Systemwalker Desktop Keeper V14g

User's Guide

Windows

B1WD-2772-04ENZ0(00)
March 2012

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 V14g(14.2.0)

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

The target readers of this guide are the users of the Windows editions of the product.

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 VMware View™ environment)
- General knowledge of Citrix XenApp™ (when using the monitoring function of Citrix XenApp™)

Structure of This Guide

This guide consists of four chapters and a glossary.

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
Systemwalker Desktop Keeper User's Guide (This Manual)	This manual describes the summary and operating environment of Systemwalker Desktop Keeper.

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

Note: "Systemwalker Desktop Keeper User's Guide for 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.

Icons

The following icons are used in the guides.

Note

The above symbol applies to items requiring special attention.

Point

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

Abbreviations

The manual uses abbreviations of the following products.

Product Name	Abbreviation
Systemwalker Desktop Keeper Base Edition V12.0L10	BEV12.0L10
Systemwalker Desktop Keeper Base Edition V12.0L20	BEV12.0L20
Systemwalker Desktop Keeper Base Edition V13.0.0	BEV13.0.0

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

The manual uses abbreviations of the following operation systems.

Operation System Name	Abbreviation
Microsoft® Windows Server® 2008 Foundation, Microsoft® Windows Server® 2008 Standard, Microsoft® Windows Server® 2008 Enterprise, Microsoft® Windows Server® 2008 Standard without Hyper-V™, Microsoft® Windows Server® 2008 Enterprise without Hyper-V™, Microsoft® Windows Server® 2008 R2 Foundation, Microsoft® Windows Server® 2008 R2 Standard, Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® Small Business Server 2011 Essentials	Windows Server® 2008 (*)
Microsoft® Windows Server® 2003, Standard Edition, Microsoft® Windows Server® 2003, Enterprise Edition, Microsoft® Windows Server® 2003, Standard x64 Edition, Microsoft® Windows Server® 2003, Enterprise x64 Edition Microsoft® Windows Server® 2003 R2, Standard Edition, Microsoft® Windows Server® 2003 R2, Enterprise Edition, Microsoft® Windows Server® 2003 R2, Standard x64 Edition Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	Windows Server® 2003 (*)
Microsoft® Windows® 2000 Professional operating system, Microsoft® Windows® 2000 Server operating system, Microsoft® Windows® 2000 Advanced Server operating system	Windows® 2000
Microsoft® Windows NT® Server Version 4.0, Microsoft® Windows NT® Workstation Version 4.0	Windows NT®
Microsoft® Windows® XP Professional, Microsoft® Windows® XP Home Edition	Windows® XP (*)
Windows Vista® Home Basic, Windows Vista® Home Premium, Windows Vista® Business, Windows Vista® Enterprise, Windows Vista® Ultimate	Windows Vista® (*)

Operation System Name	Abbreviation
Windows® 7 Ultimate, Windows® 7 Enterprise, Windows® 7 Professional, Windows® 7 Home Premium	Windows® 7 (*)
Microsoft® Windows® Millennium Edition	Windows® ME
Microsoft® Windows® 98 Second Edition	Windows® 98
Microsoft® Windows® 95 operating system	Windows® 95
Microsoft® Windows Server® 2008 Foundation, Microsoft® Windows Server® 2008 Standard, Microsoft® Windows Server® 2008 Enterprise, Microsoft® Windows Server® 2008 Standard without Hyper-V™, Microsoft® Windows Server® 2008 Enterprise without Hyper-V™, Microsoft® Windows Server® 2008 R2 Foundation, Microsoft® Windows Server® 2008 R2 Standard, Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® 2003, Standard Edition, Microsoft® Windows Server® 2003, Enterprise Edition, Microsoft® Windows Server® 2003 R2, Standard Edition, Microsoft® Windows Server® 2003 R2, Enterprise Edition, Microsoft® Windows Server® 2003, Standard x64 Edition, Microsoft® Windows Server® 2003, Enterprise x64 Edition, Microsoft® Windows Server® 2003 R2, Standard x64 Edition, Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition, Microsoft® Windows® 2000 Professional operating system, Microsoft® Windows® 2000 Server operating system, Microsoft® Windows® 2000 Advanced Server operating system, Microsoft® Windows® XP Professional, Microsoft® Windows® XP Home Edition, Windows Vista® Home Basic, Windows Vista® Home Premium, Windows Vista® Business, Windows Vista® Enterprise, Windows Vista® Ultimate, Windows® 7 Ultimate, Windows® 7 Enterprise, Windows® 7 Professional, Windows® 7 Home Premium, Microsoft® Windows® Millennium Edition, Microsoft® Windows® 98 Second Edition	Windows

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

- Windows Server® 2008 64 bit Edition
- Windows Server® 2008 R2
- Windows Server® 2003 x64 Edition
- Windows Server® 2003 R2 x64 Edition
- Windows® XP 64 Bit Version
- Windows Vista® 64 Bit Version
- Windows® 7 64 Bit Version

Specific Operations of Operating System

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

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

Export Restriction

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

General Restriction

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

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

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

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

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

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

Systemwalker Desktop Keeper Base Edition V12.0L10

Systemwalker Desktop Keeper Base Edition V12.0L20

Systemwalker Desktop Keeper Base Edition V13.0.0

Systemwalker Desktop Keeper Base Edition V13.2.0

Systemwalker Desktop Keeper Base Edition V13.3.0

Systemwalker Desktop Keeper Standard Edition V13.2.1

Systemwalker Desktop Keeper Standard Edition V13.3.0

Systemwalker Desktop Keeper V14g (14.0.0)

Systemwalker Desktop Keeper V14g (14.0.1)

Systemwalker Desktop Keeper V14g (14.1.0)

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

Trademarks

March 2012

Revision History
March 2012 First Edition

Contents

Chapter 1 Overview of Systemwalker Desktop Keeper....1
1.1 Product Positioning....1
1.2 New Functions and Changed Functions of V14.2.0....2
1.3 System Structure....5

Chapter 2 Functions of Systemwalker Desktop Keeper....9
2.1 Prohibition Function....9
2.2 Record Function....10
2.3 Management Function....11
2.4 Log Analysis Function....12
2.5 Report Output Function....13

Chapter 3 Operating Environment....17
3.1 Hardware....17
3.1.1 Hard Disk / Memory Requirements....17
3.1.2 Estimating Database Capacity....21
3.1.2.1 Management Server/Master Management Server....21
3.1.2.2 Log Analyzer Server....26
3.2 Software....27
3.2.1 OS....28
3.2.2 Necessary Software....32
3.2.3 Database....33
3.2.4 Analysis Function Module....34
3.2.5 Products that cannot be used in Mixture....34

Chapter 4 Link with Other Products....37

Glossary....38

Index....43

Chapter 1 Overview of Systemwalker Desktop Keeper

This chapter provides an overview of the Systemwalker Desktop Keeper.

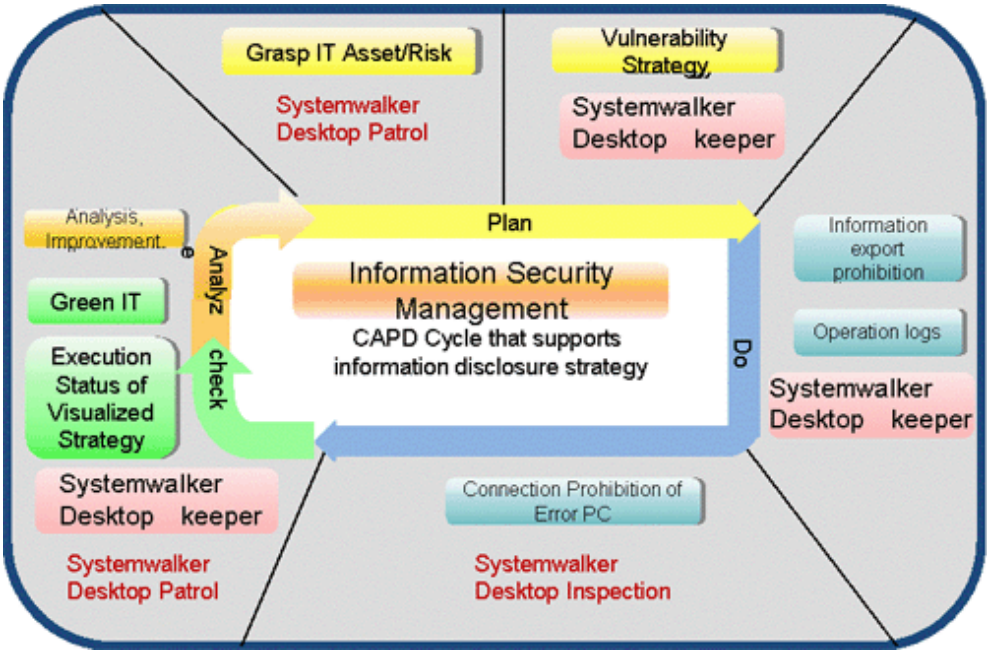
1.1 Product Positioning

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.

It knows the assets of customer systems and implements necessary security policies such as installing security patches, checking security settings, encrypting files, limiting PC operations, limiting file operations and collecting/analyzing logs, etc., and supports the "CAPD cycle" for continuous improvement.

Based on the previous security policies, the Systemwalker Desktop V14g series achieves the green IT policies for reducing CO2 emission through power-saving settings and a reduction of paper costs.



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 New Functions and Changed Functions of V14.2.0

The following section describes the newly added functions and modified functions of Systemwalker Desktop Keeper V14.2.0.

Newly Added Functions

Prohibition Function

- When changing to be able to start in safe mode for client (CT), still operate the prohibition (suppression) function.

  Reference: User's Guide: for Administrator "Usage Mode and Valid Prohibition Operation/Collected Log"

- Add the printing volume monitoring function.

  Change to be able to set the standard value of printing pages through this function, when exceeding the standard value, a warning and printing prohibition appear and it can be notified to administrator.

  Reference: User's Guide: for Administrator "Perform Terminal Initial Settings"

- Change to be able to prohibit accessing to the specified Web sites. When performing the operation against this prohibition policy, it is to collect Web operation prohibition log.

  Reference: User's Guide: for Administrator "Settings of [URL Access Prohibition] Tab", "Web Operation Prohibition Log"

- Change to be able to prohibit connecting the FTP server not allowed. When performing the operation against this prohibition policy, it is to collect FTP operation prohibition log.

  Reference: User's Guide: for Administrator "Settings of [FTP Server Connection Prohibition] Tab", "FTP Operation Prohibition Log"

- Change to be able to prohibit downloading from Web sites not allowed. When performing the operation against this prohibition policy, it is to collect Web operation prohibition log.

  Reference: User's Guide: for Administrator "Settings of [Web Upload and Download Prohibition] Tab", "Web Operation Prohibition Log"

- The clipboard operation of the virtual environment and the physical environment can be prohibited. When the operation against this prohibition policy is executed, the prohibition log of the clipboard operation will be collected.

  Reference: User's Guide: for Administrator "Setting of the [Virtual Environment setup] Tab", "Clipboard Operation Prohibition Log"

- Unauthorized network drive operation can be prohibited.

  Reference: User's Guide: for Administrator "Setting of the [File Export Prohibition] Tab"

- Reading from CD/DVD drive can be prohibited.

  Reference: User's Guide: for Administrator "Setting of the [File Export Prohibition] Tab"

- Uploading to websites can be prohibited.

  Reference: User's Guide: for Administrator "[Web Upload and Download Prohibition]"

Record Function

- When changing to be able to start in safe mode for client (CT), still operate the prohibition (suppression) function.

  Reference: User's Guide: for Administrator "Usage Mode and Valid Prohibition Operation/Collected Log" .

- Change to be able to collect FTP operation log (FTP upload and Download).

  Reference: User's Guide: for Administrator "FTP Operation Log" of "Policy Settings of Record Function".

- Change to be able to collect Web operation log (Web upload and download).

  Reference: User's Guide: for Administrator "Web Operation Log" of "Policy Settings of Record Function"

- Change to be able to save the text and file attachment of outgoing E-mail, and view them in Log Viewer.

  Reference: User's Guide: for Administrator "E-mail Sending Log" of "Policy Settings of Record Function"

- The clipboard operation of the virtual environment and the physical environment can be collected.

  Reference: User's Guide for Administrator "Clipboard Operation Log" of "Policy Settings for Record Function"

- The logs of connection to and disconnection from the virtual environment can be collected.

  Reference: User's Guide for Administrator "Logon/Logoff Log" of "Policy Settings for Record Function"

Management Function

- The following functions are added in Management Console.

  Change to be able to set the following conditions in CT/CT group search window.

  Active Directory Linkage

  DTPID

  The following items are added in CT/CT group search window (result bar).

  [Active Directory Linkage]

  [Opt-in Status of Network]

  [Affiliated Domain Name]

  The items are added in CT list window.

  [Active Directory Linkage]

  [Opt-in Status of Network]

  [Affiliated Domain Name]

  Change to be able to output the department administrator information as CSV file.

  Change to be able to modify the user password logging on Management Console.

  Change to be able to collect the remote inspection data of client (CT) through Management Console.

  Reference: User's Guide: for Administrator "Prepare Operating Environment"

  Reference Manual "Use Data Collection Tool" of.

- The following functions are added in terminal initial settings.

  Change to be able to specify the time when logs are sent from client (CT) to server.

  Reference: User's Guide: for Administrator "Perform Terminal Initial Settings".

- The self-version management function has made the following improvements.

  When applying modification long before, display and confirm whether to apply the modified window in the client (CT) window. Change to be able to set whether to display window by administrator.

  Reference: Installation Guide "Version Upgrade CT".

- The self-version management function has made the following improvements.

  That regarding all CTs as application objects long before changes to be able to specify applied CT according to IP address.

  Reference: Installation Guide "Version Upgrade CT".

- The following functions change to be able to be set easily on Management Server.

  Modify the connection target of Management Server

  Modify the IP address of backup Management Server

  Set the communication port between Management Servers

Printing Monitoring Mode

Modify the E-mail sending monitoring port number

After modifying the E-mail sending monitoring mode, set communication port for monitoring.

Modify the size of operation log file and prohibition log file

Modify the size and saving days of error log file

Modify the size of trace log file

Modify the inheritance mode of user policy

Reference: User's Guide: for Administrator "Change CT Environment".

- The following master PC management functions of virtual environment are supported:

  a. VMware View™

     Automated Pool(Dedicated/Floating)

     Manual Pool(Dedicated/Floating)

  b. Citrix XenDesktop™

     Pre-allocation, allocation at first use, and pooling

  Reference: Installation Guide "Installation using Master PC/Master Virtual PC"

  User's Guide: for Administrator "Start Management Console"

- The maximum number of clients (CTs) can be managed has been extended to 5,000.

  Reference: Installation Guide "Determine System Structure"

- Policy can be applied when the client (CT) is offline.

  Reference: User's Guide for Administrator "How to Apply Policy"

  User's Guide for Client "Apply Off-line Policy"

Log Viewing and Searching in Log Viewer

- The unit of search in Log Viewer is changed to Management Server. In addition, it changes to be able to specify several log types in the search conditions.

  Reference: User's Guide: for Administrator "View in [CT Operation Log] Window"

- In the Log Viewer, the CT group of client (CT) who performed violation operation changes to be displayed in red marks.

  Reference: User's Guide: for Administrator "View in [CT Operation Log] Window"

- The operation performed under the virtual environment and physical environment can be viewed in time sequence.

  Reference: User's Guide for Administrator "Start Log Viewer"

- The backup operation logs can be viewed by restoring them to the Log Viewing Database.

  Reference: Installation Guide "Construct Database"

  User's Guide for Administrator "Start Log Viewer"

Linkage Function with Other Product

- The following contents are added in the linkage function with Systemwalker Desktop Patrol.

  Start to import configuration information after use

  The previous settings to import configuration information will be cancelled, and it is allowed to import the configuration information immediately only after the installation. Beginning from this version, though the configuration information is imported, the settings information will not be cancelled and then the configuration information still can be imported after use.

  User information linkage

  The user information of Systemwalker Desktop Patrol can be imported to user policy list.

Reference: User's Guide: for Administrator "Import Information from Systemwalker Desktop Patrol".

- The structure information of Systemwalker Desktop Patrol can be obtained automatically.

  Reference: Installation Guide "Set the Link with Other Systems"

  User's Guide: for Administrator "Obtain Information From Systemwalker Desktop Patrol"

- The assets management window of Systemwalker Desktop Patrol can be invoked.

  Reference: User's Guide for Administrator "View in the [CT Operation Log] window"

File Export Utility

- Change to be able to specify to start File Export Utility according to period and time. Start File Export Utility in operating time only and use it when temporary export is allowed.

  Reference: User's Guide: for Administrator "Perform Terminal Initial Settings".

- Change to be able to select whether to create the icon of File Export Utility when installing CT.

  Reference: Installation Guide "Install CT".

- When changing to be able to use File Export Utility, input the export causes.

  Reference: User's Guide: for Administrator "Settings of [File Export Prohibition] Tab".

  Reference: User's Guide: for Client "Export Files and Folders Using File Export Utility".

Log Analysis Function and Report Output Function

- Change to be able to aggregate and analyze the log through Log Analyzer function.

  Or change to be able to view aggregation and analysis results of logs in the format of report though report output function.

  Reference: User's Guide "Log Analysis Function"

  User's Guide "Report Output Function"

  User's Guide: for Administrator "Tendency for Checking Client (CT) Operation"

  User's Guide: for Administrator "Create Monitoring Data".

Web Console

- Log Viewer is changed to Web Console.

  Reference: User's Guide: for Administrator "Monitor Operation in Client (CT) through Log Viewer"

- Change to be able to aggregate the sets of PC who performed information disclosure risk operation in all systems and confirm it in the status window.

  In addition, asset management information (Systemwalker Desktop Patrol) is also changed to be displayed in the same window.

  Reference: User's Guide: for Administrator "Preparation Required for Using Status Window", "Check Tendency in Status Window".

1.3 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, sets the security policy of subordinate PCs and distributes policy to each PC. The information of subordinate PCs 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. When the defined policy is CT policy, the policy can be updated immediately or at the next time when the client (CT) starts. 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. Please refer to the "Systemwalker Desktop Keeper 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) 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 definition of logs collected from client (CT). 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 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 worst 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.

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 "Systemwalker Desktop Keeper Installation Guide" for the setting standard of the server.

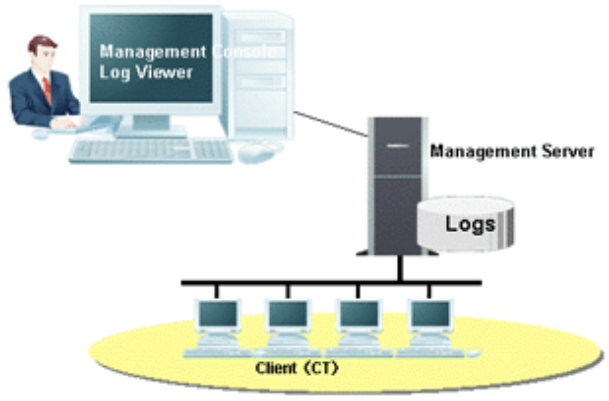
Here, the following four modes are described as examples of system structure:

- 2-Level System Structure
- 3-Level System Structure
- 3-Level System Structure (with Virtual Environment)

- 3-Level System Structure (with Log Analysis/Report Output and Citrix XenApp Monitoring)

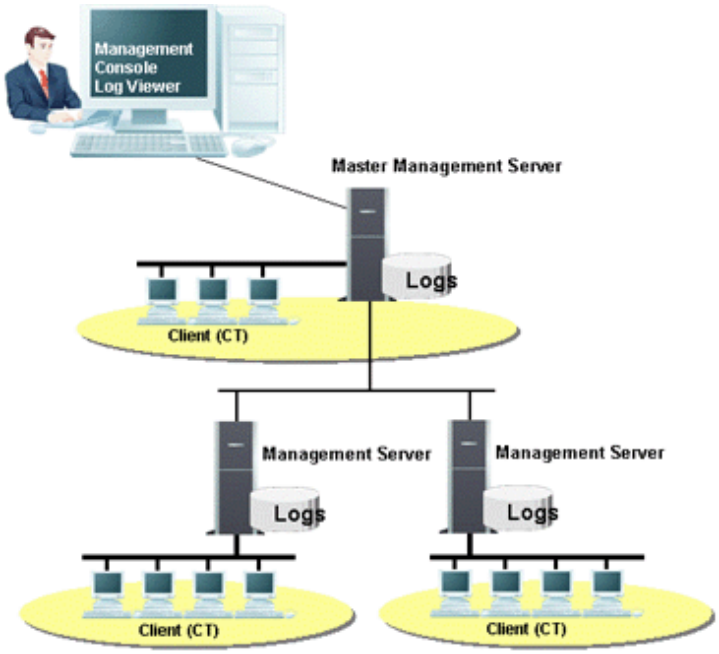
2-Level System Structure

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



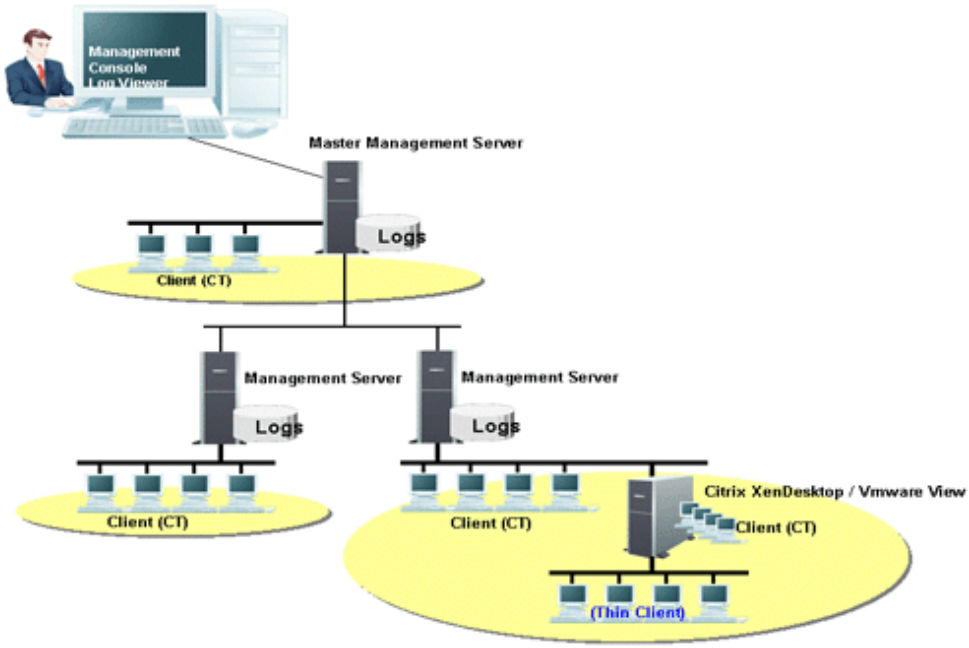
3-Level System Structure

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



3-Level System Structure (with Virtual Environment)

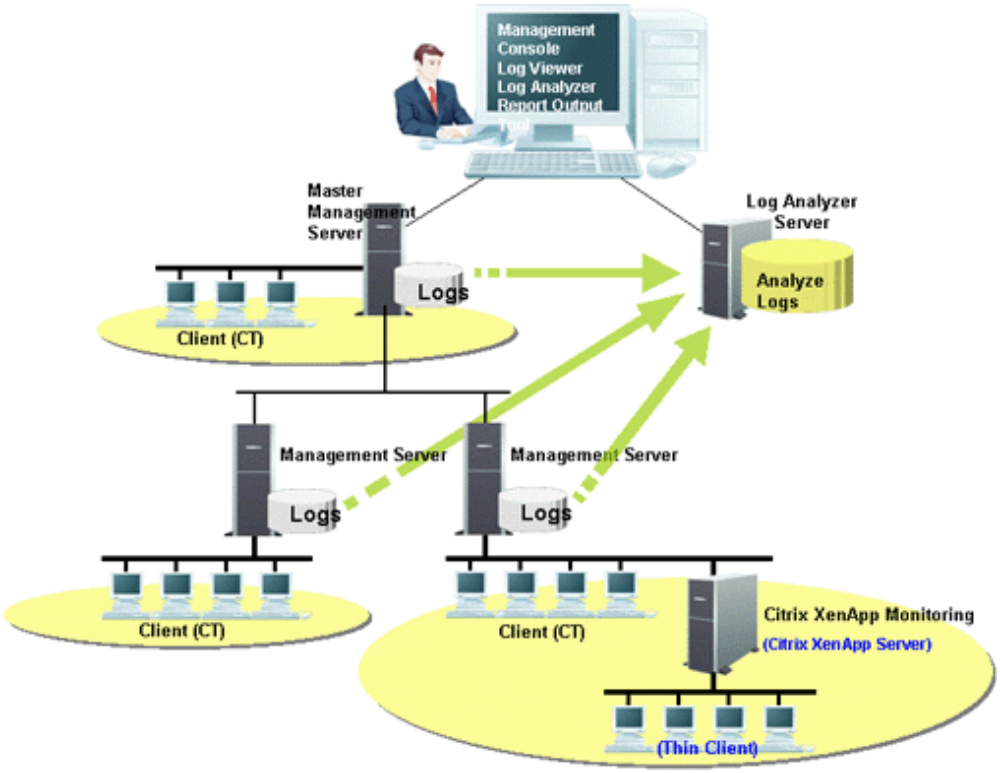
This is a structure in which the master management server is set for managing multiple management servers and the client (CT) is installed to the Citrix XenDesktop™ and VMware View™ environment.



3-Level System Structure (with Log Analysis/Report Output and Citrix XenApp Monitoring)

The Citrix XenApp Monitoring function is not available.

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 while the monitoring function of Citrix XenApp is used.



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, please refer to the "Systemwalker Desktop Keeper User's Guide: for Administrators".

2.1 Prohibition Function

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.

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 not available.

This sets the group that prohibits logon. 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, the use of the file export utility and the execution of encryption. When the prohibited operation is being performed, a prohibition log will not be recorded.

E-mail File Attachment Prohibition

This function is not available.

This prohibits the prohibited file from being attached to an E-mail for sending and saving (notes). When the prohibited operation is being performed, a prohibition log will be recorded.

Notes: The saving prohibition can only be used in a compatible mode of V12.0L20-V13.0.0.

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.

2.2 Record Function

The operations in the client (CT) can be collected as logs and recorded to the master management server and management server. The logs to be collected can be set through the management console.

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
- Terminate E-mail sending (**This function is not available.**)
- Command line operation **(This function is not available.)**
- 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 opeartion (upload, download)
- Web opeartion (upload, download)
- Clipboard operation
- Attached data (screen capture, original file, E-mail content)

Record Device Configuration Change

When devices are added, such as the installation of USB memory, 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.

- 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 can:

- Set client (CT) policy
- Search/View the collected logs
- Receive notifications when illegal operations occur in the client (CT)
- Backup/Recover the database that stores the collected logs
- See status display

Define Policy

This refers to defining of CT policy and user policy on the management server, distributing of policies to the client (CT) and the definition of logs collected from the client (CT).

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

- CT Policy

  This is the policy set in the client (CT) unit.

- 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).

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

The types, setting methods and application scope of CT policy are different from those of user policy. Please refer to "Systemwalker Desktop Keeper User's Guide: for Administrators" 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 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.

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.

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).

Status display

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

Notification to Client (CT)

This function is not available.

By notifying the client (CT) the paper usage status, the personal awareness of cost reduction can be improved.

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

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.

- Related reports of all-in-one machine

  This function is not available.

  According to the information collected by the all-in-one machine, the conversion results of paper usage volume and CO2 emission can be output into a report.

  By reporting the volume of paper used by each all-in-one machine or each person, visualizing the changes of actual performance and prohibiting unnecessary printing, contributions can be made for reducing printing costs and CO2 emissions.

  In addition, as the usage condition of all-in-one machine will also be output, reducing the number of all-in-one machines and changing to the low function model with lower maintenance fees is also a useful way to use the material to reduce operation cost.

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.

   - Worst 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. Improvment 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 worst 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

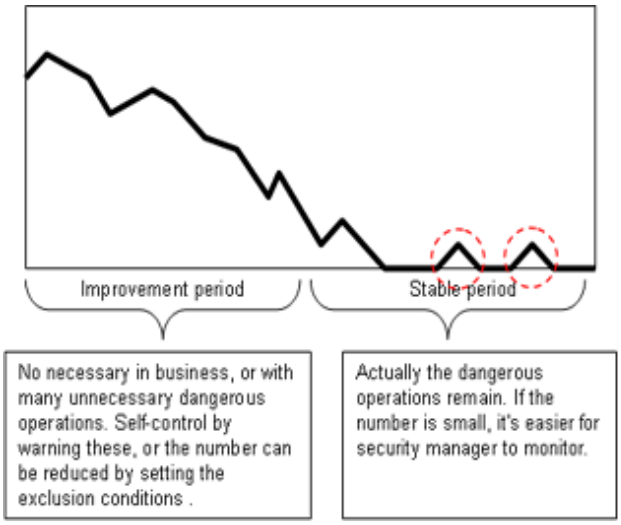
      The comments in the report show the trend of improvement and deterioration in the long term.

      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

  Pentium®4 or Xeon® 1GHz or higher (Note)

- Memory (Note 1)

  At least 1GB (excluding OS)

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

  - Database system (added by Systemwalker Desktop Keeper)

    At least 250MB

  - Database space

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

  - Backup file space

    ```
    The entire log CSV file = average record length (byte) × the number of clients × backup time
    (days) × number of operation logs per day (piece/day) * the average record length is 400 bytes.
    ```

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

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

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

    The space for saving backup data of original files should be set according to the terminal operation settings of the Management Console. The initial value is 50MB.

  - 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, please 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

(Note 1) The requirement for memory and disk capacity may change according to system structure, scale and available resources.

Note

Issues to be considered according to the capacity of installation drive of database-related folders

Please specify a drive that can be guaranteed to have the following capacity to be the installation drive of database-related files.

- Program of database system: about 500MB.
- Work space during backup (used during operation only)

  A space of about 8GB is required for processing 10 million records, so please figure out the required space according to the number of records to be processed.

```
Number of records × 400 (average record length) × 2 (coefficient)
```

  For example, to backup a maximum of 10 million tables,

```
10 million × 400 bytes × 2 = about 8GB
```

- Work space during restoration (used during operation only)

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

Log Analyzer Server

- CPU

  Pentium®4 or Xeon® 1GHz or higher (Notes)

- Memory (Note 1)

  At least 2GB (excluding OS)

- Hard Disk Capacity

  At least 320MB

- Disk capacity for database (Note 1)

  For information on how to estimate capacity, please refer to “3.1.2 Estimating Database Capacity”

  (Note 1) The requirements for memory and disk capacity may change according to system structure, scale and available resources.

Management Console

- CPU

  Pentium®III 600MHz or higher

- Memory (Note 1)

  At least 256MB (excluding OS)

- Hard disk capacity

  At least 20MB

Note

Logs cannot be displayed in the following cases:

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

If the number of logs reaches 100,000, memory of 100,000 × 7.5KB= 750MB 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

  Pentium4 2GHz or higher

- Memory (Note 1)

  At least 512MB (including OS)

- Hard disk capacity

  At least 50MB

- Disk capacity for log output (Note 1)

  The following disk capacity is required

```
400 bytes × output logs
```

(Note 1) The requirements for memory and disk capacity may change according to system structure, scale and available resources.

Client (CT)

- CPU

  Pentium®III 600MHz or higher

- Memory (Notes 1)

  At least 64MB (excluding OS)

- Hard disk capacity

  At least 88MB

  At least 850MB (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)	15MB	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 50MB, the screen capture data will not be collected.
Attached data (backup original file data)	700MB	If the original file backup function is used when exporting files using the file export utility, the attached data will be

Item Name	Required Disk Capacity	Description
		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)	50MB	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.
Violation log	10MB	If the client (CT) cannot be connected with the Master Management Server or Management Server, the violation 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 100MB, multiple new files can be created. The maximum size of a file is 10MB. Besides, if the available capacity of the drive in which the folder for saving violation logs is located is less than 100MB, the following violation logs will be deleted. The drive for saving violation 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	30MB	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 200MB, multiple new files can be created. The maximum size of a file is 30MB. Besides, if the available capacity of the drive in which the folder for saving violation logs is located is less than 200MB, the following violation 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>
Error log	60MB	On the client (CT), the initial setting of operation records and error information is a maximum if 2MB per day over a period time of 30 days, so a maximum of 60MB can be saved in total. Thus, the capacity is 60MB. The capacity of the error log can be changed. For the change method, please refer to “Systemwalker Desktop Keeper 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	3MB	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

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 months for saving operation logs
- Number of non-file operation logs
- Number of file operation logs
- Amount of attached data
- Capacity for saving E-mails

In 3-level structure

- Number of the clients (CTs) in total
- 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
- Amount of attached data
- Capacity for saving E-mails

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 and when using the Citrix XenApp monitoring function, please add the number of users connecting to the virtual environment as the number of CTs.

Number of clients (CTs) 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.

Number of non-file operation logs

This is the total number of all events excluding file operation executed at one client 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	The number of obtained logs
Application Startup Log	Yes	The number of times an application has been started [For example] The count is "1" when an application is started once.
Application Termination log	Yes	The number of times an application has been terminated. [For 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. [For 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. [For example] The count is "1" when one E-mail has been sent.
E-mail Sending Suspension Log	Yes	The number of times E-mail sending to unauthorized domains has been suspended. [For 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. [For example] The count is “1” when the command has been executed once.
Device Configuration Change Log	Yes	The number of times a device has been added. [For example] The count is "1" when a device has been added once.
Printing Operation Log	Yes	The number of times printing has been used. [For 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

Operation Log Type	Selectable	The number of obtained logs
		[For example] The count is “1” when one file has been exported.
File Operation Log	Yes	The number of times file operations have occurred. [For example] The count is "1" when one file has been created/viewed/ overwritten/copied/moved/deleted once.
External Application Log	Yes	The number of times logs are sent by external applications. [For example] The count is "1" when a log has been sent by an external 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. [For example] The count is "1" when having logged onto a windows system once.
PrintScreen Key Operation Log	Yes	The number of times the PrintScreen key is pressed. [For 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. [For 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. [For 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. [For example] The count is “2” when clipboard is used for copying from the virtual terminal to the physical terminal once.
Violation Log	No	The number of times a logon prohibited group has been logged on. [For 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. [For example] The count is "1" when a Startup Prohibited Application has been started once.

Operation Log Type	Selectable	The number of obtained logs
		The number of times a Disabled PrintScreen Key is pressed. [For 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. [For 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. [For 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. [For example] ・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 [For example] The count is "1" when the prohibited FTP server has been accessed once.
		The number of times the prohibited clipboard has been used [For example] The count is "1" when the prohibited clipboard has been used once.
Others (configuration change log)	No	The number of times policy configuration has been changed via the Management Console. [For example] The count is "1" when the File Export Prohibition policy has been changed on one client (CT) via the Management Console.

If "Selectable" is indicated as "Yes", it means that the "Operation Log Type" can be configured in the [Log Switches] tab via the Management Console.

Amount of attached data

This is the total value of screen capture data capacity, backup original data capacity and clipboard data capacity.

Capacity for saving E-mails

This is the file size capacity including both E-mail text and file attachments.

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), 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)	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	10,705MB	44,960MB

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

Number of the clients (CTs)	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	18,534MB	86,674MB

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: 150K (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)) × 2 (capture times/day) × 90 (days to save) × 150KB = 26GB
```

Data capacity of backup original file

This section describes data capacity of backup original files.

Data capacity of the backup original file is the same as the capacity of the exported file.

Example 1) When attached data are saved to server

When exporting 10MB files from the client (CT), the 10MB 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 10MB files from the client (CT), the 10MB 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: 150K (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)) × 2 (times of clipboard operation per day) × 90 (days to save) ×
150KB × 2 (collect in virtual/physical environment) = 52GB
```

Example 2) When text data is copied via clipboard

Text data at 1 operation: 1K

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

Example 3) When files are copied through clipboard

File path at 1 operation: 80B

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)) × 2 (times of clipboard operation per day) × 90 (days to save) ×
80B × 2 (collect in virtual/physical) = 28MB
```

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	17,547MB	28,190MB

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	160,166MB	266,596MB

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× number of clients × (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 × (number of non-file operation logs+ number of file operation logs)
```

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 × (1000+ 500) × 500 × 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.

However, this product cannot be operated under IPv6. Please use it in the IPv4 operating environment.

Management Server/Master Management Server

- Microsoft® Windows Server® 2003, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack 2
- Microsoft® Windows Server® 2003, Standard x64 Edition Service Pack 2 (Note 2)
- Microsoft® Windows Server® 2003, Enterprise x64 Edition Service Pack 2 (Note 2)
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition Service Pack 2 (Note 2)
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Service Pack 2 (Note 2)
- Microsoft® Windows Server® 2008, Standard Edition (Without Service Pack/ 2) (Note 2)(Note 3)
- Microsoft® Windows Server® 2008, Enterprise Edition (Without Service Pack/2) (Note 2)(Note 3)
- Microsoft® Windows Server® 2008 Standard without Hyper-V™ (Without Service Pack/ 2) (Note 2)(Note 3)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ (Without Service Pack/ 2) (Note 2)(Note 3)
- Microsoft® Windows Server® 2008 R2 Standard (Without Service Pack/1) (Note 2)(Note 3)
- Microsoft® Windows Server® 2008 R2 Enterprise (Without Service Pack/1) (Note 2)(Note 3)
- Microsoft® Windows Server® Small Business Server 2011 Essentials (Note 2)(Note 3)

  Notes 1) Microsoft Data Access Components (MDAC) 2.7 Sp1 Refresh or higher is required.

  Notes 2) x64 Edition should be operated under 32-bit compatible mode.

  Notes 3) Server Core cannot be used.

Log Analyzer Server

- Microsoft® Windows Server® 2003, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack 2
- Microsoft® Windows Server® 2003, Standard x64 Edition Service Pack 2 (Note 1)
- Microsoft® Windows Server® 2003, Enterprise x64 Edition Service Pack 2 (Note 1)
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition Service Pack 2 (Note 1)
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Service Pack 2 (Note 1)
- Microsoft® Windows Server® 2008, Standard Edition (Without Service Pack/ 2) (Note 1)(Note 2)
- Microsoft® Windows Server® 2008, Enterprise Edition (Without Service Pack/ 2) (Note 1)(Note 2)
- Without Microsoft® Windows Server® 2008 Standard Hyper-V™ (Without Service Pack/ 2) (Note 2)
- Without Microsoft® Windows Server® 2008 Enterprise Hyper-V™ (Without Service Pack/ 2) (Note 2)
- Microsoft® Windows Server® 2008 R2 Standard (Without Service Pack/ 1) (Note 1)(Note 2)

- Microsoft® Windows Server® 2008 R2 Enterprise (Without Service Pack/ 1) (Note 1)(Note 2)
- Microsoft® Windows Server® Small Business Server 2011 Essentials (Notes 1)(Notes 2)

  Notes 1) x64 Edition should be operated under 32-bit compatible mode.

  Notes 2) Server Core cannot be used.

Management Console

- Microsoft® Windows® XP Professional Service Pack 2/3 (Note 1)
- Microsoft® Windows Server® 2003, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack 2
- Microsoft® Windows Server® 2003, Standard x64 Edition Service Pack 2 (Note 2)
- Microsoft® Windows Server® 2003, Enterprise x64 Edition Service Pack 2 (Note 2)
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition Service Pack 2 (Note 2)
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition Service Pack 2 (Note 2)
- Windows Vista® Business (Without Service Pack /1/ 2) (Note 1)
- Windows Vista® Enterprise (Without Service Pack /1/2) (Note 1)
- Windows Vista® Ultimate (Without Service Pack /1/2) (Note 1)
- Windows® 7 Ultimate (Without Service Pack /1) (Note 2)
- Windows® 7 Enterprise (Without Service Pack /1) (Note 2)
- Windows® 7 Professional (Without Service Pack /1) (Note 2)
- Microsoft® Windows Server® 2008, Standard Edition (Without Service Pack /2) (Note 2)(Note 3)
- Microsoft® Windows Server® 2008, Enterprise Edition (Without Service Pack /2) (Note 2)(Note 3)
- Without Microsoft® Windows Server® 2008 Standard Hyper-V™ (Without Service Pack/2) (Note 3)
- Without Microsoft® Windows Server® 2008 Enterprise Hyper-V™ (Without Service Pack/2) (Note 3)
- Microsoft® Windows Server® 2008 R2 Standard (Without Service Pack /1) (Note 2)(Note 3)
- Microsoft® Windows Server® 2008 R2 Enterprise (Without Service Pack /1) (Note 2)(Note 3)
- Microsoft® Windows Server® Small Business Server 2011 Essentials (Note 2)(Note 3)

  Note 1) x64 Not compatible with x64 Edition of Windows® XP and Windows Vista®

  Note 2) x64 Edition should be operated under 32-bit compatible mode.

  Note 3) Server Core cannot be used.

Client (CT)

- Microsoft® Windows® XP Professional Service Pack 2/3 (Note 1)
- Microsoft® Windows® XP Home Edition Service Pack 2/3
- Microsoft® Windows Server® 2003, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003, Enterprise Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Standard Edition Service Pack 2
- Microsoft® Windows Server® 2003 R2, Enterprise Edition Service Pack 2

- Windows Vista® Home Basic (Without Service Pack /1/2)
- Windows Vista® Home Premium (Without Service Pack /1/2)
- Windows Vista® Business (Without Service Pack /1/2)
- Windows Vista® Enterprise (Without Service Pack /1/2)
- Windows Vista® Ultimate (Without Service Pack /1/2)
- Windows® 7 Ultimate (Without Service Pack /1)
- Windows® 7 Enterprise (Without Service Pack /1)
- Windows® 7 Professional (Without Service Pack /1)
- Windows® 7 Home Premium (Without Service Pack /1)
- Microsoft® Windows Server® 2008, Standard Edition (Without Service Pack /2) (Note 1)
- Microsoft® Windows Server® 2008, Enterprise Edition (Without Service Pack /2) (Note 1)
- Microsoft® Windows Server® 2008 Standard Hyper-V™ (Without Service Pack /2) (Note 1)
- Microsoft® Windows Server® 2008 Enterprise Hyper-V™ (Without Service Pack /2) (Note 1)
- Microsoft® Windows Server® 2008 R2 Foundation (Without Service Pack /1) (Note 1)
- Microsoft® Windows Server® 2008 R2 Standard (Without Service Pack /1) (Note 1)
- Microsoft® Windows Server® 2008 R2 Enterprise (Without Service Pack /1) (Note 1)
- Microsoft® Windows Server® Small Business without Server 2011 Essentials (Note 1)

  Note 1: Server Core cannot be used.

Note

Functional restrictions relating to OS

[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 Vista® Home Basic
- Windows Vista® Home Premium
- Windows Vista® Business
- Windows Vista® Enterprise
- Windows Vista® Ultimate
- Microsoft® Windows® XP Professional (Note 1)
- Microsoft® Windows® XP Home Edition

Note 1: Not compatible with x64 Edition

[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 Vista® Home Basic
- Windows Vista® Home Premium
- Windows Vista® Business
- Windows Vista® Enterprise
- Windows Vista® Ultimate

[64-bit OS that can use E-mail sending log recording and E-mail file attachment prohibition function]

- Microsoft® Windows Server® 2008, Standard Edition (Without Service Pack/2)
- Microsoft® Windows Server® 2008, Enterprise Edition (Without Service Pack/2)
- Microsoft® Windows Server® 2008 R2 Standard
- Microsoft® Windows Server® 2008 R2 Enterprise
- Microsoft® Windows Server® Small Business Server 2011 Essentials
- Windows® 7 Ultimate
- Windows® 7 Enterprise
- Windows® 7 Professional
- Windows® 7 Home Premium
- Windows Vista® Home Basic
- Windows Vista® Home Premium
- Windows Vista® Business
- Windows Vista® Enterprise
- Windows Vista® Ultimate

[Functions cannot be used in the OS installed with Microsoft Internet Explorer 6®]

The following functions cannot be used in the OS installed with Microsoft Internet Explorer 6®:

- Log collection for FTP operations (FTP upload log, FTP download log and FTP server connection prohibition log)
- Log collection for Web operations (Web upload log, Web download log, URL access prohibition log, Web upload prohibition log and Web download prohibition log)
- FTP operation prohibition (\FTP server connection prohibition)
- Web operation prohibition (URL access prohibition, Web upload prohibition and Web download prohibition)

Report Output Tool

- Microsoft® Windows® XP Professional Service Pack 2/3 (Note 1)
- Windows Vista® Business (Without Service Pack /1/2) (Note 1)
- Windows Vista® Enterprise (Without Service Pack /1/2) (Note 1)
- Windows Vista® Ultimate (Without Service Pack /1/2) (Note 1)
- Windows® 7 Ultimate (Without Service Pack /1) (Note 2)
- Windows® 7 Enterprise (Without Service Pack /1) (Note 2)

- Windows® 7 Professional (Without Service Pack /1) (Note 2)

Note 1: Not compatible with x64 Edition

Note 2: x64 Edition should be operated under 32-bit compatible mode.

3.2.2 Necessary Software

Software required by Systemwalker Desktop Keeper is as follows.

Necessary software

Common

One of the following is required:

- Windows® Internet Explorer® 7
- Windows® Internet Explorer® 8
- Windows® Internet Explorer® 9

Management Server/Master Management Server

Software required for installing a Management Server is as follows:

Microsoft Data Access Components (MDAC) 2.7 Sp1 Refresh or higher

(Web server)
One of the following is required:

- Internet Information Services 6.0
- Internet Information Services 7.0
- Internet Information Services 7.5

[Log Analyzer Server]

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

- Microsoft® .NET Framework 2.0 or higher
- Microsoft Data Access Components (MDAC) 2.8 or higher

[Report Output Tool]

Software required in the PC for installing report output tool is as follows:

- Microsoft Data Access Components (MDAC) 2.8 or higher

Also, one of the following is required:

- Microsoft® Office Excel 2007 (installation of "Virtual Basic for Applications" of "Office share function" is required)
- Microsoft® Office Excel 2010 (excluding "Web Edition")

[Web Console]

One of the following is required in the PC that uses the Web console:

- Microsoft® Internet Explorer® 6 ServicePack 1
- Windows® Internet Explorer® 7
- Windows® Internet Explorer® 8
- Windows® Internet Explorer® 9

Related Software

The following software is required when sharing structure information:

- Systemwalker Desktop Patrol V14g (V14.2.0)
-
- One of the following software is required when using on a virtual OS.

Operating Environment of Management Server/Master Management Server

- VMware Infrasructure 3
- VMware vSphere 4
- Microsoft Hyper-V
- Windows Server 2008 R2&SCVMM 2008 R2

Client (CT)

- VMware Infrasructure 3
- VMware vSphere 4
- VMware View 3
- VMware View 4
- Citrix XenDesktop 4.0
- Citrix XenDesktop 5.0
- Microsoft Hyper-V
- Windows Server 2008 R2&SCVMM 2008 R2

3.2.3 Database

Symfoware Server will be bundled to Systemwalker Desktop Keeper as a database. During the installation of components, various functions of Symfoware Server will be automatically installed.

- When installing the Management Server or the Log Analyzer Server, the following functions of Symfoware Server will be automatically installed:
  - Server functions of Symfoware Server
  - Client functions of Symfoware Server
- When installing the report output tool, the following functions of Symfoware Server will be automatically installed:
  - Client functions of Symfoware Server

Apart from being bundled with Symfoware Server, Systemwalker Desktop Keeper can also use the following Symfoware Server products as a database:

- Windows Edition Symfoware Server Enterprise Edition V10.1.0 (x86/x64 Edition)
- Windows Edition Symfoware Server Enterprise Edition V9.1.1 (x86/x64 Edition)
- Windows Edition Symfoware Server Enterprise Edition V8.0
- Windows Edition Symfoware Server Enterprise Edition V7.0
- Windows Edition Symfoware Server Enterprise Edition V6.0

If the server function and client function of Symfoware Server of the above products are installed during the installation of components, the bundled Symfoware Server cannot be installed.

When the server function and client function of Symfoware Server of the above products are not installed, if the version of the installed Symfoware Server products is consistent with that of the bundled Symfoware Server, the functions will be automatically installed.

In addition, because the reason for failure in automatic installation is the installation error, please install server functions and client functions of Symfoware Server with the same version as the installed Symfoware Server products.

When Symfoware Server Enterprise Edition V9.1.1/V10.1.0 (x64 Edition) for Windows is used, please install before the installation of the Management Server, Master Management Server and Log Analyzer Server. If the Management Server, Master Management Server and Log Analyzer Server are installed first, they cannot coexist with the Symfoware Server.

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 9.2.0

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 coexisted with the Management Server / Master Management Server:

- Systemwalker Desktop Monitor V10.0
- Systemwalker Centric Manager V12.0 Earlier Editions (Note 1)
- Systemwalker Centric Manager V13.0.0 ~ V13.2.0 Operation Management Server (Note 2)
- Systemwalker Centric Manager V13.3.0 ~ V13.3.1 Operation Management Server (Note 3)
- Systemwalker Centric Manager (x86 Edition) V13.4.0 Operation Management Server (Note 3)
- Systemwalker Centric Manager (x64 Edition) V13.4.0 Operation Management Server
- Systemwalker Centric Manager (x64 Edition) V13.5.0 Operation Management Server (Note 4)
- Symfoware Server Enterprise Edition V5.0 or earlier
- Symfoware Server Standard Edition All versions
- Symfoware Server Base Edition All versions
- Symfoware Server for Windows All versions
- Symfoware Server for WindowsNT All versions
- SymfoWARE Programmer's Kit All versions
- Symfoware Server Connection Manager V8.0.0
- Products that are bundled with Symfoware Server Enterprise Edition (x64 Edition)(Note 6)

Note 1: Conditions for coexistence

- They can coexist when "HelpDesk client (ODBC)" is not installed in the section server or business server that has Systemwalker Centric Manager V12.0 or earlier installed.

- Coexistence is possible when neither "HelpDesk client (ODBC)" nor "HelpDesk database" is installed in the HelpDesk server that has Systemwalker Centric Manager V12.0 or earlier installed.

Please confirm the installation information of Systemwalker Centric Manager by using "Product Information Display Command". For information on how to use "Product Information Display Command", please refer to "Systemwalker Centric Manager Reference Manual".

Note 2: Conditions for coexistence

- Coexistence is possible when Systemwalker Desktop Keeper is installed prior to Systemwalker Centric Manager.
- When Systemwalker Desktop Keeper is installed after Systemwalker Centric Manager, it is not possible to coexist when "HelpDesk Client (ODBC)" of Systemwalker Centric Manager has been installed. When "HelpDesk Client (ODBC)" is not installed, please perform additional installation according to the reference manual of Systemwalker Centric Manager.

Please confirm the installation information of Systemwalker Centric Manager by using "Product Information Display Command". For information on how to use "Product Information Display Command", please refer to "Systemwalker Centric Manager Reference Manual".

Note 3: Conditions for coexistence

Coexistence is possible when Systemwalker Desktop Keeper is installed prior to Systemwalker Centric Manager.

Note 4: Conditions for coexistence

Coexistence is possible when Systemwalker Desktop Keeper is installed after Systemwalker Centric Manager.

Note 6: Conditions for coexistence

- Coexistence is possible when Symfoware Server Enterprise Edition V10.1.0 (x64 Edition) is bundled and it is installed before Systemwalker Desktop Keeper.
- Coexistence is possible when Symfoware Server Enterprise Edition V9.1.1 (x64 Edition) is bundled and the following conditions are satisfied:
  - Symfoware Server Client Function has been installed.
  - It is installed prior to Systemwalker Desktop Keeper.

Products That Cannot Coexist with Client (CT)

- The attached tool of Systemwalker Desktop Patrol contains an external storage media write protection tool.
  Please use the file export utility of Systemwalker Desktop Keeper.
- SecureKeeper (Product of Fujitsu China Systems)

Products That Cannot Coexist with Log Analyzer Server

The following products cannot coexist with the Log Analyzer Server:

- Systemwalker Desktop Monitor V10.0
- Systemwalker Centric Manager V12.0 or earlier (Note 1)
- Systemwalker Centric Manager V13.0.0 ~ V13.2.0 Operation Management Server (Note 2)
- Systemwalker Centric Manager V13.3.0 ~ V13.3.1 Operation Management Server (Note 3)
- Systemwalker Centric Manager(x86 Edition) V13.4.0 Operation Management Server (Note 3)
- Systemwalker Centric Manager(x64 Edition) V13.4.0 Operation Management Server
- Systemwalker Centric Manager(x64 Edition) V13.5.0 Operation Management Server (Note 4)
- Symfoware Server Enterprise Edition V5.0 All versions
- Symfoware Server Standard Edition All versions

- Symfoware Server Base Edition All versions
- Symfoware Server for Windows All versions
- Symfoware Server for WindowsNT All versions
- Symfoware Server Client V5.0 or earlier
- SymfoWARE Programmer's Kit All versions
- Symfoware Server Connection Manager V8.0.0
- Products that are bundled with Symfoware Server Enterprise Edition (x64 Edition)(Note 5)

Note 1: Conditions for coexistence

- Coexistence is possible when "HelpDesk client (ODBC)" is not installed in the section server or business server that has Systemwalker Centric Manager V12.0 or earlier installed.
- Coexistence is possible when neither "HelpDesk client (ODBC)" nor "HelpDesk database" is installed in the HelpDesk server that has Systemwalker Centric Manager V12.0 or earlier installed.

Please confirm the installation information of Systemwalker Centric Manager by using "Product Information Display Command". For information on how to use "Product Information Display Command", please refer to "Systemwalker Centric Manager Reference Manual".

Note 2: Conditions for coexistence

- Coexistence is possible when Systemwalker Desktop Keeper is installed prior to Systemwalker Centric Manager.
- When Systemwalker Desktop Keeper is installed after Systemwalker Centric Manager, it is not possible to coexist when "HelpDesk Client (ODBC)"of Systemwalker Centric Manager has been installed. When "HelpDesk Client (ODBC)" is not installed, please perform additional installation according to the reference manual of Systemwalker Centric Manager.

Please confirm the installation information of Systemwalker Centric Manager by using "Product Information Display Command". For information on how to use "Product Information Display Command", please refer to "Systemwalker Centric Manager Reference Manual".

Note 3: Conditions for coexistence

Coexistence is possible when Systemwalker Desktop Keeper is installed prior to Systemwalker Centric Manager.

Note 4: Conditions for coexistence

Coexistence is possible when Systemwalker Desktop Keeper is installed after Systemwalker Centric Manager.

Note 5: Conditions for coexistence

- Coexistence is possible when Symfoware Server Enterprise Edition V10.1.0 (x64 Edition) is bundled and it is installed prior to Systemwalker Desktop Keeper.
- Coexistence is possible when Symfoware Server Enterprise Edition V9.1.1 (x64 Edition) is bundled and the following conditions are satisfied:
  - The Client function of Symfoware Server has been installed.
  - It is installed before Systemwalker Desktop Keeper.

Products Cannot Coexist with Report Output Tool

The following products cannot coexist with the Report Output Tool:

- Symfoware Server Client V5.0 or earlier

Chapter 4 Link with Other Products

Systemwalker Desktop Keeper can be linked with the following products:

- Systemwalker Desktop Patrol

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, please refer to "Determine the installation method of client (CT)" and "Installation by using Systemwalker Desktop Patrol" of "Systemwalker Desktop Keeper 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, please refer to "Systemwalker Desktop Keeper User's Guide: for Administrators".
  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, please 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.
  The import and export of structure information can be performed through the Management Console of Systemwalker Desktop Keeper. (Systemwalker Desktop Patrol V14.2.0 or lower)

- 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)

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.

Citrix XenApp ServerTM

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 XenApp Client

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

Citrix XenDesktopTM

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.

VMware ViewTM

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.

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 Version

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

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.

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.

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.

Legal Size

Legal size mainly refers to the paper size used in the United States (8.5×14 inch).

Letter Size

Letter size mainly refers to the paper size used in the United States (8.5×11 inch).

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.

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 Inspection

Systemwalker Desktop Inspection is the software that controls network devices through the client inspection to achieve network inspection.

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 Keeper V14g).

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 V14g.

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 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.

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.

UNC (Universal Naming Convention)

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

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 5.5(but only use in Microsoft® Windows® 2000 Professional operating system)
- Microsoft® Outlook® Express 6.0
- Microsoft® Outlook® 2000
- Microsoft® Outlook® 2002
- 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.

Web Console (State Interface)

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

Web Console (Log Analyzer)

This is used for viewing the result of aggregation and analysis in log analysis 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.

Collective Management

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

Level Control Service

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

Operation Database

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

Log Viewing Database

This is the database for restoring and viewing the log information that is less frequently used.

Group Policy

Policy set in the unit of a CT group.

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.

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.

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.

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.

Self-decrypting Encryption

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.)

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.

Backup Management Server

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

Drive Letter

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

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.

Manage by Section

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

Policy

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

Aggregate by Objectives

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

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 a self-decrypting file according to the settings of the management console.

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 Policy

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

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 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.

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.

Log Analyzer Server

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

Index

[Special characters]

[OS that can use CD-R/RW media export function].....30
[OS that can use DVD-R/RW media export function].....30

[A]

Amount of attached data.....24
Attached Data.....11

[C]

Changed Functions.....2
Client (CT).....6
Client (CT).....19,29
Conditions for coexistence.....34,36
Configuration Components.....5

[D]

Database.....33
Data capacity of backup original file.....25
Define Policy.....11

[E]

E-mail Notification.....12
Estimating Database Capacity.....21,25
Estimating database capacity.....26
Estimating temporary disk capacity required for sending log data 27
Estimating the capacity of screen capture data.....25
Example of calculating temporary disk capacity.....27

[F]

Function of counting by purpose.....13

[H]

Hard Disk / Memory Requirements.....17
Hardware.....17

[L]

Level Management.....12
Link with Other Products.....37
Log Analysis Function.....12
Log Analysis Report.....13
Log Analyzer.....6
Log Analyzer Server.....6,18,26,28
Log Filter.....11
Log Viewer.....6

[M]

Management Console.....6,18,29
Management Function.....11
Management Server.....5
Management Server/Master Management Server.....17,21,28
Master Management Server.....6

[N]

Necessary Software.....32
Necessary software.....32
New Functions.....2
Number of clients (CTs).....21
Number of clients (CTs) in total.....22
Number of file operation logs.....22
Number of months to save operation logs.....22
Number of non-file operation logs.....22

[O]

Operating Environment.....17
OS.....28

[P]

Prevention and Diagnosis Function against Information Disclosure.....12
Printer.....21
Product Positioning.....1
Products Cannot Coexist with Report Output Tool.....36
Products that cannot be used in Mixture.....34
Products That Cannot Coexist with Client (CT).....35
Products That Cannot Coexist with Log Analyzer Server.....35
Products that cannot coexist with Management Server･Master Management Server.....34
Prohibition Function.....9

[R]

Record Function.....10
Record to Event Log.....12
Related Software.....33
Report for Green IT Policy.....14
Report Output Function.....13
Report Output Tool.....6,19,31

[S]

Self Version Management.....12
Software environment.....27
System Structure.....5
Systemwalker Desktop Patrol.....37

[T]

Temporary disk capacity.....27

[V]

View, Search and Trace Logs.....11