FUJITSU

FUJITSU Software
Systemwalker Desktop Keeper

Installation Guide

Windows

Preface

Purpose of This Guide

This guide describes how to use the following products:

- Systemwalker Desktop Keeper V15.1.1

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 Microsoft(R) SQL Server (when updating from V12)

- 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 Design

This chapter introduces the design of Systemwalker Desktop Keeper.

Chapter 2 Installation

This chapter describes how to install Systemwalker Desktop Keeper.

Chapter 3 Maintenance

This chapter describes how to maintain Systemwalker Desktop Keeper.

Chapter 4 Upgrading

This chapter describes how to update from old versions of Systemwalker Desktop Keeper to Systemwalker Desktop Keeper V15.1.0 or later.

Chapter 5 Uninstallation

This chapter describes how to uninstall Systemwalker Desktop Keeper.

Appendix A Server Silent Installation

This appendix describes files, commands, and messages used in silent installation of the Systemwalker Desktop Keeper server.

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.

Manual Name	Content
Systemwalker Desktop Keeper Installation Guide (this 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 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 Centralized Management Guide	This guide explains how to centrally manage Systemwalker Desktop Keeper deployed at sites within and outside Japan.
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 Systemwalker Desktop Keeper V15.1.1	V15.1.0
Windows(R) Internet Explorer(R) 7 Windows(R) Internet Explorer(R) 8 Windows(R) Internet Explorer(R) 9 Windows(R) Internet Explorer(R) 10 Windows(R) Internet Explorer(R) 11	Internet Explorer(R)

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) 10 Home Windows(R) 10 Pro Windows(R) 10 Enterprise Windows(R) 10 Education	Windows(R) 10 (*1)
Windows(R) 8.1 Enterprise Windows(R) 8.1 Pro Windows(R) 8.1	Windows(R) 8.1 (*1)
Windows(R) 8 Enterprise Windows(R) 8 Pro Windows(R) 8	Windows(R) 8 (*1)

OS	Abbreviation
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(R) 10 Home Windows(R) 10 Pro Windows(R) 10 Enterprise Windows(R) 10 Education	Windows

OS	Abbreviation
Microsoft(R) Windows(R) Millennium Edition Microsoft(R) Windows(R) 98 Second Edition	
Android(TM) 3.0 - Android(TM) 5.1	Android
iOS 5.0 - iOS 8.4	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

- Windows(R) 10 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

November 2015

Revision History
July 2015, First Edition November 2015, Second Edition

Contents

Chapter 1 Design

This chapter describes the design of Systemwalker Desktop Keeper.

1.1 Considerations for Installation

This section explains the considerations for installing Systemwalker Desktop Keeper.

For considerations relating to each particular function, refer to *Systemwalker Desktop Keeper User's Guide for Administrator*.

Network Environment

- Use the following protocols to communicate:

    - [Management Server/Master Management Server] - [Management Server/Master Management Server]: HTTP

    - [Management Server/Master Management Server] - [Management Console]: HTTP

    - [Management Server/Master Management Server] - [Client (CT)]: TCP/IP Socket communications

    - [Management Server/Master Management Server] - [Log Analyzer Server]: TCP/IP Socket communications

    - [Management Server/Master Management Server] - [Web Console]: HTTP
      HTTPS is recommended.

    - [Log Analyzer Server] - [Report Output Tool]: TCP/IP Socket communications

- In [Management Server/Master Management Server] - [Client (CT)], or [Management Server/Master Management Server] - [Management Server/Master Management Server], when the communication data packet is restricted by the firewall, the server must be configured in a place where communication with the client (CT) can be performed. At this time, it will be closed within the domain area available for communication, and multiple independent systems that are not linked will start working.

- Communications between the Management Server/Master Management Server and client (CT) are encrypted.
  Therefore, there are restrictions on some 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. The following types of communication cannot be performed:

    - Immediate sending of a policy from a Management Server or Master Management Server of V15.0.0 or later to a client (CT) of V14.3.1 or earlier (to which the communication encryption update has not been applied)

    - Remote acquisition of materials by a Management Server or Master Management Server of V15.0.0 or later from a client (CT) of V14.3.1 or earlier (to which the communication encryption update has not been applied)

    - Setting of a CT debugging trace by a Management Server or Master Management Server of V15.0.0 or later for a client (CT) of V14.3.1 or earlier (to which the communication encryption update has not been applied)

    - Retrieval of a list of services from or control of services in a client (CT) of V14.3.1 or earlier (to which the communication encryption update has not been applied) by a Management Server or Master Management Server of V15.0.0 or later

    - Retrieval of a list of processes from or control of processes in a client (CT) of V14.3.1 or earlier (to which the communication encryption update has not been applied) by a Management Server or Master Management Server of V15.0.0 or later

    - Registration of a client (CT) by a client (CT) of V12.0L20 or earlier (to which the communication encryption update has not been applied) to a Management Server or Master Management Server of V15.0.0 or later

    - Policy retrieval request from a client (CT) of V12.0L20 or earlier (to which the communication encryption update has not been applied) to a Management Server or Master Management Server of V15.0.0 or later

- When communication between segments is restricted due to the use of VLAN, servers that can communicate directly must be set in each domain, which means that multiple Systemwalker Desktop Keeper servers need to be set.

- When performing the following communications, ports 137-139 and port 445 must be opened.
  When the printing logs of printing jobs performed on the printer server are not obtained, it is unnecessary to open these ports.

    - Communications between Master Management Server and Management Servers

    - Communications between Master Management Server and client (CT)

- Communications between Management Server and client (CT)

- If there is a NAT (Network Address Translation) environment between the server and the client (CT), the following types of communication cannot be performed:

  - Immediate sending of a policy from a Management Server or Master Management Server to a client (CT)

  - Remote acquisition of materials by a Management Server or Master Management Server from a client (CT)

  - Setting of a CT debugging trace by a Management Server or Master Management Server for a client (CT)

  - Retrieval of a list of services from or control of services in a client (CT) by a Management Server or Master Management Server

  - Retrieval of a list of processes from or control of processes in a client (CT) by a Management Server or Master Management Server

  - Communication of the self version management feature from a client (CT) of V15.0 or earlier to a Management Server or Master Management Server

  - Registration of a client (CT) by a client (CT) of V12.0L20 or earlier to a Management Server or Master Management Server

  - Policy retrieval request from a client (CT) of V12.0L20 or earlier to a Management Server or Master Management Server

- When connecting the Management Server/Master Management Server with the client (CT) through a VPN connection, the operations of Systemwalker Desktop Keeper, such as the collection of E-mail sending logs, may be affected. It is recommended to confirm the operations in advance when operating under such environment.

- If using a firewall in the Log Analyzer Server, open the port to be used by it. For information regarding the port used by the Log Analyzer Server, refer to "Port Numbers and Services" of *Systemwalker Desktop Keeper Reference Manual*.

- IPv6 addresses can be used.

- If using Log Analyzer in an environment that uses IPv6 addresses, host name resolution is required.

- Do not use link-local addresses. Behavior is not guaranteed if link-local addresses are used.

- The client (CT) must have resolved (forward or reverse lookup) the name of the Management Server or Master Management Server.

- The Management Server must have resolved (forward or reverse lookup) the name of the Master Management Server, or the Master Management Server must have resolved (forward or reverse lookup) the name of the Management Server.

- Line switching (dial-up) adapters cannot be used in clients (CT) because they cannot communicate with the Management Server.

Virtual Environment

- In a provisioning environment, depending on settings, user data may be discarded during shutdown of the virtual PC. If the log storage folder is in the disk of a virtual PC, accumulated operation logs and violation logs may be discarded. Take any of the following measures to prevent logs from being discarded:

  - In the settings of the virtual environment, set to not discard user data on the virtual PC.

  - In the settings of the provisioning environment, set an area in which user data will not be discarded and save the log saving folder in this area.

- In case of a dirty shutdown of the virtual PC (cut off the power of the virtual PC by force, etc.), and in case of a dirty shutdown of the running terminal of the virtual PC (cut off the power of the physical PC or Hypervisor, etc.), operation logs and violation logs may not be saved. Be sure to shut down the virtual PC and physical PC by normal procedure.

- For a clone PC, since it is not managed on the Management Server, CT policy and user policy cannot be applied immediately. Apply user policy after logging off and then logging on again.

Installer

- Considerations for using Unicode characters
  When the ID for logon to Windows is a user ID (*1) that contains Unicode-specific characters, an error will occur in all installers

during the installation process and installation will be interrupted.

*1: Applicable to a device in which a user ID that contains Unicode-specific characters was used during the installation process or at least once for logon.

- If a Windows firewall is enabled in any of the following OS, after the product has been installed, register the port number used in the product as "Exception" in the firewall and open the port.

    - Windows(R) 7

    - Windows Vista(R)

    - Windows Server(R) 2003

    - Windows Server(R) 2008

    - Windows(R) 8

    - Windows(R) 10

    - Windows Server(R) 2012

Management Server/Master Management Server

- If the IP address specified using the Server Settings Tool differs from the actual IP address, the Management Server or Master Management Server service will not start.

- Do not make significant changes to the system time of the Management Server and Master Management Server. When the system time is modified, the Management Server and Master Management Server may not run normally.
  When the system time is modified significantly, restart the Management Server and Master Management Server.

- The logon information in the Server Settings Tool and the execution information of the Active Directory Linkage will be output to the event log (application).

- When Systemwalker Desktop Keeper V14.3.0 or earlier is upgraded, the Web Console is provided as a 32-bit application. When the Management Server or Master Management Server is installed, IIS is set automatically to create 32-bit worker processes. As a result, 64-bit applications can no longer be used in IIS.

- When Systemwalker Desktop Keeper V15.0.0 or later is first installed to a 64-bit operating system, the Web Console is provided as a 64-bit application. As a result, 64-bit applications can be used in IIS.

Log Analyzer Server

- When the log data aggregation results and the number of target items exceeds 2GB and the available disk space is not enough, aggregation processing and result display or report output will not run normally and an error will occur.

- About character data
  Non-Shift JIS characters (such as Unicode characters that do not have a corresponding Shift JIS, including JIS2004, code) cannot be used in strings (such as an installation path, folder path, user ID or password) to be set in the Log Analyzer Server. Non-Shift JIS characters cannot be used for Log Analyzer users (Windows accounts that will log on to Windows) either.
  Non-Shift JIS characters will not be handled correctly. For example, they will be converted to other characters or an error will occur. However, in the **Keyword** column of **Aggregate by Objective** of Log Analyzer (Web Console), and in the **Keyword** column of **Screening Condition Settings** of the **Configuration Management** window, Unicode characters including JIS 2004 can be used.

Smart Device Relay Server

- Only CT policies can be applied to smart devices (agent). User policies cannot be applied.

- Even if a smart device (agent) is not being operated, data communication will be periodically performed (policies are periodically sent and received, and operation logs are periodically sent) between a smart device (agent) and the Smart Device Relay Server. Preferably use a fixed price plan for data communication from your smart device (agent).

- Reinstalling the Smart Device Relay Server initializes the information regarding connection to the database. Use SDSVSetMS.EXE (Change Configuration of Smart Device Relay Server) to reset the information regarding connection to the database. Refer to "SDSVSetMS.EXE (Change Configuration of Smart Device Relay Server)" in the *Systemwalker Desktop Keeper Reference Manual* for details on the command.

Management Console

- In a 3-level system structure, the Management Console can be installed in both the Management Server and Master Management Server. If a Policy is set from multiple Management Consoles, the Policy that was set last is reflected in the client (CT).

Client (CT)

- When applications similar to Systemwalker Desktop Keeper control, such as the filter driver control that restricts writing in devices and hook control (when installing products like INSTANT COPY), exist at the same time, operation will not be guaranteed. Moreover, VMware ThinApp does not operate properly due to a conflict with the hook control of Systemwalker Desktop Keeper.

  What is hook control:

  Hook control refers to the control that intercepts and views required content from the data transferred through a particular interface, and returns to the original processing flow after processing.

- After upgrading an OS with the client (CT) installed, the client (CT) may not run normally. (for example, upgrading from Windows(R) 7 to Windows(R) 8)
  When upgrading the OS, perform the upgrade after uninstalling the client (CT), and then install the client (CT) again. To associate and register the client with the same CT as previously during reinstallation, open the **System settings** window in the Server Settings Tool and specify **Not use** for **OS Type** in the conditions for determining an identical CT during CT registration.

  Moreover, you can restore Windows(R) 10 to the pre-upgrade version. (for example, restoring to Windows 8.1 after upgrading to Windows(R) 10).
  In this case, if the client (CT) is installed, it will no longer operate properly. Perform the same procedure as that when upgrading the operating system.

- When a new CD/DVD device is connected for the first time, restart. Without restarting, the newly connected CD/DVD device will not work properly.

- If an export prohibition for the CD/DVD has been set, the DVD-ROM (DVD-Video) or CPRM DVD may not be playable in the DVD play software. Remove the export prohibition for the CD/DVD temporarily, or use another DVD play software.

- The CT cannot coexist with "Net screen Remote" of Juniper Corporation. It can be run by uninstalling the Virtual Adapter function of "Net screen Remote".
  In addition, in an environment where there is coexisting VPN software (such as Net screen Remote), communication may fail.

- In an environment where there is a coexisting capture product, neither function may run normally.

- When the client (CT) is installed on the computer with Virus Buster 2007 installed, the "Network connection environment has been changed" dialog box of Virus Buster 2007 may be displayed, but this is okay.

- When the OS of the client (CT) is Windows Vista(R), Windows Server 2008(R), Windows(R) 7, Windows(R) 8, Windows(R) 10, or Windows Server(R) 2012 and authority promotion is allowed and operation can be continued in UAC, the following logs cannot be collected:

  - The printing log oriented for network printer

  - The structure change log of network driver

- Under the environment with TC Plink installed, after the PrintScreen key has been pressed, the network printer may print two pieces of paper.
  Modify the settings of this network printer from "Lan Manager Printer Port" to "Standard TCP/IP Port".

- In an environment using an Intel LAN adapter under Windows Vista(R) (No Service Pack), when using the "Receiving scaling" function of the LAN adapter, E-mail may not be sent. Use Windows Vista(R) Service Pack 1 or later.

When Shutting down or Restarting Computer

When shutting down or restarting the Management Server and Master Management Server, it is necessary to follow the steps below.

Note

How to stop server correctly

In order to prevent loss of previous logs of the client (CT) saved in the database, be sure to follow the steps below.

1. When the Windows Services window is displayed in the Management Server or Master Management Server, select the following services, and select "Stop" from the "Action" menu. It may take about 30 seconds to 1 minute to stop. In addition, immediately after restarting SWServerService or after the date has changed (00:00), available space in the database will be checked. This check takes approximately 15 minutes, and services may not stop during this time. Wait for a few moments and then check if the services have stopped.

   - SWLevelControlService

   - SWServerService

   - PostgreSQL RDB SWDTK

2. Shun down or restart the Management Server/Master Management Server.

Restrictions of Remote Operation

Under the following environments, operations such as "Remote Desktop Connection" of Windows cannot be performed through the Windows Terminal Service. It is the same when the session of a remote connection remains. Be sure to log off after establishing a remote connection.

- When shifting command is used to perform a version upgrade of Systemwalker Desktop Keeper V13.0.0/V13.2.0/V13.2.1

- An environment in which a version prior to V13.2 of the following products that share a database with Systemwalker Desktop Keeper is installed before Systemwalker Desktop Keeper:

   - Systemwalker Centric Manager

   - Systemwalker Desktop Patrol

   - Systemwalker Desktop Rights Master

When Performing System Backup

When the system backup software is used in the Management Server/Master Management Server/Log Analyzer Server for system backup, note the following:

- Even if the Management Server, Master Management Server, or Log Analyzer Server is installed to a drive other than the system drive, some Systemwalker Desktop Keeper programs will be installed to the system drive.
  Perform backup and restore for both the installation drive and the system drive.

- It is required to stop the service during backup. Perform backup according to the following procedure:

   In case of Management Server/Master Management Server

   1. When the Windows Services window is displayed in the Management Server or Master Management Server, select the services in the following order, and select "Stop" from the "Action" menu. It may take about 30 seconds to 1 minute to stop. In addition,

immediately after restarting SWServerService or after the date has changed (00:00), available space in the database will be checked. This check takes approximately 15 minutes, and services may not stop during this time. Wait for a few moments and then check if the services have stopped.

   a. SWLevelControlService

   b. SWServerService

   c. PostgreSQL RDB SWDTK

   d. PostgreSQL RDB SWDTK2

2. After system backup has completed, start the stopped serviced in the following order:

   a. PostgreSQL RDB SWDTK2

   b. PostgreSQL RDB SWDTK

   c. SWServerService

   d. SWLevelControlService

In case of Log Analyzer Server

1. Confirm the Log Analyzer functions that are not used.

2. When the Windows Services window is displayed in the Management Server or Master Management Server, select the services in the following order, and select "Stop" from the "Action" menu. It may take about 30 seconds to 1 minute to stop.

   a. SymfoWARE RDB SWDTLA

3. After system backup has completed, start the stopped services in the following order:

   a. SymfoWARE RDB SWDTLA

64-bit support

- 64-bit components cannot be installed to a 32-bit operating system.

- 64-bit components cannot be upgraded in a 32-bit component environment. Upgrade installation is not supported for the Log Analyzer Server.

- Connection between the Management Server and the Log Analyzer Server is possible only when both are the same version (32-bit or 64-bit).

- Only the 64-bit version can coexist with a 64-bit WSUS server. Similarly, only the 32-bit version can coexist with a 32-bit WSUS server.

- The Report Output Tool does not support the 64-bit version of Microsoft(R) Office.

1.2 Determine Operation Method

Based on various elements such as the scale of the Client being managed, functions being used, methods of importing the configuration information, configuration of administrators, etc., there are several operation methods. To help you determine the operation method, this section explains the requisite design elements and how you can combine them.

1.2.1 Determine System Structure

This section describes the recommended system structure when Systemwalker Desktop Keeper is used.

The whole image of the system structure of Systemwalker Desktop Keeper is as follows:
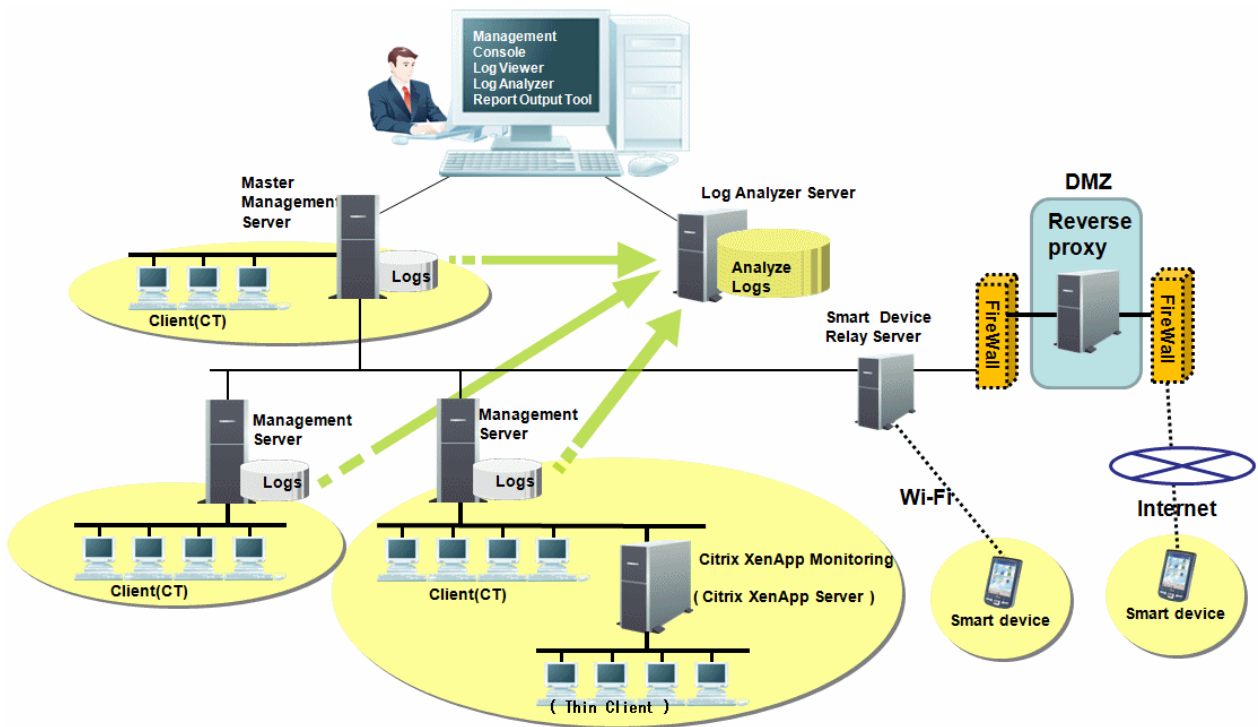
This describes the setting standard for the Management Server, Master Management Server, the Log Analyzer Server, and the Smart Device Relay Server. When using the log analysis function or the report output function, determine the structure after judging the respective setting standard of the Management Server/Master Management Server or the Log Analyzer Server comprehensively.

1.2.1.1 Determine the Installation Standard for Management Servers

The number of Management Servers required can be judged according to the number of clients (CTs) and smart devices (agents) being managed and whether file operation logs are collected.
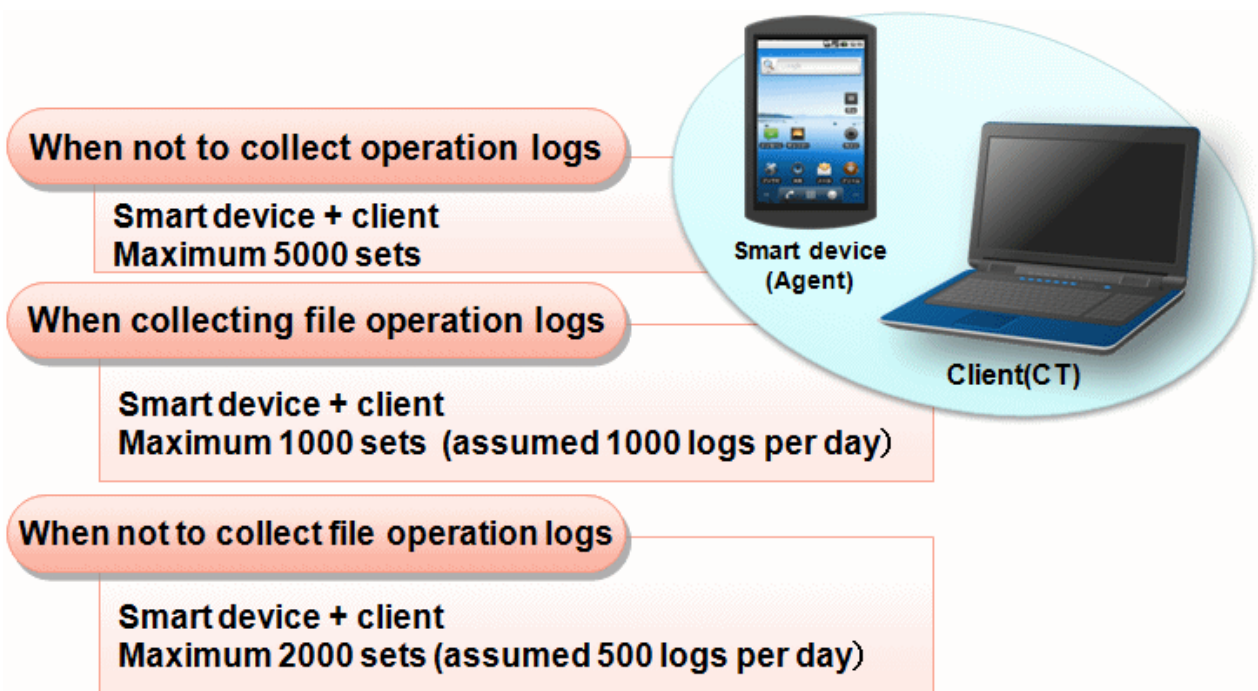
A single Management Server can manage a total of 5000 clients (CTs) and smart devices (agents). The standard is as follows:

When not to collect operation logs

- The maximum recommended number of clients (CTs) and smart devices (agents) is 5000.

When collecting file operation logs

- The maximum recommended number of clients (CTs) and smart devices (agents) is 1000 (assuming 1000 logs/day).

When not to collect file operation logs

- The maximum recommended number of clients (CTs) and smart devices (agents) is 2000 (assuming 500 logs/day).

1.2.1.2 Determine the Installation Standard for Master Management Servers and Expansion Standard for Management Servers

If the number of clients (CTs) that can be managed by one Management Server exceeds the standard, it is better to add more Management Servers, and equally allocate those clients (CTs) under each Management Server. Meanwhile, one Master Management Server should be set.
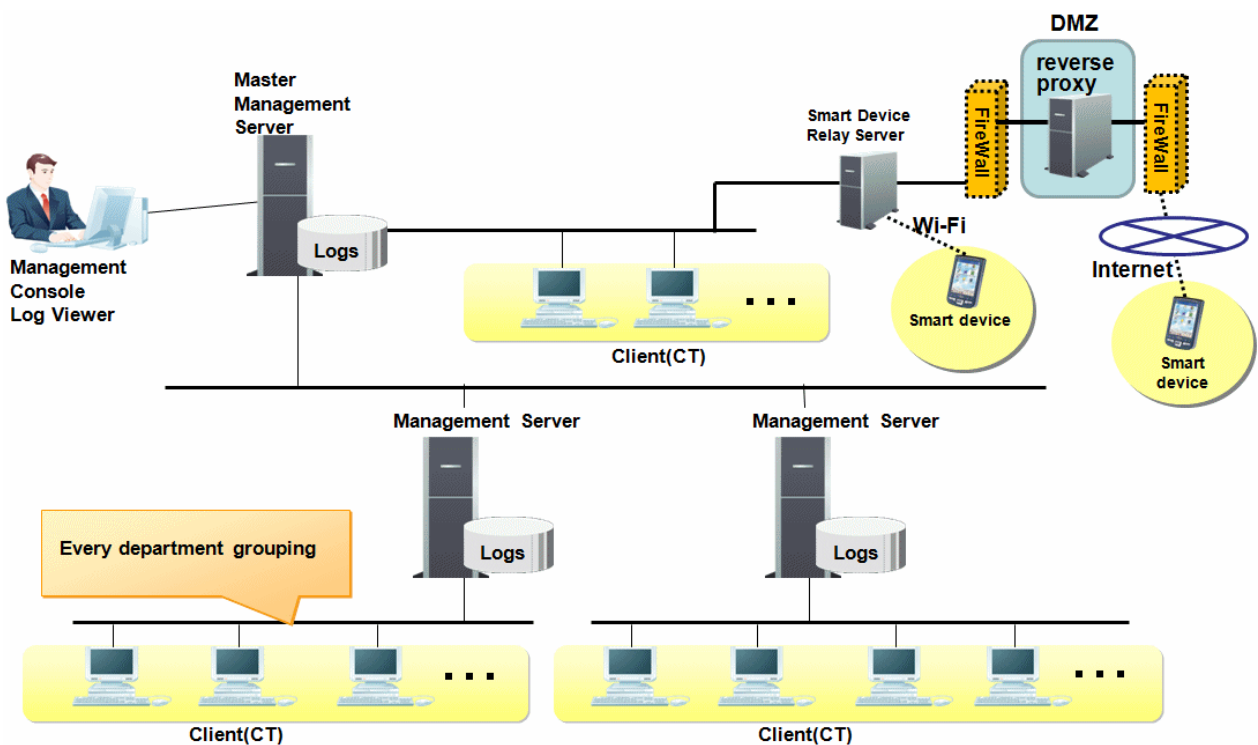
P Point

Create client (CT) group for every department

Creating a group for each organization facilitates client (CT) management.

However, client (CT) groups cannot be created across multiple Management Servers. Create a client (CT) group using clients (CTs) managed by the same Management Server.

1.2.1.3 Determine the Installation Standard for Log Analyzer Server

When the log analysis function and report output function are used, the number of needed Log Analyzer Servers can be judged.

Judgment of the number of Log Analyzer Servers to be set can be performed according to the following three points:

- **Organization structure**

    Log analysis and report output of Systemwalker Desktop Keeper is performed in the unit of the Log Analyzer Server.

    If one organization (company) is made up of multiple Log Analyzer Servers, neither the aggregation of the whole organization (company) nor the whole organization (company) can be summarized in one report.

    It is necessary to consider organization structure, determine the aggregation unit and report summarization unit and set the Log Analyzer Server accordingly.

- **Aggregation condition**

    In order to analyze and aggregate logs, "Screening Condition" and "Exclusion Condition" can be set in the unit of the Log Analyzer Server.

    The keyword for log aggregation, etc., can be set in "Screening Condition". A PC that is not the aggregation target can be set in "Exclusion Condition".

    If the same Log Analyzer Server is set when conditions differ depending on the organization, the range of conditions will be too great, which may lead to lower accuracy of analysis. It is necessary to set the Log Analyzer Server in the organization unit with relatively similar conditions.

    For what kind of conditions should be set, refer to "1.2.8 Determine Analysis Condition of the Log Analyzer".

- **Amount of logs**

    When the amount of logs being analyzed or aggregated is too great, the aggregation process may take some time, and an error may occur.

    The maximum recommended standard for the number of logs to be analyzed by the Log Analyzer Server is 180 million, assuming there are 500 clients (CTs) and one PC collects 1000 logs/day and stores them for one year. In addition, take around 500 thousand logs to be moved in at most per day as a standard.

    When this standard is exceeded, consider adding more Log Analyzer Servers.

Apart from examining the above factors, the relationship with the Management Server/Master Management Server should also be considered.

The Log Analyzer Server can be installed on the computer with the Management Server/Master Management Server installed. In addition, it can also be installed on a computer that is different from the one with the Management Server/Master Management Server installed.

Log information of multiple Management Servers/Master Management Servers can be analyzed on one Log Analyzer Server. However, log information on one Management Server/Master Management Server cannot be distributed to multiple Log Analyzer Servers for analysis and aggregation.

In addition, the environment between the Log Analyzer Server and the Management Server/Master Management Server must enable the setting of a network shared folder. The shared folder is created on the Log Analyzer Server.

The following information is transferred from the Management Server/Master Management Server to the Log Analyzer Server using this shared folder:

- Operation logs collected on the Management Server/Master Management Server

- Administrator information

The transmission schedule can be set separately, but it is recommended to perform this during the night while business is stopped. Log transmission will be performed only once per day.

The system structure of the Management Server/Master Management Server and the Log Analyzer Server includes the following two patterns:

When setting Log Analyzer Server for one Management Server

When operating with one Management Server, configure the Log Analyzer Server on this Management Server. However, when hardware requirements are not satisfied, it is okay to use another server.

When setting Log Analyzer Server for multiple Management Servers

When operating with multiple Management Servers/Master Management Servers, the user must install Log Analyzer Servers based on the number of clients (CTs) and the log saving period on the Log Analyzer Server.

The setting standard of one Log Analyzer Server is as follows, calculated from 1000 logs as the log amount of one client (CT) per day:

Log Saving Period	Number of CTs managed in the Log Analyzer Server	Average number of Management Servers (including the Master Management Server) (Notes)
2 months	3000 pcs	6 pcs
3 months	2000 pcs	4 pcs
6 months	1000 pcs	2 pcs
12 months (1 year)	500 pcs	1 pcs

Notes: Calculated from 500 clients (CTs) managed by one Management Server.

If the log saving period is 2 months, the structure example of 1 Master Management and 5 Management Servers (average number of clients (CTs) of each server is 500) is as follows:

Management Server/Master Management Server = count 6 sets
* 500 sets of CT are managed by each server on average
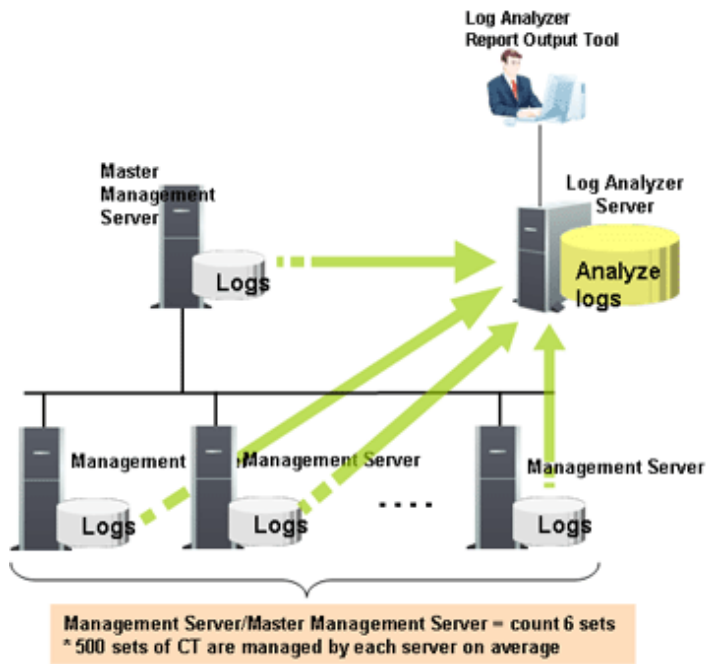
1.2.1.4 Determine the Installation Standard for Smart Device Relay Servers

The number of smart devices (agents) that can be managed is as follows:

- Only one Smart Device Relay Server can be installed.

- Up to 1,000 smart devices (agents) can be managed by one Smart Device Relay Server.

When both Systemwalker Desktop Keeper and Systemwalker Desktop Patrol are used to manage iOS devices, the Smart Device Relay Server and Systemwalker Desktop Patrol SS must coexist.

P Point
. . . .

Relative position of the Management Server/Master Management Server and the Smart Device Relay Server

In a 3-level system structure, connect the Smart Device Relay Server to the Master Management Server.

In a 2-level system structure that does not contain a Master Management Server, connect the Smart Device Relay Server to the Management Server.

Figure 1.1 3-level system structure
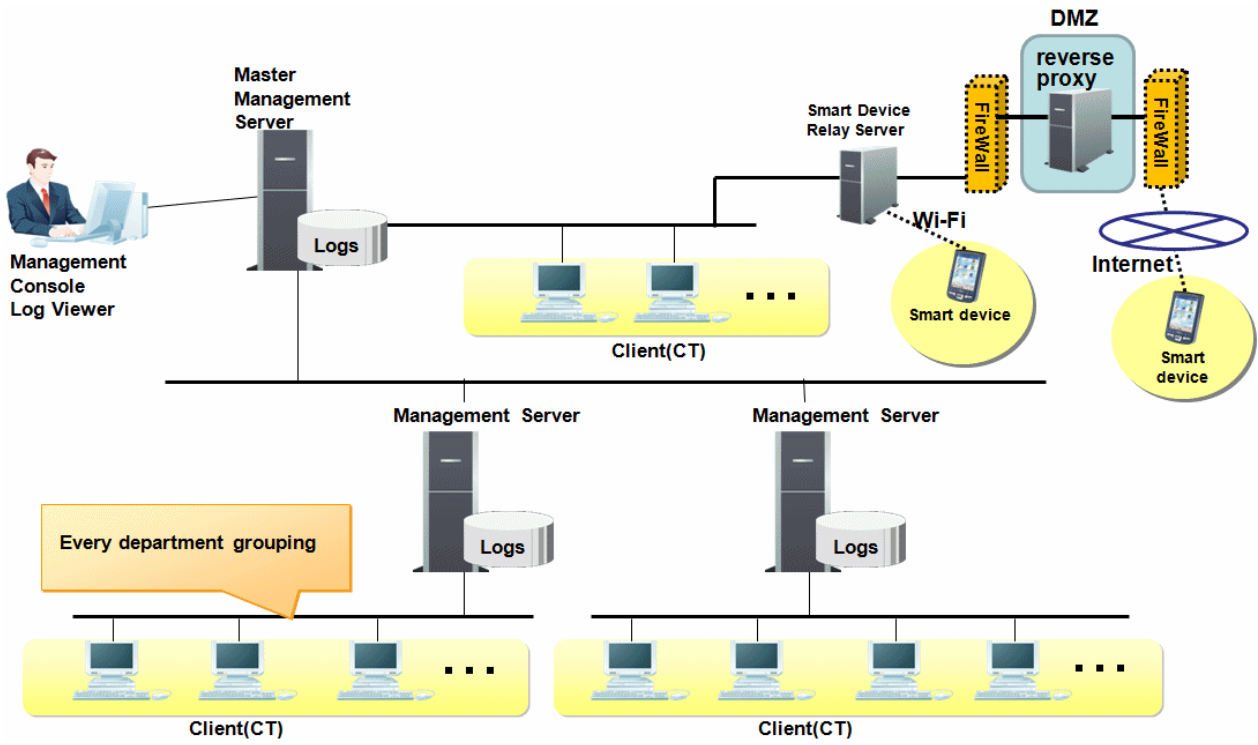
Figure 1.2 2-level system structure

··
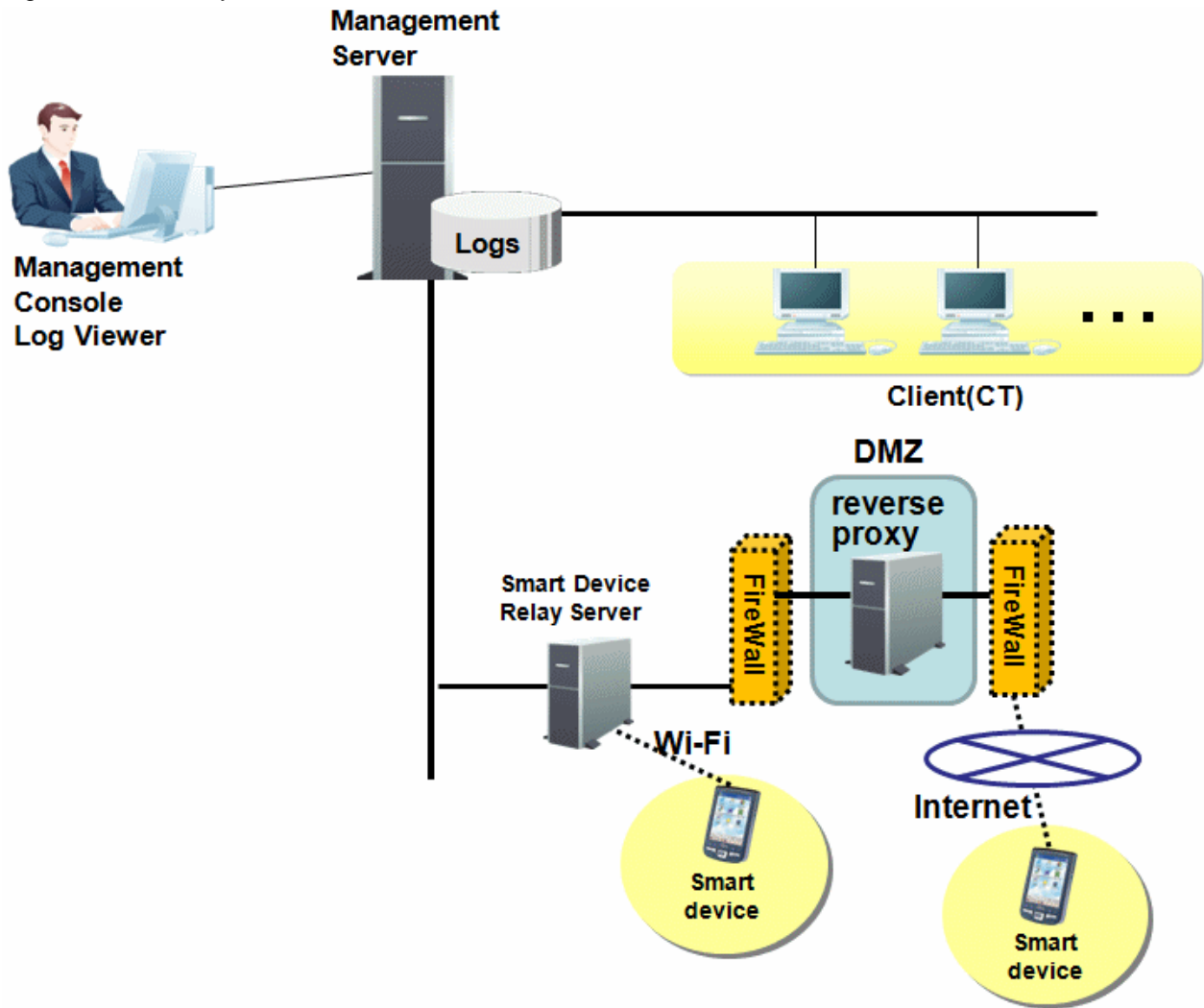
1.2.2 Determine Structure of Administrators

This department describes the types of Systemwalker Desktop Keeper administrators and their roles.

There are several types of administrators differentiated below.

System Administrator

    The system administrator defined in this product refers to the administrator who defines and manages policies such as the prohibition of client (CT) and smart device operation and the collection of operation logs, and takes charge of the security of the entire system. Apart from setting policies, the system administrator can also view and operate CT information, smart device (agent) information, user information, or log information of the entire system.

Department Administrator

    Differing from the system administrator, department administrators only have authority under a particular department. Department administrators are assigned with necessary rights depending on purpose, and they cannot view or operate information of departments for which they are not authorized. Department administrators can be set in each client (CT) group and user group.

    The system administrator will be overloaded if he or she must always control the whole system.

    By setting department administrators who only have authority under particular departments (CT groups) and assigning them with appropriate rights for managing information, the system administrator can reduce his or her own workload.

    The department administrator settings can also be configured after the operation has been started. For details of functions that can be used by department administrator, refer to "Functions Available for Each Type of Administrator".

USB Device Administrator

Differing from the system administrator and department administrator, USB device administrators are only authorized to register/modify/delete USB devices. They cannot perform policy settings, etc. By setting USB device administrators, the workload of the system administrator and department administrators can be reduced.

Collective Management based on System Administrator (Applied when Department Administrators are not configured)

This is a setting in which all policy settings and log viewings are performed by the system administrator. Policy setting and log viewing of all users and all clients (CTs) and smart devices (agents) can be performed and all functions can be used.

Distributed Management based on Multiple Administrators (Applied when Department Administrators are configured)

This is a setting in which a department administrator is set for every department to set policies and view logs within each department. Because policies can be modified and logs can be viewed by the Department Administrator, management of the system becomes easier under this configuration.
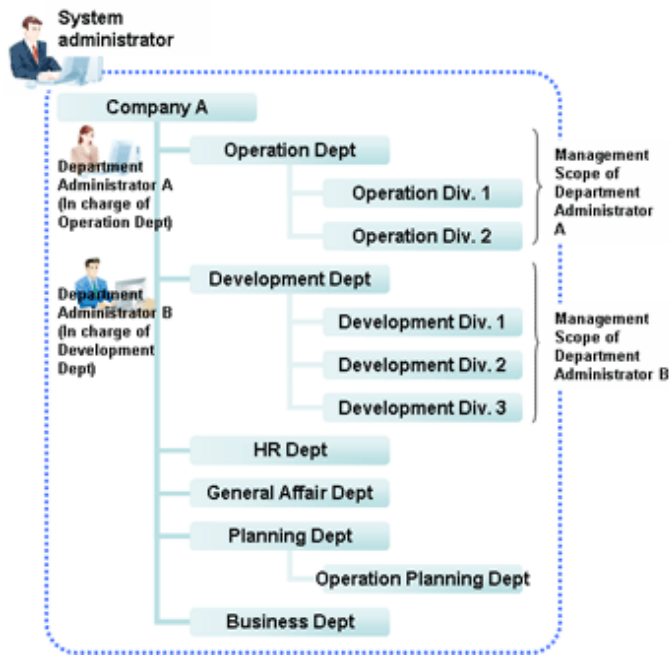
The system administrator can manage the security of the entire system under the Root directory, while department administrators only have authority for a particular department. For example, as shown in the image above, Department Administrator A can define policy for "Business Department" and view logs, but cannot define policy for "Development Department" or view logs there.

The functions that can be used primarily by department administrators are as follows. For detailed information about the function and scope of each operation window, refer to "Functions Available for Each Type of Administrator".

- The client (CT) group that is set as department administrator has the following functions:

    - View management information of clients (CTs) and smart devices (agents)

    - Move (within department management group), delete clients (CTs) and smart devices (agents)

    - View, modify CT policy

    - Create, move (within department management group) and delete CT group

    - Search, view logs

    - CSV export of logs, view and save (restrict as well) attached data

- The user group that is set as department administrator has the following functions:

    - Add, view and modify user information

    - Move (within department management group), delete user information

    - View, modify user policy

    - Create, move (within department management group) and delete user group

    - Search, view logs

    - CSV export of logs, view and save (restrict as well) attached data

Functions Available for Each Type of Administrator

This section describes the function differentiations under administrator mode and department management mode in the Management Console and the Log Viewer of Systemwalker Desktop Keeper.

Function Differentiations in Management Console

This section describes the function differentiations between system administrator and department administrator in the Management Console.

Classification		Function	Allowed			
			System Administrator	Department Administrator	USB Device Administrator	Remarks
Menu Bar	File	Search CT/CT Group	Y	R	N	
		Create CT Group	Y	R	N	*5
		Delete CT Group	Y	R	N	*5
		Set Department Administrator of CT Group	Y	N	N	
		Export CT Information in CSV Format	Y	R	N	*2
		Export CT Group Information in CSV Format	Y	N	N	*2
		Import Department Administrator of CT Group in CSV Format	Y	N	N	*1
		Export Department Administrator of CT Group in CSV Format	Y	N	N	*2
		Collect Remote Materials	Y	N	N	
		CT Debugging Trace	Y	Y	N	
		Output IP Address of Subordinate CT	Y	Y	N	
		Change Password	Y	Y	Y	
	Display	View/Set Terminal Information	Y	R	N	
		Get/Control Service List	Y	R	N	
		Get/Control Process List	Y	R	N	
	Tree Settings	Refresh Tree (All Servers)	Y	Y	N	
		Refresh Tree (Selected Servers)	Y	Y	N	
		Unfold All Trees	Y	Y	N	
		Fold All Trees	Y	Y	N	
		Do not Display Empty Group	Y	Y	N	
		Reflect CT Group Structure	Y	Y	N	
		Display Server	Y	Y	N	*3
		Display "Deleted" Group	Y	N	N	
	List Settings	Settings of CT List Display Columns	Y	Y	N	
	Operation Settings	Terminal Initial Settings	Y	N	N	

Classification		Function		Allowed			
				System Administrator	Department Administrator	USB Device Administrator	Remarks
		Terminal Operation Settings			N	N	
		USB Device Registration		Y	Y	Y	*6
		Get Latest Information at Startup		Y	Y	N	
		Debugging Trace		Y	N	N	
		Management Console Trace		Y	Y	N	
	User Settings	**User Policy Settings**		Y	R	N	
	Link with Other System	**Link with Systemwalker Desktop Patrol**	**Import Configuration Information**	Y	N	N	*1, *4
			Export Configuration information	Y	N	N	*2, *4
CT List window		**Copy Policy**		Y	R	N	
		Paste Policy		Y	R	N	
		Delete CT		Y	R	N	*5
		Collect Remote Material		Y	N	N	
		CT Debugging Trace		Y	Y	N	
Policy List window		**Set CT Group Policy**		Y	R	N	
		Set CT Policy		Y	R	N	
		Refresh Policy		Y	R	N	
		Update at Next Startup		Y	R	N	
		Update Immediately		Y	R	N	
Drag-and-drop operation		Move CT Group		Y	R	N	*5
		Move CT		Y	R	N	*5

Legend: Y=No restriction, N=Cannot be used, R=Restricted, can be used within the range managed by department administrator
*1: Authority to import CSV file is required
*2: Authority to save CSV file is required
*3: Configure the settings to always display the server during linkage with Active Directory.
*4: Cannot be used when linking with Active Directory
*5: Can be used only in Local group during linkage with Active Directory
*6: Authority to register/update/delete USB device is required

User Policy Settings window

Classification		Function	Allowed		
			System Administrator	Department Administrator	Remarks
Menu Bar	**File**	**Search User/User Group**	Y	R	
		Create User Group	Y	R	*3

Classification		Function	Allowed		
			System Administrator	Department Administrator	Remarks
		Delete user group	Y	R	*3
		Set Department Administrator of User Group	Y	N	
		Import Department Administrator of User Group in CSV Format	Y	N	*1, *3
		Export Department Administrator of User Group in CSV Format	Y	N	*2
	Tree Settings	Refresh Tree	Y	Y	
		Unfold All Trees	Y	Y	
		Fold All Trees	Y	Y	
		Do not Display Empty Group	Y	Y	
		Reflect User Group Structure	Y	Y	
	Link with CSV	Import User Information in CSV Format	Y	R	*1, *3
		Export User Information in CSV Format	Y	R	*2
User List window		Copy Policy	Y	R	
		Paste Policy	Y	R	
		Delete User	Y	R	*3
User Properties window		Enter a New User	Y	R	*3
		Update User Information	Y	R	AD link items cannot be modified
User Policy List window		Apply Group Policy	Y	R	
		Do not Apply Group Policy	Y	R	
		Set Terminal Initial Setting Value	Y	R	
Drag-and-drop operation		Move User Group	Y	R	*3
		Move User	Y	R	*3

Legend: Y=No restriction, N=Cannot be used, R=Restricted, can be used within the range managed by department administrator
*1: Authority to import CSV file is required
*2: Authority to save CSV file is required
*3: Can be used only in Local group during linkage with Active Directory.

Function Differentiations in Log Viewer

This department describes the function differentiations between system administrator and department administrator in the Log Viewer.

Classification	Function	Allowed		
		System Administrator	Department Administrator	Remarks
Database	Operation Database	Y	R	

Classification	Function		Allowed		
			System Administrator	Department Administrator	Remarks
	Log Viewing Database		Y	R	
CT Operation Log/ User operation log/ Configuration Change Log *3	Select Department		Y	R	
	Refresh		Y	Y	
	Search Conditions		Y	R	
	List of logs		Y	R	
	Display items settings	Display items settings	Y	R	
		Department display settings	Y	N	
		Violation CT display settings	Y	R	
	CT/CT group search		Y	R	
	CSV Export		Y	R	*2
CT Operation Log window	List of Problem PC(s)		Y	R	
	File Trace		Y	R	
	View/Save Additional Information		Y	R	*1,*4

Legend: Y=No restriction, N=Cannot be used, R=Restricted, can be used within the range managed by department administrator
*1=When viewing **Additional** information and executing **Save File**, "Authority to View/Save Additional Information" is required
*2="Authority to Save CSV File" is required
*3= When viewing the **Configuration Change Log** window, "Authority to View Configuration Change Log" is required"
*4=When viewing E-mail sending content through **Additional** information, "Authority to View E-mail Content" is required"

Function Differentiations in Status Window

This section describes the function differentiations between system administrator and department administrator in the Status Window.

Classification	Function	Allowed		
		System Administrator	Department Administrator	Remarks
Status Window	View the status window	Y	R	
Environment Setup Window	Set aggregation conditions	Y	N	

Legend: Y=No restriction, N=Cannot be used, R=Restricted, can be used within the range managed by department administrator

Function Differentiations in Log Analyzer

This section describes the function differentiations between system administrator and department administrator in the Log Analyzer.

Classification	Function	Allowed		
		System Administrator	Department Administrator	Remarks
Information Disclosure Prevention Diagnosis window	Information Disclosure Prevention Diagnosis	Y	N	*1
	Ranking	Y	N	*1

Classification	Function	Allowed		
		System Administrator	**Department Administrator**	**Remarks**
	Graph Display	Y	N	*1
Aggregate by Objective window	Result List (Aggregation Result)	Y	N	*1
	Result List (Detailed Result)	Y	N	*1
	CSV File	Y	N	*1
Ranking Settings window	Set Ranking Display	Y	N	*1
Screening Condition Settings window	Register/Add/Delete Screening Conditions	Y	N	*1
Exclusion Condition Settings window	Set Exclusion Conditions	Y	N	*1
Operation Settings window	Set Violation and Eco Auditing	Y	N	*1
Select Server window	Select Log Analyzer Server	Y	N	*1

Legend: Y=No restriction, N=Cannot be used, R=Restricted, can be used within the range managed by department administrator

*1=In case of 3-level systems, only the system administrator of Master Management Server can use

Function Differentiations in Report Output Tool

This section describes the function differentiations between system administrator and department administrator in the Report Output Tool.

Classification	Function	Allowed		
		System Administrator	**Department Administrator**	**Remarks**
Comprehensive analysis report	Output comprehensive analysis report	Y	R	
Information disclosure analysis report	Output information disclosure analysis report	Y	R	
Terminal usage analysis report	Output terminal usage analysis report	Y	R	
Violation operation analysis report	Output violation operation analysis report	Y	R	
Printing volume auditing report	Output print volume auditing report	Y	R	

Legend: Y=No restriction, N=Cannot be used, R=Restricted, can be used within the range managed by department administrator

1.2.3 Determine How to Create Configuration Information

This section explains the configuration information of managed targets in Systemwalker Desktop Keeper.

The configuration information is composed of the following three types of information:

- Organization information

- User information

- Client (CT) information (Computer information and smart device information)

There are three approaches to create configuration information during initial installation. Decide which approach will be used for creation in the process of design.

- Link with the Active Directory (smart device information is not included)

- Link with Systemwalker Desktop Patrol (smart device information is not included)

- Input in the Management Console window

Examples of creating configuration information are shown in the images below.

Active Directory Linkage

After the configuration information has been imported by linking with the Active Directory, the imported information will be located under the domain group. The organization structure, user information, and computer information that is not managed through the Active Directory will be managed in the Local group.

Smart device information is also managed by the Local group.

When importing entire organization information
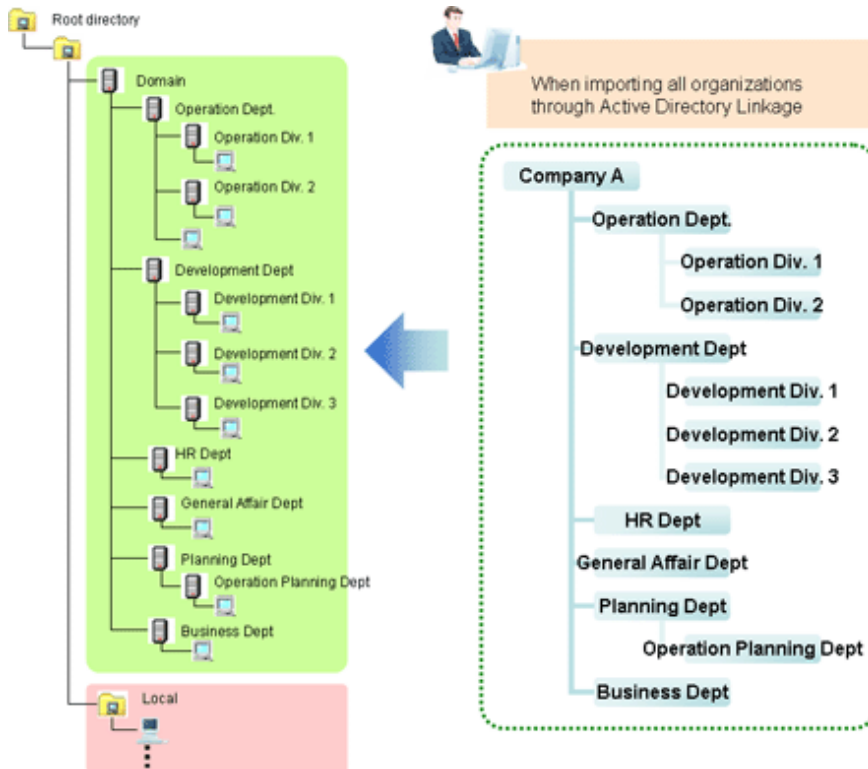
When importing part of organization information and operating the organization that is not imported with Local
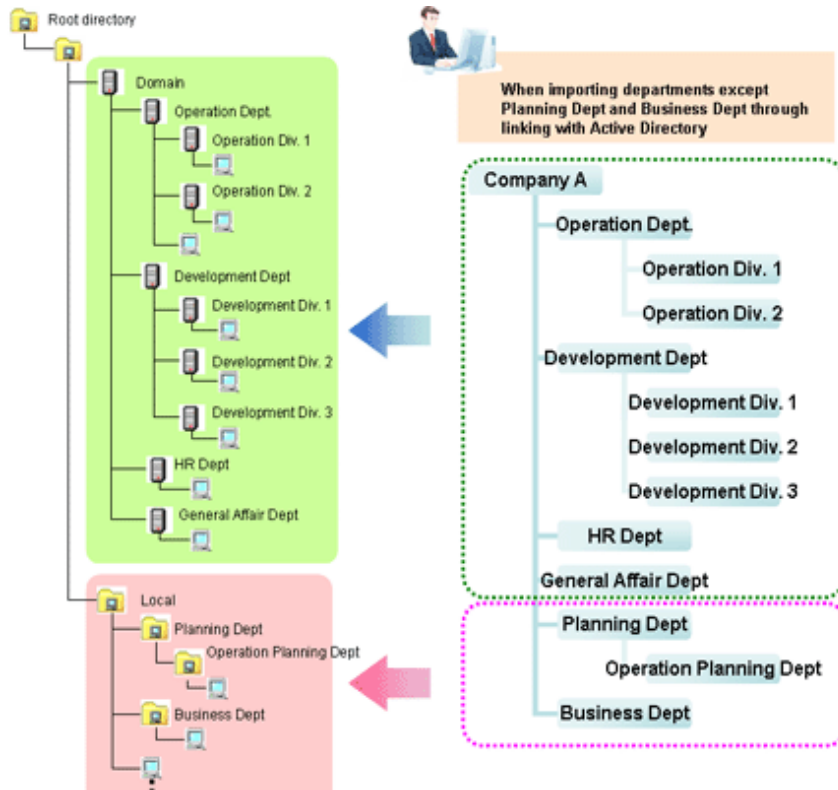
Domain: the group managed after linking with the Active Directory.

Local: the group managed when linking with the Active Directory is not performed.

When linking with Systemwalker Desktop Patrol and entering information to the a Management Console
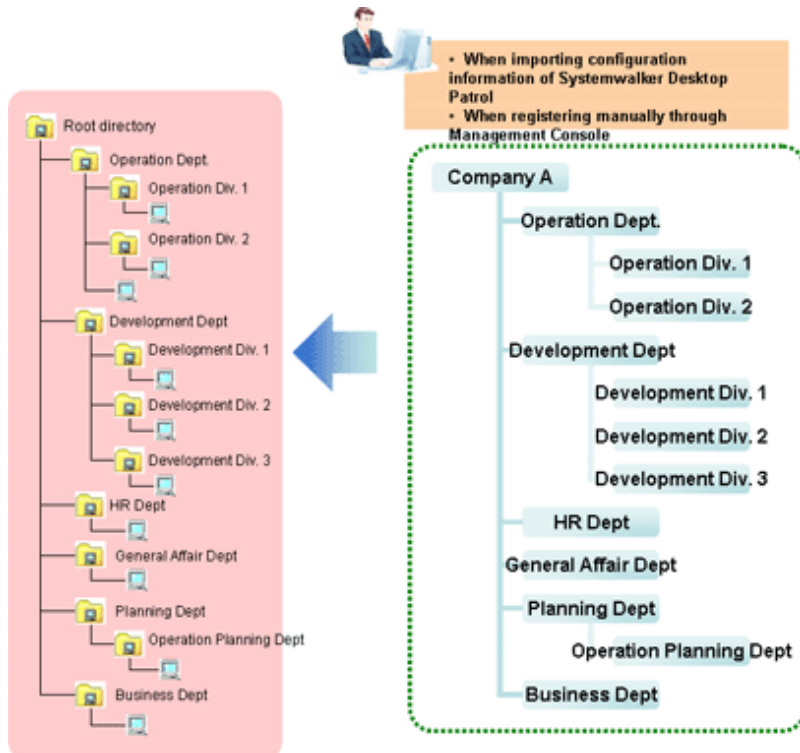
1.2.3.1 Active Directory Linkage

By linking with the Active Directory server that is used to manage organization structure, user information and computer information, each piece of information is imported into Systemwalker Desktop Keeper.

Because the client (CT) group tree, user ID and user group tree can be created automatically based on the organization structure, user information and computer information of the Active Directory, the workload from installing Systemwalker Desktop Keeper and changing the structure can be reduced.

In addition, because the organization structure, user information and computer information are collectively managed by the Active Directory, even though the change of structure or personnel takes place for the system administrator of Systemwalker Desktop Keeper, information can be imported from the Active Directory without needing to reconstruct the configuration information.
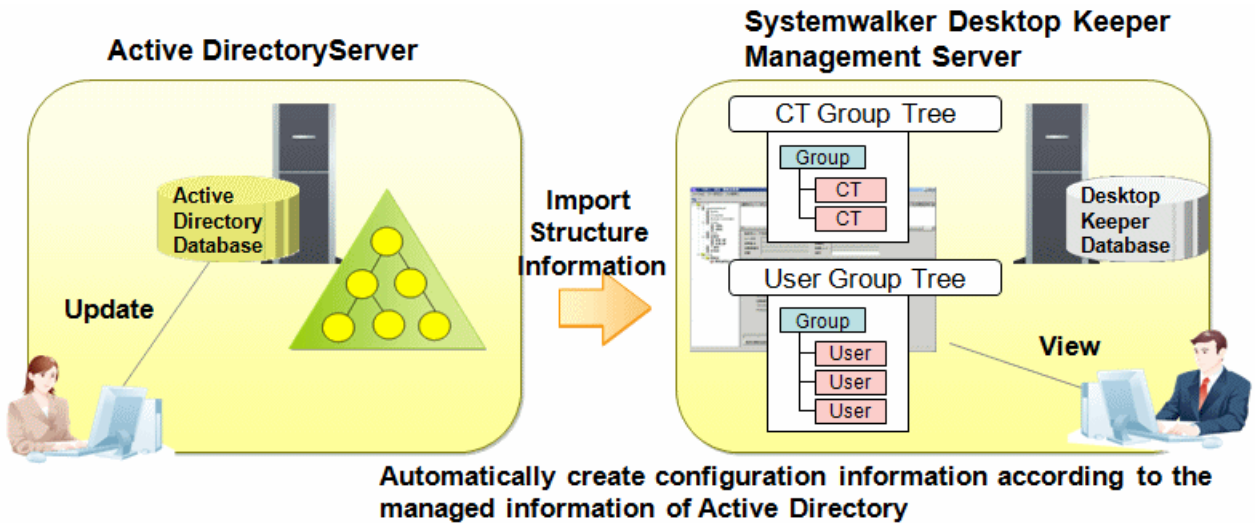
The following functions can be achieved by using the Active Directory Linkage function:

Function	Function Description
Automatically create CT group tree	According to the **Organization Unit (OU)** information of Active Directory, the CT group tree of Systemwalker Desktop Keeper can be created automatically.
Automatically register CT on the CT group to which the client (CT) belongs	According to **Computer** and the affiliated **Organization Unit (OU)** information of Active Directory, the client (CT) can be registered automatically on the CT group tree it belongs. The client (CT) that belongs to the **Computer** of the **Container** that is not linked with the Active Directory will be registered to Local.
Automatically create user information and user group tree	According to the **User** information and affiliated **Organization Unit (OU)** information of the Active Directory, the user ID and user group tree of Systemwalker Desktop Keeper can be created automatically. When the **Container** to which the user belongs is not linked with the Active Directory, the user ID of this **User** cannot be created.

Set whether to link with the Active Directory when installing Systemwalker Desktop Keeper. In addition, for information on linking with the Active Directory, refer to"DTKADCON.EXE (Active Directory Linkage" of *Systemwalker Desktop Keeper Reference Manual*.

After linkage with the Active Directory has been executed, the following configuration information will be imported.
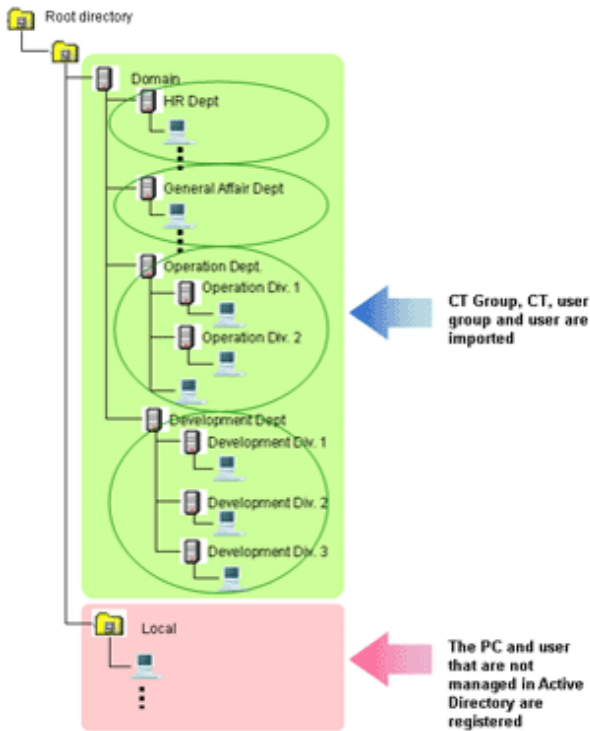
When the User IDs with the same name exist in Local, even if they are operated through the Active Directory, user policy of Local will be applied.

However, because the following OS does not have the function to join a domain, even if an Active Directory Linkage has been executed, it will be managed in Local.

- Windows Vista(R) Home Basic

- Windows Vista(R) Home Premium

- Windows(R) 7 Home Premium

- Windows(R) 8

- Windows(R) 10

P Point

. . . .

Organization that is not linked with the Active Directory can be managed in Local

Systemwalker Desktop Keeper cannot be used to modify the following information, which is created automatically through linkage with Active Directory: CT group tree, user group tree, group to which the client (CT) belongs, and group to which the user information belongs. However, CT groups, user groups, or user information can be created in Local on Systemwalker Desktop Keeper. The CT group, user group or user information that is not linked with the Active Directory will be applied during local authentication, instead of domain authentication. Even if linking with the Active Directory again, they will not be deleted or modified.

. . . .

How to Link

The methods of importing Active Directory information are as follows.

Import using "Server Settings Tool"

After starting to apply the Active Directory Linkage function, the modified new management information of Active Directory server can be imported through the Server Settings Tool window.

When personnel or PCs are changed, organizations are added or deleted because of changes in organization structure, perform the linkage and update the information if necessary.

Linkage can be performed by selecting "Execute Active Directory Linkage" from the "Settings" menu of the Server Settings Tool. For details, refer to "Import Information from Active Directory" of *Systemwalker Desktop Keeper User's Guide for Administrator*.

Import using "Active Directory Linkage command"

After starting to use the Active Directory Linkage function, the modified new management information of Active Directory server can be imported by executing the "Active Directory Linkage command".

Register the "Active Directory Linkage command" in the Task Scheduler, and update the configuration information of Active Directory Linkage on a regular interval. Thus, even when it is unknown whether the configuration information has been modified or not, this information can always remain up-to-date.

For details of the Active Directory Linkage command, refer to "DTKADCON.EXE (Active Directory Linkage)" of *Systemwalker Desktop Keeper Reference Manual*.

Only import CT information (computer information) from external data

Sometimes, only the user information is managed in the level composition of the Active Directory, and the computer information is not managed in the level composition.

In this case, by creating and importing the list (in CSV format) of user information and CT information (computer information) saved in the linked Active Directory, level composition of the CT information (computer information) can be constructed.

For details on how to import, refer to "2.3.6.2 Perform System Settings".

Linkage Structure

In a 3-level Management Server, user policies (user information) are collectively managed by the Master Management Server. Therefore, when performing Active Directory Linkage, the Management Console must be connected to the Master Management Server. (When connecting to the Management Server, it will be overwritten with the setting values of Master Management Server.)

The group structure and user information obtained after the Management Console is linked with Active Directory cannot be moved, registered, updated or deleted. But notes and part of the data items can be modified.

In a 3-level system structure, CT information is collectively imported by each Management Server, and the user information is collectively imported by the Master Management Server.

1.2.3.2 Link with Systemwalker Desktop Patrol

The CT group information and client (CT) configuration information that is saved in Systemwalker Desktop Patrol can be imported to Systemwalker Desktop Keeper in CSV format.

However, when linking with the Active Directory, linkage with configuration information of Systemwalker Desktop Patrol will not be performed.

For details on products that can be linked with Systemwalker Desktop Patrol, refer to "Related Software" of *Systemwalker Desktop Keeper User's Guide*.

Systemwalker Desktop Patrol CSServer — **Systemwalker Desktop Keeper Management Server**

Automatically create configuration information according to the configuration information extracted in Desktop Patrol
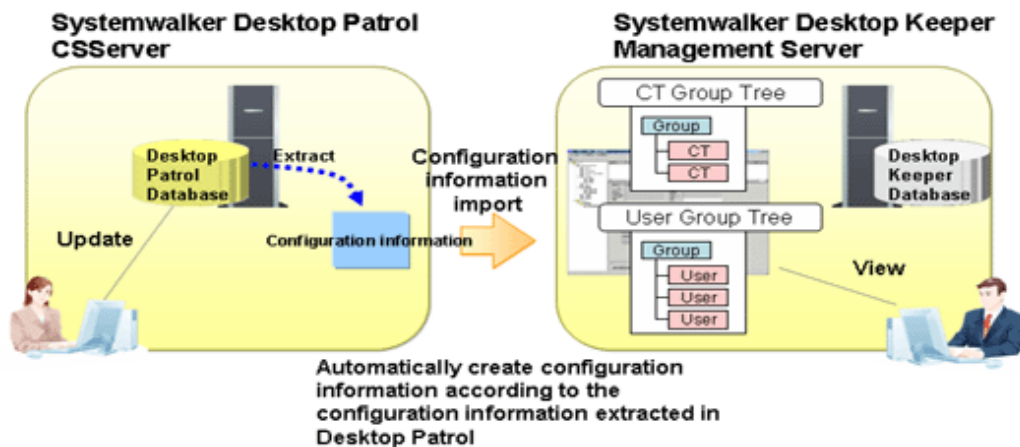
How to Link

Automatically import configuration information of Systemwalker Desktop Patrol

By setting automatic import of Systemwalker Desktop Patrol configuration information, the configuration information of Systemwalker Desktop Patrol will be imported once per day. Even when it is unknown whether the configuration information has been modified or not, this information can always remain up-to-date. For details of the setting method, refer to "2.3.6.5 Set the Link with Other Systems".

Import through "Systemwalker Desktop Patrol configuration information import command"

By executing "Systemwalker Desktop Patrol configuration information import command", the configuration information output from Systemwalker Desktop Patrol can be imported.

Register the "Systemwalker Desktop Patrol configuration information import command" to the Task Scheduler, and update the configuration information of Systemwalker Desktop Patrol on a regular interval. Thus, even when it is unknown whether the configuration information has been modified or not, this information can always remain up-to-date.

For details of Systemwalker Desktop Patrol configuration information import command, refer to "DTKIMPDP.EXE (Import Systemwalker Desktop Patrol Configuration Information)" of *Systemwalker Desktop Keeper Reference Manual*.

1.2.3.3 Input in Management Console Window

The configuration information can be constructed from the Management Console window. Create the organization information and user information respectively in each window.

Since the client (CT) information and smart device (agent) information will be automatically registered to the Root directory, it can be created by moving to the affiliated organization. However, when linking with the Active Directory, it will be registered to the Local group instead of Root directory.

1.2.4 Determine How to Manage User Policy

Even if the Active Directory Linkage cannot be performed, user policies (user information) can be collectively managed by the Master Management Server. When user policies (user information) are managed collectively, make sure that the Management Console is connected with the Master Management Server.

Collective management of user information can be achieved in a 3-level system structure.

In a 3-level system structure, it is necessary to determine whether user policies and user information are managed by the Master Management Server or Management Servers. (When linking with the Active Directory, it will automatically set to be collectively managed by Master Management Server.)

The features of each management method are as follows.

Setting	Features
Collectively managed by Master Management Server	- Because it is unnecessary to register new user information and set user policies in each Management Server, the application will become easier. - Because the user policy settings in all Management Servers are same, the settings cannot be modified in each Management Server. - When unable to communicate with the Master Management Server, the Management Server will not be able to use the latest user policy and user information of the Master Management Server. Therefore, the policies saved in Management Server will be applied. In addition, in the Management Server, the information set under the situation that communication with the Master Management Server cannot be performed will return to the values set in the Master Management Server when the communication with the Master Management Server is started again. - When you use the user operation log search feature of the Log Viewing Database, centrally managing user information facilitates selection of the user to search for.
Managed by each Management Server	- Settings can be modified in the Management Servers. - Because it is necessary to register new user information and set user policies in each Management Server, the application will become more complicated.

Set the methods of managing user policies while installing Systemwalker Desktop Keeper.

Collective management by the Master Management Server
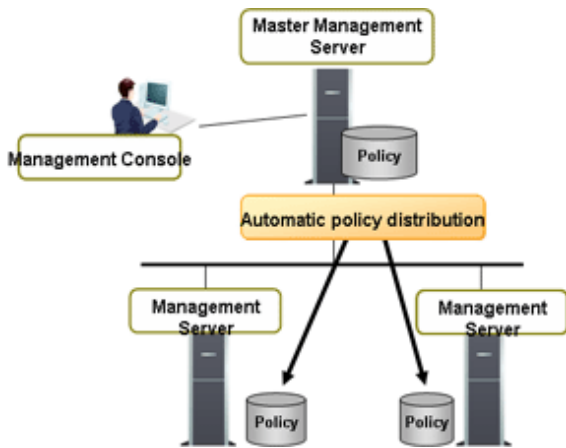
Management by Management Servers
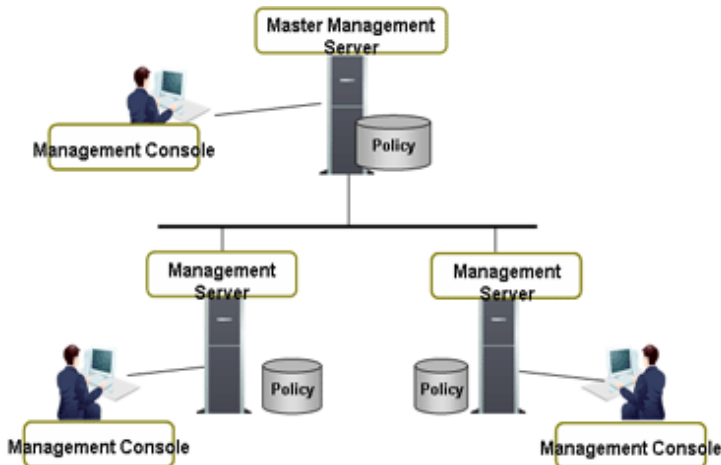
Note

. . . .

Notes when changing to collectively manage user policies after application has started

After the application of Systemwalker Desktop Keeper has been started, changing to collective management by the Master Management Server is allowed.

Although the function of transferring the information set by Management Servers to the Master Management Server is provided (user definition transfer command), if a user group with the same name exists on the same container of each Management Server, a group with the same name will be created in the user group tree after the collective management. Therefore, it is necessary to perform operations such as moving users and deleting user groups after the transfer.

. . . .

1.2.5 Determine How to Install Client (CT)

There are four types of approaches to install the client (CT) of Systemwalker Desktop Keeper:

- Install by single installation.

- Install using master PC/master virtual PC

- Install using software distribution function of Systemwalker Desktop Patrol

- Install using Active Directory Group Policy

Determine the installation approach by considering factors such as the number of extracted clients and whether Systemwalker Desktop Patrol has been installed.

Install by Single Installation

Use the setup disk of Systemwalker Desktop Keeper and install the client (CT) in each PC through the following two approaches:

- Installation in Wizard style

- Silent installation

Note

. . . .

Verification when registering client (CT) devices

In the **Terminal Operation Settings** window of Management Console, set a client management password. Refer to "Perform Terminal Operation Settings" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

It is recommended that you change the client management password after installation is completed.

. . . .

Install using Master PC/Master Virtual PC

Install the client (CT) in the master PC/master virtual PC, create a master image and extract the master image to all PCs/virtual PCs for installation.
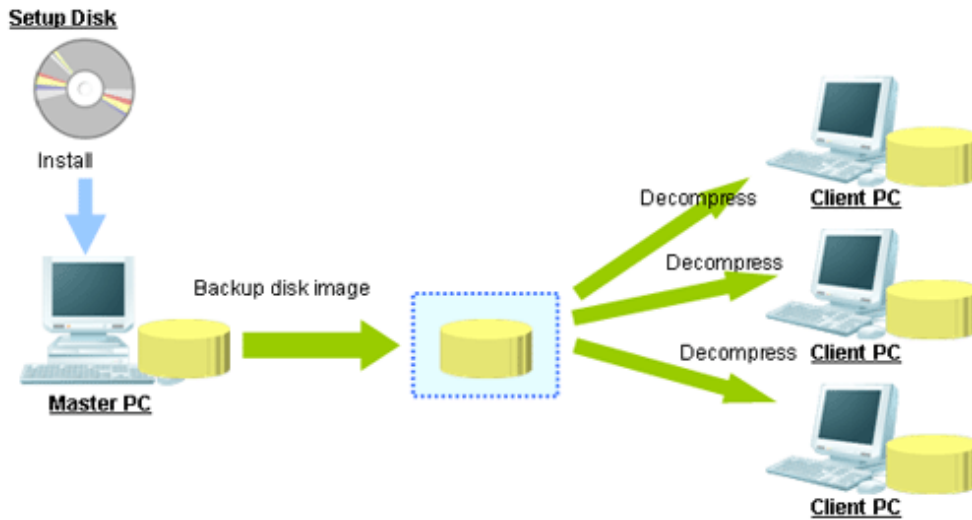
Install using Software Distribution Function of Systemwalker Desktop Patrol

By using the software distribution function of Systemwalker Desktop Patrol, the client (CT) of Systemwalker Desktop Keeper can be distributed to the computer of the managed target to perform installation.
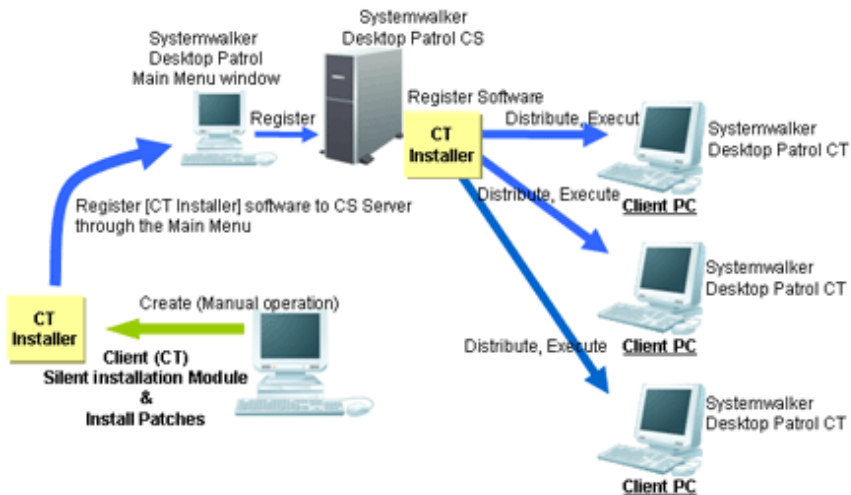
Install Using Active Directory Group Policy

The Active Directory Group Policy enables the user to install a Systemwalker Desktop Keeper client (CT) to the machine to be managed.
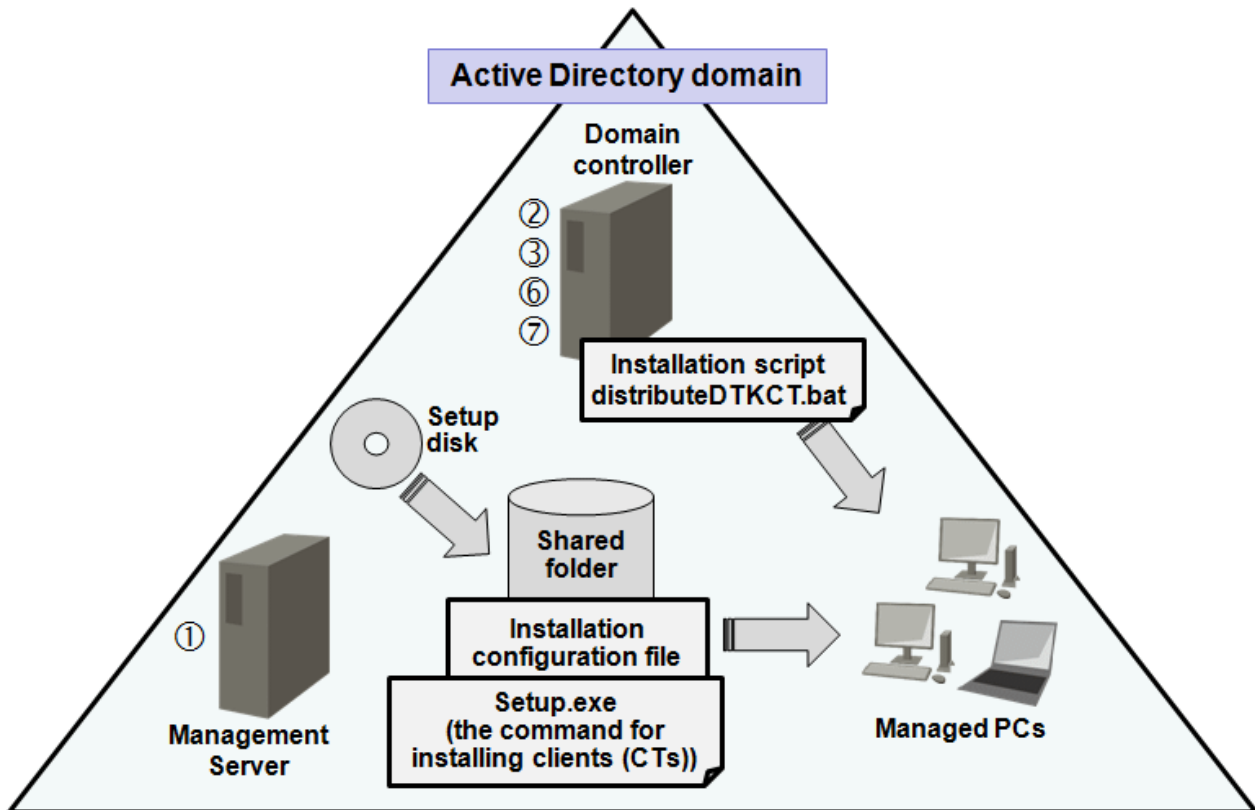
Procedure

1. Create an installation configuration file.

2. Edit the installation script "distributeDTKCT.bat".

3. Edit the Group Policy.

4. Store the file created in step 1 and Setup.exe (the command for installing clients (CTs)) in the shared folder.

5. The client (CT) is automatically installed to the PC to which the Group Policy was applied.

6. Confirm that installation to the client (CT) was completed successfully.

7. Cancel the Group Policy.

1.2.6 Determine How to Install to Smart Devices (Agents)

There are four ways of installing Systemwalker Desktop Keeper to a smart device (agent):

- Having the smart device user download (install) Desktop Keeper Client from Google play.

- Copying Systemwalker Desktop Keeper to an SD card and distributing it to smart devices (*1).

- Distributing Systemwalker Desktop Keeper to smart device users by email (*1).

- Publishing Systemwalker Desktop Keeper on a corporate web server, and having each smart device user download it.

    *1: Supported only if the smart device to be managed runs Android.
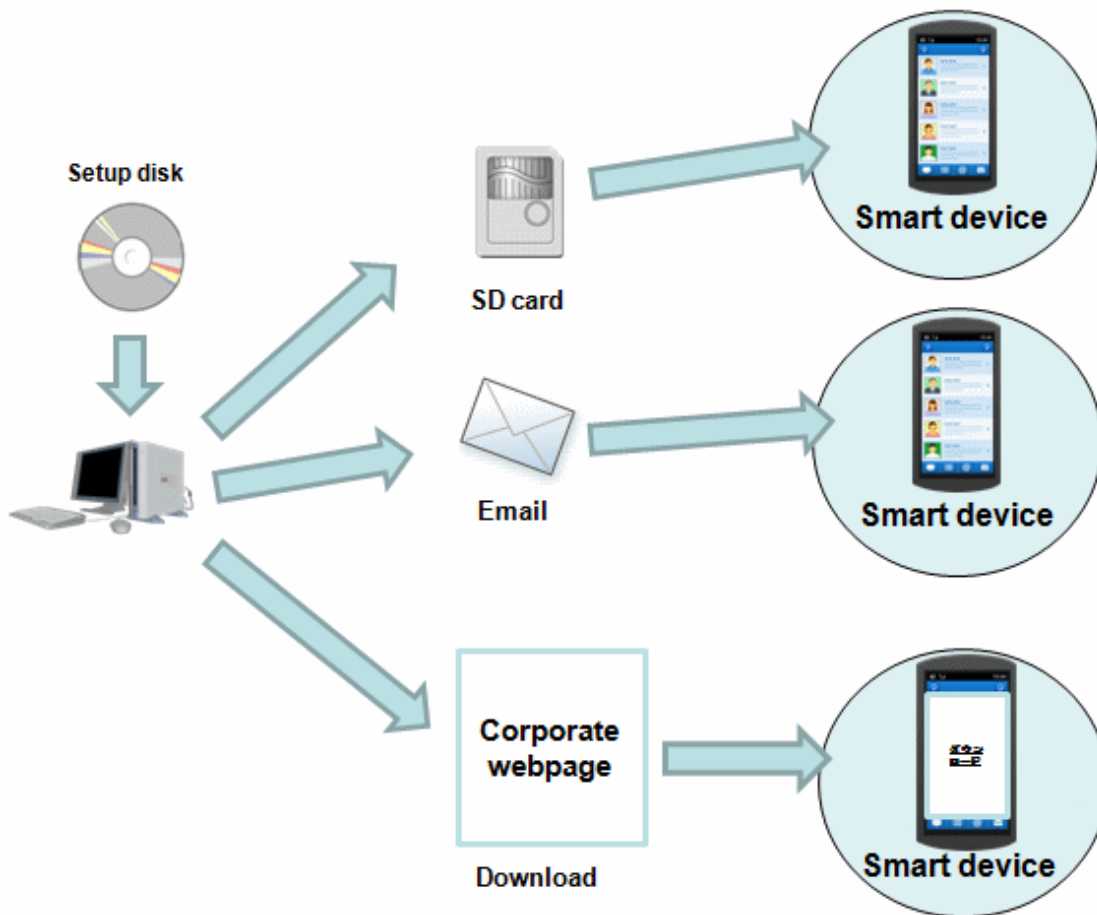
1.2.7 Determine How to Operate Logs

The following describes the items that should be examined during the design process regarding the operation method of logs.

Items to be examined in Management Server/Master Management Server

When Systemwalker Desktop Keeper is used to collect logs continuously, the storage space will be insufficient. Therefore, through regularly backing up logs on the Management Server/Master Management Server and deleting database space, stable operation can be achieved without insufficient database space.

The following three items in Management Server/Master Management Server should be determined in advance:

- Database capacity (operation database, log viewing database)

- Log backup and deletion method

- Backup method of attached data

Determine database capacity

- Determine the capacity of the operation database

  The operation database is the database that manages daily operation information (management information, operation log information).

  Examine the following information during the design process to determine the factors of capacity estimation during the construction of the operation database.

  - Number of clients (CTs) managed

- Number of file operation logs

- Number of non-file operation logs

- Number of months to save

For the number of months to save, since it will become linked with log backup and deletion period, it is necessary to determine which period the logs are always viewed.

- Determine the capacity of the log viewing database

The log viewing database is the database for moving the previous operation logs for viewing.

Examine the following information during design process and determine the factors of estimating the capacity during the construction of log viewing database:

- Number of clients (CTs) managed

- Number of months to save

For the number of file operation logs and non-file operation logs, estimate the capacity according to the value of the operation database.

To search the Log Viewing Database including downstream Management Servers once in a 3-level system structure, include the number of clients (CTs) of downstream Management Servers when specifying the number of clients (CTs) to be managed.

Determine how to backup and delete logs

Log backup/deletion can be performed by executing tasks with the GUI and command. When performing fixed operations, create the batch file for executing the backup command and execute regularly. For the example of creating a GUI, command and batch file, refer to "3.1.2 Back Up User Assets". You must also back up and delete the setting change logs. One way of doing this is to use a command to execute a task. Refer to "3.1.2 Back Up User Assets" for details on commands and how to use them.

Viewpoint of Log Backup

The following are points about the timing for backing up logs:

- Backup the logs that exceed the saving period and delete the logs that have been backed up

- Backup recent logs and delete the logs that exceed the saving period

It is necessary to note the situation when the log amount increases temporarily and construct a sufficient number of months to save.

Determine how to backup attached data

Attached data cannot be saved to the database. In addition, since it is not the backup target of the backup tool, it is likely that a large amount of screen capture data and original file backup data will be accumulated on the server by settings, which will lead to an exhaustion of disk capacity. Therefore, different from the log operation mentioned above, perform capacity confirmation, as well as backup and deletion regularly.

The structure of folder for saving the screen capture data with attached data and original file backup data is as follows. For the destination to save attached data, refer to "2.3.6.9 Set Saving Target Folder".

Structure:

Target folder for saving attached data
+-Folder of day unit

+-Folder of CT unit

Example:

Determine how to backup E-mail data

E-mail data cannot be saved to database. In addition, since it is not the backup target of the backup tool, it is likely that large amount of E-mail text and attachments will be accumulated on the server through settings, which will lead to an exhaustion of disk capacity. Therefore, different from the log operation mentioned above, perform capacity confirmation, as well as backup and deletion regularly.

To delete, use DTKMLDL.BAT (Delete E-mail Content) command. For details of how to use the command, refer to "DTKMLDL.BAT (Delete E-mail Content)" of *Systemwalker Desktop Keeper Reference Manual*.

The structure of folder for saving E-mail text and attachments is as follows. For the destination to save E-mail data, refer to "2.3.6.9 Set Saving Target Folder".

Structure:

Target folder for saving E-mail content

+- Folder of day unit
+- Folder of CT unit

Example:
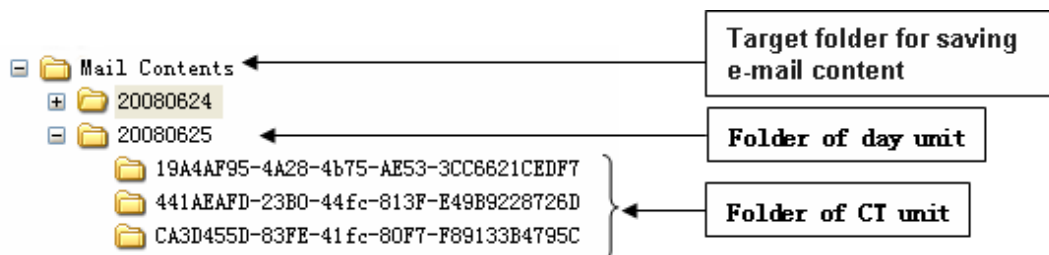
Items to be examined in the Log Analyzer Server

When building the Log Analyzer Server and using the log analysis function and report output function, logs collected by the Management Server/Master Management Server will be transferred to the shared folder of the Log Analyzer Server.

Logs saved in the shared folder will be analyzed, aggregated and saved to the database of the Log Analyzer Server, but the logs on the shared folder will be kept all the time.

Therefore, by regularly backing up logs saved in the shared folder on the Log Analyzer server and deleting the logs that have been backed up, stable operation without running out of shared folder space can be achieved.

In addition, since transmission to the shared folder (data transfer) and saving to the database of the Log Analyzer Server (data move-in) are required to be performed once a day, operate after registering commands to Task. During this Task registration, the time of executing task also needs to be examined (leave sufficient time required for transmission after the transmission has completed; since the transmission/ moving process will increase workload, it will be performed during night-time, etc.).

Determine how to backup shared folder 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 shared folder regularly and delete the logs that have been analyzed and aggregated after they have been backed up.

The structure of the shared folder of the Log Analyzer Server is as follows:
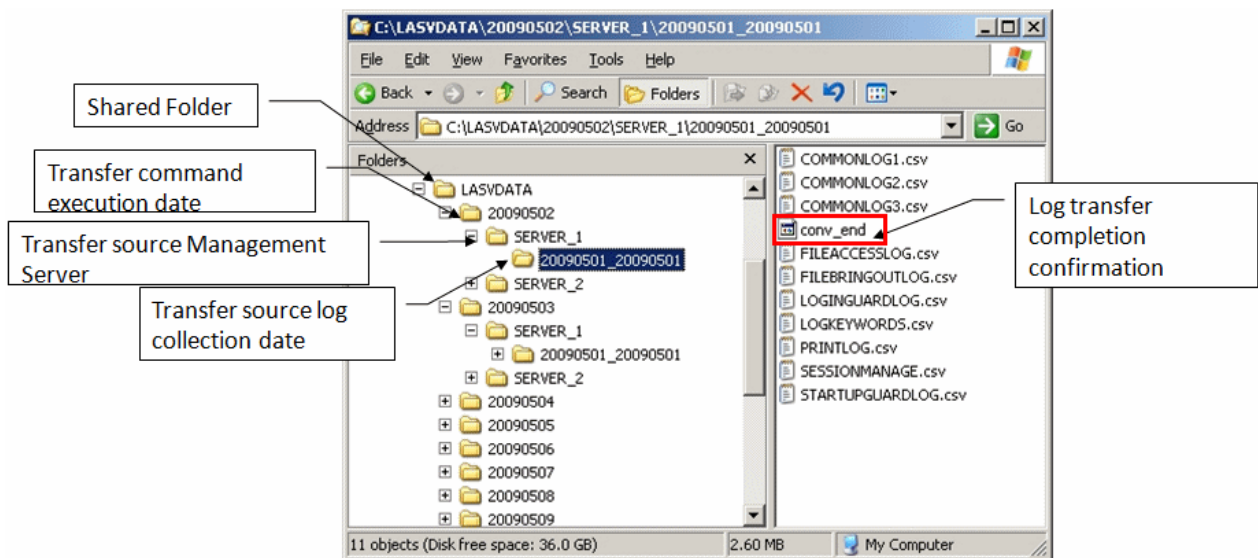
Do not backup or delete the logs for which analysis and aggregation has not been completed in the Log Analyzer Server.

The "File for conforming completion of log transmission (conv_end)" folder created under the folder of transmission source log collection day indicates that the log analysis and aggregation has been completed and logs have been saved to the database on Log Analyzer Server.

When "File for conforming completion of log transmission (conv_end)" has been created in all "Folder of transmission source log collection day" exist 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 in the unit of "Transmission Command Execution Day" folder.

1.2.8 Determine Analysis Condition of the Log Analyzer

When analyzing and aggregating the collected logs in the Log Analyzer Server, set the screening condition and exclusion condition that have been set in advance.

If the setting of this condition is inappropriate, the accuracy of analysis and aggregation results will be reduced. Therefore, determine what kind of condition should be set during the design stage.

The settings are as follows:

Screening Condition

Specify the following items and determine the analysis condition.

- Keyword: string contained in a file or file path (partially match)

- Domain: string contained in E-mail address (partial match)

- URL: string contained in URL (partially match)

- Application: executable file name apart from extensions (complete match)

Exclusion Condition

In order to exclude PC from the aggregation target, determine the exclusion conditions as follows.

- PC required to access to important files on business

- PC that performs large amount of daily file access

In order to perform analysis with higher accuracy, it is necessary to consider the following:

- Set screening conditions on every Log Analyzer Server. Therefore, when multiple organizations are targeted, after the keyword limited to particular organizations has been set, analysis that is not for this organization may become inappropriate.

Try to extract common keywords and do not refine the setting of keywords limited to the department.
In addition, configure the organization that processes same confidential information to the same Log Analyzer Server for management.
For viewpoints of configuration, refer to "1.2.1.3 Determine the Installation Standard for Log Analyzer Server" of "1.2.1 Determine System Structure

- Distinguishing the exception PC mentioned above is important for exclusion conditions. Do not set a PC with lower accuracy in aggregate results as the aggregation target.

1.2.9 Determine the Aggregation Condition of Status Window

In order to aggregate logs collected by the Management Server/Master Management Server and confirm the number of malfunctioning PCs and smart devices, aggregation conditions should be set in environment setup in advance. When the setting of this condition is inappropriate, the accuracy of the aggregation result will be reduced. Therefore, examine and determine what kind of condition should be set in design stage.

The settings are as follows:

- Overall settings
  Set the following items and determine the aggregation and display condition:

  - Aggregation schedule

  - Graph color

  - URL of Systemwalker Desktop Patrol

  - Notify/Do not notify department administrator by E-mail

- Setting of each aggregation item
  Set the following items and determine the aggregation condition:

  - Aggregate/Do not aggregate

  - Auditing period

  - Setting items of each item (Time frame, day of a week, type of target drive, etc.)

1.2.10 Confirm Port Number

Confirm whether any problem exists in the port number used in Systemwalker Desktop Keeper and whether it is available for use in the design stage.

For the port number used in Systemwalker Desktop Keeper, refer to "Port Numbers and Services" of *Systemwalker Desktop Keeper Reference Manual*.

When the port number to be used in Systemwalker Desktop Keeper is already used in the system, modify the port number.

In addition, management is performed by using a Web browser in Systemwalker Desktop Keeper. In order to use and manage IIS, set the port number of IIS to "80".
If the port number "80" is already used in the system, modify the port number.

For how to modify the port number, refer to "Port Numbers and Services" of *Systemwalker Desktop Keeper Reference Manual*.

Chapter 2 Installation

This chapter explains how to install Systemwalker Desktop Keeper.

2.1 Installation Steps

This section describes the installation steps of Systemwalker Desktop Keeper.

When log analysis function and report output function are not used

The installation steps for the fundamental structure (without the Log Analyzer Server) of Systemwalker Desktop Keeper are as follows:
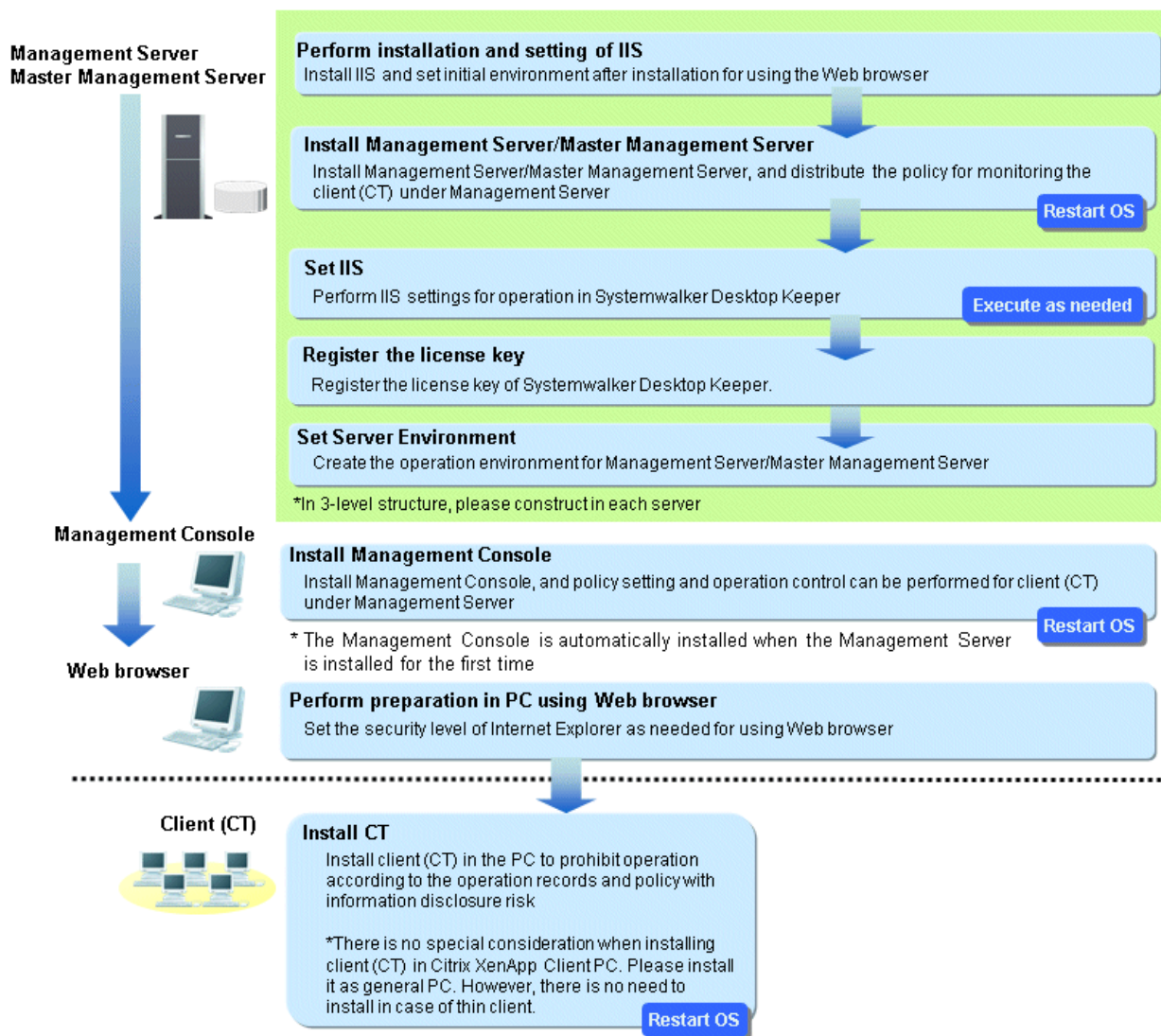
When the smart device management feature is used

When managing smart devices, you will need to build the Smart Device Relay Server in addition to the above procedure. Note that you should perform the procedure below before extracting the smart device (agent).

Build the Smart Device Relay Server after completing the build of the Management Server or Master Management Server.

Management Server
Master Management Server

Configure the publishing setting for the database

Smart Device Relay Server

Install the Smart Device Relay Server

When log analysis function and report output function are used

When the Log Analyzer Server is built and the functions of log analysis and report output are used, the following steps are required apart from the above steps.

In addition, the following steps can also be performed before extracting the client (CT) and the smart device (agent).

[Log Analyzer Server]

Install Log Analyzer Server
Install Log Analyzer Server analyzes logs and executes information disclosure prevention diagnosis and aggregation by objectives.
OS Restart

Construct Database
Construct database environment for recording log analysis result .etc.

[Management Server]
[Master Management Server]

Set Connection Environment of Log Analyzer Server
Set Log Analyzer environment on Management Server/Master Management Server.

Transfer administrator information to Log Analyzer Server
Transfer the administrator information set in Management Server/Master Management Server to Log Analyzer Server.

Register Log Analyzer Server information
Register Log Analyzer Server information to Management Server/Master Management Server

[Log Analyzer Server]

Register Administrator Information
Register the transferred administrator information to Log Analyzer Server.

[Report Output Tool]

Install Report Output Tool
Install the report output tool that performs information disclosure prevention diagnosis result and print volume reduction result.
OS Restart

Set Environment of Report Output
Set the operation environment required for report output.

When a client (CT) is installed on Management Server/Master Management Server

The steps to install a client (CT) on a Management Server/Master Management Server are as follows:

1. Install Management Server/Master Management Server;

2. Install a client (CT).

Install the Management Server/Master Management Server first. Otherwise, it will be unable to install the Management Server/Master Management Server.

About server to be connected

When installing a client (CT) on a Management Server/Master Management Server, the client (CT) can only be registered on the Management Server/Master Management Server of this server (refer to the following diagram).
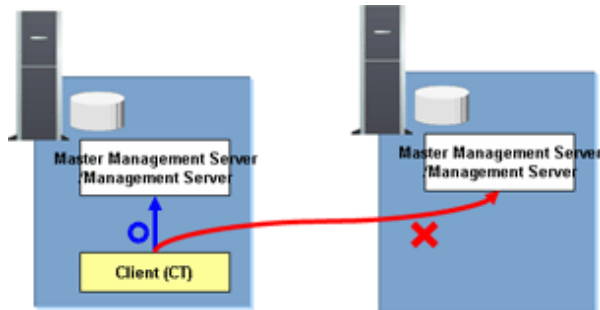
2.2 Advance Preparation

Advance preparation for managing iOS devices

To manage iOS devices, Systemwalker Desktop Keeper uses the Apple Push Notification Service provided by Apple.

For this reason, the MDM certificate issued by Apple must be obtained by following the steps shown below. The MDM certificate must be set to "Smart Delay Server" during its installation.

🛑 Note

....

Execute the following steps on a Mac OS.

....

1. Register in the iOS Developer Enterprise Program
    Access the following URL (as of February 2015), and register in the "iOS Developer Enterprise Program".

    https://developer.apple.com/jp/programs/ios/enterprise/

2. Obtain the signing certificate (MDM Signing Certificate)
    Contact Apple via phone or email, and request an MDM vendor registration. Once Apple is informed that you want to be registered as an MDM vendor, they will start the registration process.
    Follow Apple's instructions to create a signing certificate. The private key created in this step will later be required in step 3.

3. Export the private key
    Export the private key used to create the signing certificate in PKCS#12 format. It can be exported using Keychain Access. The passphrase specified in this step will also be required in step 6.

4. Obtain the Apple Inc. intermediate certificate
    Obtain the intermediate certificate (Worldwide Developer Relations) from the following URL (as of February 2014):

    http://www.apple.com/certificateauthority/

5. Obtain the Apple Inc. Root Certificate
    Obtain the root certificate (Apple Inc. Root Certificate) from the following URL (as of February 2014):

    http://www.apple.com/certificateauthority/

    Create the MDM certificate request file
    Using the certificate and private key obtained in steps 2 to 5, create the MDM certificate private key and MDM certificate request file. These can be created by executing the sign_csr.sh (create MDM certificate application file) script. Refer to the *Systemwalker Desktop Keeper Reference Manual* for details on how to use this script.
    This script is stored in:

    ```
    dtkDvdRom:\win32\SmartDevice\x86\Server\unified\Tool\sign_csr.sh
    ```

6. Obtain the MDM certificate

By uploading the request file created in step 6 to the Apple Inc. website, the MDM certificate will become available for download (as of February 2014).

https://identity.apple.com/pushcert/

7. Convert the MDM certificate format

Convert the format of the downloaded MDM certificate.

Open **Terminal**, and execute the command shown below. The MDM certificate will be converted into PKCS#12 format. The converted file must be registered to the Smart Device Relay Server.

```
openssl pkcs12 -export -in mdmCertificate -inkey mdmCertificatePrivateKey -out outFile
```

For *mdmCertificate*, specify the downloaded MDM certificate (required).

For *mdmCertificatePrivateKey*, specify the private key created in step 6 (required).

For *outFile*, specify the file name of the converted certificate with the p12 extension (required).

2.3 Construct Management Server/Master Management Server

This section describes the installation and environment construction of a Management Server/Master Management Server of Systemwalker Desktop Keeper.

2.3.1 Installation and Settings of IIS

![Note icon] **Note**
. . . .
HTTPS is recommended for communication.
. . . .

In Systemwalker Desktop Keeper, use Web viewer to perform log viewing and analysis. In order to perform management with IIS, it is necessary to install and set IIS before installing a Management Server/Master Management Server.

Under Windows Server(R) 2008 (IIS 7.0/IIS 7.5) environment

Under Windows Server(R) 2008, ISAPI extensions should be installed in advance.

Installation steps of ISAPI extensions are as follows:

Installation steps of ISAPI extensions when newly installing IIS

1. Select **Administrative Tools** > **Server Manager** from **Control Panel**.

2. The **Server Manager** window is displayed. Click **Add Roles**.
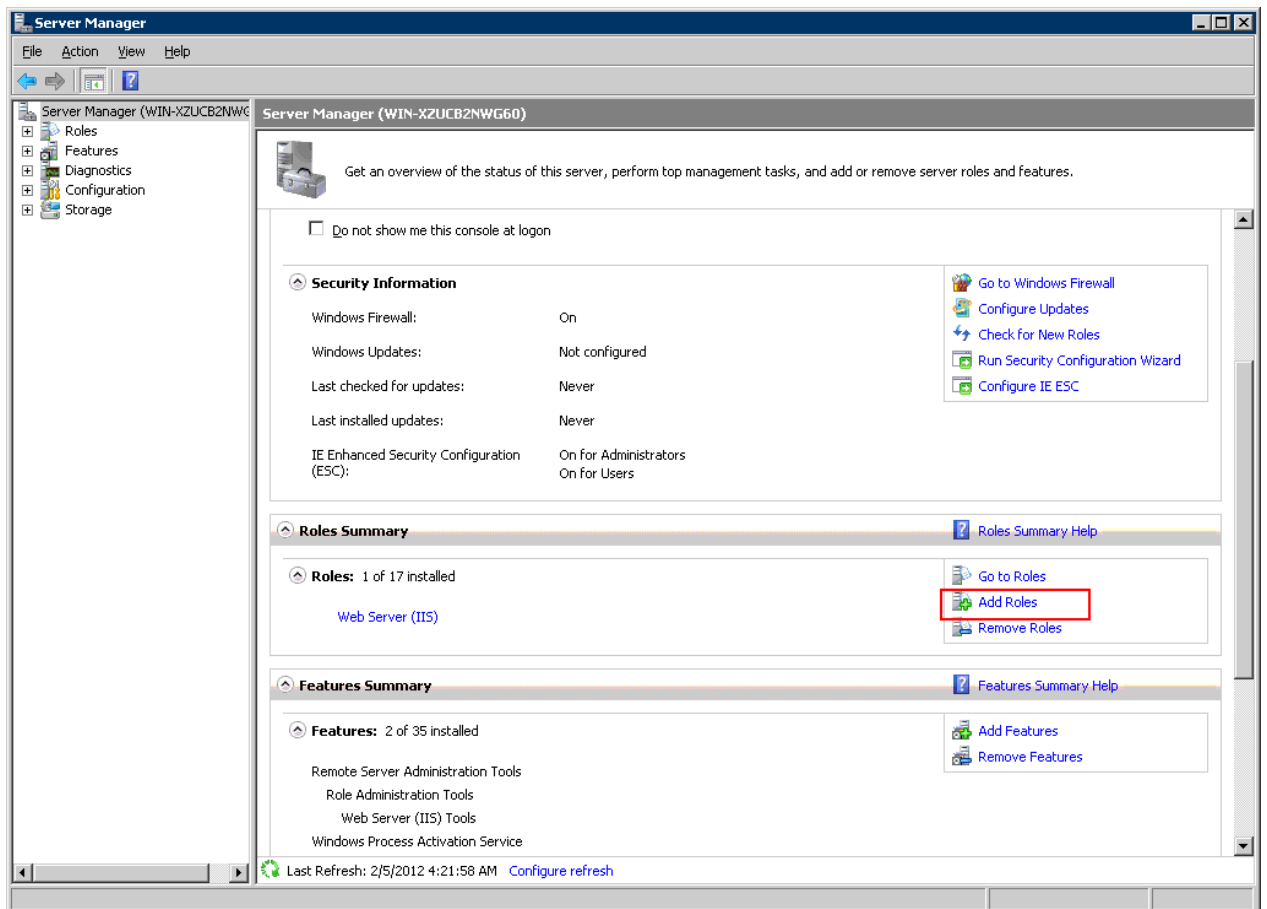
3. After the window **Before You Begin** of **Add Roles Wizard** is displayed, click **Next**.

4. The **Select Server Roles** of **Add Roles Wizard** window is displayed. Select **Web Server (IIS)** and click **Next**.

5. The **Web Server (IIS)** of **Add Roles Wizard** window is displayed. Click **Next**.

6. The **Select Role Services** of **Add Roles Wizard** window is displayed. Select the following items and click **Next**:

   - **Application Development** > **ISAPI Extensions**

   - **Management Tools** > **IIS 6 Management Compatibility**

   In addition, select the following items if they are not selected:

   - **Common HTTP Features** > **Static Content**

   - **Common HTTP Features** > **Default Document**

   - **Common HTTP Features** > **Directory Browsing**

   - **Common HTTP Features** > **HTTP Errors**

7. **Add Roles Wizard** of the **Confirm Installation Selections** window is displayed. Click **Install**.

8. After the installation has completed, Click **Close**.

ISAPI extensions installation steps when IIS has been already installed

1. Select **Administrative Tools** > **Server Manager** from **Control Panel**.

2. The **Server Manager** window is displayed. Select **Roles** > **Web Server (IIS)** in the tree view.
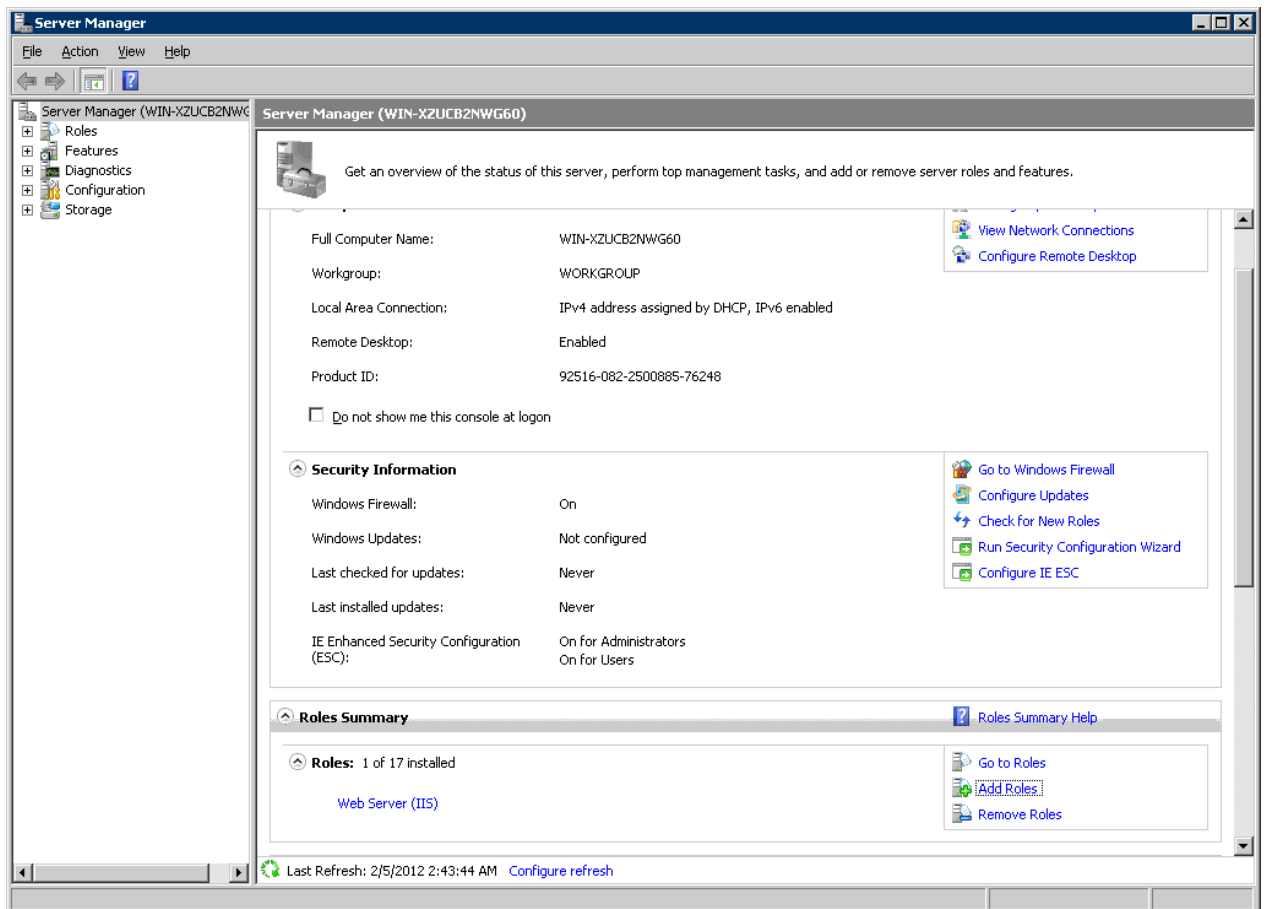
3. After the **Web server (IIS)** window is displayed, click **Add Role Services**.

4. The **Select Role Services** of **Add Role Services** window is displayed. Select the following items when they are not selected and click **Next**:

   - **Application Development** > **ISAPI Extensions**

   - **Administrative Tools** > **IIS6 Management Compatibility**

   In addition, select the following items if they are not selected:

   - **Common HTTP Features** > **Static Content**

   - **Common HTTP Features** > **Default Document**

   - **Common HTTP Features** > **Directory Browsing**

   - **Common HTTP Features** > **HTTP Errors**

5. After **Confirm Installation Selections** window is displayed, click **Install**.

6. After the installation has completed, click **Close**.

Under Windows Server(R) 2012 (IIS 8.0/IIS 8.5) environment

Under Windows Server(R) 2012, ISAPI extensions should be installed in advance.

Installation steps of ISAPI extensions are as follows:

Installation procedure for the ISAPI extensions when IIS is installed for the first time

1. In the **Start** window, click **Server Manager**.

2. In the **Server Manager** window, click **Add Roles and Features**.

3. The **Add Roles and Features Wizard** will be opened. In the **Before You Begin** window, click **Next**.

4. In the **Installation Type** window, select **Role-based or feature-based installation**, and click **Next**.

5. In the **Server Selection** window, select **Select a server from the server pool**, and click **Next**.

6. In **Server Roles** > **Roles**, ensure that **Web Server (IIS)** is selected, and click **Next**.
   The **Add features that are required for Web Server (IIS)?** confirmation window will be displayed. Click **Add Features**.
   Again, in **Server Roles** > **Roles**, ensure that **Web Server (IIS)** is selected, and click **Next**.

7. In the **Features** window, click **Next**.

8. In the **Web Server Role (IIS)** window, click **Next**.

9. In **Role services**, ensure that the following items are selected, and click **Next**.

   - **Application Development** > **ISAPI Extensions**

   - **Management Tools** > **IIS6 Management Compatibility**

   - **Management Tools** > **IIS6 Management Compatibility** > **IIS 6 Metabase Compatibility**

   - **Management Tools** > **IIS6 Management Compatibility** > **IIS6 WMI Compatibility**

   - **Management Tools** > **IIS6 Management Compatibility** > **IIS6 Scripting Tools**

   - **Management Tools** > **IIS6 Management Compatibility** > **IIS6 Management Console**

   Also, if the following items have not been selected, ensure that they are selected.

   - **Common HTTP Features** > **Static Content**

   - **Common HTTP Features** > **Default Document**

   - **Common HTTP Features** > **Directory Browsing**

   - **Common HTTP Features** > **HTTP Errors**

   The **Add features that are required for Web Server (IIS)?** or **Add features required for IIS6 WMI?** confirmation window will be displayed. Click **Add Features**.

10. In **Confirmation**, click **Install**.

11. Upon completion, click **Close**.

Installation procedure for the ISAPI extensions when IIS is already installed

1. Perform step 1 to 5 of **Installation procedure for the ISAPI extensions when IIS is installed for the first time** above.

2. In **Server Roles** > **Roles**, ensure that **Web Server (IIS) (Installed)** is selected.

   In the tree view, ensure that the following items are selected, and click **Next**.

   - **Web Server (Installed)** > **Application Development** > **ISAPI Extensions**

   - **Management Tools (Installed)** > **IIS6 Management Compatibility**

   - **Management Tools (Installed)** > **IIS6 Management Compatibility** > **IIS 6 Metabase Compatibility**

   - **Management Tools (Installed)** > **IIS6 Management Compatibility** > **IIS6 WMI Compatibility**

   - **Management Tools (Installed)** > **IIS6 Management Compatibility** > **IIS6 Scripting Tools**

   - **Management Tools (Installed)** > **IIS6 Management Compatibility** > **IIS6 Management Console**

   The **Add features that are required for Web Server (IIS)?** or **Add features required for IIS6 WMI?** confirmation window will be displayed. Click **Add Features**.

3. In **Confirmation**. click **Install**.

4. Upon completion, click **Close**.

2.3.2 Install Management Server/Master Management Server

This section describes how to install a new Management Server and Master Management Server of Systemwalker Desktop Keeper.

When installing for the first time, the Management Console will also be installed.

There are two ways to install the Management Server or Master Management Server:

- Installation using the wizard

- Silent installation

If the old version of the Management Server/Master Management Server has been installed, when installing Management Server/Master Management Server of V15.1.0, refer to "Chapter 4 Upgrading".

📝 Note

∙∙

Upon completion, the primary administrator (secureadmin) password will be set as follows in the Server Settings Tool, Backup Tool, and Restoration Tool.

secureadmin initial password: secureadmin

Also, if a database is constructed during installation, the user ID and password will be set for the Management Console and Log Viewer.

Management Console/Log Viewer user ID: systemadmin
Management Console/Log Viewer password: systemadmin

When logging after installation using the initial password, the user will be prompted to change the password. Follow the prompt to change it.

The password is recommended to be at least eight characters long and contain a combination of alphanumeric characters and symbols. It is recommended to change the password periodically.

∙∙

2.3.2.1 Items to be Confirmed Before Installation

- Refer to the "Operating Environment" in the *Systemwalker Desktop Keeper User's Guide* to confirm if the required disk capacity can be ensure in the drive specified in the installation target of database related files.

- Refer to "Operating Environment" in the *Systemwalker Desktop Keeper User's Guide* to confirm "Products that cannot be used in mixture".

- Refer to the "Port Number List" in the *Systemwalker Desktop Keeper Reference Manual* to confirm the port numbers being used.

- When copying the Systemwalker Desktop Keeper installer from the DVD-ROM to a local disk, ensure that the target path does not contain double-byte characters.

- Installation will not be possible if any of the databases below remain in the system:

    - Symfoware RDB SWDTK

    - Symfoware RDB SWDTK2

    To check if one of these databases remains in the system, click **Control Panel** > **Administrative Tools** > **Services**.

- If you install Systemwalker Desktop Keeper in an environment where Systemwalker Desktop Keeper is already installed, services that manage iOS devices will automatically stop.
  In this case, you cannot use the services that manage iOS devices until you restart the operating system.

2.3.2.2 Installation using the Wizard

Steps to install a Management Server/Master Management Server are as follows. In addition, refer to the *Systemwalker Desktop Keeper User's Guide* for information on the operating environment.

1. Log in to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. If other applications are being used, close them.

2. After the DVD-ROM of Systemwalker Desktop Keeper is inserted into the PC, the installer window will be displayed. Select **Management Server/Management Console Installation**.
   If the above-mentioned installer is not started, start "swsetup.exe" from the DVD-ROM drive.

3. After the "Welcome to use Systemwalker Desktop Keeper Server installation" window is displayed, click the **Next** button.

4. The **Select the installation target** window is displayed.
   If the installation target displayed is not to be changed, click **Next**.
   If the installation target displayed is to be changed, click the **Browse** button of the folder to be changed, and click the **Next** button after the folder has been changed.
   The installation folder of each component is as follows:

   - Management Server or Master Management Server: *installFolder*\Server

   - Management Console: *installFolder*\MngConsole

   - Database-related files: *installFolder*\DB

   - Log Analyzer linkage commands: *installFolder*\LogAnalyzer

   ## 📙 Note

   When the installation target folder of server functions and the installation target folder of the following database related files are taken as compressed or encrypted target, the running of the application might be affected. Do not perform compression or encryption settings.

   Specify **Installation Target Folder** using up to 85 halfwidth characters, except for commas (,), semicolons (;), number signs (#), and halfwidth kana (it cannot contain fullwidth spaces, hiragana, katakana, and kanji).

   The specified drive must be NTFS-formatted (it cannot be a network drive).

5. The **Installation parameter settings** window will be displayed.
   Enter the required information, and click **Next**.
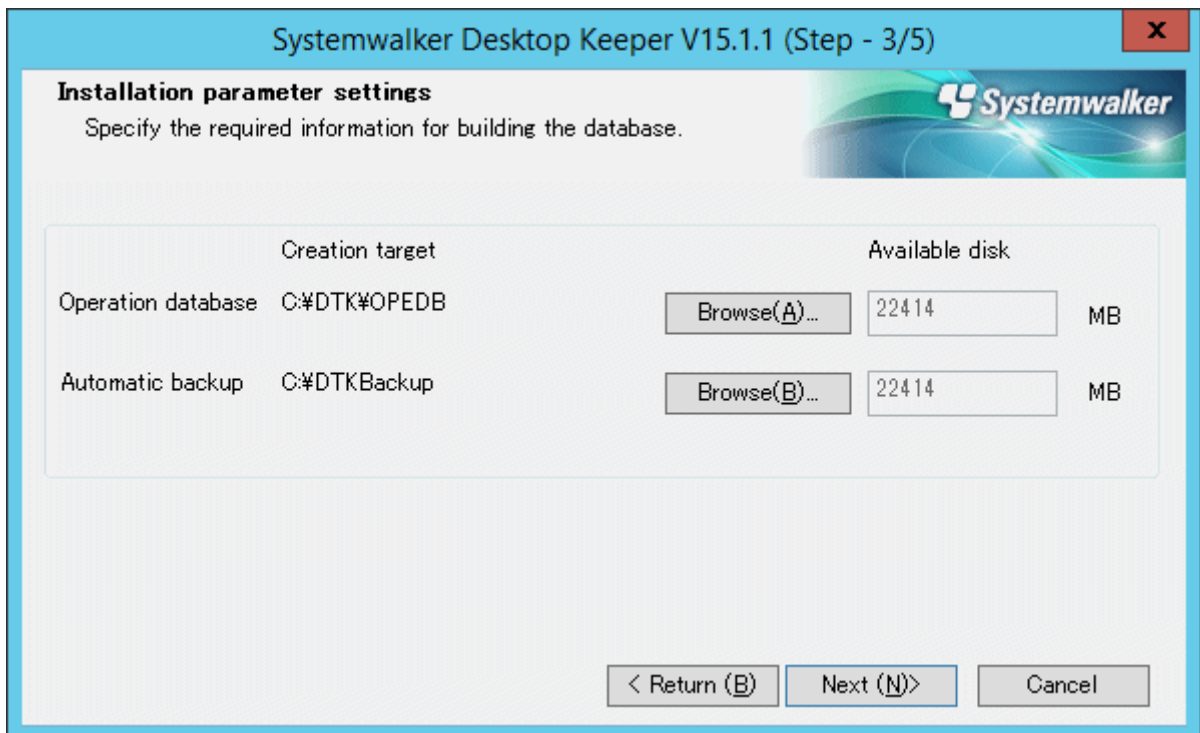
Item	Description
Operation database > **Creation target**	Specify the database creation folder. It must meet the following conditions:

Item	Description
	- The drive root cannot be specified. - It cannot contain fullwidth characters. - Specify the path using up to 96 halfwidth characters. - A network drive cannot be specified. - Specify a folder that has been NTFS-formatted. - The folder name cannot contain the following characters: \ / : * ? " < >	& ^
Automatic backup > **Creation target**	Specify the automatic backup folder. It must meet the following conditions: - The drive root cannot be specified. - A network drive cannot be specified. - You can enter the absolute path using up to 189 halfwidth characters (94 fullwidth characters). - The folder name cannot contain the following characters: \ / : * ? " < >	
Operation database > **Availabe disk**	Displays the disk availability of the specified operation database creation folder.
Automatic backup > **Availabe disk**	Display the disk availability of the specified automatic backup creation folder.

Note

For **Operation database** > **Creation target**, and **Automatic backup** > **Creation target**, estimate the required database availability beforehand using the database availability estimation tool, and specify a drive with sufficient disk availability.

Note

The initial values of automatic backup/deletion are set as follows:

- Automatic backup: Use

- Task name: DTK_Auto_Backup_Command

- Backup folder: Folder specified during installation

- Schedule type: Once daily

- Execution start time: 0:00

- Save period: 30 days

With these settings, the data will be saved for 30 days, and then deleted after that (31 days or longer).

Refer to "3.1.2.2 Automatic Data Backup and Deletion" for details on each item and changing the settings.

6. The "The installation preparation is completed." window is displayed.

   When starting the installation, click the **Install** button to start installation.

   When confirming the set content or wishing to modify it, click the **Return** button to reset.

7. The message below will be displayed. Click **OK** and continue with the installation process.

```
Register the following as login information of the Server Settings Tool:
 User ID: secureadmin
```

```
Password: secureadmin


Register the following as login information of Management Console/main menu:
 User ID: systemadmin
 Password: systemadmin
```

8. The message below will be displayed. Click **OK** and continue with the installation process.

```
Upon completion, a window informing that the installation completed successfully will be
displayed.
Installation will continue until the window is displayed, so wait until completion.
```

9. The message below will be displayed. Click **Finish**.

```
The installation of Systemwalker Desktop Keeper management server was completed.
```

10. Upon successful completion, the confirmation window will be displayed.
    To use the program, click **Yes**. The operating system will restart.

2.3.2.3 Performing Silent Installation

📌 **Note**

. . . .

- Silent installation of the Management Server or Master Management Server can only be performed when you are performing installation for the first time.

- When performing silent installation in an environment where the Management Server or Master Management Server will coexist with the Log Analyzer Server, you should install the Management Server or Master Management Server first.

- Installation process must not be interrupted during silent installation.

. . . .

Follow the procedure below to perform silent installation of the Management Server or Master Management Server:

1. Create an installation parameter CSV file.
   If you are performing installation using the default values for all parameters, this step is not required.
   Refer to "A.1.1 Installation Parameter CSV File" for details.

2. Use the parameter setup command to create a response file.
   If you did not create an installation parameter CSV file in step 1, this step is not required.
   Refer to "A.1.2 Parameter Setup Command" for details.

3. Use the silent installation script to execute installation.
   Refer to "A.1.4 Silent Installation Script" for details.

4. Check the installation result.
   Check the returned value and message from the silent installation script.

2.3.3 Construct Database

This section describes how to create a new database for a Systemwalker Desktop Keeper Management Server/Master Management Server.

Database includes the operation database for saving operation information (management information and operation log information) and the log viewing database for migrating and viewing the previous operation logs.

The operation database is required. If the Management Server or Master Management Server is newly installed, the database will be constructed automatically. Construct the log viewing database according to need.

When the database information used in the old version is used directly in V15.1.0, refer to "Chapter 4 Upgrading". However, you need to delete V15.0.0 or earlier databases.
When constructing the database during installation of the Management Server or Master Management Server, automatic backup and deletion will be configured for the data stored in the database. Refer to "3.1.2.2 Automatic Data Backup and Deletion" for details on changing the configuration.

In addition, in order to prevent database insufficiency, perform notification setting when the database space is insufficient. For notification settings when database is insufficient, refer to "2.3.6.8 Set Administrator Notification". If depletion of database space is reported, reconstruct the database immediately. Refer to "Reconstruct Database of Management Server" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

📙 Note
. . . .

If depletion of database space is reported, space is not secured until the database is reconstructed, so the notification continues to be output. Lower the notification threshold value or immediately reconstruct the database.
. . . .

📙 Note
. . . .

When constructing database, there are following restrictions and notes

[Compression and encryption of database creation target]

Do not set compression or encryption for the drive and the folder to construct database.

[Virus scan of database creation target]

Exclude the folder to construct database from the target of virus scan software.

[Users at database creation]

For the logon user name of Windows, specify alphanumeric characters beginning with a letter and with no more than 18 characters, with the Administrator authority.

[Settings of event viewer]

Confirm the maximum log size of event viewer (application log) and the settings of operation when the maximum is reached in advance so that the new event log can be recorded without any problems. Database construction may be interrupted if no event log is recorded.
. . . .

Items to be confirmed before database construction

Use the following ports to access database in Management Server/Master Management Server:

- Operation database: 42050

  If the above-mentioned port number has been used, before constructing the operation database, refer to the "Port Number List" in the *Systemwalker Desktop Keeper Reference Manual* to change the environment of Systemwalker Desktop Keeper.

- Log viewing database: 42051

  When the above-mentioned port number has been used, before constructing the log viewing database, refer to the "Port Number List" in the *Systemwalker Desktop Keeper Reference Manual* to change the environment of Systemwalker Desktop Keeper.

Guideline for the database construction time

DB construction time: 1 min.
Note: More time may be consumed depending on server performance and RAID structure.

Construct operation database

If the Management Server or Master Management Server is newly installed, the operation database will be constructed automatically. Follow the procedure below to construct the operation database manually:

1. Log in to Windows with the user that belongs to the Administrators group or the user that belongs to the Domain Admins group. When other application is being used, close it.

   Refer to the notes mentioned above for existence condition of user name.

2. Select **Start** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool** or **Apps** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool**.

3. Log on using the primary administrator account:

   - User ID: secureadmin

   - Password: Specify the initial value "secureadmin", or the password modified after installation of Management Server or Master Management Server

In the Server Settings Tool menu, click **Build, delete, or show information of database**.

The **Build, delete, or show information of database** window will be displayed.

Item Name	Description
Database creation folder	Database creation folder. The initial value is "C:\DTK\OPEDB". To change the value, click **Browse** and select the desired folder. Specify the database creation folder name using up to 96 halfwidth characters. You cannot specify the following drives: - Network drive - Non-NTFS file system drive The folder name cannot contain the following characters: - Symbols (\ / : * ? " < > | & ^) - Multibyte characters such as hiragana, katakana and kanji - Halfwidth kana - Control characters
Database usage	Usage of the created database. If the database has not been built, this item will be blank.
Disk availability	Available space on the creation destination disk.

4. Click **Construct**.
   The confirmation message is displayed. Click **OK**.

5. Creation of the database will start.

6. When the process is completed normally, the process completion message will be displayed. Click **OK**.

7. The **Automatic Backup Settings** window is displayed.

Target	Backup window

Automatic backup/ deletion	To set up if carrying out automatic backup or deletion or not:
	
	   - **Execute**: to perform automatic backup and deletion;
	
	   - **Do not execute**: not to perform automatic backup or deletion.
	
	Initial setting: **Execute**

Automatic backup/ deletion settings	To perform setting of automatic backup and deletion.
Task name	It is the task name registered in task scheduler. Fixed value (DTK_Auto_Backup_Command).

Backup target folder	Specify a folder for saving data during automatic backup. It can be specified as follows:
	
	   - Enter the absolute path of a folder
	       Enter the absolute path of the management information folder.
	
	   - Click **View**
	       In the **Browse For Folder** window, select the management information folder, and then click **OK**.
	
	Specify up to 189 bytes (can be a combination of fullwidth and halfwidth characters and symbols). The folder name cannot contain the following symbols: \ / : * ? " < > |
	
	The backup management information is stored in the subfolder MS*yyyyMmDd* of the specified folder (*yyyyMmDd* indicates the backup execution date).
	
	If multiple backups are executed to the same folder on the same date, a unique sequential number enclosed by parentheses will be appended to the subfolder name. The first backup will be saved in MSyyyymmdd, the second one in MSyyyymmdd(1), the third one in MSyyyymmdd(2), and so on.
	
	Initial value**:** Folder specified during installation

Schedule Type	Set the interval of automatic backup and deletion:

Target	Backup window
	- **Day**: perform every day; - **Week**: perform once a week; - **Month**: perform once a month. **Initial value: day**
Execution week	When **Week** is selected in **Schedule Type** , select a day of the week for execution. Monday - Sunday can be selected. Initial setting: Monday
Execution date	When **Month** is selected in **Schedule Type** , enter the date for execution. 1-31 can be entered. **Initial value:** 1
Execution start time	The time for executing automatic backup and deletion can be set. 00:00-23:59 can be specified. **Initial value:** 0:0

Saving date	Duration for operation log saved can be set.
	
	   - **Day**: 1-366 can be specified;
	
	   - **Week**: 1-54 can be specified;
	
	   - **Month**: 1-13 can be specified.
	
	 If **Day** is selected in **Schedule Type** , only **Day** can be selected.
	
	 If **Week** is selected in **Schedule Type** , **Day** and **Week** can be selected.
	
	 If **Month** is selected in **Schedule Type** , **Day** and **Month** can be selected.
	
	 Initial value:
	
	   - **Day**: 30
	
	   - **Week**: 4
	
	   - **Month**: 1
	
	 Operation log data outside the specified period will be deleted.
	
	 Example: When a period of 30 days is specified, operation log data for the 31st and later days will be deleted

Refer to "3.1.2.2 Automatic Data Backup and Deletion" for details on each item and changing the settings.

8. Select **Automatic backup/deletion** > **Execute**, and then click **Set**.

📒 Note
. . . .

Data that was automatically backed up will not be deleted automatically, and if left as is, the backup drive space may become depleted. Therefore, you should periodically delete (move) data.

. . . .

The message "[BKCI-INF001] The schedule of automatic backup has been set." will be displayed. Click **OK**.
Alternatively, select **Automatic backup/deletion** > **Do not execute**, and then click **Set**.
The message "[BKCI-INF002] The schedule of automatic backup has been canceled." will be displayed. Click **OK**.

Note

When a date after the 29th is specified in the **Execution date**, a message will be displayed to indicate that the command will not be executed for months in which the specified date does not exist.

According to the execution month, if the specified date does not exist, automatic backup and deletion cannot be conducted. In order to guarantee that the operation can be performed every month, specify the date to be before the 28th.

Note

About the time spent for automatic backup and deletion

Automatic backup and deletion will backup management information, log information in Log Viewer format and log information, and delete log information, therefore automatic backup and deletion may take some time.

Create log viewing database

The following describes how to construct a log viewing database. In addition, the log viewing database requires the construction of an operation database.

1. Log in to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. When other applications are being used, close them.

2. Refer to the attentions mentioned above for the existence condition of the user name.

3. Select **Start** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool** or **Apps** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool**.

4. Log on using the primary administrator account:

   - User ID: secureadmin

   - Password: Specify the initial value "secureadmin", or the password modified after installation of Management Server or Master Management Server

5. In the Server Settings Tool menu, click **Build, delete, or show information of database**.

   The **Build, delete, or show information of database** window will be displayed.

Item Name	Description
Database creation folder	Database creation destination folder.

Item Name	Description
	The initial value is "C:\DTK\REFDB". When changing the displayed creation target, click the **View** button to change the folder.
	The number of characters in the file name of the database creation target can be specified to be no more than 96 halfwidth characters.
	You cannot specify the following drives:
	- Network drive
	- Non-NTFS file system drive
	The folder name cannot contain the following characters:
	- Symbols (\ / : * ? " < > | & ^)
	- Multibyte characters such as hiragana, katakana and kanji
	- Halfwidth kana
	- Control characters
Database usage	Usage of the created database.
	If the database has not been built, this item will be blank.
Disk availability	Available space on the creation destination disk.

6. Click **Construct**.
   The confirmation message is displayed. Click **OK**.

7. Creation of the database will start.

8. When the process is completed normally, the process completion message will be displayed. Click **OK**.

Building an iOS Management Database

To manage iOS devices, an iOS management database must be constructed. Follow the procedure below to create an iOS management database:

1. Log on to Windows as a user that belongs to the Administrators group or Domain Admins group. If other applications are being used, then they must be closed.

   Refer to the notes above for details on conditions that apply for user names.

2. Select **Start** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool** or **Apps** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool**.

3. Log on using the primary administrator account:

   - User ID: secureadmin

   - Password: Specify the initial value "secureadmin", or the password modified after installation of Management Server or Master Management Server

4. In the Server Settings Tool menu, click **Build, delete, or show information of database**.

   The **Build, delete, or show information of database** window will be displayed.

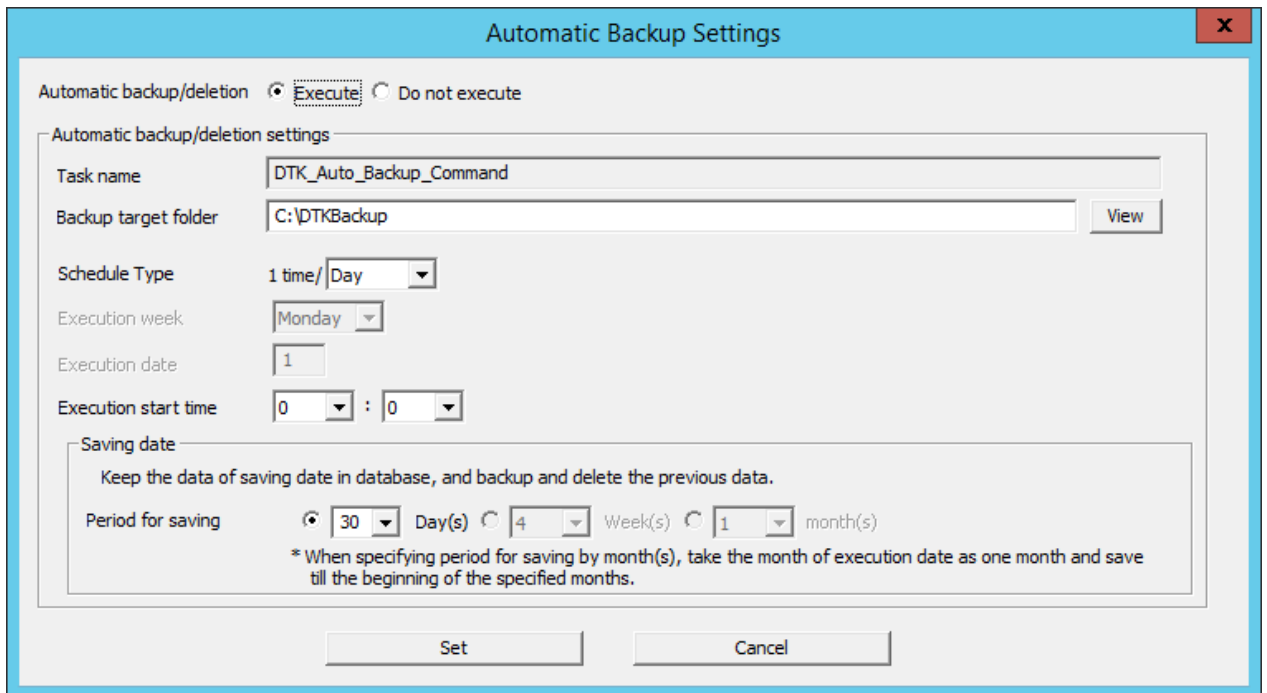| Item Name	Description
Database creation folder	Database creation folder.
	The initial value is "C:\DTK\MDMDB". To change the value, click **Browse** and select the desired folder.
	Specify the database creation folder name using up to 96 halfwidth characters.
	You cannot specify the following drives:
	- Network drive
	- Non-NTFS file system drive
	The folder name cannot contain the following characters:
	- Symbols (\ / : * ? " < > | & ^)
	- Multibyte characters such as hiragana, katakana and kanji
	- Halfwidth kana
	- Control characters
Database usage	Usage of the created database.
	If the database has not been built, this item will be blank.
Disk availability	Available space on the creation destination disk.

5. Click **Construct**.
   The confirmation message is displayed. Click **OK**.

6. Creation of the database will start.

7. When the process is completed normally, the process completion message will be displayed. Click **OK**.

The port in which the iOS management database waits will be set with the initial value (55432). If this value needs to be modified, refer to "How to Modify the Port Number" in the *Systemwalker Desktop Keeper Reference Manual*.

> 📝 **Note**
>
> - If managing iOS devices in both Systemwalker Desktop Patrol and Systemwalker Desktop Keeper, an iOS management database must be constructed for both products.
>
> - If the operating system is to be restarted after an iOS management database is constructed, the PostgreSQL_swdtmdm service must be stopped first. Open the Windows **Services** window, select the **PostgreSQL_swdtmdm** service, and click **Action** > **Stop**.
>   If the operating system is restarted before stopping the service, the following message may be output to the event log
>
> ```
> ERROR: canceling statement due to user request
> ```
>
> This is a message displayed when the operating system stops the service, and does not cause any problem to the operation.

2.3.4 IIS Settings

In order to perform management on the Web browser used in Systemwalker Desktop Keeper, IIS will be used as the Web server.

IIS will be set automatically when a Management Server/Master Management Server is being installed.

Under the environment of Windows Server(R) 2008/Windows Server(R) 2012, the application pool (**DTK**) will be created automatically.

> 📝 **Note**
>
> **Under the environment of Windows Server(R) 2008/Windows Server(R) 2012**
>
> Do not set **Read User Profile** to **True** in the detailed setting of the application pool ("DTK") used in Systemwalker Desktop Keeper.
>
> If it is set to **True**, the Web Console will not be able to run normally.

2.3.5 Register the license key

If you already have a license key, register it using the license key input command after the product is installed. This will make you an official user of the product. Official use of the product will start once you start it after becoming an official user.

If you are not yet an official user of the product, you will not be able to start the product.

The license key is registered using the fjlic register command (license key input command). The command can be executed either by specifying the license key in the parameter directly or by specifying the license key file. Refer to the *Systemwalker Desktop Keeper Reference Manual* for details on the command.

- Specifying the license key in the fjlic register command directly

```
fjlic.exe register -k <license key>
```

- Specifying the license key file in which the license key is stored in the fjlic register command

```
fjlic.exe register -f <license key file full path>
```

2.3.6 Set Environment of Management Server/Master Management Server

> 📝 **Note**
>
> **Communication security settings**
>
> To receive self version management requests from a client (CT) of V14.3.1 or earlier, switch the communication security settings. You can use the security enhancement command to switch the communication security settings. Refer to "DTKSETCN.exe (Security Enhancement)" in the *Systemwalker Desktop Keeper Reference Manual* for details.

Note

Verification when registering client (CT) devices

When performing verification during client (CT) device registration, the password to be entered during installation must be the same as the client management password specified in the **Terminal Operation Settings** window of the Management Console. Refer to "Perform Terminal Operation Settings" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

After installing a Management Server/Master Management Server and creating the database, configure the server environment to use the Sever Setting Tool.

Functions of Sever Setting Tool

The Sever Setting Tool has the following functions:

[Setting at Installation]

This is the function of setting during the initial environment construction of a Management Server/Master Management Server.

- Construct, delete, or show information of database

- System setting

- Active Directory linkage setting

- Server information setting

- Other system linkage setting

Refer to "2.3.3 Construct Database" for details on the features to construct, delete and show information on the database.

[Operation Information Setting]

This is the function of registering an administrator and setting the content and the operation for notifying the administrator during the process of operation. Set at initial environment construction.

- Administrator information setting

- Administrator notification setting

For Administrator information setting, register the user of "Management Console and Log Viewer" with access authority at the time of installation.

[Environment Setup]

This is the function used at the communication environment setup and maintenance of the Management Server.

- Management Server setting

- Trace setting

- Folder/CT self version upgrade settings

For the setting of target folder in the folder/CT self version upgrade settings

, confirm there is no problem in the initial setting at the time of installation.

[Tool]

This is the function used during silent installation of the client (CT).

- Generate CT silent installation file

Refer to "2.6.1.2 Perform Silent Installation" for details on CT silent installation file generation function.

Start method of the Server Settings Tool

The startup method of the Sever Setting Tool is as follows:

1. Log in Windows with the user that belongs to the Administrators group or the user that belongs to the Domain Admins group.

2. Select **Systemwalker Desktop Keeper** > **Server** > **Server Settings Tool** from **Start**/**Apps**. The login window will be displayed.

3. Log in with the primary administrator's account, which is:

   - User ID: secureadmin

   - Password: Specify the password modified after installation of Management Server or Master Management Server.

   In addition, a user registered in the Sever Settings Tool (requesting access authority executable by the Management Console) can be used to log in, but the functions that can be used are limited to **Administrator notification settings**.

   The password is set to "secureadmin" immediately after installing the Management Server.

4. Click the **OK** button. The following window will be displayed.
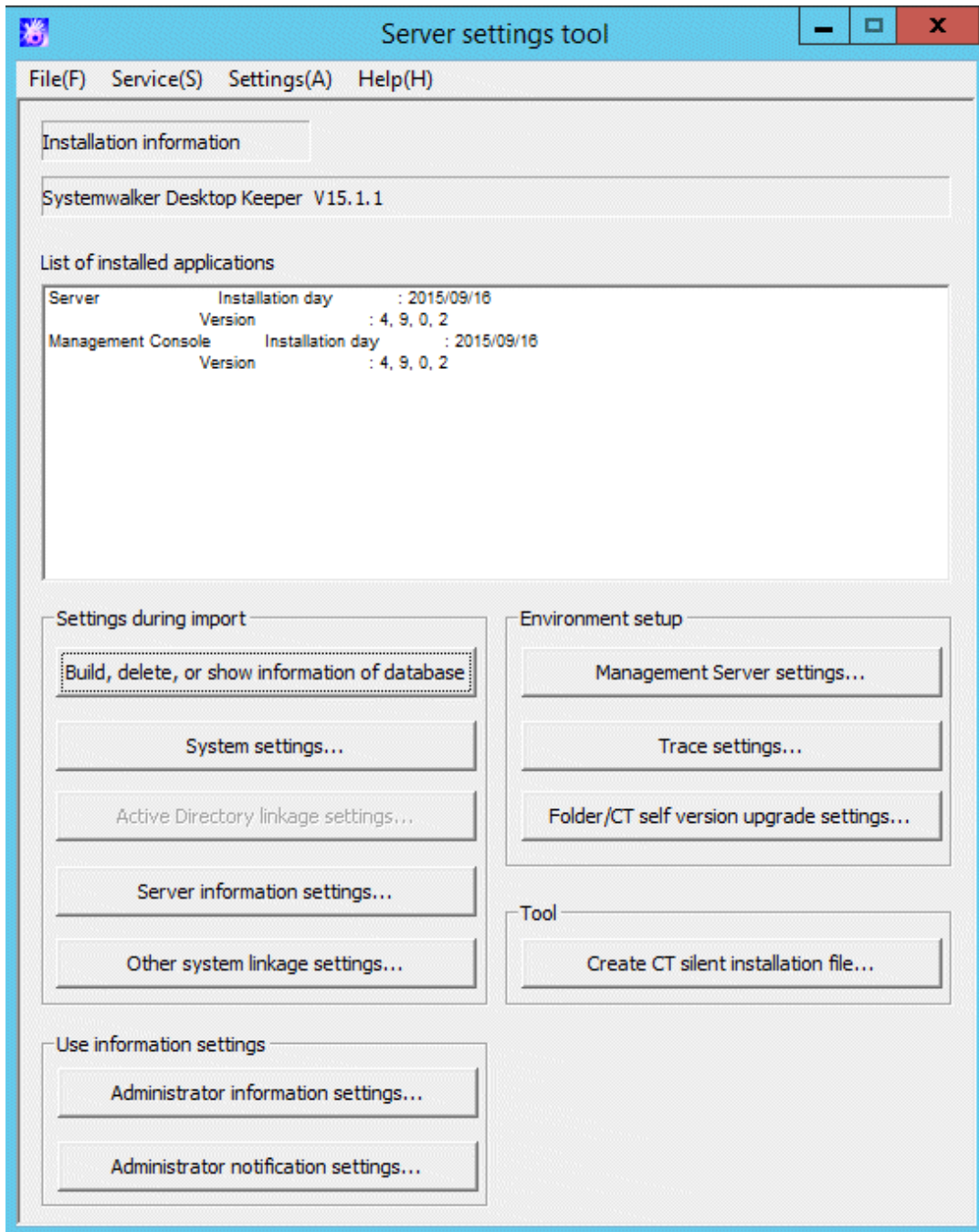
The following describes the menu bar in the **Sever settings tool** window.

Menu bar		Function summary
File	**End**	To exit Sever Setting Tool.
Service	**Confirm Service Status**	To display the operation status of **Level Control Service** and **Server Service** on the target server.
	Start Service	To start **Level Control Service** and **Server Service** on the target server.
	Stop Service	To stop **Level Control Service** and **Server Service** on the target server.
Settings	**Execute Active Directory Linkage**	To execute the processing of Active Directory Linkage.
	Execute Systemwalker Desktop Patrol Linkage	To execute the processing of linking with Systemwalker Desktop Patrol.
	Change Password	To modify the password of primary administrator; Specify the password within 32 single-bytes alphanumeric characters and symbols. The following symbols cannot be specified: & < > | \ " ~ ' ? : ^ Single-byte and double-byte spaces cannot be entered.
	Trace Server Settings Tool / **OFF**	Trace of Sever Setting Tool will not be collected.
	Summary	Trace of Sever Setting Tool will be collected in summary mode.
	Details	Trace of Sever Setting Tool will be collected in details mode.
Help	**Online Help**	To display the online manual of Systemwalker Desktop Keeper.
	Version Information	To display copyright information and version information.

To close the Sever settings , select **End** of the **File** menu.

2.3.6.1 Steps of Server Environment Setup

The steps for configuring the server environment after the installation of a Management Server/Master Management Server and database construction are as follows:

📝 **Note**

· ·

When using after the operation has been started, the service should be stopped.

If the service is not started in the settings at installation, it is not needed to stop the service. However, if the Sever Setting Tool is used to perform settings after the operation has been started, the services of the Management Server/Master Management Server should be stopped. There is no need to stop service when performing the following settings:

  - Administrator information setting

  - Administrator notification setting

  - Generate CT silent installation file

To stop services, 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:

Management Server
Master Management Server

Perform installation and setting of IIS

Install Management Server/Master Management Server — OS Restart

Construct Database

Set IIS — Execute as needed

Register the license key

Set Server Environment
Use Server Setting Tool to create the operation environment of Management Server/Master Management Server

System Settings
Perform data link method of Management Server and settings related to overall system operation.

Active Directory linkage setting
Set the Active Directory server information to be linked.
*Please perform linkage settings only when linking with Active Directory.

Server Information Setting
Set the information of this server or set information of other related server in case of 3-level system structure.

Setting of Link with Other System
Set the time of importing configuration information of Systemwalker Desktop Patrol.
* Please set only when configuration information of Systemwalker Desktop Patrol is imported automatically.

Administrator Information Settings
Register authentication user of Management Console, Log Viewer and Maintenance Tool.
* When collectively managing user information, please set in Master Management Server.

Administrator Notification Settings
Notify (e-mail notification/write event logs) the events occurred in client (CT) and database to administrator.

Saving Target Folder Settings
Set the target folder for saving command logs, attached data and unified logs.

Service Start
Start the service of Management Server (level control service, server service).

How to start service

The method to start service of the Management Server is as follows:

1. Select **Start Service** from the **Service** menu of the **Sever settings tool** window.

2. After the service startup confirmation window is displayed, click the **OK** button.

Select **Confirm Service Status** from the **Service** menu of the **Sever settings tool** window to check if the service has been started.

Note

Log in to the web console after the service has been started

After the service of the Management Server has been started, log in to the Web Console and display the status window after executing the procedure in "2.5 Settings of PC with Web Browser Installed". When not logged in, the following error may be output to the event log:

```
Event ID: 3403s
Type: Error
Source: SWDTK_LC
```

Refer to "Display Status Window" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on how to log in to the Web Console.

. . . .

2.3.6.2 Perform System Settings

Perform the settings related to overall system operation of Systemwalker Desktop Keeper Management Server.

Note
. . . .

In 3-level system structure, perform the same settings in all Management Servers.

. . . .

The system setting procedure is as follows:

1. Click the **System settings** button from the menu of Sever Setting Tool.

    The **System Setting** window is displayed.
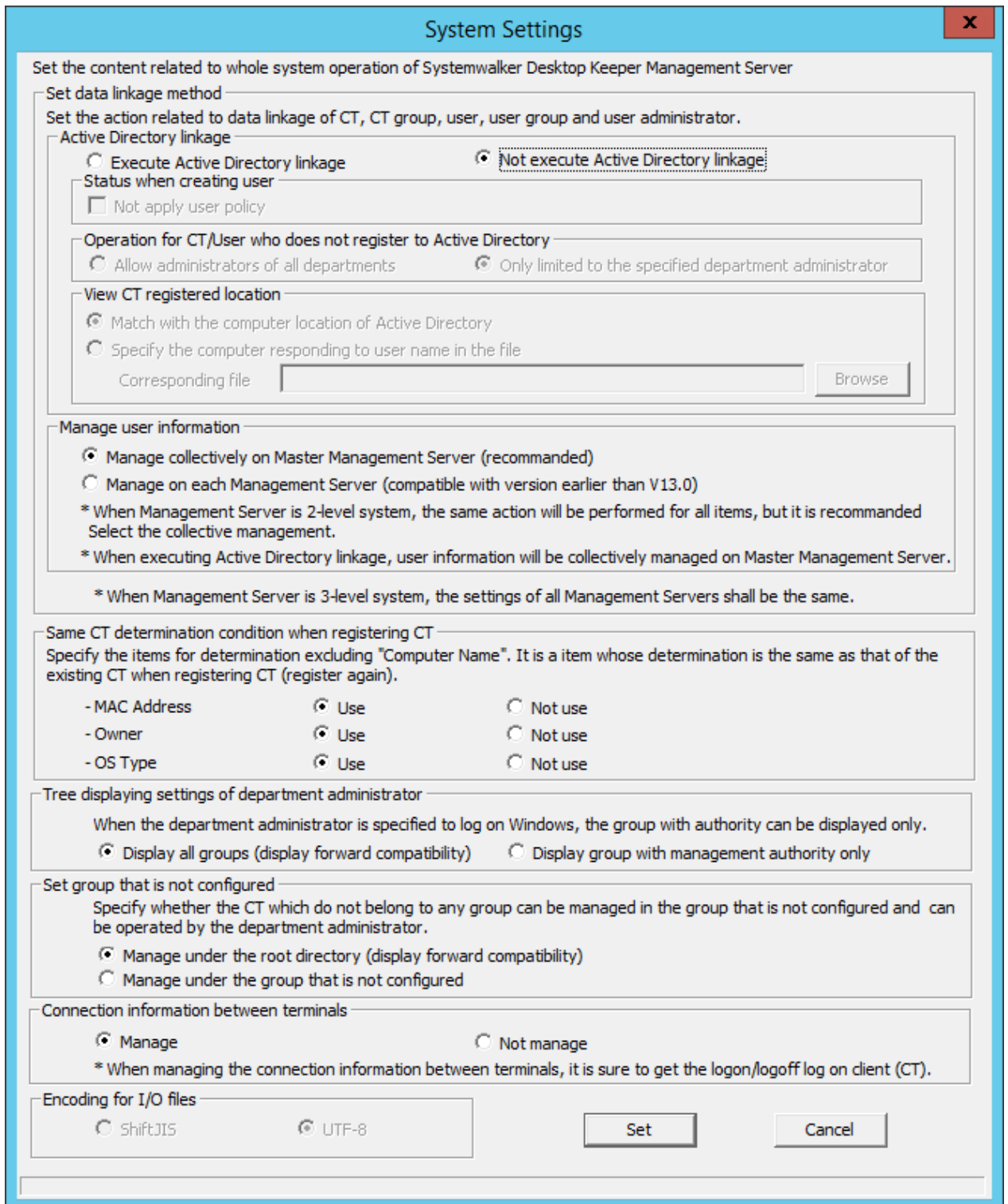
[Set data linkage method]

Item Name	Description
Active Directory linkage	To set whether to perform Active Directory Linkage or not. The setting has been specified at installation of the Management Server.

Item Name	Description
	Therefore, the setting should be performed when changing the settings at installation of the Management Server.
	Execute Active Directory linkage
	When "Execute Active Directory linkage" is selected, the following information is created according to the information of Active Directory. Therefore, it is not necessary to set in Systemwalker Desktop Keeper. When linking with Active Directory, information of local management not linked can also be set.
	- CT group and tree information
	- CT group affiliation information of the client (CT)
	- User group and tree information
	- User name
	- User group affiliation information of user name
	Not execute Active Directory linkage
	To select when it is not linked with Active Directory.
	When "Not execute Active Directory linkage" is selected, the configuration information of Systemwalker Desktop Patrol cannot be imported. In addition, the information of the product cannot be output to Systemwalker Desktop Patrol.
	After using Systemwalker Desktop Keeper and when changing the setting of active directory linkage, refer to the "Change Import Method of Configuration Information" in the *Systemwalker Desktop Keeper User's Guide for Administrator*.
Status when creating user	For a new user of Active Directory, select **Do not Apply User Policy** when importing under the **Not apply user policy** status.
Operation for CT/User who does not register to Active Directory	Specify the handling of client (CT) and user ID not registered to Active Directory. (Handle client (CT)/user ID under local management.)
	This setting has been specified at the installation of the Management Server. Therefore, set when changing the setting at the installation of the Management Server.
	Allow administrators of all departments
	This is selected when all department administrators are allowed to process the client (CT) and user ID that are not registered to Active Directory.
	Only limited to the specified department administrator
	Only the administrators specified in the Management Console are allowed to process the client (CT) and user ID that are not registered to Active Directory. When this is set to not link with Active Directory, it is limited to specified department administrators only.
	When the setting is "Only limited to the specified department administrator", the department administrators cannot set local group affiliation, CT and user directly that belong to the local group will not be displayed. In this case, the system administrator should move the CT and user to the group that can be processed by department administrators.

Item Name		Description
	View CT registered location	Select whether to acquire client (CT) location information through Active Directory or through corresponding files. Match with the computer location of Active Directory To select when acquiring location information of CT from Active Directory. Specify the computer responding to user name in the file Select this when acquiring the location information of the client (CT) from the "List of Correspondence between Computer and User". (In Active Directory, when computer information is not managed under level composition, association can be performed separately.) When this item is selected, click the **Browse** button to import corresponding files (in CSV format) that have already been created. The maximum length of the absolute path that can be specified is 255 single-byte characters (127 fullwidth characters). However, the following symbols should not be used in the file name. The following symbols cannot be specified: \ / : * ? " < > | For information on how to create corresponding files, refer to "Reference File of Active Directory Linkage" in *Systemwalker Desktop Keeper Reference Manual*.
Manage user information		In a 3-level system structure, the setting of whether to perform collective management of the user policy information in the Master Management Server or not will be configured. Because this setting has been specified when the Management Server is installed, perform the setting when changing the setting at the time of Management Server installation. Manage collectively on Master Management Server (recommended) To select when managing the user policy information in the Master Management Server. When this is set as linked with Active Directory, it is unconditionally set as the Master Management Server. Manage on each Management Server(compatible with version earlier than V13.0) Select this when managing user policy information in each Management Server.

[Same CT determination condition when registering CT]

Item Name	Description
MAC Address	Set whether the MAC address will also be taken as the judgment item for client (CT) consistency at client (CT) registration (re-registration) apart from computer name. Use Select this when MAC address is used as consistency judgment item. Not use Select this when MAC address is not used as consistency judgment item.

Item Name	Description
Owner	Set whether the owner information will also be taken as the judgment item for client (CT) consistency at client (CT) registration (re-registration) apart from the computer name.
	Use
	Select this when owner's information is used as consistency judgment item.
	Not use
	Select this when owner's information is not used as consistency judgment item.
OS Type	Set whether the OS type will also be taken as the judgment item for client (CT) consistency at client (CT) registration (re-registration) apart from computer name.
	In addition, Service Pack or version type will not be taken as consistency judgment condition.
	Use
	Select this when OS type is used as consistency judgment item.
	Not use
	Select this when OS type is not used as consistency judgment item.

Tree displaying settings of department administrator

Item Name	Description
Display all groups (display forward compatibility)	To display the group tree that is displayed when Management Console or Log Viewer is started.
Display group with management authority only	To display only the group that has administrator authority when Management Console or Log Viewer is started.

Set group that is not configured group

Item Name	Description
Manage under the root directory (display forward compatibility)	To directly manage the client (CT) that is newly registered to Management Server and the client (CT) that does not belong to any group under the Root directory group.
Manage under the group that is not configured	To directly manage the client (CT) that is newly registered to Management Server and the client (CT) that does not belong to any group under the unconfigured group.
	Perform the settings when the following operations are performed:
	- When department administrator is expected to configure the client (CT) newly registered in the Management Server;
	- When department administrator is expected to manage the policy of the client (CT) that does not belong to any group.
	![Note icon] **Note**
	About the status window and Log Viewer
	Department administrator cannot view the group that is not configured. Only the system administrator can view the group that is not configured.
	About Log Analyzer or Report Output Tool

Item Name	Description
	Even this setting has been performed in Log Analyzer or Report Output Tool, the client (CT) will not be managed in the "Unconfigured" group, but in the "root" group instead.

Connection information between terminals

Item Name	Description
Manage	To manage the information of remote connection to physical PC and virtual PC.
Not manage	Not manage the information of remote connection to physical PC and virtual PC.

Encoding for I/O files

Item	Description
Shift-JIS (not selectable)	Specify Shift-JIS as the encoding format for I/O files.
UTF-8	Specify UTF-8 as the encoding format for I/O files.

2. Confirm the content of settings and change according to the needs. Click the **Set** button.

2.3.6.3 Perform Settings of Active Directory Linkage

When linking with Active Directory, set the server information of the Active Directory to be linked.

The steps for Active Directory linkage setting are as follows.

1. Click **Active Directory linkage settings** in the menu of the **Sever settings tool**.

   The **Active Directory Linkage Settings** window is displayed.

Item Name	Description
Computer name	Enter the computer name of the Active Directory to be linked.
	Up to 15 single-byte characters can be entered. Only single-byte alphanumeric characters and hyphen "-" can be entered (Hyphen "-" should not be specified at the beginning or the end).
	When computer name has been omitted, NetBIOS name will be acquired according to the domain address and registered to the database. "(Automatic Judgment)" will be displayed on the window.
Domain name (required)	Enter the domain name of the Active Directory to be linked.
	Specify up to 155 halfwidth alphanumeric characters, periods and hyphens (however, do not specify periods or hyphens at the beginning or at the end). IP address and NetBIOS domain name cannot be entered.
	Specification example: desktopkeeper.domain.com
	There is only 1 Active Directory server (domain) that can be linked.
NetBIOS name (required)	NetBIOS name.
	If you click **Add** or **Update** with no value is specified, the DNS will be browsed based on **Domain name** and the NetBIOS name will be obtained. If the NetBIOS name cannot be obtained, you will need to specify it manually.

Item Name	Description
	Specify up to 16 halfwidth characters and the following symbols: ~ ! @ # $ % ^ & ( ) _ - { } [ ] ' . /

Execute linkage (required)	Set to execute or stop Active Directory linkage.
	
	Execute
	
	    To execute Active Directory linkage.
	
	Stop
	
	    To stop Active Directory linkage.
	    When scheduler is used to execute Active Directory linkage, this should be used when the linkage is stopped temporarily.

User Name (required)	Enter the user name registered in Active Directory for viewing the information of Active Directory (before @ of the logon name of user in Active Directory). Up to 40 single-byte characters can be entered. Characters that can be entered include single-byte alphanumeric characters, spaces and the following symbols: ! # $ % & ' ( ) - . ^ _ ` { } As long as the user is registered in Active Directory, you will be able to link with Active Directory no matter what user is specified.
Password (first entry) (required when adding)	Enter the password of the above user name. Up to 32 single-byte characters can be entered. Characters that can be entered include single-byte alphanumeric characters, spaces and the following symbols: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /
Password (re-entry) (required when adding)	In order to avoid wrong registration, enter the password again.

2. Enter the required setting items, and click the **Add** button.

3. Click the **Close** button.

2.3.6.4 Set Server Information

Information of the server will be registered during initial installation. In a 3-level system structure, information of other relevant servers will be set.

Steps to set server information are as follows:

1. Click the **Server information settings** button in the menu of **Sever settings tool**.

    The **Server Information Settings** window is displayed.

Item Name	Description

Node type	Select the classification of the server node to be set.
	
	Own node
	
	    Select this in the following cases:
	
	      - When setting 2-level Management Server
	
	      - When setting this server on 3-level Master Management Server
	
	      - When setting this server on 3-level Management Server.
	
	    Local node information will be registered as initial status. Select at the time of update.
	
	Other node
	
	    Select this in case of setting other servers:
	
	      - When setting a Master Management Server on the 3-level Management Server
	
	In a 3-level Master Management Server:
	
	Information of other nodes will be automatically registered when the communication with Management Server is started. Therefore, it is not necessary to set the information of other nodes.
	
	In a 2-level the Management Server:
	
	Register only the local node and the node of Master Management Server. Do not set the node of other Management Server.

Node name	Enter the node name of the server being set. Up to 36 single-byte characters can be entered. Only single-byte alphanumeric characters and hyphen "-" can be entered (hyphen "-" should not be specified at the beginning or the end). Single-byte lower-case letter will be automatically converted to single-byte upper-case letter. It will automatically set as the local computer name under local node, but will set to "NODE" when it is unable to acquire from the system or the computer name exceeds 16 characters. Set again at this time if necessary.

Item Name	Description
Computer name	When the node is classified as local node, enter the computer name of the server.
	When the node is classified as other node, enter the computer name of Master Management Server.
	Up to 15 single-byte characters can be entered. Only single-byte letters, numbers and hyphen "-" can be entered (hyphen "-" should not be specified at the beginning or the end).
	Under local node, the computer name will be set automatically. However, when it is unable to acquire from the system or the computer name exceeds 16 characters, it will be set to "COMPUTER". Set again at this time if necessary.
	The computer name set here will be displayed in the CT group of the Management Console.
Server IP address or server name	When the node is classified as local node, enter the IP address of the server.
	When the node is classified as other node, enter the IP address of the Master Management Server.
	In addition, under local node, the IP address of the computer will be set automatically during construction of the database. However, when it is unable to acquire from the system or the IP address has not been set at the time of registration, it will be set to loop back address. Reset at this time.
	- If a server name is specified:
	- Specify up to 15 halfwidth alphanumeric characters and hyphens (-).
	- Do not specify only numbers.
	- If an IPv4 address is specified:
	- Specify up to 15 halfwidth numbers and periods (.).
	- If an IPv6 address is specified:
	- Specify up to 39 halfwidth letters (A-F, a-f), numbers, and colons (:).
	- Do not specify a link-local address, otherwise behavior is not guaranteed.
	Note: It is necessary to be able to resolve the host name of the Management Server or Master Management Server on each machine. Otherwise, communication will not be possible between the Master Management Server and Management Server, and between the Management Server or Master Management Server and the client (CT).
	Note: IPv6 addresses can be abbreviated using RFC 5952-compliant format.
Server classification	Enter the classification of server.
	Root Server:
	Select this in case of an upper-level server:
	- When it is the Management Server of 2-level system;
	- When it is the Master Management Server of 3-level system.
	Sub-Level Server
	Select this in case of a sub-level server:
	- When it is the Management Server of 3-level system.
	In initial status, it will be set to "Root Server" (not relying on construction options).
Update date and time	To display the date on which the server information is updated. The date of updating other nodes (Management Server) in the Master Management Server of 3-level system will be updated when the level control service is started in other nodes (Management Server).

Item Name	Description
	The date of updating other nodes (Master Management Server) in a Management Server of a 3-level system is blank.
	In initial status, the date of database construction will be displayed in the list.
Registration date and time	To display the date on which the server information is registered. The date of registering other nodes (Management Server) in the Master Management Server of 3 a-level system will be registered when the level control service is started in other nodes (Management Server) for the first time.
	In initial status, the date of database construction will be displayed in the list.

2. Enter the required setting items and click the **Add** button.

3. Click the **Close** button.

2.3.6.5 Set the Link with Other Systems

Perform the setting when Systemwalker Desktop Patrol configuration information is imported automatically.

1. Click the **Other system linkage settings** button in the menu of Sever Setting Tool.

2. The **Other System Linkage Settings** window is displayed.
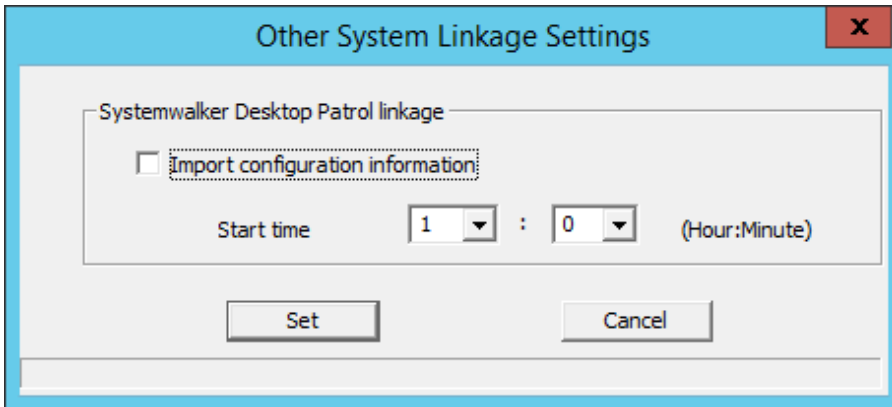
Item Name	Description
Import configuration information	Select this when the configuration information of Systemwalker Desktop Patrol is imported automatically.
Start time	Time to start the automatic import. Only takes effect if **Import configuration information** is selected. 📌 **Note** . . . . Do not set the time frame when the Management Server service is stopped. . . . .

📌 **Note**

. . . .

If the configuration information of Systemwalker Desktop Patrol is imported automatically, it is necessary to specify the URL of Systemwalker Desktop Patrol in **URL of Desktop Patrol** under **Environment Setup** in the global navigation of the web console.

. . . .

2.3.6.6 Set Administrator Information

Register the authenticated user of the Management Console, Log Viewer, Log Analyzer, status window, environment setup, report output tool, backup tool and restoration tool. In addition, when department management mode is used, register the department administrator. During installation, make sure to register the administrator whose access authority is "Management Console and Log Viewer".

However, in case of collectively managing user policy (user information) in the Master Management Server with a 3-level structure, if setting has been performed in the Master Management Server, then it is no need to set in the Management Servers. After the operation has been started, it will be reflected to all Management Servers automatically.

There are following two methods for the procedure of administrator information settings:

- Register administrators one by one;
- Use CSV file to register administrators collectively

Register administrators one by one

1. Click the **Administrator information settings** button in the menu of Sever Setting Tool.

   The **Administrator Information Settings** window is displayed.

Item Name	Description
User ID	Up to 40 single-byte characters (20 double-byte characters) can be entered. It cannot contain spaces, halfwidth katakana, and the following symbols: & < > | \ " ~ ' ? : ^ Double-byte or single-byte spaces should not be entered. It is not case-sensitive.
User name	Up to 40 single-byte characters (20 double-byte characters) of alphanumeric characters, Chinese characters and symbols can be entered.

Item Name			Description
Access authority			Select the following authority.
			No Authority for Browsing
			Users that cannot execute Management Console, Log Viewer, Log Analyzer, status window, environment setup, report output tool, backup tool, backup command, restoration tool and Sever Settings Tool (some functions) (to use when they do not have execution authority temporarily)
			Log Viewer
			Users that can only execute Log Viewer, Log Analyzer, status window, environment setup, and report output tool.
			Management Console / Log Viewer
			Users that can execute Management Console, Log Viewer, Log Analyzer, status window, environment setup, report output tool and Sever Settings Tool (partial functions).
			Management Console
			Users that can execute the administrator notification setting of the Management Console and Sever Settings Tool.
			(Department Administrator) Log Viewer
			Department administrators that can only execute Log Viewer, status window and report output tool.
			(Department Administrator) Log Viewer / Management Console
			Department administrators that can execute Management Console, Log Viewer, status window and report output tool.
			(Department Administrator) Management Console
			Department administrators that can only execute Management Console.
			Backup / Restore
			Users that can execute backup tool, restoration command and restoration tool.
Password (first entry)			Specify up to 32 halfwidth alphanumeric characters, except for spaces and the following symbols: & < > | \ " ~ ' ? : ^
Password (re-entry)			In order to avoid wrong registrations, re-enter the password.
E-mail address			Enter the E-mail address of registered user.
			Specify up to 255 bytes (can be a combination of fullwidth and halfwidth characters), except for the following: < > ( ) [ ] \ : ; "
Notes			Up to 256 single-byte characters (128 double-byte characters) of alphanumeric characters, Chinese characters and symbols can be entered.
Detailed authority	**Management**	**Import CSV file**	Select when granting the following execution authority in the Management Console to the registered users (selected).
			- Import user information of user policy
			- Import configuration information through Systemwalker Desktop Patrol linkage

Item Name			Description
		Save CSV file	Select when granting the following execution authority in Management Console to the registered user (selected). - User information export of user policy - Export configuration information through Systemwalker Desktop Patrol linkage
		Register/ update/ delete USB device	Select when granting the operation authority of the USB device individual identification function in the Management Console to the registered user (selected).
		Unable to use other functions	Select when granting registration/modification/deletion authorities to USB device through Management Console (selected). This can only be set when the setting of **Access Authority** is **(Department Administrator) Management Console**.
	Log Viewer	Save CSV file	Select when granting the execution authority of CSV export log in the Log Viewer to the registered user (selected).
		View/save attached information	Select when granting the following execution authorities in the Log Viewer to the registered user (selected): - Display the image of screen capture data - Save original backup file
		Save E-mail contents	Select when granting the following execution authorities in the Log Viewer to registered user (selected): - View the content of sent E-mail - View the content of file attachment
		View Configuration Change Log	Select when granting the view authorities of configuration change logs in the Log Viewer to the registered user (selected).
		View backup log	Select when granting the view authorities of backup log logs in the Log Viewer to the registered user (selected).
Password change date			Display the last date on which the password is changed.
Update date and time			Display the date on which the user information is updated.
Registration date and time			Display the date on which the user information is registered.

2. Enter necessary setting items and click **Add**.
   Repeated the Step 2. for continuous setting.

3. Click **Close**.

P Point
. . . .

When modifying administrator information

- When it is not necessary to change the password when modifying administrator information, leave the password input field blank (Password (first entry), Password (re-enter)).

- When it is expected to change the user ID only instead of changing other conditions such as user and authority, add a new administrator. Set the same conditions for other input items.

About automatic backup and deletion of user

Register the following information during database construction, database migration and restoration for the administrator to perform automatic backup and deletion.

User ID: AUTOBACKUPUSER

User Name: Auto backup user

Access Authority: Backup / Restore

Only password can be changed for automatic backup and deletion user. When the initial value of the password is changed, change the password.

. . . .

Note

. . . .

Deleting the administrator information

- Deleting the department administrator causes department administrator information to be deleted as well.

- When deleting the system administrator or department administrator, they are managed as separate persons even if created again under the same name. If the department administrator will use the Log Viewing Database, you should restore the latest administrator information to the Log Viewing Database.

. . . .

Method to register administrators collectively

The following describes how to register administrators collectively by using the administrator information file.

For administrator information file, refer to "Administrator Information File" in the *Systemwalker Desktop Keeper Reference Manual*.

1. Click the **Administrator information settings** button in the menu of Sever Setting Tool.

2. Select **Import file**. The following window will be displayed.

Item Name	Description

Import file (required)	Specify the created CSV file. The specification method is as follows.
	
	- Enter the file name with full path.
	  Enter with a full path till the CSV file to be imported in the input field.
	
	- Enter through the **Browse** button.
	  When **Specify the imported file** window is displayed, specify the importing CSV file and click the **Save** button.
	
	The length of the full path that can be specified should be no more than 218 single-byte characters (109 double-byte characters). The following symbols cannot be used as the

Item Name	Description
	file name. The following symbols cannot be specified: \ / : * ? " < > |
Execution log file (required)	Specify the file to output execution result when importing CSV file. The error during import will also be output in this file. The specification method is as follows. - Enter the file name with full path. Enter with a full path till the log file to be output in the input field. - Enter through the **Browse** button. When **Specify the executed log file** window is displayed, specify the log file to be exported and click the **Save** button. The length of the full path that can be specified should be no more than 218 single-byte characters (109 double-byte characters). The following symbols cannot be used as the file name. The following symbols cannot be specified: \ / : * ? " < > |
When execution log file exists (required)	In **Execution log file**, select the exporting method when the file for log output has been already specified. - **Add** Add execution log with the previous information being retained. - **Overwrite** Output execution log without retaining the previous information.

3. Enter all the items and click the **Start Import** button. The **Display the import status of administrator information** window will be displayed, and processing will be started.

4. Confirm the information displayed in the execution status, and click the **OK** button.

2.3.6.7 Output Administrator Information

This section describes how to output administrator information.

For administrator information file, refer to "Administrator Information File" in *Systemwalker Desktop Keeper Reference Manual*.

1. Click the **Administrator information settings** button in the menu of Sever Setting Tool.

2. Select **Output file**. The following window will be displayed.
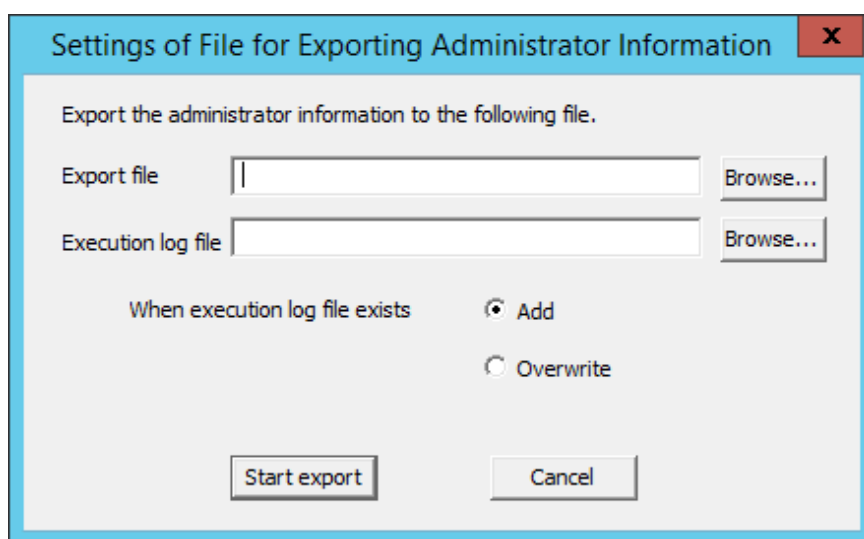
Item Name	Description
Export file (required)	Specify the CSV file to be output. The specification method is as follows.

Item Name	Description
	- Enter the file name with full path. Enter with a full path till the CSV file to be imported in the input field. - Enter through the **Browse** button. When **Specify the output file** window is displayed, specify the importing CSV file and click the **Save** button. The length of the full path that can be specified should be no more than 218 single-byte characters (109 double-byte characters). The following symbols cannot be used as the file name. The following symbols cannot be specified: \ / : * ? " < > |
Execution log file (required)	Specify the file to output execution result when importing CSV file. The error during import will also be output in this file. The specification method is as follows. - Enter the file name with full path. Enter with a full path till the log file to be output in the input field. - Enter through the **Browse** button. When **Specify the executed log file** window is displayed, specify the log file to be exported and click the **Save** button. The length of the full path can be specified should be no more than 218 single-byte characters (109 double-byte characters). The following symbols cannot be used as the file name. The following symbols cannot be specified: \ / : * ? " < > |
When execution log file exists (required)	In **Execution log file**, select the exporting method when the file for log output has been already specified. - **Add** Add execution log with the previous information being retained. - **Overwrite** Output execution log without retaining the previous information.

3. Enter all the items and click the **Start export** button.

2.3.6.8 Set Administrator Notification

Events occurred in the client (CT) and database can be notified to the administrator (E-mail notification, writing to event log).

Events that can be notified and timing of notification are as follows:

- Notification of prohibition operation and violation operation in the client (CT).

  Notify immediately after prohibition logs are collected.

  System administrator and department administrator can be notified by E-mail.

- Notification of database exception

  Notify when the threshold of database space and disk space is reached.

  Notify immediately when there is no available database space and it is unable to write information into the database.

  Only notification to the system administrator by E-mail is allowed.

- Notification of client (CT) information

  When the client (CT) is started, notify immediately when Management Server detects modification of client (CT) information.

  System administrator and department administrator of CT group can be notified by E-mail.

When notifying the department administrator, refer to "Allocate Department Administrator" in *Systemwalker Desktop Keeper User's Guide for Administrator*.

The steps to set administrator notification are as follows:

1. Click the **Administrator notification settings** button in the menu of Sever Settings Tool.

    The **Administrator Notification settings** window is displayed.
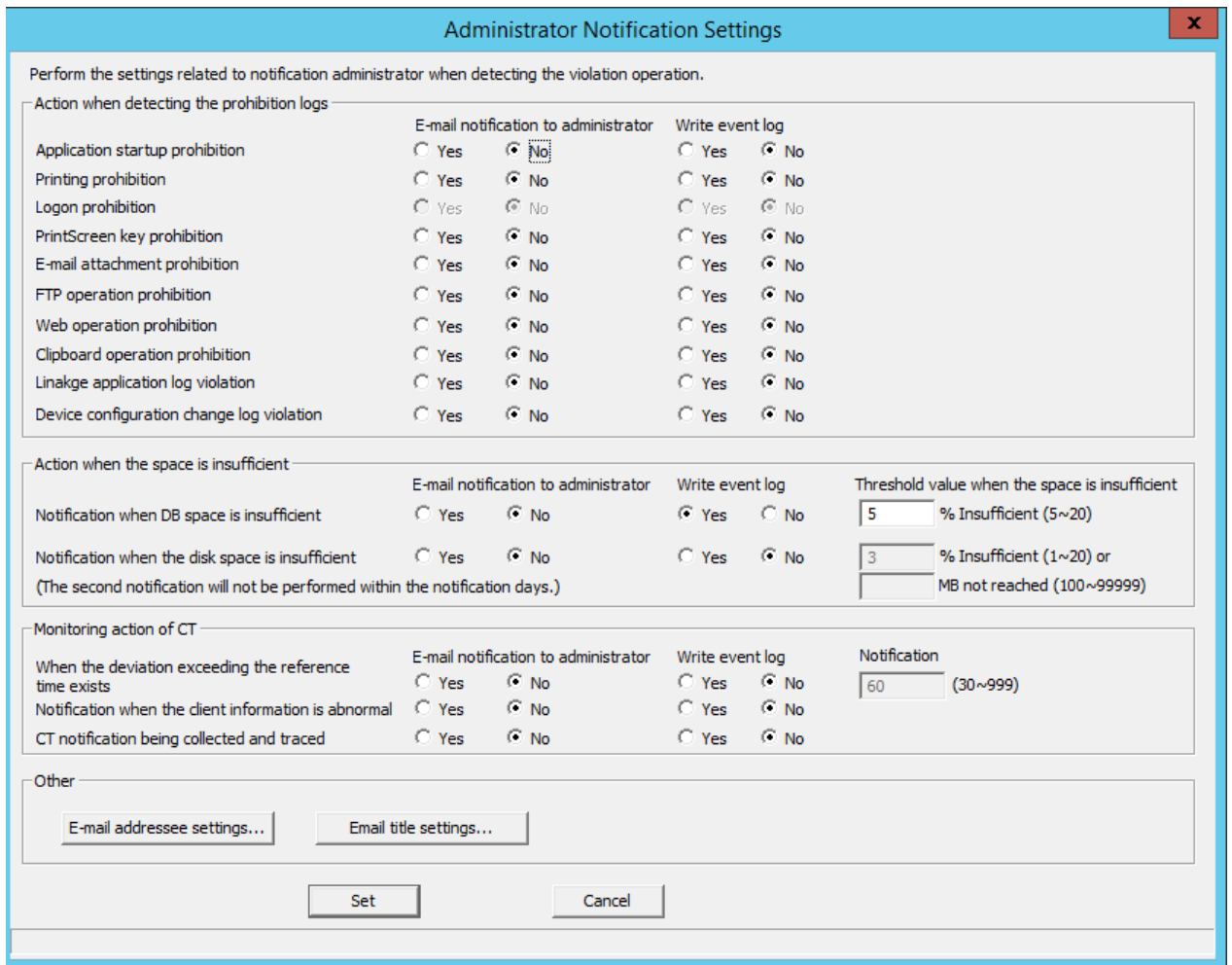
[Action when detecting the prohibition logs]

Set whether the E-mail notification to administrator or writing to event log exists when each prohibition log is detected.

The following types of logs can be set:

- **Application startup prohibition**

- **Printing prohibition**

- **Logon prohibition**

- **PrintScreen key prohibition**

- **E-mail attachment prohibition**

- **FTP operation prohibition**
  When FTP server connection prohibition log is detected.

- **Web operation prohibition**
  When URL access prohibition log, Web upload prohibition log and Web download prohibition log are detected.

- **Clipboard operation prohibition**
  When clipboard operation prohibition log is detected.

- **Linkage application log violation**
  Note: In case of linkage application log (classified as violation)

- **Device configuration change log violation**

Note

Email notifications for the smart device (agent) administrator and writing to the event log

The following violation logs recorded using the smart device (agent) belong to the **Device configuration change log**, however, email notifications to the administrator and writing to the event log will not be performed.

- Wi-Fi connection prohibition log

- Bluetooth connection prohibition log

- Application usage prohibition log

As actions when all logs are detected, the contents that can be set are as follows:

Item Name	Description
E-mail notification to administrator	Yes Send notification E-mail when detected. No Do not send notification E-mail when detected.
Write event log	Yes Write violation log information to event log when detected. No Do not write violation log information to event log when detected.

[Action when the space is insufficient]

Set whether to notify the administrator by E-mail or write to event log when the disk for writing collected log is insufficient.

Types of space that can be set are as follows:

- **Notification when DB space is insufficient**

  1. When available space in database becomes insufficient, information cannot be written to the database.

  2. When available space in database is lower than the value set in the [Threshold value when the space is insufficient].

  The database availability check is performed at the following timing:
  - When the date is changed (0:00)

- **Notification when the disk space is insufficient**

  Disk space is insufficient, i.e. the available space of the disk in which the following specified folders are located is lower than the value set in **Threshold value when the space is insufficient**.

  - Attached data saving folder

  - E-mail content folder

  - Command log folder

  - Collective log sending folder

  - Trace log folder

  - Trouble investigation data saving target folder

  - Automatic backup target folder

When space is insufficient, the contents that can be set are as follows:

Item Name	Description
E-mail notification to administrator	Yes Send notification E-mail when detected. No Do not send notification E-mail when detected.
Write event log	Yes Write violation log information to event log when detected. No Do not write violation log information to event log when detected.
Threshold value when the space is insufficient Note: When database space is insufficient	Set the value for domain value of notification at insufficiency by specifying % (unit: insufficiency %). Positive integer within 5-20 can be set. Enter when at least one item of **E-mail notification to administrator** and **Write event log** is set to **Yes**. Initial value is 5%.
Threshold value when the space is insufficient Note: When disk space is insufficient	Set the value for domain value of notification at insufficiency by specifying % (unit: insufficiency %) or capacity (unit: insufficiency MB). Enter when at least one item of **E-mail Notification to Administrator** and **Write event log** is set to **Yes**. When both domain value values of notification have been set for both % and capacity specification at the time of insufficiency, the domain value of smaller capacity will be effective. Positive integer within 1-20 can be set in % specification. Initial value is less than 3%. Positive integer within 100-99999 can be set in capacity specification. There is no initial value. In addition, when entering 100MB, the value calculated by the following calculation formula can be set. 100*1024*1024=104,857,600 bytes

[Monitoring action Of CT]

Set this to notify the administrator by email and write to the event log on startup of the client (CT) if the client (CT) information has been changed.

The notification content that can be set are as follows:

- **When the deviation exceeding the reference time exists**

System time of the client (CT) and the system time of the Management Server have deviation that exceeds the standard time.

A check for deviations is performed upon communication with the Management Server during client registration or after the operating system starts up on the client.

- **Notification when the client information is abnormal**

When intrinsic information "CTID" is detected on the client (CT) repeatedly.

Notify administrator and event log about the event described as "MAC Address Modification".

Repetition of "CTID" may occur when the master PC is used to extend the client (CT).

- **CT notification being collected and traced**

When client (CT) that is collecting and tracking is detected.

By notifying the administrator the client (CT) in the status of trace and collection, this can be set as trace not collected by administrator.

Checking of the client (CT) during trace collection will be performed at the following timing:
- When the Systemwalker Desktop Keeper service starts (including when the server starts)
- When the date changes (0:00)

The setting will be valid within 1 month after the last logon date. Therefore, no notification will be issued after it exists in the environment that has not been cancelled by the file server for more than one month.

For the client (CT) monitoring action, the contents that can be set are as follows:

Item Name	Description
E-mail notification to administrator	Yes Send notification E-mail when detected. No Not send notification E-mail when detected.
Write event log	Yes Write violation log information to event log when detected. No Not write violation log information to event log when detected.
Notification (note)	Taking minute as unit, specify the time difference between the system time of the client (CT) and the system time of the Management Server. Positive integer within 30-999 can be set. Enter when at least one between **E-mail notification to administrator** and **Write event log** is set to **Yes**. Initial value is 60 minutes.

Note: Setting items when **Deviation that Exceeds Standard Time Exists**.

📭 Note

Email notifications for the smart device (agent) administrator and writing to the event log

Email notifications to the administrator and writing to the event log will not be performed for the following notification items in the smart device (agent):

- **When the deviation exceeding the reference time exists**

- **Notification when the client information is abnormal**

- **CT notification being collected and traced**

Other Settings/E-mail addressee settings

Click **E-mail addressee settings**. The **E-mail Addressee Settings** window will be displayed.

Specify the required information for email notifications to the administrator.

Item Name	Description

Send mail server IP address or server name	When notifying the administrator by E-mail, enter the SMTP server name.
	
	 - If a server name is specified:
	
	    - Specify up to 255 halfwidth alphanumeric characters and hyphens (-), and halfwidth periods (.) as label delimiters.
	
	    - Symbols cannot be specified, except for halfwidth hyphens (-). When SMTP server name shall be restricted, use IP address to specify.
	
	    - Do not specify hyphens (-) at the beginning or at the end of the label.
	
	    - It cannot contain only numbers.
	
	 - If an IPv4 address is specified:
	
	    - Specify up to 15 halfwidth numbers and periods (.).
	
	    - A loopback address (127.0.0.1) cannot be specified.
	
	 - If an IPv6 address is specified:
	
	    - Specify up to 39 halfwidth letters (A-F, a-f), numbers, and colons (:).
	
	    - A loopback address (::1) cannot be specified.
	
	    - Do not specify a link-local address, otherwise behavior is not guaranteed.
	
	 Note: IPv6 addresses can be abbreviated using RFC 5952-compliant format.

port number	Enter the port number used for sending E-mail. Initial value is 25.
Perform SMTP authentication	Set whether to perform SMTP authentication in the communication with the E-mail sending server.

Item Name		Description
		Yes
		Select when performing SMTP authentication.
		No
		Select when SMTP authentication is not performed.
	Authentication method	Select authentication method when **Perform SMTP authentication** is set to **Yes**. The methods that can be selected are as follows: - CRAM-MD5 - LOGIN - PLAIN - AUTO When AUTO is selected, authentication method will be automatically determined according to the following sequence. The initial value is AUTO. 1) CRAM-MD5 2) PLAIN 3) LOGIN
	Authentication user ID	Enter the user ID when carrying out SMTP authentication in the communication with the E-mail sending server. Specify up to 40 halfwidth characters. Authentication user IDs including any of the characters below or comprised only of periods cannot be entered. \ / [ ] : | < > + = ; , ? * @ "
	Authentication password (first entry)	Enter the password of SMTP authentication user ID. Specify up to 32 halfwidth characters, except for kana.
	Authentication password (re-entry)	Re-enter the password in order to avoid wrong registration.
E-mail address (TO)		Enter the address of E-mail recipient (To) when notifying the system administrator by E-mail. Specify up to 5 email addresses using up to 255 halfwidth characters, except for the following symbols: \ " ( ) [ ] < > , . ; : Specify up to 5 email addresses. Use a semicolon (;) to separate email addresses.
E-mail address (CC)		Enter the address of E-mail recipient (CC) when notifying the system administrator by E-mail. It is not required to enter when not sending to CC. Specify up to 5 email addresses using up to 255 halfwidth characters, except for the following symbols: \ " ( ) [ ] < > , . ; : Specify up to 5 email addresses. Use a semicolon (;) to separate email addresses.
E-mail address (FROM)		Enter the address of the E-mail sender when notifying the system administrator by E-mail. Specify up to 255 halfwidth characters, except for the following symbols: \ " ( ) [ ] < > , . ; :

Other Settings/Email title settings

Click **Email title settings** - the **Email title settings** window is displayed.

Specify the title of email notifications for the administrator.

Item Name	Description
Prohibition log detection (required)	Title of email notifications for the administrator sent when prohibition logs are detected. Specify up to 255 bytes (can be a combination of fullwidth and halfwidth characters). The initial value is "Systemwalker Desktop Keeper WARNING Report at {@DATE} {@TIME}". To restore the initial value, click **Initial value**. - Refer to "Parameters that can be set" for details.
Operation when space is depleted (required)	Title of email notifications for the administrator sent when depletion of space is detected. Specify up to 255 bytes (can be a combination of fullwidth and halfwidth characters). The initial value is "Systemwalker Desktop Keeper WARNING Report at {@DATE} {@TIME}". To restore to the initial value, click **Initial value**. Refer to "Parameters that can be set" for details.
CT monitoring operation (required)	Title of email notifications for the administrator sent when client (CT) information has been changed. Specify up to 255 bytes (can be a combination of fullwidth and halfwidth characters). The initial value is "Systemwalker Desktop Keeper WARNING Report at {@DATE} {@TIME}". To restore to the initial value, click **Initial value**. Refer to "Parameters that can be set" for details.

Parameters that can be set

The parameters that can be set for each notification are described below.

Parameter	Content in the email title if specified	Prohibition log detection	Operation when space is depleted	CT monitoring operation
{@DATE}	Operation date for logs notified to the administrator	Y	Y	Y
{@TIME}	Operation time for logs notified to the administrator	Y	Y	Y
{@KIND}	Type of log notified to the administrator	Y	N	Y
{@SV}	Name of the (integrated) server where logs notified to the administrator have accumulated	Y	Y	Y
{@CT}	Name of the client (CT) where the operations for which the logs are notified to the administrator were performed	Y	N	Y
{@COMP}	Name of the client (CT) computer where the operations for which the logs are notified to the administrator were performed	Y	N	Y
{@USER}	Name of the user that performed the operations for which the logs are notified to the administrator were performed	Y	N	Y
{@ERR}	Errors that have occurred	N	Y	N

2. Enter the required setting items and click the **Set** button.

E-mail notification format

Format of notifying events occurred in the client (CT) and database to administrator by E-mail is as follows:

When using a dual stack client (CT), only IPv4 addresses are displayed in the device column.

Item Name	Format
E-mail Title	Systemwalker Desktop Keeper WARNING Report at **yyyy/mm/dd hh:mm:ss** Note: If the email title parameter still contains the initial value.

Text (Subject)	When prohibition log is detected
	
	    Operation category:
	    Management server:
	    User name:
	    Terminal:
	    CT version:
	    Operation date:
	    Details:
	
	When database is abnormal
	
	    Error contents:
	    Management server:
	    Occurrence date and time:
	    Details:

Item Name	Format

	When MAC address is changed
	
	   Operation category:
	   Management server:
	   User name:
	   Terminal:
	   CT version:
	   Operation log:
	   Details:
	   -MAC Address
	   Before modification: [ ]
	   After modification: [ ]
	
	   -Computer Name
	   Before modification: [ ]
	   After modification: [ ]
	
	   -IP Address
	   Before modification: [ ]
	   After modification: [ ]

Event log display format

This describes the format of the event occurred in the client (CT) and database displayed in the event viewer of Windows.

The notified information is displayed in "Application Log" of the event log of Windows. When using a dual stack client (CT), only IPv4 addresses are displayed in the device column. The displayed contents are describes as follows:

Item Name	Description
Category	[Warning] will be displayed.
Date	Date of notification information displayed in event viewer.
Time	Time of notification information displayed in event viewer.
User	User ID.
Computer Name	Computer name.
Source	[SWDTK] will be displayed.
Category	[None] will be displayed.

Event ID	The following serial numbers will be displayed.
	
	When prohibition log is detected
	
	   8001: Application startup prohibition
	
	   8002: Printing prohibition
	
	   8003: Logon prohibition
	
	   8004: PrintScreen key is pressed.
	
	   8005: Linkage application
	
	   8006: E-mail attachment prohibition
	
	   8010: Device configuration change
	
	   8012: URL access prohibition
	
	   8013: FTP server connection prohibition
	
	   8014: Web upload prohibition

Item Name	Description
	8015: Web download prohibition
	8017: Clipboard operation prohibition
	Monitoring action of client (**CT**)
	8007: Client (CT) terminal time inconsistent
	8008: MAC address changed
	8011: Client (CT) that is collecting trace
	When database is abnormal
	3006: Database space is insufficient
	3007: Disk space of attached data saving folder is insufficient
	3008: Disk space of command log folder is insufficient
	3009: Disk space of collective log sending folders is insufficient
	3010: Disk space of trace log folder is insufficient
	3015: Disk space of E-mail contents saving target is insufficient
	3016: Disk space of trouble investigation data saving target is insufficient.
	3019: Disk space of Database space is insufficient
	For details, refer to "Message Output with Event Log" in *Systemwalker Desktop Keeper Reference Manual*.
Explanations	The following information will be displayed.
	When prohibition log is detected
	Operation category: Management server: User name: Terminal: CT version: Operation date: Details:
	When database is abnormal
	Error contents: Management server: Occurrence date and time: Details:
	When MAC address is changed
	Operation category: Management server: User name: Terminal: CT version: Operation log: Details: -MAC Address Before modification: [ ] After modification: [ ] -Computer Name Before modification: [ ] After modification: [ ]

Item Name	Description
	-IP Address Before modification: [ ] After modification: [ ]

2.3.6.9 Set Saving Target Folder

Set all kinds of folders in the Systemwalker Desktop Keeper Management Server.

The steps of setting the saving target folder are as follows:

1. Click the **Folder/CT self version upgrade settings** button in the menu of Sever Setting Tool.

   The **Folder/CT Self Version Upgrade Settings** window is displayed.

2. Confirm the initial value of saving target of the following information displayed in **Folder settings**. Click the **Browse** button to modify the saving target.

3. (It is not necessary to set **CT self-version upgrade settings** here. For the setting content, refer to "4.7 Upgrading the client (CT)".)

[Folder settings]

Item Name		Description

Command line and log saving target settings		The method to specify the saving target folder of command log in Management Server is as follows:
		
		- Enter folder name with full path.
		  Enter the path of saving target folder of command log with full path. Network drive cannot be specified.
		
		- Specify through the **Browse** button.
		  The **Browse For Folder** window will be displayed. Select the folder to save command log and click the **OK** button.
		
		The length of the full path that can be specified is no more than 96 single-byte characters (48 double-byte characters).
		The following symbols cannot be specified in the folder name: \ / : * ? " < > |

	Received data saving target	Specify the folder to save the data in operation.
	Target for log viewing	Specify the folder to save data for log viewing. Specify when creating the log viewing database and restoring operation logs.

Attached data saving target settings		Specify the saving target folder of additional data (screen capture data, original backup file, and clipboard operation original backup file) in the Management Server. The specification method is as follows:
		
		- Enter folder name with full path.
		  Enter the path of saving target folder of attached data with full path. Network drive cannot be specified.
		
		- Specify through the **Browse** button.
		  The **Browse For Folder** window will be displayed. Select the folder to save command log and click the **OK** button.
		
		- The length of the full path that can be specified is no more than 96 single-byte characters (48 double-byte characters).
		  The following symbols cannot be specified in the folder name: \ / : * ? " < > |

	Received data saving target	Specify the folder to save the data in operation.
	Target for log viewing	Specify the folder to save data for log viewing. Specify when creating the log viewing database and restoring operation logs.

Collectively receiving log and data saving target settings		Specify the saving target folder of collective log data in the Management Server. The specification method is as follows:
		
		- Enter folder name with full path.
		  Enter the path of saving target folder of collective log data with full path. Network drive cannot be specified.
		
		- Specify through the **Browse** button.
		  The **View Folder** window will be displayed. Select the folder to save command log and click the **OK** button.
		
		The length of the full path that can be specified is no more than 96 single-byte characters (48 double-byte characters).
		The following symbols cannot be specified in the folder name: \ / : * ? " < > |

Item Name		Description

E-mail content saving target settings		Specify the saving target folder of E-mail contents data (E-mail text and attachment) in the Management Server. The specification method is as follows:
		
		- Enter folder name with full path.
		  Enter the path of saving target folder of E-mail contents data with full path. Network drive cannot be specified.
		
		- Specify through the **Browse** button.
		  The **Browse For Folder** window will be displayed. Select the folder to save command log and click the **OK** button.
		
		The length of the full path that can be specified is no more than 96 single-byte characters (48 double-byte characters).
		The following symbols cannot be specified in the folder name: \ / : * ? " < > |

	Received data saving target	Specify the folder to save the data in operation.
	Target for log viewing	Specify the folder to save data for log viewing. Specify when creating the log viewing database and restoring operation logs.

Failure investigation data saving target settings		Specify the saving target folder of QSS (Trouble Investigation Data) collected remotely in the Management Server. The specification method is as follows:
		
		- Enter folder name with full path.
		  Enter the path of saving target folder of trouble investigation data with full path. Network drive cannot be specified.
		
		- Specify through the **Browse** button.
		  The **Browse For Folder** window will be displayed. Select the folder to save command log and click the **OK** button.
		
		The length of the full path that can be specified is no more than 96 single-byte characters (48 double-byte characters).
		The following symbols cannot be specified in the folder name: \ / : * ? " < > |

2.4 Install Management Console

This section describes how to newly install Systemwalker Desktop Keeper Management Console.

If the Management Server was installed for the first time, the Management Console will have been installed already, so this task is not required.

If the Management Console of an old version has been installed, refer to "Chapter 4 Upgrading" when installing the Management Console of V15.1.0.

Items to be confirmed before installation

- Refer to the "Port Number List" in *Systemwalker Desktop Keeper Reference Manual* to confirm the port number being used.

- When setting the (Master) Management Server to be connected, ensure the existence of the computer name being specified.

- When the Management Server is installed for the first time, the Management Console will also be installed.
  In this case, the port number **10015** and IP address **localhost** will be set for the connection destination.

Installation

Installation steps for the Management Console are as follows. In addition, refer to *Systemwalker Desktop Keeper User's Guide* for the operating environment.

1. Log in Windows with the user that belongs to the Administrators group or the user that belongs to the Domain Admins group.

2. After the DVD-ROM of Systemwalker Desktop Keeper is inserted into the PC, the installer window will be displayed:

   Select **Management Console Installation**.

   If the installer window is not started, start the "swsetup.exe" in the DVD-ROM drive.

3. After the window "Welcome to Systemwalker Desktop Keeper Management Console Setup" is displayed, click the **Next** button.

4. The **Select the installation target** window will be displayed.

   If the displayed installation target is not to be changed, click the **Next** button.

   If the displayed installation target is to be changed, click the **Browse** button of the folder to be changed, and click the **Next** button after the folder has been changed.

   ## Note
   ....

   If the installation folder of the Management Console is targeted for compression or encryption, this may impact on program operation. Do not configure compression or encryption settings.

   Specify up to 96 halfwidth characters for the **Installation Target Folder**. You cannot specify the following drives:

   - Network drive

   - Non-NTFS drive

   It cannot contain commas (,), semicolons (;) , number signs (#) or halfwidth kana characters.
   ....

5. The **Enter server information** window will be displayed. Set the information of server to be connected and click the **Next** button.

   The procedure of setting the server to be connected is as follows.

   a. Set the following information as the information of server to be connected and click the **Add** button.

      ## Note
      ....

      Confirm the setting of the (Master) Management Server to be connected.

      Set the information of the (Master) Management Server to be connected to be the same as the setting in the Management Console. The confirmation method is as follows:

      1. Start **Systemwalker Desktop Keeper** > **Server** > **Sever Settings Tool** from the **Start/Apps** on the connected (Master) Management Server.

      2. Click the **Management Server Settings** button.

      3. Confirm the following items:

         - Configuration value of **IP address of server** of **Server settings**;

         - Configuration value of **Management Console <---->Level Control Service** of the **Port number settings**.
      ....

      - **Computer name or IP address of connected (Master) Management Server**
        Enter the computer name or IP address of the connected (Master) Management Server.
        When entering the computer name, confirm the correctness of the name. If the name cannot be analyzed correctly, the (Master) Management Server and Management Console cannot be connected.
        IPv4 and IPv6 addresses can be specified. However, do not specify a link-local address, otherwise behavior is not guaranteed.
        The value set here will be displayed as the alternative selection of **Connection Target Server Name** in the login window of the Management Console.
        Note: IPv6 addresses can be abbreviated using RFC 5952-compliant format.

      - **Port number being used**
        Enter the port number used for communication between the Management Console and level control service.
        The number must be the same as the value set for **Management Console** <----> **Level Control Service** in **Port number**

> **settings**.
>
> After being added, the set information will be displayed under the **Add** button.

> b. If there are multiple servers being connected, perform the operation in Step a. according to the number of servers.
>
> In addition, move up or down the servers that are often connected using the **Up** or **Down** buttons.

6. The **Complete installation preparation** window will be displayed.

   When starting the installation, click the **Install** button to start installation.

   When confirming the set content or wishing to modify it, click the **Return** button to reset.

7. The message below will be displayed. Click **OK** and continue with the installation process.

```
Upon completion, a window informing that the installation completed successfully will be
displayed.
Installation will continue until the window is displayed, so wait until completion.
```

8. The message below will be displayed. Click **Finish**.

```
The installation of Systemwalker Desktop Keeper management console was completed.
```

9. Upon successful completion, the **Confirm** window will be displayed.
   To use the program, click **Yes**. The operating system will restart.

🔆 Note

··

It is required to register the administrator information when using the Management Console.

When using the Management Console, the Sever Setting Tool should be used to register administrator information. Refer to "2.3.6.6 Set Administrator Information" for details on registration of administrator information.

During installation of the Management Console, only the background of the installer may be displayed continuously for several minutes.

It is normal for the installer processing to take time due to the device load or exclusive status, so do not forcibly terminate it. However, if a forced restart is performed, complete the installation by performing an overwrite installation.

Set the following on PCs that use the Management Console so as to prevent improper operations.

- A password for use of the Management Console

- A password-enabled screensaver. (Recommended value: Up to 10 mins)

··

2.5 Settings of PC with Web Browser Installed

In Systemwalker Desktop Keeper, use a Web browser to perform log viewing and analysis.

Set the security level of Internet Explorer according to needs of the PC that uses the Web browser.

If the security level of the zone to which site (URL) of Web browser belongs is higher than the following levels, it will not be able to run normally:

- "Medium High" in Microsoft(R) Internet Explorer(R) 7

- "Medium High" in Microsoft(R) Internet Explorer(R) 8

- "Medium High" in Microsoft(R) Internet Explorer(R) 9

- "Medium High" in Microsoft(R) Internet Explorer(R) 10

- "Medium High" in Microsoft(R) Internet Explorer(R) 11

When it is impossible to run normally due to the above reasons, the site (URL) of Web browser should be adjusted to the zone with lower security level than the above, or the security level of the current zone should be reduced.

Normally, because the zones of "Intranet" or "Trusted Sites" are in the security levels by default, it is suggested to register the site (URL) of Web browser to **Site** of any zone.

In addition, when Web browser is displayed, the current zone ("Intranet", "Internet" and etc.) will be displayed at the bottom right of the browser.

In Microsoft(R) Internet Explorer(R) 8

> Before logon to the Web console, change (add or delete) the registration status of "Trusted Site" of the site (URL) of Web console. If this operation is performed during the logon process, operations such as logout may be unable to perform.

Note

. . . .
The "HTTPS" setting is recommended for using the Web Console and Log Viewer. Configure this using the IIS web browser.
. . . .

About settings of Internet Explorer(R) in 64-bit OS

In 64-bit OS, use the 32-bit Internet Explorer(R) as Web browser.

Setting when file is not downloaded successfully

There are several types of file download operations:

- File download in the CSV export function after log searching, file tracing and search of configuration change log;

- File download in the function of "Command Log Content Downloading";

- File download in the function of "Attached Data of File Export Log";

- Download through file saving from the image display window.

If the downloading operation of the above files has been executed, after entering the file name of the saving target, the [~ copied] window will be displayed continuously, and download will take some time. Sometimes, the downloading may not be finished.

At that time, modify the following settings:

When using Windows(R) Internet Explorer(R) 8

> Register the site of Systemwalker Desktop Keeper to trusted sites, and prohibit the **SmartScreen Filter Function** of Internet Explorer(R).
> In addition, through this setting, **SmartScreen Filter Function** will be prohibited in all the sites registered to trusted sites.

> 1. Start Log Viewer and display the **Login** window.
>   Perform the following settings when the **Login** window is displayed. For information on how to start Log Viewer, refer to "Start Log Viewer" in *Systemwalker Desktop Keeper User's Guide for Administrator*.

> 2. Select **Tool** > **Internet Options** from the menu of Internet Explorer(R). The **Internet Options** window will be displayed.

> 3. Open the **Security** tab, click **Trusted Sites** icon and click the **Sites** Button. **Trusted Sites** window will be displayed.

> 4. Confirm the site (URL) of Systemwalker Desktop Keeper that has already been set in **Add this website to zone**, and click the **Add** button.

> 5. Click the **Close** button in **Trusted Sites** window to close the window.

> 6. Select **Trusted Sites** icon in **Internet Options**, and click **User-defined Level**.

> 7. Select **Others** > **Use SmartScreen Filter Function** in the settings of the **Security Settings** > **Trusted Zone** window, and click the **Disable** button.

> 8. Click the **OK** button in the **Security Settings** > **Trusted Zone** window to close it.

> 9. Click the **OK** button in the **Internet Options** window to close it.

Settings for linking with Systemwalker Desktop Patrol

To link with Systemwalker Desktop Patrol and use Windows(R) Internet Explorer(R) 8 or higher, configure the following settings:

1. On Internet Explorer(R), click **Tools** > **Internet options**, and select the **Security** tab.

2. Select the zone to which the Systemwalker Desktop Keeper and Systemwalker Desktop Patrol sites (URLs) belong, and click **Custom level** to open the **Security Settings** window.

3. In **Settings**, select **Miscellaneous** > **Navigate windows and frames across different domains** > **Enable**.

4. In the **Security Settings** window, click **OK**.

5. In the **Security** tab, click **Apply** or **OK**.

2.6 Install the Client (CT)

This section describes how to newly install the client (CT) of Systemwalker Desktop Keeper.

The installation method of the client (CT) of Systemwalker Desktop Keeper is as follows. For an overview, refer to "1.2.5 Determine How to Install Client (CT)".

- Single installation

    - Wizard-style installation

    - Silent installation

- Installation using master PC/master virtual PC

- Installation using the distribution function of Systemwalker Desktop Patrol

- Installation using Active Directory Group Policy

If the old version of the client (CT) has been installed, refer to "Chapter 4 Upgrading" when installing the client (CT) V15.1.0.

Note

When installing the client (CT) on Management (Master Management) Server

When installing the client (CT) on a Management Server, pay attention to the following two points:

- Installation sequence

- Server to be connected

For details, refer to "When a client (CT) is installed on Management Server/Master Management Server".

When unable to confirm the installed client (CT) through Management Console

When unable to confirm the installed client (CT) through the Management Console, the following reasons can be taken into consideration:

- IP address of the Management Server specified during client (CT) installation is incorrect.

- Port number specified during client (CT) installation is different from the configuration value of the Management Server.

- Due to reasons such as the router, the port used between the client (CT) and the Management Server has been blocked.

Network has been disconnected in the installation process of the client (CT)

The network will be temporarily disconnected during the installation of the client (CT). If the network folder is opened by Windows Explorer, close it.

Notes on installing a client (CT) on Windows(R) 8, Windows(R) 10

If you have upgraded a client (CT) and clicked **No, restart the computer later** in the **Installation Complete** window, you must restart the operating system.

Even clicking **Shut Down** (operation for shut down and power on a system) to shut down the operating system does not apply the client (CT) feature.

Do not forget your password

When uninstalling the client (CT), you will need the password that you used during its installation.

Write down the password in case you forget it.

Verification when registering client (CT) devices

When performing verification during client (CT) device registration, the password to be entered during installation must be the same as the client management password specified in the **Terminal Operation Settings** window of the Management Console.

Refer to "Perform Terminal Operation Settings" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on setting a client management password in the Management Console.

 Point

Installation in Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10 and Windows Server(R) 2012

The following information will be output in the event log during installation.

```
Event log content
Source : Service Control Manager Eventlog Provider
Time ID: 7030
Level: Error
Content: The SWServerService service is marked as an interactive service.
        However, the system is configured to not allow interactive services.
        This service may not function properly.
```

This message is displayed because the OS does not recommend interactive service, but it will not affect the operation.

2.6.1 Single Installation

There are two methods for a single installation of a client (CT).

Wizard-style installation

Installation of wizard style is carried out in interactive mode. Refer to "2.6.1.1 Wizard-style Installation".

Silent installation

Automatic installation can be used for silent installation according to the prepared installation setting files. Refer to "2.6.1.2 Perform Silent Installation" for details.

2.6.1.1 Wizard-style Installation

 Note

If a user whose user name contains fullwidth characters installs a client (CT), an error message may be displayed.

When installing a client (CT), use a user name that contains halfwidth characters only.

This section describes how to newly install a client (CT) of Systemwalker Desktop Keeper in wizard style.

Items to be confirmed before installation

- Refer to "Port Number List" in the *Systemwalker Desktop Keeper Reference Manual* to confirm the port number being used.

Installation

The steps to install a client (CT) in wizard style are as follows. In addition, for operating environment, refer to *Systemwalker Desktop Keeper User's Guide*.

1. Log in to Windows with the user that belongs to the Administrators group or the user that belongs to the Domain Admins group. When other applications are being used, close them.

2. After the DVD-ROM of Systemwalker Desktop Keeper is inserted into the PC, the installer window will be displayed:

   Select **CT (Client) Installation**.
   If the installer is not started, start the "swsetup.exe" in the DVD-ROM drive.

3. After the "Welcome to use Systemwalker Desktop Keeper Client installation" window is displayed, click the **Next** button.

4. The "Select the installation target" window of CT (client) will be displayed. If the installation target displayed is not to be changed, click the **Next** button.

   If the installation target displayed is to be changed, click the **Browse** button of the folder expected to be changed, and click the **Next** button after the folder has been changed.

📑 Note
. . . .

Exclude compressed and encrypted targets

When the installation target folder of the CT (client) and the installation target folder of the following log files are taken as compressed or encrypted targets, the running of program may be affected. Therefore, do not turn on the compression or encryption settings.
. . . .

5. The "Select the installation target" window of the log saving target to be set will be displayed. When the displayed saving target is not to be changed, click the **Next** button.

   When the displayed saving target is to be changed, click the **Browse** button of the folder expected to be changed, and click the **Next** button after the folder has been changed.

   Set folder under Windows system disk in the folder path for saving log files. (When the OS is installed to the C Drive, the C Drive will be the system disk.)

📑 Note
. . . .

Do not specify the drive with export prohibition

Because logs may be lost, do not specify the drive with export prohibition in the saving target of the log file.
. . . .

6. Since the **Enter the server information** window is displayed, set the information of server to be connected and click the **Next** button.

- **IP Address of Connected (Master) Management Server:** enter the IP address or server name of the (master) Management Server to be connected.

  When installing a client (CT) on the Management Server/Master Management Server, it is not required to specify **IP Address of Connected (Master) Management Server**. (127.0.0.1 (IPV4),::1(IPv6),127.0.0.1(IPv4/IPv6) is displayed in IP address, unable to enter).

  IPv4 and IPv6 addresses can be specified. However, do not specify a link-local address, otherwise behavior is not guaranteed.

  The IP address or server name must meet the following conditions:

  - The server name can contain up to 15 halfwidth alphanumeric characters, hyphens (-), and underscores (_).

  - The IPV4 IP address can contain up to 15 halfwidth numbers and periods (.).

  - The IP address (IPv6) can contain up to 39 halfwidth letters (A-F, a-f), numbers, and colons (:).

  - The server name and IP addresses cannot contain only numbers

- **IP Address of Backup Management Server:** when the (Master) Management Server to be 127.0.0.1is abnormal, enter the IP address or computer name of the backup Management Server for inquiring user policy.

  IP address of a backup Management Server can be omitted. In addition, the function is effective when all the following conditions are satisfied: IPv4 and IPv6 addresses can be specified. However, do not specify a link-local address, otherwise behavior is not guaranteed.

  - The Management Server is in a 3-level structure.

  - Users are managed collectively

  - Action of the client (CT) is controlled through user policy.

  Selection points of the backup Management Server are as follows:

  - In case of the client (CT) connecting to the Master Management Server

    Specify any lower-level Management Server.

  - In case of the client (CT) connecting to the Management Server

    Specify the Master Management Server.

  The IP address or server name must meet the following conditions:

  - The server name can contain up to 15 characters

  - The IP address (IPv4) can contain up to 15 characters

  - The IP address (IPv6) can contain up to 39 characters

  - The IP address (IPv4) can contain halfwidth numbers (0-9) and halfwidth periods (.)

  - The IP address (IPv6) can contain halfwidth alphanumeric characters (A-F, a-f, 0-9) and halfwidth colons (:)

  - The server name can contain halfwidth alphanumeric characters (A-Z, a-z, 0-9), halfwidth hyphens (-), and underscores (_).

  - The server name and IP addresses cannot contain only numbers.

- **Used Port Number (for Receiving):** enter the port number (for receiving at CT side) used for communication between the client (CT) and server service.
  Enter a value from 5001 to 60000.

- **Used Port Number (for Sending):** enter the port number used for communication between the client (CT) and server service (for sending logs immediately at CT side).
  Enter a value from 5001 to 60000.
  When entering the following items, ensure that they are not duplicated:

  - **Used Port Number (for Sending)**

  - **Used Port Number (for Sending 2)**

- **Used Port Number (for Sending 2):** enter the port number used for communication between the client (CT) and server service (for sending logs collectively at the client (CT) side).
  Enter a value from 5001 to 60000.
  When entering the following items, ensure that they are not duplicated:

  - **Used Port number (for Sending)**

  - **Used Port Number (for Sending 2)**

See

It is necessary to be able to resolve the host name of the Management Server or Master Management on each machine. Otherwise, communication will not be possible between the Management Server or Master Management Server and the client (CT).

7. The **Set printing monitoring mode** window is displayed. Select any option for printing monitoring mode and click the **Next** button.

   - **Monitoring the printing of all printers set in this terminal (Recommended):** Select when collecting a printing operation log at each client (CT). In this case, the printing operation log will be collected on each client (CT).

   - **Monitoring the printing of local printer only:**
     Select when the printing in the client (CT) under the same Master Management Server or Management Server as the printer server is performed through the printer server. The client (CT) should also be installed on the printer server as well. In this case, printing operation log cannot be collected through the client (CT) that is not the printer server. The printing operation log will be collected through the printer server.

Note

Notes for printing monitoring mode

Unify in Master Management Server and Management Server

Unify the above selection on the client (CT) of the Master Management Server or the Management Server. If it is not unified, the printing operation log may not be collected.

Setting when Installing Printer Server on Non-Server OS

If the non-server OS (Windows Server(R) 2008 or Windows Server(R) 2012) is taken as the printer server and set to **Monitoring the Printing of All Printers Set in this Terminal (Recommended)**, no more than 10 clients can be connected to the printer server to print. At this time, set to **Monitoring Printing of Local Printer Only**.

Point

Register user ID on printer server

When "Monitoring Printing of Local Printer Only" is selected on the printer server before installing the client (CT), it is required to register the User ID used in the client (CT) that performs printing on the printer server. If it is not registered, the user ID of the printing log will be output as follows.

- In the client (CT) that performs printing, when user authority is set for only the user ID being used, the **User ID** of the log will be collected as **Guest**.

- When it is required to log on the printer server as Administrator, the **User ID** of the log will be collected as **Administrator**.

8. The **Set E-mail Control Mode** window will be displayed. Set the mode of E-mail attachment prohibited and click the **Next** button.

- - **Port Number for E-mail Sending and Monitoring:** When port monitoring mode is selected, enter the port number used for communication between client (CT) and SMTP server.
    Specify a value from 0 to 65535.
    The specified value cannot match the value of any of the settings below:

    - - **Used Port Number (for Receiving)**

    - - **Used Port Number (for Sending)**

    - - **Used Port Number (for Sending 2)**

    - - **Port Number for E-mail Sending and Monitoring**

    - - **Port Number for E-mail Attachment Prohibition**

    - - **Port Number 2 for E-mail Attachment Prohibition**

  - **Port Monitoring Mode (Recommended):** Select when using the prohibition function through the drive for E-mail file attachment prohibition. Normally, take this setting as default.
    When updating from a version before V13.0.0, select the E-mail file attachment prohibition under port monitoring mode before setting the same prohibition action as before V13.0.0.

    - - **Port Number for E-mail Attachment Prohibition:** When port monitoring mode is selected, enter the port number used internally in the E-mail attachment prohibition processing.
        Specify a value from 0 to 65535.
        The specified value cannot match the value of any of the settings below:
        - **Used Port Number (for Receiving)**
        - **Used Port Number (for Sending)**
        - **Used Port Number (for Sending 2)**
        - **Port Number for E-mail Sending and Monitoring**
        - **Port Number for E-mail Attachment Prohibition**
        - **Port Number 2 for E-mail Attachment Prohibition**

    - - **Port Number 2 for E-mail Attachment Prohibition:** When port monitoring mode is selected, enter the port number used internally in the E-mail attachment prohibition processing.
        Specify a value from 0 to 65535.
        The specified value cannot match the value of any of the settings below:

- **Used Port Number (for Receiving)**
- **Used Port number (for Sending)**
- **Used Port Number (for Sending 2)**
- **Port Number for E-mail Sending and Monitoring**
- **Port Number for E-mail Attachment Prohibition**
- **Port Number 2 for E-mail Attachment Prohibition**

- **V12.0L20 - V13.0.0 Compatible Mode:** Select when using the prohibition function based on any mode before V13.0.0. In the version upgrade starting from the version before V13.0.0, it is only required to be specified when the same prohibition action is needed.

📝 Note

Notes for setting E-mail attachment prohibition mode

In Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 , Windows(R) 10 or Windows Server(R) 2012

In Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10, or Windows Server(R) 2012, only port monitoring mode can be selected as the mode for E-mail file attachment prohibition.

Confirm if Port is Not Used

For port of E-mail attachment prohibition, specify the port not used in other processing or during communication.

9. The "Creation Settings of File Exporting Utility Icon" window is displayed. Set whether to create the icon of file export utility and click the **Next** button.

- **Create in [Desktop]:** Select when creating the file export utility icon.

- **Create in the [Send to] Menu:** select when creating the file export utility icon in the **Send to** menu.

10. When the "Enter the password" window is displayed, set the password for displaying the client status and modifying the utility, and click the **Next** button.

The password set here is required when executing the uninstallation and maintenance commands of the client (CT). The conditions for contents to be entered are as follows:

- Up to 32 bytes of single-byte alphanumeric characters as well as contents apart from the following symbols can be entered

- The following symbols cannot be specified: & < > | \ " ~ ' ? : ^

- Double-byte or single-byte space is not allowed.

- Single-byte Kana are not allowed.

📝 Note

Do not forget password

This password is required when executing the uninstallation and maintenance commands of the client (CT). Pay attention to that if the password is forgotten, the uninstallation and maintenance commands will be unable to be executed.

Verification when registering client (CT) devices

When performing verification during client (CT) device registration, the password to be specified during installation must be the same as the client management password specified in the **Terminal Operation Settings** window of Management Console.

11. The "The installation preparation is completed." window is displayed.

When installation is started, click the **Install** button to start the installation.

When it is expected to confirm or modify the setting, click the **Return** button to reset.

12. After the processing has completed normally, the "Installation is completed." window will be displayed.

It is necessary to restart the operating system to use the program. Select either of the following items and click the **Finish** button.

- [Yes, restart the computer immediately.]

- [No, restart the computer later.]

2.6.1.2 Perform Silent Installation

🍜 Note

. . . .

If a user whose user name contains fullwidth characters installs a client (CT), an error message may be displayed.

When installing a client (CT), use a user name that contains halfwidth characters only.

. . . .

Create installation settings file

Create the installation settings file (InstConf.ini) to be used in a silent installation of the client (CT) using the Sever Setting Tool.

In addition, this procedure should be followed when performing silent installation if version upgrade is performed using the self version management function.

The creation procedure is as follows:

1. Select **Systemwalker Desktop Keeper** > **Server** > **Sever Settings Tool** from the **Start**/**Apps** menu and log on.

2. Click the **Create CT Silent Installation Files** button.

The following window will be displayed.

3. Enter the following information and click the **Start to output** button.

Setting Item	Value
Server IP address or server name(CT Management Server)	IP address or server name of the Management Server or Master Management Server that you will connect to. - If a server name is specified: - Specify up to 15 halfwidth characters.

Setting Item	Value
	- It can contain halfwidth alphanumeric characters (A-Z, a-z, 0-9) and halfwidth hyphens (-).
	- It cannot contain only numbers.
	- If an IPv4 address is specified:
	- Specify up to 15 halfwidth characters.
	- It can contain halfwidth numbers (0-9) and halfwidth periods (.).
	- A loopback address (127.0.0.1) cannot be specified.
	- If an IPv6 address is specified:
	- Specify up to 39 halfwidth characters.
	- It can contain halfwidth alphanumeric characters (A-F, a-f, 0-9) and halfwidth colons (:).
	- A loopback address (::1) cannot be specified.
	- Do not specify a link-local address, otherwise behavior is not guaranteed.
	Note: It is necessary to be able to resolve the host name of the Management Server or Master Management on each machine. Otherwise, communication will not be possible between the Management Server or Master Management Server and the client (CT).
Server IP address or server name(backup Management Server)	When the connected (Master) Management Server is abnormal, enter the IP address or server name of the backup Management Server for inquiring user policy. Under initial status, the same value as **Server IP Address (CT Management Server)** will be displayed. Modify if necessary.
	The function will be effective all the following conditions are satisfied.
	- The Management Server is in a 3-level structure
	- Users are managed collectively
	- The actions of the client (CT) are controlled by user policy
	If the conditions are not applicable, set the same value as **Server IP Address (CT Management Server)**.
	If a server name is specified:
	- Specify up to 15 halfwidth characters.
	- It can contain halfwidth alphanumeric characters (A-Z, a-z, 0-9) and halfwidth hyphens (-).
	- It cannot contain only numbers cannot.
	If an IPv4 address is specified:
	- Specify up to 15 halfwidth characters can be entered.
	- It can contain halfwidth numbers (0-9) and halfwidth periods (.).
	- A loopback address (127.0.0.1) cannot be specified.
	If an IPv6 address is specified:
	- Specify up to 39 halfwidth characters.
	- It can contain halfwidth alphanumeric characters (A-F, a-f, 0-9) and halfwidth colons (:).
	- A loopback address (::1) cannot be specified.

Setting Item		Value
		- Do not specify a link-local address, otherwise behavior is not guaranteed.
		Note: IPv6 addresses can be abbreviated using RFC 5952-compliant format.
		Note: It is necessary to be able to resolve the host name of the Management Server or Master Management on each machine. Otherwise, communication will not be possible between the Management Server or Master Management Server and the client (CT).
Set port number	**Port number (for receiving)**	Enter the port number (for CT receiving) used for communication between client (CT) and server service. Enter a value from 5001 to 60000.
	Port number (for sending)	Enter the port number (for sending CT logs immediately) used for communication between client (CT) and server service. Enter a value from 5001 to 60000.
	Port number (for sending 2)	Enter the port number used (for sending CT logs collectively) for communication between client (CT) and server service. Enter a value from 5001 to 60000.
	Port number (for E-mail attachment prohibition)	When **E-mail Attachment Prohibited Function** is selected as **Port monitoring mode (Recommended)**, enter the port number used internally for E-mail attachment prohibition processing. When **E-mail Attachment Prohibited Function** is selected as **V12.0L20 - V13.0.0 Compatible Mode**, entering the port number is not required. Enter a value from 5001 to 60000.
	Port number (for E-mail attachment prohibition 2)	When **E-mail file attachment prohibition** is selected as **Port monitoring mode (Recommended)**, enter the port number used internally for E-mail attachment prohibition processing. When **E-mail file attachment prohibition** is selected as **V12.0L20 - V13.0.0 Compatible Mode**, entering the port number is not required. Enter a value from 5001 to 60000.
	Port number (for E-mail sending monitoring)	Enter the port number for the E-mail sending monitoring. Enter a value from 5001 to 60000.
Password (first entry)		Enter the password. Up to 32 bytes of single-byte alphanumeric characters as well as contents apart from the following symbols can be entered. The following symbols cannot be specified: & < > | \ " ~ ' ? : ^ Multi-byte or single-byte space is not allowed. 📒 **Note** . . . . **Do not forget password** This password is required during the execution of uninstallation and maintenance commands of the client (CT). Be aware that if the password is forgotten, the uninstallation and maintenance commands will be unable to be executed. **Verification when registering client (CT) devices** When performing verification during client (CT) device registration, the password to be specified during installation must be the same as the client management password specified in the **Terminal Operation Settings** window of Management Console. . . . .
Password (re-entry)		In order to avoid incorrect registration, re-enter the password.

Setting Item	Value
Log output target folder	Specify the folder under the Windows system disk as the folder to save the logs of the client (CT). When the OS is installed to the C Drive, the C Drive will become the system disk. The length of absolute path that can be specified is no more than 96 single-byte characters. However, the following symbols cannot be used as the folder name. The following symbols cannot be specified: \ / : * ? " < > | Environment variable can also be specified. Example: %ProgramFiles% ![Note] **Note** . . . . - Because the log may be lost, do not specify the drive with the export prohibition in the saving target of log file. - Because program operation might be affected, do not perform compression or encryption setting in the saving target of log file. . . . .

Reboot OS after specifying installation (*1)	Specify to restart OS after installation.
	
	Display the reboot confirming window
	
	  After installation has been implemented in the client (CT), the restart window will be displayed. This item is only effective when "Reboot by Force" is not selected. After "Reboot by Force" is selected, this button will be grayed out.
	
	  When this item is selected, restart will be performed automatically after the installation has completed.
	  Select either one from "Yes, restart the computer immediately.", or "No, restart the computer later".
	
	  If no item is selected, nothing will be displayed after the installation has completed. Whether to restart will be determined according to the **Restart by Force** setting of the following items.
	
	Force to reboot (It is valid only when the reboot confirming window is not displayed)
	
	  Select to restart by force after the installation of client (CT). The item is only effective when "Display Restart Confirmation Window" is not selected. If "Display Restart Confirmation Window" is selected, the button will be grayed out.
	
	  When this item has been selected, restart will be executed automatically after the installation has completed. When file is opened, the content will not be saved but directly completed, pay attention to that content might be lost.
	
	  If it is not selected, processing will be completed after the installation has completed. If "Display Restart Confirmation Window" is not selected, the restart confirmation window will not be displayed, and restart will not be executed automatically. Instead, user has to restart manually.

Installation target of client	Specify the path of the client (CT) installation folder. The absolute path length that can be specified is no more than 255 single-byte characters. However, the following symbols cannot be specified in the file name: \ / : * ? " < > | Environment variable can also be specified. For example: %ProgramFiles%

Setting Item	Value
	Note
	Exclude the compressed and encrypted targets
	Because the operation of program might be affected, do not enable compression or encryption settings in the client installation target.
Printing monitoring mode (*1)	Specify the monitoring mode of printing.
	Monitor printing of all printers set in the terminal (recommended):
	Specify when the printing operation log is selected at each client (CT). In this case, the printing operation log will be collected in each client (CT).
	Monitor printing of local printer only:
	Printing operation in the client (CT) that is in the same Management Server/ Master Management Server as the printer server will be selected through the printer server. The client (CT) should also be installed on the printer server. In this case, the printing operation log cannot be collected through the client (CT) that is not the one of printer server. The printing operation log will be collected through the printer server.
	Note
	- Unify the printing monitoring mode in the client (CT) under the Management Server/Master Management Server. If unification is not achieved, printing operation logs may not be collected
	- If the OS that is not of server type (Windows Server(R) 2008 or Windows Server(R) 2012) is used as the printer server, and the setting is **Monitoring the Printing of All Printers Set in this Terminal (Recommended)**, the printer server cannot connect with more than 10 clients for printing. At this time, set to **Monitoring the Printing of Local Printer Only**.
E-mail attachment prohibition (*1)	Specify the E-mail attachment prohibited function.
	Port monitoring mode (recommended):
	Port monitoring mode based on drivers. This setting is specified as default.
	V12.0L20~V13.0.0 compatible mode
	It is the E-mail attachment prohibition mode in the previous version. When the version is updated, the setting should be performed when the prohibition is the same as the previous version.
Apply policy immediately after logging on Windows	Specify whether to apply user policy immediately after logon.
	User policy (under Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 , Windows(R) 10 or Windows Server(R) 2012 only)
	Apply user policy immediately after logon. (Initial value)
	It is always as CT policy (V12.0L20~V13.2.0 compatible format)
	Run with CT policy after logon.
Set the creation of File Export Tool icon (*1)	Specify whether to create icons of File Export Utility.
	Create on the [Desktop]
	Select when File Export Utility icons are created on desktop.

Setting Item	Value
	Create in the [Send to] menu
	Select when File Export Utility icons are created in the **Send to** menu.
Installation settings file	Specify the saving target of silent installation setting file (InstConf.ini). The specification method is as follows:
	- Enter file name with absolute path. Enter the path of silent installation setting file with absolute path.
	- Select through the **View** button. The **Save As** window will be displayed. Select the folder to save silent installation setting file, and click the **Save** button after entering the file name.
	The absolute path length that can be specified is no more than 96 single-byte characters. The following symbols cannot be specified: \ / : * ? " < > |

🅿 Point

Items become effective when self version management function is used to perform version upgrade

When the self version management function is used to perform the version upgrade, the above 4 items with (*1) will be effective.

- **Printing monitoring mode**

- **E-mail attachment prohibition**

- **Reboot OS after specifying installation**

- **Set the creation of File Export Tool icon**

Other items will be omitted even if they have been set.

🅿 Point

Register user ID on printer server

When "Monitoring the printing of local printer only" is selected and the client (CT) is installed on the printer server, it is also necessary to register the user ID used in the printing client (CT) on the printer server. If it is not registered, the user ID for printing logs will be output as follows:

- When only setting user authority to the user ID being used in the printing client (CT), **User ID** of log will be collected as **Guest**.

- When it is required to log in printer server and register as Administrator at the time of printing, **User ID** of log will be collected as **Administrator**.

Perform silent installation

Before installation, refer to "Port Number List" in *Systemwalker Desktop Keeper Reference Manual* to confirm the port number being used.

When silent installation of a client (CT) is performed on a PC that has a CT installed, installation by overwriting will be performed. In this case, modify the IP address, port number and log saving target directory. In addition, even if the password used in initial installation is specified to be modified, the password will not be changed.

1. Logon to the PC as a user who belongs to the Administrators group of local computer or a user that belongs to the Domain Admins group of domain. When other applications are being used, close them.

2. Insert the setup disk into the drive.
Copy the silent installation settings file (InstConf.ini) for client (CT) created according to "Create installation settings file" to any drive or folder.

3. Select **Run** or start the command prompt.

4. Execute installation command (Setup.exe). The installation command is in the "win32\DTKClient" folder of setup disk.

   - Options are not case-sensitive.

   - If no option is specified, error message will be displayed and installation will be terminated.

   Specification Example

   Assume the following conditions.

      - Setup disk is inserted into D Drive.

      - The Setup.exe command is under D:\win32\DTKClient.

      - Installation settings file is in C:\Dtk.

   ```
   D:\win32\DTKClient\Setup.exe /Silent "C:\Dtk\InstConf.ini"
   ```

Note

When executing the command in Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8 , Windows(R) 10, or Windows Server(R) 2012, execute this command in the command prompt run by the administrator.

After the installation has completed, the CT silent installation file is generated and specified as "Display Dialog" and the window prompting restart of the operating system will be displayed.

5. The window prompting restart of the operating system will be displayed.
   Then, select one of the following items and click the **Finish** button.
   [Yes, restart the computer immediately.]: select to restart immediately.

6. **[No, restart the computer later.]**: select to restart later.

2.6.2 Installation Using Master PC/Virtual Master PC

Install to physical environment

The method of installation using a master PC in the physical environment is as follows. For an overview of the installation method, refer to "1.2.5 Determine How to Install Client (CT)".

1. Remove the LAN Cable of the PC being used as the master PC.
   Do not connect the LAN Cable before the following Step 3. is completed.

2. Install the client (CT).
   For installation method, refer to single installation "2.6.1.1 Wizard-style Installation" or "2.6.1.2 Perform Silent Installation".

3. Create the master image with image creation software.

4. Distribute images of the client (CT) to each PC to which the client (CT) is installed.

5. Start the PC where the client (CT) was distributed to, and confirm the content registered to the Management Server.

   (Next, execute when managing the terminal as master PC on the Systemwalker Desktop Keeper Management Server.)

6. Connect the LAN Cable of the master PC and restart Windows.

7. Confirm the content of the master PC registered to the Management Server.

Note

Notes for creating master PC

When creating the client (CT) image and installing the client (CT), it is necessary to install the client (CT) and create the image when the Management Server is not connected to network. (When creating the image and extracting to other PCs under the status that communication with Management Server has been performed only once, be aware that the PC will be registered to the server by mistake.)

In addition, be aware that the structures of image creation source terminal and decompression target terminal are the same. When installing the drive connected with a USB (such as the CD Drive) when creating the image, an error message will be displayed in the event log of the decompression target terminal.

Installation under virtual environment

The method to install a client (CT) in the virtual environment is as follows. For an overview of the installation method, refer to "1.2.5 Determine How to Install Client (CT)".

1. Install the client (CT) in the master image of the virtual environment.
   For installation method, refer to single installation "2.6.1.1 Wizard-style Installation" or "2.6.1.2 Perform Silent Installation".
   Make sure to restart after installation.

2. Log on to the master image of the virtual environment with administrator's authority.

3. Start the Management Console and confirm the client (CT) installed in the master image has been registered.

4. Start the command prompt in the master image of the virtual environment, and execute the following command.

```
fsw11ej7.exe [password] /image provisioning
```

5. Save the master image using the functions of the virtual environment.

2.6.3 Installation Using Systemwalker Desktop Patrol

The method to collectively install the clients (CT) of Systemwalker Desktop Keeper to the management target computer using the software distribution function of Systemwalker Desktop Patrol is as follows. For an overview of the installation method, refer to "1.2.5 Determine How to Install Client (CT)".

1. Create silent installation settings file using the Sever Setting Tool.
   For information on how to create, refer to "Create installation settings file".

2. Log on to the PC as a user that belongs to the Administrators group of local computer or a user that belongs to the Domain Admins group of domain. When other applications are being used, close them.

3. Insert the setup disk into the drive.

   Copy the silent installation settings file (InstConf.ini) for client (CT) created according to "Create installation settings file" to any drive or folder.

4. Copy the folder "win32\DTKClient" to any folder (Example: C:\work\dtkclient).

5. Copy the installation setting file (InstConf.ini) created in Step 1 to any folder created in Step 4 (Example: C:\work\dtkclient).

6. Create the batch file executed through the Contents distribution function of Systemwalker Desktop Patrol.
   The following example of batch is the situation when silent installation file is created as InstConf.ini. (Batch name: Setup.bat)

```
rem ******************************************************
rem * Systemwalker Desktop Keeper Contents Distribution Registration Batch *
rem ******************************************************
@ECHO OFF
SETLOCAL
rem acquire batch startup drive
SET STARTDRIVE=%~d0
rem acquire batch startup directory
SET STARTDIR=%~p0
rem create installation path
SET INSTALLDIR=%STARTDRIVE%%STARTDIR%
```

```
rem move the drive

%STARTDRIVE%

rem move the current directory

cd %INSTALLDIR%

rem execute silent installation

.\setup.exe /Silent "%INSTALLDIR%InstConf.ini"
```

7. Register Contents to Systemwalker Desktop Patrol so as to execute Setup.bat.
   For information on how to use the software distribution function of Systemwalker Desktop Patrol, refer to *Systemwalker Desktop Keeper User's Guide for Administrator*.

2.6.4 Installation using Active Directory Group Policy

Note

- -

- In this procedure, the client (CT) is extracted using the startup script for the Active Directory group policy so the client (CT) will be installed with the SYSTEM account.

- This procedure supports for new installations only.

- Execute this procedure as a user with administrator privileges.

- The installation script contains a non-encrypted password. It is the responsibility of the user to manage the installation script.

- -

Follow the procedure below to use the Active Directory group policy to install a Systemwalker Desktop Keeper client (CT) to the machine to be managed. Refer to "1.2.5 Determine How to Install Client (CT)" for an overview of the installation method.

1. Create an installation configuration file

2. Edit the installation script

3. Register the group policy

4. Check the installation results

5. Cancel the group policy

2.6.4.1 Create an Installation Configuration File

Create an installation configuration file. Refer to "Create installation settings file" for details.

Note

- -

- Create the installation configuration file with the default name "InstConf.ini".

- -

2.6.4.2 Edit the Installation Script

Edit the installation script in accordance with the environment.

File name

distributeDTKCT.bat

Character encoding

The character encoding used is Shift JIS.

Format

The sections to be edited are as follows.

```
set SHARE_DIR=uncPathForTheSharedFolderContainingSetupDotExe
set SHARE_ID=userIdToAccessFolderSpecifiedInShareDirEnvVar
set SHARE_PW=passwordOfUserIdSpecifiedInSharIdEnvVar
```

Parameters

The table below explains the values set for the installation script.

No.	Environment variable	Default value	Description
1	SHARE_DIR	None	UNC path for the shared folder containing Setup.exe (the command for installing clients (CTs)). This environment variable is required. This value will be used in "2.6.4.3 Register the Group Policy".
2	SHARE_ID	None	User ID used to access the folder specified in SHARE_DIR. Specify a user with write permission to the folder.
3	SHARE_PW	None	Password of the user specified in SHARE_ID.

Example

Example of edited installation script is shown below:

```
set SHARE_DIR=\\192.168.10.10\share
set SHARE_ID=user1@domain.local
set SHARE_PW=hogehoge1!
```

📝 **Note**

....

- If SHARE_ID and SHARE_PW are omitted, the local SYSTEM account will be used to access SHARE_DIR.

- If connection to SHARE_DIR using SHARE_ID and SHARE_PW fails, the local SYSTEM account will be used to access SHARE_DIR.

....

2.6.4.3 Register the Group Policy

This section explains how to register the group policy to the Active Directory.

It is recommended to register the group policy for a small number of users and perform extraction tests first.

If the domain controller runs Windows Server 2008 or Windows Server 2012

1. Click **Start** > **Administrative Tools** > **Group Policy Management**.

2. In the **Group Policy Management** window, click **Forest:** *domain* > **Domains** > *domain* > **Group Policy Objects**.

3. Create a Group Policy Object in the group where the computer on which the CT will be extracted exists.
   If you are using an existing GPO, there is no to create another one.

4. Right-click the GPO to be used, and click **Edit**.

5. In the **Group Policy Management Editor** window, click **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)**.
   In the right pane, click **Startup** and click **Properties**.

6. In the **Startup Properties** window, click **Add**.
   In the **Add a Script** dialog box, enter "distributeDTKCT.bat" in **Script Name**, and click **OK**.

7. Copy "distributeDTKCT.bat" to the folder displayed by selecting **Show Files**.

8. Copy the installation configuration file and Setup.exe (the command for installing clients (CTs)) to the folder specified for the SHARE_DIR environment variable in the installation script.
   Setup.exe is located in the win32\DTKClient folder of the setup disk.

9. In the **Startup Properties** dialog box, click **OK** to enable the settings.

10. In PCs where the group policy is applied, the CT will be automatically installed during startup.

Note

In PCs on which the CT is extracted, the operating system must be restarted after installation is completed.

2.6.4.4 Check the Installation Results

Use one of the following procedures to check if the CT extraction was completed normally..

- Use the Management Console to check if the PC to which the extracted client (CT) was installed is displayed.

- Check the installation script log output to the location below:

    - Folder

      If completed normally: *folderSpecifiedInShareDirEnvVar*\DTK\log\

      If did not complete normally: *folderSpecifiedInShareDirEnvVar*\DTK\log\error\

    - File

      yyyyMmDdHhMmSs.millisec_computerName.log (Example: 20140424120000.85_COMPUTER1.log)

If installation did not complete normally, refer to the installation result log and take appropriate action.

2.6.4.5 Cancel the Group Policy

Follow the procedure below to check if installation of the extracted client (CT) was completed successfully.

Once CT extraction is completed, cancel the group policy.

If the domain controller runs on Windows Server 2008 or Windows Server 2012

1. Click **Start** > **Administrative Tools** > **Group Policy Management**.

2. In the **Group Policy Management** window, click **Forest:** *domain* > **Domains** > *domain* > **Group Policy Objects**.

3. Right-click the GPO of the group in which the client (CT) is extracted, and click **Edit**.

4. In the **Group Policy Management Editor** window, click **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)**.
   In the right pane, right-click **Startup** and click **Properties**.

5. In the **Startup Properties** window, click "distributeDTKCT.bat" and click **Remove**.

6. Remove "distributeDTKCT.bat" from the folder displayed by clicking **Show Files**.

7. Delete the installation configuration file and Setup.exe (the command for installing clients (CTs)) from the folder specified for the SHARE_DIR environment variable in the installation script.

8. In the **Startup Properties** dialog box, click **OK** to enable the settings.

9. Remove the GPO selected in step 3.
   If the GPO is used for other purposes, it is not necessary to remove it.

2.7 Construct Log Analyzer Server

This section describes the installation and environment construction of Systemwalker Desktop Keeper Log Analyzer Server.

2.7.1 Install Log Analyzer Server

This chapter describes how to newly install Systemwalker Desktop Keeper Log Analyzer Server.

There are two ways to install the Log Analyzer Server:

- Installation using the wizard

- Silent installation

If installing the Log Analyzer Server of V15.1.0 or later when the Log Analyzer Server of Systemwalker Desktop Keeper V14.2.0 has already been installed, refer to "4.8 Upgrading the Log Analyzer Server and Report Output Tool" in "Chapter 4 Upgrading".

Note
....
If the Windows firewall is enabled in Windows Server(R) 2008, or Windows Server(R) 2012, the communication ports used by the Log Analyzer Server become unavailable, and you may no longer be able to connect from the web console or the Report Output Tool. Register the port number (the default number is 30004) used by the Log Analyzer Server as exceptions for the Windows firewall.
....

2.7.1.1 Items to be Confirmed Before Installation

- Refer to the "Operating Environment" in the *Systemwalker Desktop Keeper User's Guide* to confirm if the disk capacity required for the drive specified in installation target of database related file can be guaranteed.

- Refer to the "Operating Environment" in the *Systemwalker Desktop Keeper User's Guide* to confirm the "Products that cannot be used in mixture".

- Refer to "Port Number List" in *Systemwalker Desktop Keeper Reference Manual* to confirm the port number to be used.

  The following port will be taken as the default value in the Log Analyzer Server.

    - 30004: for report output tool and Log Analyzer.

- When copying the installer of Systemwalker Desktop Keeper from DVD-ROM to local disk, make sure that the path of the copy target does not contain double-byte characters.

- If the same version and level of the Log Analyzer Server is already been installed, it is not possible to perform an overwrite install (the installer will close without warning).

Note
....
About Log Analyzer user

The so-called "Log Analyzer User" is the Windows account used for database creation and data transfer on the Log Analyzer Server when the log analyzing function of Systemwalker Desktop Keeper is being used.

Before installation, confirm the conditions and authority standards that can be specified as the following Log Analyzer users.

- If a local account has been specified in Log Analyzer, execute the installation with the local account. In addition, if a domain account has been specified in the Log Analyzer, execute the installation with the domain account.

- When a domain account is specified as the Log Analyzer user, confirm that no local account with the same name exists.

- The following authorities should be set for the Windows account specified as the Log Analyzer user:

    - It belongs to the Administrator group if it is a local account, and Domain Admins group if it is a domain account;

    - Password without deadline has been set

- The following authorities will be granted to the Windows account specified as the Log Analyzer user automatically:

    - Logon as service;

- Function as part of the operating system

- Logon as batch job

2.7.1.2 Installation using the Wizard

The steps to install the Log Analyzer Server are as follows. In addition, for the operating environment, refer to *Systemwalker Desktop Keeper User's Guide*.

1. Log on to Windows with the user that belongs to the Administrators group or the user that belongs to the Domain Admins group. When other application is being used, close it.

2. After the DVD-ROM of Systemwalker Desktop Keeper is inserted into the PC, the installer window will be displayed:

   Select **Log Analyzer Server Installation**.

   If the installer is not started, start the "swsetup.exe" in the DVD-ROM drive.

3. After the "Welcome to Systemwalker Desktop Keeper Log Analyzer Server setup" window is displayed, click the **Next** button.

4. The **Required environment Information** window is displayed.

   If prior preparation displayed in the window has been implemented, click the **OK** button.

   If no prior preparation has been performed, click the **Cancel** button to pause the installation. After prior preparation displayed in the window has been implemented, execute the installation again.

5. The "Select installation target" window of the Log Analyzer Server is displayed.

   Confirm **Required capacity/ Available capacity** of **Installation target drive** displayed in the window.

   If the Installation target folder is not to be changed, click the **Next** button.

   If the Installation target folder is to be changed, click the **Browse** button of the folder expected to be changed, and click the **Next** button after the folder has been changed.

   Multi-byte characters such as space, Hiragana, Katakana and Chinese characters cannot be specified in the installation folder of the Log Analyzer Server. The following drives cannot be specified:

   - Root directory of drive (C:\, D:\, etc.)

   - Network drive

   - Non-NTFS drive

   The path cannot contain commas (,), semicolons (;), number signs (#) or halfwidth kana characters.

   ## Note

   Exclude compressed and encrypted targets

   When the installation target folder of the Log Analyzer Server function and the installation target folder of the following database related files are taken as compressed or encrypted targets, the application may be affected. Therefore, do not apply compression or encryption settings.

6. The "Select installation target" window of database-related files is displayed. (When the Symfoware Server is installed, this setting window will not be displayed. Continue with the following installation steps.)

   Confirm that **Required capacity/Available capacity** of **Installation target drive** is displayed in the window.

   If the Installation target folder is not to be changed, click the [Next] button.

   If the Installation target folder is to be changed, click the **Browse** button of the folder expected to be changed, and click **Next** after the folder has been changed.

   Multi-byte characters such as space, Hiragana, Katakana and Chinese characters cannot be specified in the installation folder of the database-related files. In addition, the following drives cannot be specified. Single-byte space cannot be specified either.

   - Root directory of drive (C:\, D:\, etc.)

- Network drive

- Non-NTFS drive

The path cannot contain commas (,), semicolons (;),number signs (#) or halfwidth kana characters.

📋 **Note**

. . . .

Specify the path of **Installation target folder** using up to 96 halfwidth characters.

. . . .

7. The "Enter the port number" window is displayed. Set the port number to be used by the Log Analyzer Server and click the **Next** button.

    When modifying the default value of port number, use an unused port number between 5001 and 60000. Non-digital character strings cannot be specified.

    - **Communication port 3:** for reporting output tool and Log Analyzer. The initial value is 30004.

8. The "Start Copying Files" window will be displayed.

    Confirm the set content. When starting installation, click the **Next** button, and installation will be started.

    When the settings are expected to be changed, click the **Back** to reset.

9. The message below will be displayed. Click **OK** and continue with the installation process.

```
Upon completion, a window informing that the installation completed successfully will be
displayed.
Installation will continue until the window is displayed, so wait until completion.
```

10. The message below will be displayed. Click **Finish**.

```
The installation of Systemwalker Desktop Keeper Log Analyzer Server was completed.
```

11. Upon successful completion, the confirmation window will be displayed.
    To use the program, click **Yes**. The operating system will restart.

2.7.1.3 Performing Silent Installation

📋 **Note**

. . . .

- Silent Installation of the Log Analyzer Server can only be performed when you are performing installation for the first time.

- Installation process must not be interrupted during silent installation.

- Define a non-encrypted password in the installation parameter CSV file.
  It is the responsibility of the user to manage the installation parameter CSV file. After silent installation is completed, delete the installation parameter CSV file created.

. . . .

Follow the procedure below to perform silent installation of the Log Analyzer Server:

1. Create an installation parameter CSV file.
   Refer to "A.2.1 Installation Parameter CSV File" for details.

2. Use the parameter setup command and installation parameter CSV file created in step 1 to create a response file.
   Refer to "A.2.2 Parameter Setup Command" for details.

3. Use the silent installation script and response file created in step 2 to perform silent installation.
   Refer to "A.2.4 Silent Installation Script" for details.

4. Check the installation result.
   Check the returned value and message from the silent installation script.

2.7.2 Construct Database

This section describes how to newly construct a database of Systemwalker Desktop Keeper Log Analyzer Server.

⚑ Note

....

When constructing database, be aware of the following restrictions and notes

[Database of Systemwalker Desktop Log Analyzer Unable to Directly Transferred]

When migrating from Systemwalker Desktop Log Analyzer to Systemwalker Desktop Keeper V15.0.0 or later, data shall be transferred again. Before constructing database, refer to "Chapter 4 Upgrading".

[About Compression and Encryption of Database Creation Target]

Do not set compression or encryption settings for the drive and folder for constructing the database.

[About Virus Scan of Database Creation Target]

Exclude the folder for constructing the database from the targets of virus scan software.

[About User at Database Creation (Log Analyzer User)]

Do not delete the Windows logon user (Log Analyzer user) who has constructed the database environment constructed. When deleting the database environment, migrating database environment and restoring management information and log data, the Windows logon user used when the database environment was constructed is required.

[About Setting of Event Viewer]

Confirm the maximum log size of the event viewer (application log) and the operation settings when the maximum is reached in advance, and confirm that the event logs can be recorded properly. Construction of the database will be interrupted if no event log is recorded.

....

Items to be confirmed before database construction

In the Log Analyzer Server, the following ports will be used for access to database:

- No. 30004

If the above port numbers have been used, refer to "Port Number List" of *Systemwalker Desktop Keeper Reference Manual* before constructing the database, and change the environment of Systemwalker Desktop Keeper.

Standard of database construction time

The amount of time needed to construct the database will depend on the capacity of the database. The standard of creation time is as follows:

- When database capacity is about 50GB, (Xeon 3.16GHz, memory 4GB and RAID1 structure)

    Measured conditions

    - Number of clients: 250 sets

    - Number of file operation logs: 500 pieces

    - Number of non-file operation logs: 500 pieces

    - Number of months to save: 4 months

    Database construction time: around 30 minutes

    Note: Processing time is a reference value because changes will occur due to reasons such as the operation status of CPU, memory, disk performance and other applications of PC.

The steps to construct Systemwalker Desktop Keeper Log Analyzer Server database are as follows:

1. Log on as a Log Analyzer user (Windows account set at installation of Log Analyzer Server).

2. Select **Systemwalker Desktop Keeper** > **Log Analyzer** > **Operating Environment Maintenance Wizard** from the **Start/Apps** menu.

3. The "Welcome to Operating Environment Maintenance Wizard" window is displayed. Click the **Next** button.

4. **Select processing** window is displayed. Set **Processing executed** and click the **Next** button.
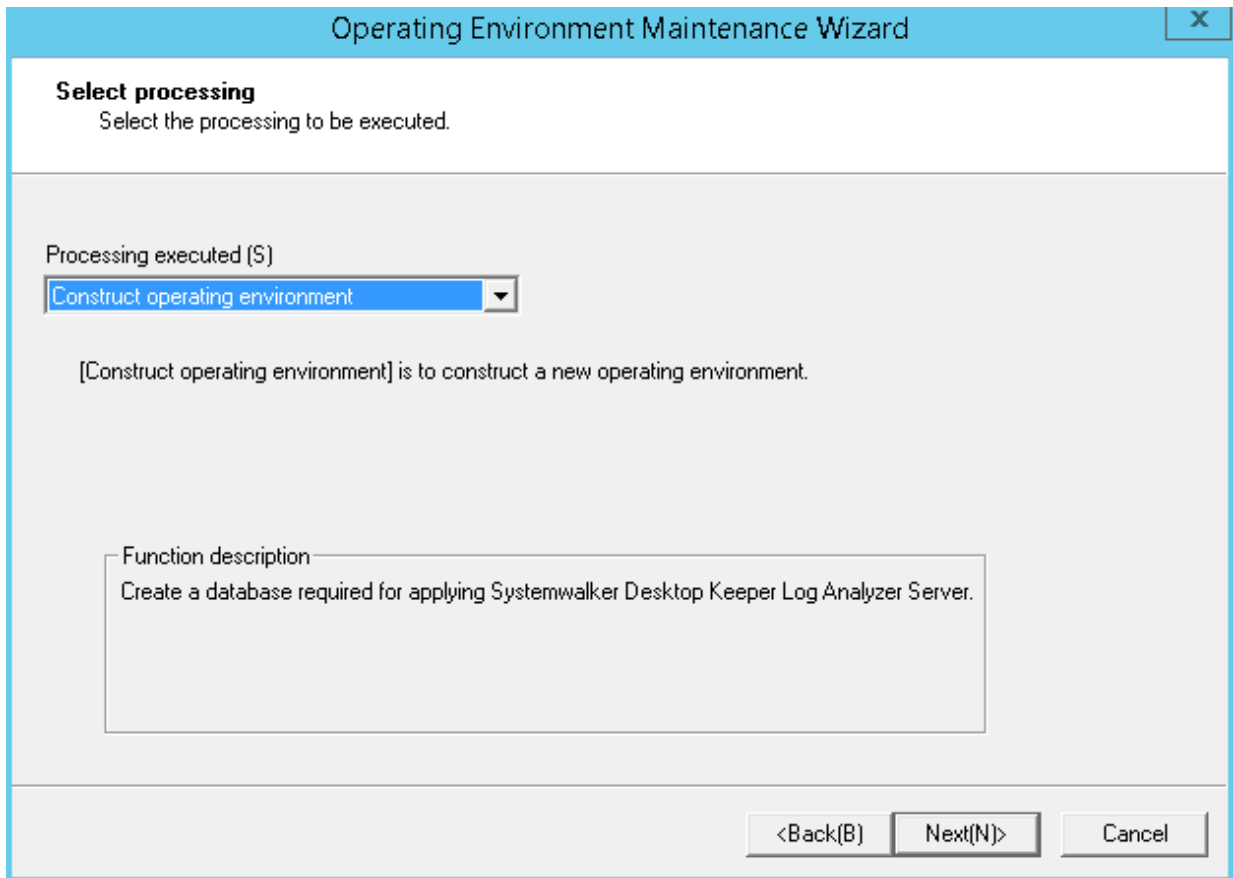
Item Name	Description
Processing executed	Select the processing to be executed. Select "Construction of Operating Environment" here. - Construction of Operating Environment - Deletion of Operation Environment

5. The **Input database information** window will be displayed.

   Set **Database saving target** and **Database estimation**, and click **Capacity calculation** button.

   Confirm **Database capacity** and **Available disk capacity** displayed in **Capacity**, and change **Database saving target** when **Available disk capacity** is insufficient. In addition, **Database capacity** can be added according to the needs. Set **Database capacity** directly.

After confirming **Database saving target** and **Database estimation**, click the **Next** button.

Item Name		Description
Database saving target		Enter the creation target of database. The initial value is "C:\DTK_LOGANALYZER\SFWD". When changing the creation target to be displayed, click the **Browse** button to change the folder.
		Up to 32 characters can be specified for the database storage folder name. Multi-byte characters such as space, some symbols (tab , ; # '), Hiragana, Katakana and Chinese characters cannot be specified.
		In addition, the following drives cannot be specified:
		- Root directory of drive (C:\, D:\, etc.)
		- Network drive
		- Non-NTFS drive
Database estimation	**Number of Clients** (required)	Enter the number of CTs managed in this server within the range of 1-99999.
	Number of file operation logs (required)	Enter the number of file operation logs within the range of 1-99999.
	Number of non-file operation logs (required)	Enter the number of non-file operation logs within the range of 1-99999.
	Number of saving months (required)	Select the number of months to save between 1-12.
Capacity	**Database capacity** (required)	Set the items in **Database estimation** and display the estimated value when the **Capacity calculation** button is clicked.

Item Name	Description
	When disk capacity available for the database creation target is sufficient, and creation is made with the capacity expected to be larger than the estimated capacity, reset this item within the range of disk capacity available.
Available disk capacity	The capacity available of the target disk of creation is displayed.

Note

. . . .

About [Number of Months to Save]

The partition of the database is the specified number of months to save x 31 log saving spaces.

For example, if the number of months to save is 3, it is divided into 3*31=93 saving spaces.

Every time when data transfer command is started, data will be saved to saving space 1, saving space 2 and saving space 3, etc. However, after the saving space 93, it will return to saving space 1 and overwrite. Therefore, the old data of correspondent space will be deleted.

In addition, when the data saved by overwriting cannot be written into the existing saving space, several saving spaces after that might be deleted.

As mentioned above, in spite of circulated use of the saving space corresponding to **Number of Months to Save**, be aware that not only the oldest data in operation time, but the old data that has been transferred in the earliest will also be overwritten.

. . . .

6. The **Confirm the settings content** window is displayed. Confirm if the content displayed in the window has mistakes, and click the **Next** button.

   The **Processing** window is displayed, and database creation is started.

7. After the processing has completed normally, the **Processing Completed** window will be displayed. Click the **Finish**.

2.7.3 Set Log Analyzer Server Environment

After the Log Analyzer Server has been installed and the database has been created, the environment of the server will be constructed. The environment setup of the server is composed of the environment construction operation on the Management Server/Master Management Server and the environment construction operation on the Log Analyzer Server.

Perform the following preparations on servers before environment construction work.

Preparation 1: Create shared folder (operations on Log Analyzer Server)

In order to collect logs and administrators' information on the Management Server/Master Management Server, it is required to create shared folders on the Log Analyzer Server.

Use the full path and create shared folders no greater than 140 characters. In addition, perform the following security-related settings for the folders:

- Set the number of users allowed to be connected equal to the number of sets of Management Server/Master Management Server.

- Set the user name that belongs to the Administrator group or the Domain Admins group to full control in the user with connection permission.

- In the security setting of shared folders, set the following groups and users to full control:

   - Users set as "User with Connection Permission".

   - Administrators group

   - SYSTEM user

The shared folders created here will be used in the settings of the Log Analyzer and data transfer commands later.

- Specify the format of shared network folder name (\\IP address\folder path) specified in the "Log Analyzer Settings" window.

- Specify the local path of shared folders in "Data Transfer Command".

Preparation 2: Create target folder for saving logs temporarily (operations on Management Server/Master Management Server)

The target folder for saving logs temporarily needs to be created on the Management Server/Master Management Server.

Specify the target folder for saving logs temporarily with a full path no greater than 140 characters. In addition, the shared folder created in Preparation 1 cannot be used as the target folder for saving logs temporarily.

For an estimation of disk capacity required for the target folder for saving logs temporarily, refer to the "Operating Environment" of *Systemwalker Desktop Keeper User's Guide*, and refer to the "Estimating temporary disk capacity required for sending log data".

Preparation 3: Confirm [IP Address] of self-node in the [Server Information Settings] window (operation on Management Server/Master Management Server)

In the server information settings of the Management Server/Master Management Server, when the self-node IP address is set to the loop back address "127.0.0.1" or "::1", update it to the correct IP address before the following operations.

For the setting method, refer to "2.3.6.4 Set Server Information".

📋 Note

Refer to "IPv6 Support" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on specifying an IPv6 address.

📋 Note

When importing data from multiple Management Servers to a single Log Analyzer Server, ensure that the I/O file encoding settings are the same in the Server Settings Tool of each Management Server.

2.7.3.1 Set Log Analyzer Environment on Management Server/Master Management Server

Set the Log Analyzer Server link with the Management Server/Master Management Server on the Management Server/Master Management Server, and transfer the logs and the administrator information collected on the Management Server/Master Management Server to the environment of the Log Analyzer Server.

The following settings should be performed on the Management Server/Master Management Server.

📋 Note

Configure the Log Analyzer settings in a time period when services can be stopped.

When configuring the Log Analyzer settings, the Management Server services below will stop. Therefore, configure the settings in a time period when they can be stopped.

- SWLevelControlService

- SWServerService

Note that immediately after restarting SWServerService or after the date has changed (0:00), available space in the database will be checked. This check takes approximately 15 minutes, and services may not stop during this time.

Therefore, do not configure the Log Analyzer settings in the above time period.

1. Select **Start** > **Systemwalker Desktop Keeper** >**Server**> **Log Analyzer Settings**, or **Apps** > **Systemwalker Desktop Keeper** > **Log Analyzer Settings**.

   The **Log Analyzer Server Settings** window is displayed.
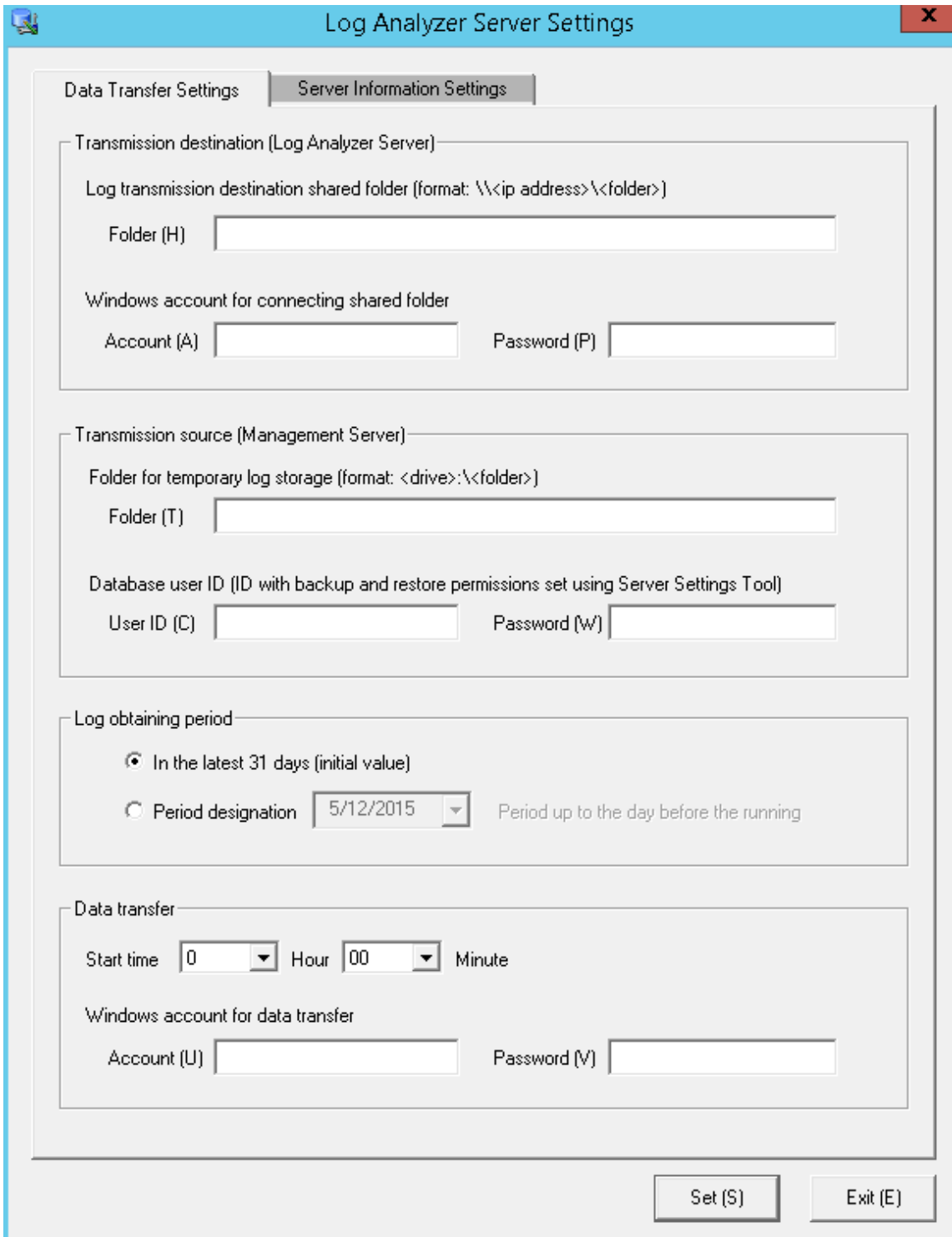
2. In the **Log Analyzer Server Settings** window, select **Data Transfer Settings**, and enter the following items.

Item Name		Description
Transmission destination	**Log transmission**	Shared folder name on the Log Analyzer Server for sending logs using UNC format (*ipAddress**sharedFolderName* example: \\192.168.0.1\share).

Item Name		Description
(Log Analyzer Server)	**destination shared folder**	Refer to "IPv6 Support" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on specifying an IPv6 address. Even if the Log Analyzer Server and the Management Server/Master Management Server are on the same computer, set the shared folder and specify to the above format.
	Windows account for connecting shared folder	Account name and password set as "User with Connection Permission" in "Preparation 1: Create shared folder (operations on Log Analyzer Server)". Use the following format for the account name: - Local account: *computerName\accountName* - Domain account: *domainName\accountName* Up to 64 characters can be specified in the password. If the password exceeds 65 characters, change it to a password less than 64 characters and apply this setting.
Transmission source (Management Server)	**Folder for temporary log storage**	This is the folder that saves logs temporarily (Note 1). Up to 140 characters can be specified.
	Database user ID	Set the user ID and password set in Sever Setting Tool of the Management Server/Master Management Server with the access authority to "Backup and Restoration". Up to 64 characters can be specified in password. If the password exceeds 65 characters, change it to a password less than 64 characters and apply this setting. Database name is a fixed value, which cannot be modified.
Log obtaining period		Set log acquisition start date. This item should be set at installation. Decide the transmission schedule of logs in the stage of organizing the operating environment and perform this setting. For detailed information, refer to "Set Log Obtaining Period on Management Server" in *Systemwalker Desktop Keeper User's Guide for Administrator*.
Data transfer	**Start time**	Data transfer start time. This item is used to configure the settings to transfer data regularly. Specify a time of day such as night time during which few users are using the client (CT).

	Account	Set a Windows account to execute tasks for transferring data regularly.
		
		- If a local account is specified, you should execute the Log Analyzer settings in the local account.
		  Likewise, if a domain account is specified, execute the Log Analyzer settings in the domain account.
		
		- Before specifying a domain account, ensure that a local account of the same name does not exist.
		
		- The following privileges and settings apply to Windows accounts specified using **Data transfer** > **Account**.
		
		  - Local accounts must belong to the Administrators group, and domain accounts must belong to the Domain Admins group
		
		  - The password for the user must not expire

Item Name		Description
		Use the following format for the account name: Local and domain accounts: *accountName*
	Password	Specify the password using up to 64 characters. Note that if the password exceeds 64 characters, change it to one that is up to 64 characters before performing these settings.

Note 1: Specify the folder created in preparation 2.

3. Click the **Server Information Settings** tab.
   In the **Log Analyzer Server Settings** window, select **Server Information Settings**, and specify each item.

Item Name		Description
Log analyzer server information	**IP address or host name**	Specify the IP address or host name of the Log Analyzer Server, using up to 18 characters.
		To use IPv6 for communication, do not specify the IPv6 address directly but instead specify a host name of up to 18 characters that exists in the hosts file. Behavior is not guaranteed if a link-local address is specified.
		If specifying multiple Log Analyzer Servers, specify all of the Log Analyzer Servers while ensuring that the IP addresses (or host names) are not duplicated.
	Communication port 1	-
	Communication port 3	Specify the port number for Report Output Tool and Log Analyzer Server using 4 to 5 characters. It must match the value specified for **Communication port 3** during installation of the Log Analyzer Server.
		Specify a number from 5001 to 60000 (using only halfwidth digits).

4. Click **Set** to apply the settings.

5. When you click **Set**, the administrator information transfer will be automatically executed and the command prompt window will then be displayed.
   Upon completion, the command prompt window will close automatically.

6. Close the **Log Analyzer Server Settings** window.

Information

. . . .

In **Data transfer** > **Start time**, register TRANS.bat (data transmission of the Log Analyzer Server) to the task feature of the operating system on which the Management Server is running, and enable regular transfer of data.

Refer to "Setting Data Transfer Time on the Management Server" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on setting the data transfer start time.

The task feature setting values (except for task start time) are set automatically.

Refer to "Change the Data Transfer Task on the Management Server" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on changing the values of advanced setting items.

. . . .

2.7.3.2 Configuring the Log Analyzer Environment on the Log Analyzer Server

On the Log Analyzer Server, configure the environment for importing logs and administrator information collected on the Management Server or Master Management Server to the Log Analyzer Server.

1. Use the Log Analyzer user (the Windows account set when the Log Analyzer Server is installed) to register the Log Analyzer Server.

2. Click **Start** > **Systemwalker Desktop Keeper** > **Log Analyzer** > **Data Import Settings**, or **Apps** > **Systemwalker Desktop Keeper** > **Data Import Settings**.
   The **Data Import Settings** window is displayed.
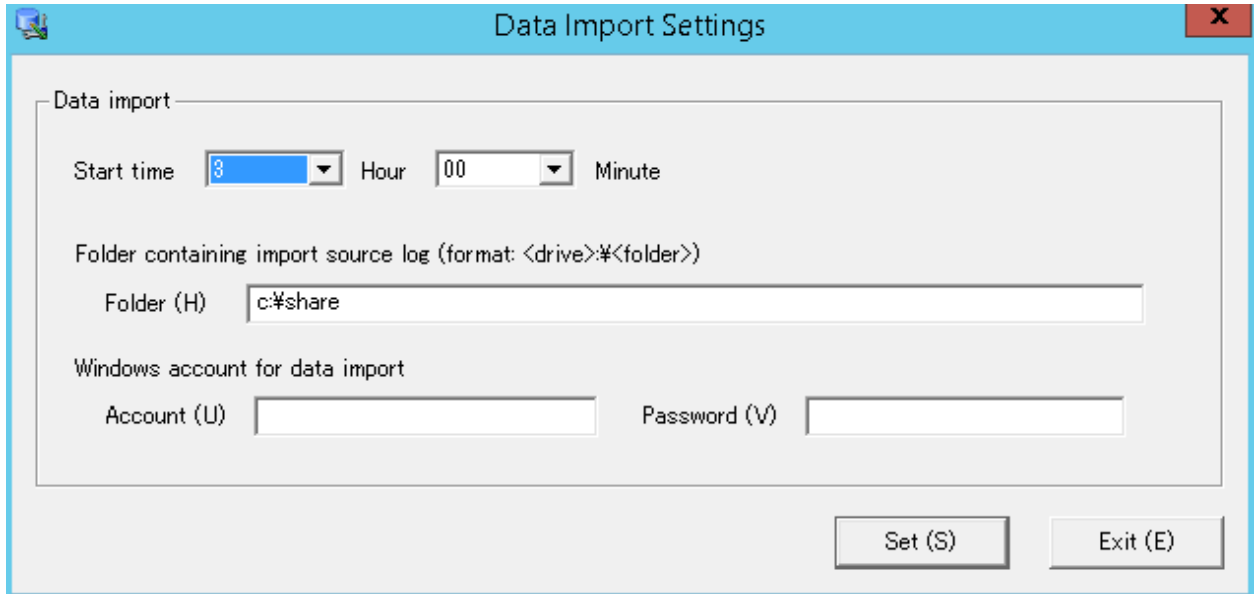
	Item	Description
Data import	**Start time**	Data import start time.
		This item is used to configure the settings to import data regularly.
		Specify a time after the data transfer start time, so that the data import will start after data transfer is performed.
	Folder containing import source log	Transfer destination shared folder of the Log Analyzer settings. (*1)
		Specify the folder using local path format. A network folder cannot be specified.
		*1: Specify the shared folder created during step 1 of advanced preparation.
	Windows account for data import	Specify the Windows account and its password used when constructing the database.

3. Click **Set** to apply the settings.

4. When you click **Set**, the administrator information import command will be automatically executed and the command prompt window will then be displayed.
   Upon completion, the command prompt window will close automatically.

5. Close the **Data Import Settings** window.

Information

....

In **Data import** > **Start time**, register DTTOOLEX.EXE (data transfer to/delete from the Log Analyzer Server) to the task feature of the operating system on which the Log Analyzer Server is running, and enable regular saving of data to the database.

Refer to "Setting Data Import Time on the Log Analyzer Server" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on setting the data import start time.

The advanced setting items of the task feature (except for task start time) are set automatically.

Refer to "Change the Data Import Task on the Log Analyzer Server" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on changing the advanced setting items.

....

2.8 Construct Environment of Report Output

The following describes the installation and environment construction of Systemwalker Desktop Keeper Report Output Tool.

2.8.1 Install Report Output Tool

This section describes how to newly install the Report Output Tool of Systemwalker Desktop Keeper.

Items to be confirmed before installation

- Refer to "Operating Environment" in *Systemwalker Desktop Keeper User's Guide* to confirm "Products that cannot be used in Mixture".

- Refer to "Port Number List" in *Systemwalker Desktop Keeper Reference Manual* to confirm the port number to be used.

- When copying the installer of Systemwalker Desktop Keeper from DVD-ROM to local disk, make sure that the path of the copy target does not contain double-byte characters.

- IPv6 addresses cannot be specified. For communication with the Log Analyzer Server in IPv6 environments, configure the hosts file.

- If the same version and level of the Report Output Tool is already been installed, it is not possible to perform an overwrite install (the installer will close without warning).

Installation

The steps to install Report Output Tool are as follows. In addition, refer to the *Systemwalker Desktop Keeper User's Guide* for the operating environment.

1. Log in to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group.

2. After the DVD-ROM of Systemwalker Desktop Keeper is inserted into the PC, the installer window will be displayed.

   Select "Report Output Tool Installation".

   If the installer is not started, start "swsetup.exe" in the DVD-ROM drive.

3. After the "Welcome to Systemwalker Desktop Keeper Report Output Tool Setup" window is displayed, click the **Next** button.

4. The "Select installation target" window of Report Output Tool function is displayed.

   Confirm the **Required Capacity/Available Capacity** displayed in **Installation Target Drive**.

   If the displayed installation target is not to be changed, click the **Next** button.

   If the displayed installation target is to be changed, click the **Browse** button of the folder expected to be changed, and click the **Next** button after the folder has been changed.

   Multi-byte characters such as space, Hiragana, Katakana and Chinese characters cannot be specified in Report Output Tool. In addition, the following drives cannot be specified:

   - Root directory of drive (C:\, D:\, etc.)

   - Network drive

   - Non-NTFS drive

   The settings cannot be changed during overwriting installation (the **Browse** button will be disabled).

   The path cannot contain commas (,), semicolons (;),number signs (#) or halfwidth kana characters.

5. The "Select installation target" window of database-related files is displayed.

   Confirm the **Required Capacity/Available Capacity** displayed in **Installation target folder**.

   If the displayed installation target is not to be changed, click the **Next** button.

   If the displayed installation target is to be changed, click the **Browse** button of the folder expected to be changed, and click the **Next** button after the folder has been changed.

   Multi-byte characters such as space, Hiragana, Katakana and Chinese characters cannot be specified in database-related files. In addition, the following drives cannot be specified. Single-byte space cannot be specified either.

- Root directory of drive (C:\, D:\, etc.)

- Network drive

- Non-NTFS drive

If you perform an overwrite install from Systemwalker Desktop Keeper V15.0.0 or later version/level, you will not be able to change the settings.

The path cannot contain commas (,), semicolons (;) or number signs (#).

![Note icon] Note

Specify the path of **Installation target folder** using up to 96 halfwidth characters.

6. The "Enter Log Analyzer Server information" window is displayed.

Set the connection destination and communication port number of the Log Analyzer Server to be connected, and click the **Next** button.

IP Address: Specify the IP address or host name of the Log Analyzer Server to be connected (specify a host name that exists in the hosts file, using up to 18 characters). For communication using IPv6, ensure that a host name is specified. Behavior is not guaranteed if a link-local address is specified.

Communication Port: Set the value that is the same as the one specified in "Communication Port 3" used in Report Output Tool in the "Enter Port Number" window during the installation of Log Analyzer Server.

In addition, the settings cannot be changed during overwriting installation.

7. The "Start Copying Files" window is displayed.

Confirm the set contents. When the installation is started, click the **Next** button to start installation.

When the setting is expected to be changed, click the **Back** to reset.

8. The message below will be displayed. Click **OK** and continue with the installation process.

```
Upon completion, a window informing that the installation completed successfully will be
displayed.
Installation will continue until the window is displayed, so wait until completion.
```

9. The message below will be displayed. Click **Finish**.

```
The installation of Systemwalker Desktop Keeper report output tool was completed.
```

10. Upon successful completion, the **Confirm** window will be displayed.
    To use the program, click **Yes**. The operating system will restart.

After the Report Output Tool has been installed, the environment used for running the Report Output Tool should be set. (The information of the Log Analyzer Server to be connected will be effective after the environment setup has been performed.)

Continue referring to "2.8.2 Set Environment of Report Output" to perform environment setup.

2.8.2 Set Environment of Report Output

After the Report Output Tool has been installed, the environment for using the Report Output Tool should be constructed. This section describes the procedure for environment setup and the contents of setting required for report output.

Items to be set are as follows:

Server setting

Set the Log Analyzer Server connected when report is generated.

Batch user setting

Set the user ID and password of the administrator for executing the report output batch command in the Log Analyzer Server.

Trace level

Specify the detail level of logs to be output by the Report Output Tool.

Note

Environment setup must be performed after the installation of Report Output Tool

After the installation of the Report Output Tool, only **Trace Level** will be set. (for information of Log Analyzer Server, only the setting at installation is disabled.)

Before executing the Report Output Tool, perform the settings in sequence of **Server** setting and **Batch User** setting according to the following operation procedure.

In addition, it is not necessary to change the setting of **Trace Level**.

The operation procedure is as follows:
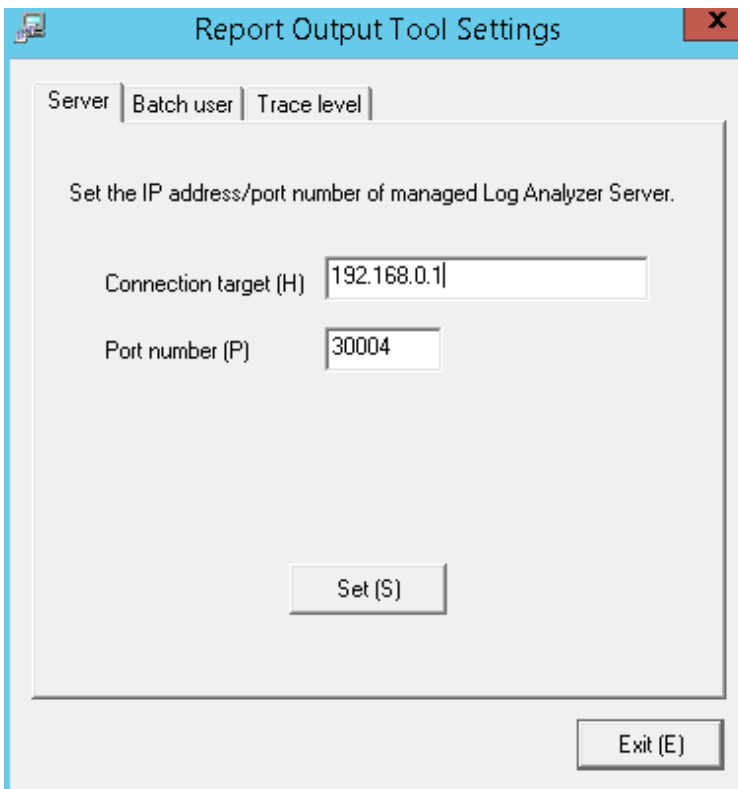
1. On the PC with Report Output Tool installed, log on to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group.

Note

Do not forget the logon account

The user name and the password logged on to Windows here are required at the logon to Windows when the report output schedule is set. Write a note, and do not forget the password.

2. Select **Systemwalker Desktop Keeper** > **Log Analyzer** > **Report Output Environment Setup** from the **Start]/Apps** menu.

3. Select the **Server** tab to set server information.

Item Name	Description
Connection target	Connection destination (IP address or host name) of the Log Analyzer Server to be connected.
	The field will be initialized with the value specified during installation - modify if necessary.
	Specify up to 18 halfwidth characters. IPv6 addresses cannot be specified. Note that if using an IPv6 environment, specify a name specified in the hosts file. Behavior is not guaranteed if a link-local address is specified.
Port number	Port number of the Log Analyzer Server to be connected.
	The field will be initialized with the value specified during installation - please modify if necessary.
	Specify up to 5 halfwidth characters..

4. Click the **Set** button. The setting confirmation window will be displayed. Click the **Yes** button to continue. In addition, the value after setting will become the default value at next startup.

5. After the sever setting has been perform normally, the completion message will be displayed. Click the **OK** button.

6. Select the **Batch user** tab and set the information of batch users.

Item Name	Description
Management Server	Systemwalker Desktop Keeper Master Management Server or Management Server for which user IDs for batch users have been registered.
	The fields contains a lists of the IP address or server name of each Management Server set in the Server Settings Tool.
User ID	Specify the user ID. The user ID of the administrator that already existed in the Sever Setting Tool can be specified.
Password	Specify the password of the user ID to be entered in **User ID**.

7. Click the **Set** button. The setting confirmation window will be displayed. Click the **Yes** button to continue.

8. After the setting of batch user has been performed normally, the completion message will be displayed. Click the **OK** button.

9. Select the **Trace level** tab to set the detail level of log.

Item Name	Description
Trace level	Specify the detail level of log. Values can be specified are as follows: **1:** Output startup/completion and error; **2:** Output detailed trace information. The initial value is 1.

10. Click the **Set** button. The setting confirmation window will be displayed. Click the **Yes** button to continue.

11. After the setting of trace level setting has been performed normally, the completion message will be displayed. Click the **OK** button.

12. After all the settings have been completed, click **Exit** to close the **Report Output Tool Settings** window.

2.9 Building a Smart Device Relay Server Environment

This section explains how to install and build the environment of the Smart Device Relay Server of Systemwalker Desktop Keeper.
Only users that belong to the Administrators group or Domain Admins group can perform the procedures on the Management Server,
Master Management Server and Smart Device Relay Server.
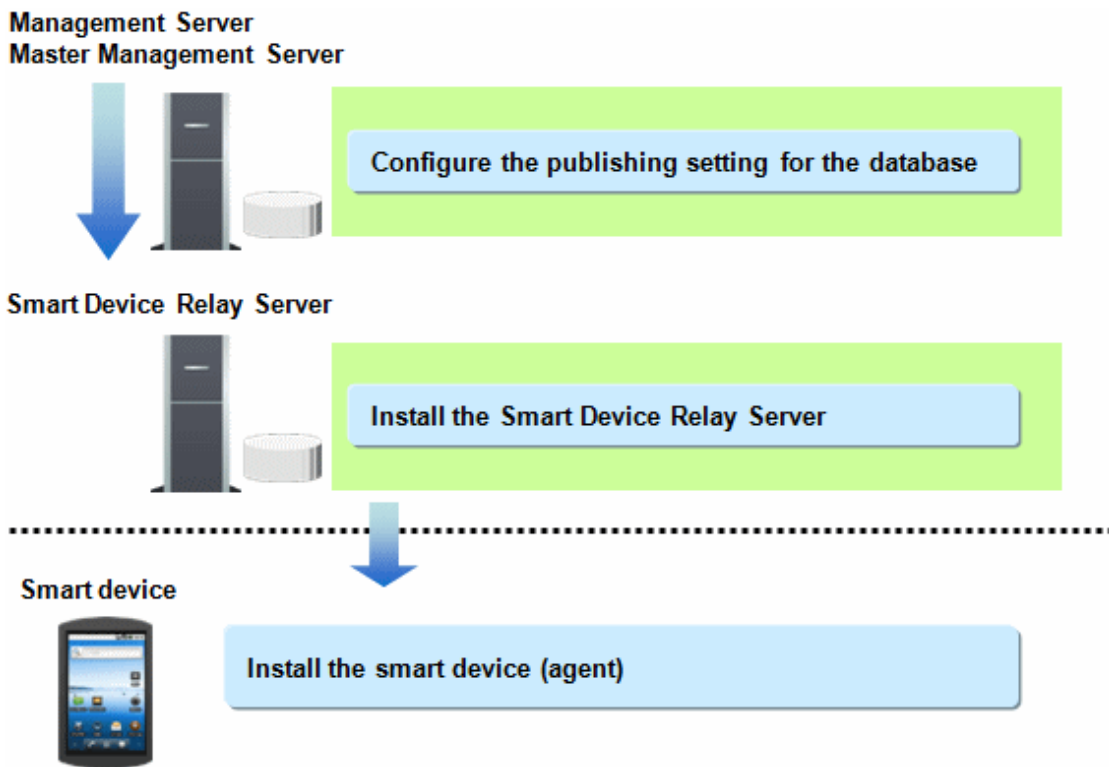
2.9.1 Configuring the Publishing Settings for the Database (Master Management Server or Management Server)

The following is the initial value for connecting from the Smart Device Relay Server to the Management Server or Master Management Server database:

Port number: 42050

If you want to modify this value, follow the procedure below:
Perform the change on the Management Server or Master Management Server of Systemwalker Desktop Keeper.
Perform the change after completing the build of the Management Server or Master Management Server of Systemwalker Desktop Keeper.

P Point
. . . .

Relative position of the Master Management Server or Management Server and the Smart Device Relay Server

In a 3-level system structure, connect the Smart Device Relay Server to the Master Management Server.

In a 2-level system structure that does not contain a Master Management Server, connect the Smart Device Relay Server to the Management Server. Refer to "1.2.1.4 Determine the Installation Standard for Smart Device Relay Servers" for details.
. . . .

1. In the firewall, open the port used for remote connections.
   To open the port used for enabling the Smart Device Relay Server to connect remotely to the Operation Database of the Management Server, register the port number as an exception for the firewall.
   The port number to be opened is specified by clicking **Management Server Settings** in the **Server settings tool** window, and then selecting **Port number settings** > **Management Console** <----> **Level Control Service**.

2.9.2 Installing the Smart Device Relay Server

This section explains how to perform a new installation of the Smart Device Relay Server of Systemwalker Desktop Keeper.

There are two ways to install the Smart Device Relay Server:

- Installation using the wizard

- Silent installation

2.9.2.1 Installation in Wizard Format

Follow the procedure below to perform installation of the Smart Device Relay Server.

1. Log on to Windows as a user that belongs to the Administrators group or Domain Admins group. If you are using other applications, close them.

2. Insert the Systemwalker Desktop Keeper DVD-ROM in the PC - the installer window is displayed.
   Select **Smart Device Relay Server Installation**.
   If the installer is not started, start "swsetup.exe" in the DVD-ROM drive.

3. In the **Welcome to the InstallShield Wizard for Systemwalker Desktop Keeper Smart Device Relay Server** window, click **Next**.

4. The **Set installation target folder** window is displayed.
   To use the installation folder displayed, click **Next**.

   To change the installation folder, click **Browse**, specify a different folder, and then click **Next**.

🔷 Note

. . . .

If the installation folder of the Smart Device Relay Server is targeted for compression or encryption, this may impact on program operation. Do not configure compression or encryption settings.
Specify up to 100 halfwidth alphanumeric characters, hyphens (-), or underscores (_) for **Installation target folder**.
You cannot specify the following drives:

   - Network drive

   - Non-NTFS/FAT drive

The path cannot contain commas (,), semicolons (;),number signs (#) or halfwidth kana characters.
. . . .

5. The "File copy start" window will be displayed.

   Confirm the set content. When starting installation, click the **Next** button, and installation will be started.

   When the settings are expected to be changed, click the **Back** to reset.

6. The message below will be displayed. Click **OK** and continue with the installation process.

```
Upon completion, a window informing that the installation completed successfully will be
displayed.
Installation will continue until the window is displayed, so wait until completion.
```

7. The message below will be displayed. Click **Finish**.

```
The installation of Systemwalker Desktop Keeper Smart Device Relay Server was completed.
```

8. Upon successful completion, the confirmation window will be displayed.
   To use the program, click **Yes**. The operating system will restart.

2.9.2.2 Performing Silent Installation

🔷 Note

. . . .

- Silent Installation of the Smart Device Relay Server can only be performed when you are performing installation for the first time.

- Installation process must not be interrupted during silent installation.
. . . .

Follow the procedure below to perform silent installation of the Smart Device Relay Server.

1. Create an installation parameter CSV file.
   If you are performing installation using the default values for all parameters, this step is not required.
   Refer to "A.3.1 Installation Parameter CSV File" for details.

2. Use the parameter setup command to create a response file.
   If you did not create an installation parameter CSV file in step 1, this step is not required.
   Refer to "A.3.2 Parameter Setup Command" for details.

3. Use the silent installation script to execute installation.
   Refer to "A.3.4 Silent Installation Script" for details.

4. Check the installation result.
   Check the returned value and message from the silent installation script.

2.9.3 Configuring the Operating Environment of the Smart Device Relay Server

This section explains how to configure the operating environment of the Smart Device Relay Server.

2.9.3.1 Setting Smart Device Information

For each smart device (Android device or iOS device) to be managed, configure the settings below.

- Android device:

   1. Use SDSVSetMS.EXE (change configuration of Smart Device Relay Server command) to set the following:

      - Enable management of Android devices: Specify the -Android.enabled option.

      - Set the Management Server or Master Management Server: Specify the -h option.

   2. If the default port number (48080) must be changed, refer to "How to Modify the Port Number Being Used" in the *Systemwalker Desktop Keeper Reference Manual* and change the port number.

   3. To perform HTTPS communication with a smart device (agent) (Android), build a certificate environment for HTTPS communication.
      Refer to "2.9.3.2 Configuring HTTPS Communication" for details. The procedure is the same as that for managing iOS devices, so you do not need to configure the settings if you have done so on an iOS device.

   4. Use SDSVService.bat (start/stop service of Smart Device Relay Server command) to start the Smart Device Relay Server.

Note

. . . .

The items set in steps 2 and 3 (except for the Management Server and Master Management Server ports in step 2) are also used by Systemwalker Desktop Patrol. If you have already set these items in Systemwalker Desktop Patrol, you do not need to set them here.

. . . .

- iOS device:

Point

. . . .

You can configure the settings in steps 1 to 4 below at one time.

. . . .

   1. Enable management of iOS devices.
      Execute SDSVSetMS.EXE (change configuration of Smart Device Relay Server command) with the -iOS.enabled option.

   2. Set the Management Server and Master Management Server.
      Execute SDSVSetMS.EXE with the -h option.
      This procedure is the same as that for managing Android devices, so you do not need to configure the settings if you have done so on an Android device.

   3. Set the server or reverse proxy that is to be connected to from the iOS device.
      Execute SDSVSetMS.EXE with the -iOS.connect.h, -iOS.connect.p, and -iOS.connect.profile.p options.

4. Set the iOS management database.
   Execute SDSVSetMS.EXE with the -iOSmgr.h option.
   To manage iOS devices with Systemwalker Desktop Keeper only, specify the Management Server.
   To manage iOS devices even with Systemwalker Desktop Patrol, specify the Management Servers or Systemwalker Desktop Patrol CSs that are running the iOS management database.
   Do not change this setting after configuring it.

5. If necessary, change the default port number (55432) to be used for communication with the iOS management database.,
   Refer to "How to Modify the Port Number Being Used" in the *Systemwalker Desktop Keeper Reference Manual* for details.

6. Build the certificate environment to perform HTTPS communication with a smart device (agent) (iOS),.
   Refer to "2.9.3.2 Configuring HTTPS Communication" for details.
   The procedure is the same as that for managing Android devices, so you do not need to configure the settings if you have done so on an Android device.

7. Install the MDM certificate prepared in "2.2 Advance Preparation".
   Execute swss_ImportAppleCert.bat (register Apple Inc. certificate command).

8. Start the Smart Device Relay Server.
   Execute SDSVService.bat (start/stop service of Smart Device Relay Server command).

Refer to "Command Reference" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

📝 Note

. . . .

Notes regarding coexistence with Systemwalker Desktop Patrol SS

- The following options of SDSVSetMS.EXE (change configuration of Smart Device Relay Server command) in steps 1 to 4 are used only in Systemwalker Desktop Keeper:

  - -h

  - -p

  - -Android.http.p

  - -Android.https.p

  - -Android.enabled

  - -iOS.enabled

- The following items options of SDSVSetMS.EXE (change configuration of Smart Device Relay Server command) are also used in Systemwalker Desktop Patrol:

  - -iOSmgr.h

  - -iOSmgr.p

  - -iOS.profile.p

  - -iOS.https.p

  - -iOS.connect.h

  - -iOS.connect.p

  - -iOS.connect.profile.p

- The items set in steps 6 and 7 are also used in Systemwalker Desktop Patrol.

- For items also used in Systemwalker Desktop Patrol, specify the same values in both products.
  After the items are set in Systemwalker Desktop Keeper, specifying different values in the same items in Systemwalker Desktop Patrol will result in the settings initially configured in this product changed to the new values specified in Systemwalker Desktop Patrol. After the items are set in Systemwalker Desktop Patrol, specifying different values in the same items in this product will result in the settings initially configured in Systemwalker Desktop Patrol changed to the new values specified in this product.

. . . .

2.9.3.2 Configuring HTTPS Communication

This section describes how to configure HTTPS communication between the Smart Device Relay Server and a smart device (agent). The configuration procedure depends on whether the server certificate used is prepared by the user or is the Systemwalker certificate.

Settings during installation of the certificate

Perform the procedure below to configure the settings:

If using a server certificate prepared by the user:

1. Use SDSVMakeCSR.exe to generate the certificate signature request for the server certificate.

2. Send the certificate signature request that was generated in step 1 to the CA, to obtain the CA certificate (intermediate CA certificate) and server certificate issued by the CA.

3. Use SDSVService.bat to stop the Smart Device Relay Server.

4. Use SDSVImportCert.exe to register the CA certificate (intermediate CA certificate) obtained in step 2.

5. Use SDSVImportCert.exe to register the server certificate obtained in step 2.

6. Use SDSVConfig.exe to enable the use of the server certificate prepared by the user.

7. Use SDSVService.bat to start the Smart Device Relay Server.

📝 Note
. . . .

If step 5 is mistakenly performed before step 4, repeat the procedure from step 1.
. . . .

If using the Systemwalker server certificate:

1. Use SDSVMakeCSR.exe, and specify the -certfile option to generate a server certificate.

2. Use SDSVService.bat to stop the Smart Device Relay Server.

3. Execute SDSVImportCert.exe with the -CACERT option specified.

4. Use SDSVImportCert.exe to register the server certificate generated in step 1.

5. Use SDSVConfig.exe to enable the use of the server certificate that you registered in step 4.

6. Use SDSVService.bat to start the Smart Device Relay Server.

📝 Note
. . . .

If step 4 is mistakenly performed before step 3, repeat the procedure from step 1.
. . . .

Certificate renewal settings

Perform the procedures below to configure the settings:

If using a server certificate prepared by the user:

1. Use SDSVMakeCSR.exe to generate the certificate signature request for the server certificate.

2. Send the certificate signature request that was generated in step 1 to the CA, to obtain the server certificate issued by the CA.

3. Use SDSVService.bat to stop the Smart Device Relay Server.

4. Use SDSVImportCert.exe to register the server certificate obtained in step 2.

5. Use SDSVService.bat to start the Smart Device Relay Server.

If using the Systemwalker server certificate:

1. Use SDSVMakeCSR.exe, and specify the -certfile option to generate a server certificate.

2. Use SDSVService.bat to stop the Smart Device Relay Server.

3. Use SDSVImportCert.exe to register the server certificate generated in step 1.

4. Use SDSVService.bat to start the Smart Device Relay Server.

Refer to "Command Reference" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

🗊 Note

In coexistence with the SS of Systemwalker Desktop Patrol V15.0.0 or later, if a certificate is registered in Systemwalker Desktop Patrol after another certificate is registered in Systemwalker Desktop Keeper, then the certificate registered in Systemwalker Desktop Patrol will be used for HTTPS communication between iOS devices and the Smart Device Relay Server.

2.10 Installing the Smart Device (Agent) (Android)

This section explains how to perform a new installation of the smart device (agent) (Android) of Systemwalker Desktop Keeper.

2.10.1 Installing the Smart Device (Agent) (Android)

There are two ways to install the smart device (agent) (Android):

- If downloading from the website:
  Having the smart device user download (install) Desktop Keeper Client from Google play.

- When the following method is used to distribute the smart device (agent) Android app file (with the extension .apk) included in the Systemwalker Desktop Keeper DVD-ROM to the smart device, and the install is performed by the smart device user:

  - Copy to an SD card and distribute (an application that allows file operations may be needed to install the smart device (agent) (Android))

  - The smart device user downloads the file from an internal web server, file server, etc.

  - Distribute the file to the smart device user as an email attachment

The path of the smart device (agent) (Android) apk file on the Systemwalker Desktop Keeper DVD-ROM is as follows:

```
dtkDvdromRoot\win32\SmartDevice\x86\Client\Systemwalker_Log_Agent.apk
```

When you select the distributed Systemwalker_Log_Agent.apk file, the **Install** button will be enabled. Tap **Install**. The window shown below will be displayed.
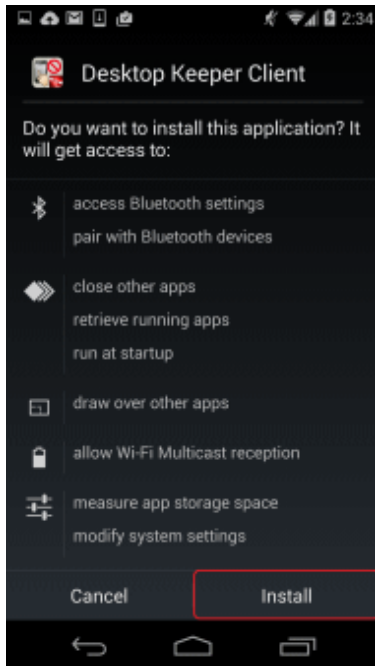
Tap **Install** to begin installation.

Note

If installation is blocked:
The procedure for Android 4.2.2 is shown below. The procedure may differ according to the operating system and device type, so refer to the product manual for details.

If the following warning screen is displayed during installation, you must change the settings and perform the installation again.
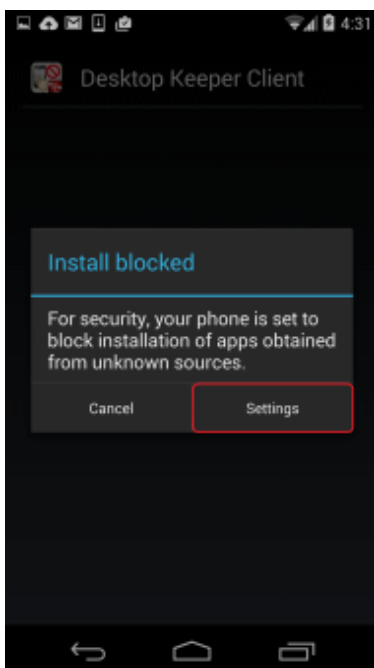
If the above warning screen is displayed, install the agent as follows:

1. Tap **Settings** to show the **Security** screen.

2. In the **Security** screen, select **Unknown sources**.
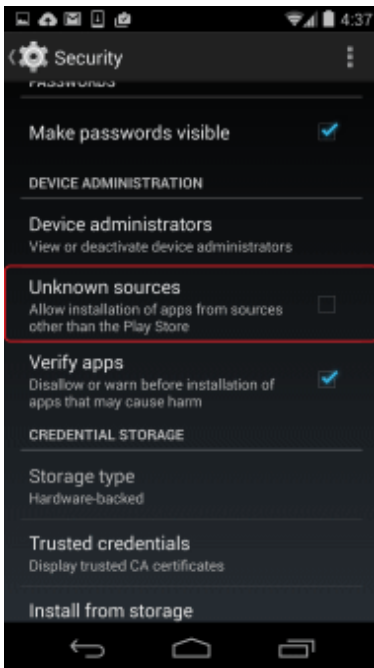
3. A confirmation dialog box will be displayed. Tap **OK**.
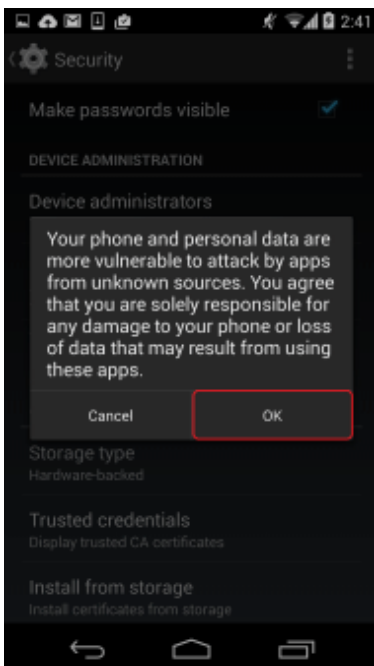
4. Install the smart device (agent) (Android) again.

5. Once installation is complete, open the **Security** screen and then tap **Application**.
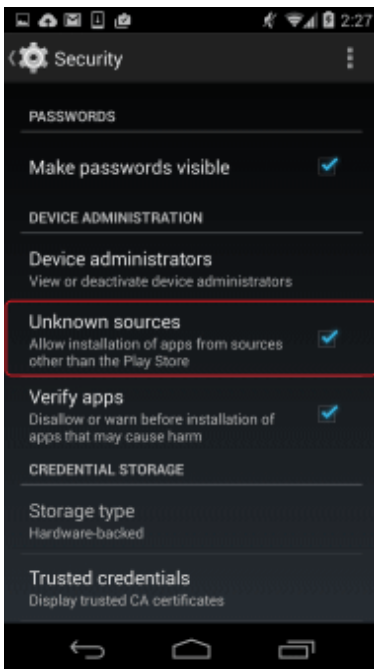
6. Clear **Unknown sources**.
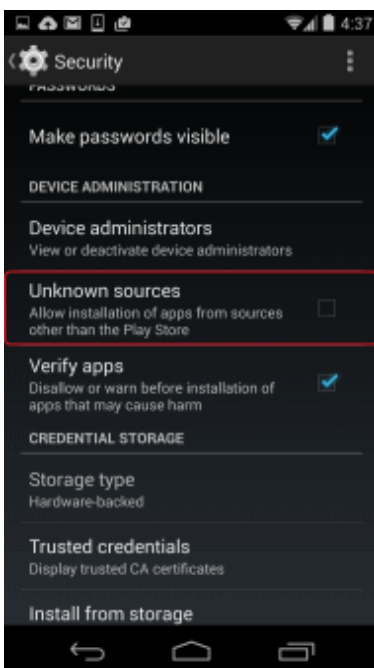
This will only allow installation of applications from the official application store.

2.10.2 Configuring the URL for Synchronizing with the Smart Device Relay Server

After installing the smart device (agent) (Android), set up the URL for synchronizing communication with the Smart Device Relay Server.

🦜 Note

Immediately after installation of the smart device (agent) (Android)

- The smart device (agent) (Android) will not perform any operation log collection or operation prohibition until the URL for synchronization is set up and the device is synchronized with the Smart Device Relay Server. Therefore, after installing the smart device (agent) (Android), you must set up the URL for synchronization, and synchronize with the Smart Device Relay Server.

- Immediately after the smart device (agent) (Android) is installed, it is configured so that it can be uninstalled.
  To prevent uninstallation, synchronize with the Smart Device Relay Server after setting a client management password.

. . . .

1. Start the agent (Desktop Keeper Client) that you installed.
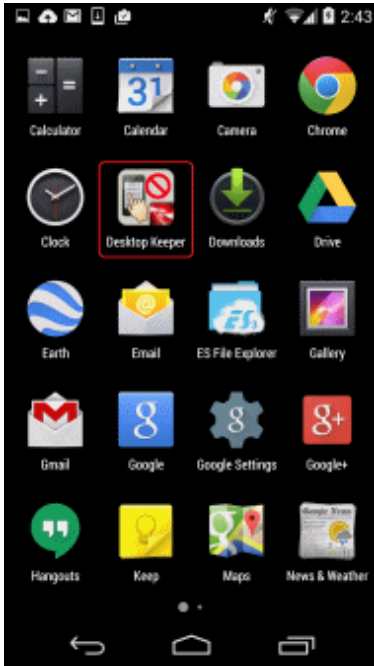
2. After starting the installed agent, tap the menu to display the options menu. Then tap the lower right of the screen and tap **Settings**.
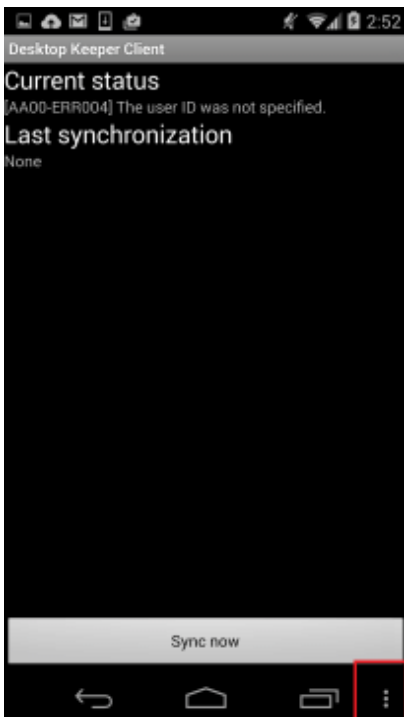
3. In the settings screen, tap **URL for synchronization**.
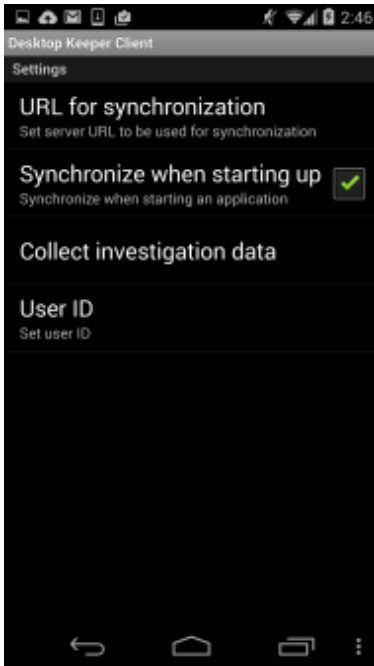
4. Enter the URL of the Smart Device Relay Server in **URL for synchronization**, and tap **OK**.
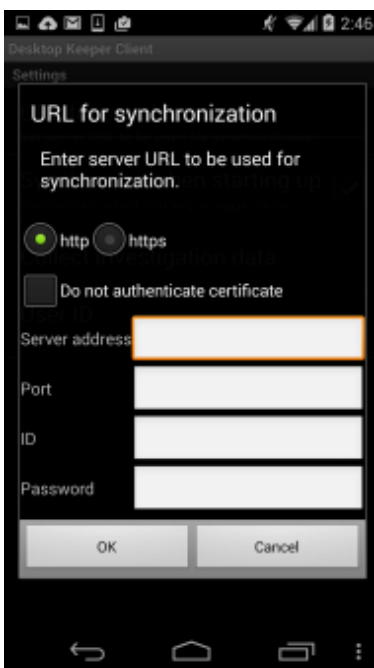
Configure the URL for synchronization as follows:

- If connecting to the Smart Device Relay Server:

  a. **http**, **https**
     Set the protocol for communication with smart devices.
     If you configured HTTPS communication using the procedure in "2.9.3.2 Configuring HTTPS Communication", select **https**.

  b. **Do not authenticate certificate**
     Not selected: Do not connect if the certificate is untrusted. (Initial value)
     Selected: Connect even if the certificate is untrusted.

c. **Server address**

Specify the address of the Smart Device Relay Server.

- If a server name is specified:
  - Specify up to 15 halfwidth characters.
  - It can contain halfwidth alphanumeric characters (A-Z, a-z, 0-9) and halfwidth hyphens (-).
  - Symbols other than hyphens (-) cannot be specified.
  - It cannot contain only numbers.

- If an IPv4 address is specified:
  - Specify up to 15 halfwidth characters.
  - It can contain halfwidth numbers (0-9) and halfwidth periods (.).

Note: If a server name is specified, it is necessary to be able to resolve it. Otherwise, communication will not be possible between the Management Server or Master Management Server and the client (CT).

d. **Port**

HTTP/HTTPS listener port: Port number specified using the procedure in "2.9.3.1 Setting Smart Device Information"

e. **ID**

Not supported

f. **Password**

Not supported

- If connecting via a Proxy server:

a. **http**, **https**

Set the protocol for communication with the Proxy server.
Select **http** or **https**.

b. **Server address**

Specify the address of the Proxy server.
If a server name is specified:

- Specify up to 15 halfwidth characters.
- It can contain halfwidth alphanumeric characters (A-Z, a-z, 0-9) and halfwidth hyphens (-).
- Symbols other than hyphens (-) cannot be specified.
- It cannot contain only numbers.

- If an IPv4 address is specified:
  - Specify up to 15 halfwidth characters.
  - It can contain halfwidth numbers (0-9) and halfwidth periods (.).

Note: If a server name is specified, it is necessary to be able to resolve it. Otherwise, communication will not be possible between the Management Server or Master Management Server and the client (CT).

c. **Port**

HTTP/HTTPS listener port: Port number of the Proxy server

d. **ID**

ID for basic authentication
(When performing basic authentication using the Proxy server)

e. **Password**

Password for basic authentication
(When performing basic authentication using the Proxy server)

5. In the settings screen, tap **User ID**.
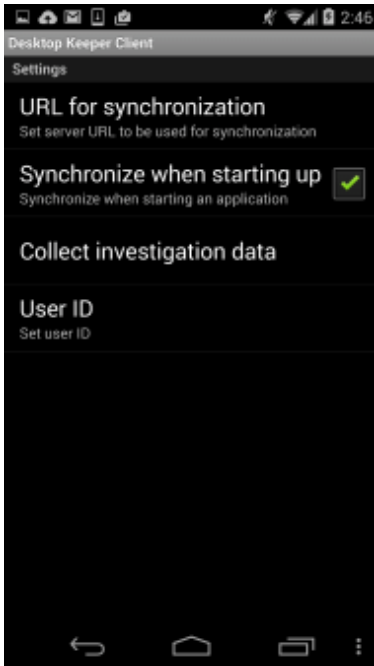
6. Enter the user ID, and tap **OK**.
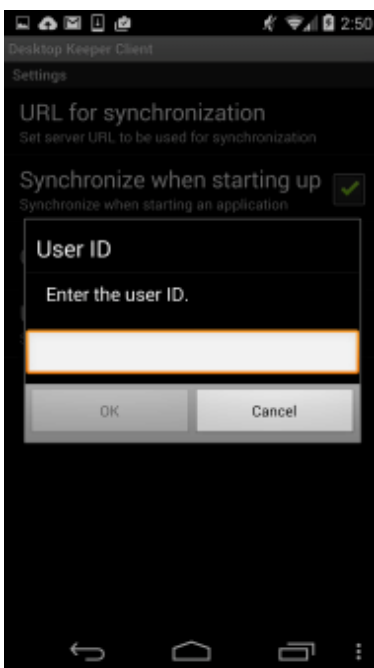
If you tap **Cancel** without entering a user ID, the following message will be displayed.

```
AA001-SEL001 Cannot communicate to the server without a user ID. Finish?
```

To exit, tap **OK**. However, the device will not be able to communicate with the Management Server.
To return to the **User ID** screen, tap **Cancel**.
You can use the following characters for the user ID:

- You can specify up to 20 characters.

- The halfwidth alphanumeric characters and symbols "-", "@", ".", "_" can be used.

- Alphabetic characters are case-sensitive.

7. In the settings screen, check the **Synchronize when starting up** setting. If it has not been selected, tap it to select.
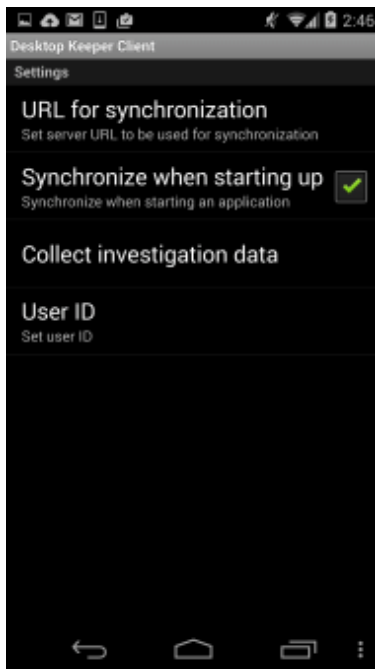
8. Tap the back button to return to the agent screen.

9. In the agent screen, tap **Sync now**.
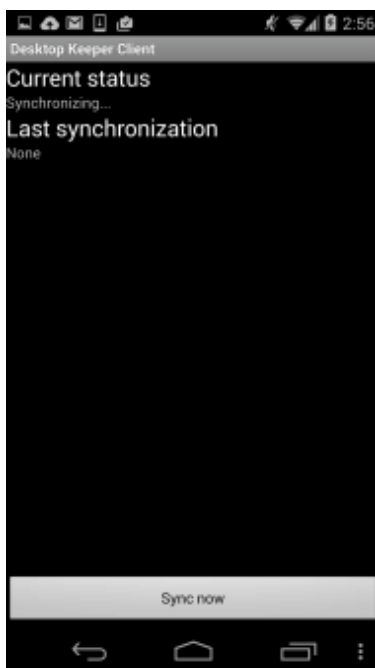
10. When **Synchronization has been completed** is displayed, synchronization is complete. The latest policy will be applied at this time.
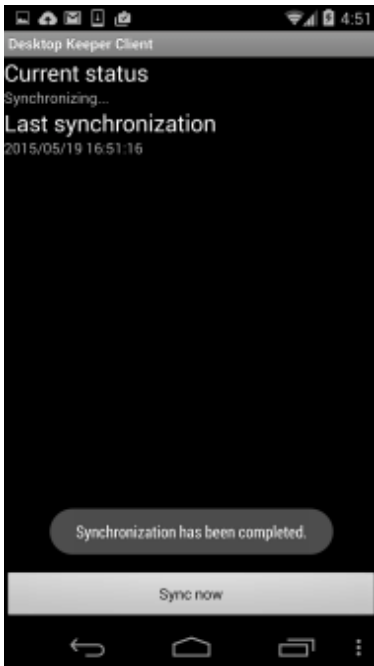
To prevent uninstallation

When you start Desktop Keeper Client, the confirmation message shown below will be displayed.

When you tap **Activate**, this will prevent uninstallation of Desktop Keeper Client.

After tapping **Cancel**, to uninstall Desktop Keeper Client you will need to enter the password that was set in **Client management password** in the **Terminal Operation Settings** window of the Management Console.
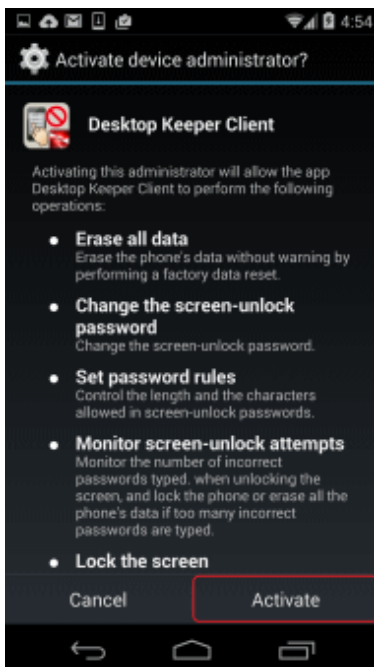
It is recommended that you configure Desktop Keeper Client to prevent uninstallation.

2.11 Installing the Smart Device (Agent) (iOS)

This section explains how to perform a new installation of the smart device (agent) (iOS) of Systemwalker Desktop Keeper.

2.11.1 Installing the Smart Device (Agent) (iOS)

🖐 Note

. . . .

Send the following URL to the iOS device user.

https://*smartDeviceRelayServerHostName*/*ipAddress:portNumber*/mdmi/systemwalker/

The host name or IP address to be published must match the values specified in the -CN option for SDSVMakeCSR.exe (create application for certificate issuance command). If they do not match, an error will be detected in certificate verification.

Set up a network so that the host name or IP address to be published can only be accessed within the company.
You can check the port number by executing SDSVSetMS.EXE (change configuration of Smart Device Relay Server command) without any options specified. Specify the port number set for iOS.connect.profile.p.
The default value is "50080".

. . . .

1. Access the URL provided by the administrator.

🖐 Note

. . . .
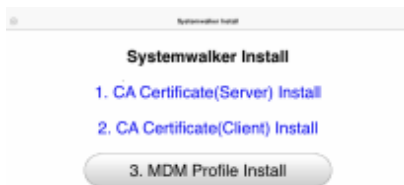
If the CA certificate (server) and the CA certificate (client) are already installed on the iOS device, these two certificates will be overwritten.
If the MDM profile is already installed on the iOS device, delete the MDM profile (Profile Service Enroll) on the iOS device once, and then install the MDM profile.
Refer to "5.4 Uninstalling Smart Device (Agent) (iOS)" for details on how to delete the MDM profile (Profile Service Enroll).

. . . .

2. Tap **1.CA Certificate(Server) Install**.

3. The screen for installing the CA certificate will start on the iOS device. Tap **Install**.

4. During installation, the message "The authenticity of "certificate" cannot be verified. Installing this profile will change settings on your iPad(iPhone)." is displayed. Tap **Install Now** to continue. If you have set a pass code lock on the iOS device, you must enter the pass code during installation.

5. Upon completion, the **Profile Installed** window will be displayed. Tap **Done**.

6. Tap **2.CA Certificate(Client) Install**.

7. The screen for installing the CA certificate will start on the iOS device. Tap **Install**.

8. During installation, the message "The authenticity of "certificate" cannot be verified. Installing this profile will change settings on your iPad(iPhone)." is displayed. Tap **Install Now** to continue. If you have set a pass code lock on the iOS device, you must enter the pass code during installation.

9. Upon completion, the **Installation is completed** window will be displayed. Tap **Done**.

10. Tap **3.MDM Profile Install**.

11. The **MDM Profile** installation screen will be displayed. Tap **Install**.

12. During installation, **Installing this profile will change settings on your iPad (iPhone)** is displayed. Tap **Install Now** to proceed. If you have set a pass code lock on the iOS device, you must enter the pass code during installation.

13. During installation, the "MOBILE DEVUCE MANAGEMENT" warning screen is displayed. Tap **Install** to continue.

14. Upon completion, the **Installation is completed** window will be displayed. Tap **Done**.

Chapter 3 Maintenance

This chapter describes how to back up and restore the Systemwalker Desktop Keeper assets.

The assets of the Systemwalker Desktop Keeper are stored on the Management Server/Master Management Server and Log Analyzer Server. This chapter describes the backup targets and the methods of backup and restoration in terms of the Management Server/Master Management Server and Log Analyzer Server. In addition, the Management Server/Master Management Server and Log Analyzer Server are independent of each other and require separate asset backup.

3.1 Maintenance of Management Server/Master Management Server

This section describes how to maintain the Management Server/Master Management Server of the Systemwalker Desktop Keeper.

3.1.1 Targets and Methods

The following are two purposes for the backup and restoration of Systemwalker Desktop Keeper Management Server/Master Management Server.

For precaution against environmental exceptions

Data backup is necessary to prevent data loss and restore data in case of a hard disk failure or file corruption.

For stable usage of backup logs

- To avoid database space becoming insufficient, set the storage life of the log information and delete the log information saved for a period longer than the set storage life.
Note: For details about the related windows, refer to "1.2.7 Determine How to Operate Logs".

- Regular backups with the aim of browsing using the Log Viewing Database

The backup targets can be classified into the "product assets" related to the product operation, including configuration files, and the "user assets" including the log information. The following table describes the backup targets of the product asset classification and user asset classification and the backup targets and methods corresponding to the preceding purposes:

Classification	Backup Target	Format	Backup Method	Backup in Case of Environmental Exceptions	Stable Log Backup
Product asset	Configuration file	File	Manual backup	Y	N
	CT update module of the self version management function	File	Manual backup	Y	N
User asset	Management information	Database	Backup Tool (GUI/Command)	Y	Y
	Log information (not including command logs)	Database	Backup Tool (GUI/Command)	Y	Y
	Log information (command logs)	File	Backup Tool (GUI/Command)	Y	Y
	Attached data	File	Manual backup	Y	O
	E-mail contents	File	Manual backup	Y	O
	Configuration Change Logs	Database	Command (DTKSTCV.EXE and DTKDELST.EXE)	Y	Y

Classification	Backup Target	Format	Backup Method	Backup in Case of Environmental Exceptions	Stable Log Backup
	iOS management database	Database	Backup tool (command)	Y	Y

Legend: Y=back up, N=do not back up, O=optional

3.1.1.1 Product Assets

This section describes the data to be backed up and restored as product assets and the backup methods.

Configuration Files

The following table describes the configuration files that require backup and restoration. In addition, if the OS installation folder changes, it is possible that the file saving folders are different from those listed in the table. (In the following table, it is assumed that the OS is installed on drive C.)

No.	Backup Target	Content and Target Folder
1	SWCTVerSettings.ini	Configuration file of the self version management function
		This file is saved to the Master Management Server and Management Server.
		For Windows Server(R) 2012: C:\Windows\SYSWOW64
		For Windows Server(R) 2008: C:\Windows\system32
		For Windows Server(R) 2008 64-bit edition and Windows Server(R) 2008 R2: C:\Windows\SYSWOW64
		For Windows Server(R) 2003: C:\Windows\system32
		For Windows Server(R) 2003 x64 edition and Windows Server(R) 2003 R2, x64 edition: C:\Windows\SYSWOW64
2	SWCTVerSettings2.ini	Configuration file of the self version management function
		This file is saved to the Master Management Server and Management Server only when the self version upgrade function is used to perform version or edition upgrade.
		For Windows Server(R) 2012: C:\Windows\SYSWOW64
		For Windows Server(R) 2008: C:\Windows\system32
		For Windows Server(R) 2008 64-bit edition and Windows Server(R) 2008 R2: C:\Windows\SYSWOW64
		For Windows Server(R) 2003: C:\Windows\system32
		For Windows Server(R) 2003 x64 and Windows Server(R) 2003 R2, x64 edition: C:\Windows\SYSWOW64
3	SWDB.ini	Configuration file of the Systemwalker Desktop Keeper database connection
		For Windows Server(R) 2012: C:\Windows
		For Windows Server(R) 2008: C:\Windows
		For Windows Server(R) 2003: C:\Windows
4	SWMailSettings.ini	Configuration file of the administrator notification function (E-mail notification)
		For Windows Server(R) 2012: C:\Windows
		For Windows Server(R) 2008: C:\Windows
		For Windows Server(R) 2003: C:\Windows

No.	Backup Target	Content and Target Folder
5	SWEventViewer.ini	Configuration file of the administrator notification function (event log) This file is saved to the Master Management Server or Management Server. For Windows Server(R) 2012: C:\Windows\SYSWOW64 For Windows Server(R) 2008: C:\Windows\system32 For Windows Server(R) 2008 64-bit edition and Windows Server(R) 2008 R2: C:\Windows\SYSWOW64 For Windows Server(R) 2003: C:\Windows\system32 For Windows Server(R) 2003 x64 edition and Windows Server(R) 2003 R2, x64 edition: C:\Windows\SYSWOW64
6	TRANS_SETTING.ini	Configuration file of the data transmission command This file is saved to the Master Management Server or Management Server. <Management Server installation folder>\LogAnalyzer\TRANS
7	taskmng.ini	Configuration file of the Web console This file is saved to the Master Management Server or Management Server. IIS folder\Scripts\DTK
8	swdtkenv.ini	Configuration file for database construction This file is saved to the Master Management Server or Management Server. <Installation target folder of the database-related files>\DBEnv\Env When newly installing Management Server V15.1.0, the installation folder for database-related files is *mgmtServerInstallFolder*\DB.
9	DTKTaskRegist.ini	Configuration file of the statistical command This file is saved to the Master Management Server or Management Server. <Management Server installation folder>\Server\LogCount
10	mail.ini	E-mail configuration file This file is saved to the Master Management Server or Management Server. <Management Server installation folder>\Server\LogCount
11	LA_connect_Info.csv	Configuration file of the Log Analyzer This file is saved to the Master Management Server or Management Server. <Management Server installation folder>\LogAnalyzer\TRANS
12	CONV_SETTING.ini	Data import configuration file. This file is stored under the Log Analyzer Server folder. *logAnalyzerServerInstallFolder*\bin\SWDTLAENV

[Backup and restoration methods]

Backup:

Back up the files saved at the locations described in the preceding table.

Restoration:

Save the backup files to the locations described in the preceding table.

For No.7, perform the following steps to edit the file after saving the file:

1. Open the file by using the text editor (notepad).

2. If the **Update** section contains the "Flag=0" statement, change the statement to "Flag=1". If the original statement is "Flag=1," do not change it.

3. Save the file and exit the text editor.

CT Update Module of the Self Version Management Function

The following table describes the target folder for saving the CT update module of the self version management function. When the default value of **Target for Saving CT Upload Module** is changed, backup the modification target.

No.	Backup Target	Target Folder
1	All the contents in the UpdateModule folder.	Target folder for saving the CT upload module of the self version management function, specified by the Server Settings Tool of the Master Management Server or Management Server Default value: C:\DTK\UpdateModule

[Backup and restoration methods]

Backup:

Back up all the contents in the backup target folder.

Restoration:

Save all the contents in the backup folder to the location described in the preceding table.

3.1.1.2 User Assets

This section describes the data to be backed up and restored as user assets and the backup methods.

Management Information

The following table describes the management information that requires backup and restoration.

No.	Backup Target (Table Name)	Content
1	LEVELTARGET	Level target information
2	LEVELCOMPOSITION	Level structure information
3	PRINTPERMISSION	Printing permission
4	LOGINGUARD	Logon prohibition
5	STARTUPGUARD	Application startup prohibition
6	MAILATTACHSET	E-mail attachment prohibition
7	USERINFO	User information
8	NODEINFO	Node information
9	PHYSICALNODELIST	Physical node list
10	SETTINGS	Configuration value
11	SETTINGSLOG	Configuration change log
12	FILEACC_ACQUIREPROCESS	Registered process for file operation log
13	FILEACC_ACQUIREEXTENSION	Registered extension for file operation log
14	USERPOLICYINFO	User policy information
15	LOGONUSER_PRINTPERMISSION	Registered Printing permission by user
16	LOGONUSER_STARTUPGUARD	Registered Application startup prohibition by user
17	USERMAILATTACHSET	Registered E-mail attachment prohibition by user
18	LOGONUSER_SETTINGSLOG	Registered Configuration change log by user

No.	Backup Target (Table Name)	Content
19	WINDOWTITLELOGFILTER	Filtering conditions of window title logs
20	LOGONUSER_WINDOWTITLELOGFILTER	Registered Filtering conditions of window title logs by user
21	WINDOWCAPTUREFILTER	Screen capture conditions
22	LOGONUSER_WINDOWCAPTUREFILTER	Registered Screen capture conditions by user
23	EXCLUSIONCONTROL	Exclusion control information
24	DOMAINSETTINGS	Domain setting information
25	TARGET_CONTROL	Setting information of CT Department administrator
26	LOGONUSER_LEVELCOMPOSITION	User level configuration information
27	LOGONUSER_CONTROL	Setting information of user Department administrator
28	USBMASTER	USB setting information
29	POLICYTABLE	Common policy
30	DTK_AUDIT_SETTING	Setting information of status window
31	DTK_TOTAL_ALERTLOG	Number of abnormal operations
32	DTK_ALERT_LIST	Abnormality list
33	DTK_ALERTPC_LIST	Abnormal PC list
34	DTK_PRINTER_TARGETMASTER	Target management for all-in-one PC
35	DTK_PRINTER_PRINTUSERMASTER	Operator management for all-in-one PC
36	DTK_PRINTER_PAPERNUM_BASIC	Aggregate number of pages for all-in-one printer
37	All tables of the iOS management database	iOS management database

[Backup and restoration methods]

Backup:

Use the Backup Tool (GUI) or backup commands. For details, see "3.1.2 Back Up User Assets".

When managing iOS devices, use the backup commands. The backup tool (GUI) does not back up iOS management databases.
When Management Server or Master Management Server for Systemwalker Desktop Keeper coexists with CS for Systemwalker Desktop Patrol, and iOS devices are being managed by both products, back up the management information of Systemwalker Desktop Patrol.

Restoration:

Use the Restoration Tool (GUI). For details, see "3.1.3 Restoring User Assets".

When managing iOS devices, execute the restore command for iOS management databases in addition to the Restoration Tool (GUI) to recover iOS management databases.
When Management Server or Master Management Server for Systemwalker Desktop Keeper coexists with CS for Systemwalker Desktop Patrol, and iOS devices are being managed by both products, restore the management information of Systemwalker Desktop Patrol.

Log Information (Not Including Command logs)

The following table describes the log information that requires backup and restoration.

No.	Backup Target (Table Name)	Content
1	COMMONLOG1	Common log 1 - Application startup log - Application termination log - E-mail sending log - E-mail sending interruption log

No.	Backup Target (Table Name)	Content
		- E-mail attachment prohibition log (note 1)
		- PrintScreen Key Prohibition Log
		- PrintScreen key operation log
		- Clipboard operation prohibition log
		- Clipboard operation log
2	COMMONLOG2	Common log 2
		- Window Title Obtaining Log
		- Printing prohibition log
		- Command log (including only the index information)
		- Linkage application log
3	COMMONLOG3	Common log 3
		- E-mail attachment prohibition log (note 1)
		- Window Title Obtaining Log (with URL)
		- Logs of logon, logoff, PC startup, PC shutdown, PC hibernate, PC recovery, PC connection, and PC disconnection
		- Device Configuration Change Log (note 2)
		- Web operation log
		- Web operation prohibition log
		- FTP operation log
		- FTP operation prohibition log
		- Application usage log (smart device)
		- SD card mount/unmount log (smart device)
		- Bluetooth connection log (smart device)
		- SIM card mount/unmount log (smart device)
		- Wi-Fi connection log (smart device)
		- Web access log (smart device)
		- Incoming/outgoing calls log (smart device)
		- Application configuration change log (smart device)
		- Application usage prohibition (smart device)
		- Bluetooth connection prohibition (smart device)
		- Wi-Fi connection prohibition (smart device)
4	STARTUPGUARDLOG	Application startup prohibition log
5	LOGINGUARDLOG	Logon prohibition log
6	PRINTLOG	Printing operation log
7	FILEBRINGOUTLOG	File export log
8	LOGKEYWORDS	Keywords for log searching
9	FILEACCESSLOG	File operation log
10	SESSIONMANAGE	Virtual environment connection information

No.	Backup Target (Table Name)	Content
11	USERLIST	Management information for user searching

Note 1:

For the product versions earlier than V13.2.0, the E-mail attachment prohibition logs are saved in COMMONLOG3. For the product versions later than V14.2.0, the E-mail attachment prohibition logs are saved in COMMONLOG1, or they are saved in COMMONLOG3 under the following condition:

The V12.0L20-V13.0.0 interchangeable mode is used.

Note 2:

For the product versions earlier than V13, the device configuration change logs are saved in COMMONLOG1.

[Backup and restoration methods]

Backup:

Use the Backup Tool (GUI) or backup commands. For details, see "3.1.2 Back Up User Assets".

Restoration:

Use the Restoration Tool (GUI). For details, see "3.1.3 Restoring User Assets".

Log Information (Command logs)

The following table describes the target folder for saving command logs. When the default value of **Target for Saving Command Line and Logs** is changed, backup the modification target.

No.	Backup Target	Target Folder
1	All the contents in the PromptLog folder	Target folder for saving the command lines and logs, specified by the Server Settings Tool of the Master Management Server or Management Server (Default value: C:\DTK\PromptLog)

[Backup and restoration methods]

Backup:

Use the Backup Tool (GUI) or backup commands. For details, see "3.1.2 Back Up User Assets".

Restoration:

Use the Restoration Tool (GUI). For details, see "3.1.3 Restoring User Assets".

Attached Data

The following table describes the target folder for saving the attached data. When the default value of **Target for Saving Attached Data** is changed, backup the modification target.

No.	Backup Target	Target Folder
1	All the contents in the ScreenCapture folder	Target folder for saving the attached data, specified by the Server Settings Tool of the Master Management Server or Management Server (Default value: C:\DTK\ScreenCapture) The attached data is saved in [Folder of Day Unit]-[Folder of CT Unit] under the preceding target folder.

[Backup and restoration methods]

Backup:

Back up all the contents in the backup target folder.

Back up the attached data separately as required. In addition, the attached data cannot be deleted even by the Backup Tool or backup commands.

Restoration:

Save all the contents under the backup folder to the location described in the preceding table.

E-mail Contents

The following table describes the target folder for saving the E-mail contents. When the default value of **Target for Saving E-mail Content** is changed, backup the modification target.

No.	Backup Target	Target Folder
1	All the contents in the MainContents folder	Target folder for saving the E-mail contents, specified by the Server Settings Tool of the Master Management Server or Management Server (Default value: C:\DTK\MailContents) The E-mail contents are saved in [Folder of Day Unit]-[Folder of CT Unit] under the preceding target folder.

[Backup and restoration methods]

Backup:

Back up all the contents in the backup target folder.

Back up the E-mail contents separately as required. In addition, the E-mail contents cannot be deleted even by the Backup Tool or backup commands.

Restoration:

Save all the contents under the backup folder to the location described in the preceding table.

Trouble Investigation Data

The following table describes the target folder for saving the trouble investigation data. When the default value of **Target for Saving Trouble Investigation Data** is changed, backup the modification target.

No.	Backup Target	Target Folder
1	All the contents in the CTQSSSave folder	Target folder for saving the trouble investigation data, specified by the Server Settings Tool of the Master Management Server or Management Server (Default value: C:\DTK\CTQSSSave) The trouble investigation data is saved in [Folder of Day Unit]-[Folder of CT Unit] under the preceding target folder.

[Backup and restoration methods]

Backup:

Back up all the contents in the backup target folder.

Back up the trouble investigation data separately as required. In addition, the trouble investigation data cannot be deleted even by the Backup Tool or backup commands.

Restoration:

Save all the contents under the backup folder to the location described in the preceding table.

3.1.2 Back Up User Assets

This product provides the following three backup functions for user assets.

Backup Tool (GUI)

Set backup conditions through a GUI.

This command does not back up iOS management databases.

Backup tool (automatic)

Use the GUI window to configure the automatic backup conditions, so that backup will be performed automatically.

Backup Commands

Set backup conditions through command parameters. The commands themselves do not have a scheduling function.

Point

Adding the backup commands to the Task Scheduler will facilitate the command execution.

After being incorporated in a scheduled batch file, the backup commands can be executed at the specified time.

The Backup Tool (GUI) and backup commands can be used to perform the following operations:

- Back up data.

  Data backup is a precaution against a hard disk failure or file corruption. In addition, the backup data can be used to re-construct the database. The data that can be backed up is classified into the following two types:

  - Management information

  - Log information (log data in the database and command logs)

  For details about the information that can be backed up, see "3.1.1.2 User Assets".

  The time required for backing up data can be estimated according to the number of logs to be backed up. The estimation is as follows:

  - 7,000 per second (Xeon, 2.0 GHz, 2 GB memory, and RAID1 architecture)

    Note: More time may be consumed, depending on the server performance and RAID architecture.

- Delete data.

  Delete the unnecessary data in the database to prevent the database from running out of space.

  In addition, the time required for deleting data can be estimated according to the number of logs to be deleted. The purpose is as follows:

  - 200 per second (Xeon, 2.0 GHz, 2 GB memory, and RAID1 architecture)

    Note: More time may be consumed, depending on the server performance and RAID architecture.

- Output log information (in Log Viewer format).

  Output operation logs and prohibition logs to CSV files in Log Viewer format and view the logs. The information output in Log Viewer format, however, cannot be used for restoration.

  The time required by log information output can be estimated according to the number of logs to be backed up. The estimation is as follows:

  - 2,000 per second (Xeon, 2.0 GHz, 2 GB memory, and RAID1 architecture)

    Note: More time may be consumed, depending on the server performance and RAID architecture.

- Set scheduled tasks for deleting or backing up data, which is supported only by the Backup Tool (GUI).

  Set scheduled tasks so that data can be automatically backed up or deleted. The scheduled tasks will be added to the Task Scheduler. The following operations can be automatically performed:

  - Back up data (management information, log information, and configuration change logs).

  - Delete data (log information and configuration change logs).

  - Output log information (in Log Viewer format).

  - When an error occurs during automatic operation execution, an E-mail for notification will be sent to the administrator.
    Select **Server Settings Tool** > **Administrator Notification Settings** > **E-mail Sending Settings**, and then set the E-mail address for notification.

The operational status of the Backup Tool (GUI) or backup commands will be output to event logs.

The Backup Tool (GUI) and the backup commands can back up the user assets (including management information and log information) except the attached data, but they do not back up the information about programs and settings information of the product. Use other software to regularly back up all the information.

3.1.2.1 Using the Backup Tool (GUI)

This section describes how to back up the user assets by using the Backup Tool (GUI).

🔰 Note

Notes on using the Backup Tool (GUI)

[Available space on the output target disk]

Ensure that there is sufficient available space on the disk specified as the output target disk for the backup files. If the disk space is insufficient to save a large amount of data, correspondingly narrow the date range of the targets to be saved.

[Available space on the installation target disk of the database-related files]

Ensure that there is sufficient available space on the installation target disk of the database-related files. When a large number of logs are to be backed up, there must be enough available space on the installation target disk of the database-related files. For details about disk capacity requirements, refer to "Operation Environment" in the *Systemwalker Desktop Keeper User's Guide*.

[Back up and restore on each server]

In a 3-level system architecture, each Management Server is installed with a database; therefore, perform the backup or restoration operation on each Master Management Server and Management Server separately.

[Data conversion]

The Backup Tool may convert data in a log and then output the converted log to a CSV file. The following data is converted:

- Tab, carriage return, line feed replaced with halfwidth space

- Double quotation mark (") escaped with double quotation mark ("")

[Attached data processing]

The Backup Tool/backup commands do not back up the attached data (including the screen capture data and backup original files). In addition, the attached data cannot be deleted even by the log deletion operation. Refer to "Attached Data" in "3.1.1 Targets and Methods" for details on backing up and restoring attached data.

[Email contents data processing]

Email contents data (email body, attachments) is not backed up when using the backup tool or backup commands. Also, even if you delete logs, the email contents data will not be deleted. Refer to "E-mail Contents" in "3.1.1 Targets and Methods" for details on backing up and restoring email contents data.

🅿 Point

Logon history of the Backup Tool (GUI)

The logon history of the Backup Tool (GUI) will be output to event logs (application).

Preparations

When backing up data for restoration, record the following setting information. (Obtain the collected bitmaps and notes of the windows.)

Target	Window to Be Backed Up
Management console	**Terminal Operation Settings**
Server Settings Tool	**System Settings**
	Setting of Active Directory Linkage

Target	Window to Be Backed Up
	Note: when the Active Directory linkage function is used
	Administrator Notification Settings
	Management Server Settings
	Trace Settings
	Self Version Upgrade Settings for Folder/CT

Perform the following steps to display the **Terminal Operation Settings** window:

1. Start **Management Console**.

2. Select **Terminal Operation Settings** from the **Operation Settings** menu.

   The **Terminal Operation Settings** window is displayed.

For details about how to display the windows of the Server Settings Tool, refer to "2.3.6 Set Environment of Management Server/Master Management Server".

🛈 Note

. . . .

Properly store the recorded information.

The preceding setting information cannot be backed up using the Backup Tool. After restoring data, it is necessary to restore the terminal operation settings to the status before backup; therefore, ensure that the information recorded along with the backup data is properly stored.

. . . .

Start Backup

The procedure for using the Backup Tool is as follows:

1. When managing Android or iOS devices, use SDSVService.bat (start/stop service of Smart Device Relay Server command) to stop 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 on the command.

2. Log on to the Windows OS as a user of the Administrators group or Domain Admins group.

3. Select **All Programs** > **Systemwalker Desktop Keeper** > **Server** > **Backup Tool** from the **Start**/**Apps** menu on the PC installed with the Master Management Server or Management Server.

   The **Systemwalker Desktop Keeper - Backup Tool** window is displayed.

4. Enter the user ID (granted with the authority to back up and restore information) and password registered in the Server Settings Tool, and then click **OK**. (The user ID and password of the Primary Administrator can also be used for logon.)

The **Backup Tool** window is displayed.
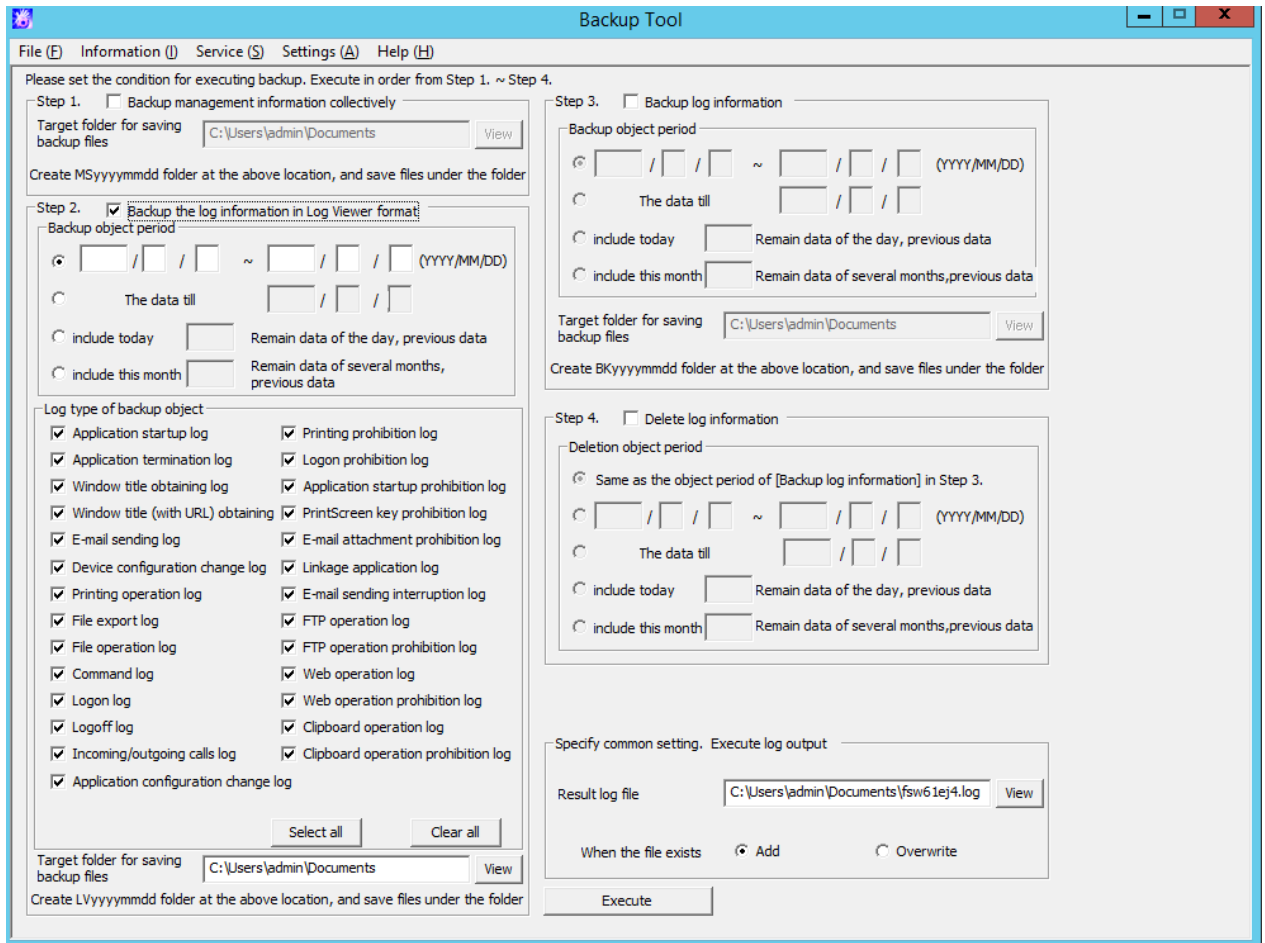
The following table describes the menu bar in the **Backup Tool** window.

Menu Bar		Function Summary
File	Exit	Exit the Backup Tool.
Information	Confirm number of tables	Display the number of records in the log information table in the database.
Service	Conform service status	Display the operational status of the "Level Control Service" and "Server Service" on the target server.
	Start service	Start the "Level Control Service" and "Server Service" on the target server.
	Stop service	Stop the "Level Control Service" and "Server Service" on the target server.
Settings	Set extraction item	When backing up the logs in the Log Viewer format, backing up the log table and deleting the records in the log table, enter the date related to data item extraction and deletion. - Process according to Client Occurrence Date and Time (Standard)

Menu Bar		Function Summary
		- Process according to Server Saving Date and Time
	Automatic backup settings	Display the Automatic Backup Settings window.
	Backup tool trace	**No**	Do not collect the traces of the Backup Tool.
		Summary	Collect the traces of the Backup Tool in summary mode.
		Details	Collect the traces of the Backup Tool in details mode.
Help	**Online Help**	Display the online help manual.
	Version Information	Display the copyright information and version information.

5. Before backing up the "management information" and "log information" by using the Backup Tool, it's necessary to stop the "Level Control Service" and "Server Service" on the target server.

   a. Select **Stop Service** from the **Service** menu. A confirmation window is displayed. Click **OK** in the window to stop the services.

   b. The operation result window is displayed.

6. For first-time backup, set the data extraction method for log information backup and deletion. Select **Extraction item settings** from the **Settings** menu.

   The **Extraction item settings** window is displayed.

   The extraction item settings specify the time for log backup and deletion. This can be the time that logs were generated on the client or the time that logs were stored on the server.

   - **Process in the client occurrence date and time (standard):** Select this option when you want to operate based on the time that logs were generated on the client.

   - **Process in the server saving date and time:** Select this option when you want to operate based on the time that logs were stored on the server.

7. To extract logs according to the time that logs were generated on the client (CT), select **Process in the client occurrence date and time (standard)**. To extract logs according to the time that logs were stored on the server, select **Process in the server saving date and time**. Then, click **Set**.

Note

Do not change the extraction item settings after they are put into use.

Do not change the extraction item settings after they are put into use. Otherwise, certain log data may fail to be backed up. If a change is required, make the change after the preceding data is backed up.

8. In the **Backup Tool** window, enter the information described in steps 1 to 4.

   Step 1 Back up management information collectively

Item Name	Description
Backup management information collectively	Select it when backing up the management information.
Target folder for saving backup files	Select a folder for saving the backup management information. There are two methods for selecting such a folder: - Enter the absolute path of a folder. - Enter the absolute path of a folder for saving the output management information.

Item Name	Description
	- Click **Browse**.
	- The **Viewing Folder** window is displayed. Select a folder for saving the output management information and then click **Open**.
	An absolute path can contain a maximum of 189 single-byte characters (94 fullwidth characters). The folder name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".
	The backup management information is saved in the MSyyyymmdd sub-folder of the specified folder. (yyyymmdd indicates the backup execution date.)
	If multiple backups are executed to the same folder on the same date, a unique sequential number enclosed by parentheses will be appended to the subfolder name. The first backup will be saved in MSyyyymmdd, the second one in MSyyyymmdd(1), the third one in MSyyyymmdd(2), and so on.

Step 2 Back up the log information in Log Viewer format

Item Name	Description
Backup the log information in Log Viewer format	Select it when backing up the log information in the format that enables the logs to be viewed in the Log Viewer.
Backup object period	There are four options for specifying a backup target period:
	- Back up the logs later than the specified period.
	- The entered value of year ranges from 2000 to 9999, the value of month ranges from 1 to 12, and the value of date ranges from 1 to 31. (The period must end before or on the current date.)
	- Back up the logs earlier than the specified date.
	- The entered value of year ranges from 2000 to 9999, the value of month ranges from 1 to 12, and the value of date ranges from 1 to 31. (The date can be earlier than or equal to the current date.)
	- Back up the logs earlier than the specified number of days, counting from the current day.
	- The entered value ranges from 0 to 999.
	- If the entered value is 1, the logs earlier than the end of the last day will be backed up. If the entered value is 0, the logs earlier than the present moment will be backed up.
	- Back up the logs earlier than the specified number of months, counting from the current month.
	- The entered value ranges from 0 to 99.
	- If the entered value is 1, the logs earlier than the end of the last month will be backed up. If the entered value is 0, the logs earlier than the present moment will be backed up.

Item Name	Description
Log type of backup target	Select the type of logs to be backed up.

Target folder for saving backup files	Select a folder for saving the backup log information. There are two methods for selecting such a folder.
	
	  - Enter the absolute path of a folder.
	
	  - Enter the absolute path of a folder for saving the output logs.
	
	  - Click **Browse**.
	
	  - The **Viewing Folder** window is displayed. Select a folder for saving the output log information and then click **OK**.
	
	An absolute path can contain a maximum of 189 single-byte characters (94 fullwidth characters). The folder name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".
	
	The backup logs are saved in the LVyyyymmdd sub-folder of the specified folder. (yyyymmdd indicates the backup execution date.)
	
	In addition, if the backup operation is performed for more than two times in a same day, a number is automatically added to the subfolder name, for example, (1).
	
	For the second backup operation: LVyyyymmdd(1)
	
	For the third backup operation: LVyyyymmdd(2)
	
	For the fourth backup operation: LVyyyymmdd(3)
	
	(The subsequent number can be deduced like this.)

Step 3 Back up log information

Item Name	Description
Backup log information	Select it when backing up log information.

Backup object period	There are four options for specifying a backup target period.
	
	  - Back up the logs later than the specified period.
	
	    - The entered value of year ranges from 2000 to 9999, the value of month ranges from 1 to 12, and the value of date ranges from 1 to 31. (The period must end before or on the current date.)
	
	  - Back up the logs earlier than the specified date.
	
	    - The entered value of year ranges from 2000 to 9999, the value of month ranges from 1 to 12, and the value of date ranges from 1 to 31. (The date can be earlier than or equal to the current date.)
	
	  - Back up the logs earlier than the specified number of days, counting from the current day.
	
	    - The entered value ranges from 0 to 999.
	
	    - If the entered value is 1, the logs earlier than the end of the last day will be backed up. If the entered value is 0, the logs earlier than the present moment will be backed up.

Item Name	Description
	- Back up the logs earlier than the specified number of months, counting from the current month.
	- The entered value ranges from 0 to 99.
	- If the entered value is 1, the logs earlier than the end of the last month will be backed up. If the entered value is 0, the logs earlier than the present moment will be backed up.
Target folder for saving backup files	Select a folder for saving the backup log information. There are two methods for selecting such a folder:
	- Enter the absolute path of a folder.
	- Enter the absolute path of a folder for saving the output logs.
	- Click **Browse**.
	- The **Viewing Folder** window is displayed. Select a folder for saving the output log information and then click **OK**.
	An absolute path can contain a maximum of 189 single-byte characters (94 fullwidth characters). The folder name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".
	The backup logs are saved in the BKyyyymmdd sub-folder of the specified folder. (yyyymmdd indicates the backup execution date.)
	In addition, if the backup operation is performed for more than two times in a same day, a number is automatically added to the subfolder name, for example, (1).
	For the second backup operation: BKyyyymmdd(1)
	For the third backup operation: BKyyyymmdd(2)
	For the fourth backup operation: BKyyyymmdd(3)
	(The subsequent number can be deduced like this.)

Step 4 Delete log information

Item Name	Description
Delete log information	Select it when deleting the log information.
Delete object period	There are five options for specifying a delete target period.
	- Delete the logs of the backup target period specified in step 3 "Back up log information".
	- Delete the logs of the specified period.
	- The entered value of year ranges from 2000 to 9999, the value of month ranges from 1 to 12, and the value of date ranges from 1 to 31. (The period must end before or on the current date.)
	- Delete the logs earlier than the specified date.
	- The entered value of year ranges from 2000 to 9999, the value of month ranges from 1 to 12, and the value

Item Name	Description
	of date ranges from 1 to 31. (The date can be earlier than or equal to the current date.)
	- Delete the logs earlier than the number of days, counting from the current day.
	- The entered value ranges from 0 to 999.
	- If the entered value is 1, the logs earlier than the end of the last day will be deleted. If the entered value is 0, the logs earlier than the present moment will be deleted.
	- Delete the logs earlier than the number of months, counting from the current month.
	- The entered value ranges from 0 to 99.
	- If the entered value is 1, the logs earlier than the end of the last month will be deleted. If the entered value is 0, the logs earlier than the present moment will be deleted.

9. Enter the common settings in the **Backup Tool** window.

   Specify common setting. Execute log output

Item Name	Description
Result log file	Specify the file for saving the execution results of the Backup Tool. There are two methods for selecting such a file: - Enter the absolute path of a file. - Enter the absolute path of a file for saving the execution results. - Click **Browse**. - The **Open File** window is displayed. Select the folder for saving the result log file, enter the file name, and then click **Open**. An absolute path can contain a maximum of 255 single-byte characters (127 fullwidth characters). The file name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".
When the file exists	Select the processing operation to be performed when the result log file exists at the location specified by **Result Log File**. - Add - Add a new result log to the end of the result log file if the file exists at the location specified by **Result Log File**. - Overwrite - Overwrite the last result log in the result log file if the file exists at the location specified by **Result Log File**.

10. After completing all the settings, click **Execute**.

    In the confirmation window, click **OK**.

Note

. . . .

If "Backup Target Period" and "Delete Target Period" are set to different values:

If "Backup Target Period" and "Delete Target Period" are set to different values on the Backup Tool, the Backup Tool displays the following message informing you that this operation may delete the files that are not backed up and prompting you to check whether the settings are correct.

```
[BKCI-SEL001] The [Backup Target Period] and [Delete Target Period] are set to different values.
Please check whether the target periods are correctly set.
Are you sure to continue?
```

. . . .

11. The **Backup Condition** window is displayed and the backup process starts.

12. When the backup process is completed successfully, the process completion window is displayed. Click **OK** in the window.

13. After confirming the execution status, click **Close**.
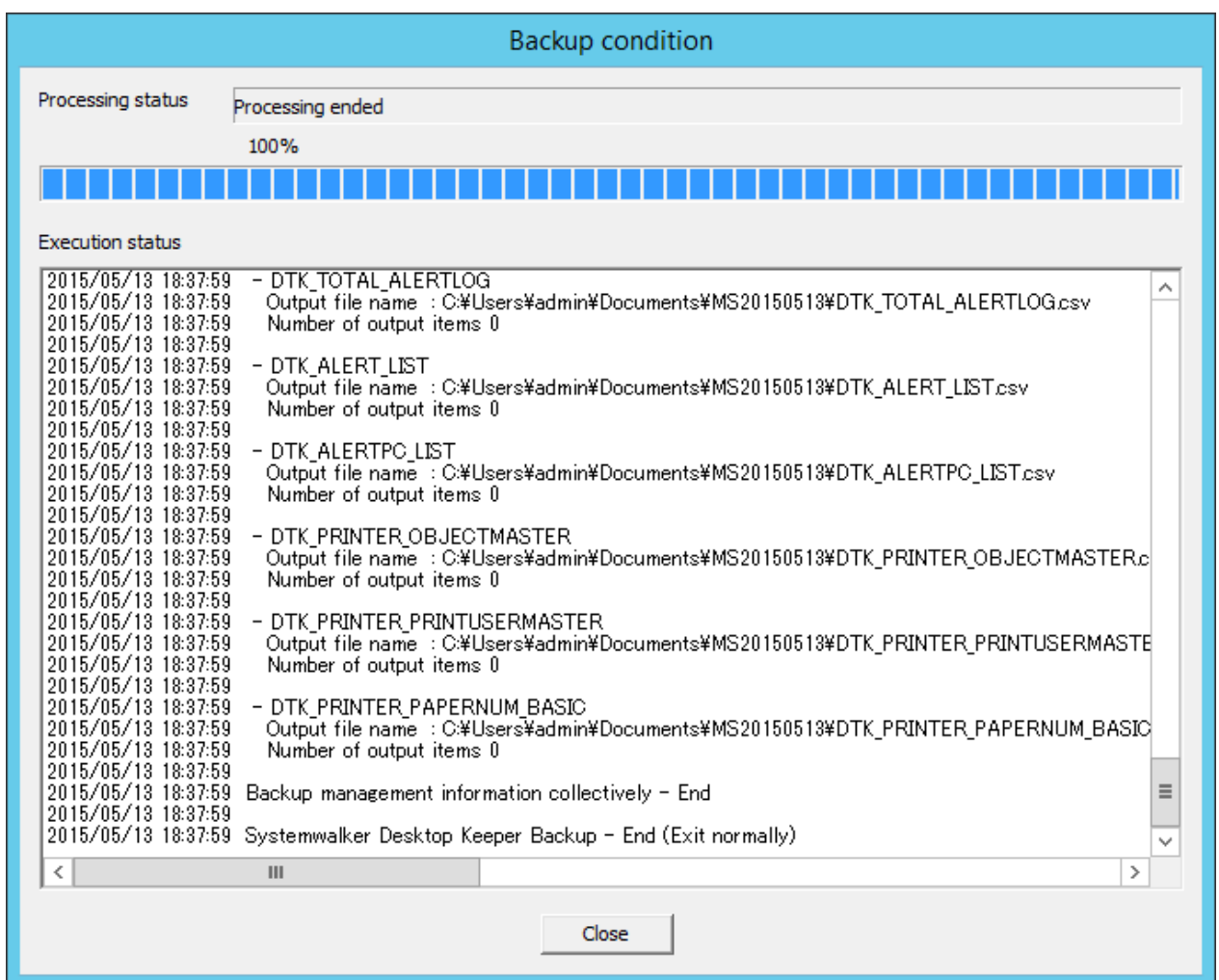
14. Start the stopped "Level Control Service" and "Server Service". Select **Start Service** from the **Service** menu. The service startup confirmation window is displayed. Click **OK** in the window to start the services.

15. The operation result window is displayed. Click **OK** in the window.

16. When managing Android or iOS devices, use SDSVService.bat (start/stop service of Smart Device Relay Server command) 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 on the command.

Confirm Service Status

During the backup process, the Backup Tool must stop the Systemwalker Desktop Keeper services on the connected Management Server. Therefore, it is necessary to confirm the service status. This part describes how to confirm the status of the Systemwalker Desktop Keeper services by using the Backup Tool.

1. Select **Confirm Service Status** from the **Service** menu.

   The **Confirm Service Status** window is displayed.

2. Click **OK** after confirmation.

Confirm the Number of Records in the Log Information Table

This part describes how to use the Backup Tool to view the number of records in the log information table that are backup targets.

1. Select **Confirm Number of Tables** from the **Information** menu.
   The **Confirm Number of Tables** window is displayed. For details about the contents in the table, refer to "Log Information (Not Including Command logs)" in "3.1.1.2 User Assets".

2. Enter a target period.

   - The value of year ranges from 2000 to 9999.

   - The value of month ranges from 1 to 12.

   - The value of day ranges from 1 to 31.

3. Click **Confirm the number of tables**.
   The number of logs is displayed in each table.
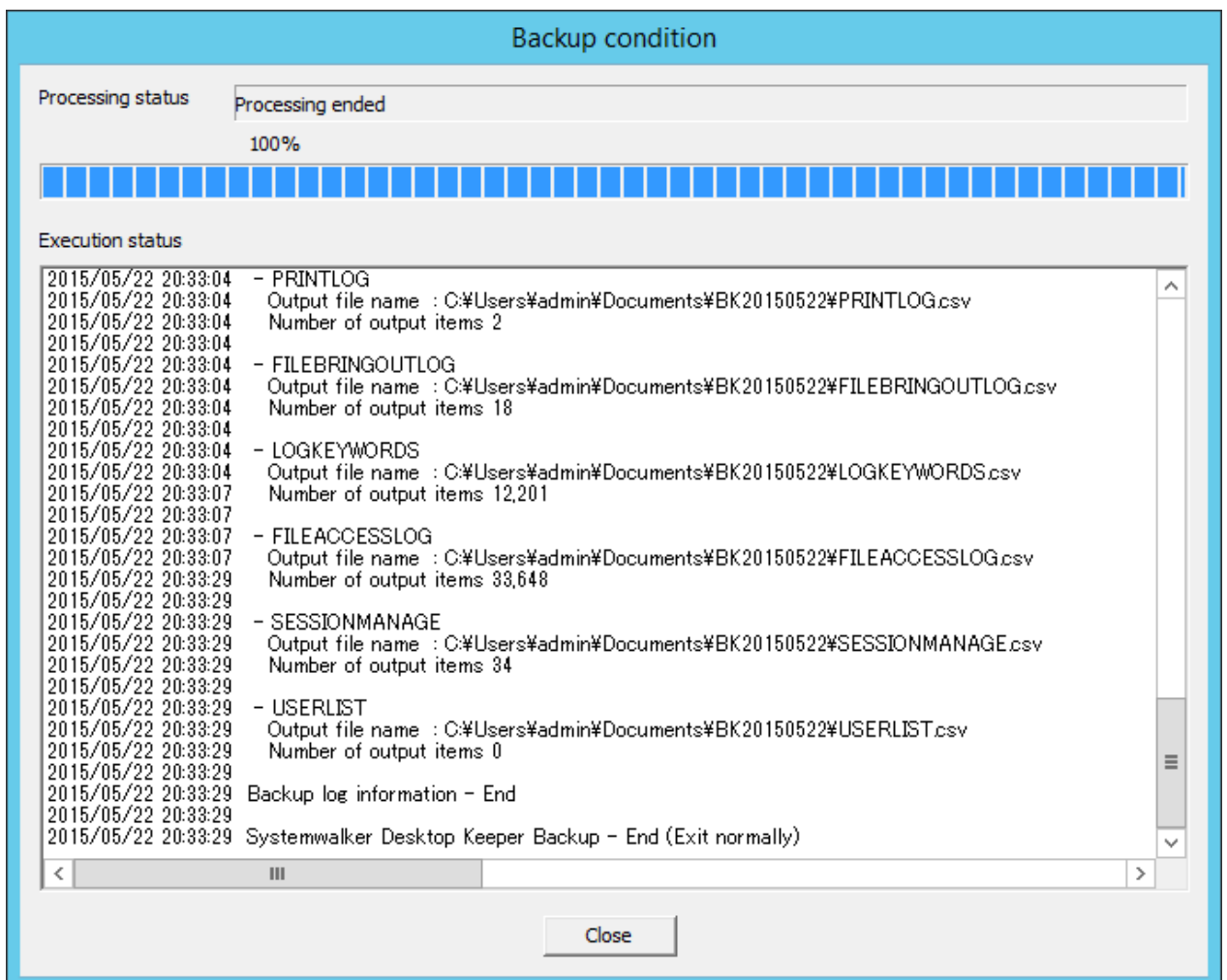
4. Click **Close** after confirmation.

Exit the Backup Tool

1. To exit the Backup Tool, select **Exit** from the **File** menu.

2. The exit window is displayed.
   Select whether to save the conditions specified in the Backup Tool window. Click **Yes** to exit with the conditions saved, click **No** to exit without saving the conditions, or click **Cancel** to cancel the exiting operation.
   In addition, the menu settings (**Extraction Item Settings** and **Settings of Debugging Trace**) are saved when they are set.

Back up user assets

Refer to "3.1.1.2 User Assets" for details.

3.1.2.2 Automatic Data Backup and Deletion

Note

. . . .

Time required by automatic data backup and deletion
The automatic data backup and deletion function will back up the management information, log information in Log Viewer format, and log information, and delete the log information.
Therefore, execution of this function may take some time.

. . . .

This section describes how to set the automatic data backup and deletion function by using the Backup Tool (GUI).
Configure this if the backup and deletion settings were not configured during creation of the Operation Database.
Automatic backup and deletion are registered to Task Scheduler in Windows.

1. Log on the Windows OS as a user of the Administrators group or Domain Admins group.

2. Select **All Programs** > **Systemwalker Desktop Keeper** > **Server** > **Backup Tool** from the **Start**/**Apps** menu on the computer installed with the Master Management Server or Management Server.
   The **Systemwalker Desktop Keeper - Backup Tool** initialization window is displayed.

3. Enter the user ID (granted with the authority to back up and restore information) and password registered in the Server Settings Tool, and then click **OK**. (The user ID and password of the Primary Administrator can also be used for logon.)

The **Backup Tool** window is displayed.
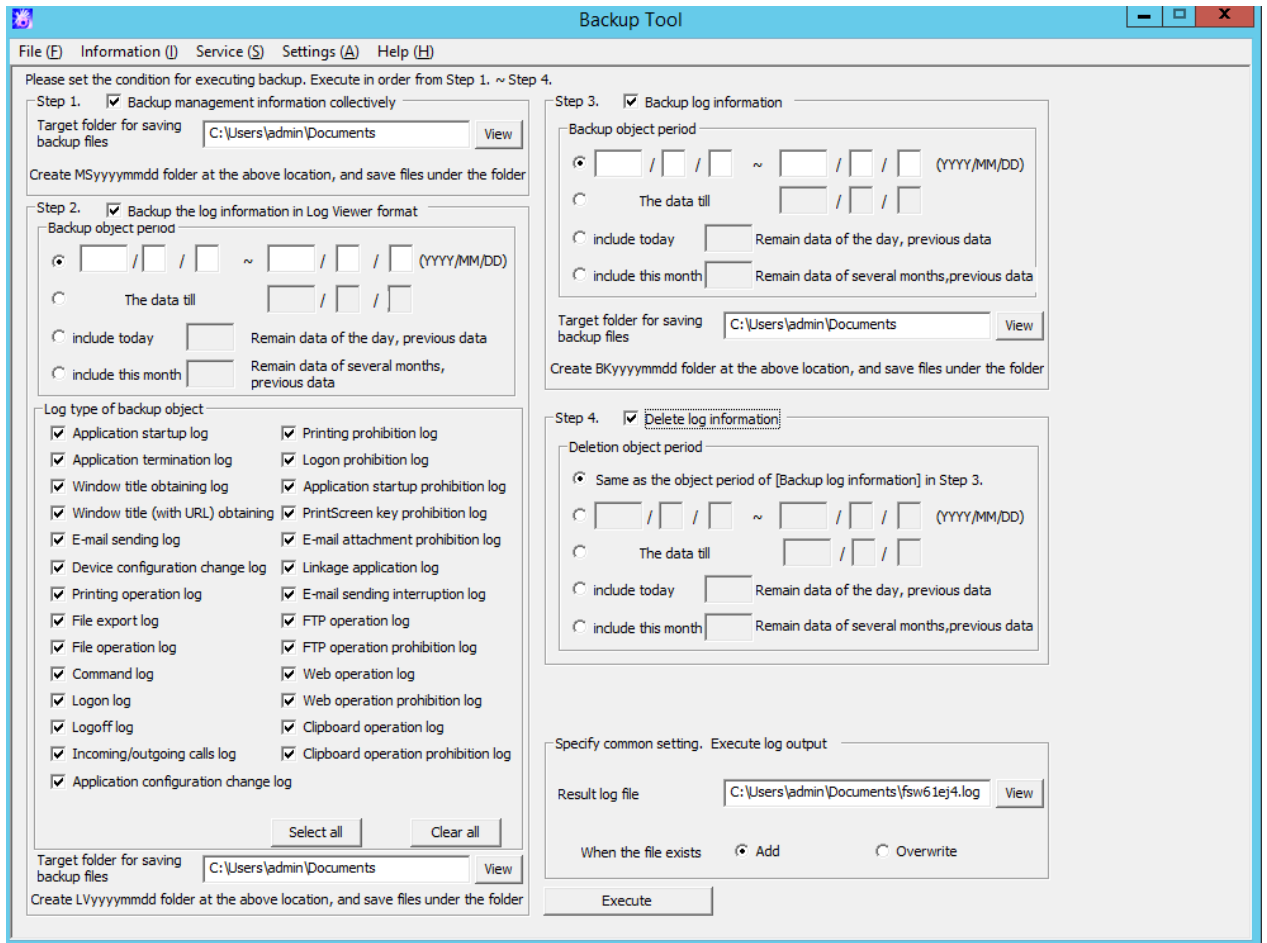
4. Select **Automatic backup settings** from the **Settings** menu.

The **Automatic backup settings** window is displayed.

Target	Window to Backed Up
Automatic backup/deletion	Set whether to automatically back up and delete data. - Execute: Automatically back up and delete data. - Do not execute: Do not automatically back up and delete data. Default value: Yes
Automatic backup/deletion settings	Set an automatic data backup and deletion task.
Task name	Specify the task name registered in the Task Scheduler. The value (DTK_Auto_Backup_Command) is fixed.

Backup target folder	Specify the folder for saving data during automatic backup.
	It can be specified as follows:
	
	- Enter the folder name using the absolute path
	  Enter the full path to the management information backup folder.
	
	- Select from **View**
	  In the **Browse For Folder** window, select the management information backup folder, and then click **OK**.
	
	You can specify up to 94 fullwidth or 189 halfwidth characters and symbols, except for following: \ / : * ? " < > |
	
	The management information will be stored in the subfolder MS *yyyyMmDd* of the specified folder (*yyyyMmDd* is the date of the backup).
	
	If multiple backups are executed to the same folder on the same date, a unique sequential number enclosed by parentheses will be appended to the subfolder name. The first backup will be saved in MS *yyyymmdd*, the second one in MS *yyyymmdd*(1), the third one in MS *yyyymmdd*(2), and so on.

Target		Window to Backed Up
		The initial value is the folder specified during installation.
	Schedule Type	Specify the interval for carrying out an automatic data backup and deletion task. - Day: The task is carried out every day. - Week: The task is carried out once a week. - Month: The task is carried out once a month. **Default value**: Day
	Execution week	After selecting **Weekly** from **Type of Schedule**, select a weekday on which the task is to be carried out. The month and date can be selected. **Default value**: Monthly
	Execution date	After selecting **Monthly** from **Type of Schedule**, enter the exact date on which the task is to be carried out. A value ranging from 1 to 31 can be entered. **Default value**: 1
	Execution start time	Set the time at which an automatic data backup and deletion task is to be carried out. A time ranging from 00:00 to 23:59 can be set. **Default value**: 00:00
	Saving date	Specify the time for saving operation logs. - Day: The value ranges from 1 to 366. - Week: The value ranges from 1 to 54. - Month: The value ranges from 1 to 13. If **Daily** is selected from **Type of Schedule**, only **Day** is available here. If **Weekly** is selected from **Type of Schedule**, **Day** and **Week** are available here. If **Monthly** is selected from **Type of Schedule**, **Day** and **Month** are available here. **Default value**: - Day: 30 - Week: 4 - Month: 1 Operation log data outside the specified period will be deleted. Example: When a period of 30 days is specified, operation log data for the 31st and later days will be deleted

5. Click **Set**.

📒 **Note**

. . . .

If a date 29 or later is specified for **Execution Date**, a message will be displayed indicating that the operation cannot be carried out on an unavailable date.

If the selected date is unavailable in the specified execution month, the automatic data backup and deletion task cannot be carried out. To ensure that the task can be carried out every month, specify a date earlier than 28.

. . . .

 Note

⋯⋯

Edit a scheduled task by using the Task Scheduler of the OS.

After completing the Automatic Backup Settings, create a task named "DTK_Auto_Backup_Command" in the Task Scheduler of the OS. If the task is directly changed, the change cannot be updated in the **Automatic backup settings** window.

In addition, if the settings are changed in the **Automatic backup settings** window after a direct task change, the task change is overwritten by the change of settings in the **Automatic backup settings** window.

The saving period used by the automatic backup feature is calculated not from the date when the log information was created on the client (CT) but from the date when the log information was saved to the Management Server.

Considerations during backup

[Attached data processing]

Attached data (screen capture data, original email storage data) is not backed up when using the backup tool or backup commands. The attached data folder structure is shown below. Back up each folder individually according to your operations. Refer to "2.3.6.9 Set Saving Target Folder" for details on the storage folder for attached data. Note that even if DTKDELR (delete logs command) is executed, the attached data will not be deleted.
[Structure]

Attached data folder

+-Folder by date
+-Folder by CT

Example:

[Email contents data processing]

Email contents data (email body, attachments) is not backed up when using the backup commands. The email contents data folder structure is shown below. Back up each folder individually according to your operations. Refer to "2.3.6.9 Set Saving Target Folder" for details on the storage folder for email contents data.

Note that even if DTKDELR (delete logs command) is executed, the email contents data will not be deleted.
To delete the data, use DTKMLDL.BAT (delete e-mail content command). Refer to "DTKMLDL.BAT (Delete E-mail Content)" in the *Systemwalker Desktop Keeper Reference Manual* for details.
[Structure]

Email contents data folder

+-Folder by date
+-Folder by CT

Example:

⋯⋯
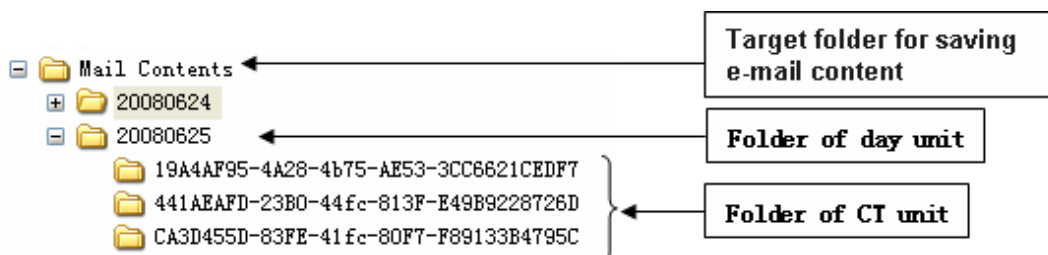
Back up user assets

Refer to "3.1.1.2 User Assets" for details,

3.1.2.3 Using the Backup Commands

This section describes how to process the data in the database by using the backup commands provided by the Systemwalker Desktop Keeper.
The backup commands do not provide the task scheduling function.

🅿 Point

Adding the backup commands to the Task Scheduler will facilitate the command execution.

The Task Scheduler provided by the OS by default or the task scheduling software ARCserve can be used to set scheduled backup tasks. If using the Windows Server(R) 2008 or later, be aware that the user who executes the tasks is required to have administrator privileges.

Note

Notes on using the backup commands

[Level at which this command can be used]

This command can be used in V15.1.0 or later. These commands may fail if they are used in the environment constructed under other versions.

[Current folder during command execution]

When manually running the backup commands, set the current folder of the backup commands to the folder that saves the backup commands.

[Saving folder]
Installation folder of the database-related files\BackupCommand
(when newly installing Management Server V15.1.0, the installation folder for database-related files is *mgmtServerInstallFolder*\DB.)

Example: C:\DTKDB\BackupCommand

Example: C:\Program Files (x86)\Fujitsu\Systemwalker Desktop Keeper\DB\BackupCommand

[Available space on the output target disk]

Ensure that there is sufficient available space on the disk specified as the output target disk for the backup files. If the disk space is insufficient to save a large amount of data, correspondingly narrow the date range of the targets to be saved.

[Available space on the installation target disk of the database-related files]

Ensure that there is sufficient available space on the installation target disk of the database-related files. When a large number of logs are to be backed up, there must be enough available space on the installation target disk of the database-related files. For details about disk capacity requirements, refer to "Operation Environment" in the *Systemwalker Desktop Keeper User's Guide*.

[Command execution authority in Windows Server(R) 2008]

In the Windows Server(R) 2008 OS, execution of the backup commands requires the administrator authority. Before running the backup commands, log on to the Windows OS as a user of the Administrators group or Domain Admins group.

[Enable the command extension function of the command prompt]

Execution of the backup commands requires that the command extension function of the command prompt be enabled.
The command extension function is enabled by default. Run "echo %CMDEXTVERSION%" in the command prompt window. If the output value is larger than or equal to 2, the command extension function is enabled.

[Date supported by the backup commands]

The date range that supports execution of the backup commands is from 2001-01-01 to 2034-12-31. The backup commands may not function on other dates.

[Data conversion]

The backup commands may convert data in a log and then output the converted log to a CSV file. The following data is converted:

- Tab, carriage return, line feed replaced with halfwidth space

- Double quotation mark (") escaped with double quotation mark ("")

[Attached data processing]

The backup tool/commands do not back up the attached data (including the screen capture data and backup original files). The structure of the target folder that saves the attached data is as follows. Back up the attached data separately by application. For details about the target folder that saves the attached data, refer to "2.3.6.9 Set Saving Target Folder". In addition, the attached data cannot be deleted even by the log deletion command (DTKDELR).
[Structure]

Target folder for saving attached data

+- Folder of day unit
+- Folder of CT unit

[Example]

[Email contents data processing]

The backup commands do not back up the E-mail contents (including the E-mail Text and attachments). The structure of the target folder that saves the E-mail contents is as follows. Back up the E-mail contents separately by application. For details about the target folder that saves the E-mail contents, refer to "2.3.6.9 Set Saving Target Folder".

In addition, the E-mail contents cannot be deleted even by the log deletion command (DTKDELR).
The DTKMLDL.BAT (Delete E-mail Content) command can be used to delete the E-mail contents. For details about how to use the command, refer to "DTKMLDL.BAT (Delete E-mail Content)" of the *Systemwalker Desktop Keeper Reference Manual*.
[Structure]

Target folder for saving e-mail content

+- Folder of day unit
+- Folder of CT unit

[Example]
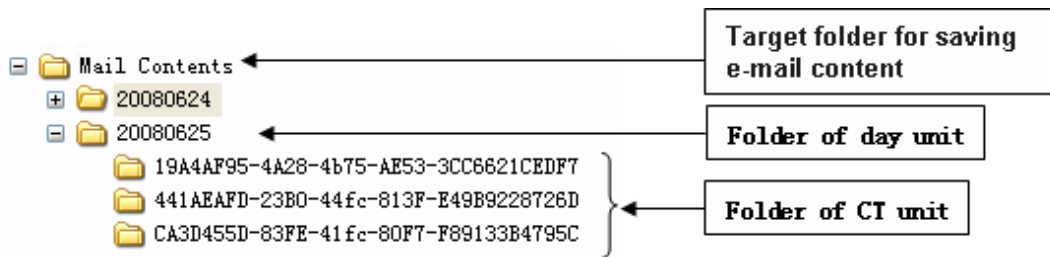
Types of Backup Commands

The Systemwalker Desktop Keeper provides 13 types of backup commands. Each command performs different operations on the data in the database. The following table describes the commands. The folders used for saving backup commands are as follows:

Target folder for saving the backup commands:

Installation target folder of the database-related files\BackupCommand
(when newly installing Management Server V15.1.0, the installation folder for database-related files is *mgmtServerInstallFolder*\DB.)

Example: C:\DTKDB\BackupCommand
Example: C:\Program Files (x86)\Fujitsu\Systemwalker Desktop Keeper\DB\BackupCommand C:\DTKDB\BackupCommand

No.	Command	Description
1	DTKMSTB.EXE	Back up each table described in "Management Information" of "3.1.1.2 User Assets" as a CSV file. When managing iOS devices, the iOS management database is also backed up.
2	DTKLGTB.EXE	Back up each table described in "Log Information (Not Including Command logs)" of "3.1.1.2 User Assets" as a CSV file.
3	DTKLG1T.EXE	Output the log information from the database to CSV files in a specified format supported by the Log Viewer for one type only or for all data of all log types in batch, and view the log information.
4	DTKLGAT.BAT	Collectively output the log information from the database to CSV files in Log Viewer format, and view the log information.
5	DTKDELR.EXE	Delete the data in all the tables described in "Log Information (Not Including Command logs)" of "3.1.1.2 User Assets" and the data described in "Log Information (Command logs)".
6	DTKBKDL.BAT	Back up each table described in "Log Information (Not Including Command logs)" of "3.1.1.2 User Assets" as a CSV file and then delete the backed up table data from the database.
7	DTKCVDL.BAT	Back up each table described in "Log Information (Not Including Command logs)" of "3.1.1.2 User Assets" as a CSV file and collectively output log information from the database to CSV files. Then, delete the backed up table data from the database.
8	DTKSTCV.EXE	Output the collected setting change log information to a CSV file for the specified period.
9	DTKDELST.EXE	Delete logs registered within the specified period for the collected setting change log information.
10	DTKMLDL.BAT	Delete "E-mail Contents" in "3.1.1.2 User Assets" from the Management Server or Master Management Server.
11	DTKBFDM.EXE	Internal command invoked by other backup commands Used for calculating the number of past days
12	DTKELSET.BAT	Internal command invoked by other backup commands Used for re-setting the value of **ERRORLEVEL**
13	DTKNUMCK.BAT	Internal command invoked by other backup commands Used for checking whether the input parameter values of the backup commands are numeric
14	DTKSERVICE.BAT	Display the start status of PostgreSQL and Desktop Keeper services, and start or stop these services.
15	DTKTBLTRUNCATE.BAT	Delete data in all tables described in "Log Information (Not Including Command logs)" in "3.1.1.2 User Assets" from the database. This command initializes the tables, deletes all logs of the applicable tables, and releases the expansion area. Unlike DTKDELR.EXE, the deletion period cannot be specified.
16	DTKTBLUNLOAD.BAT	Back up data in all tables described in "Log Information (Not Including Command logs)" in "3.1.1.2 User Assets" as a CSV file for each table.

No.	Command	Description
		This command outputs all data of the applicable tables.
		Unlike DTKLGTB.EXE, the backup period cannot be specified.
17	DailySch.bat	Sample command that backs up and deletes logs that are 91 days old or more.
		Refer to "Example I: Backing Up and Deleting the Logs Saved 91 Days Ago (Log Storage Life: 3 Months)" for details.
18	DailySch2.bat	Sample command that backs up and deletes logs that are 91 days old or more, and backs up logs for the most recent week.
		Refer to "Examples of Creating Batch Files" for details.
19	DTKTask_DailySchBackup.bat	Sample command used to register tasks when DailySch.bat and DailySch2.bat are executed from tasks.
		Refer to "Example I: Backing Up and Deleting the Logs Saved 91 Days Ago (Log Storage Life: 3 Months)" and "Examples of Creating Batch Files" for details.

Refer to "Command Reference" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command (except DailySch.bat, DailySch2.bat, and DTKTask_DailySchBackup.bat).

Refer to "Example I: Backing Up and Deleting the Logs Saved 91 Days Ago (Log Storage Life: 3 Months)" and "Examples of Creating Batch Files" for details on DailySch.bat, DailySch2.bat and DTKTask_DailySchBackup.bat.

Edit Backup Commands

The following commands must be edited before they are used. Edit the following backup commands based on the operating environment.

- DTKLGAT.BAT

- DTKBKDL.BAT

- DTKCVDL.BAT

- DTKTBLTRUNCATE.BAT

- DTKTBLUNLOAD.BAT

DTKLGAT.BAT

To use "DTKLGAT.BAT", open it with a text editor and edit the following contents that are underlined and in bold type.

```
rem ****************************************************************
rem * Block for specifying operational parameters     *
rem ****************************************************************

rem Database name
set SQLDB=DTKDB

rem User ID used for connecting to the database
set SQLuser=(*1)

rem Password corresponding to the preceding user ID
set SQLpsw=(*2)

set startday=%1
set endday=%2

rem Name of the target drive for saving the output files
set bkdrive=(*3)

rem Name of the target folder for saving the output files (in the output process)
set bkdir=(*4)
```

```
rem Name of the folder created under the preceding bkdir folder
set csvdir=(*5)

rem Extraction key (A  null value indicates that the client time is used. The value "SERVER"
indicates that the server time is used.)
set how=(*6)
```

```
rem ************************************************
rem * Block for completing the process     *
rem ************************************************

:allend0
pause(*7)
EXIT /B 0

:allend1
pause(*7)
EXIT /B 1
```

No.	Editing Content	Configuration Example
(*1)	Enter the user ID (granted with the authority to back up and restore information) registered in the Server Settings Tool.	BKUSER
(*2)	Enter the password corresponding to the preceding user ID.	BKPSW
(*3)	Enter the name of the target drive for saving the output files. (The drive letter must be followed by ":".)	C:
(*4)	Enter the name of the target folder for saving the output files in the output process. ("\" must be added before the folder name.)	\DTKBKUP
(*5)	Enter the name of the target folder for saving the output files, created under the folder set in (*4). %2 indicates the end date of the backup target period, after which the folder is named. (Example: If the end date of the backup target period is April 20, 2007, the folder name is 20070420.)	LV%2

(*6)	Set whether client time (log occurrence date and time on the CT) or server time (log saving time on the server) is used in extraction of logs of the backup/delete target period.
	
	- Not specified
	  Use the client time (log occurrence date and time on the CT).
	
	- SERVER
	  Use the server time (log saving time on the server).
		SERVER

(*7)	Enter "pause" or "rem pause".
	
	- "pause"
	  The program will remain paused after the command execution ends. To exit the pause state, press any key in the command prompt window.
	
	- "rem pause"
	  The program will close after the command execution ends.
		rem pause

DTKBKDL.BAT

To use "DTKBKDL.BAT", open it with a text editor and edit the following contents that are underlined and in bold type.

```
rem ***********************************************************
rem * Block for specifying operational parameters *
rem ***********************************************************
```

```
rem Database name
set SQLDB=DTKDB

rem User ID used for connecting to the database
set SQLuser=(*1)

rem Password corresponding to the preceding user ID
set SQLpsw=(*2)

rem Name of the target drive for saving the output files
set bkdrive=(*3)

rem Name of the target folder for saving the output files (in the output process)
set bkdir=(*4)

rem Name of the folder created under the preceding bkdir folder
set logdir=(*5)

rem Extraction key (A null value indicates that the client time is used. The value "SERVER"
indicates that the server time is used.)
set how=(*6)
```

```
rem *************************************************************
rem * Block for completing the process                *
rem *************************************************************

:allend0
pause(*7)
EXIT /B 0

:allend1
pause(*7)
EXIT /B 1
```

No.	Editing Content	Configuration Example
(*1)	Enter the user ID (granted with the authority to back up and restore information) registered in the Server Settings Tool.	BKUSER
(*2)	Enter the password corresponding to the preceding user ID.	BKPSW
(*3)	Enter the name of the target drive for saving the output files. (The drive letter must be followed by ":".)	C:
(*4)	Enter the name of the target folder for saving the output files. ("\" must be added before the folder name.)	\DTKBKUP
(*5)	Enter the name of the target folder for saving the output files, created under the folder set in (*4). %2 indicates the end date of the backup target period, after which the folder is named. (Example: If the end date of the backup target period is April 20, 2007, the folder name is 20070420.)	BK%2
(*6)	Set whether client time (log occurrence date and time on the CT) or server time (log saving time on the server) is used in extraction of logs of the backup/delete target period. - Not specified Use the client time (log occurrence date and time on the CT). - SERVER Use the server time (log saving time on the server).	SERVER

No.	Editing Content	Configuration Example

(*7)	Enter "pause" or "rem pause".
	
	- "pause"
	  The program will remain paused after the command execution ends. To exit the pause state, press any key in the command prompt window.
	
	- "rem pause"
	  The program will close after the command execution ends.
		rem pause

DTKCVDL.BAT

To use "DTKCVDL.BAT", open it with a text editor and edit the following contents that are underlined and in bold type.

```
rem **********************************************************
rem * Block for specifying operational parameters *
rem **********************************************************

rem Database name
set SQLDB=DTKDB

rem User ID used for connecting to the database
set SQLuser=(*1)

rem Password corresponding to the preceding user ID
set SQLpsw=(*2)

rem Number of days from the end date of the target period to the execution date
set bkdays=(*3)
set bkMonth=(*3)
set bkdate=(*3)

rem State date of the target period (date of the first record to be processed)

set startday=(*4)

DTKBFDM.EXE %bkdays% %bkMonth% %bkdate%
if errorlevel 20350101 goto errend4
if errorlevel 20010101 goto next1
goto errend4

:next1
set endday=%errorlevel%

rem Name of the target drive for saving the output files
set bkdrive=(*5)

rem Name of the target folder for saving the output files (in the output process)
set bkdir=(*6)

rem Name of the folder created under the preceding bkdir folder (BK indicates the backup data
format.)
set logdir=(*7)

rem Name of the folder created under the preceding bkdir folder (LV indicates the Log Viewer
format.)
set csvdir=(*8)

rem Extraction key (A null value indicates that the client time is used. The value "SERVER"
indicates that the server time is used.)
set how=(*9)
```

```
rem *************************************************************
rem * Block for completing the process            *
rem *************************************************************

:allend0
pause(*10)
EXIT /B 0

:allend1
pause(*10)
EXIT /B 1
```

No.	Editing Content	Configuration Example
(*1)	Enter the user ID (granted with the authority to back up and restore information) registered in the Server Settings Tool.	BKUSER
(*2)	Enter the password corresponding to the preceding user ID.	BKPSW
(*3)	Enter the end date of the backup/delete target period, that is, a date several days or months before the date that "DTKCVDL.BAT" is executed. For details about the values, refer to "Backup/Delete Target Period". - set bkdays= Enter the number of days or months The number of days can range from 0 to 2000, and the number of months can range from 0 to 120. <bkmonth> determines whether the value of <bkdays> indicates the number of days or months. - set bkMonth= If it is set to "MONTH", the value of <bkdays> indicates the number of months. If it is not set to any value, the value of <bkdays> indicates the number of days. If it is set to "MONTH", set <bkdays> to the number of months. - set bkdate= If the value of <bkmonth> is "MONTH", set <bkdate> to 99 or a value ranging from 1 to 31. The value ranging from 1 to 31 indicates a corresponding specific date in the specified month. The value 99 indicates the end of the specified month. If <bkmonth> does not have any value, it is not necessary to set <bkdate>.	(To specify 90 days ago:) set bkdays=90 set bkMonth= set bkdate= (To specify the first day of the month that is three months ago:) set bkdays=3 set bkMonth=MONTH set bkdate=1 (To specify the last day of the month that is three months ago:) set bkdays=3 set bkMonth=MONTH set bkdate=99
(*4)	Enter the start date of the backup/delete target period. The data between the start date and the end date set in (*4) will be backed up or deleted. The start date can be set to "00000000" or a value ranging from "20010000" to "20349999". The start date must be earlier than the end date set in (*3). Otherwise, errors may occur. If the last four digits of the value ranging from 20010000 to 20349999 cannot be found in the calendar, the following dates will be specified: - If the last four digits are "0000", the start date is January, 1. - If the last four digits are a value ranging from "1232" to "9999", the start date is January, 1 of the next year. - If the last two digits are "00", the start date is the first day of the specified month. - If the last two digits are a value ranging from "the day after the end date of the specified month" to "99", the start date is the first day of the month following the specified month. If "00000000" is entered, the start date is the date from which the database starts storing data. For details about the values, refer to "Backup/Delete Target Period".	00000000

No.	Editing Content	Configuration Example
(*5)	Enter the name of the target drive for saving the output files. (The drive letter must be followed by ":".)	C:
(*6)	Enter the name of the target folder for saving the output files in the output process. ("\" must be added before the folder name.)	\DTKBKUP
(*7)	Enter the name of the target folder for saving the output files, created under the folder set in (*6). %endday% indicates the end date of the backup target period, after which the folder is named. (Example: If the end date of the backup target period is April 20, 2007, the folder name is 20070420.)	BK%endday%
(*8)	Enter the name of the target folder for saving the output files, created under the folder set in (*6). %endday% indicates the end date of the backup target period, after which the folder is named. (Example: If the end date of the backup target period is April 20, 2007, the folder name is 20070420.)	LV%endday%

(*9)	Set whether client time (log occurrence date and time on the CT) or server time (log saving time on the server) is used in extraction of logs of the backup/delete target period.
	
	- Not specified
	  Use the client time (log occurrence date and time on the CT).
	
	- SERVER
	  Use the server time (log saving time on the server).
		SERVER

(*10)	Enter "pause" or "rem pause".
	
	- "pause"
	  The program will remain paused after the command execution ends. To exit the pause state, press any key in the command prompt window.
	
	- "rem pause"
	  The program will close after the command execution ends.
		rem pause

Backup/Delete Target Period

To use "DTKCVDL.BAT", the backup/delete target period must be specified. The following figure shows (*3) and (*4) described in the preceding table, which are related to the configuration of the target period. For details about the editing contents, refer to the preceding table.
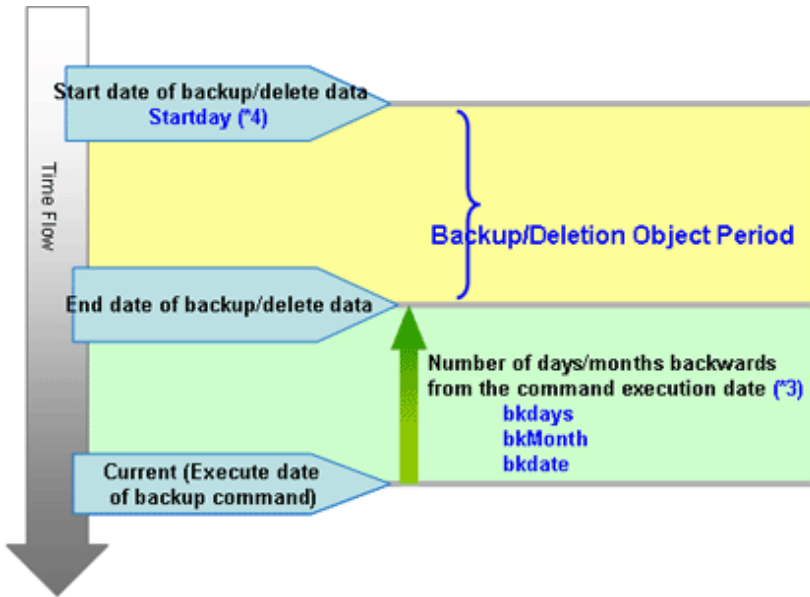
DTKTBLTRUNCATE.BAT

To use " DTKTBLTRUNCATE.BAT ", open it with a text editor and edit the following contents that are underlined and in bold type.

```
rem ********************************************************
rem * Operating Parater Specification Block                *
rem ********************************************************

rem Describe database name
set SQLDB=DTKDB

rem Describe user ID connecting to database(Manager ID of operation DB is set)
set SQLuser=(*1)

rem Describe the password corresponding to the user ID connecting to the database
set SQLpsw=(*2)
```

No.	Editing Content	Configuration Example
(*1)	Enter the user ID (granted with the authority to back up and restore information) registered in the Server Settings Tool.	BKUSER
(*2)	Enter the password corresponding to the preceding user ID.	BKPSW

DTKTBLUNLOAD.BAT

To use " DTKTBLUNLOAD.BAT ", open it with a text editor and edit the following contents that are underlined and in bold type.

```
rem ********************************************************
rem * Operating Parater Specification Block                *
rem ********************************************************

rem Describe database name
set SQLDB=DTKDB

rem Describe user ID connecting to database(Manager ID of operation DB is set)
set SQLuser=(*1)

rem Describe the password corresponding to the user ID connecting to the database
set SQLpsw=(*2)
```

No.	Editing Content	Configuration Example
(*1)	Enter the user ID (granted with the authority to back up and restore information) registered in the Server Settings Tool.	BKUSER
(*2)	Enter the password corresponding to the preceding user ID.	BKPSW

Preparations

When backing up data for restoration, record the following setting information. (Obtain the collected bitmaps and notes of the windows.)

Target	Window to Be Backed Up
Management console	**Terminal Operation Settings**
Server Settings Tool	**System Settings**
	Setting of Active Directory Linkage Note: When the Active Directory linkage function is used
	Administrator Notification Settings
	Management Server Settings
	Self Version Upgrade Settings for Folder/CT

Perform the following steps to display the **Terminal Operation Settings** window:

1. Start **Management Console**.

2. Select **Terminal Operation Settings** from the **Operation Settings** menu.
   The **Terminal Operation Settings** window is displayed.

For details about how to display the windows of the Server Settings Tool, refer to "2.3.6 Set Environment of Management Server/Master Management Server".

🖙 Note

. . . .

Properly store the recorded information.

The preceding setting information cannot be backed up by the Backup Tool. After restoring data, it is necessary to restore the terminal operation settings to the status before backup; therefore, ensure that the information recorded along with the backup data is properly stored.

. . . .

Start Backup

For details about how to use the backup commands, refer to "Command Reference" of the *Systemwalker Desktop Keeper Reference Manual*.

🖙 Note

. . . .

Ensure that services are stopped before command execution.

Stop the "Level Control Service", "Server Service" and Smart Device Relay Server before the backup or restoration operation is performed. Otherwise, data may be incomplete during backup or restoration.

When selecting backup commands after batch files are created, ensure that the Server Service and Level Control Service are stopped, as described in "Examples of Creating Batch Files in the Task Scheduler".

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, when registering to scheduled task, prevent it from executing batch file at the above time frame.

The following procedure must be manually performed:

1. Log on the PC as a user of the local Administrators group or Domain Admins group.
   If there is another running application, exit it.

2. In the displayed Windows Services window, select the following services and select **Stop** from the **Action** menu. It will take 30 seconds to 1 minute. 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. Wait for a while and check if the service has stopped.

   - SWLevelControlService

   - SWServerService

Also, when managing Android or iOS devices, use SDSVService.bat (start/stop service of Smart Device Relay Server command) to stop 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.

⋅⋅

The following examples are used to illustrate how to add the backup commands to the Task Scheduler and execute the commands in two modes.

Example I: Backing Up and Deleting the Logs Saved 91 Days Ago (Log Storage Life: 3 Months)

Execution Conditions

- Set the data storage life to 90 days. The data stored longer than this period will be backed up to files and no longer be kept in the database.

- Create a folder named after the backup date in the specified drive every day and back up the data stored in the database for longer than 91 days to the created folder.

- The backup targets are as follows:

  - All the tables described in "Management Information" (with DTKMSTB)

  - All the tables (log data in the database and command logs) described in "Log Information", as well as the log information stored in the database (with DTKCVDL)

  For details about the data to be backed up, refer to "3.1.1.2 User Assets".

- Delete the data that is already backed up from the database (with DTKCVDL).

- Use the Task Scheduler of the OS to enable automatic backup. Stop the services on the Systemwalker Desktop Keeper Server side before command execution in order to avoid conflict between the access operation of services and the database record deletion operation.

- After the server-side services are stopped, start command execution at 02:00 a.m. when there are fewer database connections.

- Verify the time required by backup and deletion of the database records. Assume that it takes about 30 minutes in total.

Execution Settings

To perform operations under the preceding execution conditions, use the provided backup commands DTKMSTB, DTKCVDL, DailySch, and DTKTask_DailySchBackup.bat.

In the execution settings, the structures of the target drive and folder for saving backup files are as follows (XXXXXXXX indicates the end date):

- All the tables described in "Management Information"
  In D:\BACKUP\XXXXXXXX\MSXXXXXXXX\

- All the tables (log data in the database and command logs) described in "Log Information"
  In D:\BACKUP\XXXXXXXX\BKXXXXXXXX\

- Log information stored in the database
  In D:\BACKUP\XXXXXXXX\LVXXXXXXXX\

For details about the data to be backed up, refer to "3.1.1.2 User Assets".
To implement the execution settings, perform the following steps:

1. Modify the DTKCVDL contents as follows:

```
set  SQLuser=bkuser          ...Set the user ID used for connecting to the database.
set  SQLpsw=bkpsw            ...Set the password corresponding to the preceding user ID.
set  bkdays=90               ...Set the data storage life.
set  bkdrive=D:              ...Set the target drive for backing up the logs.
set  bkdir=\BACKUP\%endday%  ...Set the target folder for backing up the logs.
Change pause to rem pause.
```

2. Rewrite "DailySch.bat". Refer to "Examples of Creating Batch Files" below for details on the content that is to be rewritten.

3. Add "DTKTask_DailySchBackup.bat" to the "Task Scheduler".

   a. Click **Administrative Tools** > **Task Scheduler**, and then select **Create Task**.

   b. Click **Browse** in the Start a Program window and select "DTKTask_DailySchBackup.bat".

   c. Enter the task name and set the task to run at 02:00 a.m. every day.

   d. Since task execution requires a user ID and a password, set the user ID and password of a user with administrator authority.

Examples of Creating Batch Files

Examples describing how to create a registration batch file to be registered to "DailySch.bat" and "DTKTask_DailySchBackup.bat" are stored in the following folder.

```
dbRelatedFileInstallFolder\BackupCommand\
```

When newly installing Management Server V15.1.0, the installation folder of database-related files is *mgmtServerInstallFolder*\DB.

In this example of creating batch commands, the return value of the Net command invoked inside the batch file is not used as the return value of the batch commands. Take cautions when using the return value of the Net command to control the further processing.

Open "DailySch.bat" in a text editor, and edit the underlined section in bold below.

Example of Creating DailySch.bat

```
@ECHO OFF
SETLOCAL
rem ****************************************************************************
rem *                                                                         *
rem *    Systemwalker Desktop Keeper Maintenance Tool                         *
rem *                                                                         *
rem *    Process Name : Example-The log before 91 days ago is backed up deleted *
rem *             (Log preservation period:Three months)                     *
rem *    Function Name : DailySch.bat                                         *
rem *                                                                         *
rem *    Copyright (C) FUJITSU LIMITED 2012-2015                              *
rem *                                                                         *
rem ****************************************************************************
rem
rem ********************************************************
rem * Setting                                             *
rem ********************************************************
rem The drive letter at the output target is described
SET BKDRIVE=D:

rem The folder name at the output target is described
SET BKFOLDERNAME=\BACKUP

rem The measurement days to set the processing end date are described
SET DELEND=90

rem Describe user ID connecting to database
SET SQLUSER=dtkbkuser

rem Describe password connecting to database
```

```
SET SQLPASSWORD=dtkpsw

rem The backup command storage target is described
SET BACKUPCOMMANDFOLDER=dbRelatedFileInstallFolder\BackupCommand

rem Extraction Key(Client date when omitting it,Server date when specifying SERVER)
SET HOW=SERVER

rem ***************************************************************
rem * Processing part                                             *
rem ***************************************************************
path "%BACKUPCOMMANDFOLDER%";%path%
echo Backup processing start(%TIME%)

%BKDRIVE%
CD %BKFOLDERNAME%
if ERRORLEVEL 1 goto recover5

rem Calculation on backup end day
"%BACKUPCOMMANDFOLDER%\DTKBFDM.EXE" %DELEND%

rem The directory is made on the execution day
SET TEMPDATE=%ERRORLEVEL%
MKDIR %TEMPDATE%

rem the backup target folder is made
SET MSFOLDER=%BKDRIVE%%BKFOLDERNAME%%TEMPDATE%\MS%TEMPDATE%
MKDIR "%MSFOLDER%"

echo DTK service is stopped.
call "%BACKUPCOMMANDFOLDER%\DTKSERVICE.BAT" stop
if ERRORLEVEL 1 goto recover2

rem Backup of mastering system data
"%BACKUPCOMMANDFOLDER%\DTKMSTB.EXE" DTKDB %SQLUSER% %SQLPASSWORD% "%MSFOLDER%"

if ERRORLEVEL 1 goto recover3

rem Backup and deletion of log system data
CALL "%BACKUPCOMMANDFOLDER%\DTKCVDL.BAT"
if ERRORLEVEL 1 goto recover4

echo The DTK service is started.
call "%BACKUPCOMMANDFOLDER%\DTKSERVICE.BAT" start
echo The schedule ended normally.(%TIME%)
EXIT /B 0

:recover1
echo It made an error of the stop of level control service.
echo The backup is discontinued, and the DTK service (level control service) is started.
goto allend1

:recover2
echo It made an error of the stop of server service.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:recover3
echo It made an error of the backup of administrative information.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1
```

```
:recover4
echo It made an error of the backup and the deletion of the log.
echo The backup and the deletion of the log are discontinued, and the DTK service (level control
service,server service) is started.
goto allend1

:recover5
echo The backup folder does not exist.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:allend1
echo The DTK service is started.
call "%BACKUPCOMMANDFOLDER%\DTKSERVICE.BAT" start
echo The schedule ended abnormally.(%TIME%)
EXIT /B 1
```

Example of Creating DTKTask_DailySchBackup.bat

Change the database-related file installation folder according to the environment.
Change the underlined item in bold to "DailySch.bat" below.

```
@echo off
SETLOCAL

rem ************************************************************
rem *                                                          *
rem *    Systemwalker Desktop Keeper Maintenance tool          *
rem *                                                          *
rem *    Process Name : Registration batch                     *
rem *    Function Name : DTKTask_DailySchBackup.bat            *
rem *                                                          *
rem *    Copyright (C) FUJITSU LIMITED 2012-2015               *
rem *                                                          *
rem ************************************************************
rem
rem ********************************************************
rem * Setting                                              *
rem ********************************************************
set BACKUPCOMMANDFOLDER=dbRelatedFileInstallFolder\BackupCommand

rem ********************************************************
rem * Processing                                           *
rem ********************************************************
rem Calculation on execution day
"%BACKUPCOMMANDFOLDER%\DTKBFDM.EXE" 0
SET EXECDAY=%ERRORLEVEL%

rem The execution log is made by the log file name at the execution date.(e.g.20140112.log)
rem The log file is stored in the folder set to "Start in (optional)" when the task is registered.
call "%BACKUPCOMMANDFOLDER%\DailySch.bat" > %EXECDAY%.log
if ERRORLEVEL 1 goto allend1

EXIT /B 0

:allend1
EXIT /B 1
```

Example of Result Logs of Batch File Execution

The execution result log (%EXECDAY%.log) records the execution results of the registered DailySch.bat file in the preceding example.

```
Backup processing start(18:45:42.11)
DTK service is stopped.
Sat 05/23/2015-18:45:42.45 -DTKSERVICE--------------------------------------------------------
Sat 05/23/2015-18:45:42.47 [ Service termination processing of the management server (STOP) ]
Sat 05/23/2015-18:45:42.48 --------------------------------------------------------
Sat 05/23/2015-18:45:42.97 The service of POSTGRESQL(Operation)        :operating
Sat 05/23/2015-18:45:43.26 The service of POSTGRESQL(Log view)         :operating
Sat 05/23/2015-18:45:43.28 The service of SYMFOWARE(Log analyze)       :unregistration
Sat 05/23/2015-18:45:43.53 The service of management server(SWLevelControlService)      :operating
Sat 05/23/2015-18:45:43.69 The service of management server(SWServerService)        :operating
Sat 05/23/2015-18:45:43.70 The service of management server(Log analyze)         :unregistration
Sat 05/23/2015-18:45:43.72 The service of iOS management database       :unregistration
Sat 05/23/2015-18:45:43.72 The service inquiry of the management server ended.
Sat 05/23/2015-18:45:43.73 The service of the management server (SWLevelControlService) is stopped.
Sat 05/23/2015-18:45:46.30 The SWLevelControlService was stopped.
Sat 05/23/2015-18:45:46.31 The service of the management server (SWServerService) is stopped.
Sat 05/23/2015-18:45:49.18 The SWServerService was stopped.
Sat 05/23/2015-18:45:49.93 The service of POSTGRESQL(Operation)        :operating
Sat 05/23/2015-18:45:50.10 The service of POSTGRESQL(Log view)         :operating
Sat 05/23/2015-18:45:50.10 The service of SYMFOWARE(Log analyze)       :unregistration
Sat 05/23/2015-18:45:50.26 The service of management server(SWLevelControlService)      :halt
condition
Sat 05/23/2015-18:45:50.42 The service of management server(SWServerService)        :halt condition
Sat 05/23/2015-18:45:50.42 The service of management server(Log analyze)         :unregistration
Sat 05/23/2015-18:45:50.43 The service of iOS management database       :unregistration
Sat 05/23/2015-18:45:50.45 Service stopped.
2015/05/23 18:45:50  Backup management information collectively - Start
2015/05/23 18:45:50
2015/05/23 18:45:50   Database   :  DTKDB
2015/05/23 18:45:50   Directory  :  D:\BACKUP\20150222\MS20150222
2015/05/23 18:45:50
2015/05/23 18:45:50   - LEVELOBJECT
2015/05/23 18:45:50     Output file name  : D:\BACKUP\20150222\MS20150222\LEVELOBJECT.csv
2015/05/23 18:45:50     Number of output items.....11
2015/05/23 18:45:50
2015/05/23 18:45:50   - LEVELCOMPOSITION
2015/05/23 18:45:50     Output file name  : D:\BACKUP\20150222\MS20150222\LEVELCOMPOSITION.csv
2015/05/23 18:45:50     Number of output items.....10


(Omitted)


2015/05/23 18:45:58   - LOGKEYWORDS
2015/05/23 18:45:58     Number of deleted items.....0
2015/05/23 18:45:58
2015/05/23 18:45:58   - FILEACCESSLOG
2015/05/23 18:45:58     Number of deleted items.....0
2015/05/23 18:45:58
2015/05/23 18:45:58   - SESSIONMANAGE
2015/05/23 18:45:58     Number of deleted items.....0
2015/05/23 18:45:58
2015/05/23 18:45:58  Delete log information - End
2015/05/23 18:45:58  Delete configuration change log information - Start
2015/05/23 18:45:58
2015/05/23 18:45:58  Database    :  DTKDB
2015/05/23 18:45:58  Processing start date     :  00000000
2015/05/23 18:45:58  Processing finish date    :  20150222
2015/05/23 18:45:58  Deletion indication       :  -Y
2015/05/23 18:45:58
2015/05/23 18:45:58     Processing 2015/01/01 ... 71 items are deleted
2015/05/23 18:45:59     Number of deleted items.....71
2015/05/23 18:45:59
```

```
2015/05/23 18:45:59    Delete configuration change log information - End
The DTK service is started.
Sat 05/23/2015-18:45:59.29 -DTKSERVICE----------------------------------------------------
Sat 05/23/2015-18:45:59.31    [ service start processing (START) of the Management server ]
Sat 05/23/2015-18:45:59.33 ----------------------------------------------------------------
Sat 05/23/2015-18:45:59.81 The service of POSTGRESQL(Operation)        :operating
Sat 05/23/2015-18:46:00.00 The service of POSTGRESQL(Log view)         :operating
Sat 05/23/2015-18:46:00.01 The service of SYMFOWARE(Log analyze)        :unregistration
Sat 05/23/2015-18:46:00.37 The service of management server(SWLevelControlService)      :halt
condition
Sat 05/23/2015-18:46:00.53 The service of management server(SWServerService)       :halt condition
Sat 05/23/2015-18:46:00.54 The service of management server(Log analyze)        :unregistration
Sat 05/23/2015-18:46:00.56 The service of iOS management database        :unregistration
Sat 05/23/2015-18:46:00.58 The service inquiry of the management server ended.
Sat 05/23/2015-18:46:00.61 The service of the management server (SWLevelControlService) is started.
Sat 05/23/2015-18:46:02.74 The service of the management server (SWServerService) is started.
Sat 05/23/2015-18:46:07.60 The service of POSTGRESQL(Operation)        :operating
Sat 05/23/2015-18:46:07.80 The service of POSTGRESQL(Log view)         :operating
Sat 05/23/2015-18:46:07.82 The service of SYMFOWARE(Log analyze)        :unregistration
Sat 05/23/2015-18:46:08.02 The service of management server(SWLevelControlService)       :operating
Sat 05/23/2015-18:46:08.21 The service of management server(SWServerService)        :operating
Sat 05/23/2015-18:46:08.23 The service of management server(Log analyze)        :unregistration
Sat 05/23/2015-18:46:08.23 The service of iOS management database         :unregistration
Sat 05/23/2015-18:46:08.24 Service was started.
The schedule ended normally.(18:46:08.27)
```

Example II: Deleting the Logs Saved 91 Days Ago and Backing Up the Logs Saved in the Recent Week (Log Storage Life: 3 Months)

Execution Conditions

- Set the data storage life to 90 days. The data stored longer than this period will be backed up to files and no longer be kept in the database.

- Create a folder named after the backup start date in the specified drive every day and back up the data of the recent week to the created folder.

- The backup targets are as follows:

  - All the tables described in "Management Information" (with DTKMSTB)

  - All the tables (log data in the database and command logs) described in "Log Information", as well as the log information stored in the database

  For details about the data to be backed up, refer to "3.1.1.2 User Assets".

- Delete the data saved in the database 91 days ago.

- Use the Task Scheduler of the OS to enable automatic backup. Stop the services on the Systemwalker Desktop Keeper Server side before command execution in order to avoid conflict between the access operation of services and the database record deletion operation.

- After the server-side services are stopped, start command execution at 02:00 a.m. when there are fewer database connections.

- Verify the time required by backup and deletion of the database records. Assume that it takes about 30 minutes in total.

The following figure shows an example.
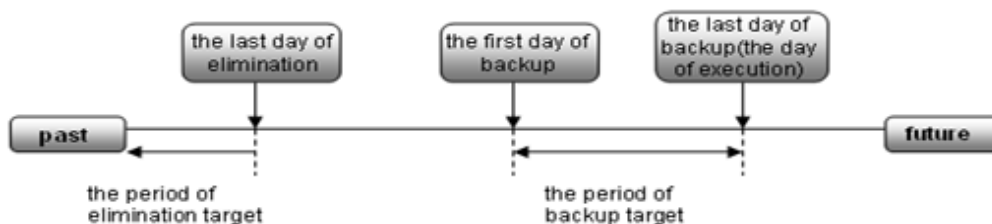
For example, set the backup target period to the week before the execution date and delete the logs saved 91 days ago.

Execution Settings

To perform operations under the preceding execution conditions, use the provided backup commands DTKMSTB, DTKLGTB, DTKLG1T, DTKDELR, DailySch2, and DTKTask_DailySchBackup.bat.

In the execution settings, the structures of the target drive and folder for saving backup files are as follows (XXXXXXXX indicates the backup start date):

- All the tables described in "Management Information"

  In D:\BACKUP\XXXXXXXX\MSXXXXXXXX\

- All the tables (log data and command logs in the database) described in "Log Information"

  In D:\BACKUP\XXXXXXXX\BKXXXXXXXX\

- Log information stored in the database

  In D:\BACKUP\XXXXXXXX\LVXXXXXXXX\

For details about the data to be backed up, refer to "".

To implement the execution settings, perform the following steps:

1. Rewrite DailySch2.bat. Refer to "Examples of Creating Batch Files" below for details on the content that is to be rewritten.
   Create the target folder for log backup, specified in the execution settings.
   That is, D:\BACKUP in the example of execution settings.

2. Add "DTKTask_DailySchBackup.bat" to the "Task Scheduler".

   a. Click **Administrative Tools** > **Task Scheduler**, and then select **Create Task**.

   b. Click **Browse** in the Start a Program window and select "DTKTask_DailySchBackup.bat".

   c. Enter the task name and set the task to run at 02:00 a.m. every day.

   d. Since task execution requires a user ID and a password, set the user ID and password of a user with administrator authority.

Examples of Creating Batch Files

Examples describing creation of DailySch2.bat and DTKTask_DailySchBackup.bat are stored in the following folder.

```
dbRelatedFileInstallFolder\BackupCommand\
```

When newly installing Management Server V15.1.0, the installation folder of database-related files is *mgmtServerInstallFolder*\DB. In this example of creating batch commands, the return value of the Net command invoked inside the batch file is not used as the return value of the batch commands. Take caution when using the return value of the Net command to control the further processing. Open "DailySch2.bat" in a text editor, and edit the underlined section in bold below.

Example of Creating DailySch2.bat

```
@ECHO OFF
SETLOCAL
rem *********************************************************************
rem *                                                                   *
rem *    Systemwalker Desktop Keeper Maintenance Tool                   *
rem *                                                                   *
rem *    Process Name : Example-The log before 91 days ago is deleted   *
rem *               and the log during one week ago from today is backed up *
rem *              (Log preservation period:Three months)               *
rem *    Function Name : DailySch2.bat                                  *
rem *                                                                   *
rem *    Copyright (C) FUJITSU LIMITED 2012-2015                        *
rem *                                                                   *
rem *********************************************************************
rem
echo Setting begins
rem ***********************************************************
```

```
rem * Setting                                                        *
rem **************************************************************
rem The drive letter at the output target is described
SET BKDRIVE=D:

rem The folder name at the output target is described
SET BKFOLDERNAME=\BACKUP

rem Whether how many days the backup begins is described
rem Example When you specify seven days ago
SET BKSTART=7

rem From how many days to ago data is deleted is described
rem Example When specifying it before 90 days ago
SET DELEND=90

rem Describe user ID connecting to database
SET SQLUSER=dtkbkuser

rem Describe password connecting to database
SET SQLPASSWORD=dtkpsw

rem The backup command storage target is described
SET BACKUPCOMMANDFOLDER=dbRelatedFileInstallFolder\BackupCommand

rem Extraction Key(Client date when omitting it,Server date when specifying SERVER)
SET HOW=SERVER

rem **************************************************************
rem * Processing part                                            *
rem **************************************************************
path "%BACKUPCOMMANDFOLDER%";%path%

echo Backup processing start(%TIME%)

%BKDRIVE%
CD %BKFOLDERNAME%
if ERRORLEVEL 1 goto recover7

echo Calculation on backup beginning day
rem Calculation on backup beginning day
"%BACKUPCOMMANDFOLDER%\DTKBFDM.EXE" %BKSTART%
SET BKSTARTDAY=%ERRORLEVEL%

rem Calculation on backup end day
"%BACKUPCOMMANDFOLDER%\DTKBFDM.EXE" 0
SET BKENDDAY=%ERRORLEVEL%

rem Calculation at deletion end date
"%BACKUPCOMMANDFOLDER%\DTKBFDM.EXE" %DELEND%
SET DELENDDAY=%ERRORLEVEL%

rem The folder is made at the backup start date(Log data)
MKDIR %BKSTARTDAY%
SET BKFOLDER=%BKDRIVE%%BKFOLDERNAME%\%BKSTARTDAY%\BK%BKSTARTDAY%
MKDIR "%BKFOLDER%"

rem The folder is made at the backup start date(Reference data)
SET LVFOLDER=%BKDRIVE%%BKFOLDERNAME%\%BKSTARTDAY%\LV%BKSTARTDAY%
MKDIR "%LVFOLDER%"

rem the backup target folder is made
SET MSFOLDER=%BKDRIVE%%BKFOLDERNAME%\%BKSTARTDAY%\MS%BKSTARTDAY%
```

```
MKDIR "%MSFOLDER%"

echo DTK service is stopped.
call "%BACKUPCOMMANDFOLDER%\DTKSERVICE.BAT" STOP

rem Backup of mastering system data
"%BACKUPCOMMANDFOLDER%\DTKMSTB.EXE" DTKDB %SQLUSER% %SQLPASSWORD% "%MSFOLDER%"

if ERRORLEVEL 1 goto recover3

rem Backup of log system data
"%BACKUPCOMMANDFOLDER%\DTKLGTB.exe" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY%
"%BKFOLDER%" %HOW%

if ERRORLEVEL 1 goto recover4

rem Backup of log system (Reference)
"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 3
"%LVFOLDER%\Application startup prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 9
"%LVFOLDER%\Printing prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 10
"%LVFOLDER%\Logon prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 12
"%LVFOLDER%\PrintScreen key prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 1
"%LVFOLDER%\Application startup log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 2
"%LVFOLDER%\Application termination log.csv" %how%
if ERRORLEVEL 1 goto recover5
"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 4
"%LVFOLDER%\Window title obtaining log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 17
"%LVFOLDER%\Window title obtaining (with URL) log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 5
"%LVFOLDER%\E-mail sending log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 7
"%LVFOLDER%\Device configuration change log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 8
"%LVFOLDER%\Printing operation log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 11
"%LVFOLDER%\File export log.csv" %how%
if ERRORLEVEL 1 goto recover5
```

```
"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 6
"%LVFOLDER%\Command operation log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 13
"%LVFOLDER%\File operation log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 16
"%LVFOLDER%\E-mail attachment prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 90
"%LVFOLDER%\Linkage application log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 14
"%LVFOLDER%\Logon,Logoff log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 24
"%LVFOLDER%\FTP operation prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 25
"%LVFOLDER%\FTP operation log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 29
"%LVFOLDER%\Web operation prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 31
"%LVFOLDER%\Web operation log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 34
"%LVFOLDER%\E-mail sending interruption log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 37
"%LVFOLDER%\Clipboard operation log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 38
"%LVFOLDER%\Clipboard operation prohibition log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 106
"%LVFOLDER%\Incoming outgoing calls log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKLG1T.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY% 107
"%LVFOLDER%\Application configuration change log.csv" %how%
if ERRORLEVEL 1 goto recover5

"%BACKUPCOMMANDFOLDER%\DTKSTCV.EXE" DTKDB %SQLUSER% %SQLPASSWORD% %BKSTARTDAY% %BKENDDAY%
"%LVFOLDER%\Configuration Change Log.csv"
if ERRORLEVEL 1 goto recover5

rem Deletion of log system data
"%BACKUPCOMMANDFOLDER%\DTKDELR.exe" DTKDB %SQLUSER% %SQLPASSWORD% 00000000 %DELENDDAY% -Y %HOW%
```

```
if %ERRORLEVEL% LSS 100 goto recover6

"%BACKUPCOMMANDFOLDER%\DTKDELST.EXE" DTKDB %SQLUSER% %SQLPASSWORD% 00000000 %DELENDDAY% -Y
if %ERRORLEVEL% LSS 100 goto recover6

goto allend0

:recover1
echo It made an error of the stop of level control service.
echo The backup is discontinued, and the DTK service (level control service) is started.
goto allend1

:recover2
echo It made an error of the stop of server service.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:recover3
echo It made an error of the backup of administrative information.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:recover4
echo It made an error of the backup of log information.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:recover5
echo It made an error of the backup of log information (Reference).
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:recover6
echo It made an error of the deletion of log information.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:recover7
echo The backup folder does not exist.
echo The backup is discontinued, and the DTK service (level control service,server service) is
started.
goto allend1

:allend0
echo The DTK service is started.
call "%BACKUPCOMMANDFOLDER%\DTKSERVICE.BAT" START
echo The schedule ended normally.(%TIME%)
EXIT /B 0

:allend1
echo The DTK service is started.
call "%BACKUPCOMMANDFOLDER%\DTKSERVICE.BAT" START
echo The schedule ended abnormally.(%TIME%)
EXIT /B
```

Example of Creating DTKTask_DailySchBackup.bat

Change the database-related file installation folder according to the environment.
Change the underlined item in bold to "DailySch2.bat" below.

```
@echo off
SETLOCAL


rem **********************************************************
rem *                                                        *
rem *    Systemwalker Desktop Keeper Maintenance tool         *
rem *                                                        *
rem *    Process Name : Registration batch                    *
rem *    Function Name : DTKTask_DailySchBackup.bat            *
rem *                                                        *
rem *    Copyright (C) FUJITSU LIMITED 2012-2015              *
rem *                                                        *
rem **********************************************************
rem
rem **********************************************************
rem * Setting                                                *
rem **********************************************************
set BACKUPCOMMANDFOLDER=dbRelatedFileInstallFolder\BackupCommand


rem **********************************************************
rem * Processing                                             *
rem **********************************************************
rem Calculation on execution day
"%BACKUPCOMMANDFOLDER%\DTKBFDM.EXE" 0
SET EXECDAY=%ERRORLEVEL%

rem The execution log is made by the log file name at the execution date.(e.g.20140112.log)
rem The log file is stored in the folder set to "Start in (optional)" when the task is registered.
call "%BACKUPCOMMANDFOLDER%\DailySch2.bat" > %EXECDAY%.log
if ERRORLEVEL 1 goto allend1


EXIT /B 0


:allend1
EXIT /B 1
```

Example of Result Logs of Batch File Execution

The execution result log (%EXECDAY%.log) records the execution results of the registered DailySch2.bat file in the preceding example.

```
Setting begins
Backup processing start(19:30:50.97)
Calculation on backup beginning day
DTK service is stopped.
Sat 05/23/2015-19:30:51.23 -DTKSERVICE----------------------------------------------------------
Sat 05/23/2015-19:30:51.23 [ Service termination processing of the management server (STOP) ]
Sat 05/23/2015-19:30:51.25 ----------------------------------------------------------------------
Sat 05/23/2015-19:30:51.83 The service of POSTGRESQL(Operation)        :operating
Sat 05/23/2015-19:30:52.14 The service of POSTGRESQL(Log view)         :operating
Sat 05/23/2015-19:30:52.15 The service of SYMFOWARE(Log analyze)        :unregistration
Sat 05/23/2015-19:30:52.48 The service of management server(SWLevelControlService)      :operating
Sat 05/23/2015-19:30:52.75 The service of management server(SWServerService)        :operating
Sat 05/23/2015-19:30:52.76 The service of management server(Log analyze)         :unregistration
Sat 05/23/2015-19:30:52.78 The service of iOS management database          :unregistration
Sat 05/23/2015-19:30:52.79 The service inquiry of the management server ended.
Sat 05/23/2015-19:30:52.81 The service of the management server (SWLevelControlService) is stopped.
Sat 05/23/2015-19:30:55.39 The SWLevelControlService was stopped.
Sat 05/23/2015-19:30:55.40 The service of the management server (SWServerService) is stopped.
Sat 05/23/2015-19:30:58.29 The SWServerService was stopped.
Sat 05/23/2015-19:30:59.04 The service of POSTGRESQL(Operation)        :operating
Sat 05/23/2015-19:30:59.21 The service of POSTGRESQL(Log view)        :operating
Sat 05/23/2015-19:30:59.23 The service of SYMFOWARE(Log analyze)         :unregistration
```

```
Sat 05/23/2015-19:30:59.38 The service of management server(SWLevelControlService)      :halt
condition
Sat 05/23/2015-19:30:59.54 The service of management server(SWServerService)      :halt condition
Sat 05/23/2015-19:30:59.54 The service of management server(Log analyze)      :unregistration
Sat 05/23/2015-19:30:59.55 The service of iOS management database      :unregistration
Sat 05/23/2015-19:30:59.57 Service stopped.
2015/05/23 19:30:59  Backup management information collectively - Start
2015/05/23 19:30:59
2015/05/23 19:30:59   Database   :  DTKDB
2015/05/23 19:30:59   Directory   :   D:\BACKUP\20150516\MS20150516
2015/05/23 19:30:59
2015/05/23 19:30:59   - LEVELOBJECT
2015/05/23 19:30:59     Output file name   : D:\BACKUP\20150516\MS20150516\LEVELOBJECT.csv
2015/05/23 19:30:59     Number of output items.....11
2015/05/23 19:30:59
2015/05/23 19:30:59   - LEVELCOMPOSITION
2015/05/23 19:30:59     Output file name   : D:\BACKUP\20150516\MS20150516\LEVELCOMPOSITION.csv
2015/05/23 19:30:59     Number of output items.....10
2015/05/23 19:30:59
2015/05/23 19:30:59   - PRINTPERMISSION
2015/05/23 19:30:59     Output file name   : D:\BACKUP\20150516\MS20150516\PRINTPERMISSION.csv
2015/05/23 19:30:59     Number of output items.....0
2015/05/23 19:30:59


(Omitted)


2015/05/23 19:31:15
2015/05/23 19:31:15   - FILEBRINGOUTLOG
2015/05/23 19:31:15     Number of deleted items.....0
2015/05/23 19:31:15
2015/05/23 19:31:15   - LOGKEYWORDS
2015/05/23 19:31:15     Number of deleted items.....0
2015/05/23 19:31:15
2015/05/23 19:31:15   - FILEACCESSLOG
2015/05/23 19:31:15     Number of deleted items.....0
2015/05/23 19:31:15
2015/05/23 19:31:15   - SESSIONMANAGE
2015/05/23 19:31:15     Number of deleted items.....0
2015/05/23 19:31:15
2015/05/23 19:31:15  Delete log information - End
2015/05/23 19:31:15  Delete configuration change log information - Start
2015/05/23 19:31:15
2015/05/23 19:31:16  Database   :  DTKDB
2015/05/23 19:31:16  Processing start date   :  00000000
2015/05/23 19:31:16  Processing finish date   :  20150222
2015/05/23 19:31:16  Deletion indication   :  -Y
2015/05/23 19:31:16
2015/05/23 19:31:16     Processing 2015/01/01 ... 71 items are deleted
2015/05/23 19:31:16     Number of deleted items.....71
2015/05/23 19:31:16
2015/05/23 19:31:16  Delete configuration change log information - End
The DTK service is started.
Sat 05/23/2015-19:31:17.10 -DTKSERVICE---------------------------------------------------
Sat 05/23/2015-19:31:17.10    [ service start processing (START) of the Management server ]
Sat 05/23/2015-19:31:17.11 ---------------------------------------------------------------
Sat 05/23/2015-19:31:17.55 The service of POSTGRESQL(Operation)      :operating
Sat 05/23/2015-19:31:17.82 The service of POSTGRESQL(Log view)      :operating
Sat 05/23/2015-19:31:17.83 The service of SYMFOWARE(Log analyze)      :unregistration
Sat 05/23/2015-19:31:18.07 The service of management server(SWLevelControlService)      :halt
condition
Sat 05/23/2015-19:31:18.27 The service of management server(SWServerService)      :halt condition
```

```
Sat 05/23/2015-19:31:18.29 The service of management server(Log analyze)         :unregistration
Sat 05/23/2015-19:31:18.30 The service of iOS management database         :unregistration
Sat 05/23/2015-19:31:18.30 The service inquiry of the management server ended.
Sat 05/23/2015-19:31:18.35 The service of the management server (SWLevelControlService) is started.
Sat 05/23/2015-19:31:20.46 The service of the management server (SWServerService) is started.
Sat 05/23/2015-19:31:25.30 The service of POSTGRESQL(Operation)         :operating
Sat 05/23/2015-19:31:25.52 The service of POSTGRESQL(Log view)         :operating
Sat 05/23/2015-19:31:25.54 The service of SYMFOWARE(Log analyze)         :unregistration
Sat 05/23/2015-19:31:25.72 The service of management server(SWLevelControlService)         :operating
Sat 05/23/2015-19:31:25.91 The service of management server(SWServerService)         :operating
Sat 05/23/2015-19:31:25.91 The service of management server(Log analyze)         :unregistration
Sat 05/23/2015-19:31:25.93 The service of iOS management database         :unregistration
Sat 05/23/2015-19:31:25.94 Service was started.
The schedule ended normally.(19:31:26.35)
```

Back up user assets

Refer to "3.1.1.2 User Assets" for details.

3.1.3 Restoring User Assets

The restoration function provided by the product carries the following Restoration Tool.

Restoration Tool

Set the restoration conditions on the GUI before restoring data.

The Restoration Tool can restore the data that is backed up through the following two methods:

- Backup Tool

- Backup commands

Data backed up using older versions of Management Server and Master Management Server can also be restored.
The following data can be restored by the Restoration Tool:

- Management information

- Log information (log data in the database and command logs)

For details about the data to be restored, refer to "3.1.1.2 User Assets".

In addition, the time required by data restoration can be estimated according to the number of logs to be restored. The estimation is as follows:

- 5,000 per second (Xeon, 2.0 GHz, 2 GB memory, and RAID1 architecture)

  Note: More time may be consumed, depending on the server performance and RAID architecture.

The operational status of the Restoration Tool will be output to event logs.

DTKTBLRESTOR (restore database command) is used to execute a restore for the Log Viewing Database, however, it cannot be used for the Operation Database.

swss_MDMDB_RESTORE.exe (restore iOS management database command)

This command is used to restore the iOS management database. Refer to "swss_MDMDB_RESTORE.exe (Restore iOS Management Database)" in the *Systemwalker Desktop Keeper Reference Manual*.

The restore iOS management database command allows you to restore backed up iOS management databases, using the following feature:

- DTKMSTB.EXE (backup of management information)

The operational status of the restore iOS management database command is output to a log file.

Note

If Systemwalker Desktop Keeper and Systemwalker Desktop Patrol coexist, use SDSVSetMS.EXE (change configuration of Smart Device Relay Server command) to check the host name of the iOS management database connected to the Smart Device Relay Server. Restore the data that was backed up on the server that matches with the iOS management database host name displayed in "iOSmgr.h" in the server that matches with the host name displayed in "iOSmgr.h".

3.1.3.1 Using the Restoration Tool

This section describes how to restore data from the database by using the Restoration Tool provided by the Systemwalker Desktop Keeper.

Note

Notes on using the Restoration Tool

[Do not restore data in the operation database]

When the Management Server or Master Management Server is running, do not restore the "management information". If the "management information" is overwritten, it may result in incomplete "management information" and "log information".

[Separately restore the terminal operation settings of the management console and the settings of the Server Settings Tool]

These settings cannot be backed up by the Backup Tool (GUI) or backup commands. Therefore, re-set these settings after the Restoration Tool restores the database.

[After the management information is restored, the old information is deleted]

After the management information is restored, the old information is overwritten. Note that the difference between the old information and the restored information will not be displayed.

[Time required by restoration]

When adding and restoring the log information in the environment where log information already exists, index information will be created after restoration; therefore, restoration will take more time. (It is three times as long as the time used by log information restoration in the environment where there are no logs.)

[The number of records when backing up the management information may be different to the number of records when executing a restore]

In the Restoration Tool, inconsistent management information is deleted, which may result in a difference between the number of records during backup and the number of records during a restore.

[When restoring the management information of the Operation Database, you should also restore the iOS management database]

When managing iOS devices, restore the data backed up in the same period so as to avoid inconsistencies between the Operation Database and iOS management database.
Refer to "swss_MDMDB_RESTORE.exe (Restore iOS Management Database)" in the *Systemwalker Desktop Keeper Reference Manual* for details on how to use the restore iOS management database command.

Point

Logon history

The logon history will be output to event logs (application).

Restore the Database in Use

The procedure for using the Restoration Tool is as follows:

1. When managing Android or iOS devices, use SDSVService.bat (start/stop service of Smart Device Relay Server command) to stop 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 on the command.

2. Log on the Windows OS as a user of the Administrators group or Domain Admins group. If there is another running application, exit it.

3. Reconfigure the following settings information of the Server Settings Tool that you took note of when executing the backup.

   - **System settings**

   - **Active Directory linkage settings** Note: When using the Active Directory linkage feature

   - **Administrator notification settings**

   - **Management Server settings**

   - **Trace settings**

   - **Folder / CT self version upgrade settings**

   Refer to "2.3.6 Set Environment of Management Server/Master Management Server" for details on how to display each window of the Server Settings Tool.

4. Select **All Programs** > **Systemwalker Desktop Keeper** > **Server** > **Restoration Tool** from the **Start**/**Apps** menu on the PC installed with the Management Server or Master Management Server.

   The **Restoration Tool** window is displayed. Click **Yes** to confirm restoration in the running database.

   The **Systemwalker Desktop Keeper - Operation Database Restoration Tool** window is displayed.

5. Log in by using the user ID (granted with the authority to back up and restore information) registered in the Server Settings Tool. (The user ID and password of the Primary Administrator can also be used for login.)

6. Click **OK**.

   The **Operation Database Restoration Tool** window is displayed.
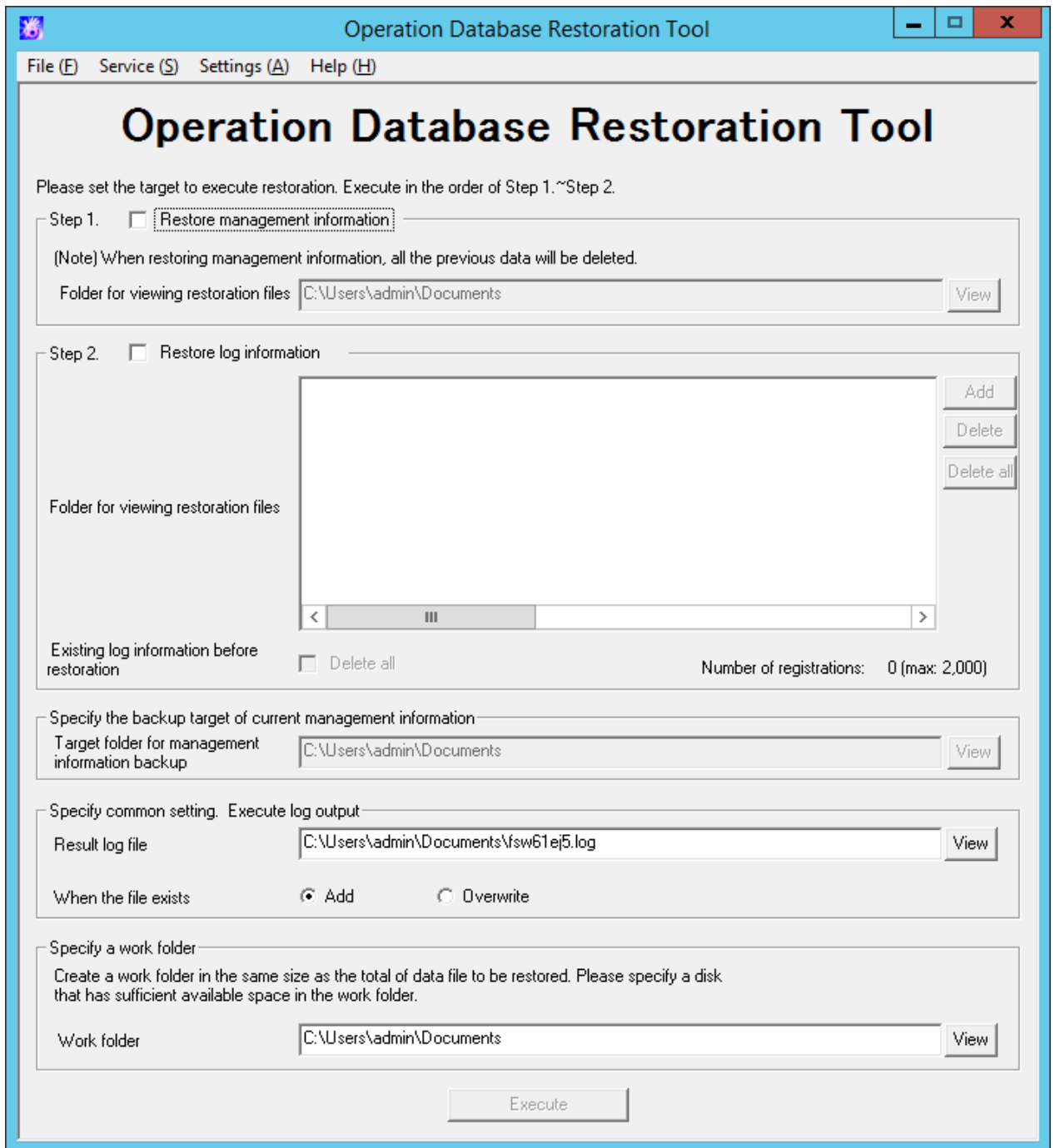
The following table describes the menu bar in the **Operation Database Restoration Tool** window.

Menu Bar		Function Summary
File	**Exit**	Exit the Restoration Tool.
Service	**Confirm Service Status**	Display the operational status of the "Level Control Service" and "Server Service" on the target server.
	Start Service	Start the "Level Control Service" and "Server Service" on the target server.

Menu Bar			Function Summary
	Stop Service		Stop the "Level Control Service" and "Server Service" on the target server.
Settings	**Trace Restoration Tool**	**No**	Do not collect the traces of the Restoration Tool.
		Summary	Collect the traces of the Restoration Tool in summary mode.
		Details	Collect the traces of the Restoration Tool in details mode.
Help	**Online Help**		Display the online help manual.
	Version Information		Display the copyright information and version information.

7. Before restoring the "management information" and "log information" by using the Restoration Tool, it is necessary to stop the "Level Control Service" and "Server Service" on the target server. Select **Stop Service** from the **Service** menu. A confirmation window is displayed. Click **OK** in the window to stop the services.

8. The operation result window is displayed. Click **OK** in the window.

9. In the **Restoration Tool of database for viewing logs** window, enter the information described in steps 1 and 2, common setting information, and working folder information.

Step 1 Restore management information

Item Name	Description
Restore management information	Select this when restoring the management information.
Folder for viewing restoration files	Specify the folder that saves the files used for restoration. (Specify the folder that contains the LEVELTARGET.csv and LEVELCOMPOSITION.csv files backing up the management information.)
	There are two methods for specifying such a folder:
	- Enter the absolute path of the folder.
	- Enter the absolute path of the folder that saves the management information used for restoration.
	- Click **Browse**.
	- The **View Folders** window is displayed. Select the folder that saves the management information used for restoration and then click **OK**.
	An absolute path can contain a maximum of 189 single-byte characters (94 fullwidth characters). The folder name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".

Step 2 Restore log information

Item Name	Description
Restore log information	Select this when restoring the log information.
Folder for viewing restoration files	Click **Add** and then specify the folder that saves the file used for restoration. Multiple files can be specified. (Specify the folder that contains the COMMONLOG1.csv and LOGKEWORDS.csv files backing up the log information.)
	The related buttons and check boxes are as follows:
	- **Add** button Select the folder as the restoration target.
	- **Delete** button Delete the selected folder from the folder list.

Item Name	Description
	- **Delete All** button Delete all the folders from the folder list. - Delete All (Fast Delete) check box This check box can only be selected when restoring the Log Viewing Database, so it is disabled in the Operation Database Restoration Tool. An absolute path can contain a maximum of 189 single-byte characters (94 fullwidth characters). If an absolute path containing more than 189 halfwidth characters (94 fullwidth characters) is entered, only 189 halfwidth characters (94 fullwidth characters) are displayed.

Specify the backup target of current management information

Item Name	Description
Target folder for management Information backup	Specify the target folder that saves the backup management information. (To avoid errors during management information restoration, back up the most recent management information before restoration is carried out.) There are two methods: - Enter the absolute path of the folder. - Enter the absolute path of the folder that saves the management information used for restoration. - Click **Browse**. The **Viewing Folder** window is displayed. Select the folder that saves the management information used for restoration and then click **OK**. An absolute path can contain a maximum of 189 single-byte characters (94 fullwidth characters). The folder name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".

Specify common settings, Execute log output

Item Name	Description
Result log file	Specify the file for saving the execution results of the Restoration Tool. There are two methods for specifying such a file: - Enter the absolute path of a file. - Enter the absolute path of a file for saving the output execution results. - Click **Browse**. - The **Open File** window is displayed. Select the folder for saving the result log file, enter the file name, and then click **Open**. An absolute path can contain a maximum of 255 single-byte characters (127 fullwidth characters). The file name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".
When the file exists	Select the processing operation to be performed when the result log file exists at the location specified by **Result Log File**. - Add - Add a new result log to the end of the result log file if the file exists at the location specified by **Result Log File**. - Overwrite

Item Name	Description
	- Overwrite the last result log in the result log file if the file exists at the location specified by **Result Log File**.

Specify a work folder

Item Name	Description
Work folder	Specify a folder for saving the working file.
	When restoring management information to this working folder, a working file that is 1.2 times the total size of the management information data files will be created.
	When restoring the log information, a working file that is 1.2 times the largest log table from the total of each log table under all of the folders will be created, therefore, ensure that there is sufficient space in the specified folder (for example, if the total size of all FILEACCESSLOG.csv files is 10 GB, then 12 GB will be required). The minimum available space required is 10 MB.
	After restoration is completed, the working file will be deleted.
	- Enter the absolute path of a folder.
	- Enter the absolute path of a working folder. Only the local hard disk can be specified for the working folder.
	- Click **Browse**.
	- The **View Folders** window is displayed. Specify a working folder and then click **OK**.
	An absolute path can contain a maximum of 189 single-byte characters (94 fullwidth characters). The folder name should not contain the following symbols: "\" "/" ":" "*" "?" """ "<" ">" "|".

10. After completing all the settings, click **Execute**.

    The confirmation window is displayed.

11. Click **OK** to start execution. The **Restoration Status** window will be displayed and the restoration process will start.

12. When the restoration process is completed successfully, the process completion window is displayed. Click **OK** in the window.

13. After confirming the execution status, click **Close**.

14. When managing iOS devices, execute swss_MDMDB_RESTORE.exe (restore iOS management database command) to restore iOS management databases. Execute this command on the Management Server.

15. Start the stopped "Level Control Service" and "Server Service". Select **Start Service** from the **Service** menu. The service startup confirmation window is displayed. Click **OK** in the window to start the services.

16. The operation result window is displayed. Click **OK** in the window.

17. Re-set the following settings in the **Terminal Operation Settings** window of the management console, which are recorded during backup.

    Perform the following steps to display the **Terminal Operation Settings** window:

    a. Start **Management Console**.

    b. Select **Terminal Operation Settings** from the **Operation Settings** menu.
       The **Terminal Operation Settings** window is displayed.

18. When managing Android or iOS devices, use SDSVService.bat (start/stop service of Smart Device Relay Server command) 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.

Restore the Database for Log Viewing

P Point

• •

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 client (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 client (CT) operation log window becomes the Management Server IP address used when building the Log Viewing Database.

• •

1. Log on the Windows OS as a user of the Administrators group or Domain Admins group. If there are other running applications, exit them.

2. Select **All Programs** > **Systemwalker Desktop Keeper** > **Server** > **Restoration Tool of Database for Log Viewing** from the **Start**/**Apps** menu on the computer installed with the Management Server or Master Management Server.

   The **Restoration Tool of database for viewing logs** window is displayed.
   Enter the user ID (user ID with backup and restore permission) and password registered using the Server Settings Tool, and then click **OK**.

You can also log in using the primary administrator user ID and password
The **Restoration Tool of database for viewing logs** window is displayed.
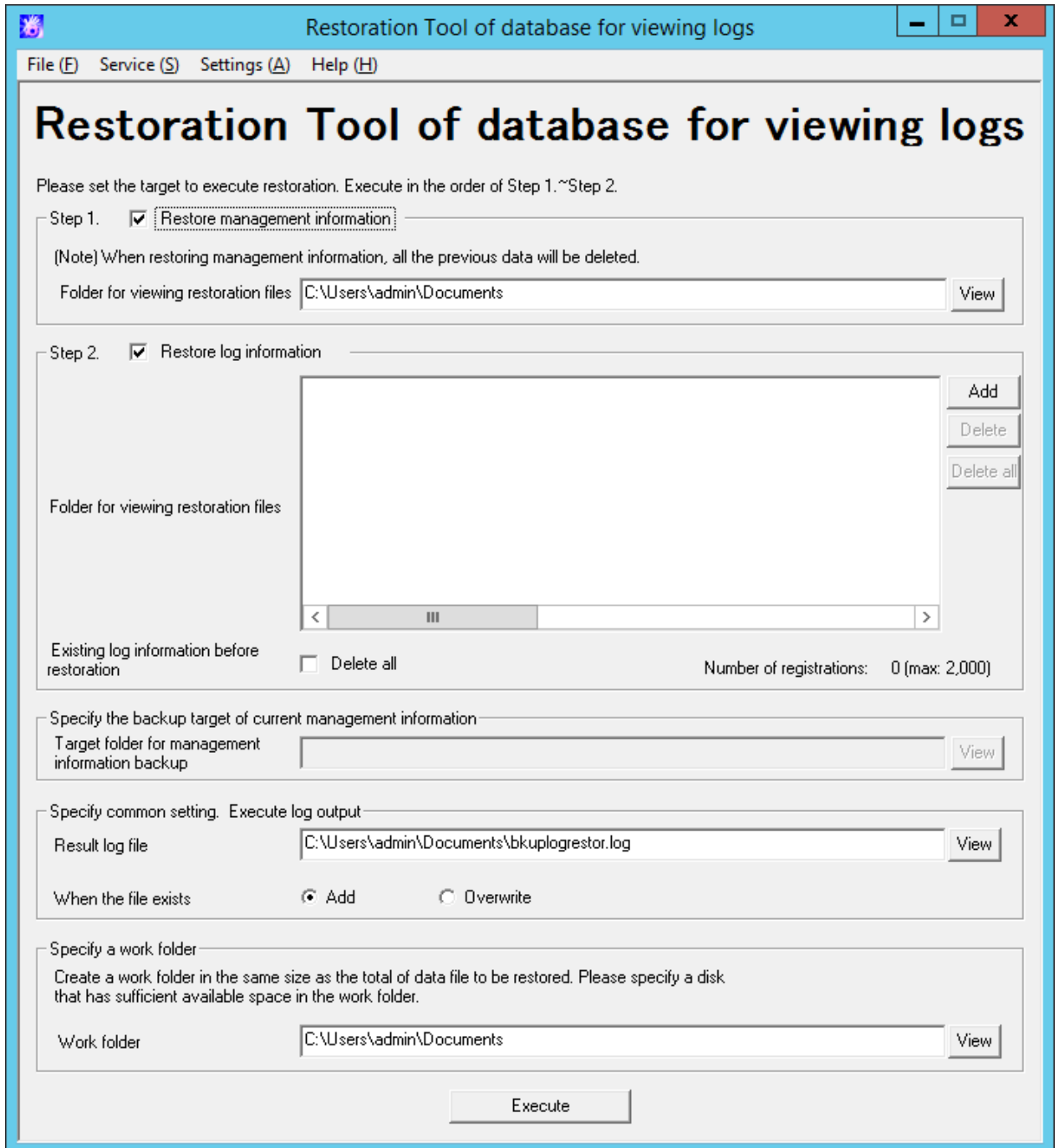
Except for certain items, the menu bar settings and input information of the Database Restoration Tool for Log Viewing are same as those of the Operation Database Restoration Tool. For details about the items that are the same for both tools, refer to the description about the Operation Database Restoration Tool. The items that can be set only by the Database Restoration Tool for Log Viewing are described here.

Step 2 Restore log information

Item Name	Description
Existing log information before restoration	If the database for log viewing contains log information, delete all the log information from the database before restoration.

3. After completing all the settings, click **Execute**.
   The confirmation window is displayed.

4. Click **OK** to start execution. The **Restoration Status** window will be displayed and the restoration process will start.

5. When the restoration process is completed successfully, the process completion window is displayed. Click **OK** in the window.

6. After confirming the execution status, click **Close**.

Exit the Restoration Tool

This describes how to exit the Restoration Tool.

1. To exit the Restoration Tool, select **Exit** from the **File** menu.

   The exit confirmation window is displayed.

2. Select whether to save the conditions specified in the Restoration Tool window. Click **Yes** to exit with the conditions saved, click **No** to exit without saving the conditions, or click **Cancel** to cancel the exiting operation.
   The menu settings (**Settings of Debugging Trace**) are saved when they are set.

Restore user assets

Refer to "3.1.1.2 User Assets" for details.

3.2 Smart Device Relay Server Maintenance

This section explains how to maintain the Systemwalker Desktop Keeper Smart Device Relay Server.

3.2.1 How to Back Up Assets

This section explains how to back up the assets of the Systemwalker Desktop Keeper Smart Device Relay Server.

Execute the following command:

```
SDSVBackup.bat -dir backupDir
```

Refer to "SDSVBackup.bat (Backup of Smart Device Relay Server)" in the *Systemwalker Desktop Keeper Reference Manual* for details.

Note

When Systemwalker Desktop Keeper coexists with Systemwalker Desktop Patrol, back up Systemwalker Desktop Patrol also.

3.2.2 How to Restore the Assets

This section explains how to restore the assets of the Systemwalker Desktop Keeper Smart Device Relay Server.

1. Use SDSVService.bat (start/stop service of Smart Device Relay Server command) to stop the service of the Smart Device Relay Server.
   Execute this command on the Smart Device Relay Server.

2. Execute the following command:

   ```
   SDSVRestore.bat -dir backupDir
   ```

3. Using swss_ImportAppleCert.bat (register Apple Inc. certificate command), register again the MDM certificate that was prepared using the procedure in "2.2 Advance Preparation".

4. After restoration, use SDSVService.bat (start/stop service of Smart Device Relay Server command) to start the service of the Smart Device Relay Server.
   Execute this command on the Smart Device Relay Server.

Refer to "Command Reference" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

3.3 Maintenance of Log Analyzer Server

This section describes how to maintain the Log Analyzer Server of the Systemwalker Desktop Keeper.

3.3.1 Summary and Backup Target Assets

This section describes the assets to be backed up and restored on the Systemwalker Desktop Keeper Log Analyzer Server.

The backup targets on the Log Analyzer Server include the setting information, statistical information, and log information. These three types of information are called "user assets". The following table describes the targets and methods of user asset backup.

	User Asset		
	Setting Information	**Statistical Information**	**Log Information**
Backup method	Backup commands	None	Data Transmission Command
Backup timing	Scheduled. Backup must be carried out when the settings change.	None	During data transmission
Backup procedure	Manual	None	Automatic
Backup file	Setting information backup CSV	None	Logs information backup CSV
Restoration method	Backup commands	None (Re-collect statistics.)	Re-transfer data through the data transfer command.

Summary on Log Analyzer Server Maintenance
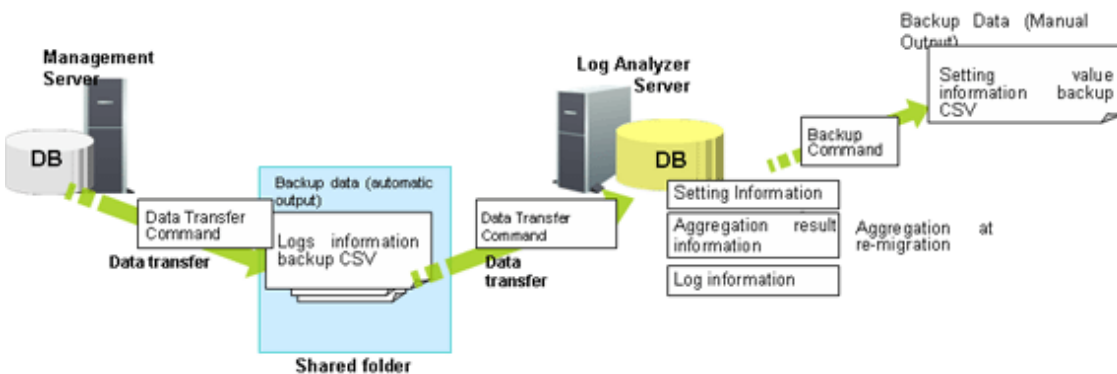
The "user assets" on the Log Analyzer Server include the "setting information", "statistical information", and "log information". The backup commands are used to back up and restore the setting information.
The log information output by the data transmission command directly becomes the backup data.
The statistical information is restored by re-transferring the log information backup CSV file to the Log Analyzer Server for statistics collection.
The setting information backup CSV and log information backup CSV files contain the backup data. Therefore, properly save them to external media without changing the folder structure.

The following table lists the names of the tables and files related to the setting information backed up by the backup commands.

Type	Table	Usage	File Name
Setting Information	SETTING_INF	Setting information	SETTING_INF.csv
	REMOVEPC	Exclusion Condition Settings	REMOVEPC.csv
	KEYWORD_INF	Screening Condition Settings	KEYWORD_INF.csv
	GROUPMASTER	Work group information	GROUPMASTER.csv
	USERMASTER	User information	USERMASTER.csv
	SVMASTER	Management Server settings	SVMASTER.csv
	PCMASTER	Terminal information	PCMASTER.csv
	PCMASTER_SV	Terminal information 2	PCMASTER_SV.csv
	GROUPMASTER_SV	Work group 2	GROUPMASTER_SV.csv
	ALARMPRINTMASTER	Upper threshold information for printing	ALARMPRINTMASTER.csv
	COMPOSITIONMASTER	configuration information	COMPOSITIONMASTER.csv
	SVNODEMASTER	Server node information	SVNODEMASTER.csv
	USERSECTIONMASTER	Section management information	USERSECTIONMASTER.csv
	PRINTERMASTER	All-in-one PC list	PRINTERMASTER.csv
	PRINTERCOUNT_SETTING_INF	Settings of the all-in-one PC linkage	PRINTERCOUNT_SETTING_INF.csv
	PRINTER_PAPERNUM_BASIC	Statistical information of the all-in-one PC linkage	PRINTER_PAPERNUM_BASIC.csv
	TARGETMASTER	Statistical unit of the all-in-one PC linkage	TARGETMASTER.csv
	PRINTUSERMASTER	User information of the all-in-one PC linkage	PRINTUSERMASTER.csv
	PRINTUSER_PAPERNUM_BASIC	User statistical information of the all-in-one PC linkage	PRINTUSER_PAPERNUM_BASIC.csv

Note

- When the settings change, ensure the statistics are re-collected during backup. Otherwise, the statistics after restoration may be different from those before restoration.

- The recommended log storage life is one year. If the log storage life is shorter than one year, the statistics stored longer than the log storage life will be deleted during statistics re-collection.

3.3.2 Back Up Assets

Among the user assets including setting information, statistical information, and log information, the log information output by the data transmission command directly becomes the backup data. The statistical information does not require backup. The setting information is backed up by using the backup commands.

3.3.2.1 Using Backup Commands

This section describes how to process the data stored in the database by using the backup commands provided by the Systemwalker Desktop Keeper Log Analyzer Server.

The backup commands do not provide the task scheduling function. The Task Scheduler provided by the OS by default or the task scheduling software ARCserve can be used to set scheduled tasks. If using the Windows Server(R) 2008 or Windows Server(R) 2012, set scheduled tasks as the administrator.

![Note icon] **Note**

. . . .

Notes on using the backup commands

[Level at which this command can be used]

> This command can be used in V15.1.0 or later. These commands may fail if they are used in the environment constructed under other versions.

[Available space on the output target disk]

> Ensure that there is sufficient available space on the disk specified as the output target disk for the backup files.

[Execution privileges for Windows Server(R) 2008 and Windows Server(R) 2012]

> In Windows Server(R) 2008 and Windows Server(R) 2012, execution of the backup commands requires administrator authority. Before running the backup commands, log on to the Windows OS as a user of the Administrators group or Domain Admins group.

[Enable the command extension function of the command prompt]

> Execution of the backup commands requires that the command extension function of the command prompt be enabled.
> The command extension function is enabled by default. Run "echo %CMDEXTVERSION%" in the command prompt window. If the output value is larger than or equals to 2, you can infer that the command extension function is enabled.

[Backup timing]

> Follow the principle of carrying out backup immediately upon a change of settings. The data lost before backup cannot be backed up or restored.

. . . .

Target folder that saves the backup commands:

> [Installation folder of the Log Analyzer Server]\bin\SWDTLAENV
> Example: C:\Program Files\Fujitsu\Systemwalker Desktop Keeper\LogAnalyzer\Server\bin\SWDTLAENV

Command Name	Operation
LADBBKRS.BAT	Back up each table related to "setting information" described in "3.3.1 Summary and Backup Target Assets" as a CSV file.

> Refer to "LADBBKRS.BAT(Backup/Restore Log Analyzer Settings)" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

Start Backup

For details about how to use the backup commands, refer to "LADBBKRS.BAT(Backup/Restore Log Analyzer Settings)" of the *Systemwalker Desktop Keeper Reference Manual*.

> 🛈 **Note**
>
> ....
>
> **Do not use the Log Analyzer during backup.**
>
> Do not use the Log Analyzer functions, such as the Web console, Report Output Tool, data transfer command, and user management command, before backup or restoration.
>
> ....

3.3.3 Restore Assets

3.3.3.1 Restoration Process

This section describes the restoration process.

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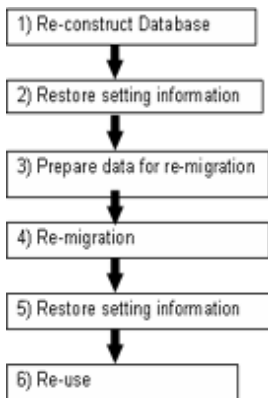
1. Log on as the Log Analyzer user (the Windows user account set during installation of the Log Analyzer Server).

2. Select **All Programs** > **Systemwalker Desktop Keeper** > **Log Analyzer** > **Operating Environment Maintenance Wizard** > from the **Start**/**Apps** menu to re-construct the database.

3. Use the setting information backup and restoration command (LADBBKRS.bat) of the Log Analyzer to restore the setting information backup CSV to the database.

   For details about the commands, refer to the "LADBBKRS.BAT (Backup/Restore Log Analyzer Settings Information)" in the *Systemwalker Desktop Keeper Reference Manual*.
   Example:

   ```
   LADBBKRS.bat -rs -d c:\backup
   ```

4. Copy the log information backup CSV from the external media to a shared folder (the folder specified by the -f option of the data transfer and deletion command adaptable to the Log Analyzer Server in step 5) without changing the folder structure.

5. Change the file name in the copied folder.

   - File name before change: conv_end

   - File name after change: trans_end

   This file exists under each folder named after a date (for example, 20080421_20080421).
   If there are a large number of such files, change the file names by running the following batch commands.
   [Example of a 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 a path to the folder.
:END
ECHO ON
```

For example, after copying the backup data from z:\DTKDATA to the share folder c:\DTKDATA, run the created batch commands.
Example:

```
conv.bat c:\DTKDATA
```

6. Use the transfer and deletion command (DTTOOLEX.EXE) adaptable to the Log Analyzer Server to re-transfer the log information backup CSV.
   The re-transfer process may take some time.
   For reference: The re-transfer of about 0.18 billion logs will take 24 hours.
   For details about the commands, refer to the "DTTOOLEX.EXE DTTOOLEX.EXE (Data Transfer to/Delete from the Log Analyzer Server)" in the *Systemwalker Desktop Keeper Reference Manual*.
   Example:

```
dttoolEx.exe -f c:\DTKDATA
```

7. Restore the setting information backup CSV to the database by using the restoration commands again.
   Example:

```
LADBBKRS.bat -rs -d c:\backup
```

8. Start operation again (by using the data transmission command and data transfer command).

Note

. . . .

Run the restoration commands for two times.
If step 7 is not performed to restore the setting information again, the data may be incorrectly restored. For example, the user ID may be deleted or the setting information may be outdated.

. . . .

3.3.3.2 Using the Restoration Commands

This section describes how to restore the backup data to the database by using the restoration commands provided by the Systemwalker Desktop Keeper Log Analyzer Server. The restoration commands are the same as the backup commands.

Note

. . . .

Notes on using the restoration commands

[Level at which this command can be used]

This command can be used in V15.1.0 or later. These commands may fail if they are used in the environment constructed under other versions.

[Execution privileges for Windows Server(R) 2008 and Windows Server(R) 2012]

In Windows Server(R) 2008 and Windows Server(R) 2012, execution of the restoration commands requires administrator authority. Before running the restoration commands, log on to the Windows OS as a user of the Administrators group or Domain Admins group.

[Enable the command extension function of the command prompt]

Execution of the restoration commands requires that the command extension function of the command prompt be enabled.
The command extension function is enabled by default. Run "echo %CMDEXTVERSION%" in the command prompt window. If the output value is larger than or equal to 2, you can infer that the command extension function is enabled.

. . . .

Target folder that saves the restoration commands:

[Installation folder of the Log Analyzer Server]\bin\SWDTLAENV

Example: C:\Program Files\Fujitsu\Systemwalker Desktop Keeper\LogAnalyzer\Server\bin\SWDTLAENV

Command Name	Operation
LADBBKRS.BAT	Restore each table related to "setting information" described in "3.3.1 Summary and Backup Target Assets" as a CSV file.

Refer to "LADBBKRS.BAT (Backup/Restore Log Analyzer Settings)" in the *Systemwalker Desktop Keeper Reference Manual* for details on each command.

Start Restoration

Refer to "LADBBKRS.BAT (Backup/Restore Log Analyzer Settings)" in the *Systemwalker Desktop Keeper Reference Manual* for details on the restoration command.

Note

・・・

Do not use the Log Analyzer during restoration.

Do not use the Log Analyzer functions, such as the Web console, Report Output Tool, data transfer command, and user management command, before backup or restoration.

・・・

Chapter 4 Upgrading

This chapter describes how to upgrade the version of Systemwalker Desktop Keeper.

4.1 Notes between Different Versions

This describes the operation status between different versions.

Between Master Management Server and Management Server

When the versions of the Master Management Server and the Management Server are different, they do not operate well. Make sure the versions are the same.

Between Management Server/Master Management Server and Log Analyzer Server

When the versions of the Management Server/Master Management Server and the Log Analyzer Server are different, they do not operate well. Make sure the versions are the same.

In addition, if you import data that was transferred between different versions of the Management Server and the Master Management Server, the servers do not operate well.

Between Management Server/Master Management Server and Management Console

When the versions of the Management Server/Master Management Server and the Management Console are different, they cannot operate well. Make sure the versions are the same.

Between Management Server/Master Management Server and Client (CT)

📒 Note

....

Communication security settings

To receive self version management requests from a client (CT) of V14.3.1 or earlier, switch the communication security settings. You can use the security enhancement command to switch the communication security settings. Refer to "DTKSETCN.exe (Security Enhancement)" in the *Systemwalker Desktop Keeper Reference Manual* for details on how to use the security enhancement command.

....

📒 Note

....

Verification when registering client (CT) devices

When registering a client (CT) earlier than V15.1.0 to a Management Server of V15.1.0 or later, you cannot use verification during registration of client (CT) devices. Cancel the client management password. Refer to "Perform Terminal Operation Settings" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

....

The operation when the versions of the Management Server/Master Management Server and the Client (CT) are different is displayed in the following table.

The CT version can be confirmed according to the CT version of the Management Console. The CT version is correspondent with product version/edition; refer to "CT Version" in the *Systemwalker Desktop Keeper Reference Manual* for information on this.

When confirming CT version in Client (CT), execute the following command:

```
fsw11ej7.exe <Password> /D /C
```

For details of the command, refer to "FSW11EJ7.EXE (System Maintenance)" of *Systemwalker Desktop Keeper Reference Manual*.

		Client (CT)							
		V12.0L20		V13.0.0		V13.2.0		V14.2.0	V15.1.0
		BE	SE	BE	SE	BE	SE		
Management Server Master Management Server	**BEV12.0L20**	Y	N	N	N	N	N	N	N
	SEV12.0L20	Y	Y	N	N	N	N	N	N
	BEV13.0.0	Y	N	Y	N	N	N	N	N
	SEV13.0.0	Y	Y	Y	Y	N	N	N	N
	BEV13.2.0	Y	N	Y	N	Y	N	N	N
	SEV13.2.0	Y	Y	Y	Y	Y	Y	N	N
	V14.2.0	Y	Y	Y	Y	Y	Y	Y	N
	V15.1.0	N	N	N	N	N	N	Y (*1)	Y

Y: Operates normally.

*1: Operates normally, but some features are restricted. Refer to "Note".

N: Operates abnormally.

📝 Note

. . . .

Communications between the Management Server or the Master Management Server and a client (CT)

Communications between the Management Server or the Master Management Server and a client (CT) are 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.

- Clients of V13.3.0 - V14.3.1 must be upgraded to V15.1, or the urgent updates released in September 2014 or later must be applied to the clients.

- Clients of V13.2.1 or earlier cannot be used. They must be upgraded to V15.1.0.

- After the Management Server is upgraded to V15.1.0, only a client of V15.0.0 or V15.1.0 can be installed.

. . . .

According to the client (CT) version/edition, policy function set in the Management Console of V15.1.0 will be restricted. According to client (CT) version/edition, whether each function can be operated are as follows:

V15.1.0 Supporting Functions	Client (CT)							
	V12.0L20		V13.0.0		V13.2.0		V14.2.0	V15.1.0
	BE	SE	BE	SE	BE	SE		
Collect File Operation Log (Local Drive)	N	N	N	N	N	N	Y	Y
Apply User Policy	N	N	N	N	N	N	Y	Y
Collect Linkage Application Log	N	N	N	N	N	N	Y	Y
Collect URL Information of Window Title Obtaining Log	N	N	N	N	N	N	Y	Y
Collect File Operation Log (Network Drive)	N	N	N	N	N	N	Y	Y
Confirm Recipient Address When E-mail Sending	N	N	N	N	N	N	Y	Y
View E-mail Content	N	N	N	N	N	N	Y	Y

V15.1.0 Supporting Functions	Client (CT)							
	V12.0L20		V13.0.0		V13.2.0		V14.2.0	V15.1.0
	BE	SE	BE	SE	BE	SE		
Set How to Send Operation Log (Excluding Sending Function with Specified Time)	N	N	N	N	N	N	Y	Y
Set How to Send Operation Log (Sending Function with Specified Time)	N	N	N	N	N	N	Y	Y
Collect Logon/Logoff Log	N	N	N	N	N	N	Y	Y
Log Filtering Function	N	N	N	N	N	N	Y	Y
Collect Screen Capture (and Set Screen Capture Conditions in Terminal Operation Settings)	N	N	N	N	N	N	Y	Y
Collect PrintScreen Key Operation Log	N	N	N	N	N	N	Y	Y
Original File Backup Function	N	N	N	N	N	N	Y	Y
Apply File Operation Log Acquisition Exclusion Folder (Excluding Arbitrary Folder Specifying Function)	N	N	N	N	N	N	Y	Y
Apply File Operation Log Acquisition Exclusion Folder (Arbitrary Folder Specifying Function)	N	N	N	N	N	N	Y	Y
Record File Size of File Operation Log	N	N	N	N	N	N	Y	Y
Write in CD-R/RW Through File Export Utility	N	N	N	N	N	N	Y	Y
Write in DVD-R/RW Through File Export Utility (OS: Windows Vista(R), Windows(R) 7)	N	N	N	N	N	N	Y	Y
Set Conditions for Export in File Export Utility - Specify Period, Time and Week - Set How to Confirm Date and Time for Startup	N	N	N	N	N	N	Y	Y
Get Export Target USB Device Information in File Export Utility	N	N	N	N	N	N	Y	Y
Input the Reason for Export in File Export Utility	N	N	N	N	N	N	Y	Y
Collect PC Startup Log/PC Shutdown Log/PC Sleep Log/PC Restoration Log	N	N	N	N	N	N	Y	Y
Collect FTP Operation Log	N	N	N	N	N	N	Y	Y
Collect Web Downloading Operation Log	N	N	N	N	N	N	Y	Y

V15.1.0 Supporting Functions	Client (CT)							
	V12.0L20		V13.0.0		V13.2.0		V14.2.0	V15.1.0
	BE	SE	BE	SE	BE	SE		
Collect Web Uploading Operation Log	N	N	N	N	N	N	Y	Y
- Apply FTP Server Connection Prohibition Policy	N	N	N	N	N	N	Y	Y
- Apply URL Access Prohibition Policy	N	N	N	N	N	N	Y	Y
- Apply Web Downloading Prohibition Policy	N	N	N	N	N	N	Y (*1)	Y
Apply Web Uploading Prohibition Policy	N	N	N	N	N	N		Y
USB Device Individual Identification	N	N	N	N	N	N	Y	Y
Clipboard Operation Log	N	N	N	N	N	N	Y	Y
Apply Clipboard Operation Prohibition Policy	N	N	N	N	N	N	Y	Y
- Apply Network Drive Connection Prohibition Policy	N	N	N	N	N	N	Y	Y
- Apply DVD/CD Read Prohibition Policy	N	N	N	N	N	N	Y	Y
Collect PC Connection/PC Disconnect Log	N	N	N	N	N	N	Y	Y

Y: Operates normally.

N: Operates abnormally.

*1: The settings are designed so both web uploads and web downloads must be either prohibited or allowed.

> 📄 **Note**
> ....
> **Database capacity enlarged during version upgrade**
>
> In V15.1.0 or earlier, the database capacity will be enlarged as the database is modified. (According to the calculation condition changes, it will be enlarged 1.2 fold.) Thus, when changing from V15.0 or earlier, pay attention to the created size of the database.
> For the required disk capacity after version upgrade, refer to "Operating Environment" of *Systemwalker Desktop Keeper User's Guide*.
> ....

Between Log Analyzer Server and Report Output Tool

When the versions of the Log Analyzer Server and the Report Output Tool are different, they do not operate well. Make sure the versions are the same.

Between Management Server or Master Management Server and Smart Device Relay Server

When the versions of the Management Server or Master Management Server and Smart Device Relay Server are different, they do not operate well. Ensure that the versions are the same.

4.2 Upgrade Procedures

This describes the procedures for version upgrade.

4.2.1 Upgrade of Management Server/Master Management Server on the Same Server

Procedures for upgrading the Management Server/Master Management Server from the old Systemwalker Desktop Keeper to V15.1.0 are described through the following 3 patterns:

- When upgrading from V12

- When upgrading from V13

- When upgrading from V14/V15

Also, the workflow for upgrading the Log Analyzer Server to the latest version is described below. It requires the Management Server or Master Management Server to be upgraded beforehand.

- Upgrading the Log Analyzer ServerUpgrading the Log Analyzer Server

- When newly install Systemwalker Desktop Keeper V15.1.0, refer to "Chapter 2 Installation"

Note

· ·

Before upgrading to V15.1.0, the user assets must be backed up so they can be restored after the upgrade to V15.1.0.
The Operation Database and the Log Viewing Database must be redefined. V15.1.0 does not provide SWDTK_DBCV (conversion of old database command) that was provided by V13.2.0.

· ·

Note

· ·

Backup operation after version upgrade

- The old backup command cannot be used after version upgrade. Use the backup command of V15.1.0.

- The backup command has been modified in V12 or later, so modify the schedule under the condition that all of the following conditions are met. Confirm that the backup command can be called correctly after modification.
  For changes of the backup command name, refer to "Management Server" of the *Systemwalker Desktop Keeper Release Information*.

    - When upgrading from V12

    - When executing the backup command by using schedule function

· ·

When upgrading from V12

The procedures for upgrading from V12.0L10 and V12.0L20 are as follows:

Management Server
Master Management Server

Version upgrade of the Management Server/Master Management Server

Stop the Level Control Service and server service

Back up management information and log information (other than the command log)

Delete the Operation Database

Install and set IIS

Overwrite-install the Management Server/Master Management Server
Overwrite-install the Management Server/Master Management Server that distributes policies for monitoring the client (CT) under the Management Server/Master Management Server
Restart OS

Construct the database
Install the database management system for recording the client (CT) information, various logs, etc.

Restore management information and log information (other than the command log)

Set IIS
Execute as needed

Register the license key

Set the server environment
Create an operating environment for the Management Server/Master Management Server

Management Console

Upgrade the Management Console version
Overwrite-install the Management Console that can configure the policy settings or control operation for the client (CT) under the Management Server/Master Management Server
Restart OS

Log Viewer

Uninstall the Log Viewer
Uninstall the older version of the Log Viewer

Management Server
Master Management Server

Start the Level Control Service

Management Console

Perform terminal initial settings and terminal operation settings

Management Server
Master Management Server

Start the server service

Client (CT)

Upgrade the CT version
Use one of the following methods:
- Wizard
- Silent version upgrade
- Self version management function
Restart OS

When upgrading from V13

The procedures for upgrading from V13.0.0, V13.2.0, V13.2.1 and V13.3.0 are as follows:
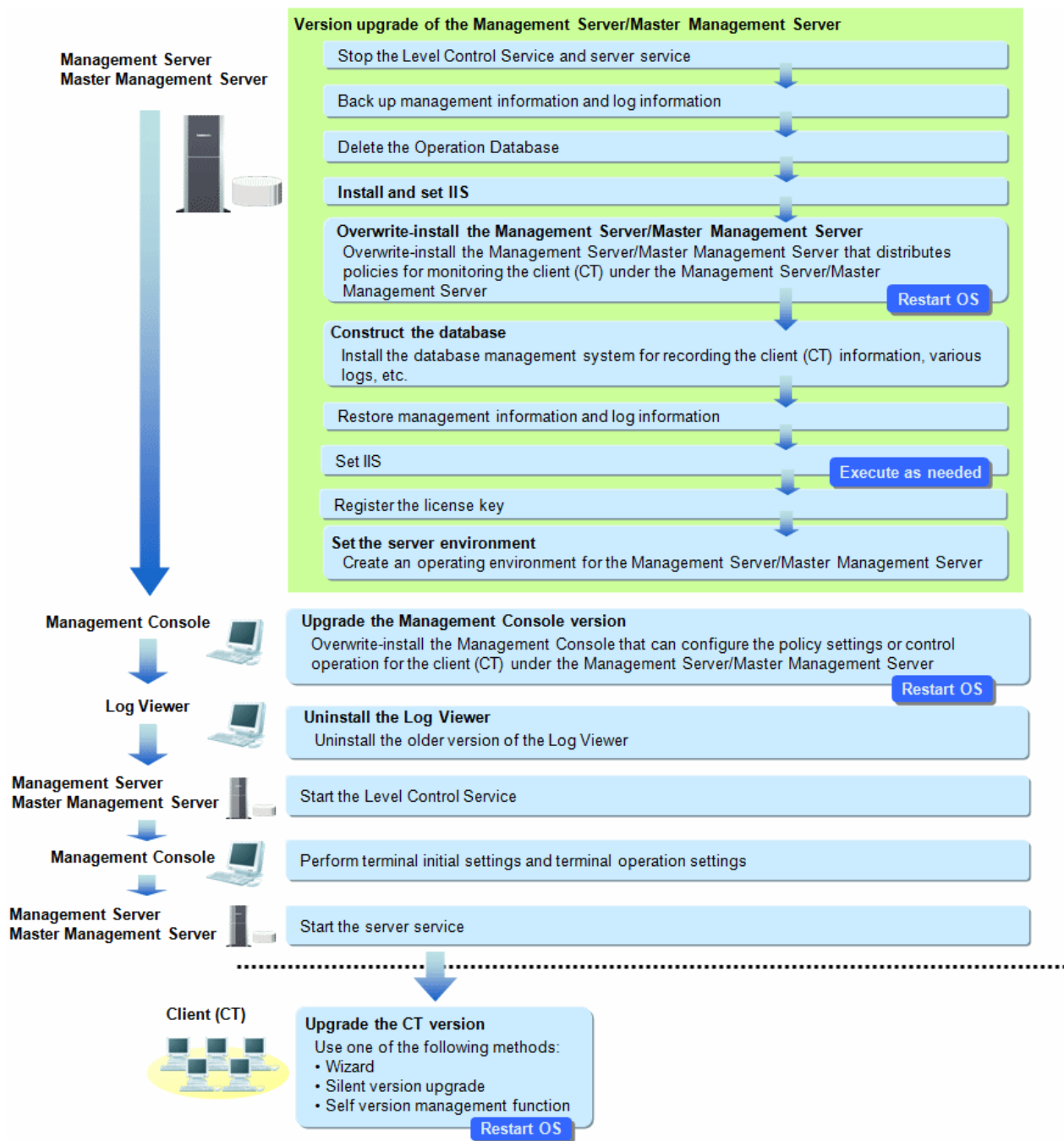
When upgrading from V14/V15

If the URL of the V14/V15 Web Console was bookmarked in a browser, access the V15.1.0 Web Console again and register the bookmark again. Refer to "Start Log Viewer" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on how to access the V15.1.0 Web Console.

The sections below describe the procedures for upgrading from V14/V15.

![Note]

Errors that may occur after upgrade of the Management Server or Master Management Server

After upgrading the Management Server or Master Management Server in an environment that uses the Log Analyzer, the following error event log may be generated on the Management Server or Master Management Server.

```
Event ID: 3421
Type: Error
```

```
Source: SWDTK_PB
Message: "In the batch processing of all-in-one machine linkage, failed to access to database of Log
Analyzer Server. (Server IP address=%1 Result code=%2 Result message=%3 Result details=%4)"
```

Note: The information in %1 - %4 will depend on the environment.

Upgrading the Log Analyzer Server solves this problem.

Management Server
Master Management Server

Version upgrade of the Management Server/Master Management Server

Stop the Level Control Service and server service

Back up management information and log information

Delete the Operation Database and Log Viewing Database

Install and set IIS

Overwrite-install the Management Server/Master Management Server
Overwrite-install the Management Server/Master Management Server that distributes policies for monitoring the client (CT) under the Management Server/Master Management Server
`Restart OS`

Construct the database
Install the database management system for recording the client (CT) information, various logs, etc.

Restore management information and log information

Set IIS
`Execute as needed`

Register the license key

Set the server environment
Create an operating environment for the Management Server/Master Management Server

Management Console

Upgrade the Management Console version
Overwrite-install the Management Console that can configure the policy settings or control operation for the client (CT) under the Management Server/Master Management Server
`Restart OS`

Management Server
Master Management Server

Start the Level Control Service

Management Console

Perform terminal initial settings and terminal operation settings

Management Server
Master Management Server

Start the server service

Client (CT)

Upgrade the CT version
Use one of the following methods:
• Wizard
• Silent version upgrade
• Self version management function
`Restart OS`

Log Analyzer Server

Upgrading the Log Analyzer Server

Uninstall the older version of the Log Analyzer Server
`Restart OS`

Install the Log Analyzer Server
`Restart OS`

Construct the database
Construct the database environment for recording the log analysis result, etc.

Prepare the operating environment for the Log Analyzer Server
Configure the log save schedule and conditions for aggregation or report output according to the operation on the Management Server/Master Management Server

Management Server
Master Management Server

Prepare the operating environment for the Log Analyzer Server
Configure the log transfer schedule according to the operation on the Log Analyzer Server

Report Output Tool

Upgrading the Report Output Tool

Overwrite-install the Report Output Tool
Overwrite-install the Report Output Tool for outputting reports about information disclosure prevention diagnosis, printing amount, etc.
`Restart OS`

Configure the environment for report output
Configure the operating environment required for report output

Refer to "4.8.1 Upgrading the Log Analyzer Server" for details on how to upgrade the Log Analyzer Server.

If using the status window without the Log Analyzer, there is no need to upgrade the Log Analyzer Server and upgrade the Report Output Tool.

Upgrading the Log Analyzer Server

The current environment must be deleted before upgrade, and the new one must then be built from scratch afterwards.
The workflow of the upgrade procedure is shown below.
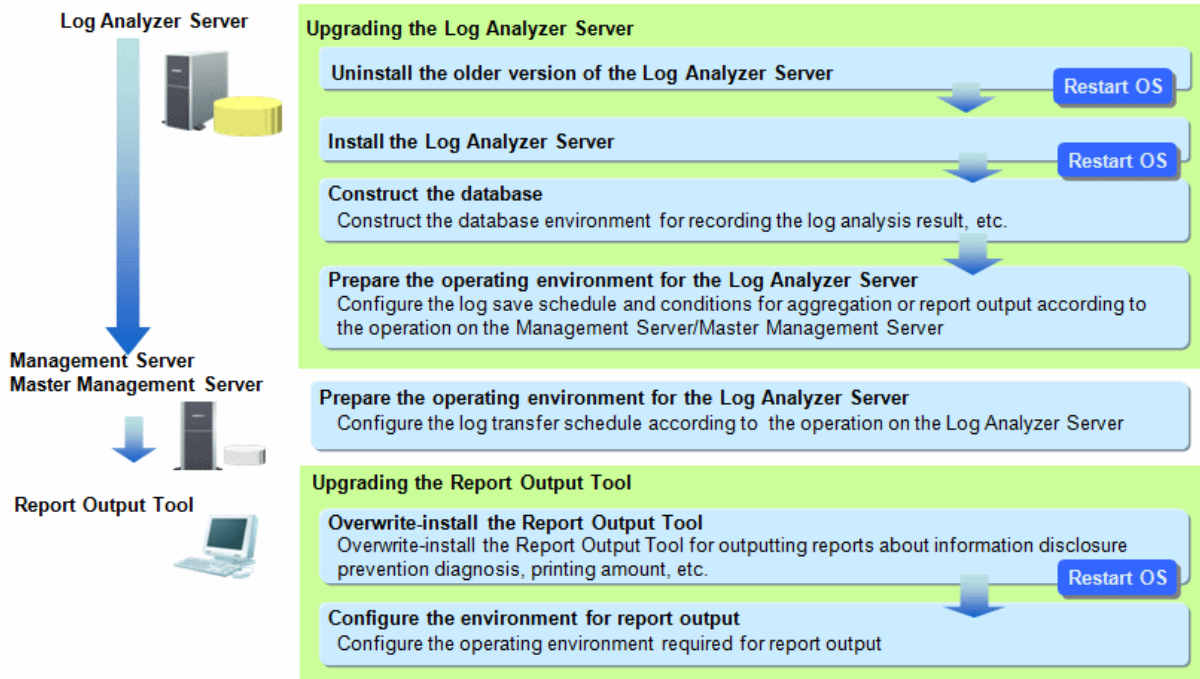
4.2.2 Upgrade of Management Server/Master Management Server on Different Servers

This describes the procedures for upgrading a Management Server/Master Management Server from the old Systemwalker Desktop Keeper to V15.1.0 on different servers.

The procedures for version upgrade are as follows:

Old Management Server
Old Master Management Server

Old Backup through Management Server/Master Management Server
- Stop Level Control Service and Server Service
- Backup Management Information and Log Information
- Copy the management information and log information backed up to new server.

New Management Server
New Master Management Server

Newly Construct Management Server/Master Management Server
- Perform installation and setting of IIS
- Newly install Management Server/Master Management Server
  Newly install Management Server/Master Management Server that distributes policies for monitoring the client (CT) under Management Server/Master Management Server.
  Restart OS
- Construct Database
  Install database management system for recording client (CT) information and various logs.
- Restore management information and log information
- Set IIS
  Execute as needed
- Register the license key
- Set Server Environment
  Create the operation environment of Management Server/Master Management Server.

Management Console

Version Upgrade of Management Console
Overwrite-install Management Console that can configure the policy settings or control operation for the client (CT) under the Management Server/Master Management Server
Restart OS

Management Console

Perform Terminal Initial Settings and Terminal Operation Settings

Client (CT)

CT Version Update
Perform version upgrade through any of the following method.
- Version update of wizard style
- Silent version update
- Version update through automatic version management function
Restart OS

4.3 Upgrading the Management Server/Master Management Server

This describes the procedures for version upgrade of a Management Server/Master Management Server.

4.3.1 Upgrading on the Same Server

This describes how to upgrade the versions of a Management Server/Master Management Server on the same server.

Issues to consider before version upgrade

About version upgrade on Windows Server(R) 2003

Version upgrade on Windows Server(R) 2003 is not supported. Construct the server on the supported operating system and perform version upgrade. For supported operating systems, refer to "OS" of *Systemwalker Desktop Keeper User's Guide*. For version upgrade on different servers, refer to "4.3.2 Upgrading on Different Servers".

Need to Stop Management Server/Master Management Server

When performing version upgrade, usage of the Management Server/Master Management Server should be stopped. Thus, execute in the time frame when there are less users so as to not affect business.

Need to Add firewall Exceptional Port

When modifying the communication port of the Management Server, add the port number after modification to the list of allowed ports in the firewall.

Consider the Time for Data Transfer

Data should be transferred when version upgrade. It takes some time to operate according to the database capacity. The time for backing up user assets from the current database, the time for defining a new database, and the time for restoring the user assets to the database must be taken into account. In addition, if using the Log Viewing Database, the time for defining the new Log Viewing Database and the time for restoring the data to be referenced must also be taken into account.

Overwriting Installation Will Take Some Time

In the environment where a large amount of attached data and command logs exist, when executing the overwriting installation of a Management Server/Master Management Server, access authority confirmation/modification of the attached data and command log will take longer time. (Time standard for overwriting installation: it takes about 30 minutes for the attached data and command log of 100,000 files.)

Definition of Primary Administrator

The available functions are different for the primary administrator created by Systemwalker Desktop Keeper V12 and the primary administrator created by Systemwalker Desktop Keeper V13 or later.

The primary administrator of V13 or later can use the server settings tool, backup tool, restore tool, and restore command.

When upgrading from V12.0.0L20 or earlier to V15.1.0, the primary administrator of V12.0.0L20 or earlier will be transferred as the administrator and can therefore continue using the Management Console and Log Viewer. However, the administrator will not become the primary administrator of V15.1.0. To use the same primary administrator (secureadmin) from V12.0.0L20 or earlier in V15.1.0, specify the password of the primary administrator in the following login windows as explained below:

- Server settings tool, backup tool, restore tool, and restore command

  When starting as the primary administrator user, specify the password for the primary administrator indicated in "Overwriting Install Management Server/Master Management Server".

- Management Console and Log Viewer
  When starting as the primary administrator (secureadmin) user from V12.0.0L20 or earlier, specify the password set in V12.0.0L20 or earlier.

IIS setting

When upgrading from V14.0.0 or later with **Allow** specified in **All Unknown ISAPI Extensions** for IIS, you will not need to configure the IIS setting again when installing the Management Server or Master Management Server. The web console will run with **Allow** specified in **All Unknown ISAPI Extensions** as is.

State window aggregation schedule

When upgrading from V14.0.1 or earlier, status window aggregation runs using the initial value of 1:00. The Level Control Service must be running during status window aggregation, so ensure that the processes for stopping status window aggregation and the Level Control Service (such as backup and restore, and data transfer) are not duplicated. If these processes are duplicated, change the status window aggregation schedule after upgrading. Refer to "Prepare for Using Status Window" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details on how to change the schedule.

Log Viewing Database

If you are using the Log Viewing Database at the time of upgrade from V14.2.0 or V14.3.0, delete it before upgrading and re-create it afterwards.

Disk space required for upgrade

In the **Confirm Number of Tables** window of the Backup Tool, check the number of records in each table.

Calculate the required disk space based on the displayed number. The size depends on the contents of the table logs, but calculate the size assuming the average of 1 KB/record.

Note that it may not be possible to back up a large volume of records at one time. In this case, split the backup period using a maximum of 20 million per table as a guide when calculating the required disk space.

In Windows Server 2012, due to enhancements to UAC security, the network drive cannot be specified if the backup tool is not started by the built-in Administrator.

Before performing backup as any user other than the built-in Administrator, assign the network drive from the elevated command prompt.

Time required for upgrade

Systemwalker Desktop Keeper V15.1.0 does not allow migration of a database of an older version, so backing up and restoring the necessary data requires additional time.

The standard time for backup and restore is as shown below.

Measurement result

1. Data backup
   Calculate using the number of logs to be backed up - the standard is as follows:

   7,000 logs/second (Xeon, 2.0 GHz, 2 GB memory, RAID 1 configuration)
   Note: More time may be required depending on server performance and the RAID configuration.

2. Deletion of databases handled by an older version of Systemwalker Desktop Keeper
   Takes just minutes, even with very large databases.

3. Database construction with Systemwalker Desktop Keeper V15.1.0
   Takes approximately 1 minute (Xeon, 2.0 GHz, 2 GB memory, RAID 1 configuration)
   Note: More time may be required depending on server performance and the RAID configuration.

4. Data restore
   Calculate using the number of logs to be restored - the standard is as follows:

   5,000 logs/second (Xeon, 2.0 GHz, 2 GB memory, RAID 1 configuration)
   Note: More time may be required depending on server performance and the RAID configuration.

Notes on coexistence with Systemwalker Desktop Patrol

If upgrading Systemwalker Desktop Keeper in an environment where Systemwalker Desktop Patrol is already installed, services that manage iOS devices will automatically stop.

In this case, the services that manage iOS devices cannot be used until the operating system is restarted.

Verification when registering client (CT) devices

When performing verification during client (CT) device registration, set a client management password in the **Terminal Operation Settings** window of Management Console. Refer to "Perform Terminal Operation Settings" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

The procedures for version upgrade of a Management Server/Master Management Server are as follows: execute the following procedure according to "4.2 Upgrade Procedures".

When IIS has not been installed here, it should be installed before version upgrade of a Management Server/Master Management Server. For IIS installation, refer to "2.3.1 Installation and Settings of IIS

Logon to Management Server/Master Management Server

1. Log on to Windows with an Administrators group affiliated user or Domain Admins group affiliated user. When other applications are in use, end these applications.

Stop Level Control Service and Server Service

1. Select **Control Panel** > **Network Connection**.

2. Select "Local Area Connection" and disable local connection. Wait for 1 minute after disabling before continuing to the following procedures.

3. When the Windows service window is displayed, select each of the following services and select **Stop** from the **Operation** menu. It will take 30 seconds to 1 minute to stop. In addition, immediately after restarting SWServerService or after the date has changed (00:00), available space in the database will be checked. This check takes approximately 15 minutes, and services may not stop during this time. Wait for a few moments and then check if the services have stopped.

   - SWLevelControlService

   - SWServerService

4. After the services above have been stopped, enable "Local Service".

Install and set IIS (when upgrading from V12 or V13)

The procedures for installing and setting IIS are the same as 2.3.1 Installation and Settings of IIS" during the new installation. Refer to these procedures.

Back up Management Information and Log Information

In the environment before version upgrade, back up the management information, log information and command log by using the backup command or backup tool of Systemwalker Desktop Keeper. Back up (by copying the file) the V12 command logs to a log file.
When backing up by directly using the batch file in the backup command installation folder, the batch file itself should be backed up because it will be overwritten during version upgrade.
Back up the batch file before version upgrade, and reflect the settings to the new batch file after version upgrade. However, because of the format change, do not restore through direct replacement.

📝 Note

Notes on backup

Must Back up Management Information

  Make sure to back up management information. If not, the system cannot be restored. When not transferring log information, there is no need to back it up.

Back up Management Information and Log Information Simultaneously

  Back up management information and log information at the same time. Data backed up not at the same time cannot be transferred normally.

All Log Information to Be Transferred Is the Database Backup Target

  See that take the data in all periods as the backup target of log information.

Log Viewing Database

  V14.2.0 and V14.3.0 do not provide any function that enables the Log Viewing Database to back up management information or log information. Therefore, if you are using the Log Viewing Database, check the scope of stored data before migrating to these versions, and prepare in advance the data to be stored in the Log Viewing Database after the upgrade.

V12 Backup Command Is Restricted

  Command log cannot be backed up through V12 backup command.

1. In V12, back up the command log.

   Back up all files in Prompt Log folder of V12 to arbitrary backup folder. Files to be backed up need not to be restored in the operation of self-version upgrade, but should be restored when restoring log information.
   PromptLog folder of V12 is the folder specified as the log file saving target when executing "Installation of Management Server/ Master Management Server". (Example: C:\DTK\PromptLog)

2. Back up all management information and log information.
   Use the backup tool (V13.0 or later) or the backup command to back up all periods of management information and log information for the Management Server and Master Management Server.
   If it is not necessary to restore the logs for all periods to the Operation Database, or if storing them in the Log Viewing Database, it is recommended that you back up the log information for each period to be referenced. In this case, preparing a batch process is useful for performing backup while splitting the periods by using the backup command.

Use the backup command provided in each version or the backup tool to perform backup. Refer to the manual for the applicable version for details on how to perform backup using the backup command or backup tool.

3. Check the backup execution result.

   It checks the backup execution result for management information and log information, and confirms that backup has been completed normally.

4. Back up the batch file for backup. However, when the batch file is not in use, or it is moved to the user's arbitrary folder that is not the installation target of Systemwalker Desktop Keeper for use, there is no need to back it up.

   For the installation target of the batch file for backup, refer to the manual of each version.

Note

. . . .

When upgrading from V13 or V14, the batch file for backup should also be backed up

When upgrading from V13 or V14, the backup procedures of the batch file for backup above will also be required. Confirm the conditions required for the backup above and Procedure 4.

. . . .

Deleting the Log Viewing Database (when upgrading from V14.2.0)

If using the Log Viewing Database, use the Operating Environment Maintenance Wizard (Construct/Delete Environment) feature to delete the Log Viewing Database.

Deleting the Operation Database (when upgrading from V13.0 to V15.0)

The older version database must be deleted.

Use the Operating Environment Maintenance Wizard (Construct/Delete Environment) tool to delete it.

If the Management Server installer is run in an environment where there is an older version database (Symfoware RDB SWDTK, Symfoware RDB SWDTK2), the following message will be displayed and upgrade will fail.

```
Systemwalker Desktop Keeper Management Server cannot be upgraded.
The following database system was not deleted.
%1
%2
```

Note: Variable information will show Symfoware RDB SWDTK, Symfoware RDB SWDTK2, or both.

After deleting the older version database, run the Management Server installer.

Deleting the Operation Database (when upgrading from V12)

The older version database must be deleted.

Follow the procedure below to delete the data area from the database:

1. Click **Start** > **All Programs** > **Microsoft SQL Server** > **Enterprise Manager**.
   The **SQL Server Enterprise Manager** window will be displayed.

2. In the tree view on the left side of the window, click **Console root** > **Microsoft SQL Servers** > **SQL Server group** > **(LOCAL) (Windows NT)** > **Database**.

3. Right-click **DTKDB** on the right side of the window and click **Remove**.

4. A message prompting you to confirm deletion of the database will be displayed. Click **Yes**.

Uninstalling the database when upgrading from V13 or V14)

Note

. . . .

If the database remains in the installation folder of database-related files in the Management Server or Master Management Server (because another application is using it, for example), do not delete the folder. Otherwise, the database management system can no longer run.

Installation folder of database-related file: C:\DTK (default path)

. . . .

Uninstall the database (in this example we use Symfoware Server).

Check if any other application is using the database (do not uninstall the database if an application is using it).

Follow the procedure below to uninstall the database:

1. Log on using the Windows account (administrator authority) used when installing the Management Server.

2. Click **Control Panel** > **Add or Remove Programs** or **Add/Remove Programs**.

3. Select "Symfoware Client" and click **Remove**.

🛈 Note

. . . .

Message when Symfoware Client is uninstalled

When uninstalling Symfoware Client, the message of "Symfoware .NET Data Provider Installer" may be displayed. Click **OK** to proceed.

. . . .

4. Select "Symfoware Server Enterprise Edition" and click **Remove**.

Overwriting Install Management Server/Master Management Server

🛈 Note

. . . .

For version upgrade order for Management Server/Master Management Server

In a 3-level structure, perform version upgrade on the Master Management Server first. After that, perform version upgrade on the Management Server.
Besides, to avoid accidents in the process of version upgrade, before completing version upgrade on all Management Serves and the Master Management Server, do not view the subordinate Management Server information through the Master Management Server.

Coexistence of the Management Server or Master Management Server and the Management Console

If the Management Console coexists with the Management Server or Master Management Server, it will be upgraded at the same time.

About upgrading steps when coexisting with Log Analyzer Server

When coexisting with the Log Analyzer Server, perform version upgrade as follows:

1. Delete database of older version Log Analyzer Server and Uninstall Log Analyzer Server
Refer to "5.6 Uninstall Log Analyzer Server" for details.

2. Upgrade Management Server

3. Install this version Log Analyzer Server and construct database
Refer to "2.7 Construct Log Analyzer Server" for details.

About setting Log Analyzer

When using the Log Analyzer regardless of coexisting with the Log Analyzer Server, set the Log Analyzer after upgrading the Management Server.
Refer to "2.7.3.1 Set Log Analyzer Environment on Management Server/Master Management Server" for details.

. . . .

The procedures for overwriting installation Management Server/Master Management Server are as follows:

1. After inserting DVD-ROM of Systemwalker Desktop Keeper into PC, the installer window is displayed.

Select **Management Server/Management Console Installation**.

When the Setup has not been started, start "swsetup.exe" of DVD-ROM drive.

2. After the "Welcome to Systemwalker Desktop Keeper Server Setup" window is displayed, click the **Next** button.

3. When upgrading from V12.0.0L20 or earlier, the "Select the installation target" window of the server function will be displayed. (Not displayed when upgrading from V13.0.0 or later to V14.3.0. Access the next procedure.)

4. When not to modify the displayed installation target, click the **Next** button.
To modify the displayed installation target, click the [View] button of the folder to be modified, and click the **Next** button after the folder is modified.

5. When upgrading from V12.0.0L20 or earlier, the installation destination of the database-related files will be the folder containing the database at the same level as the installation destination of the Management Server.
Example: Setting the following folder as the installation destination of the Management Server
C:\Program Files\Fujitsu\Systemwalker Desktop Keeper\Server
The database-related files will be installed in the following folder:
C:\Program Files\Fujitsu\Systemwalker Desktop Keeper\DB

🕝 Note

The maximum length of the path to be specified for destination folder is 96 bytes.

6. When the old Log Viewer has been installed on the Management Server/Master Management Server, the following message will appear. After click the **OK** button in the message window, the old Log Viewer will be uninstalled before installation.

When the old Log Viewer has not been installed, continue to install.

```
Log Viewer V13.2.0 or earlier has been installed.
Functions of Log Viewer V14.2.0 or later are contained in Management Server already, Log Viewer
will be uninstalled.
```

🕝 Note

Do not delete the folder, or the database cannot be transferred

When uninstalling the Log Viewer, the following message for deleting the folder will appear, but do not delete the folder. Continue installing the Management Server directly.

```
The following folder might be reserved after uninstallation, please delete it manually.
-Trace Log Saving Folder:
[%1]
%1 : Folder path of trace log saving folder
```

Do not restart here

A message prompting you to restart the operating system will appear after the Log Viewer uninstallation is completed, but do not restart and continue installing the Management Server.

If you restart the operating system by mistake, the overwriting installation of the Management Server will be interrupted, so reinstall it again. In this case, because the uninstallation of Log Viewer has been completed, the message above will not appear.

7. When the log linkage adapter of the Systemwalker Desktop Log Analyzer has been installed on the Management Server/Master Management Server, the following message will appear and the Log Viewer will be uninstalled. After clicking the [OK] button in the message window, linkage adapter will be uninstalled before installation. Also, the configuration value of the log linkage adapter in Systemwalker Desktop Log Analyzer will be adopted.

When the log linkage adapter has not been installed, continue to install.

```
Systemwalker Desktop Log Analyzer log linkage adapter V13.2.0 or earlier has been installed.
Functions of log linkage adapter V14.2.0 or later are contained in Systemwalker Desktop Keeper
Management Server already, the log linkage adapter will be uninstalled.
```

🕝 Note

Do not restart here

A message prompting you to restart the operating system will be displayed after you complete the uninstallation of the log linkage adapter; however, do not restart and continue installing the Management Server.

If you restart the operating system by mistake, the overwriting installation of the Management Server will be interrupted. If this happens, reinstall again. In this case, the message above will not appear because the uninstallation of the log linkage adapter has been completed.

⋯⋯

8. The message below will be displayed. Click **OK** and continue with the installation process.

```
Upon completion, a  window informing that the installation completed successfully will be
displayed.
Installation will continue until the window is displayed, so wait until completion.
```

9. The "I121-WRN001" message will be displayed.

10. The message below will be displayed. Click **Finish**.

```
The installation of Systemwalker Desktop Keeper management server was completed.
```

11. Upon successful completion, the confirmation window will be displayed.
To use the program, click **Yes**. The operating system will restart.

During version upgrade, the following error will be displayed in the event log, but there will be no problem:
[Type] Error
[Source] SWDTK
[Event ID] 3014
[Descriptions] Database structure of non current version. Confirm the database environment.

Construct the Operation Database

The procedures for constructing the Operation Database are the same as "2.3.3 Construct Database". Refer to that for details.

Restore management information and log information

When overwriting the installation of the management information and log information of the old version backed up by Management Server/ Master Management Server previously, restore them by using the restoration tool of Systemwalker Desktop Keeper.

1. In the **Administrator Information Settings** window of the Server Settings Tool, add a user ID that has access privileges for backup and restore.

2. Restore management information and log information by using the restoration tool V15.1.0.

After the restoration, data will be transferred and the newly created information in V15.1.0 will be added automatically. For details on how to use the restoration tool, refer to "3.1.3 Restoring User Assets".

3. If upgrading from V12, copy the log file where the command logs are saved.

Set IIS

IIS settings will be performed automatically. However, when upgrading from V12 or V13, refer to "2.3.4 IIS Settings", and create the Systemwalker Desktop Keeper specified application pool as required.

Register the license key

About the registration of the license key, refer to "2.3.5 Register the license key"

Set Environment of Server

When the version is upgraded to V15.1.0, the configuration value in the previous version is still valid.

However, when upgrading from V13.0.0 or earlier, the detailed authority of user information set in the **Administrator Information Settings** of server settings tool will be transferred under the status of possessing all authorities. To modify, perform after completing transfer.

Also, for **USB Device Registration/Update/Delete** and **E-mail Content Viewing** in the **Administrator Information Settings** window, because not all administrators are authorized, authorize them after transfer if necessarily.

When upgrading from V13.2.0 or earlier, because the status window settings are not performed, set the conditions for aggregation in the environment setup. For how to set, refer to "Prepare for Using Status Window" of *Systemwalker Desktop Keeper User's Guide for Administrator*.

Also, perform server settings if the server environment is modified. The procedures for server settings are the same as "2.3.6 Set Environment of Management Server/Master Management Server" during the initial installation. Refer to that guide for details.
If upgrading from V15.0.1 or earlier, the range for the threshold value for database depletion monitoring is "5 to 20".
If the specified value is lower than 5% when upgrading, it will be overwritten to "5%".

Construct the Log Viewing Database (when upgrading from V14.2.0)

If you were using the Log Viewing Database, click **Server settings tool** > **Build, delete, or show information of database** in V15.1.0, and define the new Log Viewing Database.
The procedure for constructing the Log Viewing Database is the same as that in "2.3.3 Construct Database", so refer to that section.
In the Log Viewing Database, store the management information and log information you want to view. Use the Systemwalker Desktop Keeper Restoration Tool or restore command to perform restore. Refer to "3.1.3.1 Using the Restoration Tool" or "DTKTBLRESTOR.EXE (Restore Database)" in the *Systemwalker Desktop Keeper Reference Manual*.

4.3.2 Upgrading on Different Servers

📙 Note

· ·

Contents to be considered before version upgrade

Aggregation Schedule of Status Window

When performing version upgrade from version prior to 14.2.0, the aggregation of status window will run according to the initial value 1:00. Level control service needs to be started during aggregation of status window. Therefore, confirm whether the aggregation of status window and stopping of level control service has been performed at the same time (backup and restoration, data transfer, etc). If processing at the same time, modify the aggregation schedule of status window after version upgrade. For how to modify, refer to "Prepare for Using Status Window" of *Systemwalker Desktop Keeper User's Guide for Administrator*.

· ·

Logon to old Management Server/Master Management Server

1. Log on to Windows with an Administrators group affiliated user or Domain Admins group affiliated user. When other applications are in use, end these applications.

Stop Level Control Service and Server Service of the old Management Server/Master Management Server.

The Windows service window is displayed, select each of the following services and select **Stop** from the **Operation** menu. It will take 30 seconds to 1 minute to stop. 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, confirm later.

- SWLevelControlService

- SWServerService

Back up the management information and log information on the old Management Server/Master Management Server

Back up the management information and log information by using the backup command or backup tool of Systemwalker Desktop Keeper. In the case of V12, back up the log file (by copying it).

Copy the management information and log information backed up on the old Management Server/Master Management Server to the new server.

Copy the management information and log information backed up on the old Management Server/Master Management Server to the new server.

Install and set IIS on new Management Server/Master Management Server.

For details on how to install and set IIS, refer to "2.3.1 Installation and Settings of IIS" during the new installation.

Newly install the new Management Server/Master Management Server

For details on how to install a Management Server/Master Management Server, refer to "2.3.2 Install Management Server/Master Management Server" during the new installation.

Construct the database in new Management Server/Master Management Server

For details on how to construct the database, refer to "2.3.3 Construct Database" during the new installation.

Restore the management information and log information on new Management Server/Master Management Server

For details on how to restore the management information and log information, refer to "3.1.3 Restoring User Assets".

When upgrading from V12, copy the log file you backed up.

Set IIS on new Management Server/Master Management Server.

IIS settings will be performed automatically. Refer to "2.3.4 IIS Settings", and create Systemwalker Desktop Keeper specified application pool as required.

Register the license key on new Management Server/Master Management Server.

About the registration of the license key, refer to "2.3.5 Register the license key"

Set the server environment on new Management Server/Master Management Server

When the version is upgraded to V15.1.0, the configuration value in the old version is still valid.

However, when upgrading from V13.0.0 or earlier, the detailed authority of user information set in the **Administrator Information Settings** of server settings tool will be transferred under the status of possessing all authorities. To modify, perform after completing transfer.

Also, for **USB Device Registration/Update/Delete** and **E-mail Content Viewing** in the **Administrator Information Settings** window, because not all administrators are authorized, authorize them after transfer if necessary.

When upgrading from V13.2.0 or earlier, because the status window settings are not performed, set the conditions for aggregation in the environment setup. For how to set, refer to "Prepare for Using Status Window" of *Systemwalker Desktop Keeper User's Guide for Administrator*.

Also, if the server environment is modified, set the server. The procedures for setting the server are the same as "2.3.6 Set Environment of Management Server/Master Management Server" during the initial installation. Refer to this guide for details.

Also, when modifying the computer names of the old server and the new server, refer to "Change System Environment with the Change of IP Address/Computer Name of Management Server/Master Management Server" of *Systemwalker Desktop Keeper User's Guide for Administrator*.
If upgrading from V15.0.1 or earlier, the range for the threshold value for database depletion monitoring is "5 to 20".
If the specified value is lower than 5% when upgrading, it will be overwritten to "5%".

4.4 Upgrading the Management Console

This describes how to upgrade the version of the Management Console.

📑 Note

. . . .

Coexistence of the Management Server or Master Management Server and the Management Console
If the Management Console exists with the Management Server or Master Management Server, it will be upgraded at the same time.
In this case, this procedure is not required.

. . . .

Overwrite the install of the Management Console. The procedures are as follows: execute the following procedures according to "4.2 Upgrade Procedures".

1. Log on to a Windows with an Administrators group affiliated user or Domain Admins group affiliated user.

2. After inserting DVD-ROM of Systemwalker Desktop Keeper into PC, the installer window is displayed.
   Select **Management Console Installation**.

   If the Setup has been not been started, start "swsetup.exe" of DVD-ROM drive.

3. After the "Welcome to Systemwalker Desktop Keeper Management Console Setup" window is displayed, click the **Next** button.

4. The "Enter server information" window is displayed. Set the target server information, and click the **Next** button.

   The procedures for setting the target server are as follows:

   a. For the target server information, click the **Add** button after setting the following information.

   ### 📒 Note

   Confirm the settings of the connected Management Server/Master Management Server

   Set the connected Management Server/Master Management Server information as the same as the settings in the Management Console. The following explains how to confirm:

   1. Start **Systemwalker Desktop Keeper** > **Server** > **Server Settings Tool** from the **Start**/**Apps** menu on the connected (Master) Management Server.

   2. Click the **Management Server settings** button.

   3. Confirm the following items.

      - Configuration value of **IP address of server** of **Server settings**

      - Configuration value of **Management Console** <----> **Level Control Service** of **Port number settings**

   ....

   - **Computer name or IP address of connected (Master) Management Server:** Input the computer name or IP address of the connected Management Server/Master Management Server.

     When inputting the computer name, input the content with name analyzed. If the name is not analyzed, Management Server/Master Management Server cannot be connected to Management Console.
     The value set here will be displayed as an option of **Connected Target Server Name** in the logon window of Management Console. You can enter both IPv4 and IPv6 IP addresses.
     Do not use link local addresses. Behavior is not guaranteed in this case.

   - **Port number being used:** Enter the port number for communication between Management Console and Level Control Service. The number must be the same as the setting for **Management Console** <----> **Level Control Service** in **Port number settings**.

   After it is added, the set information will be displayed under the **Add** button.

   b. When there are multiple target servers, operate as Procedure a. according to the number of servers.
      Servers that are connected frequently can be moved up and down through the up arrow button and the down arrow button.

5. The "Complete installation preparation" window is displayed.

   To start installation, click the **Install** button to start installation.

   To confirm or modify the settings, click the **Back** button to reset.

6. The message below will be displayed. Click **OK** and continue with the installation process.

```
Upon completion, a  window informing that the installation completed successfully will be
displayed.
Installation will continue until the window is displayed, so wait until completion.
```

7. The message below will be displayed. Click **Finish**.

```
The installation of Systemwalker Desktop Keeper management server was completed.
```

8. Upon successful completion, the confirmation window will be displayed.
   To use the program, click **Yes**. The operating system will restart.

4.5 Uninstalling the Log Viewer

This describes how to uninstall the Log Viewer V13.2.0 or earlier.

1. Log on to Windows with an Administrators group affiliated user or Domain Admins group affiliated user. When other applications are in use, end these applications.

2. Start **Add or Remove Programs** or **Add or Remove Applications** of **Control Panel**.

3. Select "Systemwalker Desktop Keeper Log Viewer" and click the **Delete** button.

4. Execute uninstallation.

4.6 Performing Terminal Initial Settings and Terminal Operation Settings

This describes how to perform terminal initial settings and terminal operation settings after the version in each environment is upgraded.

The procedures are as follows: execute the following procedures according to "4.2 Upgrade Procedures".

Start Level Control Server

Start the stopped Level Control Service.

![Note icon] Note
. . . .

Notes on starting Level Control Service

- In case of a 3-level structure, to avoid accidents, before completing the terminal initial settings and terminal operation settings on the Master Management Server, do not start the Level Control Service of a Lower-level Management Server.

- When starting the Level Control Service of a Lower-level Management Server, after performing collective management and settings of data, data synchronization will be started between Management Servers. Thus, when starting multiple Management Servers, start another after a while. Also, the Management Console and the Log Viewer cannot be used during data synchronization.

. . . .

1. When Windows service window is displayed, select Level Control Service (SWLevelControlService) and select **Start** from the **Operation** menu.

Set terminal initial settings

Open the **Terminal Initial Settings** window from the Management Console window.

1. Start the "Management Console" window.

2. Select **Terminal Initial Settings** from the **Operation Settings** menu.

   The **Terminal Initial Settings** window is displayed.

Functions that do not exist before version upgrade will be set as the initial value. Set as required. For details of settings, refer to "Perform Terminal Initial Settings" in *Systemwalker Desktop Keeper User's Guide for Administrator*.

Also, through the procedures above, though the terminal initial settings of adding policy can be set, they are not reflected to the original CT policy and user policy. Reflect to CT policy and user policy of adding policy by other means. For details on how to reflect CT policy and user policy, refer to "Modify CT Policy/User Policy" in *Systemwalker Desktop Keeper User's Guide for Administrator*.

Set terminal operation settings

When modifying the initial value of the Terminal Operation Settings window of Management Console

When modifying the initial value of the **Terminal Operation Settings** window of Management Console, execute the following procedures:

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

2. Select **Terminal Operation Settings** from the **Operation Settings** menu.

   The **Terminal Operation Settings** window is displayed.

3. Change the value of **Terminal Operation Settings**.

When not modifying the initial value of the **Terminal Operation Settings** window of Management Console, go to the next procedure.

Start server service

Start the stopped server service.

📄 Note

....

Start the service after Master Management Server settings is completed

In case of a 3-level structure, to avoid accidents, before completing "2.3.6 Set Environment of Management Server/Master Management Server", terminal initial settings and terminal operation settings, and do not start server service.

....

1. When the Windows service window is displayed, select server service (SWServerService) and select **Start** from the **Operation** menu.

4.7 Upgrading the client (CT)

This describes how to upgrade the version of the Client (CT).

📄 Note

....

Perform version upgrade of Client (CT) finally

Perform version upgrade of the Client (CT) after completing the version upgrade of the other assets according to "4.2 Upgrade Procedures".

....

📄 Note

....

When upgrading from the environment of V13.0 or earlier, the network should be disconnected.

When starting version upgrade of the Client (CT) from the environment of V13.0 or earlier, the network will be disconnected during installation. When opening the network folder through Explorer, install after closing it.

....

Version upgrade of the Client (CT) has the following 3 methods. Conduct the overwriting install Client (CT) according to these methods based on your needs:

- Version Upgrade in Wizard Pattern

- Silent Version Upgrade

- Version Upgrade through Version Auto-upgrade Management Function

📄 Note

....

Notes on installing a client (CT) on Windows(R) 8 or Windows(R) 10

If you have upgraded a client (CT) and clicked **No, restart the computer later** in the **Installation Complete** window, you must restart the operating system.

Even clicking **Shut Down** (operation for shut down and power on a system) to shut down the operating system does not apply the client (CT) feature.

. . . .

4.7.1 Upgrading Using the Wizard

🕝 Note

. . . .

If a user whose user name contains fullwidth characters upgrades a client (CT), an error message may be displayed.
When installing a client (CT), use a user name that contains halfwidth characters only.

. . . .

The procedures for version upgrade of the Client (CT) in the Wizard Pattern are as follows:

1. Log on to Windows with an Administrators group affiliated user or Domain Admins group affiliated user. When other applications are in use, end these applications.

2. After inserting DVD-ROM of Systemwalker Desktop Keeper into PC, the installer window is displayed.

   Select "CT(Client) Installation".

   If the Setup has not been started, start "swsetup.exe" of DVD-ROM drive.

3. The "Welcome to use Systemwalker Desktop Keeper Client installation" window is displayed. Click the **Next** button.

4. The **Set printing monitoring mode** window is displayed. For printing mode, select any of the following options and click the **Next** button.

   - **Monitoring the printing of all printers set in this terminal (Recommended):** This is selected when collecting printing operation logs according to each Client (CT). In this case, printing operation logs will be collected in each Client (CT).

   - **Monitoring the printing of local printer only:**
     This is selected when the printing operation in Client under the same Management Server/Master Management Server with the printing server is performed through the printing server. The Client (CT) is also required to be installed on the printing server. In this case, the printing operation log cannot be collected through a Client that is not a printing server. The printing operation log will be collected by the printing server.

🕝 Note

. . . .

Notes on print monitoring mode

Integrate in Master Management Server and Management Server

   Integrate the options above in the Client (CT) under the Master Management Server or Management Server. If not integrated, the printing operation log cannot be collected.

Settings when installing printer server in non-server OS

   In the case of taking a non-server OS (Windows Server(R) 2003, Windows Server(R) 2008 and Windows Server(R) 2012) as the print server, when set as **Monitoring the printing of all printers set in this terminal (Recommended)**, the print server will not be able to connect over 10 Clients to print. At this time, set as **Monitoring the printing of local printer only**.

. . . .

🅿 Point

. . . .

Register user ID on the print server

When installing the Client (CT) after selecting " Monitoring the printing of local printer only " for the print server, the user ID used in the print client (CT) should also be registered on the print server. If not, the user ID of print log will be output as follows:

   - When user authority is only set to the user ID being used in the print client (CT), **User ID** of the log will be collected as Guest.

- When requesting to log on to the log server as an Administrator during print, **User ID** of the log will be collected as Administrator.

5. When "**Set E-mail Control Mode**" window is displayed, set the mode for E-mail attachment prohibition, and click the **Next** button.

- **Port Number for E-mail Sending and Monitoring:** when selecting port monitoring mode, enter the port number for the communication between the Client (CT) and SMTP server.

- **Port Monitoring Mode (Recommended):** this is selected when using the prohibition function based on the driver for E-mail attachment prohibition. Set this setting as default one.
  When upgrading from V13.0.0 or earlier, select E-mail attachment prohibition under the port monitoring mode in case the prohibition to be the same as that of V13.0.0 or earlier if it has not set.

  - **Port Number for E-mail Attachment Prohibition:** when selecting port monitoring mode, enter the port number for internal use in E-mail attachment prohibition processing. In case of Base Edition, this cannot be specified.

  - **Port Number 2 for E-mail Attachment Prohibition:** when selecting port monitoring mode, enter the port number for internal use in E-mail attachment prohibition processing. In case of Base Edition, this cannot be specified.

- **V12.0L20-V13.0.0 Compatible Mode:** this is selected when using the prohibition function based on the pattern of V13.0.0 or earlier. During the version upgrade from V13.0.0 or earlier, specify only when the same prohibition is required. In case of Base Edition, this cannot be specified.

 Note

Notes when setting E-mail attachment prohibition mode

In the Case of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10 or Windows Server(R) 2012

In the case of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10 or Windows Server(R) 2012, only the port monitoring mode can be selected as the E-mail attachment prohibition mode.

Confirm Whether Port Is Not Used

For the port for E-mail attachment prohibition, make sure to specify a port not used in other processing and communication.

Need to Reboot

When performing version/edition upgrade from the following versions to V15.1.0, after installing "E-mail Sending Log Acquisition Function", the function cannot operate before rebooting:

- BEV12.0L20

- SEV12.0L20

- BEV13.0.0 /SEV13.0.0

When performing version upgrade from the following versions to V15.1.0, before rebooting, the version before version upgrade operates well:

- BEV13.2.0 /SEV13.2.0

- V14.2.0

6. When the "Creation Settings of File Export Utility Icon" window is displayed, set whether to create the icon of File Export Utility and click the **Next** button. Start installation.

   - **Create in Desktop:** This is selected when creating the File Export Utility icon on the desktop.

   - **Create in the Send to Menu:** This is selected when creating the File Export Utility icon in the **Send to** menu.

7. The **Update is completed** window will be displayed after completing normally.

   Restart the operating system when using the program. Select either of the following items and click the **Finish** button:

   - Yes, restart the computer immediately.

   - No, restart the computer later.

4.7.2 Upgrading Using Silent Upgrade

Note

If a user whose user name contains fullwidth characters upgrades a client (CT), an error message may be displayed.
If a user whose user name contains fullwidth characters upgrades a client (CT), an error message may be displayed.

When installing a client (CT), use a user name that contains halfwidth characters only.

This describes how to upgrade the version by using the prepared installation settings file.

The software distribution function of Systemwalker Desktop Patrol can be used to perform version upgrade to the Client (CT) collectively. For details on how to distribute the software of Desktop Patrol, refer to "Install using Software Distribution Function of Systemwalker Desktop Patrol".

The procedures for silent version upgrade are the same as that for "2.6.1.2 Perform Silent Installation". Refer to this Section.

Note

Notes when setting E-mail attachment prohibition mode

In Case of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10 or Windows Server(R) 2012

In case of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10 or Windows Server(R) 2012, only the port monitoring mode can be selected as E-mail attachment prohibition mode.

Confirm Whether Port Is Not Used

When selecting the port for E-mail attachment prohibition, make sure to specify a port not used in other processing and communication.

Need to Reboot

When performing version upgrade from the following versions to V15.1.0, after installing "E-mail Sending Log Acquisition Function", the function cannot operate before rebooting:

- BEV12.0L20

- SEV12.0L20

- BEV13.0.0 /SEV13.0.0

When performing version upgrade from the following versions to V15.1.0, before rebooting, the version before version upgrade can operate well:

- BEV13.2.0 /SEV13.2.0

- V14.2.0

4.7.3 Upgrading Using Self Version Management Function

This describes how to upgrade the version based on the version upgrade by using self version management function as Systemwalker Desktop Keeper function.

Note

Notes before using Self Version Management Function

Preparations for operating self version management function

The correspondent PC should be logged onto when operating the self version management function. If not, it cannot operate.

Disable firewall temporarily

In the case of operating version upgrade through self version management, after enabling the Windows firewall function, the window for confirming version upgrade cannot be displayed in the Client. After disabling the Windows firewall function on the Client terminal temporarily and rebooting OS, the window for confirming version upgrade will be displayed. Enable the Windows firewall function after completing version upgrade.

Number of terminals that can be downloaded simultaneously

Through the self version management function, the initial value of the number of terminals that can be applied simultaneously is 5. When modify this number of terminals, modify it in **Simultaneous Downloading Number (Maximum)** in the "Folder/CT Version auto-upgrade Settings" window of server settings tool. The terminal that exceeded this configuration value will execute the self version management function again when starting up next time.

When using self version management function in Windows Vista(R), Windows(R) 7, Windows(R) 8 and Windows(R) 10

When using the self version management function in the environment of Windows Vista(R), Windows(R) 7, Windows(R) 8 and Windows(R) 10, do not use the remote logon through Windows terminal service such as Windows "Remote Desktop Connection".

Windows (R) 8 and Windows(R) 10 fast startup feature

Assume that you are using Windows(R) 8 and Windows(R) 10 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 without shutting down.

Installing other software

After using the self version management feature to upgrade a client (CT), restart the operating system. If you install other software without restarting the operating system, the client (CT) may not upgrade properly.

Communication security settings

To receive self version management requests from a client (CT) of V14.3.1 or earlier, switch the communication security settings. You can use the security enhancement command to switch the communication security settings. Refer to "DTKSETCN.exe (Security Enhancement)" in the *Systemwalker Desktop Keeper Reference Manual* for details on how to use the security enhancement command.

Verification when registering client (CT) devices

When registering a client (CT) earlier than V15.1.0 to a Management Server of V15.1.0 or later, you cannot use verification during registration of client (CT) devices. Cancel the client management password. Refer to "Perform Terminal Operation Settings" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

Communication**s** between the Management Server or the Master Management Server and a client **(CT)**

Communications between the Management Server or the Master Management Server and a client (CT) are 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.

- Clients of V13.3.0 - V14.3.1 must be upgraded to V15.1, or the urgent updates released in September 2014 or later must be applied to the clients.

- Clients of V13.2.1 or earlier cannot be used. They must be upgraded to V15.1.0.

- After the Management Server is upgraded to V15.1.0, only a client of V15.0.0 or V15.1.0 can be installed.

When changing the connection destination Management Server and performing an upgrade using the self version management feature at the same time

A client (CT) of V14.3.1 or earlier to which the communication encryption update has not been applied, cannot be upgraded because communication with the new Management Server for registering management information is restricted. For this reason, the urgent updates released in September 2014 or later must be applied to clients (CT) beforehand.

![Note icon] **Note**

Notes when installing Client (CT) on (Master) Management Server

In the case of installing the Client (CT) on a (Master) Management Server, when setting version upgrade based on the self version management function of the Client (CT), whether to perform self-version upgrade through common self version management function will be requested. Because the server is required to restart after self-version upgrade, consider the application status of other Clients(CTs) such as connection status and determine whether to apply.

Behavior when confirmation windows and completion windows are hidden

Even when **Display self version upgrade confirming window** and **Display the reboot confirming window** are not selected in the client operation settings, the dialog box about copying modules from the server will be displayed on the client side.

![Note icon] **Note**

Behavior when confirmation windows and completion windows are hidden

Even when **Display self version upgrade confirming window** and **Display the reboot confirming window** are not selected in the client operation settings, the dialog box about copying modules from the server will be displayed on the client side.

![Point icon] **Point**

By specifying the IP address or computer name, self-version upgrade can be performed to the specified Client (CT).

Not all Clients (CTs) should perform self-version upgrade collectively; only the specified Client (CT) should perform the upgrade.

For example, use in the following cases:

- When trying to test the specific section before performing version upgrade completely

- When trying to perform according to the section and working place

- When trying to perform according to certain number of sets (CTs) in order to disperse the load

This function can be performed by creating "CT file (SWCTVerUpIP.txt) that can perform self-version upgrade".

The setting method is as follows: perform this procedure before performing the after-mentioned procedures for version upgrade.

1. Copy (or rename) "SWCTVerUpIP_sample.txt" as "SWCTVerUpIP.txt". Save "SWCTVerUpIP_sample.txt" to the following folder.

   In the case of any server other than Windows Server(R) 2008 and Windows Server(R) 2012:

   ```
   [OS Installation Drive] \Document and Settings\All Users\Application Data\Fujitsu\Systemwalker
   Desktop Keeper
   ```

   In the case of Windows Server(R) 2008 and Windows Server(R) 2012:

   ```
   [OS Installation Drive] \ProgramData\Fujitsu\Systemwalker Desktop Keeper
   ```

2. Open "SWCTVerUpIP.txt" through text editors such as Notepad.

3. Record the IP address or computer name of CT that can be performed self-version upgrade.

4. Save "SWCTVerUpIP.txt". (Do not move from the folder above.)

   For file details and how to specify the IP address or computer name, refer to "Settings File of Self Version Upgradable of CT " in *Systemwalker Desktop Keeper Reference Manual*.

· ·

The procedures for version upgrade based on the self version management function are as follows. The file saving target indicated in the following procedures is different from the installation target when modifying the OS.

Set Server

Perform the following settings on the subordinate Management Server/Master Management Server to the Client (CT).

1. In the Management Server/Master Management Server, select **Control Panel** > **Network Connection**.

2. Select "Local Area Connection" and disable the local area connection. Wait for 1 minute after disabling before performing the following procedures.

3. The Windows service window is displayed on the Management Server/Master Management Server. Select each of the following services and select "Stop" from the "Operation" menu". It will take 30 seconds to 1 minute to stop. 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

4. After the above services are stopped, enable "Local Connection".

5. On the Management Server/Master Management Server, save the file "SWCTVerSettings2.ini" under Setup folder "win32\DTKUpdate" to the following folder:

   - In Windows Server(R) 2008: "C:\Windows\System32"

   - In Windows Server(R) 2003: "C:\Windows\system32"

   - In Windows Server(R) 2003, 2003 R2 x64 Edition, Windows Server(R) 2008 64-bit Edition, Windows Server(R) 2008 R2 or Windows Server(R) 2012: "C:\Windows\SYSWOW64"

6. For the file "SWCTVerSettings2.ini", open the file properties, cancel the selection of "Read Only" check box, click the **OK** button.

7. On the Management Server/Master Management Server, save the following folder to the location recorded in **DistModuleDir** of file "SWCTVerSettings.ini".
   Ver4.9.0.1 folder in the win32\DTKUpdate folder on the setup disk
   Save the file "SWCTVerSettings.ini" to the following folder:

   - In Windows Server(R) 2008: "C:\Windows\System32"

- In Windows Server(R) 2003: "C:\Windows\system32"

- In Windows Server(R) 2003, 2003 R2 x64 Edition, Windows Server(R) 2008 64-bit Edition, Windows Server(R) 2008 R2 or Windows Server(R) 2012: "C:\Windows\SYSWOW64"

8. Perform the CT self version upgrade settings by using the server settings tool.
   Click the **Folder/CT Self Version Upgrade Settings** button in the server settings tool menu.

   The **Folder/CT Self Version Upgrade Settings** window is displayed.

9. Perform "**Management Server settings**" and "**Client operation settings**" displayed in **CT self version upgrade settings**.
   (No need to set **Folder settings** here. For the settings, refer to "2.3.6.9 Set Saving Target Folder".)

   Management Server settings

Item Name	Descriptions
Version	When the ini file (SWCTVerSettings2.ini) for CT self-version upgrade exists, the version specified in the ini file for CT self-version upgrade is displayed. It is not displayed when the ini file for CT self-version upgrade does not exist.

Module saving target on CT	The target folder for saving Client (CT) self-version upgrade module is specified. The specifying method is as follows: - Input the folder name in full path: input the saving target folder of module for self-version upgrade in full path. - Select **View** button: the **View Folder** window is displayed, select the saving target folder for self-version upgrade, click the **OK** button. A maximum of 96 halfwidth characters (48 fullwidth characters) can be entered in the specified full path. The followings symbols are not allowed in the folder name: Characters not allowed: "\""/"":""*""?""""""<"">""|"
Number of simultaneous download (maximum)	Multiplicity of Client (CT) self-version upgrade is set. The value that can be set is within 0-25. When specified as 0, self-version upgrade processing cannot be performed. When INI file for CT self-version upgrade does not exist, it cannot be displayed and set.

Client operation settings

Item Name	Descriptions
Display self version upgrade confirming window	Settings to confirm whether to perform self-version upgrade in Client (CT) with the user. However, when performing self-version upgrade from V13.2.0 or earlier, no matter whether **Display the Window for Confirming Version Auto-upgrade** is selected or not, the window for confirming self-version upgrade will be displayed. (This will be valid if selected when executing Edition upgrading of the same version) If this option is selected, the following information will be displayed after starting the Client (CT) terminal, and the user can select whether to execute self-version upgrade. (Operation in V13.2.0 or earlier). If this option is not selected, the confirmation window will not be displayed, execute after downloading self-version upgrade Setup file in the background. `------------------------------------------------------------------` `S101-ASK002 provides with the latest version. When updating to the latest module,` `click "Yes". Not to update, click "No".` `Reboot OS after selecting "Yes" and completing the update, thus end the application.` `------------------------------------------------------------------` Selecting **Yes** will execute self-version upgrade. Selecting **No** will not execute self-version upgrade.
Display the error sent when the self version is upgrading	Settings whether to display the error window if errors occurred when performing self-version upgrade in the Client (CT). If this option is selected, if errors occur during self-version upgrade, the following error information will be displayed and the processing will be cancelled. The user needs to close the error window manually, or self-version upgrade will not stop (up to the action of V13.2.0 or earlier). If this option is not selected, the error will not be displayed, and self-version upgrade will end directly with the error. To confirm whether self-version upgrade is applied in each Client, confirm the CT version of the correspondent Client (CT) in the Management Console. `------------------------------------------------------------------` `[I401-ERR011] Failed to install Systemwalker Desktop Keeper Client.`

		Please confirm the errors in the installation log file. Installation log file:[<u>Name of Installation Log File</u>]. Cancel installation -- --------
	Display the reboot confirming window	Settings whether to display the restart window after performing self-version upgrading in the client (CT). This item is valid only when **Reboot by force** is not selected. When **Reboot by force** is selected, this option will be grayed out. If this option is selected, after the installation based on self-version upgrade is completed, the restart window is displayed. Select either "Yes, restart the computer immediately." or "No, restart the computer later". If this option is not selected, after the installation based on self-version upgrade, no window will be displayed. Restart after completing modification through "Reboot by force" settings of the following item. Also, operate the Client (CT) of the version before applying self-version upgrade before rebooting.
	Reboot by force	Settings whether to restart by force after performing self-version upgrade in Client (CT). This item is valid only when **Reboot confirming window** is not selected. When **Reboot confirming window** is selected, this option will be grayed out. If this option is selected, reboot automatically after the installation based on self-version upgrade has been completed. When the file is opened, because it will be ended without being saved, content might be lost. If this option is not selected, the processing will be ended after the installation based on self-version upgrade has been completed. If **Display the reboot confirming window** is not selected, the restart confirmation window will not be displayed and the operation system will not be restarted. The user should restart it manually.

📒 Note

In case of Windows Vista(R), the window for reboot confirmation will not be displayed

When the OS is Windows Vista(R) and the environment self-version upgrade of V13.2.0/V13.2.1 Client (CT) has been installed, even if "Display Reboot Confirmation Window" is selected, the window for reboot confirmation will not be displayed. Although the window for reboot confirmation is not displayed, the version upgrade will take effect after PC is rebooted because the installation has been completed. If the installation version is V13.3.0 Client (CT), this case will not occur.

10. Create the CT silent installation file by using server settings tool. For details on how to use the setting tool, refer to "Create installation settings file".

📘 Point

Items viewed during version upgrade by using self version management function

Only the following items specified during creation of the CT silent installation file are referenced during a version upgrade using the self version management feature. Other items will not be referenced.

- **Printing monitoring mode**

- **E-mail attachment prohibition**

- **Creation Settings of File Export Utility Icon**

- **Port number (for E-mail attachment prohibition)**

- **Port number (for E-mail attachment prohibition 2)**

- **Port number (for E-mail sending monitoring)**

- **Apply policy immediately after logging on Windows**
. . . .

11. Save the CT silent installation file created in Procedure 10. to the following folder of the recorded location in **DistModuleDir** confirmed in Procedure 7.

    - "Ver4.9.0.1"

12. On the Management Server/Master Management Server, the Windows service window is displayed, select the services to be cancelled ("SWLevelControlService" and "SWServerService") and select **Start** from the **Operation** menu.

Operations of Client (CT)

1. Start and log on to the Client (CT) of version upgrade.

   The following message is displayed:

   ```
   [S101-ASK002] provides with the latest module.
   When updating to the latest version, please click "Yes".
   When not to update, please click "No". If selecting "Yes" and OS should be restarted after the
   update is completed, please end the application.
   ```

   ## 📙 Note
   . . . .

   Select Yes.

   Make sure to click the **Yes** button in the message window above. When clicking the **No** button, the "E-mail sending log obtaining " and "E-mail file attachment prohibition" cannot be operated before rebooting.
   . . . .

2. After clicking the **Yes** button, the "Update Completed" window will be displayed.

   ## 📙 Note
   . . . .

   Prohibition and log collection cannot be operated well if the system is not rebooted

   Make sure to restart in the following window. If not, the "E-mail Sending Log Acquisition Function" cannot operate.

   Notes when setting E-mail attachment prohibition mode

   In case of Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10 or Windows Server(R) 2012

   When using Windows Vista(R), Windows Server(R) 2008, Windows(R) 7, Windows(R) 8, Windows(R) 10 or Windows Server(R) 2012, only the port monitoring mode can be selected as E-mail attachment prohibition mode.

   Confirm whether port is not used

   For the port for E-mail attachment prohibition, make sure to specify a port not used in other processing and communication.

   Require rebooting

   When performing version/edition upgrade from the following versions to V15.1.0, after installing "E-mail sending log obtaining" and "E-mail file attachment prohibition ", these functions cannot operate before rebooting.
   - BEV12.0L20
   - SEV12.0L20
   - BEV13.0.0 /SEV13.0.0
   When upgrading from the following versions to V15.1.0, before rebooting, the version before upgrade operates well.
   - BEV13.2.0 /SEV13.2.0
   - V14.2.0
   . . . .

3. Click the **Finish** button.

   Client (CT) is restarted.

4.8 Upgrading the Log Analyzer Server and Report Output Tool

This describes how to upgrade the Log Analyzer to the latest version.

4.8.1 Upgrading the Log Analyzer Server

To upgrade to the latest version of the Log Analyzer Server, the current environment must be deleted before constructing the new Log Analyzer Server.
Also, store the log data in the Log Analyzer Server by reimporting it from Systemwalker Desktop Keeper Management Server or Master Management Server.
Before upgrading, ensure that the Management Server and Master Management Server have been upgraded.

Uninstall the older version of the Log Analyzer Server

Before upgrading, uninstall the old version of the Log Analyzer Server.
Refer to the manual applicable to the old version of the Log Analyzer Server for details on how to uninstall it.

Note

Delete the NAVIDIC and NAVISV folders
If the folders below still remain after uninstallation of the old version of the Log Analyzer Server, remove them manually, otherwise the Log Analyzer Server may not install correctly.

- oldVersionLogAnalysisServerInstallFolder\NAVIDIC

- oldVersionLogAnalysisServerInstallFolder\NAVISV

Install the Log Analyzer Server

Construct a new Systemwalker Desktop Keeper Log Analyzer Server. Refer to "2.7 Construct Log Analyzer Server" for details.

Prepare the operating environment of the Log Analyzer Server

Set up the operating environment of the Log Analyzer Server. Refer to "Schedule Log Transmission" and "Set Conditions for Aggregation/Report Output" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

4.8.2 Upgrading the Report Output Tool

To upgrade the Report Output Tool, perform overwrite installation. Refer to "2.8.1 Install Report Output Tool" for details.
After an overwrite installation, you must configure the environment.

Note

When using the older version of the Report Output Tool on Windows Server 2003, do not overwrite the install for version upgrade.

Uninstall the older version of the Report Output Tool and install the latest version on the operating system supported by the latest version.
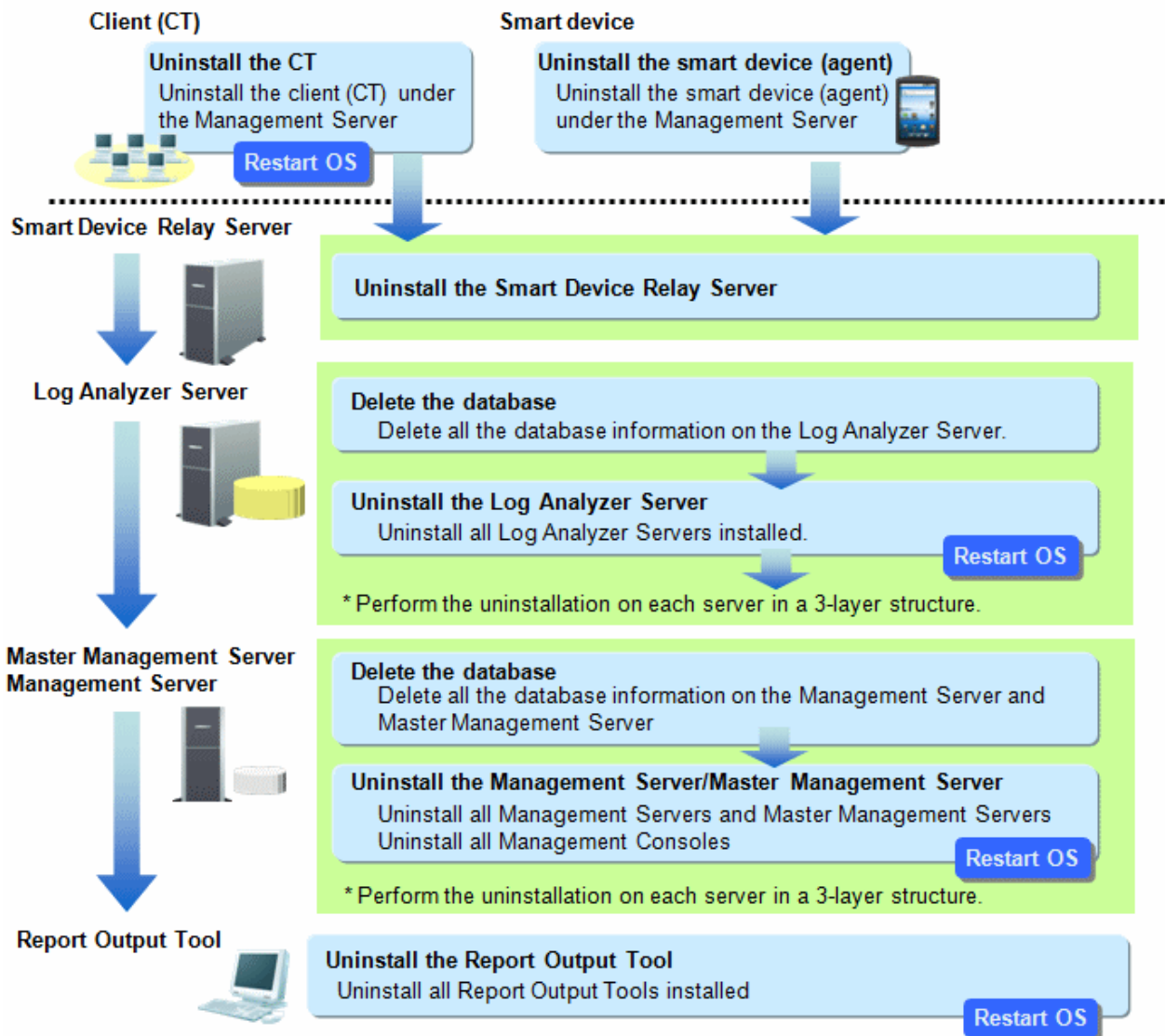
Chapter 5 Uninstallation

This chapter describes how to uninstall Systemwalker Desktop Keeper.

5.1 Uninstallation Steps

This section describes the steps to uninstall Systemwalker Desktop Keeper.

When installing client (CT) on Management Server/Master Management Server

When installing a client (CT) on a Management Server/Master Management Server, uninstall and re-install the Management Server/Master Management Server according to the following procedure. If the procedure is not followed, the Management Server/Master Management Server will not be installed again.

1. Uninstall the client (CT)

2. Uninstall the Management Server/Master Management Server

3. Install the Management Server/Master Management Server

4. Install the client (CT)

> **Note**

Uninstalling Uninstall (middleware)

Uninstall (middleware) is a common tool used by Fujitsu middleware products. It manages Fujitsu middleware products installed, as well as launching the product uninstallers. Do not uninstall Uninstall (middleware) unless it is absolutely necessary.

1. Click **Start** > **Fujitsu** > **Uninstall (middleware)** or **Apps** > **Fujitsu** > **Uninstall (middleware)**, and ensure that there are no other Fujitsu middleware products left on the system. Close the tool after confirming.

2. Execute the uninstallation command:

   - 32-bit operating system

   ```
   C:\Program Files\Fujitsu\FujitsuF4CR\bin\cirremove.exe
   ```

   - 64-bit operating system

   ```
   C:\Program Files (x86)\Fujitsu\FujitsuF4CR\bin\cirremove.exe
   ```

3. In the uninstallation confirmation message, type "y".

4. After uninstallation, the following folders/files will remain, so they must be manually deleted.

   ```
   C:\ProgramData\Fujitsu\FujitsuF4CR
   ```

   The drive may be different depending on the environment.

5.2 Uninstall Client (CT)

This section describes how to uninstall Systemwalker Desktop Keeper Client (CT).

When installing Systemwalker Desktop Keeper Client (CT) has been installed on Citrix XenApp Client, uninstall with the same procedure.

The methods of uninstalling the client (CT) include the following two types.

- Wizard-style Uninstallation

- Silent Uninstallation

> **Note**

The network will be disconnected during uninstallation of the client (CT).

The network will be disconnected temporarily during uninstallation of the client (CT). If the network folder is open (in Windows Explorer, for example), then close it.

> **Note**

Password to be used for uninstallation

If a client management password has been set in the Management Console, use that password for uninstallation. If a client management password has not been set, use the password set during installation of the client (CT).

5.2.1 Wizard-style Uninstallation

> **Note**

In Windows(R) 8 64-bit or Windows Server(R) 2012 or later, an error message may be output during uninstallation.
In Windows(R) 8 64-bit or Windows Server(R) 2012 or later, an automatic registration error may be output during uninstallation. Click

OK to proceed with the uninstallation.

Note that a similar message may be displayed during uninstallation of the Management Server or Management Console.

· ·

It describes how to uninstall Systemwalker Desktop Keeper Client (CT) with Wizard-style.

1. Log on to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. When other another application is being used, exit it.

2. Start **Control Panel** > **Programs and Features**.

3. Select **Systemwalker Desktop Keeper Client**, and click **Remove**.

4. After clicking **Yes** in the removal confirmation window, the password input window will be displayed. Enter the client management password set in the Management Console, or the password set during installation of the client (CT), and click **Next**.

5. The uninstallation begins. After it has finished normally, the "Uninstallation Completed" window will be displayed.

   The operating system needs to be restarted after uninstallation has finished. Select one of the following options, and then click **Finish**.

   - **Yes, restart the computer immediately.**

   - **No, restart the computer later.**

🔆 Note

· ·

In the case of Windows Vista(R), Windows Server 2008(R), Windows(R) 7 or later, an error message will be output when restarting

When using Windows Vista(R), Windows Server 2008(R), Windows(R) 7 or later, when restarting after uninstallation, the following message will be output. The uninstallation will run normally, so continue with the operation.

```
Error occurred when uninstalling Systemwalker Desktop Keeper Client. It may have already been
uninstalled.
Do you want to remove Systemwalker Desktop Keeper Client from [Programs and Functions]?
```

The same message will also be displayed when uninstalling the Management Console and the Log Viewer.

· ·

5.2.2 Silent Uninstallation

🔆 Note

· ·

In Windows(R) 8 64-bit or Windows Server(R) 2012 or later, an automatic registration error message may be output during uninstallation. Click **OK** to proceed with the uninstallation.

Note that a similar message may be displayed during uninstallation of the Management Server or Management Console.

· ·

The following describes how to uninstall Systemwalker Desktop Keeper Client (CT) silently.

Note that this feature can be executed in the environment where the first version of the client (CT) is installed. It cannot be executed on clients (CT) that have had updates applied.

1. Log on to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. When other applications are being used, exit them.

2. Insert the DVD-ROM of Systemwalker Desktop Keeper into the PC.

3. Start **Run** or Command Prompt.

4. Run the Setup.exe command that is located in the "win32\DTKClient" folder on the setup disk. Use the files that have been used during installation again.

Command Format

```
Specify with absolute path Setup.exe /Silent "Password:password,Reboot:flag"
```

- Available option key: "Password","Reboot"

- No space between items in "Key:*Value*" and "Key:*Value*".

- Options are not case-sensitive.

- If no option is specified, an error message will be displayed and then the uninstallation will be aborted.

The meaning of keys is as follows:

- "Password": The client management password set in the Management Console, or the password set during installation of the client (CT)

- "Reboot": The flag specified after the uninstallation has been executed.

    - 0: Do not reboot

    - 1: Display the dialog box (reboot or not)

    - 2: Reboot by force

Example

Assume the following situations:

- The setup disk is inserted in D Drive

- The Setup.exe command is located in D: \win32\DTKClient

- The password for displaying & updating the client status is admin

- Reboot by force after uninstallation

```
D:\win32\DTKClient\Setup.exe /Silent "Password:admin,Reboot:2"
```

5. When the dialog box is displayed, select whether to reboot or not.

5.3 Uninstalling Smart Device (Agent) (Android)

This section explains how to uninstall the smart device (agent) (Android) of Systemwalker Desktop Keeper.

1. Open the setup screen of the smart device, and then tap **Application**.

2. Tap **Manage applications**.

3. In the application management screen, tap **Desktop Keeper Client**.

4. In the application information screen, tap **Uninstall**.

5. In the uninstallation confirmation screen, tap **OK**.

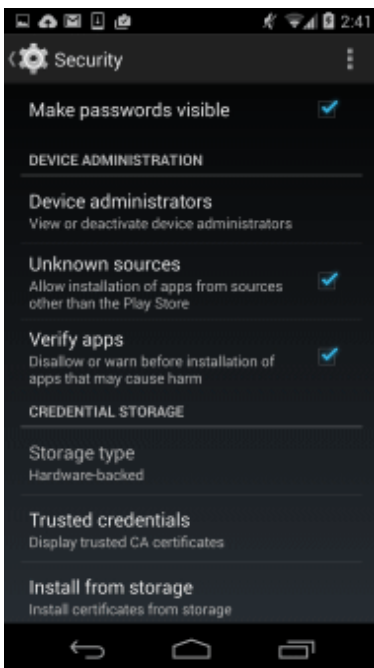6. Upon completion, the uninstallation completion screen will be displayed - tap **OK**.

Note

Steps required before uninstallation

If "To prevent uninstallation" was specified during smart device installation, follow the procedure below before performing uninstallation.
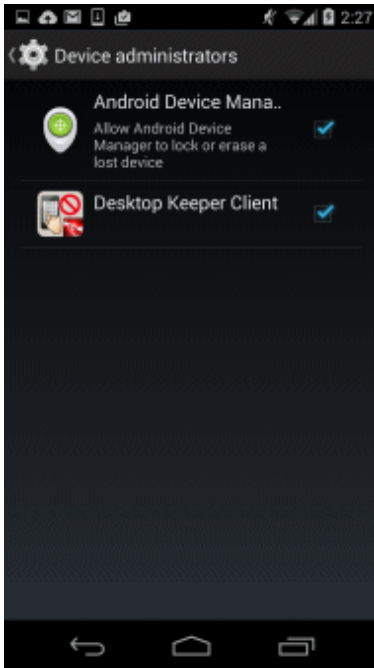
1. Tap **Security**.
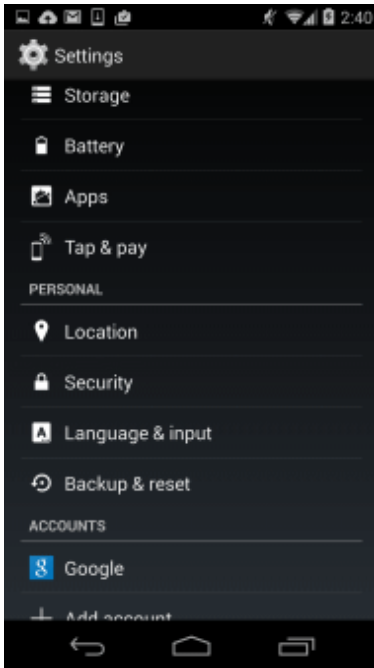
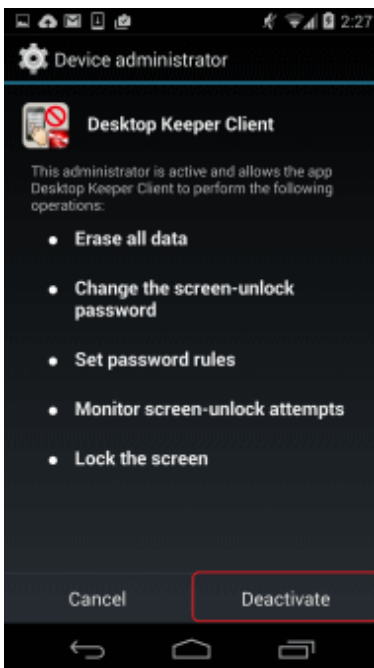2. Select **Device administrators**.

3. From the device administrator list, select **Desktop Keeper Client**.

4. In the screen for disabling the device manager, tap **Deactivate**.

5. The password entry screen for unlocking will be displayed.
   If the client management password has been set, enter the client management password, and then tap **OK**. Otherwise, tap **OK** without entering a password.

Use the Management Console to set the client management password. Refer to "Perform Terminal Operation Settings" in the *Systemwalker Desktop Keeper User's Guide for Administrator* for details.

5.4 Uninstalling Smart Device (Agent) (iOS)

This section explains how to uninstall the smart device (agent) (iOS) of Systemwalker Desktop Keeper.

1. In the iOS device, tap **Settings** > **General** > **Profiles**, and then delete the following registered profiles:

   - Profile Service Enroll

   - CA certificate (server)

   - CA certificate (client)

5.5 Uninstall Management Console

Note

In Windows(R) 8 64-bit or Windows Server(R) 2012 or later, an automatic registration error message may be output during uninstallation. Click **OK** to proceed with the uninstallation.
Note that a similar message may also be displayed during uninstallation of the Management Server and client (CT).

The following describes how to uninstall Systemwalker Desktop Keeper Management Console.

1. Log on to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. When other applications are being used, exit them.

2. Click **Start** > **Fujitsu** > **Uninstall (middleware)** or **Apps** > **Fujitsu** > **Uninstall (middleware)**.

3. In **Currently installed products**, select **Systemwalker Desktop Keeper Management Console**, and click **Remove**.

4. In the **Uninstall Systemwalker Desktop Keeper management console** dialog box, click **Uninstall**.

5. Upon completion, the uninstallation completion dialog box will be displayed - click **Finish**.

6. Restart the operating system.

5.6 Uninstall Log Analyzer Server

The following section describes how to uninstall the Log Analyzer Server of Systemwalker Desktop Keeper.

 Note

. . . .
The procedure described in this section is for this version. To uninstall an older version, refer to the manual for the applicable version.
. . . .

Delete the log transfer schedule settings

Delete the following tasks registered in the operating system.

- Data transfer task to Log Analyzer Server to be uninstalled (Management Server)
  DTK_TRANS

- Data import task on Log Analyzer Server to be uninstalled (Log Analyzer Server)
  DTK_DttoolEx

Delete the Log Analyzer Server information on the Management Server/Master Management Server

Use the Log Analyzer setting tool of the Log Analyzer Server to delete the applicable Log Analyzer Server information on the Management
Server or Master Management Server where the information of the Log Analyzer Server to be uninstalled is registered.

1. Click **Start** > **Systemwalker Desktop Keeper** > **Server** > **Log Analyzer settings**, or **Apps** > **Systemwalker Desktop Keeper** >
   Log Analyzer settings.

2. Delete the applicable Log Analyzer Server information, and then click **Set**.

Delete database of Log Analyzer Server

Before uninstalling the Log Analyzer Server of Systemwalker Desktop Keeper, delete the database. The procedures to delete the database
are as follows:

1. Log on Windows as Log Analyzer user (Windows account set when installing Log Analyzer Server).

2. Select **Systemwalker Desktop Keeper** > **Log Analyzer** > **Operating Environment Maintenance Wizard** from the **Start/Apps**
   menu.

3. The **Welcome to Operating Environment Maintenance Wizard** window will be displayed, and click **Next**.

4. The **Select processing** window will be displayed. Select **Deletion of Operating Environment** for the process to be executed, and
   click **Next**.

5. The **Confirm the settings content** window will be displayed. Confirm whether the contents displayed in window are incorrect, and
   click **Next**.

6. The execution confirmation window will be displayed, click **OK** when continuing the execution.

7. The **Executed Process** window will be displayed and then start to delete the database.

8. The **Process Completed** window will be displayed when the process is completed normally. Click **Completed**.

Uninstall Log Analyzer Server

The following procedures to uninstall the Log Analyzer Server are as follows:

1. Log on to Windows with the user used at the construction of database of Management Server/Master Management Server. When other applications are being used, exit them.

2. Click **Start** > **Fujitsu** > **Uninstall (middleware)** or **Apps** > **Fujitsu** > **Uninstall (middleware)**.

3. In **Currently installed products**, select **Systemwalker Desktop Keeper log analyzer server** and click **Delete**.

4. In the **Uninstall Systemwalker Desktop Keeper log analyzer server** dialog box, click **Uninstall**.

5. Upon completion, the uninstallation completion dialog box will be displayed - click **Finish**.

6. Restart the operating system.

If using the 64-bit version, **Systemwalker Desktop Keeper log analyzer server (x64)** will be displayed in steps 3 and 4.

Note

The procedure must be followed (starting at step 2) even if Systemwalker Desktop Keeper Log Analyzer Server has been deleted from the Control Panel.

Delete the installation folder

If the following folder remains, it must be manually deleted.

logAnalyzerServerInstallFolder\NAVIDIC

If the following note does not apply, delete the whole Log Analyzer Server installation folder.

Note

If the installation folder of database-related files is under the Log Analyzer Server installation folder and the Management Server is installed on the same server that the Log Analyzer Server, do not delete the Log Analyzer Server installation folder. Otherwise, the Management Server will no longer operate.

Note

About log analysis user after uninstallation

Though the Log Analyzer Server is uninstalled, the new Log Analyzer user in installation will not be deleted. Delete after confirming that the Log Analyzer user is not used.

When reinstalling Log Analyzer Server, be sure to restart the operating system after the above procedures are performed, and then reinstall.

5.7 Uninstalling Smart Device Relay Server

This section explains how to uninstall the Smart Device Relay Server of Systemwalker Desktop Keeper.

Note

When reinstalling the Smart Device Relay Server in an https communication environment

When reinstalling Smart Device Relay Server due to environment migration or other reason in an environment that uses https communication between smart devices and the Smart Device Relay Server, back up the server certificate before uninstalling. Also, store the CA certificate and intermediate CA certificate beforehand.

- In the command prompt, back up the server certificate:

```
smartDevRelayServerInstallFolder\bin\SDSVKeyStore.exe -export serverCertFile
```

Example:

```
C:\SWDTKSDSV\bin>SDSVKeyStore -export C:\temp\keybackup.cer
```

It is not necessary to follow the steps to register the server certificate described in "2.9.3.2 Configuring HTTPS Communication" during reinstallation.

Refer to "2.9.3.2 Configuring HTTPS Communication" for details on how to register the CA certificate and intermediate CA certificate stored beforehand. After registration, restore the backed up server certificate.

- In the command prompt, restore the server certificate:

```
smartDevRelayServerInstallFolder\bin\SDSVKeyStore.exe -import serverCertFile
```

Example:

```
C:\SWDTKSDSV\bin>SDSVKeyStore -import C:\temp\keybackup.cer
```

Refer to "SDSVKeyStore.EXE (Backup/Restore Server Certificate)" in the *Systemwalker Desktop Keeper Reference Manual* for details.

Uninstall Smart Device Relay Server

1. Log on to Windows as a user that belongs to the Administrators group or Domain Admins group. If other applications are being used, then they must be closed.

2. Use SDSVSetMS.EXE (Change Configuration of Smart Device Relay Server) to set the following options.

   - Disable the Android device management by specifying the -Android.enabled option.

   - Disable the iOS device by specifying the -iOS.enabled option.

3. Click **Start** > **Fujitsu** > **Uninstall (middleware)** or **Apps** > **Fujitsu** > **Uninstall (middleware)**.

4. In **Currently installed products**, select **Systemwalker Desktop Keeper Smart Device Relay Server**, and then click **Delete**.

5. In the **Uninstall Systemwalker Desktop Keeper Smart Device Relay Server** dialog box, click **Uninstall**.

6. Upon completion, the uninstallation completion dialog box will be displayed - click **Finish**.

7. Restart the operating system.

📝 Note

The procedure must be followed (starting at step 2) even if Systemwalker Desktop Keeper Smart Device Relay Server has been deleted via the Control Panel.

Delete the installation folder

After uninstallation, the Smart Device Relay Server installation folder remains, and must be manually deleted.

5.8 Uninstall Management Server/Master Management Server

The following describes how to uninstall Systemwalker Desktop Keeper Management Server/Master Management Server.

Note

- When installing a client (CT) on a Management Server/Master Management Server, pay attention to the uninstall order.
  For details, refer to "When installing client (CT) on Management Server/Master Management Server".

- In Windows(R) 8 64-bit or Windows Server(R) 2012 or later, an automatic registration error message may be output during uninstallation. Click **OK** to proceed with the uninstallation.
  Note that a similar message may also be displayed during uninstallation of the Management Console and client (CT).

5.8.1 Delete the database of Management Server/Master Management Server

Delete the database before uninstalling the Management Server/Master Management Server of Systemwalker Desktop Keeper. The steps for deleting a database are as follows:

1. Log on to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. When other applications are being used, exit them.

2. Select **Start** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool** or **Apps** > **Systemwalker Desktop Keeper** > **Server** > **Server settings tool**.

3. Log on using the primary administrator account:

   - User ID: secureadmin

   - Password: Specify the initial value "secureadmin", or the password modified after installation of Management Server/Master Management Server

4. In the Server Settings Tool menu, click **Build, delete, or show information of database**.
   The **Build, delete, or show information of database** window will be displayed.

Item Name	Description
Database creation folder	Database creation destination folder.
Database usage	Usage of the created database. If the database has not been built, this item will be blank.
Disk availability	Available space on the creation destination disk.

5. In the **Build, delete, or show information of database** window, click **Delete** for the database to be deleted. The confirmation message is displayed. Click **OK** - database deletion will start.

6. Upon successful completion, the completion message is displayed. Click **OK**.

   If an Operation Database, Log Viewing Database or iOS Management Database remains, execute again from step 1.

Note

. . . .

When the database area cannot be deleted

Even if **Server settings tool** > **Build, delete, or show information of database** is used to delete the operating environment, due to the database status, the database may not be deleted sometimes. If this occurs, delete the following file.

- <Database Saving Target>\RDB

. . . .

Note

. . . .

- If Systemwalker Desktop Keeper and Systemwalker Desktop Patrol coexist, and you want to stop managing the iOS devices managed in both products, delete the iOS management database in both products.

- If Systemwalker Desktop Keeper and Systemwalker Desktop Patrol coexist, and you now want to manage the iOS devices, previously managed in both products, in one product only, follow the procedure below to delete the iOS management database in one of the products:

  1. Use SDSVSetMS.EXE (Change Configuration of Smart Device Relay Server) to check the host name of the iOS management database connected to the Smart Device Relay Server. Perform backup on the server that matches the iOS management database host name displayed in "iOSmgr.h".

  2. Delete the iOS management database in both products.

  3. Build the iOS management database in the product that manages iOS devices.

  4. In the iOS management database built in step 3, restore the data backed up in step 1.

. . . .

5.8.2 Uninstall Management Server/Master Management Server

Continue to uninstall the Management Server/Master Management Server. The steps of uninstalling the Management Server / Master Management Server are as follows.

1. Log on to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. When other applications are being used, exit them.

2. Stop the level control server and server service.

   The Windows service window is displayed. Select the following services and select **Stop** from the **Operation** menu. It will take 30 seconds to 1 minute till the services are stopped. 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, confirm later.

   - SWLevelControlService

   - SWServerService

3. Click **Start** > **Fujitsu** > **Uninstall (middleware)** or **Start** or **Apps** > **Fujitsu** > **Uninstall (middleware).**

4. In **Currently installed products**, select **Systemwalker Desktop Keeper management server**, and then click **Delete**.

5. In the **Uninstall Systemwalker Desktop Keeper management server** dialog box, click **Uninstall**.

6. Upon completion, the uninstallation completion dialog box will be displayed - click **Finish**.

7. Restart the operating system.

If using the 64-bit version, **Systemwalker Desktop Keeper management server (x64)** will be displayed in steps 4 and 5.

Note

- The procedure must be followed (starting at step 3) even if Systemwalker Desktop Keeper server has been deleted via the Control Panel.

Delete the installation folder

After uninstallation, the Management Server/Master Management Server installation folder remains, and must be manually deleted.

Note

If the Log Analyzer Server is installed on the server where the Management Server/Master Management Server has been uninstalled, do not delete the Systemwalker Desktop Keeper installation folder under any circumstances. Otherwise, the Log Analyzer Server will no longer operate.

5.9 Uninstall Report Output Tool

The following describes how to uninstall the Report Output Tool of Systemwalker Desktop Keeper.

Note

The procedure described in this section is for this version. To uninstall an older version, refer to the manual for the applicable version.

Uninstall Report Output Tool

The steps of uninstalling the Report Output Tool are as follows:

1. Log on to Windows with a user that belongs to the Administrators group or a user that belongs to the Domain Admins group. When other applications are being used, exit them.

2. Click **Start** > **Fujitsu** > **Uninstall (middleware)** or **Apps** > **Fujitsu** > **Uninstall (middleware)**.

3. In **Currently installed products**, select **Systemwalker Desktop Keeper report output tool**, and then click **Delete**.

4. In the **Uninstall Systemwalker Desktop Keeper report output tool** dialog box, click **Uninstall**.

5. Upon completion, the uninstallation completion dialog box will be displayed - click **Finish**.

6. Restart the operating system.

Note

The procedure must be followed (starting at step 2) even if Systemwalker Desktop Keeper Report Output Tool has been deleted via the Control Panel.

Delete the installation directory

After uninstallation, the Report Output Tool log remains, and can be manually deleted if necessary.

- %ALLUSERSPROFILE%\Fujitsu\Systemwalker Desktop Keeper\LogAnalyzer
  (%ALLUSERPROFILE% generally is set to "C:\ProgramData")

Note

Do not delete when the database management system is not uninstalled.

Do not delete the installation folder of the Log Analyzer Server when the database management system of Systemwalker Desktop Keeper remains under the installation folder of the Log Analyzer Server. After it has been deleted, the database management system will be unable to run.

.... - 257 - ....

Appendix A Server Silent Installation

This appendix describes files, commands, and messages used in silent installation of the Systemwalker Desktop Keeper server.

A.1 Silent Installation of the Management Server or Master Management Server

This section describes files, commands, and messages used in silent installation of the Systemwalker Desktop Keeper Management Server or Master Management Server.

A.1.1 Installation Parameter CSV File

Specify the installation parameters in a CSV file using the format described in this section.

Character encoding

UTF8

Format

```
installInfo,softwareName,softwareName
installInfo,OS,os
installInfo,Version,version
installInfo,Name,softwareId
parameters,paramKey,paramValue
parameters,...,...
```

📌 **Note**

....

- Do not change any installInfo parameter from the sample content.

- Specify one or more parameters in the parameters parameter.

- If double quotation marks are used to enclose data, then all fields within the same record must be enclosed in double quotation marks.

- Do not specify spaces in the first column or in the second column.

- Spaces cannot be specified before or after fields enclosed in double quotation marks.

....

parameters parameter

The parameters are described below.

No.	Parameter	Parameter information		Description
1	Management Server installation directory	**Key**	DtkSvInstPath	Specify the installation directory for the Management Server.
		Data type	String	Specify up to 85 halfwidth alphanumeric characters and symbols, excluding characters that cannot be specified in Windows and the following symbols: , ; #
		Value can be changed	Y	
		Default value	C:\Program Files (x86)\Fujitsu \Systemwalker Desktop Keeper	If installing on a 32-bit operating system, change to: C:\Program Files\Fujitsu\Systemwalker Desktop Keeper Required

No.	Parameter	Parameter information		Description
2	Operation database creation folder	**Key**	DtkSvDBPath	Specify the database creation folder. It must meet the following conditions: The root drive cannot be specified. - It cannot contain fullwidth characters, halfwidth kana, and control characters. - It can be up to 96 halfwidth characters. - A network drive cannot be specified. - It must be NTFS-formatted. - The folder name cannot contain the following characters: \ / : * ? " < > | & ^ Required
		Data type	String	
		Value can be changed	Y	
		Default value	C:\DTK\OPEDB	
3	Automatic backup creation folder	**Key**	DtkSvAutoBackUpPath	Specify the automatic backup folder. It must meet the following conditions: - The root drive cannot be specified. - A network drive cannot be specified. - It can be up to 189 halfwidth characters. - The folder name cannot contain the following characters: \ / : * ? " < > | Required
		Data type	String	
		Value can be changed	Y	
		Default value	C:\DTKBackup	

Information

A sample installation parameter CSV file is stored in the following folder of the product media (DVD-ROM).

dvdRom:\citool\SV\sample_install_SWDTK.csv

A.1.2 Parameter Setup Command

If customizing parameters, create a response file in which the parameters were changed using the parameter setup command, and use this file for silent installation.

Command name

dvdRom:\citool\SV\dtk_instparam.exe

Syntax

```
dtk_instparam.exe -infile installParmCsvFile -outfile responseFile
```

Options

Option	Description
-infile	Specify the installation parameter CSV file. Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters. If the path includes spaces, enclose it in double quotation marks.
-outfile	Specify the response file to be output.

Option	Description
	Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters.
	If the path includes spaces, enclose it in double quotation marks.
	If the file already exists in the output destination, it will be overwritten.

Return values

If the return value is 0:

Ended normally.

If the return value is other than 0:

Ended abnormally.

Refer to the error message output to the console and take appropriate action.

Examples

The following command specifies the parameters in the installation parameter CSV file C:\sample_install_SWDTK.csv, and creates the response file C:\temp\swdtk_sv_setup.iss:

```
dtk_instparam.exe -infile C:\sample_install_SWDTK.csv -outfile C:\temp\swdtk_sv_setup.iss
```

A.1.3 Messages Output by the Parameter Setup Command

This section describes the messages output by the parameter setup command.

The environment-dependent constraints in the installation parameters are not checked by this command. Therefore, even if an error is not output by this command, an error may still occur during installation.

System error.

Cause

A system error occurred.

Action

Contact Fujitsu technical support.

Argument error: Usage: dtk_instparam -infile "input file path" -outfile "output file path".

Cause

The syntax of a required argument is incorrect.

Action

Check the syntax of the command.

Error: too long path specified(path must be less than 256 bytes).

Cause

The specified file path is too long.

Action

Specify the file path using up to 255 halfwidth characters.

Error: file not exist.

Cause

The specified file does not exist.

Action

Ensure that the specified file path is correct.

Error: failed to open file.

Cause

The file could not be opened.

Action

Ensure that the file is not in use, or is not corrupted.

Error: failed to parse csv file.

Cause

Failed to process the CSV file.

Action

Ensure that the CSV file format is correct.

Error: Command Option is not correct.

Cause

The syntax of the command argument is incorrect.

Action

Check the argument of the command that was executed.

Error: can't find out parameter from input file.

Cause

The file specified in -infile does not contain any parameters.

Action

Check the contents of the file specified in -infile.

Error. the length of install parameters exceeds the defined size.

Cause

The length of the specified parameter exceeds the defined size.

Action

Check the parameter length.

Error. Invalid character is used for install parameters.

Cause

An invalid character type is used for the parameters.

Action

Check the character types specified for the parameters.

Success: complete to edit Installation file.

Description

Successfully edited the installation parameter file.

A.1.4 Silent Installation Script

This section explains the script used for silent installation.

Script name

dvdRom:\citool\SV\silentsetup.vbs

Syntax

Execute using cscript, with the response file as the argument.

```
cscript silentsetup.vbs [responseFile]
```

Options

Option	Description
responseFile (optional)	Specify this option if you want to change the parameters to be used during setup from their default values. Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters. If the path includes spaces, enclose it in double quotation marks. Do not specify Unicode characters. If omitted, the default values will be used for all parameters.

Return values

If the return value is 0:

Ended normally.

If the return value is other than 0:

Ended abnormally.

Refer to the error message output to the console and take appropriate action.

Examples

The following command performs silent installation with the response file C:\temp\swdtk_sv_setup.iss:

```
cscript silentsetup.vbs c:\temp\swdtk_sv_setup.iss
```

Privilege required for execution/execution environment

- Administrator privileges for the target installation environment are required.

- To use this command in Windows Server(R) 2008 or Windows Server(R) 2012, display the desktop and execute this command on a **Command Prompt** window that has been started by selecting **Run as Administrator**.

A.1.5 Messages Output by the Silent Installation Script

This section explains the messages output by the silent installation script.

This program must be executed by account of Administrators.

Cause

Administrator privileges are required.

Action

Execute as a user with Administrator privileges.

Installation is failed.ErrorCode:XX

Cause

Silent installation failed.

Action

Check the installation environment and the following log file:

%ALLUSERSPROFILE%\Fujitsu\Systemwalker Desktop Keeper\DTKServer_Install.log

A.2 Silent Installation of the Log Analyzer Server

This section describes files, commands, and messages used in silent installation of the Systemwalker Desktop Keeper Log Analyzer Server.

A.2.1 Installation Parameter CSV File

Specify the installation parameters in a CSV file using the format described in this section.

Character encoding

UTF8

Format

```
installInfo,softwareName,softwareName
installInfo,OS,os
installInfo,Version,version
installInfo,Name,softwareId
parameters,paramKey,paramValue
parameters,...,...
```

📒 **Note**

. . . .

- Do not change any installInfo parameter from the sample content.

- Specify one or more parameters in the parameters parameter.

- If double quotation marks are used to enclose data, then all fields within the same record must be enclosed in double quotation marks.

- Do not specify spaces in the first column or in the second column.

- Spaces cannot be specified before or after fields enclosed in double quotation marks.

. . . .

parameters parameter

The parameters are described below.

No.	Parameter	Parameter information		Description
1	Log Analyzer Server installation directory	**Key**	DtkLaInstPath	Specify the installation directory for the Log Analyzer Server.
		Data type	String	Specify up to 85 halfwidth alphanumeric characters and symbols, excluding characters that cannot be specified in Windows and the following symbols: , ; #
		Value can be changed	Y	
		Default value	C:\Program Files (x86)\Fujitsu \Systemwalker Desktop Keeper\LogAnalyzer \Server	If installing on a 32-bit operating system, change to: C:\Program Files\Fujitsu\Systemwalker Desktop Keeper\LogAnalyzer\Server

No.	Parameter	Parameter information		Description
				Required
2	Database installation directory	**Key**	DtkLaDbInstPath	Required when the Log Analyzer Server does not coexist with the Management Server
		Data type	String	Specify the installation directory for database-related files using up to 96 halfwidth alphanumeric characters and symbols, excluding spaces, characters that cannot be specified in Windows, and the following symbols: , ; #
		Value can be changed	Y	
		Default value	C:\DTKLADB	
3	Port number 3	**Key**	DtkLaPort03	Specify a number from 5001 to 60000.
		Data type	String	Required
		Value can be changed	Y	
		Default value	30004	

📖 **Information**

. . . .

A sample installation parameter CSV file is stored in the following folder of the product media (DVD-ROM).

dvdRom:\citool\LA\sample_install_SWDTLA.csv

. . . .

A.2.2 Parameter Setup Command

If customizing parameters, create a response file in which the parameters were changed using the parameter setup command, and use this file for silent installation.

Command name

dvdRom:\citool\LA\dtkla_instparam.exe

Syntax

```
dtkla_instparam.exe -infile installParmCsvFile -outfile responseFile
```

Options

Option	Description
-infile	Specify the installation parameter CSV file.
	Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters.
	If the path includes spaces, enclose it in double quotation marks.
-outfile	Specify the response file to be output.
	Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters.
	If the path includes spaces, enclose it in double quotation marks.
	If the file already exists in the output destination, it will be overwritten.

Return values

If the return value is 0:

Ended normally.

If the return value is other than 0:

Ended abnormally.

Refer to the error message output to the console and take appropriate action.

Examples

The following command specifies the parameters in the installation parameter CSV file C:\sample_install_SWDTLA.csv, and creates the response file C:\temp\swdtk_la_setup.iss:

```
dtkla_instparam.exe -infile C:\sample_install_SWDTLA.csv -outfile C:\temp\swdtk_la_setup.iss
```

A.2.3 Messages Output by the Parameter Setup Command

This section describes the messages that are output by the parameter setup command.

The environment-dependent constraints in the installation parameters are not checked by this command. Therefore, even if an error is not output by this command, an error may still occur during installation.

System error.

Cause

A system error occurred.

Action

Contact Fujitsu technical support.

Argument error: Usage: dtkla_instparam -infile "input file path" -outfile "output file path".

Cause

The syntax of a required argument is incorrect.

Action

Check the syntax of the command.

Error: too long path specified(path must be less than 256 bytes).

Cause

The specified file path is too long.

Action

Specify the file path using up to 255 halfwidth characters.

Error: file not exist.

Cause

The specified file does not exist.

Action

Ensure that the specified file path is correct.

Error: failed to open file.

Cause

The file could not be opened.

Action

Ensure that the file is not in use, or is not corrupted.

Error: failed to parse csv file.

Cause

Failed to process the CSV file.

Action

Ensure that the CSV file format is correct.

Error: failed to encrypt password.

Cause

Failed to encrypt the password.

Action

Ensure that the specified format of the password is correct.

Error: can't find out parameter from input file.

Cause

The file specified in -infile does not contain any parameters.

Action

Check the contents of the file specified in -infile.

Error. DtkLaInstPath is invalid.

Cause

The specified content of DtkLaInstPath in the input file is invalid.

Action

Check the content specified in the parameters.

Error. DtkLaDBInstPath is invalid.

Cause

The specified content of DtkLaDBInstPath in the input file is invalid.

Action

Check the content specified in the parameters.

Error. DtkLaPort01/DtkLaPort02/DtkLaPort03 is invalid.

Cause

The specified content of DtkLaPort01/DtkLaPort02/DtkLaPort03 in the input file is invalid.

Action

Check the content specified in the parameters.

Error. DtkLaUserID is invalid.

Cause

The specified content of DtkLaUserID in the input file is invalid.

Action

Check the content specified in the parameters.

Error. DtkLaUserPW is invalid.

Cause

The specified content of DtkLaUserPW in the input file is invalid.

Action

Check the content specified in the parameters.

Success: complete to edit Installation file.

Description

Successfully edited the installation parameter file.

A.2.4 Silent Installation Script

This section explains the script used for silent installation.

Script name

dvdRom:\citool\LA\silentsetup.vbs

Syntax

Execute using cscript, with the response file as the argument.

```
cscript silentsetup.vbs responseFile
```

Options

Option	Description
responseFile (required)	Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters. If the path includes spaces, enclose it in double quotation marks. Do not specify Unicode characters.

Note

Because it is necessary to specify the password during silent installation of the Log Analyzer Server, a default response file has not been prepared. The user must create one before executing this script.

Return values

If the return value is 0:

Ended normally.

If the return value is other than 0:

Ended abnormally.

Refer to the error message output to the console and take appropriate action.

Examples

The following command performs silent installation using the response file C:\temp\swdtk_la_setup.iss:

```
cscript silentsetup.vbs C:\temp\swdtk_la_setup.iss
```

Privilege required for execution/execution environment

- Administrator privileges for the target installation environment are required.

- To use this command in Windows Server(R) 2008 or Windows Server(R) 2012, display the desktop and execute this command on a **Command Prompt** window that has been started by selecting **Run as Administrator**.

A.2.5 Messages Output by the Silent Installation Script

This section explains the messages output by the silent installation script.

This program must be executed by account of Administrators.

Cause

Administrator privileges are required.

Action

Execute as a user with Administrator privileges.

Installation is failed.ErrorCode:XX

Cause

Silent installation failed.

Action

Check the installation environment and the following log file:

%WINDIR%\dtlasvinst_message.log

A.3 Silent Installation of the Smart Device Relay Server

This section describes files, commands, and messages used in silent installation of the Systemwalker Desktop Keeper Smart Device Relay Server.

A.3.1 Installation Parameter CSV File

Specify the installation parameters in a CSV file using the format described in this section.

Character encoding

UTF8

Format

```
installInfo,softwareName,softwareName
installInfo,OS,os
installInfo,Version,version
installInfo,Name,softwareId
parameters,paramKey,paramValue
parameters,...,...
```

📑 **Note**
....

- Do not change any installInfo parameter from the sample content.

- Specify one or more parameters in the parameters parameter.

- If double quotation marks are used to enclose data, then all fields within the same record must be enclosed in double quotation marks.

- Do not specify spaces in the first column or in the second column.

- Spaces cannot be specified before or after fields enclosed in double quotation marks.

....

parameters parameter

The parameters are described below.

No.	Parameter	Parameter information		Description
1	Smart Device Relay Server installation directory	**Key**	DtkSdInstPath	Specify the installation directory for the Smart Device Relay Server.
		Data type	String	Specify up to 100 halfwidth alphanumeric characters and symbols, excluding characters that cannot be specified in Windows and the following symbols: , ; #
		Value can be changed	Y	
		Default value	C:\Program Files (x86)\Fujitsu \Systemwalker Desktop Keeper\SDSV	If installing on a 32-bit operating system, change to: C:\Program Files\Fujitsu\Systemwalker Desktop Keeper\SDSV Required

Information

....

A sample installation parameter CSV file is stored in the following folder of the product media (DVD-ROM).

dvdRom:\citool\SD\sample_install_SWDTKSD.csv

....

A.3.2 Parameter Setup Command

If customizing parameters, create a response file in which the parameters were changed using the parameter setup command, and use this file for silent installation.

Command name

dvdRom:\citool\SD\dtksd_instparam.exe

Syntax

```
dtksd_instparam.exe -infile installParmCsvFile -outfile responseFile
```

Options

Option	Description
-infile	Specify the installation parameter CSV file. Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters. If the path includes spaces, enclose it in double quotation marks.
-outfile	Specify the response file to be output. Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters. If the path includes spaces, enclose it in double quotation marks. If the file already exists in the output destination, it will be overwritten.

Return values

If the return value is 0:

Ended normally.

If the return value is other than 0:

Ended abnormally.

Refer to the error message output to the console and take appropriate action.

Examples

The following command specifies the parameters in the installation parameter CSV file C:\sample_install_SWDTKSD.csv, and creates the response file C:\temp\swdtk_sd_setup.iss:

```
dtksd_instparam.exe -infile C:\sample_install_SWDTKSD.csv -outfile C:\temp\swdtk_sd_setup.iss
```

A.3.3 Messages Output by the Parameter Setup Command

This section describes the messages that are output by the parameter setup command.

The environment-dependent constraints in the installation parameters are not checked by this command. Therefore, even if an error is not output by this command, an error may still occur during installation.

System error.

Cause

A system error occurred.

Action

Contact Fujitsu technical support.

Argument error: Usage: dtksd_instparam -infile "input file path" -outfile "output file path".

Cause

The syntax of a required argument is incorrect.

Action

Check the syntax of the command.

Error: too long path specified(path must be less than 256 bytes).

Cause

The specified file path is too long.

Action

Specify the file path using up to 255 halfwidth characters.

Error: file not exist.

Cause

The specified file does not exist.

Action

Ensure that the specified file path is correct.

Error: failed to open file.

Cause

The file could not be opened.

Action

Ensure that the file is not in use, or is not corrupted.

Error: failed to parse csv file.

Cause

Failed to process the CSV file.

Action

Ensure that the CSV file format is correct.

Error: can't find out parameter from input file.

Cause

The file specified in -infile does not contain any parameters.

Action

Check the contents of the file specified in -infile.

Error. DtkSdInstPath is invalid.

Cause

The specified content of DtkSdDBInstPath in the input file is invalid.

Action

Check the content specified in the parameters.

Success: complete to edit Installation file.

Description

Successfully edited the installation parameter file.

A.3.4　Silent Installation Script

This section explains the script used for silent installation.

Script name

dvdRom:\citool\SD\silentsetup.vbs

Syntax

Execute using cscript, with the response file as the argument.

```
cscript silentsetup.vbs [responseFile]
```

Options

Option	Description
responseFile (optional)	Specify this option if you want to change the parameters to be used during setup from their default values. Specify the full path using up to 255 halfwidth characters or 127 fullwidth characters. If the path includes spaces, enclose it in double quotation marks.

Option	Description
	Do not specify Unicode characters.
	If omitted, the default values will be used for all parameters.

Return values

If the return value is 0:

Ended normally.

If the return value is other than 0:

Ended abnormally.

Refer to the error message output to the console and take appropriate action.

Examples

The following command performs silent installation using the response file C:\temp\swdtk_sd_setup.iss:

```
cscript silentsetup.vbs c:\temp\swdtk_sd_setup.iss
```

Privilege required for execution/execution environment

- Administrator privileges for the target installation environment are required.

- To use this command in Windows Server(R) 2008 or Windows Server(R) 2012, display the desktop and execute this command on a **Command Prompt** window that has been started by selecting **Run as Administrator**.

A.3.5 Messages Output by the Silent Installation Script

This section explains the messages output by the silent installation script.

This program must be executed by account of Administrators.

Cause

Administrator privileges are required.

Action

Execute as a user with Administrator privileges.

Installation is failed.ErrorCode:XX

Cause

Silent installation failed.

Action

Check the installation environment and the following log file:

%WINDIR%\dtksdsvinst_message.log