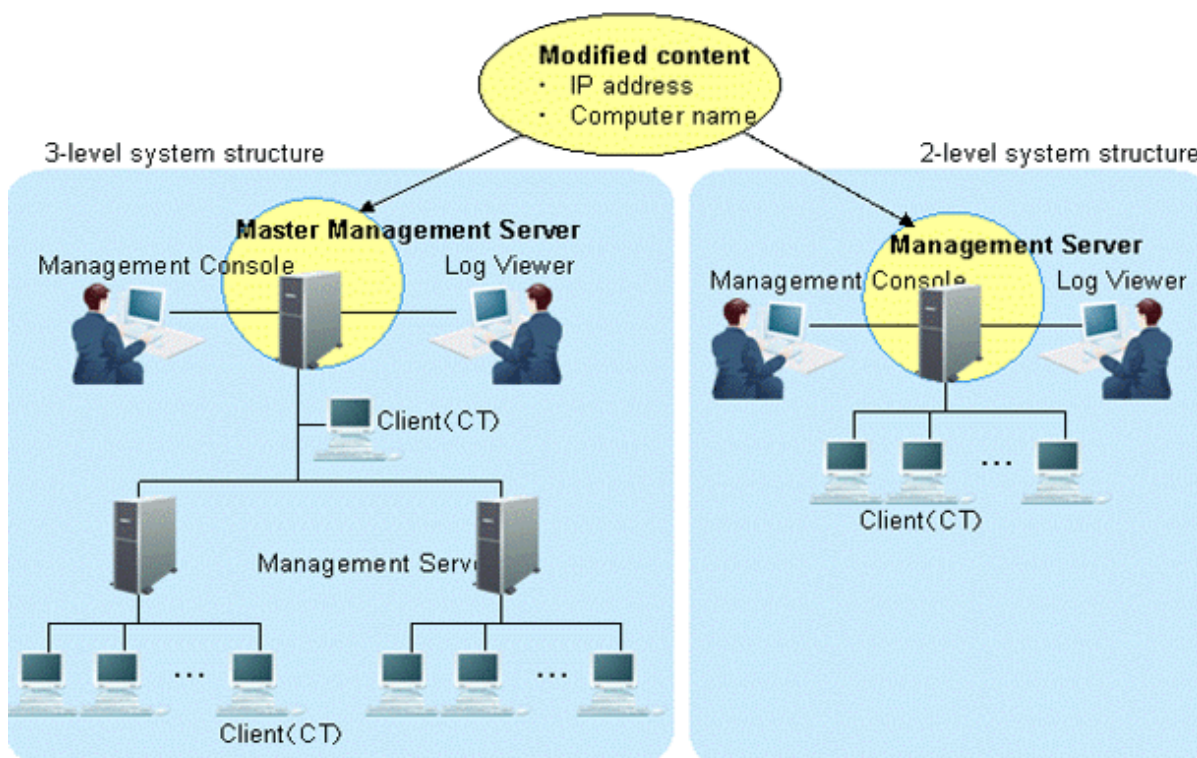
During the reflection period, the Log Analyzer of Web Console cannot be used. If you wish to use the Log Analyzer after changes are reflected immediately, reflect according to "Transfer Administrator Information to Log Analyzer Server" and "Register Administrator Information on Log Analyzer Server" of "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, 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, 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



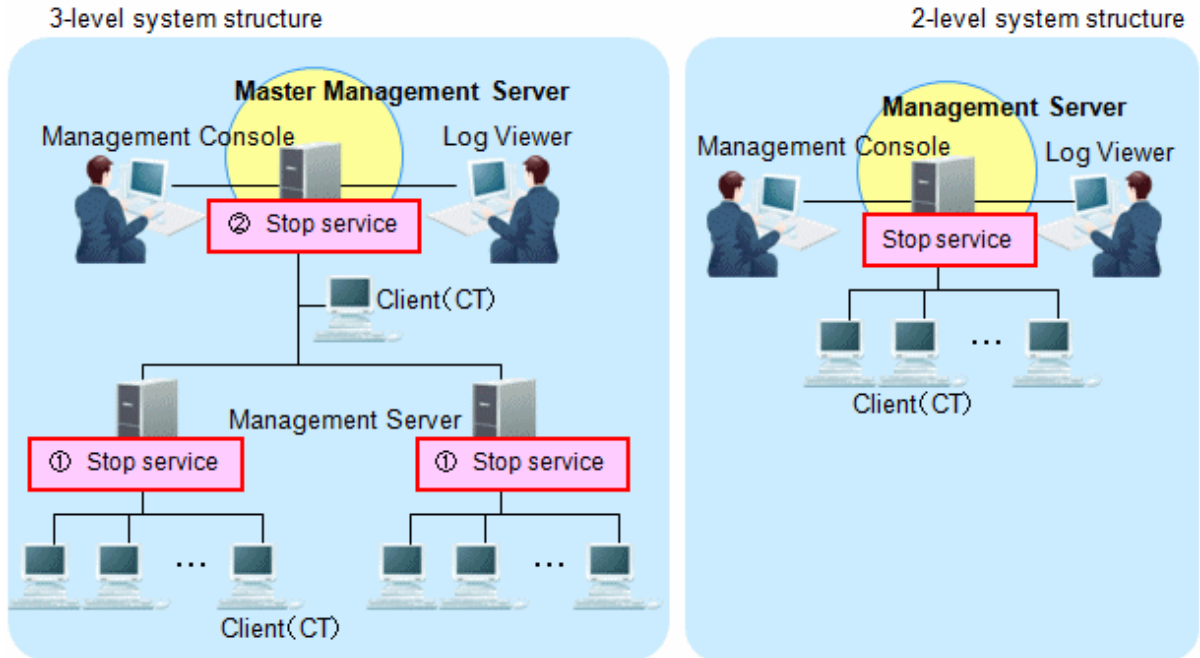
This section describes how to change the environment of the Management Server/Master Management Server when the following information is changed on the Master Management Server in a 3-level structure or Management Server in a 2-level structure.

- 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.

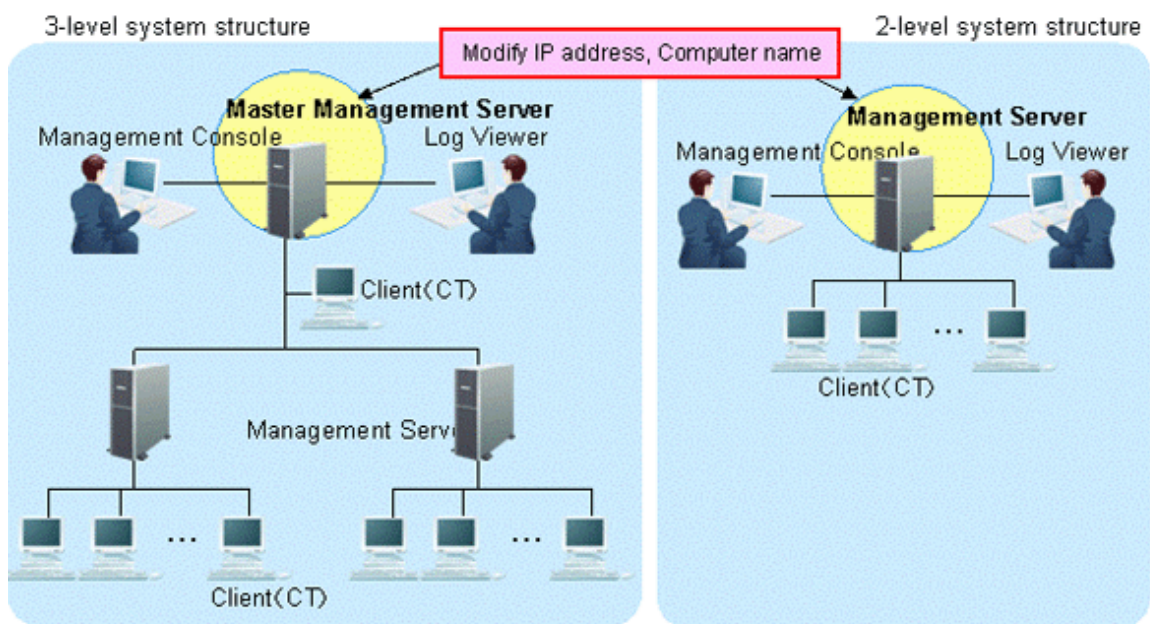
The procedure is as follows.

1. Stop the level control service and server service.



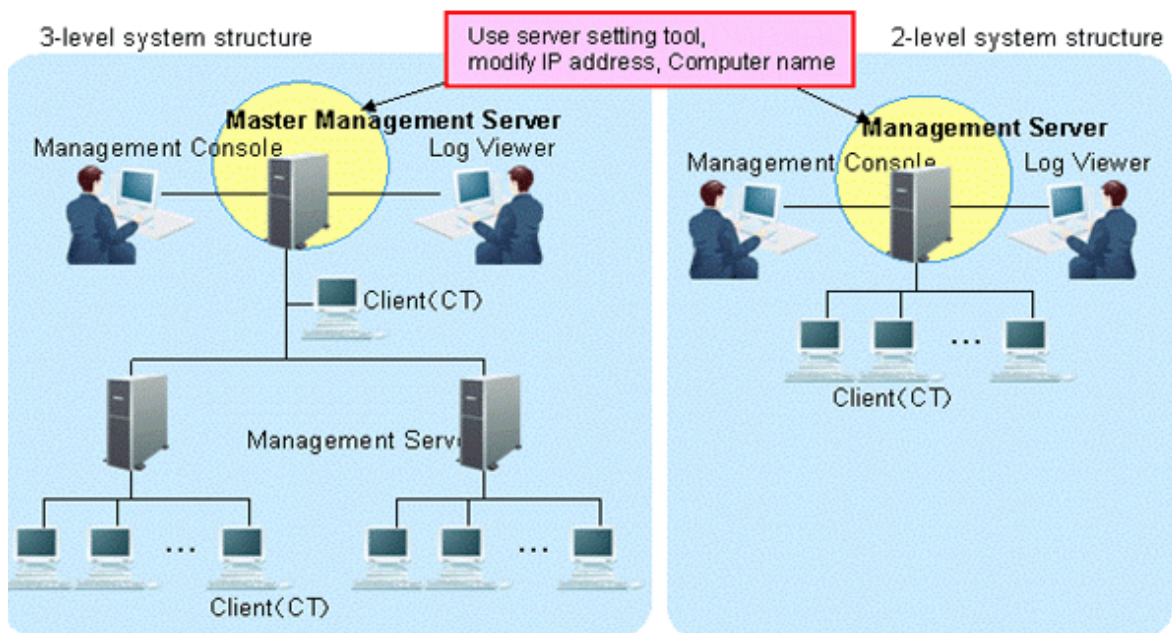
Under a 3-level structure, the Master Management Server and all Management Servers that belong to the Master Management Server can be stopped. (Start stopping from the Management Server.)

- 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, proceed to the next step.
 1. Select **Control Panel > Network Connection > Local Area Connection**. 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, proceed to the next step.
 1. Select the **Control Panel > System** 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.

Server Information Settings

Perform settings related to server.
For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
Lowercases of node name will be changed to uppercases before registration.
In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...
Own node	V70A34VJ6U001	V70A34VJ6U001	133.162.24.230	root server	2015/05/17 14:14:11	2015/05/13 17:18:04

Node type: Own node
Node name: V70A34VJ6U001
Computer name: V70A34VJ6U001
Server IP address or server name: 133.162.24.230
Server classification: Root Server

Number of regist 1 items (maximum 255 items) [Add] [Update] [Delete] [Close]

- d. Modify **Computer name** or **IP address**, click the **Update** button and click the **Close** button.



Note

Modify Computer name and IP address only.

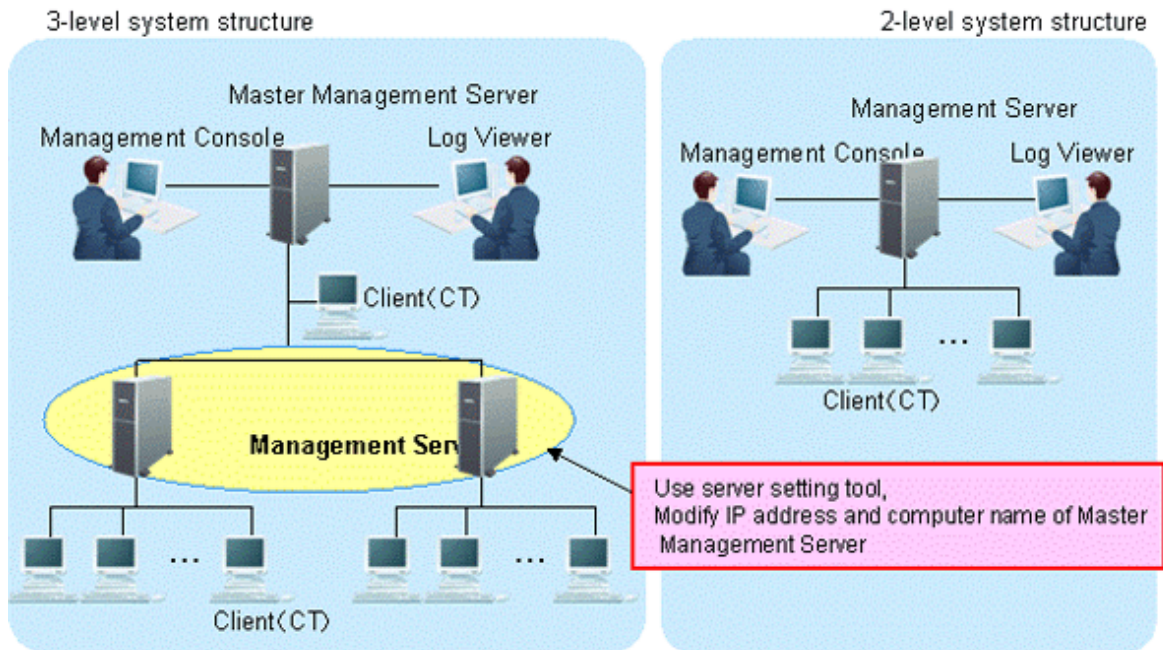
As the structure information may be inconsistent, do not modify the value of items other than **Computer name** and **IP address**.

- 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.

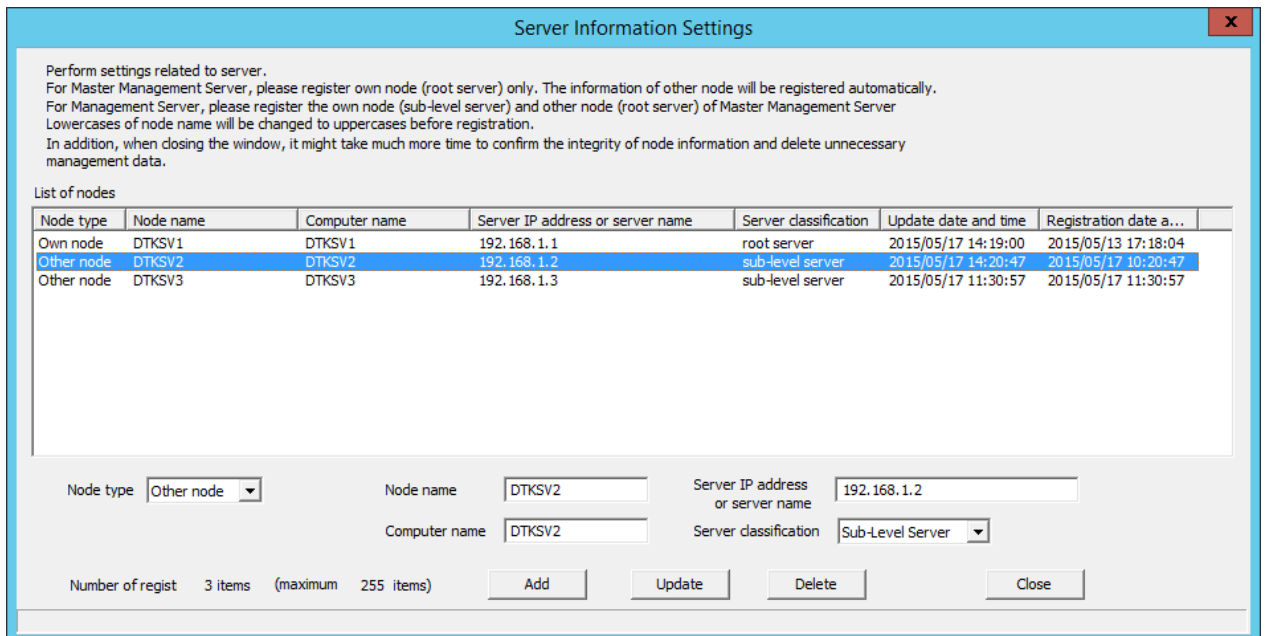
1. Start **Server Settings Tool**.
2. Select **Start Service** from the **Service** menu.
3. Exit **Server Settings Tool**.

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.

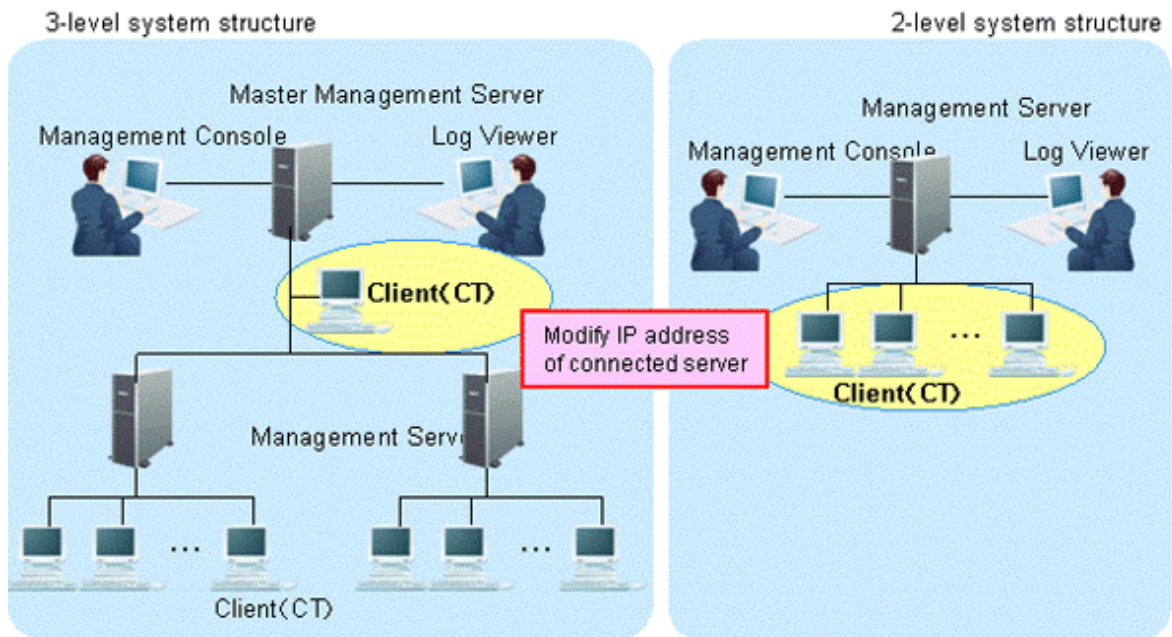
f. Start service.

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.

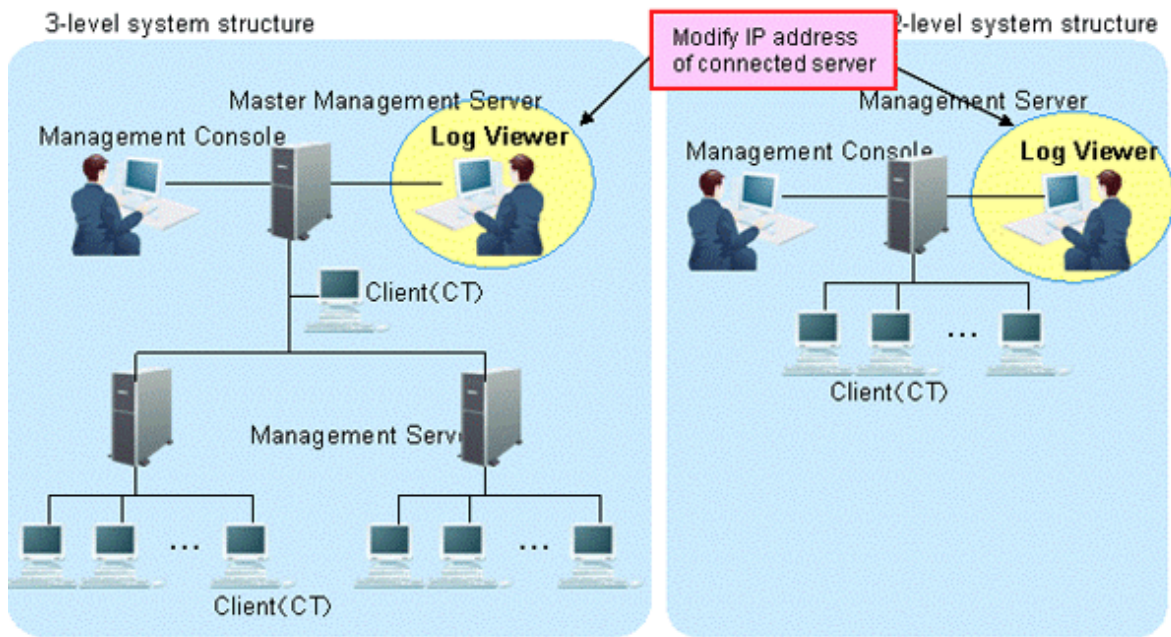
5. Change CT environment



For the following case, 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

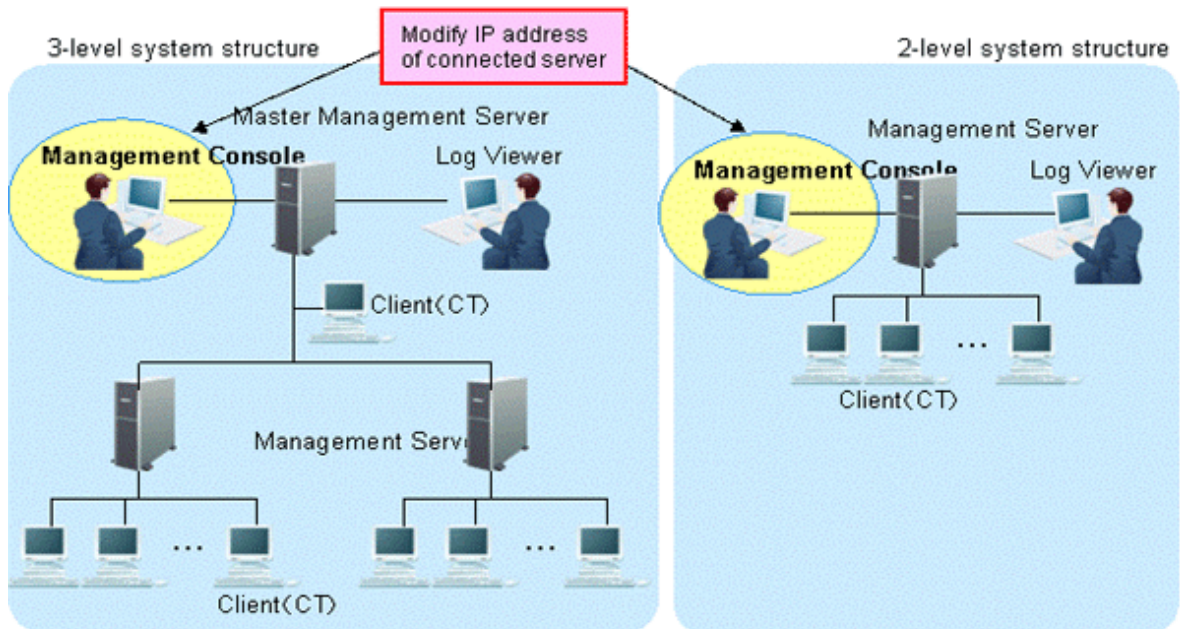
6. Change the Log Viewer environment



For the following cases, 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



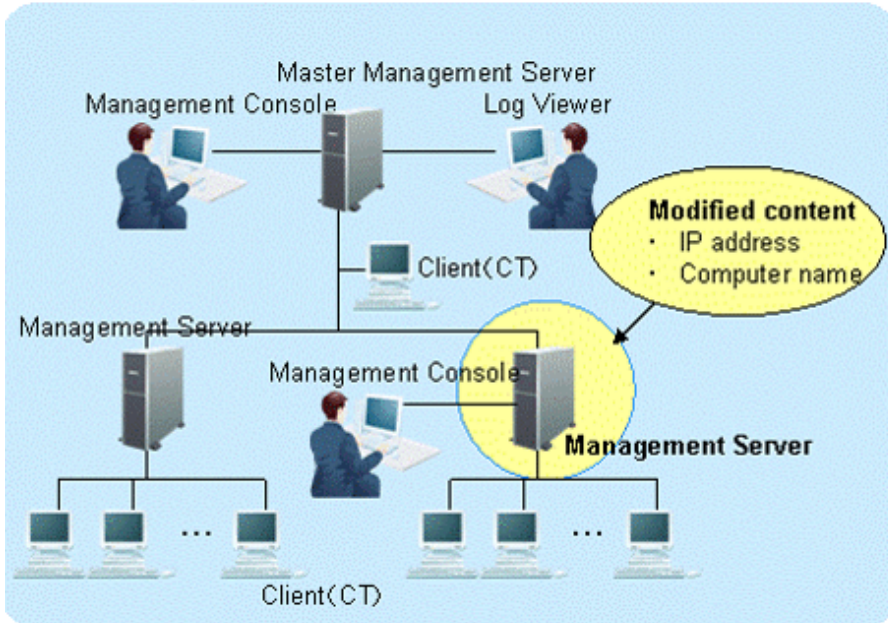
For the following cases, refer to "7.8 Change Management Console Environment" and change the Management Console environment.

- 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

3-level system structure



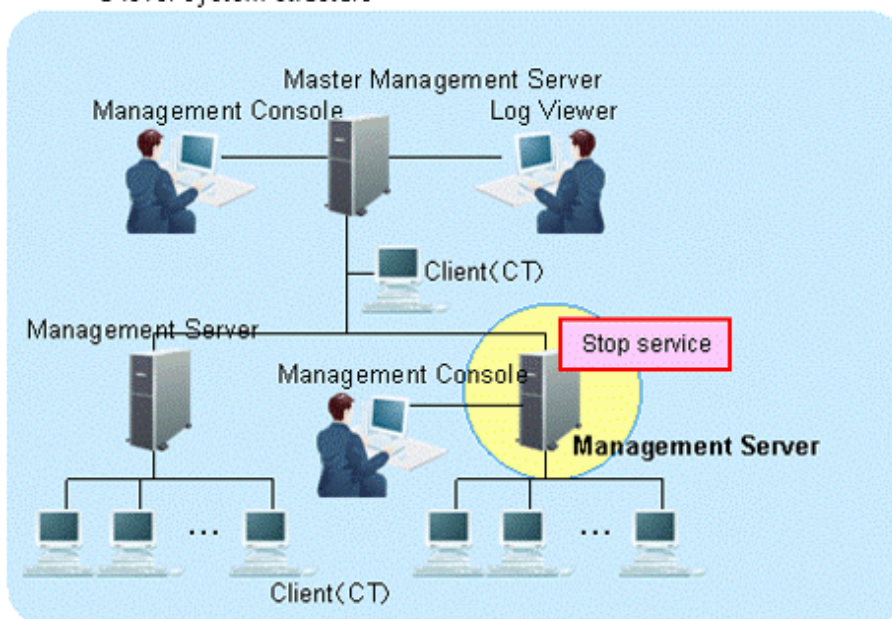
This section describes how to change the environment of the Management Server (when the Master Management Server in a 3-level structure is not changed) when the following information is modified only in the Management Server in a 3-level structure.

- IP address
- Computer name

The procedure is as follows.

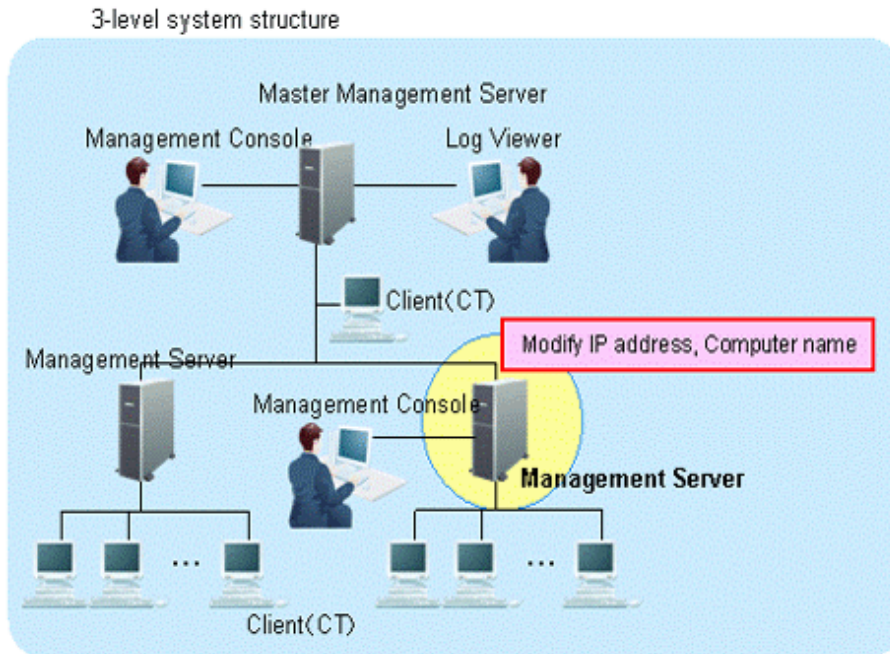
1. Stop the level control service and server service.

3-level system structure



The Management Server with IP address or computer name to be modified can be stopped.

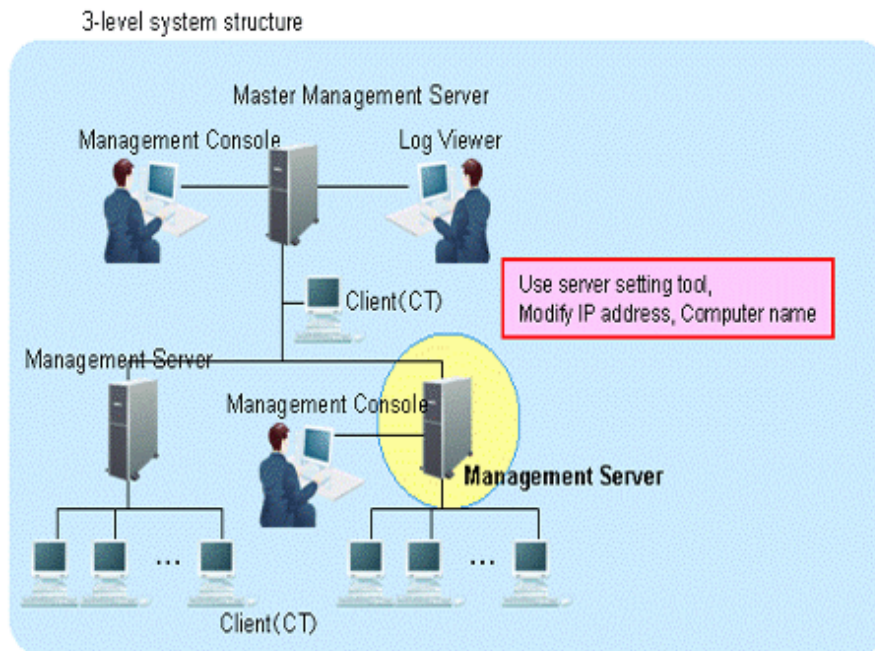
- a. Start **Server Settings Tool**.
 - b. Select **Stop Service** from the **Service** menu.
2. Modify IP address and computer name.



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, go on to the next step.
 1. Select **Control Panel > Network Connections > Local Area Connection**. 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, go on to the next step.
 1. Select the **Control Panel > System** 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.

Server Information Settings x

Perform settings related to server.
For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
Lowercases of node name will be changed to uppercases before registration.
In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...
Other node	DTKSV1	DTKSV1	192.168.1.1	root server	2015/05/17 14:19:00	2015/05/13 17:18:04
Own node	DTKSV2	DTKSV2	192.168.1.2	sub-level server	2015/05/17 14:20:47	2015/05/17 10:20:47

Node type: Node name: Server IP address or server name:

Computer name: Server classification:

Number of regist: 2 items (maximum 255 items)

- d. Modify the **Computer name** or **IP address**, click the **Update** button and then click the **Close** button.



Modify Computer name and IP address only.

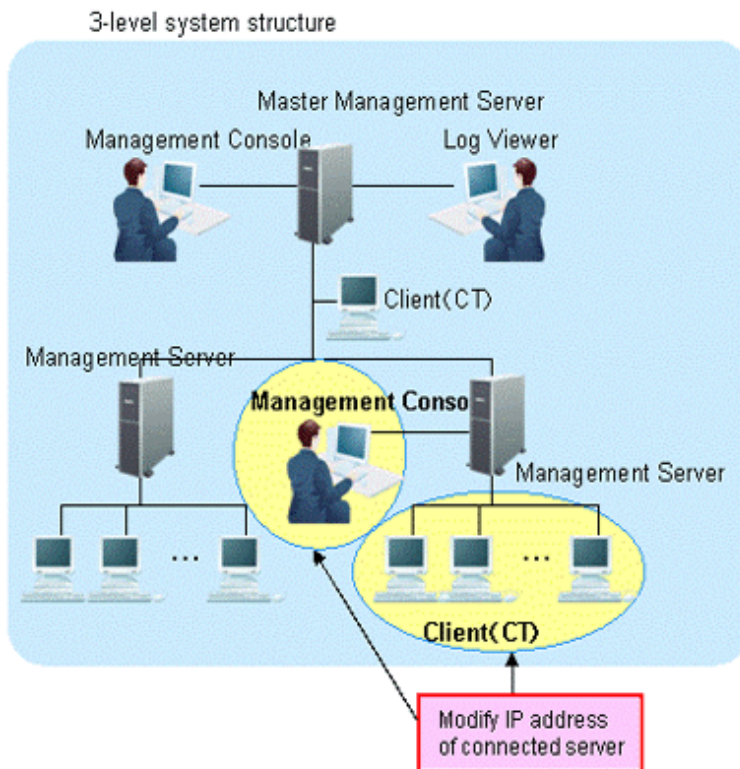
As the configuration information may not match, do not modify the value of items apart from **Computer name** and **IP address**.

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, refer to "[7.7.1 Change Management Server/Master Management Server To Be Connected](#)" and change the CT environment.

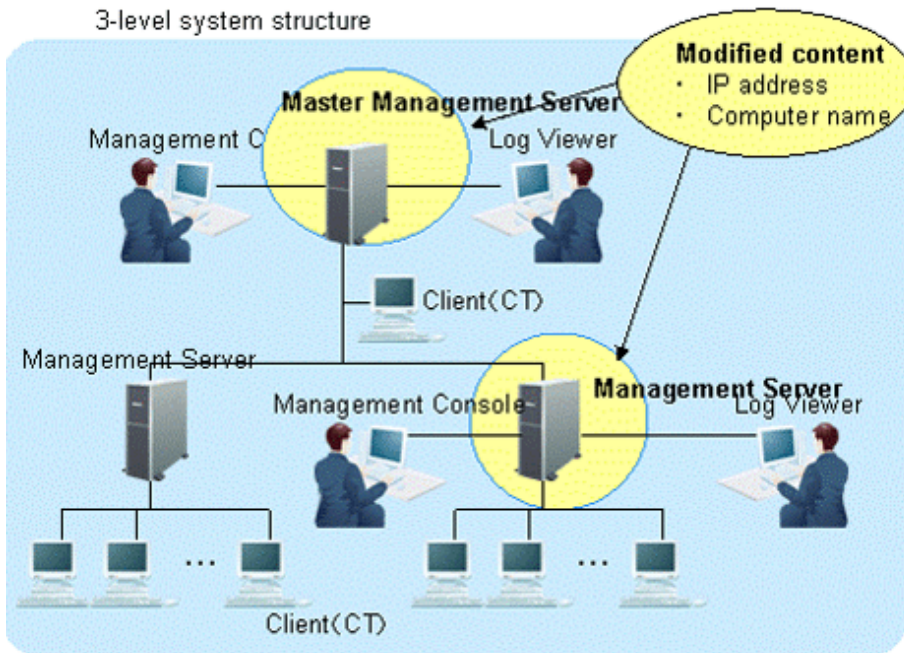
- When the IP address of the Management Server in a 3-level structure is modified and the client (CT) that belongs to this Management Server is connected

5. Change Management Console environment

For the following case, 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



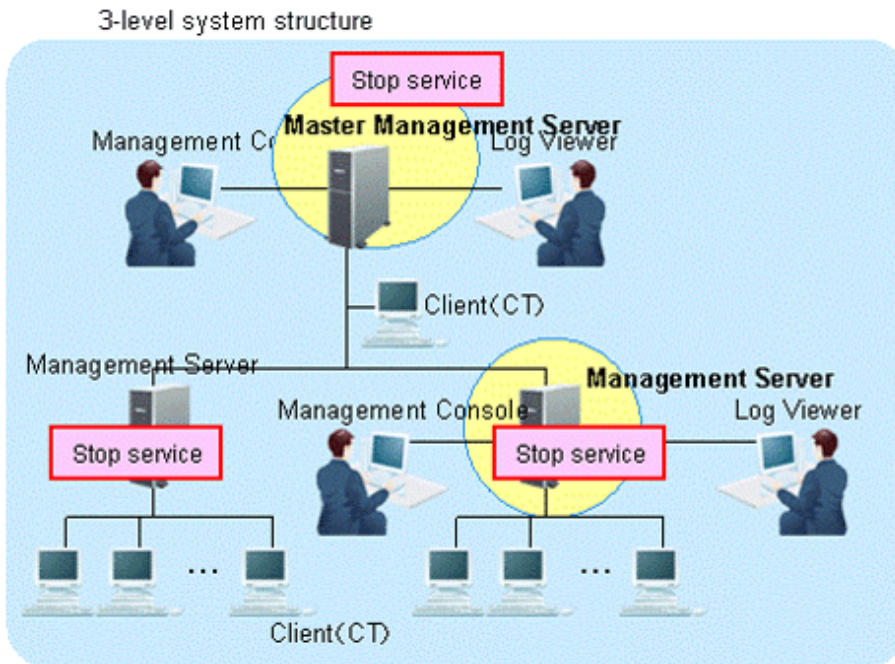
This section describes how to change the environment of the Management Server/Master Management Server when the following information is modified on the Master Management Server in a 3-level structure or a Management Server that belongs to the Master Management Server.

- 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.

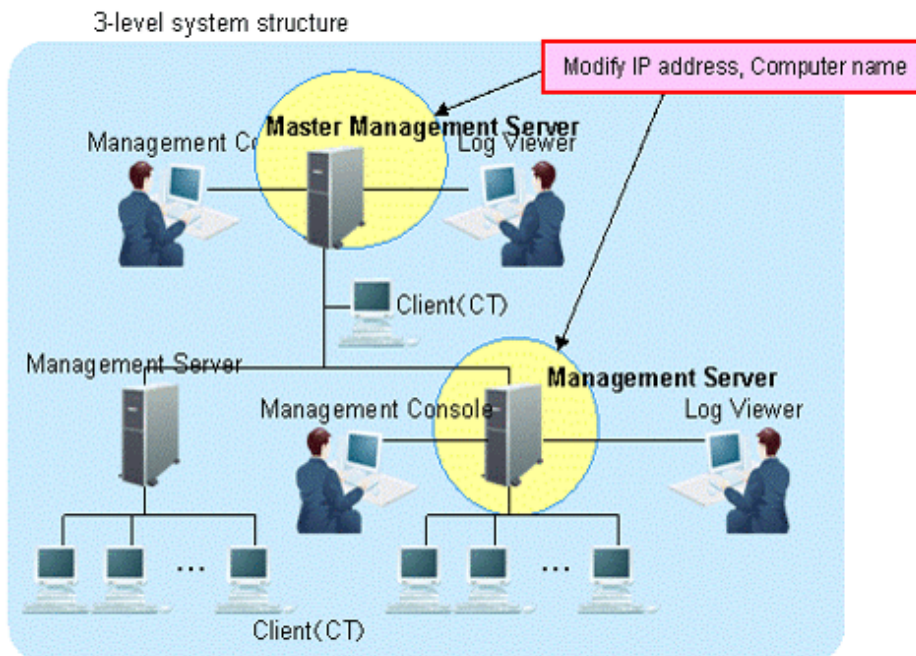
The procedure is as follows.

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.

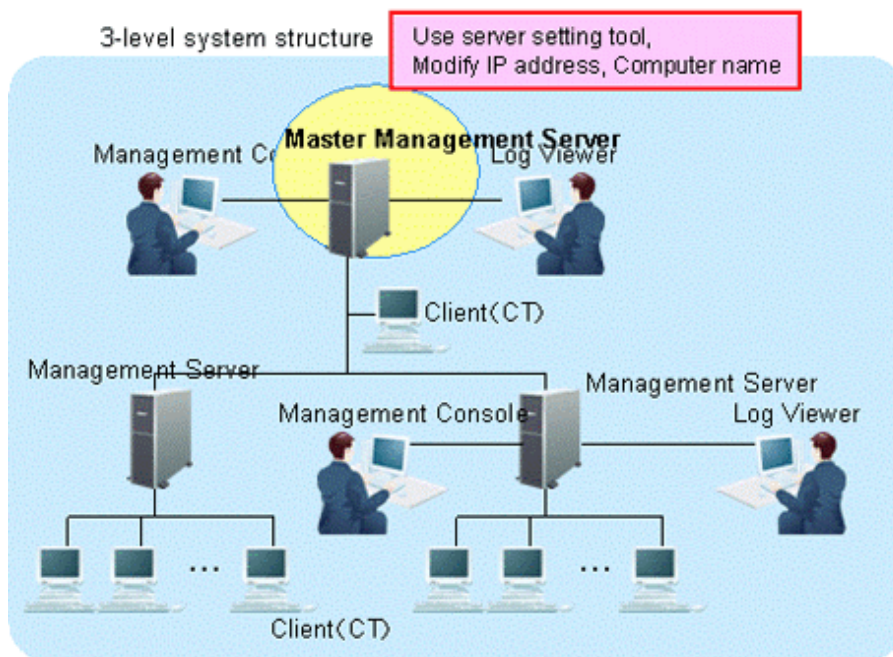
- a. Start the **Server Settings Tool**.
 - b. Select **Stop Service** from the **Service** menu.
2. Modify IP address and computer name.



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, proceed to the next step.
 1. Select **Control Panel > Network Connection > Local Area Connection**. 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, proceed to the next step.
 1. Select the **Control Panel > System** and display the **Computer Name** tab of the **System Properties** window.
 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.

Server Information Settings

Perform settings related to server.
For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
Lowercases of node name will be changed to uppercases before registration.
In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...
Own node	DTKSV1	DTKSV1	192.168.1.1	root server	2015/05/17 14:19:00	2015/05/13 17:18:04
Other node	DTKSV2	DTKSV2	192.168.1.2	sub-level server	2015/05/17 14:20:47	2015/05/17 10:20:47

Node type: Own node
Node name: DTKSV1
Computer name: DTKSV1
Server IP address or server name: 192.168.1.1
Server classification: Root Server

Number of regist 2 items (maximum 255 items) [Add] [Update] [Delete] [Close]

- d. Modify **Computer name** or **IP address**, click the **Update** button and click the **Close** button.



Note

Modify Computer name and IP address only.

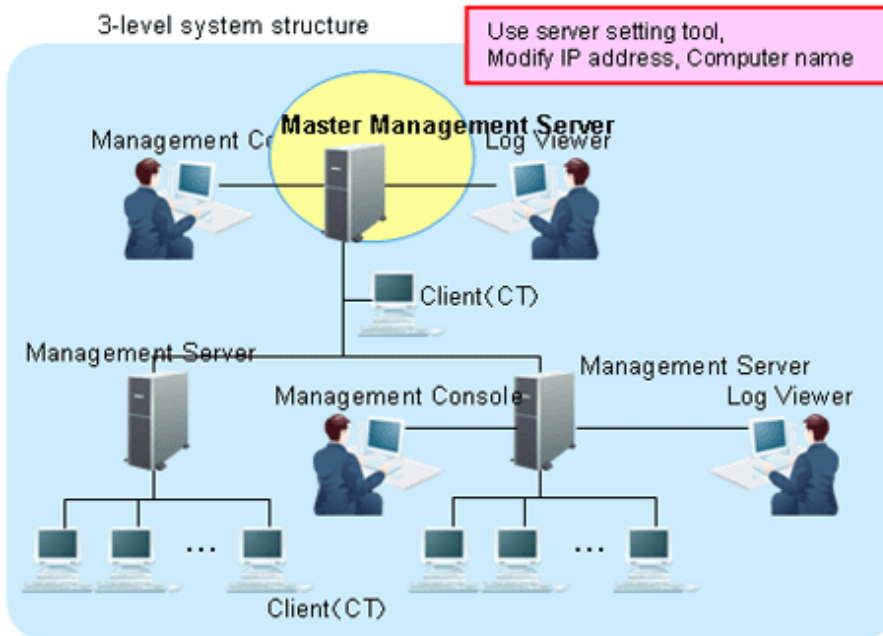
As the configuration information may not match, do not modify the value of items apart from **Computer name** and **IP address**.

- e. Start service.

Start the service of the Master Management Server in a 3-level structure for which the settings have been changed.

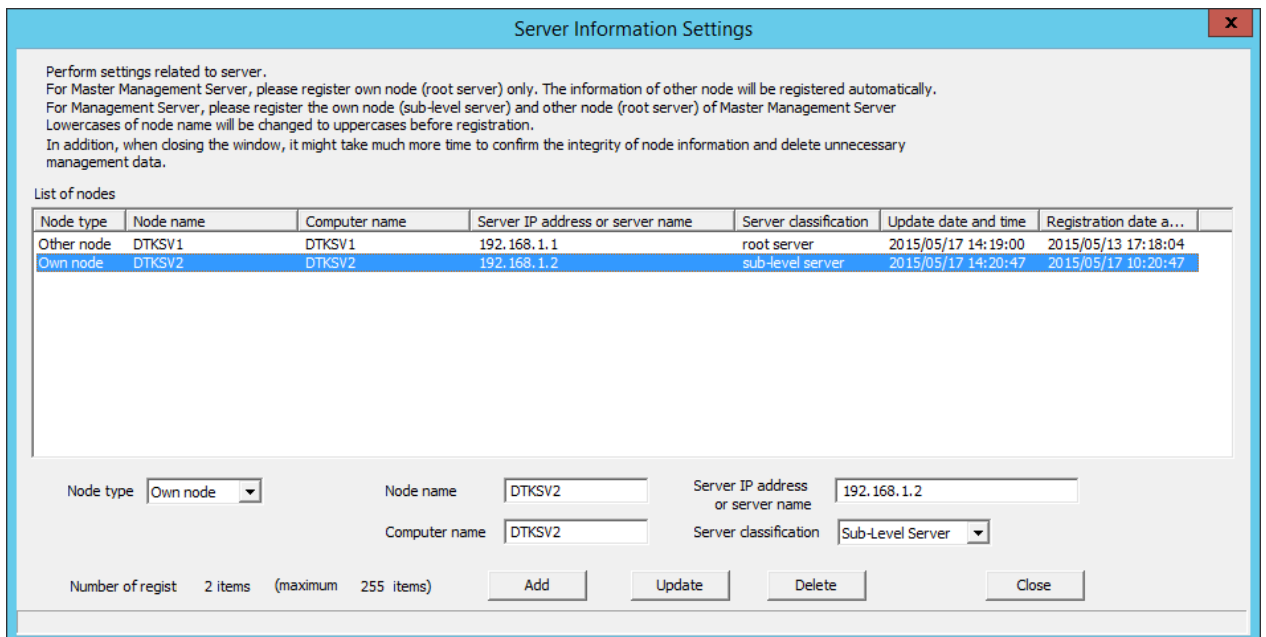
1. Start **Server Settings Tool**.
2. Select **Start Service** from the **Service** menu.

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.

Server Information Settings

Perform settings related to server.
For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
Lowercases of node name will be changed to uppercases before registration.
In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...
Own node	DTKSV1	DTKSV1	192.168.1.1	root server	2015/05/17 14:19:00	2015/05/13 17:18:04
Other node	DTKSV2	DTKSV2	192.168.1.2	sub-level server	2015/05/17 14:20:47	2015/05/17 10:20:47

Node type: Own node
Node name: DTKSV1
Computer name: DTKSV1
Server IP address or server name: 192.168.1.1
Server classification: Root Server

Number of regist 2 items (maximum 255 items) Add Update Delete Close

- 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 type: Other node
Node name, Computer name and IP address of changed Master Management Server
Server classification: Root Server

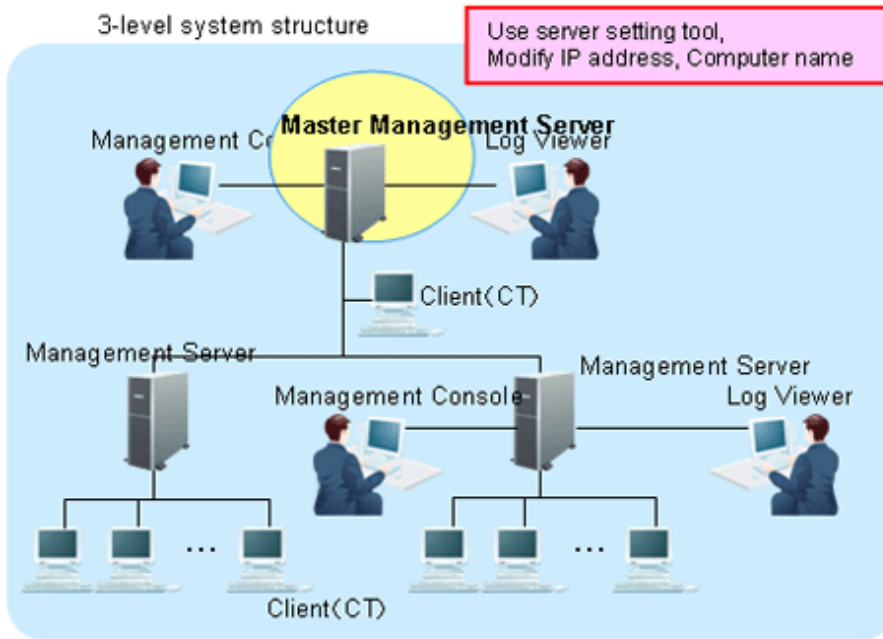
g. Click the **Close** button.

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.

Server Information Settings

Perform settings related to server.
For Master Management Server, please register own node (root server) only. The information of other node will be registered automatically.
For Management Server, please register the own node (sub-level server) and other node (root server) of Master Management Server
Lowercases of node name will be changed to uppercases before registration.
In addition, when closing the window, it might take much more time to confirm the integrity of node information and delete unnecessary management data.

List of nodes

Node type	Node name	Computer name	Server IP address or server name	Server classification	Update date and time	Registration date a...
Own node	DTKSV1	DTKSV1	192.168.1.1	root server	2015/05/17 14:19:00	2015/05/13 17:18:04
Other node	DTKSV2	DTKSV2	192.168.1.2	sub-level server	2015/05/17 14:20:47	2015/05/17 10:20:47

Node type: Node name: Server IP address or server name:

Computer name: Server classification:

Number of regist: 2 items (maximum 255 items)

- 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 type: Other node

Node name, Computer name and IP address of changed Master Management Server

Server classification: Root Server

e. Click the **Close** button.

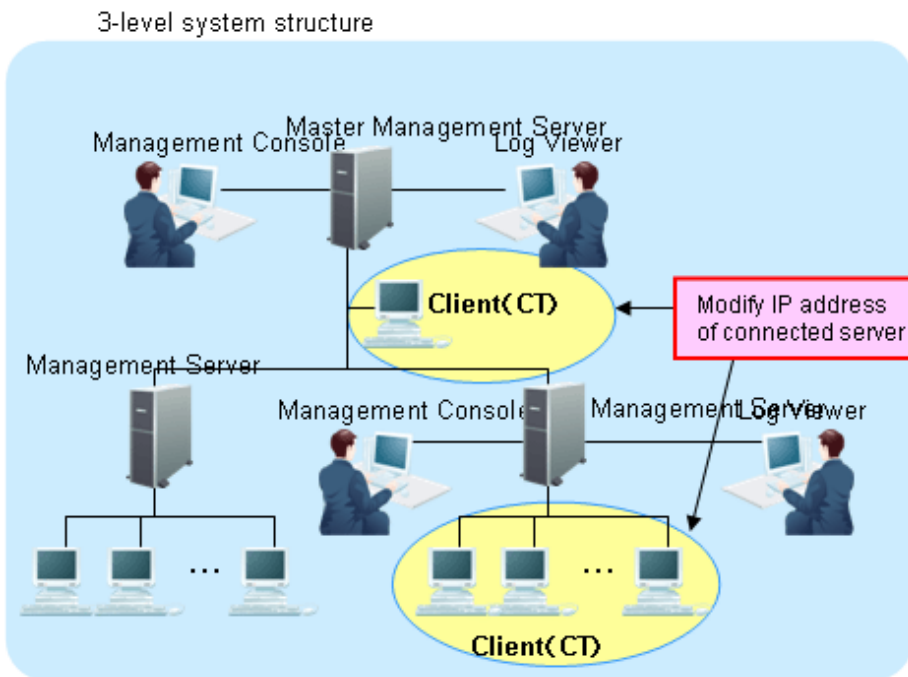
f. Start service.

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.

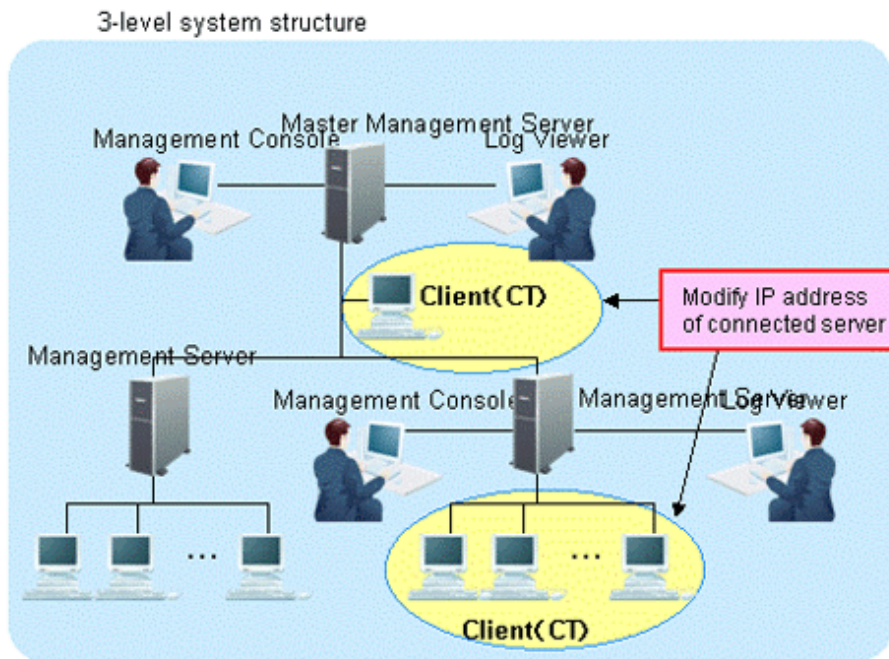
6. Change CT environment



For the following cases, 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

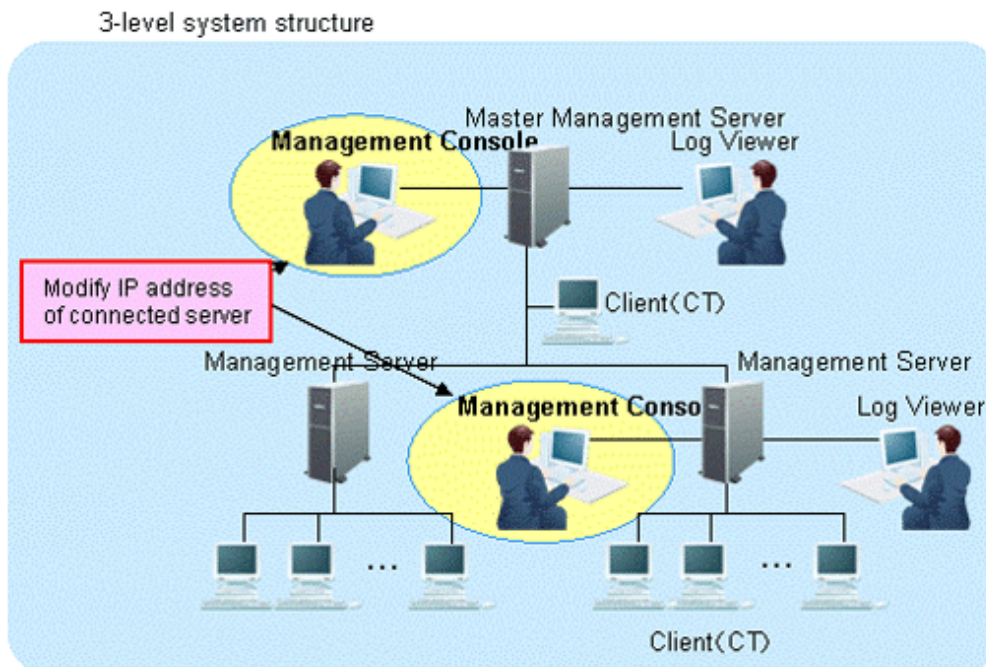
7. Change the Log Viewer environment



For the following cases, 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, 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.



Confirm the port number

Before changing the port number, refer to "Port Number List" of *Systemwalker Desktop Keeper Reference Manual* and confirm the port number being used.

1. Start the **Server Settings Tool**.
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, refer to "[Stop Management Server service](#)".

When Viewing Settings

Proceed to Step 3. If services are running, a confirmation window asking whether to display the **Management Server Settings** window should be displayed - click **Yes**.

- Click the **Management Server Settings** button.

The **Management Server Settings** window is displayed (the value set when the Management Server is installed is displayed).

Management Server Settings

Perform the setting related to communication environment of Management Server.

Server settings

Server IP address or server name: 192.168.1.1

Port number settings

Management Console <----->	Level Control Service	10015
Log Viewer <----->	Level Control Service	10022
Server Service ----->	Level Control Service	10012
Level Control Service ----->	Server Service	10017
Level Control Service (upper-level) ----->	Level Control Service(sub-level)	10008
Level Control Service (sub-level) ----->	Level Control Service(upper-level)	10008
Server Service ----->	CT	10010
CT ----->	Server Service	10010
Server Service ----->	CT(with Management Server installed)	10016
CT ----->	Server Service (image etc.)	10014
Management Server <----->	Operation Database	42050
Management Server <----->	Log Viewing Database	42051

Communication settings

Timeout value of communication between servers: 300 Second(s) (1~999)

Buttons: Set, Cancel

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. Specify a value from 5001 to 60000.
Log Viewer <-----> Level Control Service	This is the port number used in the communication between Log Viewer and level control service. Specify a value from 5001 to 60000.
Server Service ----->Level Control Service	This is the port number used in the communication from server service to level control service. Specify a value from 5001 to 60000.

Item Name	Description
Level control Service -----> Server Service	This is the port number used in the communication from level control service to server service. Specify a value from 5001 to 60000.
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). Specify a value from 5001 to 60000.
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). Specify a value from 5001 to 60000.
Server Service -----> CT	This is the port number used in the communication from server service to the client (CT). Specify a value from 5001 to 60000.
CT -----> Server Service	This is the port number used in the communication from the client (CT) to server service. Specify a value from 5001 to 60000.
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). Specify a value from 5001 to 60000.
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) Specify a value from 5001 to 60000.
Management Server <-----> Operation Database	Port number used for communication between the Smart Device Relay Server and the Operation Database on the Management Server. Specify a value from 1024 to 49151.
Server <-----> Log Viewing Database	Port number used for communication between the Smart Device Relay Server and the Log Viewing Database on the Management Server. Specify a value from 1024 to 49151.

Communication settings

Item Name	Description
Timeout value of communication between servers	Timeout value (in seconds) for connection attempt among Management Console, Log Viewer, level control service, server service and between upper level control service and lower level control service. Specify a value from 1 to 999.

4. 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, 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.

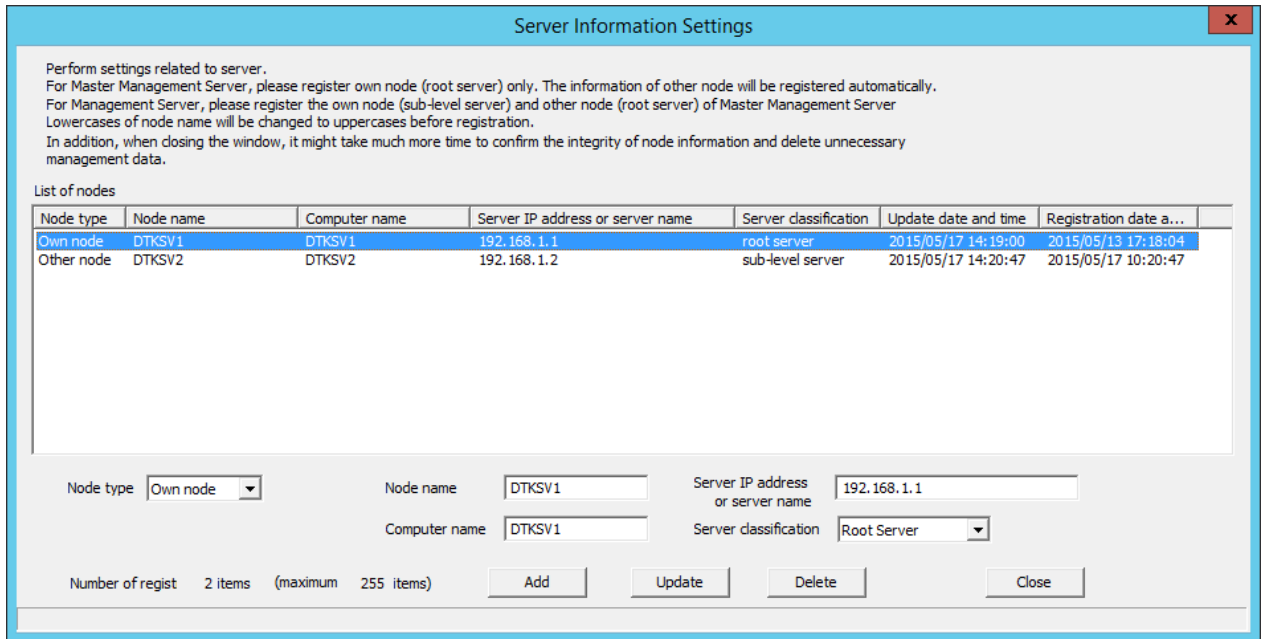
It will take 30 seconds to 1 minute before stopping. In addition, immediately after you restart SWServerService or after the date has changed (00:00), available space in the database will be checked. This check operation takes about 15 minutes, and services may not stop during this time. Wait a while and then check if the services have stopped.

- SWLevelControlService
- SWServerService

In a 3-level structure, stop the services of all Management Servers/Master Management Servers.

2. Back up the management information and log information in the computer of the transfer source.
For the backup method, 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, 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, immediately after you restart SWServerService or after the date has changed (00:00), available space in the database will be checked. This check operation takes about 15 minutes, and services may not stop during this time. Wait a while and then check if the services have stopped.
 - SWLevelControlService
 - SWServerService
6. Restore the backup data using restoration tool in the transfer target computer.
For the restoration method, 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, 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, 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. Before the transfer, in the computer (currently in operation), backup the Log Analyzer Server information file (LA_connect_Info.csv) to the external media.

The saving target of setting file is as follows:

```
[Systemwalker Desktop Keeper Installation Folder]\LogAnalyzer\TRANS
```

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 Log Analyzer Server information file (LA_connect_Info.csv) that is backed up to external media to the transfer target computer and register the Log Analyzer Server information again using the Log Analyzer setting tool.

The saving target of setting file is as follows:

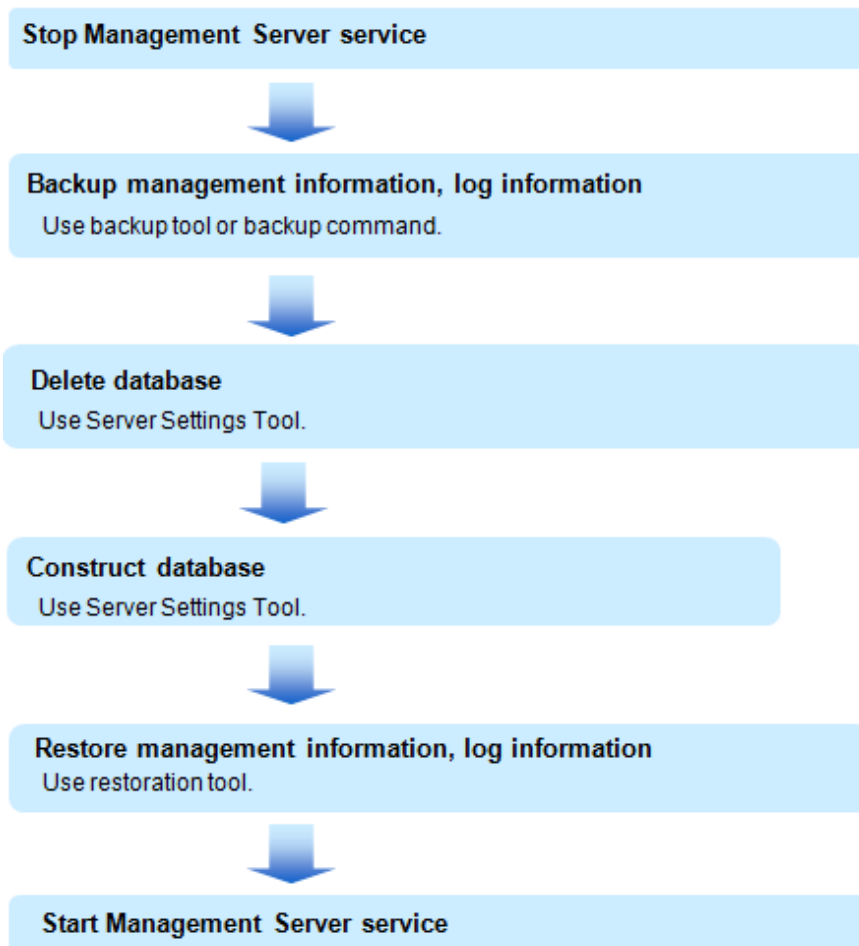
```
[Systemwalker Desktop Keeper Installation Folder]\LogAnalyzer\TRANS
```

7.10 Reconstruct Database of Management Server

When modifying the database capacity during operation, the Server Settings Tool can be used.

In database reconstruction, the current database will be deleted temporarily. Therefore, 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.

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, refer to "Use Backup Tool (GUI)" and "Use Backup Command" of *Systemwalker Desktop Keeper Installation Guide*.



Note

Make sure to back up management information and log information.

The database will be initialized through the reconstructing database. Make sure to backup management information and log information before database reconstruction. When it is not implemented, the system cannot be restored.

Delete the database

Delete the database using the Server Settings Tool. Refer to "Delete the database of Management Server/Master Management Server" in the *Systemwalker Desktop Keeper Installation Guide* for details.

Construct the database

Construct the database using the Server Settings Tool. Refer to "Construct Database" in the *Systemwalker Desktop Keeper Installation Guide* for details.

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.

Refer to "Use Restoration Tool" of *Systemwalker Desktop Keeper Installation Guide* for restoration method of management information and log information.

Start Management Server service

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 the Management Server 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, refer to "Construct Log Viewing Database" of *Systemwalker Desktop Keeper Installation Guide*.

7.12 Change Log Analyzer Environment

This section describes how to change the Log Analyzer 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: 20130421_20130421).

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 (or host name) and port number of the Log Analyzer Server is modified during operation.

The following settings can be performed on Master Management Server:

1. Click **Start > Systemwalker Desktop Keeper > Server > Log Analyzer settings**, or **Apps > Systemwalker Desktop Keeper > Log Analyzer settings**, to start the **Log Analyzer settings** window.
2. Click the **Server Information Settings** tab.

The screenshot shows the "Log Analyzer Server Settings" window with the "Server Information Settings" tab selected. The window contains a table for "Log analyzer server information" and input fields for "IP address or host name (I)", "Communication port 1 (P)", and "Communication port 3 (C)".

IP address or host name	Communication port 1	Communication port 3
localhost		30004

IP address or host name (I)

Communication port 1 (P)

Communication port 3 (C)

3. From the Log Analyzer Server information list, select a target Log Analyzer Server.
4. Click **Delete** to delete the target Log Analyzer Server.
5. Enter the IP address or host name, communication port 1, and communication port 3 for the Log Analyzer Server.
6. Click **Add** to add the Log Analyzer Server information.
7. Click **Set** to register the Log Analyzer Server information again.
8. 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:

- 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":

Modify the path of shared folder before change to "\\192.168.2.1\LASVDATA".

For details, 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 connection destination/port number of the **Server** tab to the new IP address/port number.

For details, refer to "Set Report Output Environment" of *Systemwalker Desktop Keeper Installation Guide*.

7.12.3 Change the Data Transfer Task on the Management Server

This section describes how to change the settings for the task to transfer data (such as log and user information) from the Management Server to the Log Analyzer Server.

It is recommended that the transfer process is performed every day, and the example below assumes that it is.

Ensure that no user is accessing the shared folders during data transfer to the Log Analyzer Server.

If you were accessing the shared folders as another user, you must disconnect from the network or log off.

It takes approximately 25 minutes to transfer approximately 5 million logs. The actual time taken will vary depending on factors such as PC performance and network state.



Note

For the data transfer start time, specify a time of day during which few users are using the client (CT).

That is recommended because the Management Server services below will be stopped while the log data is saved and sent as part of data transfer:

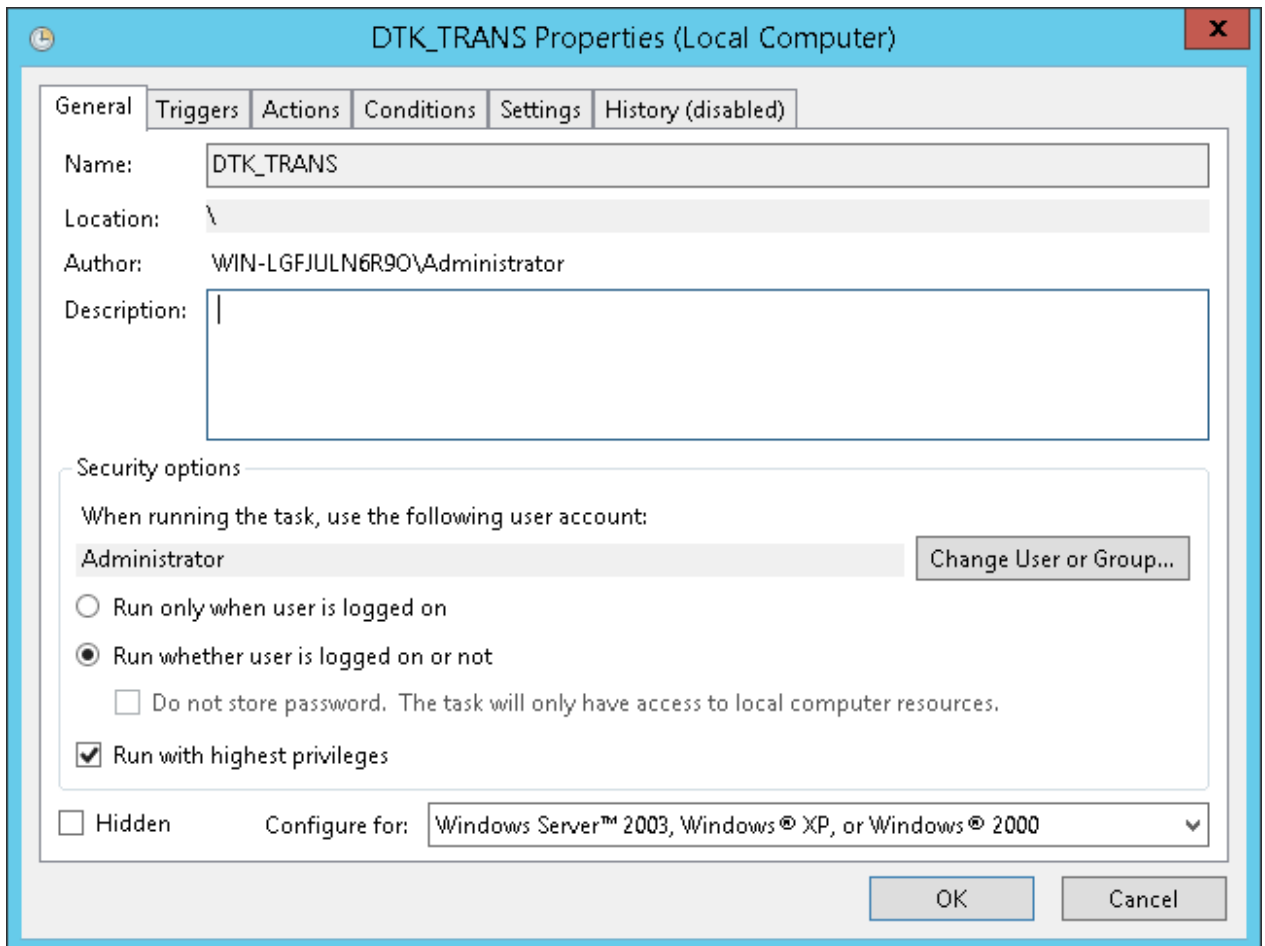
- SWLevelControlService
- SWServerService

Note that immediately after restarting SWServerService or after the date has changed (00:00), available space in the database will be checked. This check operation takes approximately 15 minutes, and services may not stop during this time. Therefore, do not perform data transfer in the above timeframe.

Follow the procedure below:

Settings on Windows Server(R) 2008 and Windows Server(R) 2012

1. Select **Task Scheduler** on Windows.
The **Task Scheduler** window will be displayed.
2. From **Task Scheduler Library**, right-click **DTK_TRANS**, and then click **Properties**.
The **Properties** window will be displayed.



3. Click the **General** tab, set the information below, and then click **OK**.
 - In **When running the task, use the following user account**, click **Change User or Group** and specify a user with administrator privileges.
 - Select **Run whether user is logged on or not**.
 - Select **Run with highest privileges**.

4. Click the **Triggers** tab, and click **Edit**.
The **Edit Trigger** window will be displayed.

Edit Trigger

Begin the task: On a schedule

Settings

One time

Daily

Weekly

Monthly

Start: 5/13/2015 2:00:00 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

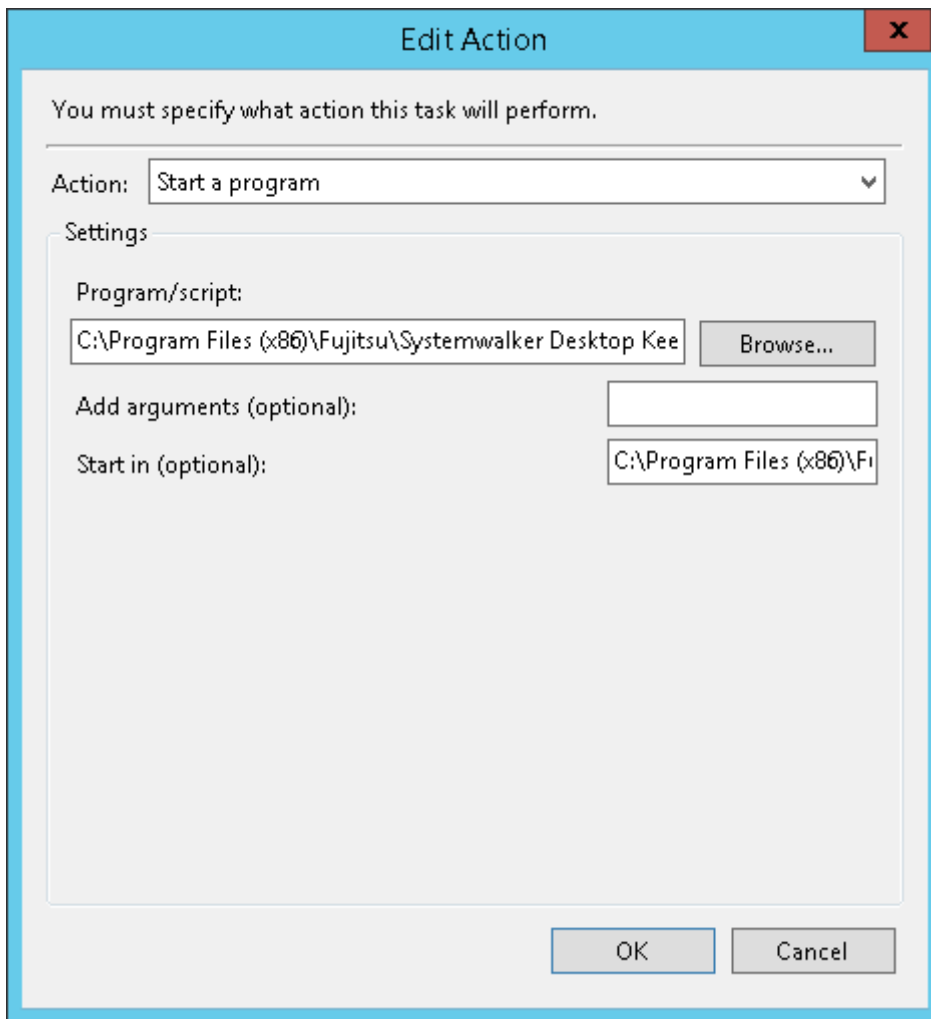
Expire: 5/12/2016 4:59:38 PM Synchronize across time zones

Enabled

OK Cancel

5. In **Settings**, set the information below, and then click **OK**.
- Select **Daily**.
 - In **Start**, set the start date and time. For the start time, specify the time of day such as night time during which few users are using the client (CT).
 - Set **Recur every** to **1**.

- Click the **Actions** tab, and click **Edit**.
The **Edit Action** window will be displayed.



- In **Settings**, set the information below, and then click **OK**.
 - **Program/script:** Specify the full path (enclosed in double quotations marks) of the TRANS.bat file:

`"dtk\instal\Folder\LogAnalyzer\TRANS\TRANS.bat"`
 - **Start in (optional):** Specify the full path of the folder in which TRANS.bat specified in **Program/script** is stored. Do not enclose the value in double quotation marks.
- Click **OK** in the **Properties** window.

Information

Log data transfer can also be executed manually.

- In the command prompt window, navigate to the TRANS folder under the folder in which the product was installed.

```
cd dtk\instal\Folder\LogAnalyzer\TRANS
```

- Execute the following batch file to save the log data as a CSV file and send it to the Log Analyzer Server.

```
TRANS.bat
```

If the command is executed as above, the command prompt window will be closed automatically upon completion. To leave the command prompt window open, execute the batch file as follows:

```
cmd /c TRANS.bat
```

7.12.4 Change the Data Import Task on the Log Analyzer Server

This section describes how to change the settings for the task to store data such as log and user information transferred from the Management Server to the Log Analyzer Server database.

It is recommended that the log storing process in to the database is performed every day, and the example below assumes that it is.

Once data import in to the Log Analyzer Server is performed, the imported logs are aggregated at the same time as the import of the log data, and the aggregation result will be updated.

At this time, the difference between the aggregation results before and after the data import will be output as a log.

- Log output destination

```
logAnalyzerServerInstallFolder\bin\batchnavi\update0.log
```

If the file size exceeds 10 MB, update0.log is renamed as update1.log, and update0.log is created. Up to update4.log will be created sequentially. The latest information will always be recorded in update0.log.

- Log text output

```
-----  
Output update information of aggregation at 2015/05/13 10:00:39
```

```
Start
```

```
20150513 OperationDay20150512 InformationDisclosure(0,0,0,0,0,0) TerminalUsing(13,0,64) ViolationOperation(0,0,0,0,0)  
PrintVolumeMonitoring(0)
```

```
End  
-----
```

In the example above, the number of logs operated on April 8, 2013 and April 9, 2013 has been updated as a result of aggregating the data imported on April 21, 2013, and the number of differences updated is displayed in parentheses.

The numbers in parentheses are differences in each log as shown below:

- InformationDisclosure (file export, file operation, print operation(times), print operation(pages), e-mail sending by recipient)
- TerminalUsing (window title with URL obtained, e-mail sending by recipient, application startup)
- Violation (application startup prohibition, print prohibition, logon prohibition, PrintScreen key prohibition, e-mail attachment prohibition)
- PrintVolumeMonitoring (number of printing operations)

Logs are displayed in the report output using the Report Output Tool. Only InformationDisclosure is displayed in the **Information Disclosure Prevention Diagnosis** window in the web console.

It takes approximately 80 minutes to import approximately 10 million logs. The actual time taken will vary depending on factors such as CPU performance, PC memory and disk capacity, and operational status of other applications.



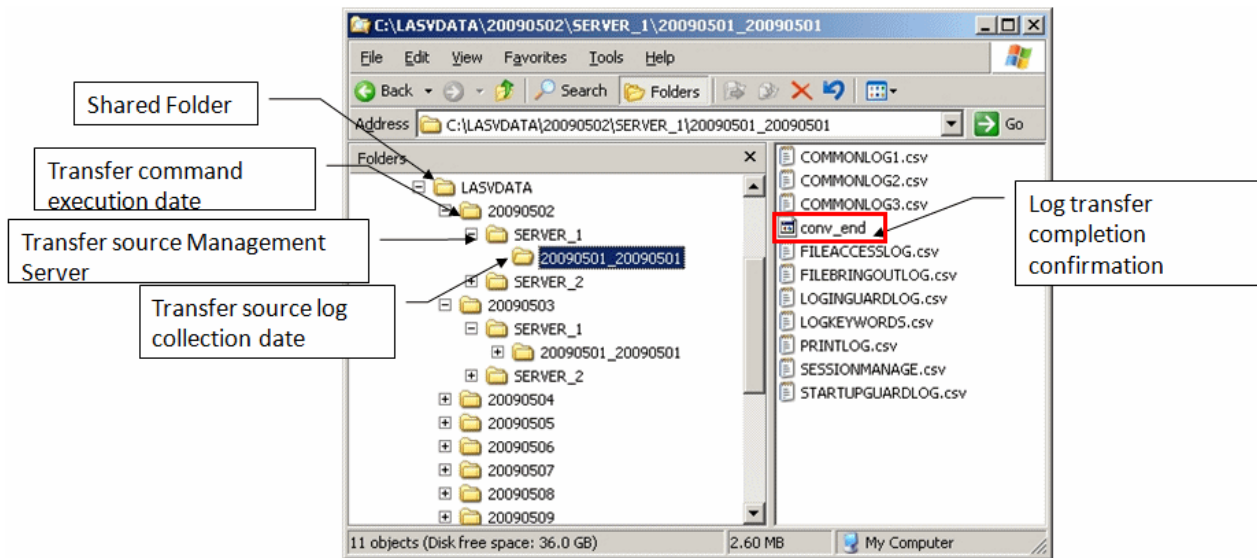
Note

To secure disk space, regularly back up CSV log files no longer required to the external media

The CSV log files sent from the Management Server to the Log Analyzer Server will remain on the Log Analyzer Server disk even after they are stored in the Log Analyzer Server database.

If shared folders are depleted, log transfer from the Management Server or Master Management Server will fail. To avoid this, regularly check the space on shared folders and back up the logs already analyzed and aggregated before deleting them.

The shared folders on the Log Analyzer Server are typically structured as follows:



Note that logs that have not been analyzed nor aggregated on the Log Analyzer Server cannot be backed up nor deleted.

If the Transfer source log collection date folder contains the log transfer completion confirmation file (conv_end), it means that log analysis and aggregation have been completed for the folder, and it has been stored in the database on the Log Analyzer Server.

In the figure above, the shared folder can be backed up and deleted if the log transfer completion confirmation file (conv_end) exists in each Transfer source log collection date folders under each Transfer source Management Server folder under the Transfer command execution date folder. Back up and delete each Transfer command execution date folder.

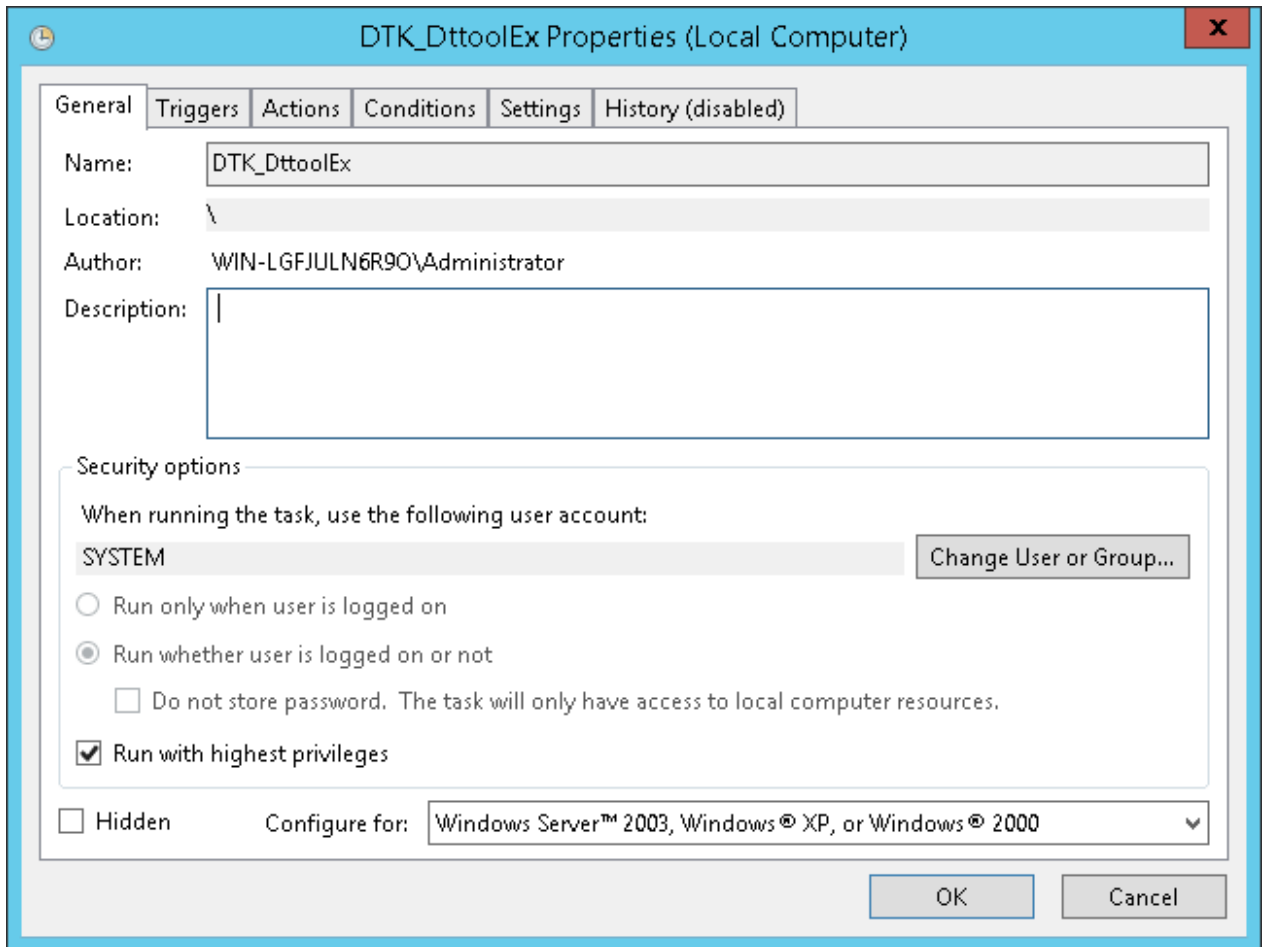


Follow the procedure below:

Settings on Windows Server(R) 2008 and Windows Server(R) 2012

1. Select **Task Scheduler** on Windows.
The **Task Scheduler** window will be displayed.

2. From **Task Scheduler Library**, right-click **DTK_DttoolEx**, and then click **Properties**. The **Properties** window will be displayed.



3. Click the **General** tab, set the information below, and then click **OK**.
- In **When running the task, use the following user account**, click **Change User or Group** and specify a Log Analyzer user.
 - Select **Run whether user is logged on or not**.
 - Select **Run with highest privileges**.

4. Click the **Triggers** tab, and click **Edit**.
The **Edit Trigger** window will be displayed.

Edit Trigger

Begin the task: On a schedule

Settings

One time

Daily

Weekly

Monthly

Start: 5/13/2015 3:00:00 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

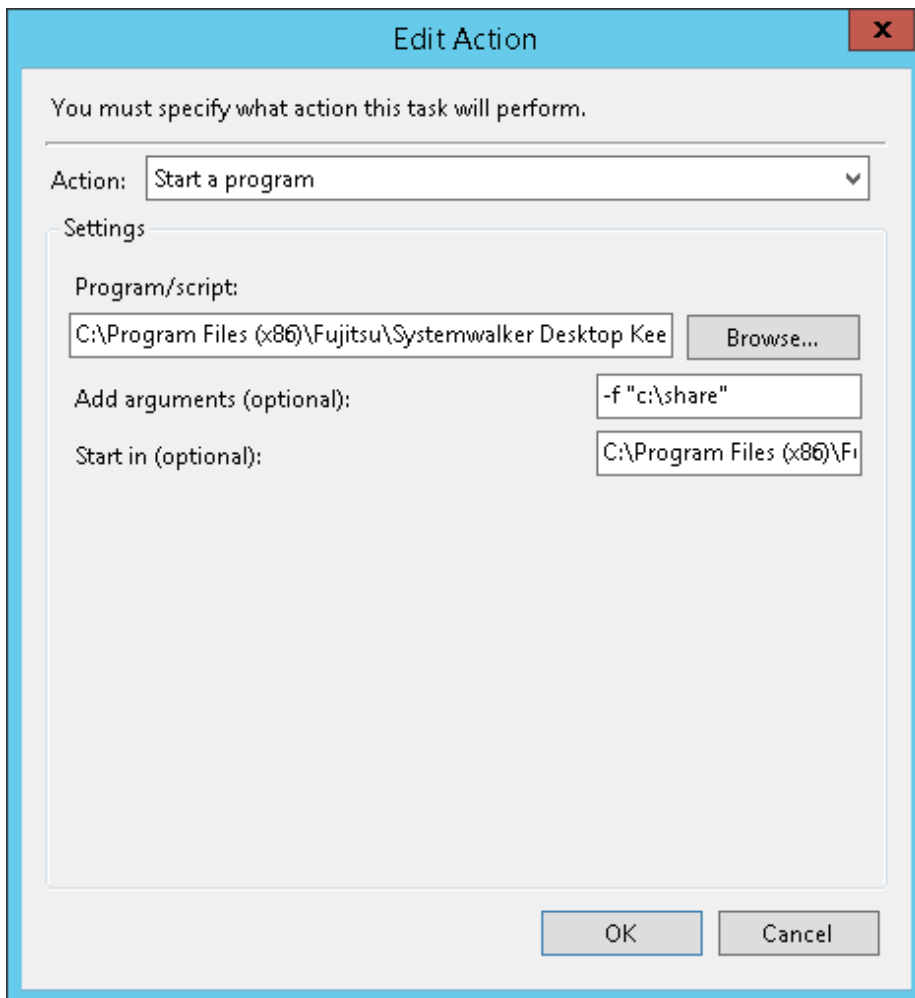
Expire: 5/12/2016 5:11:39 PM Synchronize across time zones

Enabled

OK Cancel

5. In **Settings**, set the information below, and then click **OK**.
 - Select **Daily**.
 - Set **Start** to a time after the task start time of the data transfer command, so that the task will be executed after the data transfer command is executed.
 - Select **Repeat task every**, select the interval and **for a duration of**.

- Click the **Actions** tab, and click **Edit**.
The **Edit Action** window will be displayed.



- In **Settings**, set the following information and click **OK**.

- **Program/script:** Specify the full path (enclosed in double quotation marks) of the DttoolEx.exe file:

`" / logAnalyzerServerInstallFolder\bin\dttool\DttoolEx.exe "`

- **Add arguments (optional):** Specify *logTransferDestinationSharedFolderPath* (enclosed in double quotation marks) in local path format, not in UNC format.
- **Start in (optional):** Specify the full path of the folder in which DttoolEx.exe specified in **Program/script** is stored. Do not enclose the value in double quotation marks.

- Click **OK** in the **Properties** window.

Information

Data can also be imported manually.

- In the command prompt window on the Log Analyzer Server, navigate to the folder in which the tool is stored, under the folder in which the Log Analyzer Server is installed:

`cd / logAnalyzerServerInstallFolder\bin\dttool`

2. Execute the following command to add the data to the Log Analyzer Server database.

```
DttoolEx.exe -f /logTransferDestinationSharedFolderPath
```

7.13 Change the Smart Device Relay Server Environment

This section explains how to change the Smart Device Relay Server environment.

7.13.1 Change the Connection Destination (Master) Management Server

This section describes how to change the connection destination (Master) Management Server for the Smart Device Relay Server.

When changing the Smart Device Relay Server from the Management Server change source to the Management Server change destination

1. Configure the publishing setting for the database (Management Server change destination)

Follow the procedure in "Configuring the Publishing Settings for the Database (Master Management Server or Management Server)" in "Building a Smart Device Relay Server Environment" in the *Systemwalker Desktop Keeper Installation Guide*.

2. On the Smart Device Relay Server, follow the procedure below:

- a. Stop the Smart Device Relay Server

Use SDSVService.bat (Start/Stop Service of Smart Device Relay Server) to stop the service of the Smart Device Relay Server.

- b. Execute SDSVSetMS.exe (Change Configuration of Smart Device Relay Server)

Use SDSVSetMS.exe (Change Configuration of Smart Device Relay Server) to change the Systemwalker Desktop Keeper (Master) Management Server IP address and port number registered on the Smart Device Relay Server to the Management Server destination IP address and port number.

- c. Start the Smart Device Relay Server

Use SDSVService.bat (Start/Stop Service of Smart Device Relay Server) to start the service of the Smart Device Relay Server.

Refer to "Command Reference" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

7.13.2 Change the Smart Device Relay Server IP Address

This section describes how to change the Smart Device Relay Server IP address.

When managing both Android devices and iOS devices

Follow the procedures below for managing Android devices, and the procedure for managing iOS devices.

When managing Android devices

1. Use SDSVService.bat (Start/Stop Service of Smart Device Relay Server) to stop the service of the Smart Device Relay Server.
2. If using HTTPS communication, follow the procedure in "Configuring HTTPS Communication" in the *Systemwalker Desktop Keeper Installation Guide*.
If using the same CA as the one at installation, however, do not use SDSVImportCert.EXE (Register Certificate) to register the CA certificate (intermediate CA certificate).
This procedure is also executed when iOS smart devices are managed. If managing iOS devices as well, execute this only once.
3. If the service of the Smart Device Relay Server is stopped, use SDSVService.bat (Start/Stop Service of Smart Device Relay Server) to start the service of the Smart Device Relay Server.
4. Notify the Android device users of the URL to synchronize with the Smart Device Relay Server.
5. The users who are notified of the URL should follow the instruction in the notification to configure the smart device (agent) (Android).

Refer to "Command Reference" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

When managing iOS devices

1. Use SDSVService.bat (Start/Stop Service of Smart Device Relay Server) to stop the service of the Smart Device Relay Server.
2. Use SDSVSetMS.exe (Change Configuration of Smart Device Relay Server) with the -iOS.connect.h option to set the Smart Device Relay Server or reverse proxy that is to be connected to from the iOS device.
3. Follow the procedure in "Configuring HTTPS Communication" in the *Systemwalker Desktop Keeper Installation Guide*.
If using the same CA as the one at installation, however, do not use SDSVImportCert.EXE (Register Certificate) to register the CA certificate (intermediate CA certificate).
This common procedure also applies to managed Android devices. If managing Android devices as well, execute this only once.
4. If the service of the Smart Device Relay Server is stopped, use SDSVService.bat (Start/Stop Service of Smart Device Relay Server) to start the service of the Smart Device Relay Server.
5. Follow the procedure in "Uninstalling the Smart Device (Agent) (iOS)" in the *Systemwalker Desktop Keeper Installation Guide*, and uninstall the CA certificate (server), CA certificate (client), and MDM profile.
6. Follow the procedure in "Installing the Smart Device (Agent) (iOS)" in the *Systemwalker Desktop Keeper Installation Guide*, and install the smart device (agent) (iOS) again.

Refer to "Command Reference" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

7.13.3 Install and Add Systemwalker Desktop Patrol

If you are installing and adding Systemwalker Desktop Patrol to the same machine operating Systemwalker Desktop Keeper, you must reinstall the smart device (agent) (iOS) on the iOS device. This procedure is only required when you are managing iOS devices.

Follow the procedure below:

1. If the service of the Smart Device Relay Server is stopped, use SDSVService.bat (Start/Stop Service of Smart Device Relay Server) to start the service of the Smart Device Relay Server.
Refer to "SDSVService.bat (Start/Stop Service of Smart Device Relay Server)" in the *Systemwalker Desktop Keeper Reference Manual* for details.
2. Follow the procedure in "Uninstalling the Smart Device (Agent) (iOS)" in the *Systemwalker Desktop Keeper Installation Guide*, and uninstall the CA certificate (server), CA certificate (client), and MDM profile.
3. Follow the procedure in "Installing the Smart Device (Agent) (iOS)" in the *Systemwalker Desktop Keeper Installation Guide*, and install the smart device (agent) (iOS) again.

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.



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, refer to "[1.2.8 File Export Prohibition](#)" - "[1.2.17 Application Usage Prohibition \(Smart Device\)](#)".

- File export prohibition
- File reading prohibition
- Printing prohibition
- Logon prohibition
- Application startup prohibition
- PrintScreen key prohibition
- URL access prohibition
- FTP server connection prohibition
- Web upload prohibition
- Web download prohibition
- Clipboard operation prohibition
- Wi-Fi connection prohibition (smart device)
- Bluetooth connection prohibition (smart device)
- Application usage prohibition (smart device)
- Device functionality (iOS device)
- Applications (iOS device)
- iCloud (iOS)
- Security and privacy (iOS)
- Content ratings (iOS)

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.

Note

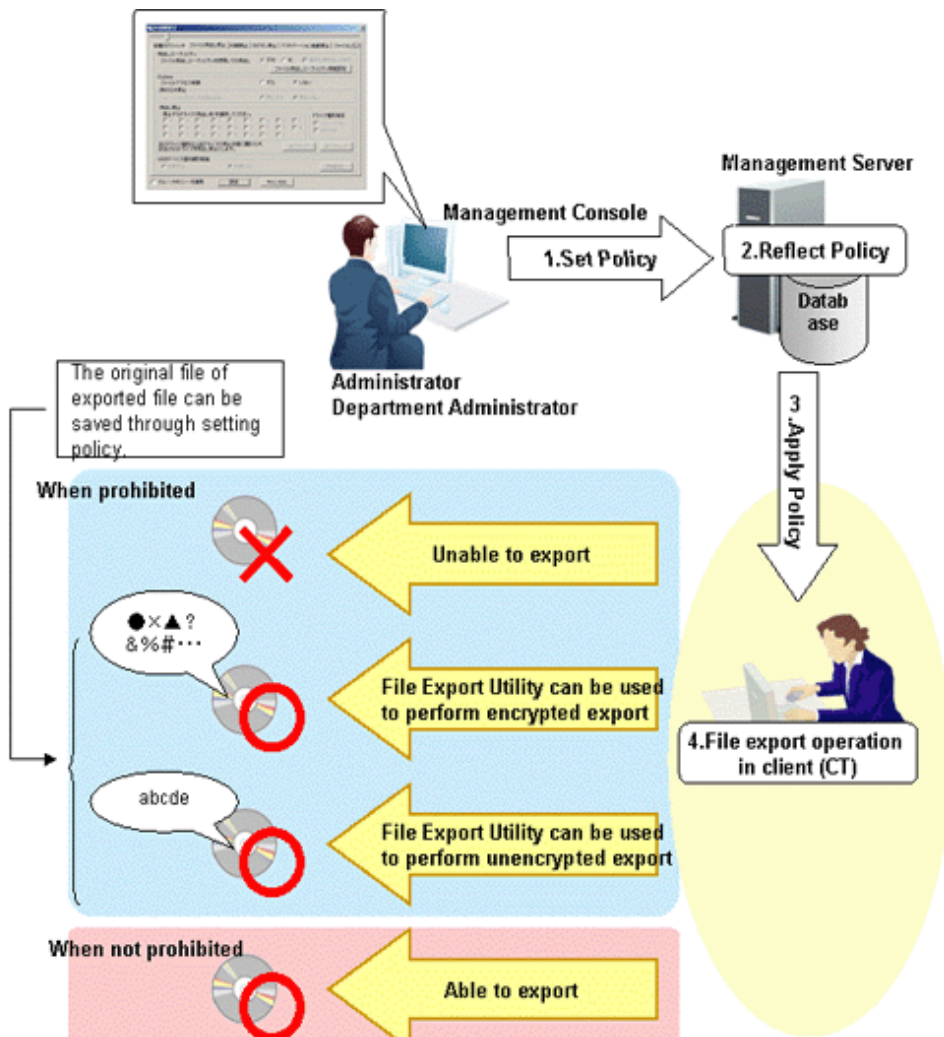
Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.
For details, 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", refer to "1.2.6 Export Utility" and "Systemwalker Desktop Keeper User'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 **File export/read**.
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
- Able to export using File Export Utility
- Able to export

When exporting to DVD/CD, the operations will be different according to the media. For details, refer to "[1.2.8 File Export Prohibition](#)" and "[1.2.6 Export Utility](#)".

For operations, refer to *Systemwalker Desktop Keeper User's Guide for Client*.

When prohibited

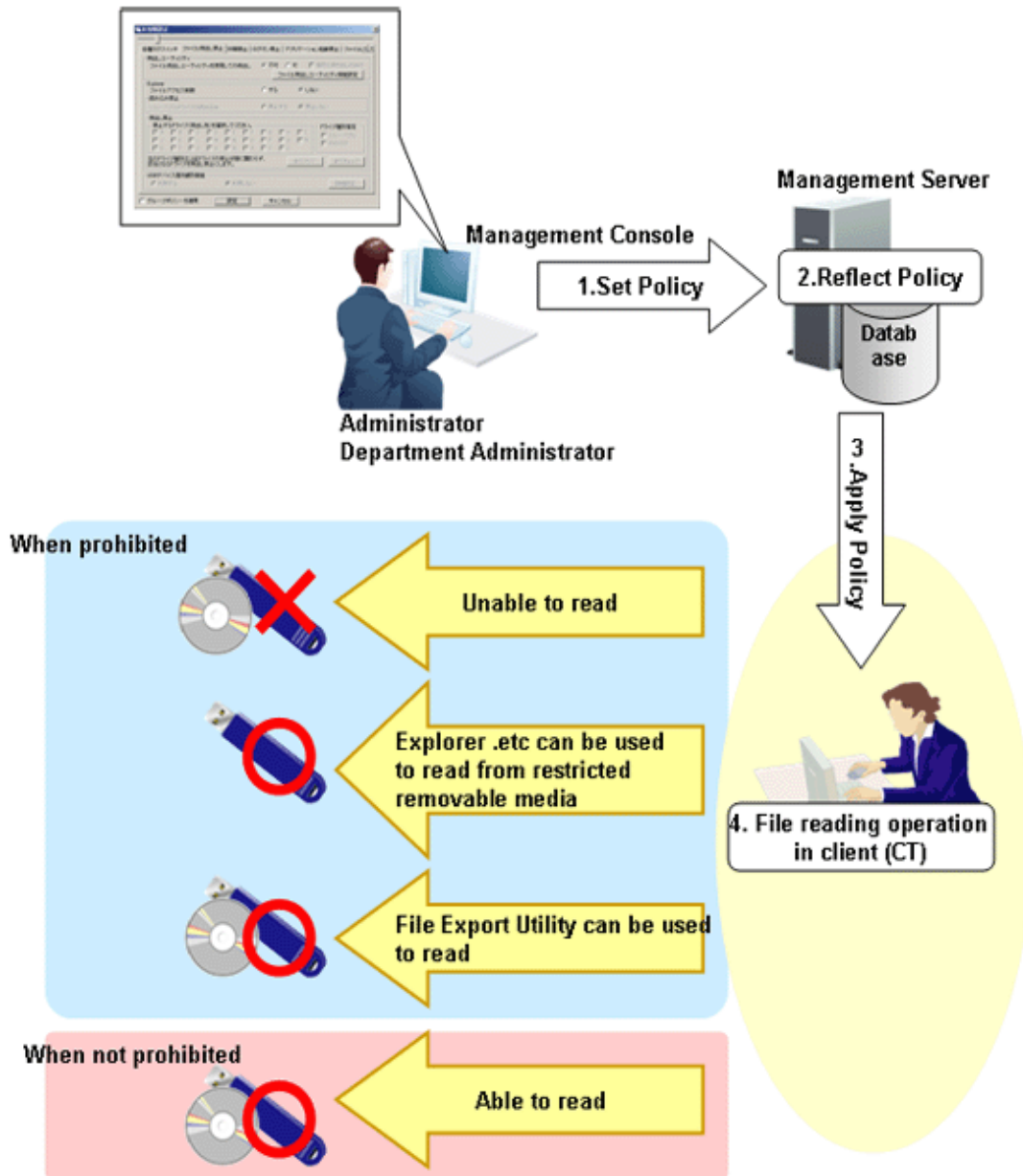
- When intending to export files and folders to the drive of a prohibited target without using "File Export Utility", the following message will be displayed in the client (CT).

You need permission to perform this action.

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, or portable device/imaging device (such as digital camera, IC recorder or scanner), 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 **File export/read** to **Yes**.

Select the media prohibited to be read in **Reading prohibition** of **File export/read**.

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: Set a policy that disables the use of File Export Utility.

Note 2: Limit the available removable media in **USB Device Individual Identification Function** of the **File export/read**. USB devices that are not specified cannot be read. For how to register and set permitted USB devices, 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.

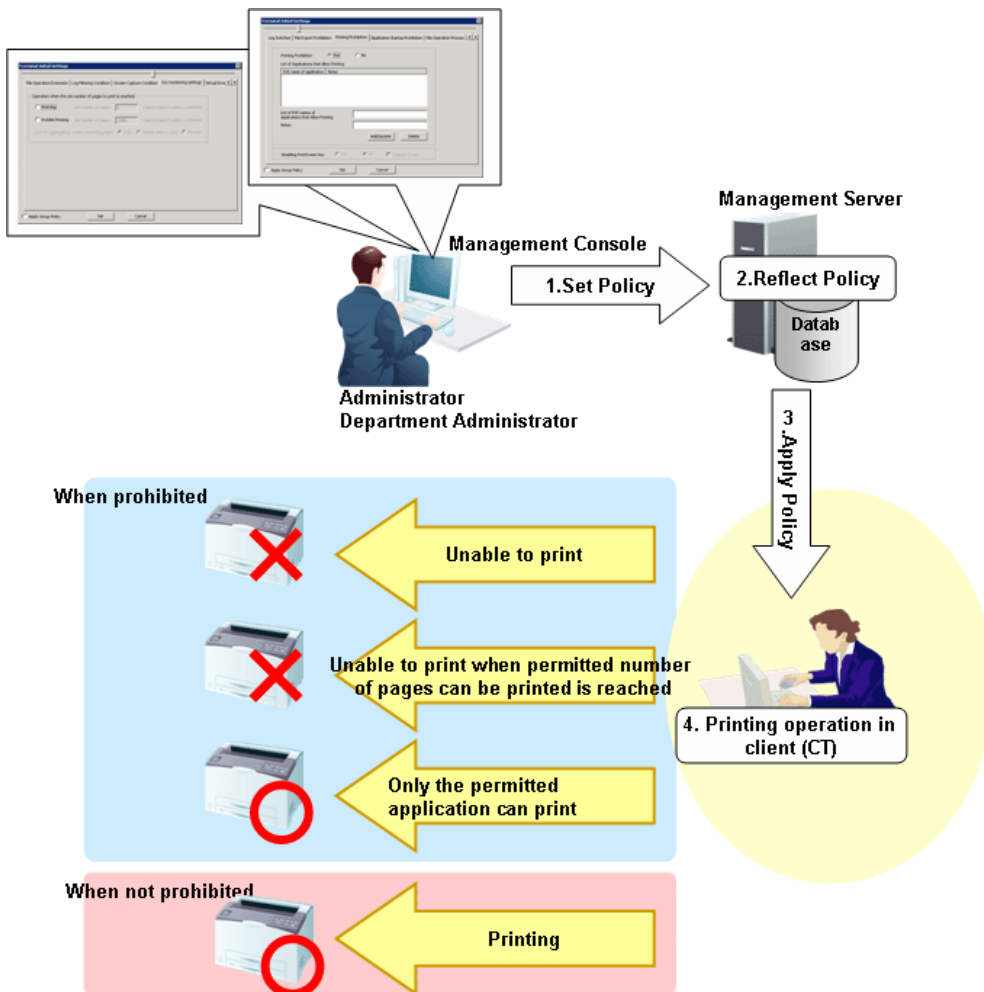


Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

For details, 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 **Print/PrintScreen**.

Set the conditions for prohibiting printing in **Eco monitoring**.

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 following message will be displayed in the client (CT). An example is shown below:

[D901-INF001] The print function of this application is prohibited by the system administrator.

8.1.4 Logon Prohibition

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:

- Microsoft accounts

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.

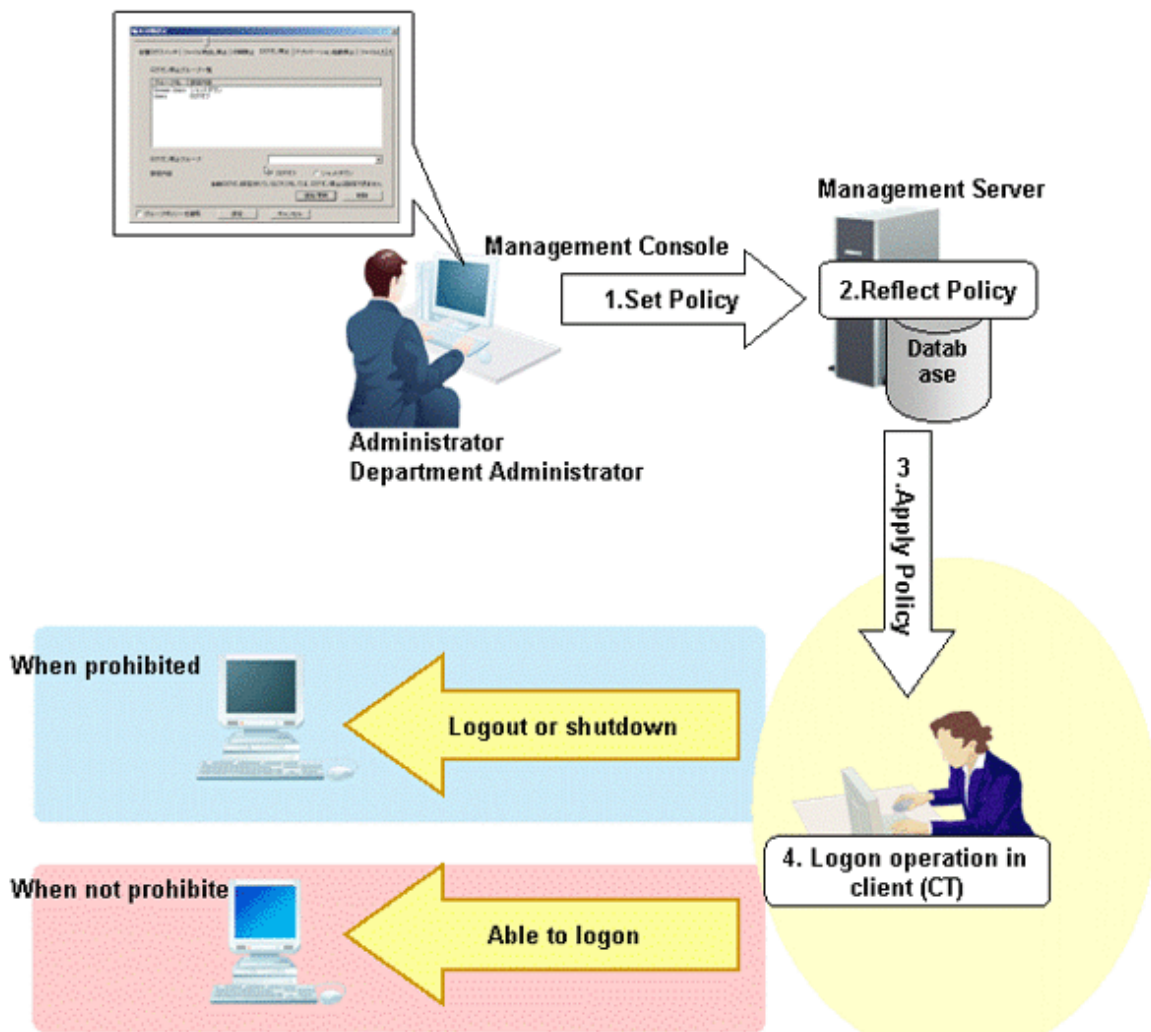
Note

Users belonging to a group within a group specified as prohibited from logon are not prohibited from logging on.

Example: In the following configuration, User A is not prohibited from logging on.

- Group prohibited from logging on: Microsoft accounts
- Group belonging to Microsoft accounts: Group1
- Users belonging to Group1: User A

Steps to make prohibition effective through policy setting



1. Set Policy

Set the group prohibited from logon in the **Terminal Initial Settings** window or **Logon** 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 message will not be displayed.

- When the client (CT) is logged off

```
[E601-INF001] The user name is prohibited by system to log on.  
It will be logged off by force after 30 seconds.
```

- When the client (CT) is shut down

```
[E601-INF001] The user name is prohibited by system to log on.  
It will be shutdown by force after 30 seconds.
```

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.

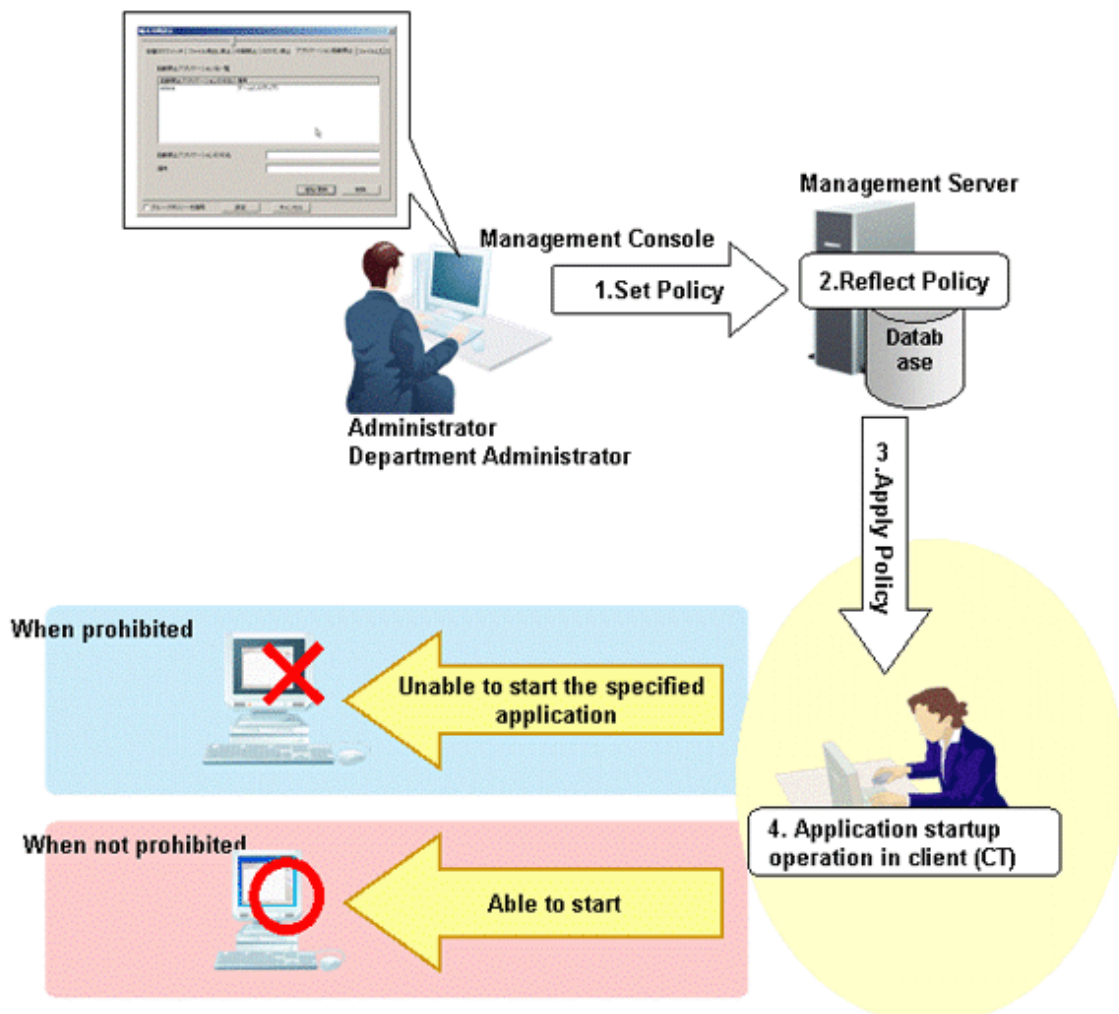


Functions may be restricted due to the environment being used

When setting the policy, functions may be restricted due to the environment being used.

For details, 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 **Application**.
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 following message will be displayed in the client (CT).

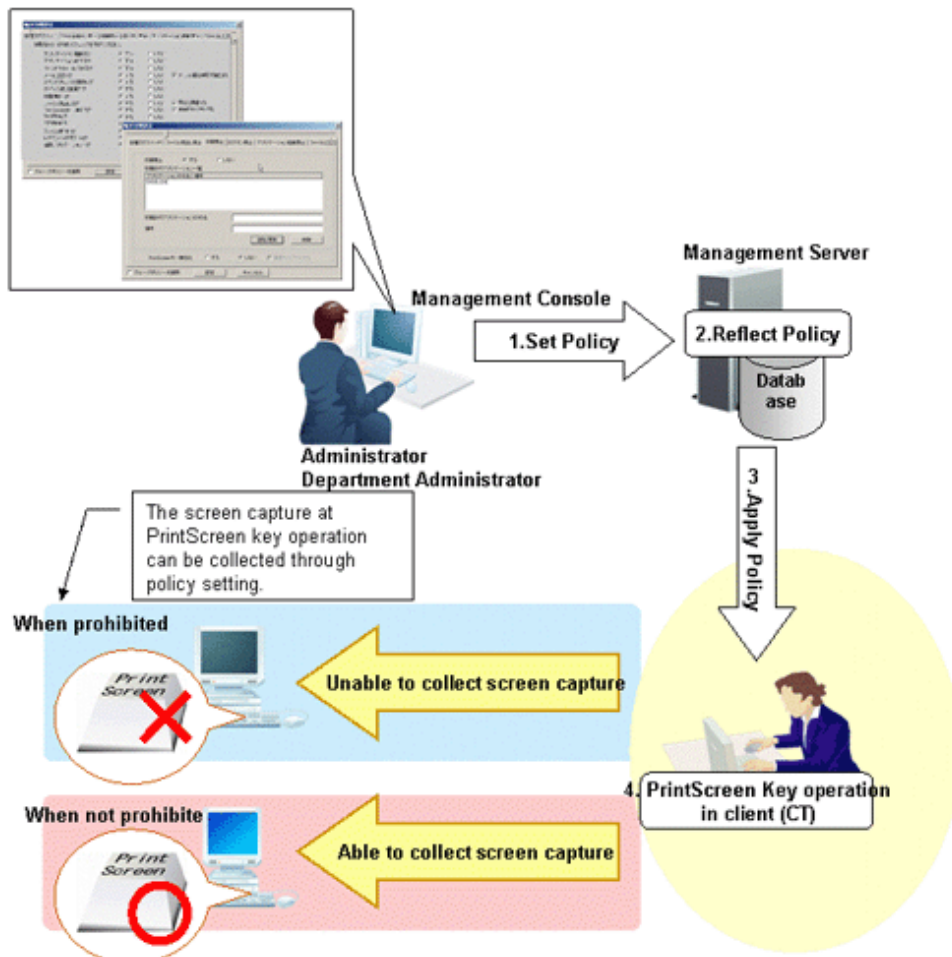
```
[D101-INF001] This application is prohibited by the system administrator.
```

8.1.6 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 **Print/PrintScreen**.

When collecting the window with the PrintScreen key operation, select the **Capture Screen** check box.

Point

In **Print/PrintScreen**, you can set **Disabling PrintScreen Key** if **PrintScreen Key Operation Log** has been set as disabled in **Windows > Log collection operation**.

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** check box 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 following message will be displayed in the client (CT). When the collection of screen capture during prohibition is set, the screen capture at PrintScreen key operation will be collected.

[D901-INF002] The PrintScreen key has already been prohibited.
--

8.1.7 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.



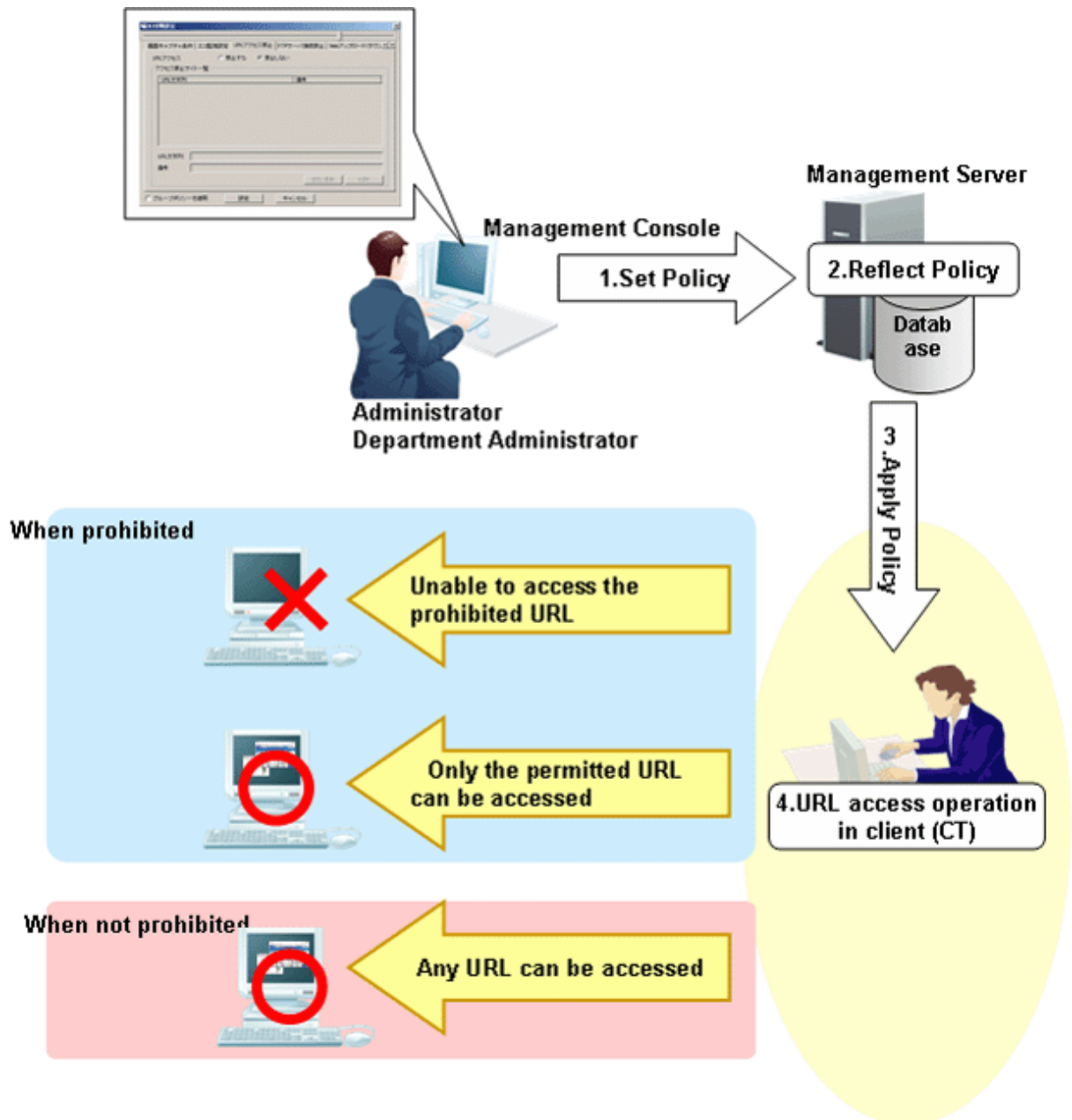
.....

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, 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 **Internet**.
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 browser, Internet Explorer(R) will be closed by force when accessing the prohibited URL. When there are multiple tabs displayed on the Web browser, only the tab that accesses the prohibited URL will be closed by force. Then, the following message will be displayed.

```
Accessing to this Web site is prohibited by system administrator.  
(Web site URL prohibited to be accessed: <URL>)
```

8.1.8 FTP Server Connection Prohibition

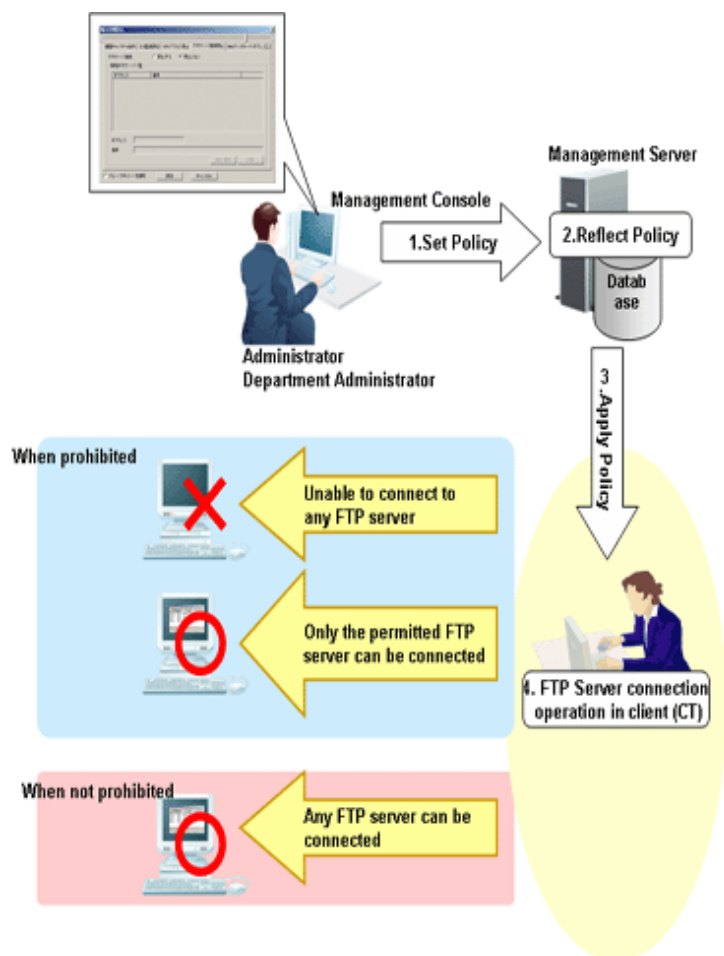
By setting the FTP server connection prohibition policy, access to the FTP server that is not permitted by the administrator can be prohibited in the client (CT) PC.



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, 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 **FTP server connection**.

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.

```
[E002-INF002] Connecting to FTP server is prohibited by system administrator.
(FTP server address prohibited to be connected: ipAddress)
```

8.1.9 Web Upload Prohibition

By setting the Web upload prohibition policy, uploading to a Website that is not permitted by the administrator can be prohibited in the client (CT) PC.



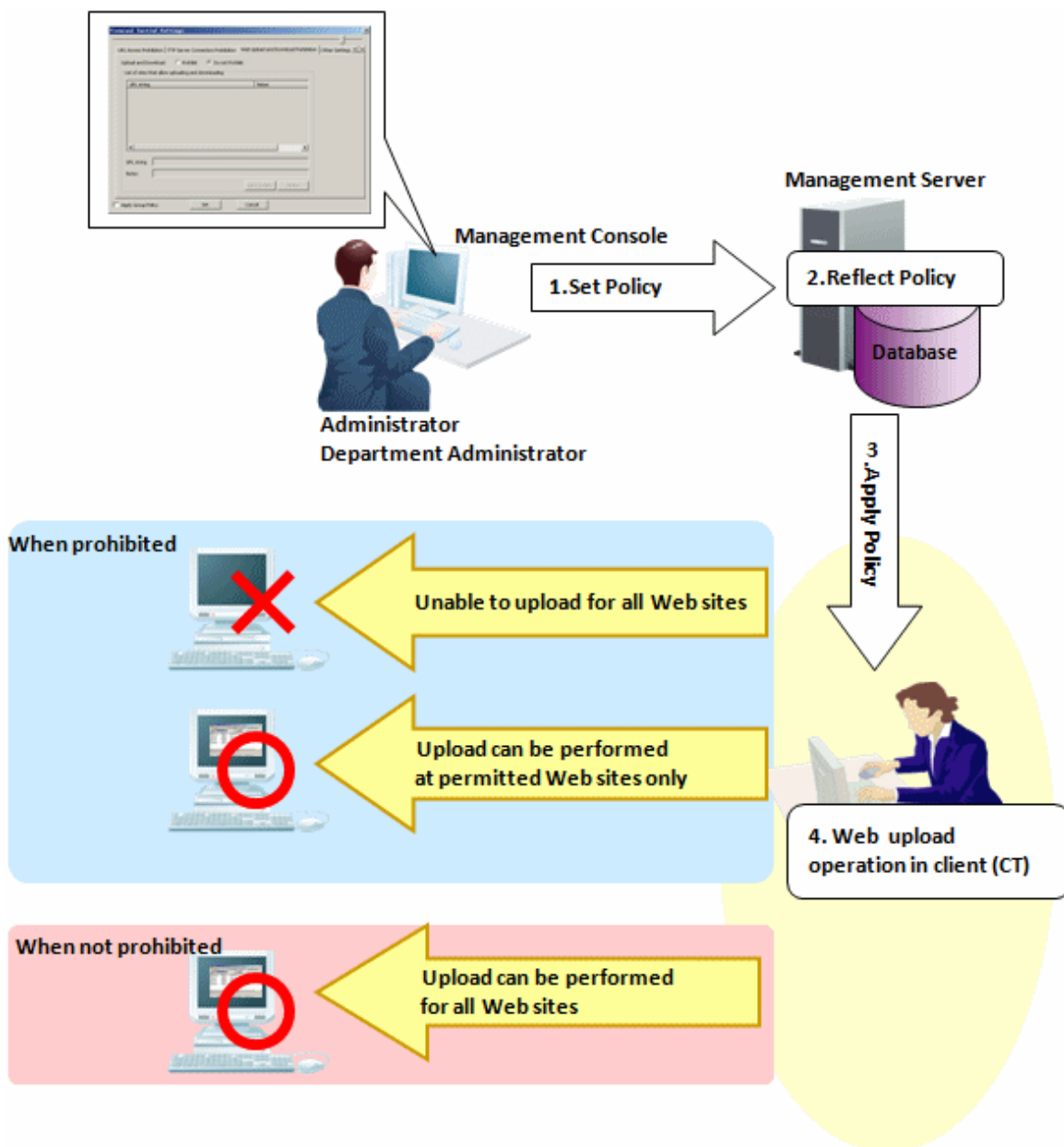
Note

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, 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).

In **Web upload/download**, select **Prohibit uploading and downloading** or **Prohibit uploading only**.

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 cannot be performed on all Web sites
 - Upload can only be performed on the permitted Web sites
 - Upload can be performed on all Web sites

When prohibited

The following message will be displayed.

[E002-INF003] Uploading files to this Web site is prohibited by system administrator.
(Web site URL prohibited to be uploaded: *ipAddress*)

8.1.10 Web Download Prohibition

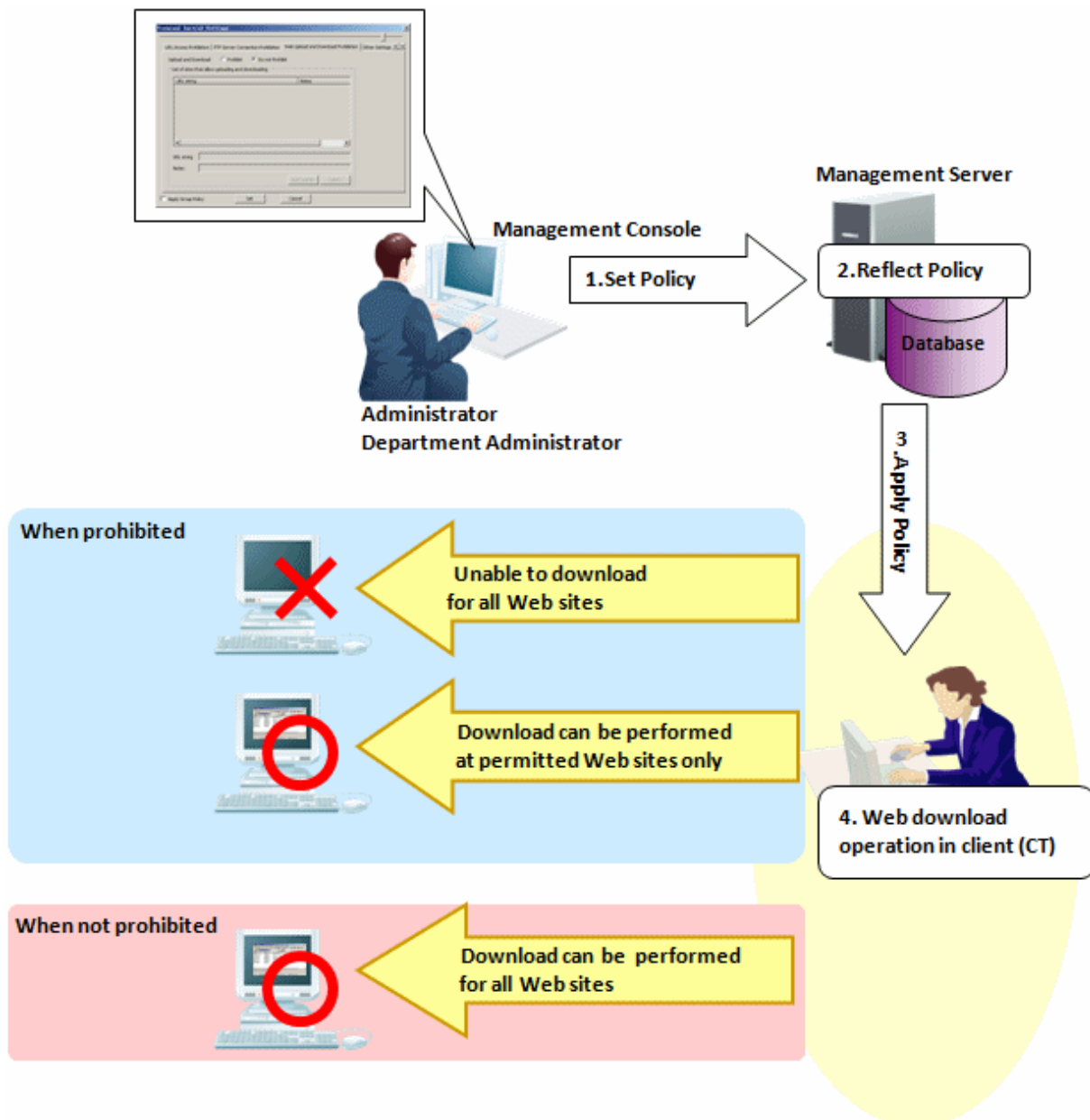
By setting the Web download prohibition policy, downloading from a website that is not permitted by the administrator can be prohibited in the client (CT) PC.



Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.
Refer to "[1.2.14 Web Upload and Download Operation Prohibition](#)" for details.

Flow from setting policy through to enabling prohibition



1. Set policy

Set the policy in the **Terminal Initial Settings** window, the **User Policy Settings** window or the window displayed after the Management Console is started (CT policy settings window).

In **Web upload/download**, select **Prohibit uploading and downloading**, or **Prohibit downloading only**.

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 a website in the client (CT), the status will become one of the following:

- Download cannot be performed on all websites
- Download can only be performed on permitted websites
- Download can be performed on all websites

When prohibited

The following message will be displayed:

```
[E002-INF004] Downloading files from this Web site is prohibited by system administrator.  
(Web site URL prohibited to be downloaded: ipAddress)
```

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.

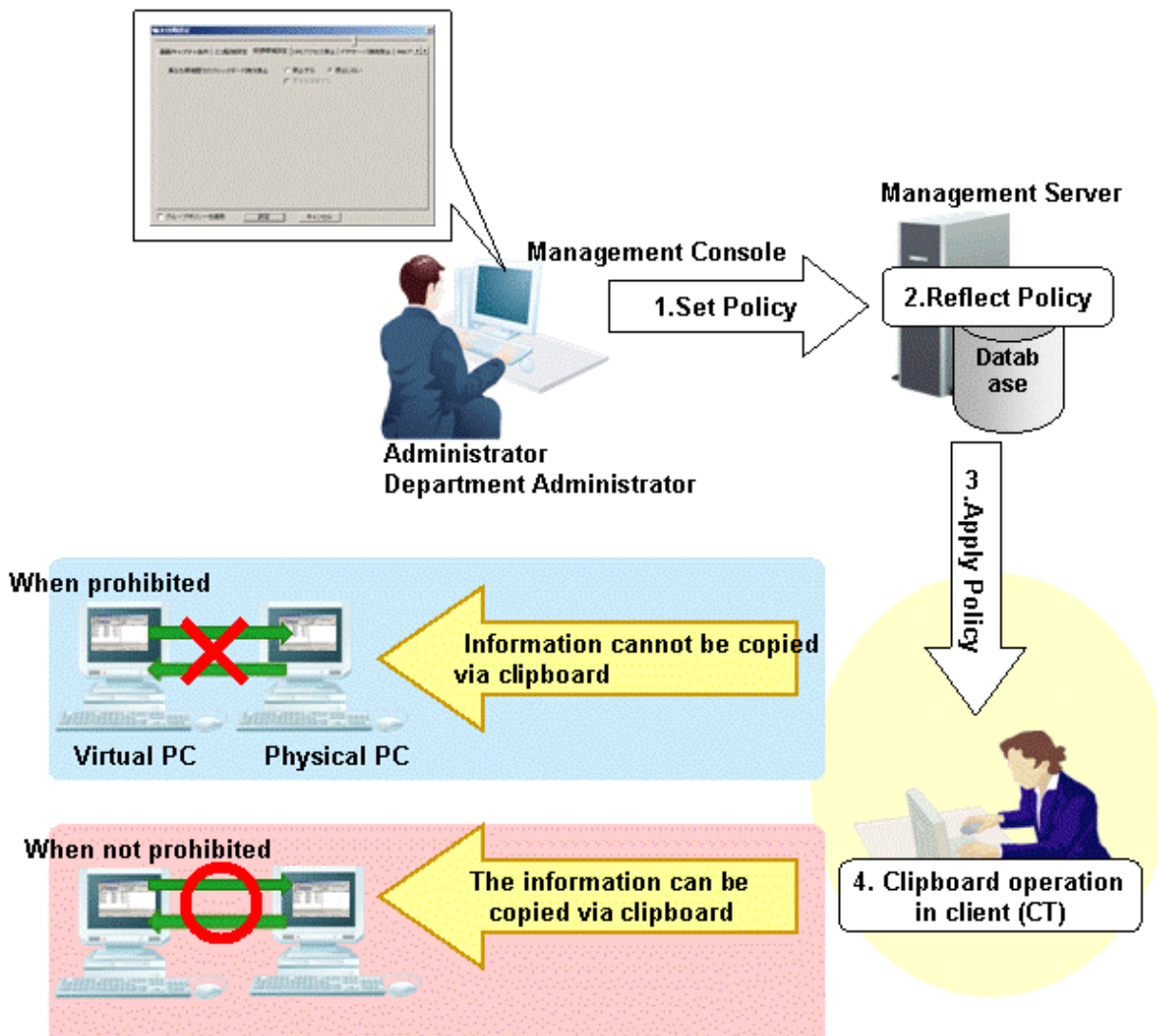


Note

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, 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).

In **Clipboard**, set **Prohibit of clipboard operation between different environments** to **Prohibit**.

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

8.1.12 Wi-Fi Connection Prohibition (Smart Device)

By setting the Wi-Fi connection prohibition policy, connections to access points not permitted by the administrator can be prohibited in smart devices that have a smart device (agent) installed.



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.

Refer to "[1.2.16 Wi-Fi Connection Prohibition \(Smart Device\)](#)" for details.

Steps to make prohibition effective through policy setting

1. Check the BSSID of the Wi-Fi router

This is normally the MAC address of the Wi-Fi router.

(There are some Wi-Fi router types that do not use the MAC address as the BSSID, so you should confirm the BSSID with the system administrator if you are unsure about this.)

2. Set policy

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

Set the access point name and BSSID.

In **Wi-Fi connection**, set **Wi-Fi connection prohibition** to **Prohibit**.

3. Reflect policy

The set policy will be reflected to the database.

4. Apply policy

The set policy will be applied to the smart device (agent).

5. Access point connection operation

When connecting to an access point using a smart device (agent), the status will become one of the following:

- Cannot connect to prohibited access points
- Can only connect to permitted access points
- Can connect to any access point

Refer to "[2.4.1.17 Wi-Fi Connection](#)" for details on how to set the policy.

When prohibited

When connecting to an access point for which connections are not permitted, the following message will be displayed on the smart device.

```
System administrator prohibits the connection to this access point.  
accessPointName  
Connection disabled.
```

8.1.13 Bluetooth Connection Prohibition (Smart Device)

By setting the Bluetooth connection prohibition policy, pairing with Bluetooth devices not permitted by the administrator can be prohibited in smart devices that have a smart device (agent) installed.

Steps to make prohibition effective through policy setting

1. Set policy
Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).
In **Bluetooth connection**, set **Bluetooth connection prohibition** to **Prohibit**.
2. Reflect policy
The set policy will be reflected to the database.
3. Apply policy
The set policy will be applied to the smart device (agent).
4. Bluetooth device pairing operation
When pairing with a Bluetooth device in a smart device (agent), the status will become one of the following:
 - Cannot pair with a prohibited Bluetooth device
 - Can only pair with permitted Bluetooth devices
 - Can pair with any Bluetooth device

Refer to "[2.4.1.18 Bluetooth Connection](#)" for details on how to set the policy.

When prohibited

When connecting to a Bluetooth device for which pairing is not permitted, the following message will be displayed on the smart device (agent).

```
System administrator prohibits the use of this Bluetooth.  
Connection disabled.
```

8.1.14 Application Usage Prohibition (Smart Device)

By setting the application usage prohibition policy, use of applications not permitted by the administrator can be prohibited in smart devices that have a smart device (agent) installed.

You can also prohibit use of specified applications outside of business hours only, delete application data outside of business hours, and so on.



Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.

Refer to "[1.2.17 Application Usage Prohibition \(Smart Device\)](#)" for details.

Steps to make prohibition effective through policy setting

1. Set policy

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

Select **Android > Application**, and then set **Application usage prohibition** to **Prohibit**.

Also, set the following information:

- Application package name for which usage is to be prohibited
- Whether to prohibit usage outside of business hours only
- Whether to delete application data outside of business hours

2. Reflect policy

The set policy will be reflected to the database.



How to obtain prohibited package names

Example: To prohibit startup of the calculator

- Enable [Application Usage Log \(Smart Device\)](#) to obtain application usage logs.
- Start the calculator on the smart device. The start log will be obtained.
- [Start the Log Viewer](#) to check the calculator start log.

Type	Application usage
Classification	Normal
Content	The [Calculator] window has been detected. Application name: [com.android.calculator2]

The above "com.android.calculator2" will be the prohibited package name.

3. Apply policy

The set policy will be applied to the smart device (agent).

4. Application usage operation

When using an application on the smart device (agent), the status will become one of the following:

- Cannot use applications of prohibited package names
- Cannot use applications of prohibited package names outside of business hours
- Can use applications of permitted package names
- Any application can be used

Refer to "[2.4.1.19 Application \(Android\)](#)" for details on how to set the policy.

When prohibited

When connecting to an application for which usage is not permitted, the following message will be displayed on the smart device (agent).

```
System administrator prohibits the use of this application.
Uninstall it.
```

8.1.15 Device Functionality (iOS Device)

By setting the device functionality policy, you can prohibit the following features on iOS devices registered on the Master Management Server (when using a 3-level structure) or Management Server (when using a 2-level structure):

- Installing Applications

- Use of camera
- Screen capture
- Automatic sync while roaming
- Siri
- Voice dialing
- Use of Passbook while device is locked
- In-app purchase
- Password not entered in iTunes Store
- Multiplayer gaming
- Adding Game Center friends

Steps to make prohibition effective through policy setting

1. Set policy

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **iOS > Device Functionality**, clear the prohibited items.
2. Reflect policy

The set policy will be reflected to the database.
3. Apply policy

The set policy will be applied to the iOS device.
4. Device feature operation

When using a prohibited feature on an iOS device, the status will become one of the following:

 - Cannot use any of the specified device features
 - Can use only the permitted device features
 - Can use all of the specified device features

Refer to "[2.4.1.20 Device Functionality](#)" for details on how to set the policy.

8.1.16 Applications (iOS Device)

By setting the application policy, you can prohibit use of the following applications on iOS devices registered on the Master Management Server (when using a 3-level structure) or Management Server (when using a 2-level structure):

- YouTube
- iTunes Store
- Safari
- Prohibit (disable) each of the following when Safari is permitted:
 - Autofill
 - Force fraud warning (access to known fraudulent websites)
 - JavaScript
 - Pop-ups
 - Cookies

Steps to make prohibition effective through policy setting

1. Set policy
Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).
In **iOS > Application**, set the items to be prohibited.
 2. Reflect policy
The set policy will be reflected to the database.
 3. Apply policy
The set policy will be applied to the iOS device.
 4. Device feature operation
When using an application of an iOS device, the status will become one of the following:
 - Cannot use prohibited applications
 - YouTube
 - iTunes Store
 - Safari
 - Autofill is not used when Safari is permitted
 - Cannot access known fraudulent websites when Safari is configured to use all the device features
 - Cannot use JavaScript when Safari is permitted
 - Pop-ups will not open when Safari is permitted
 - Use of cookies restricted when Safari is permitted
 - Any application can be used
- Refer to "[2.4.1.21 Application \(iOS\)](#)" for details on how to set the policy.

8.1.17 iCloud (iOS)

By setting the iCloud policy, you can prohibit the following features on iOS devices registered on the Master Management Server (when using a 3-level structure) or Management Server (when using a 2-level structure):

- Backup to iCloud
- Document sync
- Photo Stream
- Shared Photo Stream

Steps to make prohibition effective through policy setting

1. Set policy
Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).
In **iOS > iCloud**, clear the prohibited items.
2. Reflect policy
The set policy will be reflected to the database.
3. Apply policy
The set policy will be applied to the iOS device.
4. Device feature operation
When using iCloud on an iOS device, the status will become one of the following:
 - Cannot use any iCloud features

- Can use only the permitted iCloud features
- Can use all iCloud features

Refer to "[2.4.1.22 iCloud](#)" for details on how to set the policy.

8.1.18 Security and Privacy (iOS)

By setting the security and privacy policy, you can perform the following settings on iOS devices registered on the Master Management Server (when using a 3-level structure) or Management Server (when using a 2-level structure):

- Send diagnostic data to Apple
- Accept untrusted TLS certificates
- Encrypt backups

Steps to make prohibition effective through policy setting

1. Set policy

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **iOS > Security and privacy**, set the items to be prohibited.

2. Reflect policy

The set policy will be reflected to the database.

3. Apply policy

The set policy will be applied to the iOS device.

4. Device feature operation

When using security and privacy-related features on an iOS device, the status will become one of the following:

- Cannot use any security and privacy-related features
- Can use only the permitted security and privacy features
- Can use all security and privacy features

Refer to "[2.4.1.23 Security and Privacy](#)" for details on how to set the policy.

8.1.19 Content Ratings (iOS)

By setting the content rating policy, you can prohibit viewing of the following content on iOS devices registered on the Master Management Server (when using a 3-level structure) or Management Server (when using a 2-level structure):

- Explicit music, Podcast, iTunes U
- Adult content in iBookstore
- Unrated videos, TV programs and applications

Steps to make prohibition effective through policy setting

1. Set policy

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **iOS > Content Ratings**, set the items and ratings to be prohibited.

2. Reflect policy

The set policy will be reflected to the database.

3. Apply policy

The set policy will be applied to the iOS device.

4. Device feature operation

When viewing contents on an iOS device, the status will become one of the following:

- Cannot use any content ratings features
- Can use only the permitted content ratings features
- Can use any content ratings features

Refer to "[2.4.1.24 Content Ratings](#)" for details on how to set the policy.

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.



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.

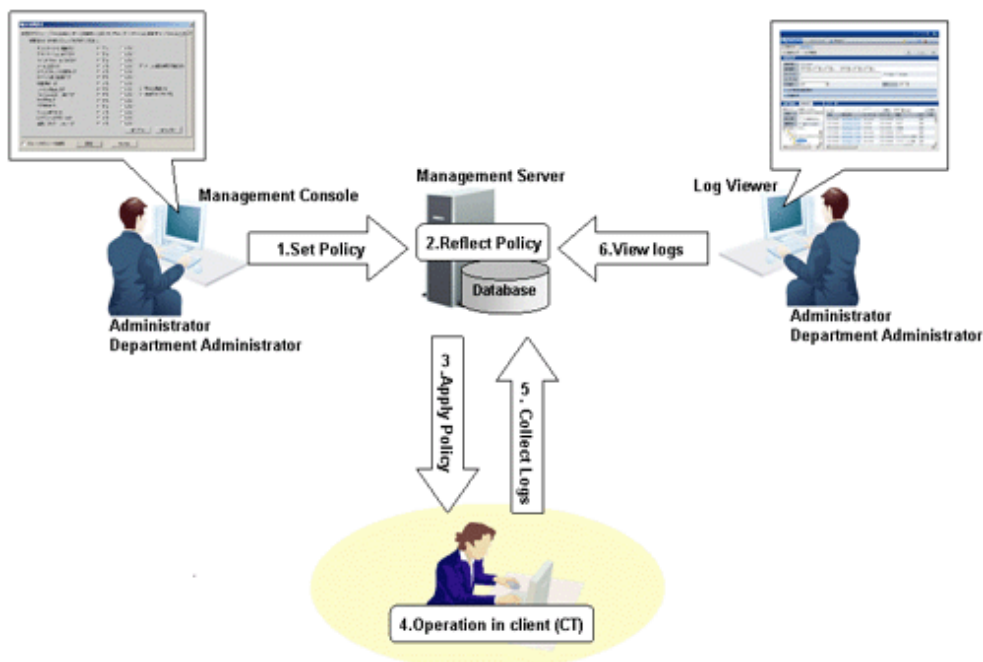
For details, refer to "[1.2.18 All Logs \(for Clients \(CT\)\)](#)" - "[1.2.41 About Collection of Logs for Investigation of Client \(CT\)](#)".

- Application startup log
- Application termination log
- Application startup prohibition log
- Window title obtaining log
- E-mail sending log
- Device configuration change log
- Printing 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
- Linkage application log

- Configuration change log
- Wi-Fi connection log (smart device)
- Wi-Fi connection prohibition log (smart device)
- Bluetooth connection log (smart device)
- Bluetooth connection prohibition log (smart device)
- Application usage log (smart device)
- Application usage prohibition log (smart device)
- Web access log (smart device)
- SD card mount/unmount log (smart device)
- SIM card mount/unmount log (smart device)
- Incoming/outgoing calls log (smart device)
- Application configuration change log (smart device)

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 **Send log** of the policy settings window.

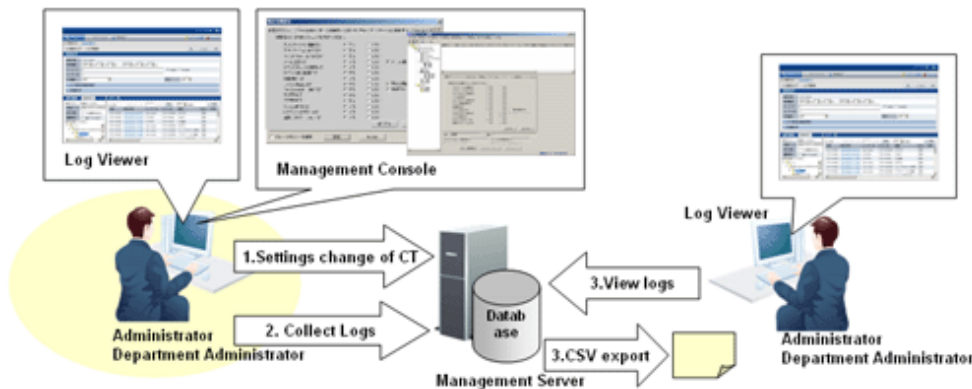
When the client (CT) cannot communicate with the connected Management Server

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 **Send log** 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, refer to "DTKSTCV.EXE (output configuration change log)" of *Systemwalker Desktop Keeper Reference Manual*.

View logs

View the collected logs in Log Viewer.

Below is an example of the CT operation log display.

The screenshot shows the 'CT Operation Log' interface. At the top, there are tabs for 'Log Viewer', 'Log Analyzer', and 'Environment Setup'. The main title is 'CT Operation Log(Operation) - Log search'. Below this, there are search filters for 'Search target' (WINDOWS-AM8TT86 (CT)), 'Search range' (2015 Year 5 Month 15 Day), 'Call search conditions', 'Keyword', 'User ID', 'Type of log' (All), and 'Device' (All). There are also buttons for 'Back', 'Output in CSV format', and 'Search'.

The 'List of logs' section shows a table with the following columns: Name, Date and time, User name, Domain name, Variety, Classification, Add, and Content. The table contains 15 rows of log entries, including Logon, Device configuration change, File operation, and Application startup events.

Name	Date and time	User name	Domain name	Variety	Classification	Add	Content
WINDOWS-AM8TT86	2015/05/15 14:48:17	admin	WINDOWS-AM8TT86	Logon	Normal		Logged or
WINDOWS-AM8TT86	2015/05/15 14:48:17	admin	WINDOWS-AM8TT86	Logon	Normal		Logged or
WINDOWS-AM8TT86	2015/05/15 14:48:17	admin	WINDOWS-AM8TT86	Logon	Normal		Logged or
WINDOWS-AM8TT86	2015/05/15 14:48:22	admin	WINDOWS-AM8TT86	Device configuration change	Normal		[Add USE
WINDOWS-AM8TT86	2015/05/15 14:48:22	admin	WINDOWS-AM8TT86	Device configuration change	Normal		[Add USE
WINDOWS-AM8TT86	2015/05/15 14:48:22	admin	WINDOWS-AM8TT86	Device configuration change	Normal		[Add USE
WINDOWS-AM8TT86	2015/05/15 14:48:22	admin	WINDOWS-AM8TT86	Device configuration change	Normal		[Add USE
WINDOWS-AM8TT86	2015/05/15 14:48:22	admin	WINDOWS-AM8TT86	Device configuration change	Normal		[Add USE
WINDOWS-AM8TT86	2015/05/15 14:48:22	admin	WINDOWS-AM8TT86	Device configuration change	Normal		[Add USE
WINDOWS-AM8TT86	2015/05/15 14:48:31	admin	WINDOWS-AM8TT86	File operation	Normal		Operation
WINDOWS-AM8TT86	2015/05/15 14:48:31	admin	WINDOWS-AM8TT86	File operation	Normal		Operation
WINDOWS-AM8TT86	2015/05/15 14:48:31	admin	WINDOWS-AM8TT86	File operation	Normal		Operation
WINDOWS-AM8TT86	2015/05/15 14:48:32	admin	WINDOWS-AM8TT86	Application startup	Normal		The lccS
WINDOWS-AM8TT86	2015/05/15 14:48:32	admin	WINDOWS-AM8TT86	Application startup	Normal		The lccS
WINDOWS-AM8TT86	2015/05/15 14:48:32	admin	WINDOWS-AM8TT86	Application startup	Normal		The lccS

For items that can be viewed in Log Viewer, refer to "5.2.1 View Logs in the CT Operation Log Window", "5.2.2 View Logs in the User Operation Log Window" or "5.2.3 View Logs in the Configuration Change Log Window".

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 **Windows > Log collection operation**, set **Application Startup Log** to **Yes**.

Displayed content

The following log content can be viewed:

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 (*1)

Example of **Content:**

```
Started [iexplore].
```

*1: 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 **Windows > Log collection operation**, set **Application Termination Log** to **Yes**.

Displayed content

The following log content can be viewed:

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 (*1)

Example of **Content:**

```
Ended [iexplore].
```

*1: 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 **Application**.

Displayed content

The following log content can be viewed:

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 (*1)
- Prohibition processing (**Ended by force**)
- Prohibition results (**Succeeded** or **Failed**)

Example of **Content**:

```
Startup of [calc][Ended by force]. Result: [Succeeded]
```

*1: 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 a window, the window title obtaining log cannot be collected.

When using "Internet Explorer(R)" 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 character 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(R) and Explorer
- Internet Explorer(R) and Internet Explorer(R)
- 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, refer to "[1.2.21 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 **Windows > Log collection operation**, set **Window Title Obtaining Log(Web access log)** to **Yes**.
- In **Window title filter**, set the filtering conditions for window title obtaining log.

The settings can be performed when **Window Title Obtaining Log(Web access log)** is set to **Yes**.

- In **Window title screen capture**, 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, refer to "[2.4.1.4 Window Title Filter](#)" and "[2.4.1.5 Window Title Screen Capture](#)".

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.

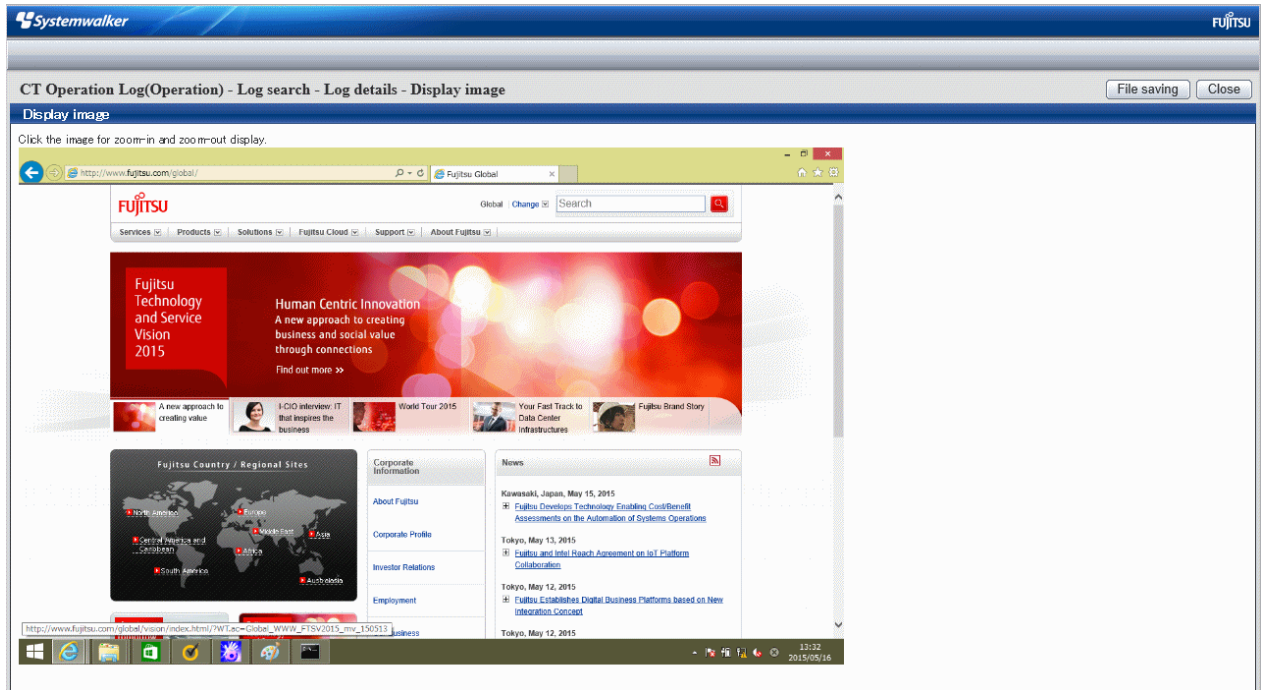
The screen capture can be viewed in window title obtaining log.

In terminal operation settings, when **CT** is selected as **Attached data accumulation settings**, screen capture data will be saved to the client (CT).

The following log content can be viewed:

- Collected window

- "Display Result of Logs"



Displayed content

The following log content can be viewed:

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 (*1)
- Name of started application (*1)

Example of **Content**:

```
Window [Start menu] has been detected. Program name: [Explorer]
```

Note: The URL of page that is displayed through browser is displayed. (*1)

*1: 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.



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, refer to "[1.2.22 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 **Windows > Log collection operation**, set **E-mail Sending Log** to **Yes**.
- When **E-mail content can be viewed** is selected in **Windows > Log collection operation**, 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**.

Displayed content

The following log content can be viewed:

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 (*1)
- Address of sender (*1)
- Address of recipient (To, Cc and Bcc information) (*1)
- Attachment name (*1)

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]
```

*1: 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 (*1)
- Processing result after the warning message is displayed (*1)

Example of **Notes**:

Warning address: [xxxx] Result: [Send After Confirmation]

*1: When performing keyword search in Log Viewer, it can be specified as keyword.

8.2.6 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 or a USB device is connected) 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 **Windows > Log collection operation**, set **Device Configuration Change Log** to **Yes**.

Collected information

The information displayed in **Notes** will be different due to the type of drive.

Drive/device type	Volume	Device Name	Internal Serial Number, Manufacturer ID, Product ID	Server Name, Shared Name
Fixed	Y	N	N	N
Removable	N	Y (*1)	Y (*1)	N
CD-ROM	N	Y (*1)	Y (*1)	N
Remote (*2)	N	N	N	Y
USB	N	Y (*1)	Y (*1)	N
USB (portable device)	N	Y (*1)	Y (*1)	N
USB (imaging device)	N	Y (*1)	Y (*1)	N

Y: Collect information.

N: Do not collect information.

*1: The information is only recorded when a USB is connected.

*2: When sharing the floppy drive and USB memory device with another PC, the drive type will be recorded as "Remote".

Displayed content

The following log content can be viewed:

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 or USB (Note 3)
- Drive type or portable device/imaging device 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 registering a device configuration change log for the drive letter

- 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

When registering a USB device configuration change log

- On startup of the PC, if there is a device added when comparing the information at last shutdown with the current USB device information
- When a USB device is added after starting up the PC (obtained even when not logged in)

Record as **Change** when any of the following operations is performed in the logon status.

When registering a device configuration change log for the drive letter

- When changing the drive type
- When allocating the shared name of server to the existing network drive

When registering a USB device configuration change log

- Not recorded as "Change".

Note: the following content is displayed:

- Volume (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. Recording as a violation occurs when **USB Device Individual Identification Function** is set to **Use**, and the following pattern applies. Even when access is set as prohibited for non-USB connections (IDE connection, IEEE connection, PCMCIA connection, etc.) of removable devices or DVD/CD devices, such connections are recorded as normal.

- Case 1

When the USB device whose **USB Identification Method** in the **USB Device Registration** window is **Unavailable** is connected

- Case 2

When the USB device whose period for use set in **Period for Using USB Device** in the **USB Device Registration** window has expired is connected

- 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 you select **Export Prohibition** (specify drive, removable, or DVD/CD) in **File export/read** and connect to a USB device that has not been permitted for use

Note that drive specification is recorded as normal in the USB device configuration change log.

- Case 5

When you select **Reading prohibition** (specify removable or DVD/CD) in **File export/read** and connect to a USB device that has not been permitted for use

- Pattern 6

When you select **Portable device/imaging device connection prohibition** in **File export/read** (specify portable device, or imaging device), and connect to a USB device that has not been permitted for use

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
Add 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
Add G: Removable	Device Name BUFFALO USB Flash Disk USB Device , Internal Serial Number B32986 , Manufacturer ID: 1111 , Product ID: 2222

When DVD/CD device connected via USB is connected

Content	Notes
Add E: CD-ROM	Device Name MATSHITA UJD330 , Internal Serial Number [], manufacturer ID: 3333 , product ID: 4444

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
Add 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 , Manufacturer ID: 1111 , Product ID: 2222

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
Modify A:Unkown->Removable	

When a USB mouse is connected

Content	Notes
Added USB	Device name: HID-compliant mouse (Logitech USB Optical Mouse USB Device) , internal serial number: [], manufacturer ID: 046D , product ID: C018

When a USB smartphone is connected

Content	Notes
Added USB (portable device)	Device name: Android Composite ADB Interface (Toshiba Corporation Toshiba HSUSB Device USB Device), internal serial number: TG12345678 , manufacturer ID: 0930 , product ID: 0D85

When a USB web camera is connected

Content	Notes
Added USB (imaging device)	Device name: USB video device #2 (Alcor Micro, Corp. USB 2.0 PC Camera USB Device) , internal serial number: [], manufacturer ID: 0458 , product ID: 7081

When violated

When the device configuration change log becomes violated, the following message will be displayed.

```
[S105-ERR001] Accessing to this drive is prohibited by system administrator. (Drive:G)
```

```
[S105-ERR002] Access to this device has been prohibited by the system administrator. (Device:Y-E DATA USB-FDU USB Device)
```

8.2.7 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.



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, refer to "[1.2.20 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 **Windows > Log collection operation**, set **Print Operation Log** to **Yes**.

Displayed content

The following log content can be viewed:

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 (for document names recognized by **See what's printing** of the printer, the content will differ according to the application) (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: [2013/04/11 19:44:59]
```

Note: (not displayed)

*) When performing keyword search in Log Viewer, it can be specified as keyword.

8.2.8 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 **Print/PrintScreen**, set **Printing Prohibition** to **Yes**.

In addition, applications with printing permission should also be set in **Print/PrintScreen**.

For details about the configuration value, refer to "[2.4.1.9 Print/PrintScreen](#)".

Displayed content

The following log content can be viewed:

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(*1)
- Name of prohibited application (*1)

Example of **Content**:

```
Prohibited print [Microsoft Word - 13.Console.doc]. Program name: [C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE]
```

*1: When performing keyword search in Log Viewer, it can be specified as keyword.

Note: (not displayed)

8.2.9 Logon Prohibition Log

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 **Logon**. For details about the configuration value, refer to "[2.4.1.6 Logon](#)".

Displayed content

The following log content can be viewed:

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 [ms-user(Microsoft account)] 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)

8.2.10 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.



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, refer to "[1.2.19 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 **Windows > Log collection operation**, set **File Export Log** to **Yes**.

- When **Backup Original File** is selected in **Windows > Log collection operation**, 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, refer to "[2.4.1.8 File Export/Read](#)".

Displayed content

The following log content can be viewed:

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 (*1)
- File name of export target (*1)
- Export method (in plain text)
- Drive letter of export target
- Drive type of export target
- Reason for export (*1)

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 2013.XLS] as [E:\Product Customer October in 2013.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 xxx Information to xxx Client in xxx Business]
```

*1: 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 (*3) (*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 **Windows > Log collection operation** of the CT policy settings window.

- When setting **Export Using File Export Utility** to **Yes** in the **Terminal Initial Settings** window **File export/read** in the policy settings window.

When setting **USB Device Individual Identification Function** to **Use** in the **File Export Utility Function Settings** window.

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]
```

8.2.11 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 **Print/PrintScreen**.
 - Set **PrintScreen Key Operation Log** to **Yes** in **Windows > Log collection operation**.
 - When the **Capture Screen** check box is selected in **Windows > Log collection operation**, 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

The following log content can be viewed:

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)

8.2.12 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 **Windows > Log collection operation**.
- Set **PrintScreen Key Invalid** to **Yes** in **Print/PrintScreen**.

- When the **Screen Capture** check box is selected in **Print/PrintScreen**, the screen capture at the time when the PrintScreen key is used can be collected.

Displayed content

The following log content can be viewed:

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)

8.2.13 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 **Windows > Log collection operation** to **Yes**.

How to search

- In the case of a web download log:

When searching in the Log Viewer, the web download log is included in the results of "Web operation" log type.

When filtering search results, select **Web operation** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "Web operation" or "Web download" is set as a keyword. The keyword is searched for using partial match.

- In the case of a web upload log:

When searching in the Log Viewer, the web upload log is included in the results of "Web operation" log type.

When filtering search results, select **Web operation** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "Web operation" or "Web upload" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

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 (*1)
- URL strings of access target (*1)
- File name (*1)

The maximum length of the string displayed in the content is 520 halfwidth characters (260 fullwidth characters). Because only the length within 520 halfwidth characters (260 fullwidth characters) is displayed when the length of string displayed in the content exceeds 520 halfwidth characters (260 fullwidth characters), 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]
```

*1: When performing keyword search in Log Viewer, it can be specified as keyword.

Note: (not displayed)

8.2.14 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 Internet** to **Prohibit**.
- In **Web upload/download**, set **Upload and download prohibition settings** to one of the following:
 - **Prohibit uploading and downloading**

- **Prohibit uploading only**
- **Prohibit downloading only**

How to search

- In the case of a URL access prohibition log
When searching in the Log Viewer, the URL access prohibition log is included in the results of "Web operation prohibition" log type.
When filtering search results, select **Web operation prohibition** for **Log type**, and **Normal** for **Classification**.
You can filter the search results even when "iexplore.exe", "Web operation prohibition", "URL access", or the URL of the site that was accessed is set as a keyword.
The keyword is searched for under partial match.
- In the case of a Web download prohibition log
When searching in the Log Viewer, the web download prohibition log is included in the results of "Web operation prohibition" log type.
When filtering search results, select **Web operation prohibition** for **Log type**, and **Normal** for **Classification**.
You can filter the search results even when "iexplore.exe", "Web operation prohibition", "Web download", or the URL of the site that was accessed is set as a keyword.
The keyword is searched for under partial match.
- In the case of a Web upload prohibition log
When searching in the Log Viewer, the web upload prohibition log is included in the results of "Web operation prohibition" log type.
When filtering search results, select **Web operation prohibition** for **Log type**, and **Normal** for **Classification**.
You can filter the search results even when "iexplore.exe", "Web operation prohibition", "Web upload", or the URL of the site that was accessed is set as a keyword. The keyword is searched for under partial match.

Displayed content

The following log content can be viewed:

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 (*1)
- URL strings of access target (*1)

The maximum length of the string displayed in the content is 520 halfwidth characters (260 fullwidth characters). Because only the length within 520 halfwidth characters (260 fullwidth characters) is displayed when the length of string displayed in the content exceeds 520 halfwidth characters (260 fullwidth characters), 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]

*1: When performing keyword search in Log Viewer, it can be specified as keyword.

Note: (not displayed)

8.2.15 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 Windows > Log collection operation** 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

The following log content can be viewed:

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 halfwidth characters (259 fullwidth characters). Because only the length within 519 halfwidth characters (259 fullwidth characters) is displayed when the length of string displayed in the content exceeds 519 halfwidth characters (259 fullwidth characters), the length of the content will be adjusted.

- FTP client program name (*1)
- IP address of FTP Server (*1)
- File name (*1)

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]
```

*1: When performing keyword search in Log Viewer, it can be specified as keyword.

Note: (not displayed)

8.2.16 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, 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 **FTP server connection**.

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

The following log content can be viewed:

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 (*1)
- IP address of FTP server (*1)

The maximum length of the string displayed in the content is 519 halfwidth characters (259 fullwidth characters). Because only the length within 519 halfwidth characters (259 fullwidth characters) is displayed when the length of string displayed in the content exceeds 519 halfwidth characters (259 fullwidth characters), the length of the content will be adjusted.

Example of **Content**:

```
prohibited connecting to [192.168.1.100]. Application name: [FTP.EXE]
```

*1: When performing keyword search in Log Viewer, it can be specified as keyword.

Note: (not displayed)

8.2.17 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.



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, refer to "[1.2.28 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 **Windows > Log collection operation**, set **Clipboard Operation Log (Virtual Environment)** to **Yes**.

Displayed content

The following log content can be viewed:

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)

8.2.18 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).

In **Clipboard**, set **Prohibit of clipboard operation between different environments** to **Prohibit**.

Displayed content

The following log content can be viewed:

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)

8.2.19 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



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, refer to "[1.2.29 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 **Windows > Log collection operation**, set **File Operation Log** to **Yes**.
- In **File operation**, set the filtering conditions for file operation log.
The settings can be performed when **File Operation Log** is set to **Yes**.
- In **Extension**, 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, refer to "[2.4.1.2 File Operation](#)" and "[2.4.1.3 Extension](#)".

Displayed content

The following log content can be viewed:

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, 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, Save As**, 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 a rename is performed during creation of a folder, a halfwidth space (size (byte): []) may be displayed in the notes column of the folder "Create" log.

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.

Also, when performing a keyword search in Log Viewer, and a keyword including any of the following operation types is specified, logs for which the operation type applies may be searched.

(Applicable operation types: "View", "Update", "Create", "Delete", "Copy", "Move", "Rename", "Save As")

Example:

When a single keyword such as "copy, source file name:G:\\" is specified in the search criteria, and an "OR" search is selected, logs of the "Copy" operation type will also be searched regardless of the file name for which the operation was performed. To perform a search where the operation type is "Copy" and the file name includes "G:\\", specify multiple keywords with an AND condition.

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 (Note 1)
- Notepad (Note 1)
- Tablet (Note 1)
- Microsoft(R) Word (2003, 2007, 2010 and 2013) (Note 2)
- Microsoft(R) Excel (2003, 2007, 2010 and 2013) (Note 2)
- Microsoft(R) PowerPoint(R) (2003, 2007, 2010 and 2013) (Note 2)
- Command in command prompt (COPY, XCOPY, MOVE, DEL, ERASE, RD, REN, MD) (Note 1)

Note 1: Does not collect "Save as" operation logs.

Note 2: In case of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 or Windows Server(R) 2012, only 2003, 2007, 2010 and 2013 are supported.

"Save as" operation logs can only be collected in versions 2007, 2010 and 2013.

However, be aware of the following points:

- "Update" operation of Microsoft(R) Word will be collected as **Create** log.
- Like Explorer and XCOPY, in **File operation, 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 the "Move" operation is performed in the above software or commands, "Copy" and "Create" (move source) 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)

Log Type	Content Display of Log Viewer
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)
Save as	Operation: Save as , Source file name: (Note 1) , Source drive type: (Note 2) . Target file name: (Note 3) , Target drive type: (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	Save as
File Operation	Log for files	In the same drive (Note 1)	View (Note 3)	Update (Note 3)	Create	Delete	Copy	Rename (Cut)	Rename	Save as
		In the same drive (Note 2)	-	-	-	-	Copy	Cut	-	Save as
Folder Operation	Log for files under a folder	In the same drive (Note 1)	-	-	-	Delete	Copy	x(Note 4) (Cut)	-	-
		Between different drives (Note 2)	-	-	-	-	Copy	Cut	-	-
	Log for folders	In the same drive (Note 1)	-	-	Create	Delete	Create (x)	Rename (Rename) (Delete)	Rename	-

Condition			File and Folder Operations							
			View	Update	Create	Delete	Copy	Cut	Rename	Save as
		Between different drives (Note 2)	-	-	-	-	Create (x)	Create Delete (Delete)	-	-

-: Operation is not possible.

x: Operation log cannot be collected.

View/update/create/delete/copy/cut/rename/Save as: 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 screenshot shows the Log Viewer application with the following search conditions:

- Search target: WINDOWS-JCN1R76 (CT)
- Search range: 2015 Year 5 Month 16 Day ~ 2015 Year 5 Month 17 Day
- Call search conditions: [Empty]
- Keyword: [Empty]
- User ID: [Empty]
- Type of log: File operation
- Device: All
- Classification: All

The List of logs table is as follows:

Name	Date and time	User name	Domain name	Variety	Classification	Add	Content
WINDOWS-JCN1R76	2015/05/17 10:48:03	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Create]. File
WINDOWS-JCN1R76	2015/05/17 10:48:03	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Create]. File
WINDOWS-JCN1R76	2015/05/17 10:48:03	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Create]. File
WINDOWS-JCN1R76	2015/05/17 10:48:06	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:06	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:06	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:12	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:12	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:12	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:12	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:12	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:12	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Delete]. File
WINDOWS-JCN1R76	2015/05/17 10:48:17	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Create]. File
WINDOWS-JCN1R76	2015/05/17 10:48:17	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [Create]. File
WINDOWS-JCN1R76	2015/05/17 10:48:17	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [View]. File
WINDOWS-JCN1R76	2015/05/17 10:48:17	admin	WINDOWS-JCN1R76	File operation	Normal		Operation: [View]. File

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 name: [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.

8.2.20 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 **Windows > Log collection operation**, 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

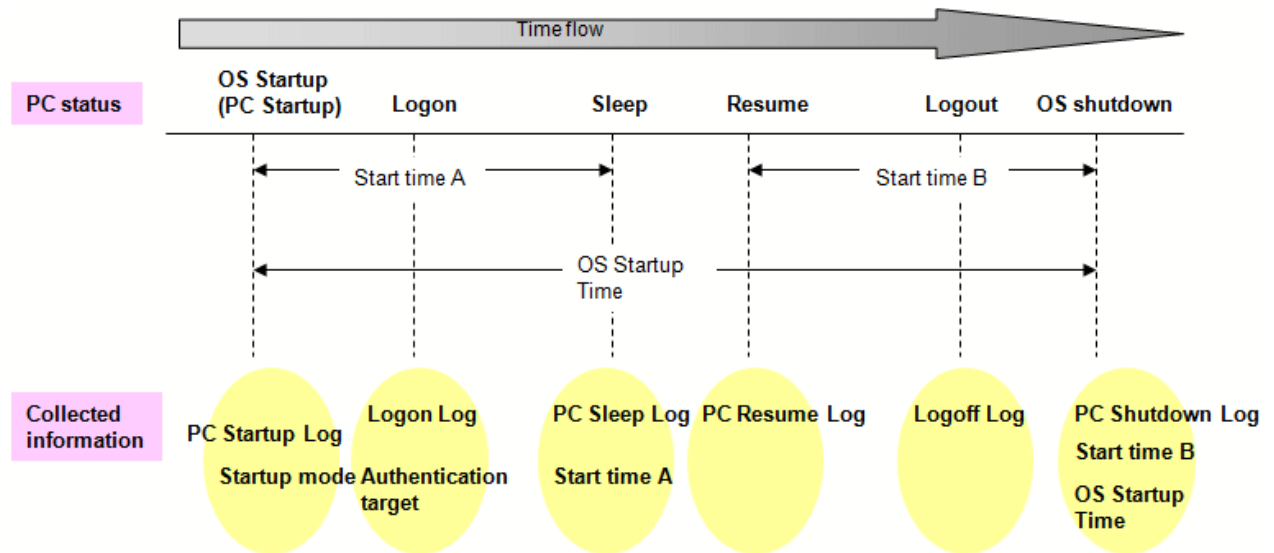
Information when the client (CT) restores from standby mode or sleep mode.

- 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".

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.

Enter the numerals ("XX" and "YY") in single-byte.

Enter "hour" and "minute" in double-byte.

Displayed content

The following log content can be viewed:

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** (*1)

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** (*1), OS startup time: **Display Startup Time** (*1)

The time and minutes are displayed in the format of **xx hours xx 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** (*1)
- At PC restoration: the computer is restored.
- At logon: the computer is logged on. Authentication target: **Display Authentication Target** (*1)
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)**.

*1: 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 (*1)
 - Operation terminal (*1)
 - Logon method (*1)
 - Logon authority (*1)
 - Session No (*1)
- When **Type** is **PC Shutdown** and the power of PC is cut off by force
 - Shutdown action: **Abnormal Shutdown** (*1)

*1: 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], Session No: [Session ID]
```

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], Session No:
[Session ID]
```

When cutting off the power of PC by force

```
Shutdown action: [Abnormal Shutdown]
```

Example of log:

```
CLIENT1 2015/05/30 01:15 SYSTEM D-DOMAIN PC startup Normal Computer has been started.Startup mode
[Normal mode startup]
CLIENT1 2015/05/30 01:20 user01 D-DOMAIN Logon Normal Logged on.Authentication target: [D-DOMAIN]
Connection method: [Local],Operation terminal: [CLIENT1],Logon method: [Domain Logon], Logon
authority: [User Authority],Session No: [0]
CLIENT1 2015/05/30 04:32 SYSTEM D-DOMAIN PC sleep Normal Computer has slept.Startup time:
[3hours12minutes]
CLIENT1 2015/05/30 05:15 SYSTEM D-DOMAIN PC restoration Normal Computer has been recoverd.
CLIENT1 2015/05/30 14:18 user01 D-DOMAIN Logoff Normal Logged off.
CLIENT1 2015/05/30 07:43 SYSTEM D-DOMAIN PC Shutdown Normal Computer has been shut down Startup time:
[2hours28minutes],OS startup time: [6hours28minutes]
```

Active Directory running in Windows Server(R) 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).

8.2.21 Linkage Application Log

This is the log sent by the application linked with the client (CT).

For applications linked with the client (CT), 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 **Windows > Log collection operation**, 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.

8.2.22 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

The following log content can be viewed:

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)

8.2.23 Wi-Fi Connection Log (Smart Device)

This log is collected when the smart device (agent) connects to a Wi-Fi access point.



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.
Refer to "[1.2.33 Wi-Fi Connection Log \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **Wi-Fi Connection Log** to **Yes**.

How to search in the Log Viewer

When searching in the Log Viewer, the web connection log is included in the results of "Device configuration change" log type.

When filtering search results, select **Smart device** for **Device**, **Device configuration change** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "Wi-Fi connection" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain name: Model name of the smart device

Type: Wi-Fi connection (fixed value) (*1)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Connection status: **connected** (fixed value) (*1)
- Access point SSID (*1)
- Access point BSSID (*1)

Example of **Content**:

Connected to Wi-Fi. Connection status: [connected], SSID: [001601830000], BSSID: [00:00:00:81:37:9c]

Note: (Not displayed)

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.24 Wi-Fi Connection Prohibition Log (Smart Device)

This log is collected when the smart device (agent) is attempting to connect to a Wi-Fi access point for which connections are prohibited.



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.
Refer to "[1.2.16 Wi-Fi Connection Prohibition \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Wi-Fi connection**, set **Wi-Fi connection prohibition** to **Prohibit**.

Also, in **Wi-Fi connection**, allow Wi-Fi connections, or specify access points to be prohibited.

Refer to "[2.4.1.17 Wi-Fi Connection](#)" for details on how to set the policy.

How to search

When searching in the Log Viewer, the Wi-Fi connection prohibition log is included in the results of "Device configuration change" log type.

When filtering search results, select **Smart device** for **Device configuration change** for **Log type**, and **Violation** for **Classification**.

You can filter the search results even when "Wi-Fi connection prohibition" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Wi-Fi connection prohibition** (fixed value) (*1)

Classification: Violation

Attachment: (not displayed)

Content: the following content is displayed:

- Connection status: **connection prohibited** (fixed value) (*1)
- Access point SSID (*1)
- Access point BSSID (*1)

Example of **Content**:

Connections to Wi-Fi are prohibited. Connection status: [connection failed], SSID: [001601830000], BSSID: [00:00:00:83:06:23]

Note: (Not displayed)

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.25 Bluetooth Connection Log (Smart Device)

This is the log collected when pairing with a Bluetooth device on the smart device (agent).

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **Bluetooth connection log** to **Yes**.



Bluetooth connection logs are obtained on completion of pairing.

Bluetooth connection logs are obtained only on completion of Bluetooth pairing. The logs are not obtained for connections after pairing. Refer to "[1.2.37 Bluetooth Connection Log \(Smart Device\)](#)" for details.

How to search

When searching in the Log Viewer, the Bluetooth connection log is included in the results of "Device configuration change" log type.

When filtering search results, select **Smart device** for **Device**, **Device configuration change** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "Bluetooth connection" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Bluetooth connection** (fixed value) (*1)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Name of paired Bluetooth device (*1)
- Type of paired Bluetooth device (*1)
- Connection status: **connected** (fixed value) (*1)
- MAC address of paired Bluetooth device (*1)

Example of **Content**:

Paired the Bluetooth device. Device name: [LBT-HS310], Device type: [Headphones], Connection status: [connected], MAC address: [00:1B:41:99:6D:D5]

Note: (Not displayed)

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.26 Bluetooth Connection Prohibition Log (Smart Device)

This log is collected when the smart device (agent) is attempting to connect to a Bluetooth device for which pairing is prohibited.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Bluetooth connection**, set **Bluetooth connection prohibition** to **Prohibit**.

Also, in **Bluetooth connection**, allow Bluetooth connections, or specify access points to be prohibited.

Refer to "[2.4.1.18 Bluetooth Connection](#)" for details on how to set the policy.

How to search

When searching in the Log Viewer, the Bluetooth connection prohibition log is included in the results of "Device configuration change" log type.

When filtering search results, select **Smart device** for **Device configuration change** for **Log type**, and **Violation** for **Classification**.

You can filter the search results even when "Bluetooth connection prohibition" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Bluetooth connection prohibition** (fixed value) (*1)

Classification: Violation

Attachment: (not displayed)

Content: the following content is displayed:

- Name of Bluetooth device for which pairing is prohibited (*1)
- Type of Bluetooth device for which pairing is prohibited (*1)
- Connection status: **connection prohibited** (fixed value) (*1)
- MAC address of Bluetooth device for which pairing is prohibited (*1)

Example of **Content**:

Bluetooth device pairing is prohibited. Device name: [LBT-HS310], Device type: [Headphones], Connection status: [connection prohibited], MAC address: [00:1B:41:99:6D:D5]

Note: (Not displayed)

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.27 Application Usage Log (Smart Device)

This log is collected when an application is used on the smart device (agent).



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.

Refer to "[1.2.34 Application Usage Log \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **Application usage log** to **Yes**.

How to search

When searching in the Log Viewer, the application usage log is included in the results of "Window title obtaining" log type.

When filtering search results, select **Smart device** for **Device**, **Window title obtaining** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "Application usage" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Application usage** (fixed value) (*1)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Application window title name (*1)
- Application name that was used (*1)

Example of **Content**:

When the application becomes active

```
The [Peaple] window has been detected. Application name: [com.android.contactsnrx]
```

Note: (Not displayed)

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.28 Application Usage Prohibition Log (Smart Device)

This log is collected when an application of a package name for which usage is prohibited is used on the smart device (agent).

Note that prohibition logs will not be collected when an application that is prohibited for use outside of business hours is started outside of business hours.



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.

Refer to "[1.2.17 Application Usage Prohibition \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

Select **Android > Application**, and then set **Application usage prohibition** to **Prohibit**.

Also, in **Android > Application**, set applications for which usage is prohibited. Refer to "[2.4.1.19 Application \(Android\)](#)" for details on how to set the policy.

How to search

When searching in the Log Viewer, the application usage prohibition log is included in the results of "Application startup prohibition" log type.

When filtering search results, select **Smart device** for **Device**, **Application startup prohibition** for **Log type**, and **Violation** for **Classification**.

You can filter the search results even when "Application usage prohibition" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Application usage prohibition** (fixed value) (*1)

Classification: Violation

Attachment: (not displayed)

Content: the following content is displayed:

- Prohibited package name (*1)
- Prohibition treatment: **Terminated by force** (fixed value) (*1)
- Prohibition result: **Successful** or **Failed** (*1)

Example of **Content**:

The startup of [com.android.camera] has been [Terminated by Force]. Result: [Successful]

Note: (Not displayed)

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.



When the prohibition result is "Failed"

When a prohibited application cannot be exited, the prohibition result will be "Failed".

8.2.29 Web Access Log (Smart Device)

This log is collected when accessing websites from the standard Android browser "Android Browser" on the smart device (agent).



Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used.

Refer to "[1.2.32 Web Access Log \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **Web access log** to **Yes**.

How to search

When searching in the Log Viewer, the web access log is included in the results of "Window title obtaining" log type.

When filtering search results, select **Smart device** for **Device**, **Window title obtaining** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "Web access" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Web access** (fixed value) (*1)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Window title name of the webpage that was accessed (*1)

Up to 519 halfwidth characters (259 fullwidth characters) can be displayed for the content. If the number of characters specified for the content exceeds this, the content will be truncated.

Example of **Content**:

The [Download Page] window has been detected.

Note: the following content is displayed:

- URL of the access destination (*1)
- Number of times accessed from the access history or bookmarks (number of visits) (*1)

The method of counting the number of visits is as follows:

- The number of visits increases by one each time an access is made from a site in the access history or bookmarks. However, the count does not increase when the same website is accessed consecutively.
- After the access history is deleted, the number of visits is set to "1" when you revisit the same URL.
- When you access a website in the access history directly, such as by direct input of the URL, or copy and paste, the number of visits to that point is increased by one.
- When you access the same website using multiple tabs, the number of visits will not increase regardless of how many times you switch the tab display.

Example of **Note**:

URL: [http://192.168.0.138/download.html], Number of visits: [2].

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.30 SD Card Mount/Unmount Log (Smart Device)

This log is collected when an SD card is mounted or unmounted on the smart device (agent).



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used. Refer to "[1.2.40 SD Card Mount/Unmount Log \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **SD card mount/unmount log** to **Yes**.

How to search

When searching in the Log Viewer, the SD card mount/unmount log is included in the results of "Device configuration change" log type.

When filtering search results, select **Smart device** for **Device**, **Device configuration change** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "SD card mount/unmount" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **SD mount/unmount** (fixed value) (*1)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Operation content: **Mount SD card** or **Unmount SD card** (*1)

Example of **Content**:

If mounting

[Mount SD card]

If unmounting

[Unmount SD card]

Note: If mounting, the following content is displayed. If unmounting, this information will not be displayed.

- Total capacity (Unit: MB) (*1)
- Used capacity (Unit: MB) (*1)
- Example of **Note**:

If mounting

Total capacity: [4096] MB, Used capacity: [2048] MB

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.31 SIM Card Mount/Unmount Log (Smart Device)

This log is collected when a SIM card is mounted or unmounted on the smart device (agent).

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **SIM card mount/unmount log** to **Yes**.

How to search

When searching in the Log Viewer, the SIM card mount/unmount log is included in the results of "Device configuration change" log type.

When filtering search results, select **Smart device** for **Device**, **Device configuration change** for **Log type**, and **Normal** for **Classification**.

You can filter the search results even when "SIM card mount/unmount" is set as a keyword. The keyword is searched for using partial match.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **SIM mount/unmount** (fixed value) (*1)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Processing content: **Mount SIM card, Change SIM card, or Unmount SIM card** (*1)

Example of **Content**:

If mounting

[Mount SIM card]

If changing

[Change SIM card]

If unmounting

[Unmount SIM card]

Note: If mounting or changing, the following content is displayed. If unmounting, this field will be blank.

- SIM serial number (*1)

- Example of **Note**:

- If mounting or changing:

Serial number: [8000000000000311363]

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

8.2.32 Incoming/Outgoing Calls Log (Smart Device)

This is the log of telephone numbers of incoming and outgoing calls used by a standard Android telephone on the smart device (agent). When those telephone numbers are registered to the standard Android phonebook, the full name of the other person is also obtained.



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used. Refer to "[1.2.36 Incoming/Outgoing Calls Log \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **Incoming/outgoing calls log** to **Yes**.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Incoming/outgoing calls** (fixed value)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Outgoing, missed, or incoming telephone number (*1)
- Name registered in the phonebook for outgoing, missed, or incoming telephone number (For numbers with no caller ID: **No caller ID**) (*1)
- Call time for outgoing or incoming calls (Missed call: **0** seconds) (*1)
- Call state: **Outgoing**, **Missed call**, or **Incoming** (*1)

Example of **Content**:

When outgoing

You called [1234567890]. Full name of recipient: [Tarou Fujitsu], Call time: [120] seconds, Call state: [Outgoing]

When missed

You received a call from [1234567890]. Full name of recipient: [Tarou Fujitsu], Call time: [0] seconds, Call state: [Missed call]

When incoming (caller ID)

You received a call from [1234567890]. Full name of recipient: [Tarou Fujitsu], Call time: [180] seconds, Call state: [Incoming]

When incoming (no caller ID)

You received a call from [No caller ID]. Full name of recipient: [], Call time: [180] seconds, Call state: [Incoming]

Note: (Not displayed)

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as keyword.

8.2.33 Application Configuration Change Log (Smart Device)

This log is collected when an application is installed or uninstalled on the smart device (agent).



Note

Features may be restricted due to the environment being used

When setting the policy, features may be restricted due to the environment being used. Refer to "[1.2.35 Application Configuration Change Log \(Smart Device\)](#)" for details.

Set policy for collection

Set the policy in the **Terminal Initial Settings** window, or the window displayed after the Management Console is started (CT policy settings window).

In **Android > Log collection operation**, set **Application configuration change log** to **Yes**.

Displayed content

The following log content can be viewed:

Name: Name of the smart device

Occurrence date and time: Date and time for collecting logs at the smart device

User ID: User ID set when the smart device (agent) was installed

Domain Name: Model name of the smart device

Type: **Application configuration change** (fixed value) (*1)

Classification: Normal

Attachment: (not displayed)

Content: the following content is displayed:

- Package name (*1)
- Processing content: **Install** or **Uninstall** (*1)

Example of **Content**:

When installing

[alarmclock] was installed.

When uninstalling

[alarmclock] was uninstalled.

Note: If installing, the following content is displayed. If uninstalling, this field is left blank.

- Application name (*1)

Example of **Content**:

When installing

Application name: [alarm]

*1: When performing keyword search in the Log Viewer, the value within the square brackets [] can be specified as a keyword.

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"> - Application name - Occurrence date and time
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"> - Name of printed file - Occurrence date and time
3	To know the status of logon prohibition	Analyze the data corresponding to logon prohibition.	User name	<ul style="list-style-type: none"> - User name - Occurrence date and time
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"> - Occurrence date and time
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"> - Name of file attachment - Occurrence date and time

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"> - Name of the export source file - Name of export destination file - Type of destination drive - Export type - Occurrence date and time
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"> - Name of the export source file - Name of export destination file - Export type - Occurrence date and time

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"> - Operation type - Name of source file - Name of destination file

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
				<ul style="list-style-type: none"> - Type of destination drive - Application name - Occurrence date and time
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"> - Operation type - Name of source file - Name of destination file - Type of destination drive - Application name - Occurrence date and time
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"> - Operation type - Name of source file - Name of destination file - Type of destination drive - Application name - Occurrence date and time

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"> - Occurrence date and time
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"> - Subject - From - To/CC/BCC - Attachment - Occurrence date and time

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"> - Name of printed file - Pages - Printer name - Occurrence date and time
2	To know the status of printing operation (pages)	Analyze the data corresponding to printed pages.	Name of printed file	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Name of printed file - Number of pages - Printer name - Occurrence date and time
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"> - Number of pages - Name of printed file - Occurrence date and time
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"> - Subject - From - To/CC/BCC - Attachment

No.	Objective	Content	Keyword Designated Target Item	Show Details Item
				- Occurrence date and time
6	To know the status of the FTP operation (upload)	Analyze the data corresponding to the FTP upload	File name	<ul style="list-style-type: none"> - FTP server - File name - Occurrence date and time
7	To know the status of the Web operation (upload)	Analyze the data corresponding to the Web upload	File name	<ul style="list-style-type: none"> - Access destination - File name - Occurrence date and time