FUJITSU Software

Systemwalker Desktop Keeper V15

Software that prevents leakage of information from clients

Systemwalker Desktop Keeper can record client operations to deter problematic activity, and can prevent leakage of electronic information within the organization. It also allows safe use of smart devices (Android, iOS).

Detect, trace, identify, audit, and analyse leakage

Operations are retrieved as logs from clients, and recorded on Management Server

- Application startup/exit
- Window titles and URL accessed via the web
- Print-via-spool information (print time,
- document name, etc.)File operations performed on file servers and
- local devicesDevice configuration changes during operation
- (Plug & Play, USB device mounts, etc.)
- Smart device (Android) operations, etc.

Policy settings

Store originals of files exported to external memory

The contents of exported files are stored together with operation logs. The contents of files intentionally or mistakenly exported can be checked at a later time.

Tracing of unauthorized operations and identification of users

Searches, such as specifying keywords, period, timeframe, or day, can be performed for the recorded or collected logs, enabling identification of clients or users that are performing a specific operation. When able to identify files that have a risk of information leakage or being exported to an external location, it is possible to ascertain what kind of operations were performed on the applicable files, and whether they were printed.

Prohibit unauthorized operations and prevent export/import of data

Forcibly prohibit various types of operations on clients

- Starting up applications not related to work
- Disabling the PrintScreen key
- Printing from unapproved applications
- Writing to external memory (DVD/CD/USB devices, etc.)
- Writing to network drives
- Using unapproved USB devices
- Accessing unapproved URLs
- Downloading from/uploading to a web server
- Accessing an FTP server (upload/download)
- Prohibition of smart device (Android) operations (Wi-Fi connections, connecting to Bluetooth devices, starting up applications)
- Restricting execution of smart device applications (can specify times) (Android)
- Remote lock or wipe (Android/iOS)

File export prohibition settings



Comprehensive management features reduce the TCO

Checking the effectiveness of implementing measures to prevent information leakage Logs can be analyzed from various perspectives. Unauthorized operations, export operations, and so on, can be checked, realizing visualization of the information leakage measures. Also, violation operations can be ranked by device, and the number of violations and violation contents can be ascertained by group and by device within a group.

Flexible operation of security policies

Policies can be configured for clients in batch from Management Console. Policies can be configured by client and also by user. Even when a client is shared by multiple users, the prohibition level can be switched according to user. Moreover, devices can be controlled according to whether they are individually-owned or company-owned.

Improved convenience by allowing temporary release of export restrictions

There are cases where it is necessary to export files for business purposes. In such cases, a period or timeframe can be specified within which file exporting is temporarily permitted. When the permitted period expires, the restrictions resume automatically, so there is no need to worry

resume automatically, so there is no need to worry about remembering to put the restrictions back in place.

File Export Prohibition - File Export Utility function setting

And the second	and the second se
Settings of File Export Utility function	
T Unable to start the format function	
Capitary anty removable devote and DVD/CD	as export destination
The season for export	
Set the date on which File Export Utility can be in	urted .
T Limit period for use	
	/ (00000000)
T Sent time for use	
00 c 00 - [23 c 10 pe	(mail)
The day of a week on which it can be used	
Sun Morr Tue Wed Thu Fit Sat The day	
DDDDDDD been	of a view that is not selected has nothing to the above setting Uhable to use.
Date and Time Confirmation Method	
d harristanerore Dalle br	ent uners a suble to determ
C trail out that strend is some	
ingan and a summit a	C
minute Author & Concern R.	Casteriostics N-
For Province	
War Contractor	(m ²)
Set	Cancel

Displaying a list of the client status

The operating status of clients can be ascertained at a glance in the top window, and can be managed with ease.

Furthermore, it is possible to identify clients with security policy violations, such as prohibited operations, file exports, and suspicious access, or other issues.

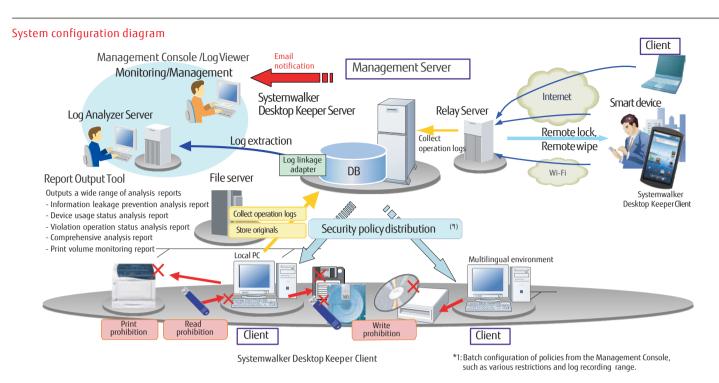
Display items (can be selected)

- Clients that are being used outside of normal hours
- Clients that are not connected to the network
- Suspicious access (starting up in safe mode, local user, operations using administrator privileges)
- Clients that performed prohibited operations (writing to USB device, printing, sending emails with attachments, starting applications)
- Clients that exported files (removable, CD/DVD, network)

Displaying a list of the client status

Appropriate Target Se	notion most				
ggregation Completi	in Date/Time 2015/06/04 0	6.41.26	Start Date Time fo	Start Date Time for Next Aggregation 2015	
PCs that export	ted files (0%)				
AT 10 Case(s), 40	Case(x) Commissionfing	ist.			
	20	49			
	I working time: Pattern	1 (0%)			
AD 10 Case(1), 5 C	aue(s) Corresponding				
	20	45	10	00	
PCs used out o	f working time: Pattern	2 (0%)			
O This item has not b	been aggregated or the correspo	adeut information does not exist.			
				11	
			40	- 20	





Management Server

A server that distributes/configures security policies forclients targeted for management, and centrally manages the various logs collected from target clients.

Log Analyzer Server

A server that analyzes trends for operation logs such as file operations/export.

Relay Server

A server that collects recorded operations of smart devices and clients, and sends them to the Management Server.

Operating environment

Management Console

A client that has the console feature of Management Server. Client management and group policy settings can be operated via GUI.

Client

A client that is targeted for management.

Product name	Server operating system	Client operating system
Systemwalker Desktop Keeper V15 (V15.2)	Microsoft(R) Windows Server(R) 2016 Microsoft(R) Windows Server(R) 2012 Microsoft(R) Windows Server(R) 2008	Windows(R) 10, Windows(R) 8.1, Windows(R) 7, Microsoft(R) Windows Server(R) 2016, Microsoft(R) Windows Server(R) 2012, Microsoft(R) Windows Server(R) 2008, Android 4.4 - 8.0, iOS 6.0 - 11.0

* Microsoft and Windows are registered trademarks of Microsoft Corporation in the USA and other countries.

* Systemwalker is a trademark registered by Fujitsu Limited. * All other proper names, such as product names, may be trademarks or registered trademarks of their respective owners. * System names, product names and other proprietary names used in this document are not always accompanied by trademark symbols (TM) or (R).

*1: Refer to the website for this product for details on the operating environment.

* The contents of this catalog are subject to change, such as for improvements, without prior notice. * This catalog is printed on recycled paper using vegetable ink.

Product information can be found on the Internet http://www.fujitsu.com/systemwalker/

FUJITSU LIMITED

Shiodome City Center, 1-5-2, Higashi-shimbashi, Minato-ku, Tokyo 105-7123, Japan