FUJITSU

FUJITSU Software
Systemwalker Desktop Keeper

User's Guide

Windows

B1WD-3252-08ENZ0(00)
March 2018

Preface

Purpose of This Guide

This guide describes the introduction and function overview of the following product, as well as the knowledge necessary to use the product.

- Systemwalker Desktop Keeper V15.2.0

Systemwalker is a general term for operation management products for distributed systems provided by Fujitsu Limited.

Intended Readers

This manual is intended for readers who construct/apply information protection system using Systemwalker Desktop Keeper.

In addition, this manual assumes readers have the following knowledge.

- General knowledge of PCs
- General knowledge of Microsoft Windows
- General knowledge of the Internet
- General knowledge of Microsoft SQL Server (when updating from V12)
- General knowledge of VMware View (when installing client (CT) in the VMware View environment)
- General knowledge of Citrix XenDesktop (when installing client (CT) in the Citrix XenDesktop environment)
- General knowledge of Google Android (when installing a smart device (agent) (Android))
- General knowledge of iOS (when installing a smart device (agent) (iOS))

Structure of This Guide

The structure of this guide is as follows:

Chapter 1 Overview of Systemwalker Desktop Keeper

This chapter describes the positioning of the Systemwalker Desktop Keeper in the Systemwalker product system, the effect of installation of Systemwalker Desktop Keeper and its features.

In addition, this chapter also describes the knowledge required when using Systemwalker Desktop Keeper.

Chapter 2 Functions of Systemwalker Desktop Keeper

This chapter describes the functions of Systemwalker Desktop Keeper.

Chapter 3 Operating Environment

This chapter describes the operating environment of Systemwalker Desktop Keeper.

Chapter 4 Link with Other Products

This chapter describes the applications that can be implemented by combining Systemwalker Desktop Keeper with other products.

Location of This Guide

The location of this guide in Systemwalker Desktop Keeper manuals is shown below.

Manual Name	Content
Release Information	This guide describes the additional functions and incompatibility information of Systemwalker Desktop Keeper.
User's Guide (This Manual)	This manual describes the summary and operating environment of Systemwalker Desktop Keeper.

Manual Name	Content
Installation Guide	This guide describes the installation settings, as well as maintenance and management measures of Systemwalker Desktop Keeper.
User's Guide for Administrator	This guide describes how to use Systemwalker Desktop Keeper.
User's Guide for Client (*1)	This guide describes the function summary and operation methods of Export Utility of Systemwalker Desktop Keeper.
Reference Manual	This manual describes the commands, files, messages and port numbers used in Systemwalker Desktop Keeper.
Centralized Management Guide	This guide explains how to centrally manage Systemwalker Desktop Keeper deployed at sites within and outside Japan.
Troubleshooting Guide	This guide describes the causes and processing methods for assumed exceptions in Systemwalker Desktop Keeper.

*1: "User's Guide for Clients" can also be viewed from the "Help" menu of the Systemwalker Desktop Keeper Export Utility.

Notations

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

Symbols Used in Commands

This subsection describes the symbols used in examples of commands.
Meaning of Symbol

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 selected.

Abbreviations

The manual uses abbreviations of the following products.

Product Name	Abbreviation
Systemwalker Desktop Keeper Base Edition V12.0L10	BEV12.0L10
Systemwalker Desktop Keeper Base Edition V12.0L20	BEV12.0L20
Systemwalker Desktop Keeper Base Edition V13.0.0	BEV13.0.0
Systemwalker Desktop Keeper Base Edition V13.2.0	BEV13.2.0
Systemwalker Desktop Keeper Base Edition V13.3.0	BEV13.3.0
Systemwalker Desktop Keeper Standard Edition V12.0L20	SEV12.0L20
Systemwalker Desktop Keeper Standard Edition V13.0.0	SEV13.0.0
Systemwalker Desktop Keeper Standard Edition V13.2.0 Systemwalker Desktop Keeper Standard Edition V13.2.1	SEV13.2.0
Systemwalker Desktop Keeper Standard Edition V13.3.0	SEV13.3.0
Systemwalker Desktop Keeper V14g (14.0.0)	V14.0.0
Systemwalker Desktop Keeper V14g (14.0.1)	V14.0.1
Systemwalker Desktop Keeper V14g (14.1.0)	V14.1.0
Systemwalker Desktop Keeper V14g (14.2.0)	V14.2.0
Systemwalker Desktop Keeper V14g (14.3.0) Systemwalker Desktop Keeper V14g (14.3.1)	V14.3.0

Product Name	Abbreviation
Systemwalker Desktop Keeper V15.0.0 Systemwalker Desktop Keeper V15.0.1	V15.0.0
Systemwalker Desktop Keeper V15.1.0 Systemwalker Desktop Keeper V15.1.1 Systemwalker Desktop Keeper V15.1.2 Systemwalker Desktop Keeper V15.1.3	V15.1.0
Systemwalker Desktop Keeper V15.2.0	V15.2.0
Windows(R) Internet Explorer(R) 9 Windows(R) Internet Explorer(R) 10 Windows(R) Internet Explorer(R) 11	Internet Explorer

The manual uses abbreviations of the following operation systems.

Operation System Name	Abbreviation
Microsoft(R) Windows Server(R) 2016 Datacenter Microsoft(R) Windows Server(R) 2016 Standard Microsoft(R) Windows Server(R) 2016 Essentials	Windows Server 2016
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 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 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 2008 (*1)
Windows(R) 10 Home Windows(R) 10 Pro Windows(R) 10 Enterprise Windows(R) 10 Education	Windows 10 (*1)
Windows(R) 8.1 Enterprise Windows(R) 8.1 Pro Windows(R) 8.1	Windows 8.1(*1)
Windows(R) 7 Ultimate Windows(R) 7 Enterprise Windows(R) 7 Professional Windows(R) 7 Home Premium	Windows 7 (*1)
Microsoft(R) Windows Server(R) 2016 Datacenter Microsoft(R) Windows Server(R) 2016 Standard Microsoft(R) Windows Server(R) 2016 Essentials	Windows

Operation System Name	Abbreviation
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 Windows(R) 7 Ultimate Windows(R) 7 Enterprise Windows(R) 7 Professional Windows(R) 7 Home Premium 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	
Android(TM) 4.4 to Android(TM) 8.0	Android
iOS 6.0 to iOS 11	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 2008 64-bit Edition
- Windows Server 2008 R2
- Windows 7 64-bit Edition
- Windows 8.1 64-bit Edition
- Windows 10 64-bit Edition

Export Restriction

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 recorded in this manual but cannot be used.

(These functions can be used in the Japanese version, but are not available in Global version.)

- 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 "Fullwidth" with multi-byte character.
- For number of characters that can be used, multi-byte characters such as fullwidth 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 V13.3.0
- Systemwalker Desktop Keeper Standard Edition V13.2.1
- Systemwalker Desktop Keeper Standard Edition V13.3.0
- Systemwalker Desktop Keeper V14g (14.0.0)
- Systemwalker Desktop Keeper V14g (14.0.1)
- Systemwalker Desktop Keeper V14g (14.1.0)
- 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

March 2018

Revision History
July 2015, First Edition November 2015, Second Edition July 2016, Third Edition February 2017, Fourth Edition March 2018, Fifth Edition

Contents

Chapter 1 Overview of Systemwalker Desktop Keeper

This chapter provides an overview of the Systemwalker Desktop Keeper.

1.1 Product Positioning

Concept of the Systemwalker Desktop Series

The Systemwalker Desktop series is a group of products that knows assets and implements green IT policies, as well as security policies such as installing security patches, limiting PC operations, collecting/analyzing logs, limiting file operations and isolating illegal PCs, etc., according to the risks of business content and the environment.

Positioning of the Systemwalker Desktop Keeper

Systemwalker Desktop Keeper is the internal information protection software that "records" or "prohibits" client operation with risks of information disclosure based on security policies.

It "prohibits" disclosure of confidential information that results from copying and printing of files inside a company. Though the "prohibition" function can prevent disclosure of information, it enables you to know the disclosure process by searching or tracing the "recorded" logs once the sending information is disclosed.

It can even analyze the trend of client operations through PC operation logs and file operation logs inside a company. At present, for the problem like "no policy can be set without seeing the actual situation", the compliance situation of the system security policy and the vulnerability of information disclosure policy can be digitalized so that the actual situation can be known and the application can be improved.

In addition, by recording client operations, PC users can know the operations that cause disclosure of information and the "prohibition effect" of mentally preventing disclosure of information can be expected.

Systemwalker Desktop Keeper is applicable for systems from the section level with tens of computers to a large-scale system at the company level. The security settings and applications including customer security policies can be conducted.

1.2 System Structure

The following section describes the configuration components and system structure of Systemwalker Desktop Keeper.

Configuration Components

Systemwalker Desktop Keeper consists of the following components:

Management Server

This server saves the logs collected from the subordinate PCs and smart devices, sets the security policy of subordinate PCs and smart devices and distributes policy to each PC and smart device. The information of subordinate PCs, smart devices and logs can be viewed. The collected logs are managed in the unit of the management server.

In addition, the management console is also used to define the CT policy and user policy in the subordinate client (CT) of the management server. The CT policy is defined in the smart device (agent).When the defined policy is CT policy, the policy can be updated immediately or at the next time when the client (CT) starts and can be updated in the smart device periodically. When the defined policy is user policy, the policy can be updated at the next time when the user logs on Window system of the client (CT). Or, when logging on with the ID with defined user policy, the user policy and the CT policy can be updated simultaneously.

The policy types, setting methods and application scope of CT policy are different from those of user policy. Refer to "What is Policy" in the *User's Guide for Administrator* for details.

Master Management Server

When there are multiple management servers, a master management server should be set. When the master management server is connected with management console and log viewer, the policy defined in each management server can be viewed and modified, and the logs can also be viewed. In addition, the master management server has the same functions as the management server, and it is able to manage toe client (CT) and smart device (agent) directly.

Log Analyzer Server

This server analyzes the trend of operations according to logs of various operations such as file export, file operation and printing status of the client.

Management Console

The Management Console is used for many collection operations, which primarily include definition of the management server, definition of CT policy and user policy, distribution of policies to the client (CT) and smart device (agent), and definition of logs collected from client (CT) and smart device (agent). These operations are set in the GUI interface.

Web Console (Status window, Log Viewer and Log Analyzer)

This is a console for viewing the logs collected from the client (CT) and smart device (agent), and trend analysis results of a log.

The aggregation result for the number of PCs with risk of information disclosure in all systems is displayed in the status window.

The conditions such as date, log type and keywords can be specified in the log viewer window for searching. The search results can be displayed in the form of a list and output in CSV files (apart from additional information). The file operations can be traced from the specified logs.

The aggregation result can be displayed based on operations in the window of the log analyzer. The error operations can be displayed in ranking or the statistics with specified previous date can be performed.

Report Output Tool

This tool takes security risk status and compliance status as report materials to print or export as files. The administrator installs and uses the tool on the PC in which the report is created.

Client (CT)

This is a client module installed in the PC that is a managed object. It distributes security policy and saves all kinds of logs according to the set policy. It also prohibits operations that violates the policy.

Smart Device (Agent)

Android

This is an agent installed in the smart device to be managed.

Storage of each log and prohibition of operation violating the policy are performed in accordance with the preset policy. Mandatory lock and wipe through remote control is enabled.

iOS

This is a profile installed in the smart device to be managed.

Operations are prohibited in accordance with the preset policy. Mandatory lock and wipe through remote control is enabled.

Relay Server

It is a Relay Server placed between the smart device (agent) and (master) management server. It is placed when the smart device (agent) is to be managed. To connect a client (CT) via the Internet, a Relay Server must exist between it and the Master Management Server.

In the case of Android device, the policy is updated from (master) management server to the smart device (agent) through the Relay Server, and logs are collected from smart device (agent) to the (master) management server through the Relay Server.

In the case of iOS device, profile is updated and controlled in the terminal by using Apple Push Notification Service (APNs).

System Structure

The operation management based on level composition can be implemented in Systemwalker Desktop Keeper.

For the large-scale model (the environment with many nodes of managed objects), it is suggested to construct a 3-level (Master Management Server - Management Server - Client) system structure. In case of small and medium scale (the environment with a few nodes of managed objects), a 2-level system structure (Management Server - Client) can also be constructed.

The system structure constructed by assembling the above-mentioned configuration components varies depending on the function used and the system scale. Please refer to "Determine System Structure" of *Installation Guide* for the setting standard of the server.

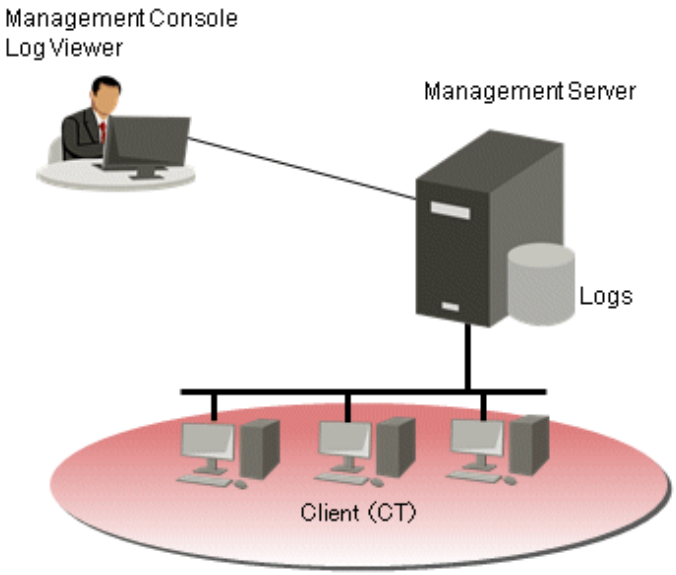
Here, the following six modes are described as examples of system structure:

- 2-Level System Structure

- 3-Level System Structure
- 3-Level System Structure (with Virtual Environment)
- 3-Level System Structure (with Log Analysis/Report Output)
- Management System Structure of Clients (CT) that Connect via the Internet
- Smart Device Management System Structure

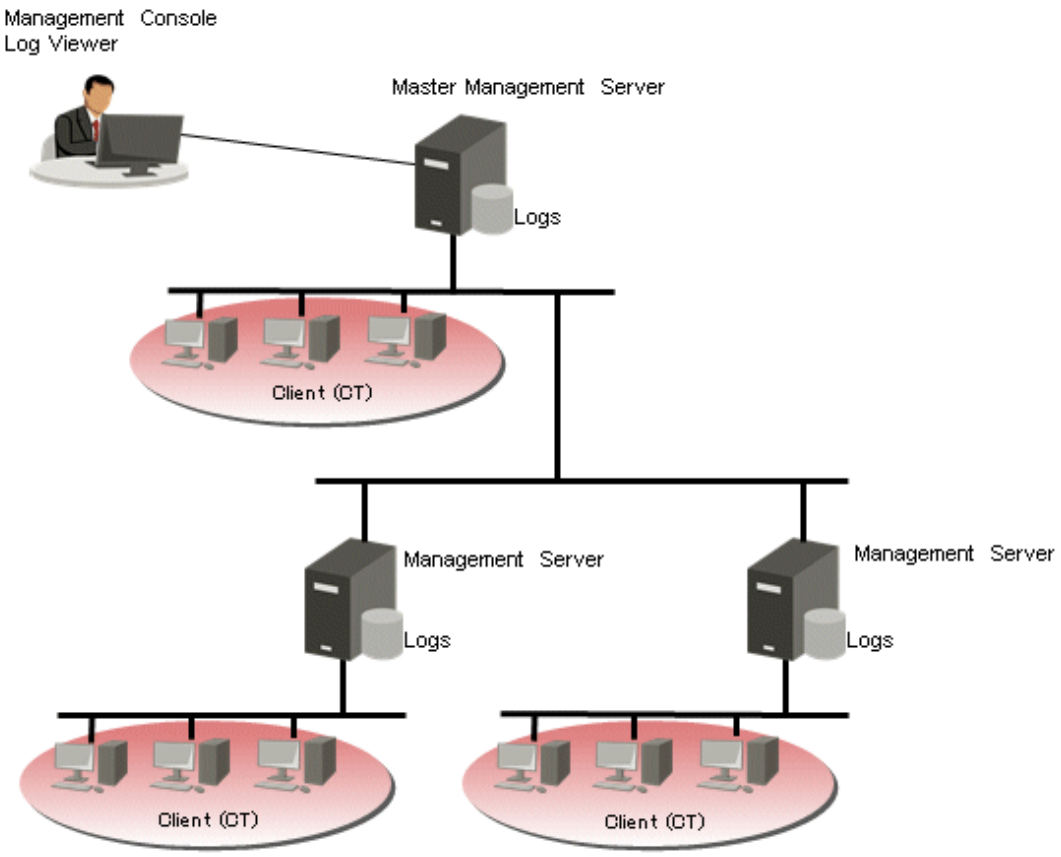
2-Level System Structure

This is a structure in which one management server is set and multiple subordinate clients (CTs) are configured.



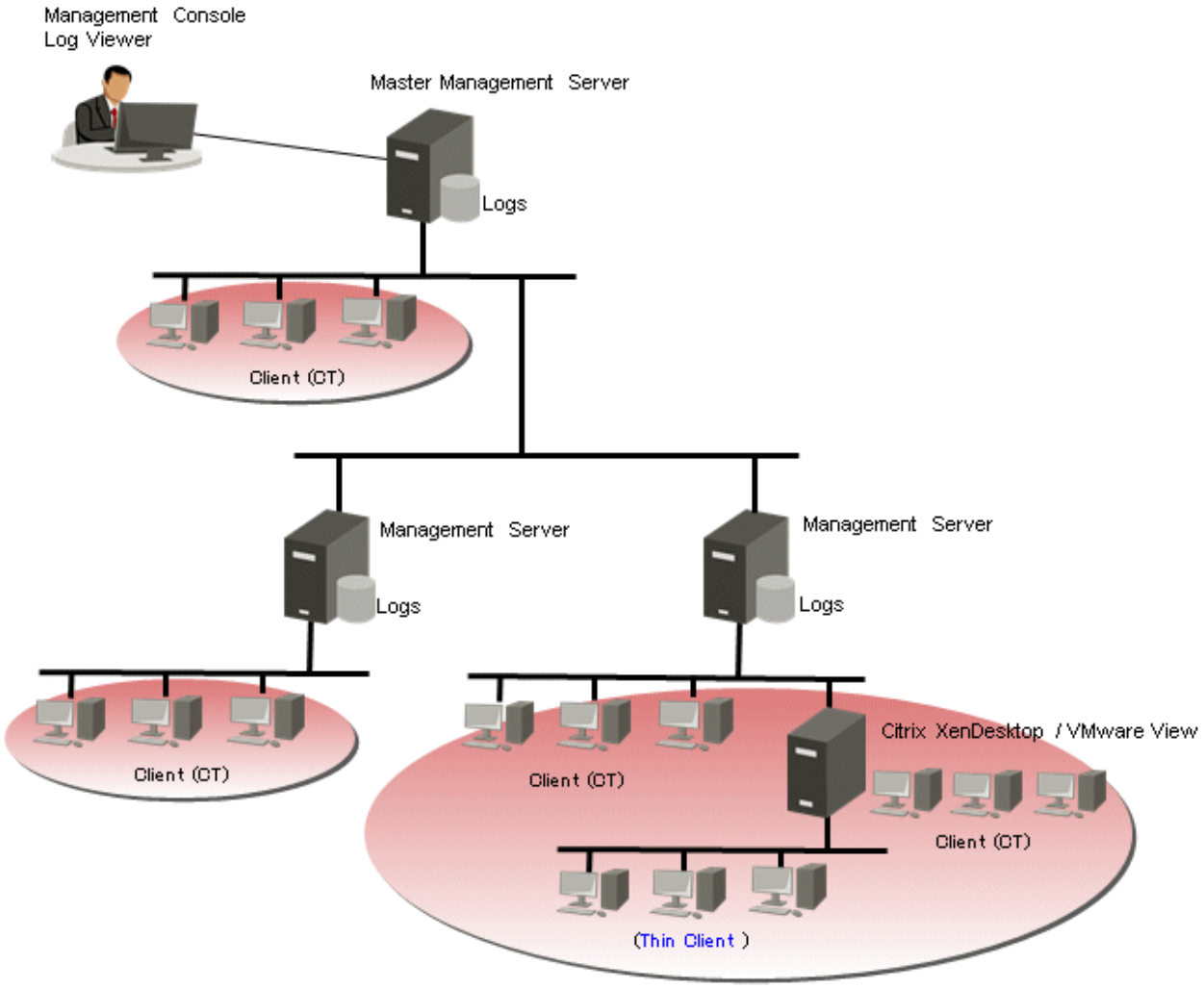
3-Level System Structure

This is a structure in which the master management server is set for managing multiple management servers.



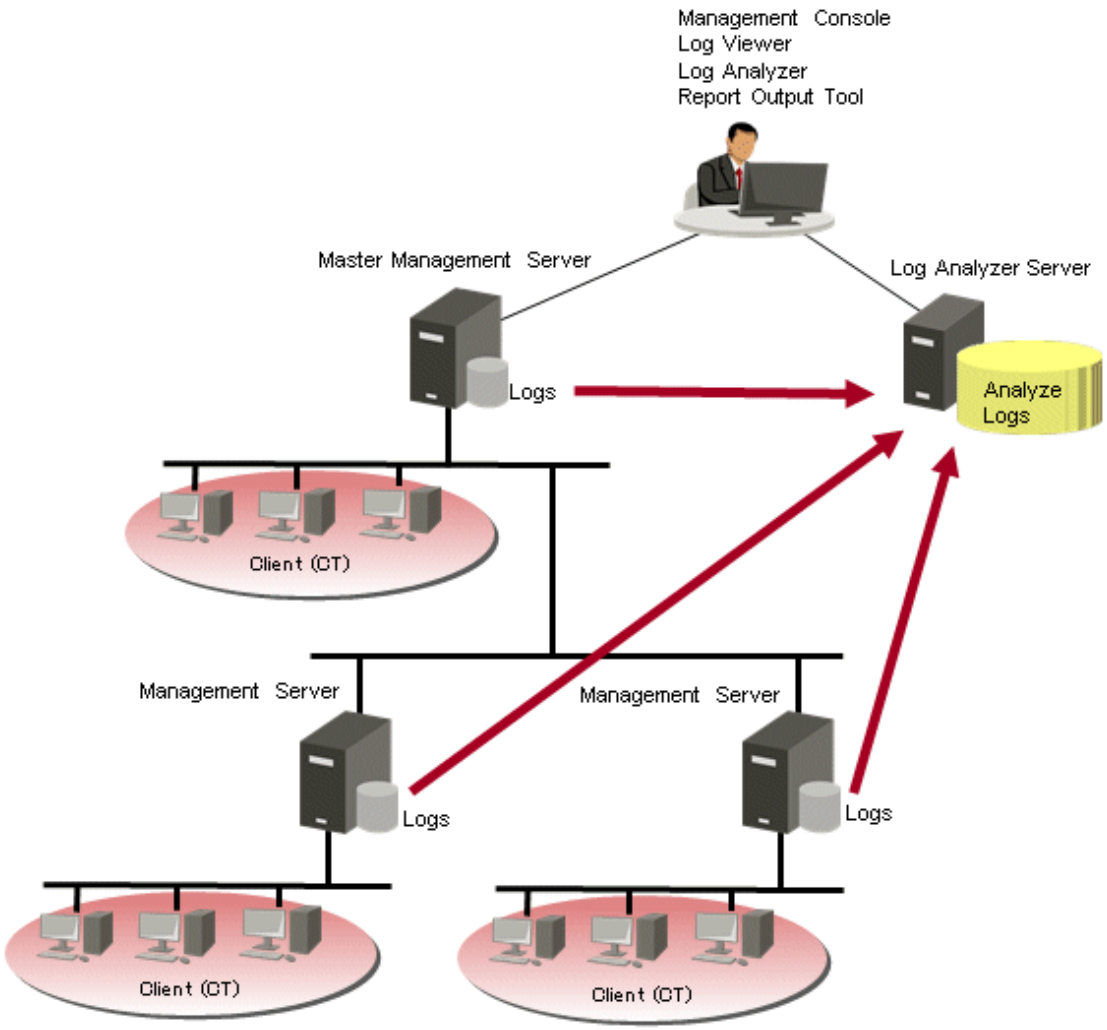
3-Level System Structure (with Virtual Environment)

This is a structure in which the master management server is set for managing multiple management servers and the client (CT) is installed to the Citrix XenDesktop and VMware View environment.



3-Level System Structure (with Log Analysis/Report Output)

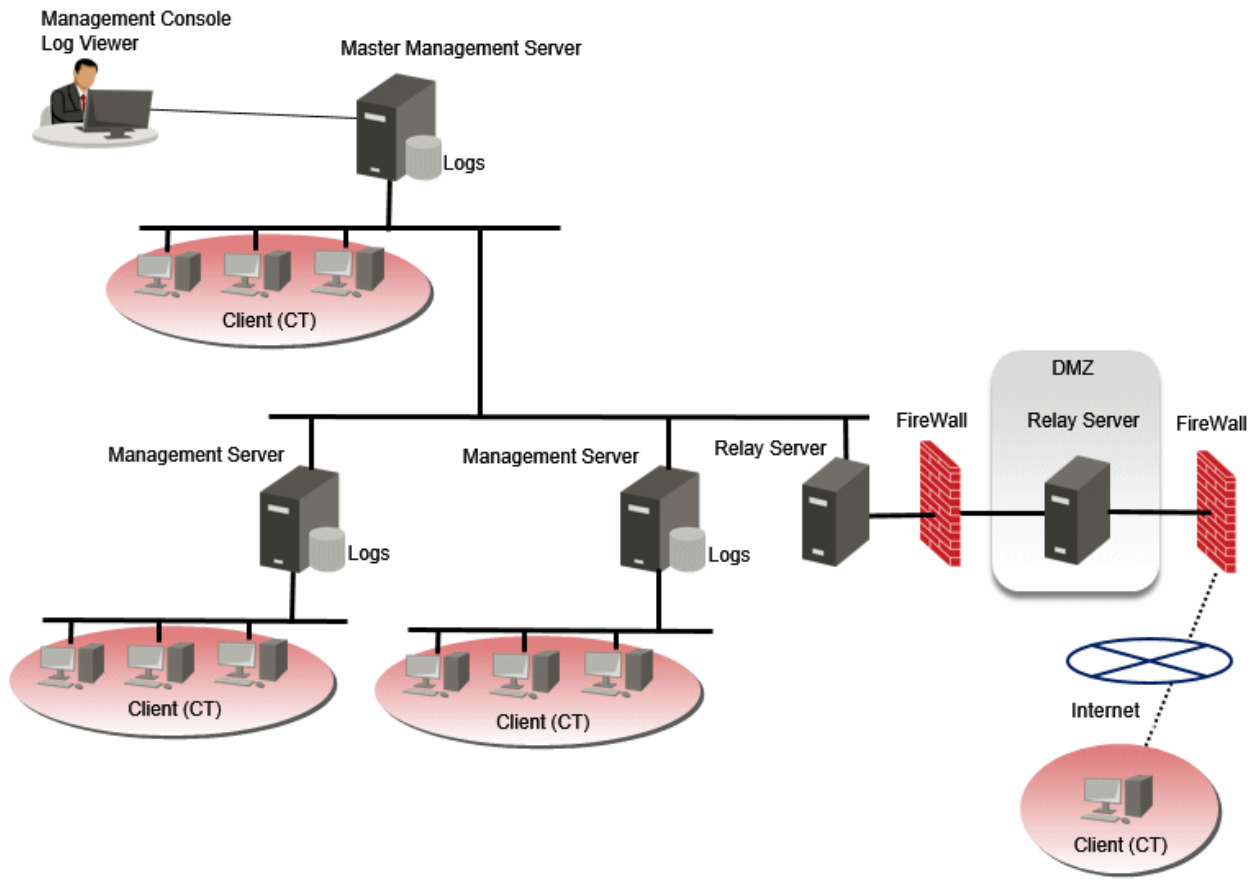
This is a structure in which the master management server is set for managing multiple management servers and log analysis and report output is performed.



Management System Structure of Clients (CT) that Connect via the Internet

This is a structure in which a Relay Server is installed to distribute policies to and collect logs from clients (CT) that connect via the Internet, for the purpose of managing those clients.

The Management Server is built inside the internal network. The Relay Server that will be directly connected to the Management Server is to be installed within the internal network. If connecting a client (CT) over the Internet, install one more Relay Server on the DMZ. Connect the client (CT) to the Relay Server on the DMZ, and connect the Relay Server installed on the DMZ to the Relay Server installed in the internal network. The recommended structure is as follows:



Smart Device Management System Structure

It is a structure in which the Relay Server is installed, a log is collected from smart device through this server, and policies are distributed for smart device through the Relay Server for the purpose of managing the smart devices.

PC is directly connected to the Management Sever as before. The smart device (which is connected to in-house access point) is separately configured to the Relay Server and is connected to that Relay Server. The Management Server and Relay Sever are configured to the in-house network.

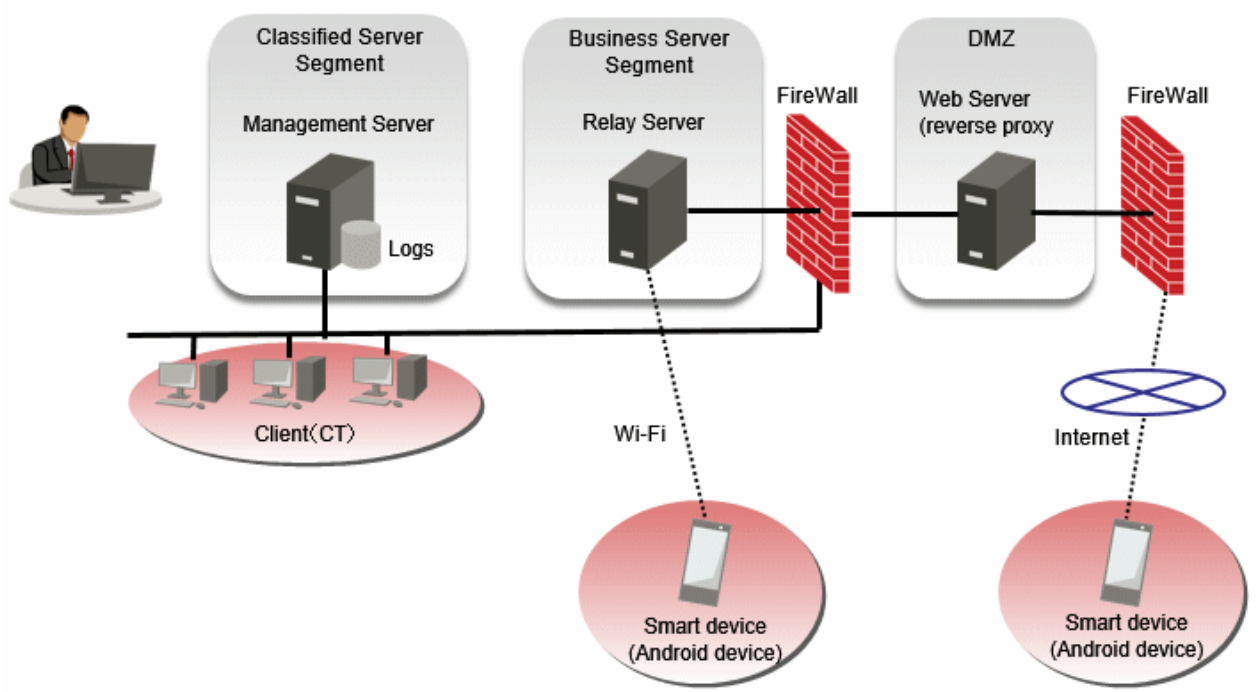
For smart devices on the Internet, please install and operate the reverse proxy in the DMZ.

The recommended structure is as follows:

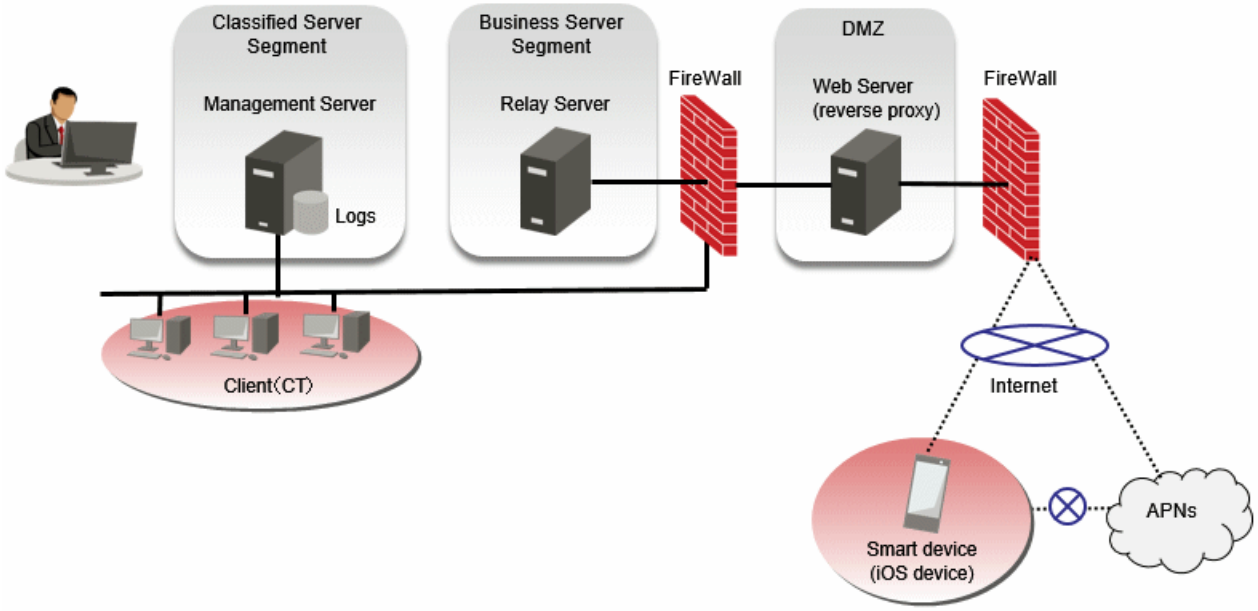
- Operation pattern of smart device

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

Smart Device (Android Device)



Smart Device (iOS Device)



Note

When managing iOS devices, it is necessary to have an environment in which Relay Server and smart devices can connect to the APNs(Apple Push Notification Service). The iOS devices cannot be managed only in an intranet environment. About environment settings to connect APNs, refer to the latest information disclosed by Apple Inc.

Setting up the following policies can be efficient while allowing export of smart devices outside the company:

- Only in-house access point and reliable access points can be connected due to Wi-Fi access prohibition.
- Prohibit the application usage and restrict the use of cloud-based tools.

- Prohibit the application usage and prohibit the use of non-standard browsers.
- Collect the Web access log, and monitor the connection to the cloud storage and cloud-based services outside the company.

With the above policies, Internet can be used on the devices by only connecting to the reliable access points outside the company. With web access being monitored, HP view which is not related to the business can also be monitored.

Point

It is recommended to setup a reverse proxy server to manage the smart device through the Internet.

Chapter 2 Functions of Systemwalker Desktop Keeper

This chapter describes the functions of Systemwalker Desktop Keeper. Systemwalker Desktop Keeper provides the following functions:

- Prohibition function
- Record function
- Management function
- Log analysis function
- Report output function

In addition, for details on settings, operations and notes of these functions, refer to the *User's Guide for Administrator*.

2.1 Prohibition Function

The agent software of Systemwalker Desktop Keeper installed on PCs and smart devices can forcibly prohibit the operations. Operations in the client (CT) can be prohibited and recorded as a prohibition log when the prohibited operation is being executed (excluding file export prohibition).

Prohibition settings can be performed through the management console.

The following section gives an overview of the prohibition function.

Prohibition Function of Smart Device (Android Device)

The following operations are prohibited with Android device. The prohibition log is recorded if the prohibited operations are performed.

- Wi-Fi connectivity
- Bluetooth connectivity
- Application usage

Prohibition Function of Smart Device (iOS Device)

The following operations are prohibited in iOS device. The prohibition log, however, is not recorded even if the prohibited operations are performed.

- Device function usage
- Application usage
- iCloud usage
- Security and privacy settings
- Content rating settings

Application Startup Prohibition

This sets the name of the application startup being prohibited and disables the startup of unnecessary applications. The prohibition operation will be recorded as a prohibition log.

Printing Prohibition

This sets which applications are allowed to print and disables prohibited applications from printing. When the prohibited operation is performed, a prohibition log will be recorded. In addition, this function monitors the printing of each user. When the total number of printed pages exceeds a specified number of pages, following attempts to print will be disabled and will yield warnings.

PrintScreen Key Prohibition

This prohibits the collection of hard copies with the PrintScreen key. When the prohibited operation is being performed, a prohibition log will be recorded.

Logon Prohibition

This function is available only against Microsoft accounts.

This sets the group that prohibits logon and prohibits the logon for the user belonging to the corresponding group. When the prohibited operation is being performed, a prohibition log will be recorded.

File Export Prohibition

Encryption Function is not available.

This sets a drive that prohibits export or reading of files. It also prohibits the export of files to the corresponding drive, or reading of files from the corresponding drive. Even if the prohibited operation is being performed, however, a prohibition log will not be recorded.

It also sets prohibition on reading of portable devices/imaging devices.

URL Access Prohibition

This prohibits the access to URLs apart from the permitted ones. When the prohibited operation is being performed, the tab being accessed will be closed or Internet Explorer will be terminated by force and a prohibition log will be recorded.

FTP Server Connection Prohibition

This prohibits connection to FTP servers apart from the permitted ones. When the prohibited operation is being performed, the FTP server connection will be terminated by force and a prohibition log will be recorded.

Web Upload/Download Prohibition

This prohibits the upload and download operations for websites apart from the permitted ones. When the prohibited operation is being performed, the upload and download operations will become invalid and a prohibition log will be recorded.

Clipboard Operation Prohibition

This prohibits the use of the clipboard for copying between the virtual environment and the physical environment. When the prohibited operation is being performed, the clipboard will become invalid and a prohibition log will be recorded.

Device Prohibition

This prohibits devices that use the following connection methods in Windows:

- Bluetooth
- Infrared ray
- Wi-Fi
- PC card
- PCI ExpressCard
- IEEE1394
- Serial port/parallel port

Emergency Procedure for Client (CT)

This enables an emergency procedure (such as disabling the network, applying the emergency procedure settings policy, or notifying the security risk) to be performed for client (CT) when a security risk arises.

2.2 Record Function

The agent software of Systemwalker Desktop Keeper installed on PCs and smart devices can collect the operations as logs and record those logs to the Master Management Server and Management Server. The logs to be collected can be set through the management console.

The log collection function, however, is not available in the smart device (agent) (iOS).

The following section gives an overview of the record function.

Record Client (CT)

As operations on the client (CT), the following information can be collected as logs and files:

- Start/Stop applications
- E-mail sending
- E-mail receiving
- Printing
- Logon/Logoff/PC startup/PC shutdown/PC pause/PC restoration/PC connection/PC disconnection
- File/Folder operation (local drive/network drive)
- Window title
- PrintScreen key operation
- URL (Uniform Resource Locator) information
- FTP operation (upload, download)
- Web operation (upload, download)
- Clipboard operation
- Attached data (screen capture, original file, E-mail content)
- Changes to the environment

Record Smart Device (Android Device)

As operations on the Android device, the following information can be collected as logs and files:

- Web Access Log
- SD Card Mount/Unmount Log
- SIM Card Mount/Unmount Log
- Wi-Fi Connection Log
- Bluetooth Connection Log
- Phone Incoming/Outgoing Call Log
- Application Usage Log
- Application Configuration Change Log

Record Device Configuration Change

When drive letters are added while installing the network or USB memory, such information can be recorded.

Record the Use of External Device

The name of the file copied to external storage media using the file export utility can be recorded.

Attached Data

- Screen Capture

  When the collected window title log satisfies the specified condition, the screen of that moment will be recorded as a hard copy. In addition, in cases of the PrintScreen key operation and PrintScreen key prohibition, the target window will be recorded as a hard copy.

- Original File

  During file exporting by export utility, the exported file is copied and its original copy is recorded.

- Text and File Attachment of E-mail

  When an E-mail has been sent, the text of the E-mail and the content of all file attachments are recorded.

  When an email is received, the text of the email is recorded.

- Clipboard Data

  When information is copied from the virtual environment to the physical environment or from the physical environment to the virtual environment via clipboard, the clipboard data is recorded as the original copy.

Log Filter

The filtering condition for window title log and file operation log can be set. As a result, unnecessary logs will not be recorded, so that the total volume of logs can be reduced and log search will become easier.

2.3 Management Function

The system administrator of Systemwalker Desktop Keeper uses the following functions to manage the system:

- Policy settings
- CT policy settings
- Search/View the collected logs
- Notifying the administrator when illegal operations occur in the client (CT)
- Backup/Restore the database that stores the collected logs
- Status display
- Process control and service control of the client (CT)
- Remote control of smart device (agent)

Define Policy

This refers to the defining of CT policy, user policy, and emergency procedure settings policy on the Management Console, and the defining of operations to be prohibited on the client (CT) and logs to be collected from the client (CT).

The policies that can be defined include the following three types:

- CT Policy

  This is the policy that is set for the client (CT) or the smart device on which agent is installed.

- User Policy

  This is the policy set for the user name that is entered during logon to the Windows system installed with the client (CT).

- Emergency procedure settings policy
  This is the policy temporarily set for the client (CT) when security risks arise.

In addition, by setting the department administrators, the authority for managing their own department can be granted.

The types, setting methods and application scope are different for the CT policy, user policy, and emergency procedure settings policy. Refer to "What is Policy" in the *User's Guide for Administrator* for details.

View, Search and Trace Logs

The search conditions such as date, log type and keywords can be specified in the Web console (Log Viewer). The search result can be displayed in the form of a list or output in a CSV file.

In addition, by setting the department administrators, the authority for managing their own department can be granted.

Also, file operation can be traced through specified logs. The types of log that can be traced are shown as follows:

- File operation log
- File export log

- E-mail sending log (with file attachment)
- E-mail receiving log (with file attachment)
- E-mail sending suspension log (with file attachment)
- E-mail attachment prohibition log
- FTP operation log (FTP upload log and FTP download log)
- Web operation log (Web upload log and Web download log)

By restoring backup operation logs to the database for viewing, the previous operation logs can be viewed. While viewing the database, logs can be searched and viewed for each user. Also, the department administrator can use this function.

Self Version Management

When the product version of the client (CT) is determined as the old version, it will be upgraded automatically. To use the self version management function, the self version management module must be configured in the management server by the system administrator of Systemwalker Desktop Keeper.

Level Management

When there are multiple servers that manage the client (CT), the master management server can be set for server management by levels.

E-mail Notification

When an operation which violates the policy that occurs in the client (CT), the violation log will be collected and an E-mail notification will be sent to the administrator.

In cases such as when emergency procedure requests and emergency procedure cancellations are made to the client, or when the database space and disk space of the management server/master management server are not enough, E-mail notifications will also be sent to the administrator.

Record to Event Log

When an operation which violates the policy that occurs in the client (CT), after the violation logs have been collected, they are recorded to the event log of the master management server or management server connected to this client (CT).
Also, even in cases such as when emergency procedure requests and emergency procedure cancellations are made to the client, or when the database space or disk space of the Management Server/Master Management Server is depleted, such events are recorded to the event log.

Status display

The number of PCs with a risk of information disclosure in all systems can be aggregated and confirmed.

Process Control and Service Control of Client (CT)

The system administration can acquire a list of processes and services on the client (CT) to control illegal processes and services.

Remote Control of Smart Device (Agent)

The system administrator can control the operations to restrict the unauthorized use of the lost smart device of the user.

2.4 Log Analysis Function

The collected logs can be aggregated and analyzed.

Prevention and Diagnosis Function against Information Disclosure

The prevention and diagnosis function against information disclosure ensures that the logs collected on the previous day will be aggregated and the aggregation result of the following operation logs that occurred in all terminals during the previous week will be displayed. The tendency of operation that is likely to cause information disclosure can be digitalized and the risk tendency can be known.

- File export log

- File operation log
- Printing log
- E-mail sending log
- FTP operation (upload)
- Web operation (upload)

Function of counting by purpose

The logs can be aggregated after specifying the aggregation unit and aggregation time interval. The risk tendencies of all kinds of operations that are likely to cause information disclosure can be analyzed one by one according to the aggregation result.

- Know violation operation status

  The violation logs of Systemwalker Desktop Keeper can be aggregated to analyze the tendency of violation operations.

- Know file export status

  The file export logs of Systemwalker Desktop Keeper can be aggregated to analyze the tendency of external data export.

- Know file access status

  The file operation logs of Systemwalker Desktop Keeper can be aggregated to analyze the tendency of whether someone is using the important data.

- Know application operation status

  The application operation logs of Systemwalker Desktop Keeper can be aggregated to analyze the tendency of application operation.

- Know printing status

  The printing logs of Systemwalker Desktop Keeper can be aggregated to analyze the tendency of printing operation.

- Know Internet access status

  The URL of the Web accessed by the client can be aggregated and analyzed.

- Know information disclosure status

  The operations that are likely to cause information disclosure can be analyzed.

2.5 Report Output Function

This function outputs the diagnosis result of the security condition and compliance condition within an organization as a report.

The security administrator can learn the security condition from this function, which prints the aggregation and analysis result of logs into a report and outputs it as a file in the format of Microsoft Excel as material for reporting to the upper level of organization.

The system administrator can output reports of all managed objects and the department administrator can output the reports of their own department.

The types of reports are shown as follows:

Log Analysis Report

From the Log Analysis Report, the security administrator can know the security condition, and can print or output the security risk condition and compliance condition into files as report material to relieve the burden on the department administrator to create report materials.

Furthermore, resetting the security policy based on the analysis result helps apply the information protection policy more effectively. The following reports can be output:

- Information disclosure prevention and analysis report

  The results of counting and analyzing the logs of Systemwalker Desktop Keeper can be output according to the risk of information disclosure.

  The risk condition of information disclosure can be known and appropriate prevention measures against information disclosure, such as restricting PC operations by terminals and uses with high risk, can be taken.

- Terminal usage status analysis report

  The results of counting and analyzing the logs of Systemwalker Desktop Keeper can be output according to the situation of whether all terminals within the organization are used properly based on policies.

  The results can also help managers understand whether the business terminal being used correctly in the scope of the business.

- Violation status analysis report

  The results of counting and analyzing the prohibition operations of Systemwalker Desktop Keeper can be output. The PCs and users trying repeatedly to prohibit operations through executing policies can be detected to learn where violations are occurring.

- Comprehensive analysis report

  The comprehensive diagnosis results can be output from the 3 points mentioned above.

The department administrator can output the reports that are limited to their own department based on the report of all managed objects output by the system administrator.

Report for Green IT Policy

- Printed volume monitoring report

  By reporting the printed volume of each department or the entire organization, visualizing the reduction objective and actual performance and prohibiting unnecessary printing, contributions can be made for reducing CO2 emission.

Point

How to operate Report Output Tool

The report output tool can be used to count and analyze logs to know the compliance condition/security risk condition, reset security policies and apply the PDCA cycle for improving the security risk condition.

- Plan (Setting of screening condition)
  Set the screening condition for more accurate analysis according to the business condition within an organization, the authority of the client user, and the business content or risk condition.

- Do (Report output)
  Output the analysis report for knowing the security condition and compliance condition.

- Check (Confirmation of analysis result)
  Know the security risk condition within the organization from the report that has been output.

- Action (Improvement activities)
  Implement necessary investigation/warning for terminals and users with high risk and study the future policy. Modify the settings, such as the PC operation limit, in Systemwalker Desktop Keeper.

<Operation Procedure>

1. Setting of screening condition

   Set conditions (including keywords of file names) for determining whether an operation is dangerous in the screening conditions of the Web console (setting management window) according to the business content of the organization or user.

2. Report output

   Output analysis report using report output tool.

   The report of the analysis result based on the number of operations (number of dangerous operations) aggregated according to the screening conditions set in Step 1 is output. The log data that satisfy the settings can be output simultaneously.

3. Confirmation of analysis result

   The following analysis information is output in the report. According to the output results, the risk condition of the organization can be known.

   - Index value

     The condition within the target time interval (the last day in case of a daily report, the last week in case of a weekly report, and the last month in case of a monthly report) of reports is indicated as the risk coefficient.

- Ranking

  The ranking of groups and terminals with a deterioration of index value (with more dangerous operations) is displayed.

- Comment

  This displays the date and operation logs of concern to security administrators and the diagnosis based on whether the index value has been improved or not.

4. Improvement activities

   a. Detailed investigation of logs

      Investigate the corresponding logs in detail to confirm whether the tendency of a user's operation has any problems by focusing on the date and operation (which are determined as highly risky) indicated by the comments in the report.

      Make a warning if there is any problem.

   b. Warning for the ranking upper class group and terminal

      Perform hearing for the group and terminal with a significant number of dangerous operations. Confirm whether these operations are necessary for business. If there are too many operations that are unnecessary for business, warn the group and terminal to voluntarily restrict PC usage that is not for business.

   c. Reset screening condition

      According to the risk condition within the organization and compliance condition provided in Procedure 3, study again to see whether the keywords set in the screening conditions are not enough or whether unnecessary content exists, so as to bring about a more suitable business environment.

   d. Setting of exclusion conditions

      If the terminal has too many daily operations, the index value will be affected.

      If it is determined to be a reliable terminal/user and excluded from the aggregation objects of security administrators, it can be set as a terminal excluded from the statistics object of the operation class through the exclusion condition setting in the setting management of Web Console.

   e. Reset improvement activities

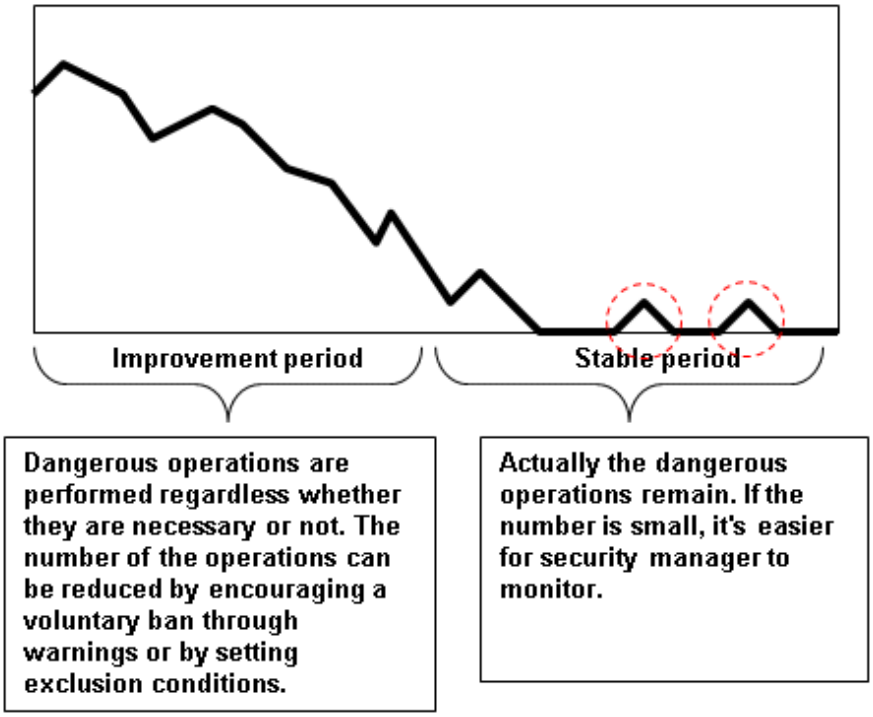
      The comments in the report show the trend of improvement and deterioration in the long term.

      If an improvement trend is shown, continue ongoing improvements. If a deterioration trend is shown, perform improvement activities.

      Change settings such as PC operation limit in Systemwalker Desktop Keeper for terminals/users with high risk.

      As index value refers to risk ratio (the rate between the number of violation operations and information disclosure operations), it is ideal to make it close to "0" as possible through improvement activities.

By continuing with the above PDCA cycle, the changes of index value output in the report are shown as follows:



- Improvement period

  This is a period in which there are many dangerous operations.

  By setting the screening conditions and exclusion conditions, the scope of monitored objects can be narrowed.
  In addition, through the warning of terminals/users with high risk, the frequency of requiring voluntary restriction on unnecessary operations is reduced.

- Stable period

  Keep the frequency at the lowest level required. Lower frequency helps security administrators with their monitoring. The security administrator monitors accidental dangerous operation (the dotted cycle part in the figure above).

Chapter 3 Operating Environment

This chapter describes the operating environment of Systemwalker Desktop Keeper.

3.1 Hardware

This section describes the required hardware environment of Systemwalker Desktop Keeper.

3.1.1 Hard Disk / Memory Requirements

Management Server/Master Management Server

- CPU

  Intel Xeon E5503 (2 GHz) or higher

- Memory (*1)

  At least 2 GB (excluding OS)

  The feature below requires additional memory.

  - Log viewing database

    0.5 GB or more

- HDD specifications

  SATA 7200 rpm in the case of RAID0

  SAS 15000 rpm in the case of RAID5

  However, RAID5 is not recommended as it lowers the update performance.

- Hard Disk Capacity (excluding OS) (*1)

  - Program Manual

    160 MB

  - Database system (added by Systemwalker Desktop Keeper)

    170 MB Database space

    For information on how to estimate capacity, refer to "3.1.2 Estimating Database Capacity".

  - Backup file space

    ```
    The entire log CSV file = average record length (byte) x the number of clients x backup time
    (days) x number of operation logs per day (piece/day) average record length: 500 bytes
    ```

  - Space for saving the Management Console

    For details on space for saving the Management Console, refer to "Management Console".

  - Space for saving the screen capture data (when using the screen capture function)

    For how to estimate the capacity needed for screen capture, refer to "Estimating the capacity of screen capture data"

  - Space for saving backup data of original files (when using the original file backup function)

    Refer to "Data capacity of backup original file" for details.

  - The disk capacity required for sending log data (when the Log Analyzer Server is used)

    For an estimation of the disk capacity required for necessary temporary workspace during the execution of log data transfer, refer to "Estimating temporary disk capacity required for sending log data".

  The available drive capacity of the following folders must be larger than 1% of the total drive capacity:

  - Folder for saving attached data

- Folder for command log
- Folder for collective log sending
- Destination folder for saving E-mail content
- Folder for trace log

*1: The requirement for memory and disk capacity may change according to system structure, scale and available resources.

Issues to be considered according to the capacity of installation drive of Management Server/Master Management Server

Specify a drive that can be guaranteed to have the following capacity to be the installation drive of Management Server/Master Management Server.

- Work space during data backup (used during operation only)

  A space of about 10 GB is required for processing 10 million records, so estimate the required space according to the number of records to be processed.

```
Number of records x 500 (average record length) x 2 (coefficient)
```

  For example, to back up a maximum of 10 million tables,

```
10 million x 500 bytes x 2 = about 10 GB
```

- Work space during data restoration (used during operation only)

  Space is the same as the size of the file to be restored.

Log Analyzer Server

- CPU

  Intel Xeon E5503 (2 GHz) or higher

- Memory (*1)

  At least 2 GB (excluding OS)

- Hard Disk Capacity

  At least 320 MB

- Disk capacity for database (*1)

  For information on how to estimate capacity, refer to "3.1.2 Estimating Database Capacity"

  *1: The requirements for memory and disk capacity may change according to system structure, scale and available resources.

Management Console

- CPU

  Celeron 2 GHz or higher

- Memory

  At least 256 MB (excluding OS)

- Hard disk capacity

  At least 80 MB

Note

Logs cannot be displayed in the following cases:

When logs are displayed in the Log Viewer, each log occupies about 7.5 KB of memory.

If the number of logs reaches 100,000, memory of 100,000 x 7.5 KB= 750 MB will be used.

Therefore, when there is less available memory in the Management Server or in the PC on which the Log Viewer is running, logs may not be displayed.

Besides, in the 3-level structure, the same memory is used when the logs of the sub-level Management Server are displayed by connecting with the Log Viewer of the Master Management Server. Thus, when there is less available memory in the sub-level Management Server or in the PC where the Log Viewer is running, logs may not be displayed.

Report Output Tool

- CPU

  Celeron G530T 2 GHz or higher

- Memory (*1)

  At least 512 MB (including OS)

- Hard disk capacity

  At least 50 MB

- Disk capacity for log output (*1)

  The following disk capacity is required:

```
400 bytes x output logs
```

  *1: The requirements for memory and disk capacity may change according to system structure, scale and available resources.

Relay Server

- CPU

  Intel Xeon E5503 (2 GHz) or higher

- Memory

  At least 2 GB (excluding OS)

- Hard disk capacity

  At least 2 GB

Client (CT)

- CPU

  Pentium III 600MHz or higher

  Core i3 2.0 GHz or higher if the local proxy method is used as the web communication monitoring method

- Memory

  At least 320 MB (excluding OS)

  640 MB or higher (excluding the operating system) if the local proxy method is used as the web communication monitoring method

- Hard disk capacity

  At least 130 MB

  At least 945 MB (when using the original file backup function and E-mail content saving function)

Detailed information is as follows:

Item Name	Required Disk Capacity	Description
Attached data (screen capture data)	15 MB	The hard copy image of the screen captured by the Screen Capture function will be saved to the client (CT) temporarily, even if it has been saved as attached data on the server. This is the required capacity. (The average capacity of the amount of screen capture data that are saved to the client (CT) is 100.) The collection still can be performed when the amount of collected data exceeds this capacity. However, if the capacity of the drive in which the folder used for saving log files of client (CT) is located is less than 50 MB, the screen capture data will not be collected.
Attached data (backup original file data)	700 MB	If the original file backup function is used when exporting files using the file export utility, the attached data will be saved to the client (CT) temporarily, even if it has been saved as attached data (original backup data) on the server. This is the required capacity. This capacity can be changed in the terminal operating settings of the Management Console. If the amount of collected data exceeds this capacity, the original file backup will not be performed.
Attached data (E-mail content data) (e-mail sending log)	50 MB	If the E-mail content saving function is used when sending E-mails, the attached data will be saved to the client (CT) temporarily, even if it has been saved as attached data (original backup data) on the server. This is the required capacity. This capacity cannot be changed. Besides, if the E-mail content data exceeds this size, the E-mail content cannot be saved.
Attached data (email content data) (e-mail receiving log)	50 MB	If using the email content saving feature when receiving emails, the attached data will temporarily be saved to the client (CT) even if it has been saved on the server. The capacity is required for that purpose. This capacity cannot be changed. Additionally, the email content cannot be saved if the email content data exceeds this size.
Prohibition log	10 MB	If the client (CT) cannot be connected with the Master Management Server or Management Server, the prohibition logs will be saved to the client (CT). If the available capacity of the drive in which the folder for saving log files of the client (CT) is located reaches 100 MB, multiple new files can be created. The maximum size of a file is 10 MB. Besides, if the available capacity of the drive in which the folder for saving prohibition logs is located is less than 100 MB, the following prohibition logs will be deleted. The drive for saving prohibition logs is the one for saving log files, which is specified during the installation of the client (CT). Initial value: <OS installation drive>
Operation log	30 MB	If the client (CT) cannot be connected with the Master Management Server or Management Server, the operation logs will be saved to the client (CT). If the available capacity of the drive in which the folder for saving log files of client (CT) is located reaches 200 MB, multiple new files can be created. The maximum size of a file is 30 MB. Besides, if the available capacity of the drive in which the folder for saving operation logs is located is less than 200 MB, the following operation logs will be deleted. The drive for saving operation logs is the one for saving log files, which is specified during the installation of client (CT). Initial value: <OS installation driver>

Item Name	Required Disk Capacity	Description
Error log	60 MB	On the client (CT), the initial setting of operation records and error information is a maximum if 2 MB per day over a period time of 30 days, so a maximum of 60 MB can be saved in total. Thus, the capacity is 60 MB. The capacity of the error log can be changed. For the change method, refer to "Change Operation Settings of Client (CT)" in the *User's Guide for Administrators*. Besides, if the capacity of the error log exceeds the disk capacity, the following error log will be overwritten.
Others	30 MB	The capacity needed for the modules and manuals.

Printer (for report output)

Printer is used according to the report output function when printing reports.

The following performance is required for the printer being used:

- A4 printing is available
- Black-and-white printing (color printing is recommended) is available
- Resolution of 600dpi or higher

Smart Device (Agent)

- Internal Memory

  At least 30 MB

  Capacity varies because the logs with variable length (such as URL) are stored.

3.1.2 Estimating Database Capacity

This section describes how to estimate the database capacity of the Management Server/Master Management Server and the Log Analyzer Server.

3.1.2.1 Management Server/Master Management Server

When there is a Master Management Server and multiple Management Servers, it is necessary to estimate the database capacity of each server respectively.

Preparation

The following information is required for estimating the capacity of database:

In 2-level structure

- Number of the clients (CTs)
- Number of smart devices (agents)
- Number of months for saving operation logs
- Number of non-file operation logs
- Number of file operation logs

In 3-level structure

- Number of the clients (CTs) and smart devices (agents) in total
- Number of the clients (CTs) and smart devices (agents) managed by the Management Server
- Number of the clients (CTs) that manage the Management Servers

- Number of months to save operation logs
- Number of non-file operation logs
- Number of file operation logs

Number of clients (CTs)

The estimated number of clients (CTs) is the number of clients (CTs) connected directly with 1 Master Management Server or Management Server that creates the database. If there is no client (CT) connecting to the Master Management Server directly, calculate as 0.

When installing the client (CT) to a virtual environment, add the number of users connecting to the virtual environment as the number of CTs.

Number of smart devices (agents)

Add the number of smart devices (agents) connected to the Relay Server, treating them as Clients (CTs). In 3-level structure, count the number of Clients (CT) that are directly connected to the Master Management Server as the number of smart devices.

Number of clients (CTs) and smart devices (agents) in total

This is the number of all the clients (CTs) connected with the Management Server or Master Management Server.

It is necessary to estimate the database capacity of the Master Management Server in a 3-level structure.

Number of months to save operation logs

This is the number of months during which the operation logs are saved in database.

Number of file operation logs

This is the total number of events of file operation executed at one client (CT) for each day. File operation refers to the "File operation log" item in the "Operation Log Type" contained in the table below.
The file operation log is not recorded for smart devices (agents).

Number of non-file operation logs

This is the total number of all events excluding file operation executed at one client and smart devices (agents) for each day. A non-file operation log refers to the all items in the "Operation Log Type" contained in the table below except for the items marked as "File Operation Log".

Operation Log Type	Selectable	Number of obtained logs
Application Startup Log	Yes	The number of times an application has been started [Example] The count is "1" when an application is started once.
Application Termination log	Yes	The number of times an application has been terminated. [Example] The count is "1" when an application is terminated once.
Window Title Obtaining log	Yes	The number of times an active window has been switched. [Example] The count is "1" when an active window has been switched once.
E-mail Sending Log	Yes	The number of E-mails that have been sent. [Example] The count is "1" when one E-mail has been sent.
E-mail receiving log	Yes	Number of emails that have been received. [Example] The count is "1" when one email has been received.

Operation Log Type	Selectable	Number of obtained logs
E-mail Sending Suspension Log	Yes	The number of times E-mail sending to unauthorized domains has been suspended. [Example] When sending E-mails to unauthorized domains, the count of logs of which "Cancel" has been selected (i.e., to terminate sending) in the confirmation window of the E-mail address is "1".
Command Operation Log	Yes	The number of times the command is executed in the command prompt. [Example] The count is "1" when the command has been executed once.
Device Configuration Change Log	Yes	Number of times the drive configuration has been changed + number of times USB devices have been connected + number of times media have been connected [Example] - The count is "1" when a network drive has been added as the Z drive. - The count is "2" when a USB flash memory is connected and F drive is added. - The count is "1" when a USB web camera is connected (without adding a drive). - The count is "3" when a USB card reader and SD card are connected, and G drive is added.
Printing Operation Log	Yes	The number of times printing has been used. [Example] The count is "1" when printing has been used once, excluding the number of times the printing has been used in a prohibited application.
File Export Log	Yes	Number of exported files [Example] The count is "1" when one file has been exported.
File Operation Log	Yes	The number of times file operations have occurred. [Example] The count is "1" when one file has been created/viewed/ overwritten/copied/moved/deleted once.
Linkage Application Log	Yes	The number of times logs are sent by linkage applications. [Example] The count is "1" when a log has been sent by a linkage application once.
Logon/Logoff Log	Yes	The number of times logon/logoff Windows system/the number of times the computer has been started or shut down/the number of times the computer sleeps or returns/the number of times it is connected to or disconnected from the virtual environment. [Example] The count is "1" when having logged onto a windows system once.
Environment change log	Yes	Number of times an IP address is changed + number of times the emergency procedure is performed or canceled.

Operation Log Type	Selectable	Number of obtained logs
		[Example] - The count is "1" when an IP address is changed. - The count is "1" when an emergency procedure is performed. - The count is "1" when an emergency procedure is canceled.
PrintScreen Key Operation Log	Yes	The number of times the PrintScreen key is pressed. [Example] The count is "1" when the PrintScreen key is pressed once.
Web Operation Log	Yes	The number of times the web upload or web download has been performed. [Example] - The count is "1" when one file has been downloaded from the Web server. - The count is "1" when one file has been uploaded to the Web server.
FTP Operation Log	Yes	The number of times FTP upload or FTP download has been performed. [Example] - The count is "1" when one file has been downloaded from the FTP server. - The count is "1" when one file has been uploaded to the FTP server.
Clipboard Operation Log(Virtual Environment)	Yes	The number of times a clipboard operation has occurred. [Example] The count is "2" when clipboard is used for copying from the virtual terminal to the physical terminal once.
Web Access Log (Smart Device)	Yes	Log indicating Web accessed from standard Android browser "Android Browser" [Example] The count is "1" when home page is accessed from "Android Browser".
SD Card Mount/Unmount Log (Smart Device)	Yes	The number of times the SD card was mounted/unmounted [Example] - The count is "1" when a smart device SD card is mounted - The count is "1" when a smart device SD card is unmounted
SIM Card Mount/Unmount Log (Smart Device)	Yes	The number of times the SIM card was mounted/unmounted [Example] - The count is "1" when a smart device SIM card is mounted - The count is "1" when a smart device SIM card is unmounted
Wi-Fi Connection Log (Smart Device)	Yes	The number of times Wi-Fi connection was established [Example] The count is "1" when a smart device gets connected to Wi-Fi

Operation Log Type	Selectable	Number of obtained logs
Bluetooth connection log (smart device)	Yes	The number of times Bluetooth connection was established [Example] The count is "1" when a smart device gets connected to Bluetooth
A log of incoming and outgoing calls (smart device)	Yes	The number of calls made and received [Example] - The count is "1" when an outgoing call is made from the smart device - The count is "1" when the smart device receives a call
Application usage log (smart device)	Yes	The number of times an application was used [Example] The count is "1" when the application is used on a smart device.
Application configuration change log (smart device)	Yes	The number of times an application was installed/uninstalled [Example] - The count is "1" when the application is installed on a smart device. - The count is "1" when the application is uninstalled from a smart device.
Prohibition log	No	The number of times a logon prohibited group has been logged on. [Example] The count is "1" when the operation of logon prohibited object has been performed once.
		The number of times a startup prohibited applications has been started. [Example] The count is "1" when a Startup Prohibited Application has been started once.
		The number of times a Disabled PrintScreen Key is pressed. [Example] The count is "1" when the Disabled PrintScreen Key has been pressed once.
		The number of times printing via a Printing Prohibited Application has been performed. [Example] The count is "1" when printing via a Printing Prohibition Application has been performed once.
		The number of times the prohibited file has been added to E-mail for sending and saving. [Example] The count is "1" when one prohibited file has been added to E-mail and has been sent successfully.
		The number of times the prohibited URL has been accessed or the number of times uploading to or downloading from a prohibited Web server has occurred. [Example]

Operation Log Type	Selectable	Number of obtained logs
		- The count is "1" when the prohibited URL has been accessed once. - The count is "1" when one file has been uploaded or downloaded from the prohibited Web server.
		The number of times the prohibited FTP server has been accessed [Example] The count is "1" when the prohibited FTP server has been accessed once.
		The number of times the prohibited clipboard has been used [Example] The count is "1" when the prohibited clipboard has been used once.
		The number of times a smart device established Wi-Fi connection with a prohibited access point when the Wi-Fi connection to the access points is prohibited for the smart device [Example] The count is "1" when a smart device establishes Wi-Fi connection with a prohibited access point.
		The number of times a smart device established pairing with a prohibited Bluetooth device when pairing with a Bluetooth device was prohibited. [Example] The count is "1" when a smart device establishes Bluetooth connection with a prohibited device.
		The number of times a smart device used a prohibited application. [Example] The count is"1" when the application is used on a smart device.
Others (configuration change log)	No	The number of times policy configuration has been changed via the Management Console. [Example] If policy has been changed via the Management Console, the number of logs output will be between "25" and "1328", depending on the changes made.

The "Operation Log Type" for which "Yes" is mentioned in the "Selectable" column can be set from **Log Collection Operation** of **Windows** of the Management Console.

The "Operation Log Type" for which "(Smart Device)" is mentioned in the "Selectable" column can be set from **Log Collection Operation** of **Android** of the Management Console.

Estimating Database Capacity

The method of estimating the database capacity is shown in the following table. Estimate and compare the number of the clients (CTs) and number of smart devices (agents), number of months for saving operation logs, number of non-file operation logs, number of file operation logs and required database capacity that are recorded in the following. In addition, the number of months for saving operation logs is in proportion with the database capacity. (For example: when setting a doubled "Number of months to save operation logs", the database capacity should also be calculated in double.)

Estimation standard 1 (number of file operation logs: 500, number of non-file operation logs: 500)

Number of the clients (CTs) +Number of smart devices (Agent)	100	500

Number of months to save operation logs	1 month	1 month
Number of file operation logs	500	500
Number of non-file operation logs	500	500
Database capacity	11,497 MB	48,724 MB

Estimation standard 2 (number of file operation logs: 1000, number of non-file operation logs: 1000)

Number of the clients (CTs)+ Number of smart devices (Agent)	100	500
Number of months to save operation logs	1 month	1 month
Number of file operation logs	1000	1000
Number of non-file operation logs	1000	1000
Database capacity	20,092 MB	94,393 MB

Estimating the capacity of screen capture data

This section describes how to estimate the capacity of screen capture data. The following is the standard of capacity estimation for screen capture data.

1 piece of screen capture data: 150 KB (when the image resolution of client (CT) is XGA)

Example of capacity estimation

- Number of clients (CTs): 1000
- The number of times for 1 client (CT) to collect screen capture data per day (prediction value): 2
- Storage period for screen capture data: 90 days

Estimation result

```
1000 (number of the clients (CTs)) x 2 (capture times/day) x 90 (days to save) x 150 KB = 26 GB
```

Data capacity of backup original file

This section describes data capacity of backup original files.

The size of the backup original file will be the size of the exported files, plus the size of the sent emails and the received emails.

Example 1) When attached data are saved to server

When exporting 10 MB files from the client (CT), the 10 MB files will be saved to the folder for saving attached data of the Management Server.

Example 2) When attached data are saved to CT

When exporting 10 MB files from the client (CT), the 10 MB files will be saved to the log saving directory of the client.

Capacity of clipboard original data

This section describes the capacity of original data when the clipboard is used. The total value of Example 1), Example 2) and Example 3) is the capacity of clipboard original data. Clipboard original data will be imported to the client (CT) in virtual and physical environment.

Example 1) When image data is copied via clipboard

Image data at 1 operation: 150 KB (when the image resolution of client (CT) is XGA)

Example of capacity estimation

- Number of clients (CTs): 1000
- The number of times for 1 client (CT) to copy image data per day (prediction value): 2
- Storage period: 90 days

Estimation result

```
1000 (number of clients (CTs)) x 2 (times of clipboard operation per day) x 90 (days to save) x 150
KB x 2 (collect in virtual/physical environment) = 52 GB
```

Example 2) When text data is copied via clipboard

Text data at 1 operation: 1 KB

Examples of capacity estimation

- Number of clients (CTs): 1000
- The number of times for 1 client (CT) to copy text data per day (prediction value): 2
- Storage period: 90 days

Estimation result

```
1000 (number of clients (CTs)) x 2 (times of clipboard operation per day) x 90 (days to save) x 1 KB
x 2 (collect in virtual/physical environment) = 352 MB
```

Example 3) When files are copied through clipboard

File path at 1 operation: 80 bytes

Example of capacity estimation

- Number of the clients (CTs): 1000
- Frequency for each client (CT) to copy files per day (estimated value): 2
- Storage period: 90 days

Estimation result

```
1000 (number of clients (CTs)) x 2 (times of clipboard operation per day) x 90 (days to save) x 80
bytes  x 2 (collect in virtual/physical) = 28 MB
```

3.1.2.2 Log Analyzer Server

Estimating database capacity

The standard for estimating the database capacity is shown in the following table. Estimate and compare the number of the clients (CTs) expected for operation, number of months to save operation logs, number of non-file operation logs, number of file operation logs and required database capacity that are recorded in the following.

If there are multiple Log Analyzer Servers, it is necessary to estimate the database capacity of each server.

Estimation standard 1 (number of file operation logs: 500, number of non-file operation logs: 500)

Number of clients (CTs)	100	100
Number of months to save operation logs	3 months	6 months
Number of file operation logs	500	500
Number of non-file operation logs	500	500
Database capacity	22,933 MB	38,898 MB

Estimation standard 2 (number of file operation logs: 1000, number of non-file operation logs: 1000)

Number of clients (CTs)	500	500
Number of months to save operation logs	3 months	6 months
Number of file operation logs	1000	1000
Number of non-file operation logs	1000	1000
Database capacity	213,513 MB	373,158 MB

Estimating temporary disk capacity required for sending log data

This section describes how to estimate the disk capacity required for temporary workspace on the Management Server when sending log files from the Management Server to the Log Analyzer Server.

Preparation

The following information is required when estimating temporary disk capacity

- Number of clients (CTs) of Systemwalker Desktop Keeper
- Number of file operation logs per day
- Number of non-file operation logs per day

Temporary disk capacity

The method of estimating the temporary disk capacity required for each Management Server is shown below.

```
Temporary disk capacity= (A) capacity of operation log information x number of clients x (B) number
of days to output
```

(A) Capacity of operation log information

Capacity of operation log is the capacity of operation log information obtained from one client (CT) per day

The formula for calculating the capacity of operation log information is shown below.

```
Capacity of operation log information capacity= average record length x (number of non-file
operation logs+ number of file operation logs)
```

(B) Number of days to output

The number of days to output is supposed to be 1.

Example of calculating temporary disk capacity

- Average record length: 400 bytes
- Number of non-file operation logs: 1000
- Number of file operation logs: 500
- Number of clients: 500

Estimation results

```
Temporary disk capacity = 400 bytes x (1000+ 500) x 500 x 1 day ~= 280[MB]
```

3.2 Software

This section describes the software operating environment of Systemwalker Desktop Keeper.

3.2.1 OS

The OS requirements of each function component are as follows.

Management Server/Master Management Server/Relay Server

- Microsoft Windows Server 2008, Standard Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008, Enterprise Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 Standard without Hyper-V Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 Enterprise without Hyper-V Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 R2 Standard Service Pack 1 (*1)(*2)(*3)

- Microsoft Windows Server 2008 R2 Enterprise Service Pack1 (*1)(*2)(*3)
- Microsoft Windows Small Business Server 2011 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 Datacenter (*1)(*2)(*3)
- Microsoft Windows Server 2012 Standard (*1)(*2)(*3)
- Microsoft Windows Server 2012 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 Foundation (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Datacenter (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Standard (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Foundation (*1)(*2)(*3)
- Microsoft Windows Server 2016 Datacenter (*1)(*2)(*3)(*4)
- Microsoft Windows Server 2016 Standard (*1)(*2)(*3)(*4)
- Microsoft Windows Server 2016 Essentials (*1)(*2)(*3)(*4)

  *1: If the 32-bit version of Management Server/Master Management Server is installed on a 64-bit operating system, it will run as a 32-bit application on a Windows 32-bit On Windows 64-bit subsystem. Additionally, the 64-bit version of Management Server/ Master Management Server can only be installed on a 64-bit operating system.
  If the Relay Server is installed on a 64-bit operating system, it will run as a 32-bit application on a Windows 32-bit On Windows 64-bit subsystem.

  x64 Edition should be operated under 32-bit compatible mode on Relay Server.

  *2: Server Core cannot be used.

  *3: This product can be used in any of the following environments:

  IPv4-only operating environment

  IPv4/v6 mixed environment

  IPv6-only operating environment (do not uninstall IPv4, that is, do not execute "netsh interface ipv4 uninstall")

  *4: Nano Server cannot be used.

Log Analyzer Server

- Microsoft Windows Server 2008, Standard Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008, Enterprise Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 Standard without Hyper-V Service Pack2 (*2)(*3)
- Microsoft Windows Server 2008 Enterprise without Hyper-V Service Pack 2 (*2)(*3)
- Microsoft Windows Server 2008 R2 Standard Service Pack 1 (*1)(*2)(*3)
- Microsoft Windows Server 2008 R2 Enterprise Service Pack 1(*1)(*2)(*3)
- Microsoft Windows Small Business Server 2011 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 Datacenter (*1)(*2)(*3)
- Microsoft Windows Server 2012 Standard (*1)(*2)(*3)
- Microsoft Windows Server 2012 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 Foundation (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Datacenter (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Standard (*1)(*2)(*3)

- Microsoft Windows Server 2012 R2 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Foundation (*1)(*2)(*3)
- Microsoft Windows Server 2016 Datacenter (*1)(*2)(*3)(*4)
- Microsoft Windows Server 2016 Standard (*1)(*2)(*3)(*4)
- Microsoft Windows Server 2016 Essentials (*1)(*2)(*3)(*4)

  *1: If the 32-bit version of Log Analyzer Server is installed on a 64-bit operating system, it will run as a 32-bit application on a Windows 32-bit On Windows 64-bit subsystem. Additionally, the 64-bit version of Log Analyzer Server can only be installed on a 64-bit operating system.

  *2: Server Core cannot be used.

  *3: This product can be used in any of the following environments:

  IPv4-only operating environment

  IPv4/v6 mixed environment

  IPv6-only operating environment (do not uninstall IPv4, that is, do not execute "netsh interface ipv4 uninstall")

  *4: Nano Server cannot be used.

Management Console

- Microsoft Windows Server 2008, Standard Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008, Enterprise Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 Standard without Hyper-V Service Pack 2 (*2)(*3)
- Microsoft Windows Server 2008 Enterprise without Hyper-V Service Pack 2 (*2)(*3)
- Microsoft Windows Server 2008 R2 Standard Service Pack 1 (*1)(*2)(*3)
- Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 (*1)(*2)
- Microsoft Windows Small Business Server 2011 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 Datacenter (*1)(*2)(*3)
- Microsoft Windows Server 2012 Standard (*1)(*2)(*3)
- Microsoft Windows Server 2012 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 Foundation (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Datacenter (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Standard (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Essentials (*1)(*2)(*3)
- Microsoft Windows Server 2012 R2 Foundation (*1)(*2)(*3)
- Microsoft Windows Server 2016 Datacenter (*1)(*2)(*3)(*4)
- Microsoft Windows Server 2016 Standard (*1)(*2)(*3)(*4)
- Microsoft Windows Server 2016 Essentials (*1)(*2)(*3)(*4)
- Windows 7 Ultimate (Without Service Pack /1) (*1)(*3)
- Windows 7 Enterprise (Without Service Pack /1) (*1)(*3)
- Windows 7 Professional (Without Service Pack /1) (*1)(*3)
- Windows 8.1 Pro(*1)(*3)
- Windows 8.1 Enterprise(*1)(*3)
- Windows 10 Pro(*1)(*3)

- Windows 10 Enterprise(*1)(*3)
- Windows 10 Education(*1)(*3)

*1: If the Management Console is installed on a 64-bit operating system, it will run as a 32-bit application on a Windows 32-bit On Windows 64-bit subsystem.

*2: Server Core cannot be used.

*3: This product can be used in any of the following environments:

IPv4-only operating environment

IPv4/v6 mixed environment

IPv6-only operating environment (do not uninstall IPv4, that is, do not execute "netsh interface ipv4 uninstall".

*4: Nano Server cannot be used.

Client (CT)

- Microsoft Windows Server 2008, Standard Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008, Enterprise Edition Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 Standard without Hyper-V Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 Enterprise without Hyper-V Service Pack 2 (*1)(*2)(*3)
- Microsoft Windows Server 2008 R2 Foundation Service Pack 1 (*1)(*2)(*4)
- Microsoft Windows Server 2008 R2 Standard Service Pack 1 (*1)(*2)(*4)
- Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 (*1)(*2)(*4)
- Microsoft Windows Small Business Server 2011 Essentials (*1)(*2)(*4)
- Microsoft Windows Server 2012 Datacenter (*1)(*2)(*4)
- Microsoft Windows Server 2012 Standard (*1)(*2)(*4)
- Microsoft Windows Server 2012 Essentials (*1)(*2)(*4)
- Microsoft Windows Server 2012 Foundation (*1)(*2)(*4)
- Microsoft Windows Server 2012 R2 Datacenter (*1)(*2)(*4)
- Microsoft Windows Server 2012 R2 Standard (*1)(*2)(*4)
- Microsoft Windows Server 2012 R2 Essentials (*1)(*2)(*4)
- Microsoft Windows Server 2012 R2 Foundation (*1)(*2)(*4)
- Microsoft Windows Server 2016 Datacenter (*1)(*2)(*4)(*5)
- Microsoft Windows Server 2016 Standard (*1)(*2)(*4)(*5)
- Microsoft Windows Server 2016 Essentials (*1)(*2)(*4)(*5)
- Windows 7 Ultimate (Without Service Pack /1) (*2)(*3)
- Windows 7 Enterprise (Without Service Pack /1) (*2)(*3)
- Windows 7 Professional (Without Service Pack /1) (*2)(*3)
- Windows 7 Home Premium (Without Service Pack /1) (*2)(*3)
- Windows 8.1 (*2)(*3)
- Windows 8.1 Pro (*2)(*3)
- Windows 8.1 Enterprise (*2)(*3)
- Windows 10 Home (*2)(*3)

- Windows 10 Pro (*2)(*3)
- Windows 10 Enterprise (*2)(*3)
- Windows 10 Education (*2)(*3)

*1: Server Core cannot be used.

*2: This product can be used in any of the following environments:

IPv4-only operating environment

IPv4/v6 mixed environment

IPv6-only operating environment (do not uninstall IPv4, that is, do not execute "netsh interface ipv4 uninstall")

*3: If the client (CT) is installed on a 64-bit operating system, it will run as a 32-bit application on a Windows 32-bit On Windows 64-bit subsystem.

*4: The client (CT) will run as a 32-bit application on a Windows 32-bit On Windows 64-bit subsystem.

*5: Nano Server cannot be used.

Note

Features supported by operating system

[OS that can use CD-R/RW media export function]

OS that can use the CD-R/RW media export function of the export utility are shown as follows:

- Windows 7 Ultimate
- Windows 7 Enterprise
- Windows 7 Professional
- Windows 7 Home Premium
- Windows 8.1 Pro
- Windows 8.1 Enterprise
- Windows 10 Home
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Education

[OS that can use DVD-R/RW media export function]

OS that can use the DVD-R/RW media export function of the export utility are shown as follows:

- Windows 7 Ultimate
- Windows 7 Enterprise
- Windows 7 Professional
- Windows 7 Home Premium
- Windows 8.1 Pro
- Windows 8.1 Enterprise
- Windows 10 Home
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Education

[The operating systems that can export information from the Active Directory Server]

- Windows Server 2008
- Windows Server 2012
- Windows Server 2016

Only when the Active Directory environment is in native mode. (Native mode is a standard operational mode of the Active Directory constructed in Windows 2000 Server and higher versions)

[Online Manual]

If you log in by using the built-in Administrator account in any of the following OS, you can access the online manual by using the Internet Explorer or Microsoft Edge on the desktop. Note that the manual cannot be accessed from the Modern UI Internet Explorer.

- Microsoft Windows Server 2012 Datacenter
- Microsoft Windows Server 2012 Standard
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation
- Microsoft Windows Server 2012 R2 Datacenter
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 R2 Foundation
- Microsoft Windows Server 2016 Datacenter
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2016 Essentials
- Windows 8.1 Pro
- Windows 8.1 Enterprise
- Windows 10 Home
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Education

To select the Internet Explorer on the desktop:

1. Select **Internet Options** > **Programs** tab
2. Then select **Always in Internet Explorer on the desktop**

Smart Device (Agent)

- Android 4.4 to Android 8.0
- iOS 6.0 to iOS 11

Report Output Tool

- Windows 7 Ultimate (Without Service Pack /1) (*1)
- Windows 7 Enterprise (Without Service Pack /1) (*1)
- Windows 7 Professional (Without Service Pack /1) (*1)
- Windows 8.1 Pro (*1)

- Windows 8.1 Enterprise (*1)
- Windows 10 Pro (*1)
- Windows 10 Enterprise (*1)
- Windows 10 Education (*1)

*1: If the Report Output Tool is installed on a 64-bit operating system, it will run as a 32-bit application on a Windows 32-bit On Windows 64-bit subsystem.

3.2.2 Necessary Software

Software required by Systemwalker Desktop Keeper is as follows.

Necessary software

[Common]

One of the following browsers is required in order to view the online manual or online help:

- Windows Internet Explorer 9
- Windows Internet Explorer 10
- Windows Internet Explorer 11
- Microsoft Edge

[Management Server/Master Management Server]

One of the following is required:

- Internet Information Services 7.0
- Internet Information Services 7.5
- Internet Information Services 8.0
- Internet Information Services 8.5
- Internet Information Services 10.0

[Log Analyzer Server]

Software required in the server for installing Log Analyzer Server is as follows:

- Microsoft .NET Framework 4.5.2 or later

[Report Output Tool]

One of the following is required in the PC for installing report output tool:

Additionally, the web version and 64-bit version are not supported.

- Microsoft Excel 2010
- Microsoft Excel 2013
- Microsoft Excel 2016

[Web Console]

Internet Explorer or Microsoft Edge can be used.

Recommended versions of Internet Explorer are shown below:

- Windows Internet Explorer 9
- Windows Internet Explorer 10
- Windows Internet Explorer 11

Note

Internet Explorer from Windows Store apps

If you have logged on using the built-in Administrator account of the operating systems below, use Internet Explorer or Microsoft Edge in the Desktop application on Web Console. Internet Explorer from Windows Store apps is not supported.

- Microsoft Windows Server 2012 Datacenter
- Microsoft Windows Server 2012 Standard
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation
- Microsoft Windows Server 2012 R2 Datacenter
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 R2 Foundation
- Microsoft Windows Server 2016 Datacenter
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2016 Essentials
- Windows 8.1 Pro
- Windows 8.1 Enterprise
- Windows 10 Home
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Education

Related Software

The following software is required when sharing structure information:

- Systemwalker Desktop Patrol V14g (14.0.0/V14.0.1/V14.1.0/V14.2.0/V14.3.0/V14.3.1)
- Systemwalker Desktop Patrol V15.0.0/V15.0.1/V15.1.0/V15.1.1/V15.1.3/V15.2.0

To compress data from the client and send logs, the following software must be installed on the Management Server and Client (CT).

- Visual C++ 2005 redistributable package (8.0.59193 or higher)
- Microsoft .NET Framework 4.6

One of the following software is required when using on a virtual OS.

Operating Environment of Management Server/Master Management Server

- VMware vSphere 5 to VMware vSphere 6.5
- Microsoft Hyper-V
- KVM

Client (CT)

- VMware vSphere 5 to VMware vSphere 6.5
- VMware View 4 to VMware View 5.1
- VMware Horizon View 5.2 to VMware Horizon View 6.2

- VMware Horizon 7 to VMware Horizon 7.2
- Citrix XenDesktop 5.0 to Citrix XenDesktop 7.15
- Microsoft Hyper-V

3.2.3 Database

The database is bundled in Systemwalker Desktop Keeper and is automatically installed during the installation of the Management Server/ Master Management server and Log Analyzer Server. This database cannot be used in products other than this product.

3.2.4 Analysis Function Module

This module is not installed.

Interstage Navigator Server will be bundled with Systemwalker Desktop Keeper as an analysis function module and it will be automatically installed during the installation of the Log Analyzer Server.

- Interstage Navigator Server Standard Edition 9.3.0

In addition, Interstage Navigator Server cannot use the modules that are not bundled.

If Interstage Navigator Server has been installed previously, it cannot coexist with the Log Analyzer Server.

3.2.5 Products that cannot be used in Mixture

Products that cannot coexist with Management Server / Master Management Server

The following products cannot coexist with the Management Server / Master Management Server:

- CS of Systemwalker Desktop Patrol V15.0.0 or higher (*1)
- Windows Server Update Services (WSUS) function when the server is of 64-bit environment (*2)

*1: Conditions for non-coexistence

The following combinations cannot coexist:

- Systemwalker Desktop Keeper 32-bit version and Systemwalker Desktop Patrol 64-bit version
- Systemwalker Desktop Keeper 64-bit version and Systemwalker Desktop Patrol 32-bit version

*2: Conditions for coexistence

Coexistence is possible in the 64-bit version of Management Server.

Products that cannot coexist with Client (CT)

- The attached tool of Systemwalker Desktop Patrol contains an external storage media write protection tool.
  Use the file export utility of Systemwalker Desktop Keeper.
- SecureKeeper (Product of Fujitsu China Systems)
- IT Policy N@vi

  If the check box of the **Use Operation/Usage restrictions** is cleared when creating an IT Policy N@vi client installer, IT Policy N@vi can coexist with the client (CT).
  Refer to the relevant IT Policy N@vi manual for details on how to operate IT Policy N@vi.
- FUJITSU Cloud Service MobileSUITE Device Management

  If the check box of the **Use Operation/Usage restrictions** is cleared when creating a FUJITSU Cloud Service MobileSUITE Device Management client installer, FUJITSU Cloud Service MobileSUITE Device Management can coexist with the client (CT).
  Refer to the relevant FUJITSU Cloud Service MobileSUITE Device Management manual for details on how to operate FUJITSU Cloud Service MobileSUITE Device Management.
- Citrix Presentation Server 4.5

- Citrix XenApp 5.0 to Citrix XenApp 7.15
- VMware Horizon RDSH 6.1 to VMware Horizon RDSH 7

Products that cannot coexist with Smart Device (Agent)

- IT Policy N@vi(Fujitsu Systems West products)
- FUJITSU Cloud Service MobileSUITE Device Management

Chapter 4 Link with Other Products

Systemwalker Desktop Keeper can be linked with the following products:

- Systemwalker Desktop Patrol
- Virtual desktop service V-DaaS
- iNetSec SF

Systemwalker Desktop Patrol

The following functions can be used by linking with Systemwalker Desktop Patrol:

- By using the software delivery function of Systemwalker Desktop Patrol, the client (CT) of this product can be automatically distributed and installed.
  For details, refer to "Determine the How to Install Client (CT)" and "Installation using Systemwalker Desktop Patrol" in *Installation Guide*.
- When "Systemwalker Desktop CT" of Systemwalker Desktop Patrol and the Client (CT) of Systemwalker Desktop Keeper are installed on one computer, "User ID (+) PC Name" of "Systemwalker Desktop CT" of Systemwalker Desktop Patrol can be obtained automatically and viewed through the CT list in the Management Console window. For the CT list of the Management Console window, refer to *User's Guide for Administrator*.
  By using "User ID (+) PC Name" in the CT list of the Management Console window, the asset information of the target computer can be viewed briefly through Systemwalker Desktop Patrol. For the asset information that can be viewed and the method of viewing, refer to the manual of Systemwalker Desktop Patrol.
- The structure information managed by Systemwalker Desktop Patrol can be imported to Systemwalker Desktop Keeper in the form of CSV files. Conversely, the structure information managed by Systemwalker Desktop Keeper can also be imported to Systemwalker Desktop Patrol.

  Configuration information files can be imported or output by using DTKIMPDP.EXE (import Systemwalker Desktop Patrol configuration information command). Refer to "DTKIMPDP.EXE (Import Systemwalker Desktop Patrol Configuration Information)" in the *Reference Manual* (Systemwalker Desktop Patrol V13.3.0 or later) for details.

  Also, the Systemwalker Desktop Patrol configuration information can be imported automatically every day. Refer to "Set the Link with Other Systems" in the *Installation Guide* (Systemwalker Desktop Patrol V14.2.0 or later) for details.

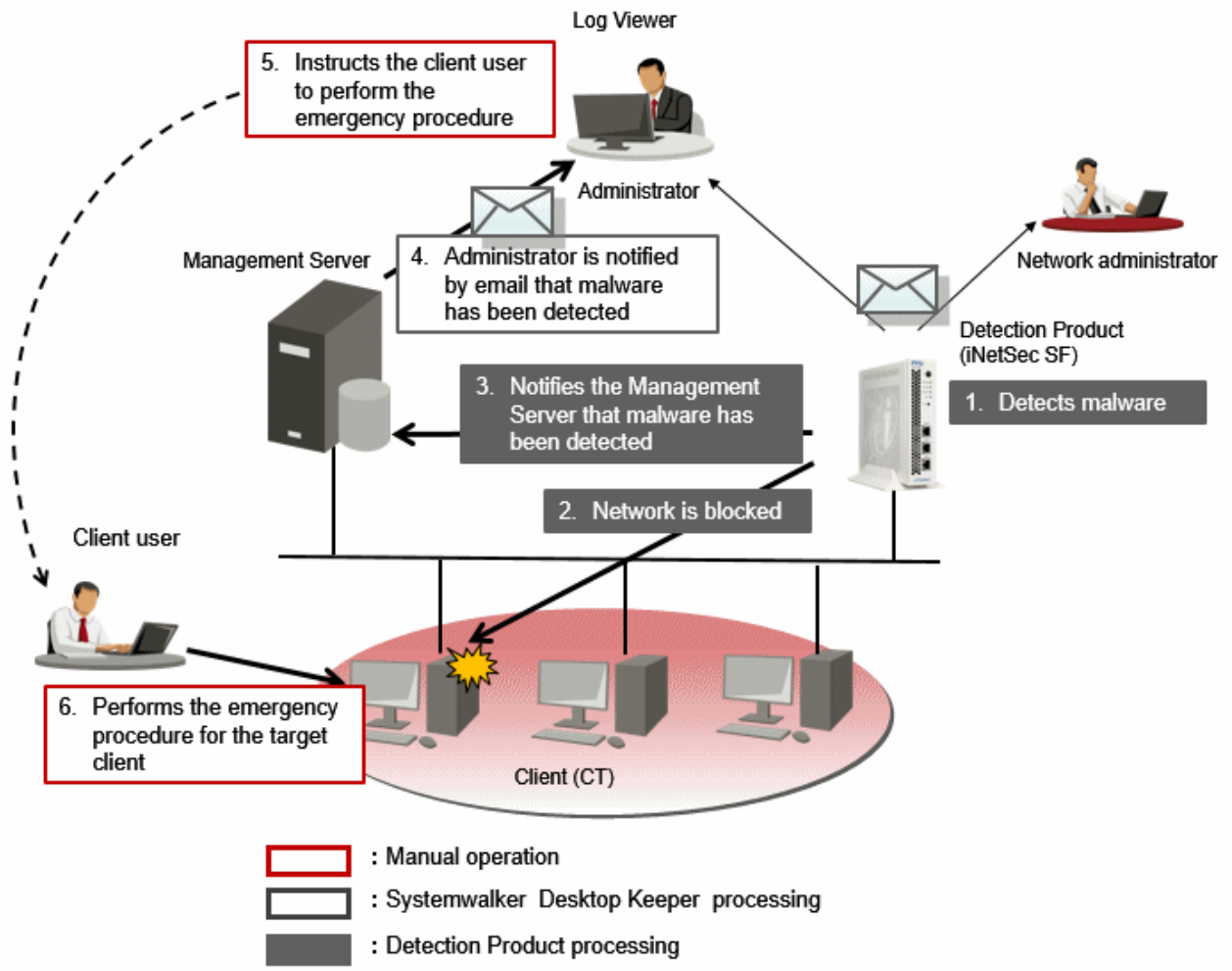
  Note that configuration information can be imported and output using the Systemwalker Desktop Keeper Management Console as well, however it is recommended to use it for the first configuration only because all groups will be deleted and then recreated when the Management Console is used for import. (Systemwalker Desktop Patrol V13.0.0 or later)
- The policy information that is set in the Systemwalker Desktop Keeper Client (CT) can be viewed as security auditing information of Systemwalker Desktop Patrol. (Systemwalker Desktop Patrol V14.2.0 or lower)
- The asset information managed by Systemwalker Desktop Patrol can be displayed in Systemwalker Desktop Keeper. (Systemwalker Desktop Patrol V14.2.0 or lower)

Virtual desktop service V-DaaS

Systemwalker Desktop Keeper can be installed on the virtual desktop service V-DaaS.

iNetSec SF

When Systemwalker Desktop Keeper is linked with iNetSec SF, iNetSec SF blocks the network when it automatically detects malware, and notifies the Management Server/Master Management Server. Furthermore, by performing an emergency procedure for the client (CT) using Systemwalker Desktop Keeper, it is possible to address security risks early on, and prevent damage from spreading.


Log Viewer
5. Instructs the client user to perform the emergency procedure
Administrator
Network administrator
Management Server
4. Administrator is notified by email that malware has been detected
Detection Product (iNetSec SF)
3. Notifies the Management Server that malware has been detected
1. Detects malware
2. Network is blocked
Client user
6. Performs the emergency procedure for the target client
Client (CT)
: Manual operation
: Systemwalker Desktop Keeper processing
: Detection Product processing

Glossary

Active Directory Linkage

This is a function that automatically generates organization information (tree information), user information and CT information (Computer information) based on the Active Directory management information of Microsoft Corporation. Through linking with Active Directory, installation will become easier and the operation effects after installation will be improved.

Android device

A smart device equipped with Android is called as Android device.

Backup Management Server

This is the backup server used for getting user policy when the management server connected to the client has an exception.

Blank Media

The media of CD-R, CD-RW, DVD-R and DVD-RW without any information, including the volume label being recorded, is called blank media.

Citrix XenApp Client

This is used when user accesses Citrix XenApp Server from a client PC. That is, Citrix XenApp Server Client Software.

Citrix XenApp Server

This is a product of Citrix Systems, Inc. All applications and data are saved and managed on the server. The user can perform remote logon to the server from client PC to operate open applications.

Citrix XenDesktop

This is a product of Citrix Systems, Inc. OS, application and data are completely virtualized and managed. This is used after a user performs a remote logon to the virtual PC from the client PC.

Client (CT) Terminal Registration Authentication

This authentication checks whether a password entered during client (CT) installation and management server registration by the client (CT), and a client management password set in the management console are the same. Also, this function registers the terminal only if both the passwords match.

Count by Purpose

Log is aggregated after conditions such as the aggregation unit and period have been specified.

Collective Management

This is a pattern that collectively manages user information on the master management server.

CT

This refers to computers at lowest level managed by Systemwalker Desktop Keeper. Policy can be set in the CT unit.

CT Policy

This is the policy set for the CT unit.

CT Level Control

A CT can be managed by levels according to the organization. Management of CT by levels is called CT Level Control.

CT Group

A CT group is obtained from CT level control. Policy can be set in the CT group unit.

CT Group Tree

This is a tree that shows the CT group and CT level. It can be displayed in the Management Console and Log Viewer.

CT List

This is a list of CTs displayed in the Management Console and Log Viewer. The type of information displayed in the CT list can be modified through the Management Console.

CT Version

This is the version of Systemwalker Desktop Keeper CT installed on the computer.

Device

Piece of hardware managed by Systemwalker Desktop Keeper.

Device information collection tool

Tool that retrieves information of devices attached to a PC and outputs it to a CSV file.

Name/media name

Name of the setting value on Systemwalker Desktop Keeper. This can be set by the user.

Disc at Once Closed

Burn the CD-R and CD-RW in disk mode, and write all data in one session. Adding data to the disk cannot be performed the next time.

Drive Letter

This indicates the drive information in the CT. (For example: "A" indicates the A drive. "D" indicates the D drive.)

DTPID

This indicates the "User ID (+) PC name" set in Systemwalker Desktop Patrol CT.
This is displayed when Systemwalker Desktop Keeper CT and Systemwalker Desktop Patrol CT are installed on the same computer at the same time.

Emergency procedure settings policy

Policy temporarily set for the client (CT) when a security risk arises.

Export Utility

This is a utility used to export a file after an encrypted file has been created. The destination for saving the encrypted file can be specified to any drive or folder on the local computer.

This, like Windows Explorer will be unable attempting to export a file from the computer installed with Systemwalker Desktop Keeper CT to a removable drive if the drive has been prohibited.

When this needed to export files to a removable drive, the Export Utility installed in the CT can be used to export files to the prohibited removable drive. In addition, the exporting file can be an encrypted file according to the settings of the management console.

Group Policy

Policy set in the unit of a CT group.

Hook Method

Method that returns the flow of processing back to its original state after intercepting the required data for referring to or processing in some way, from amongst the data sent via a specific interface.

Imaging Device

This indicates the devices such as mobile phones, digital camera, IC recorder, and media player.

iNetSec SF

Product of PFU Limited. This is a security product that addresses risks by blocking unsafe devices from the network.

Internal serial number

Unique identifier of a USB managed by Systemwalker Desktop Keeper.

Each USB device is assigned an individual serial number.

iOS Management Database

This is a database constructed in the server to manage iOS device.

iOS device

A smart device equipped with iOS is called as iOS device.

Legal Size

Legal size mainly refers to the paper size used in the United States (8.5x14 inch).

Letter Size

Letter size mainly refers to the paper size used in the United States (8.5x11 inch).

Level Control Service

This is the function of level control server, which can be used to achieve a level control of the server.

Local Proxy Method

Method of monitoring web communication on the Internet via a local proxy.

Log Analyzer Server

This aggregates the logs collected by the Management server and publishes the result to the Web console.

Log Viewing Database

This is the database for restoring and viewing the backed up log information.

Manage by Section

This is a pattern in which user information is managed by sections on the master management server and management server.

Management Console

As the setting function in Systemwalker Desktop Keeper, it can set and update policy. It can also confirm the GUI for the administrator who is currently setting information and can change settings to CT group unit and CT unit, or user group unit and user unit.

Media

Media managed by Systemwalker Desktop Keeper.

The media that can be used with the individual media identification function are listed below (it does not include blank media).

- SD card
- SDHC card
- SDXC card
- miniSD card
- miniSDHC card
- microSD card

- microSDHC card
- microSDXC card

Open Application

This is an application installed on a Citrix XenApp Server or server firm and open to multiple users of the Citrix XenApp client.

Operation Database

This is the database for saving the management policy that is currently being used on the server or log information.

Original Backup Function

This is the function that, when exporting files to the outside external File Export Utility, confirms exported files by automatically copying the exported files and saving them on the management server.

PMA (Program Memory Area)

This indicates an area on a CD-R or CD-RW for temporarily saving the track number and start/end position (TOC of session), when writing track in a session that has not been closed yet.

Policy

This refers to the setting information configured in Systemwalker Desktop Keeper Management Console.

Portable Device

This refers to the Windows Portable Device (WPD). It refers to mobile phones, digital cameras, IC recorders, and media players.

Relay Server

While using the log acquisition function or prohibition function of smart devices, a Relay Server needs to be installed. Relay Servers convert information from smart devices and sends it to the Management Server.

If a client (CT) is connecting via the Internet, a Relay Server must be installed between the client (CT) and the (Master) Management Server.

Removable Device

The following media that are recognized according to drive letter are called removable devices:

- Floppy disk (built-in, external)
- External hard disk
- MO (built-in, external)
- USB memory
- Compact flash memory
- Other removable drives and types of media that are displayed as removable device in "My Computer" of Windows.

Self-decryption

This is the encryption type that can be created by the export utility on the computer installed with Systemwalker Desktop Keeper CT. Even on a computer without Systemwalker Desktop Keeper, decryption can be done by running the encrypted file. (The EXE file of the decryption program has been attached in the encrypted file.)

Server

This is a server that manages policy or log information in Systemwalker Desktop Keeper. The server can be in level structure, and level composition can be adopted to form a server based on organization and management pattern.

Session

This is displayed in the command log of the log viewer and takes a command prompt as its operation unit. It manages the command that is run in one command prompt and the result output by command as one session.

By selecting session in the log viewer, the command log list of the session unit can be viewed.

Smart Device

This is a smart device managed by Systemwalker Desktop Keeper. Log acquisition and prohibition functions are enabled by installing the agent or profile.

Systemwalker Desktop Encryption

Systemwalker Desktop Encryption is the software that prevents disclosure of information resulted from a stolen PC, and ensures safe file delivery by encrypting files.

Systemwalker Desktop Keeper

Systemwalker Desktop Keeper is the software that prevents disclosure of internal information through the "record", "prohibit", "manage", "log analysis" and "report output" functions.

Systemwalker Desktop Log Analyzer

Systemwalker Desktop Log Analyzer is the software that collects logs of Desktop series and performs operation tendency analysis.

The functions of Systemwalker Desktop Log Analyzer have been integrated into this product.

Systemwalker Desktop Patrol

Systemwalker Desktop Patrol is the software that automatically applies the security patches corresponding to the security condition of PC, collects hardware/software information of PC, eliminates discarded PC hardware information, etc., and protects and manages IT assets according to security threats.

Systemwalker Desktop Patrol Assessor

Systemwalker Desktop Patrol Assessor is an extension product of Systemwalker Desktop Patrol (optional).
This is the software that provides machine management, contract management, inventory support, form generation and other functions based on the functions of Systemwalker Desktop Patrol to achieve internal control for the management/use of PCs.

The functions of Systemwalker Desktop Patrol Assessor have been integrated into Systemwalker Desktop Patrol.

Thin Client

Thin client refers to the general term of a system that keeps the minimum function of a client and manages applications, files and other resources on a server. Client refers to the computer that emphasizes functions, especially the computer without a hard disk.

TOC (Table Of Contents)

This indicates the management information recorded in a CD-R or CD-RW, such as the number of tracks, start position and the total length of data area, etc.

Track at Once Closed

Burn the CD-R or CD-RW in track mode. Though data cannot be added to the disk again after writing, a new track can be added.
In addition, the disk of Track at Once Closed cannot be written in Systemwalker Desktop Keeper.

Track at Once Open

Burn the CD-R or CD-RW in track mode. Data can be added to the disk the next time unless the capability of the disk is full.

UNC (Universal Naming Convention)

This is a method used to describe network resources under the Windows network environment.

USB device

Collective name for peripheral devices compatible with connection standard USBs.

In Systemwalker Desktop Keeper, this indicates USB devices that can be individually identified.

User

This is a certification key used for applying user policy, which is registered in the Management Console with the information that is same as the logon ID entered while logging onto a Windows computer.

User Group

This is a group of users organized through user level control. User policy can be set in the user group unit.

User Group Tree

This is a tree that shows user groups and user levels. The user group tree can be displayed in the Management Console.

User Level Control

This is able to manage users according to the level of its organization. The level management of users is called user level control.

User Policy

This is the policy set for the logon ID that is entered when logging onto a Windows computer with CT installed.

V12.0L20-V13.0.0 Compatible Mode

This is the mode of prohibition with the method implemented in Systemwalker Desktop Keeper V12.0L20-V13.0.0, when using the E-mail file attachment prohibition function. When this method is being used, the E-mail file attachment prohibition function can be used only when the following software is used:

- Microsoft Outlook Express 6.0
- Microsoft Outlook 2003

V13.2.0 Mode (Port Monitoring Mode)

This is the prohibition mode when the E-mail software uses SMTP protocol when the E-mail file attachment prohibition function is used.

VMware View

This is a product of VMware, Inc. OS, application and data are completely virtualized and managed. This is used after a user performs a remote logon to the virtual PC from the client PC.

Web Console (Log Analyzer)

This is used for viewing the result of aggregation and analysis in Log Analyzer Server. Various categories or keywords can be specified and displayed in detail.

Web Console (Log Viewer)

This is the function for viewing and searching the logs saved in the management server.

Web Console (Status window)

This is used for showing the aggregation result for the number of PCs with risk of information disclosure in all systems.