Integrated Operations Management

Asset and distribution management

Introducing JP1/IT Desktop Management 2

- Protecting your increasingly diverse IT assets -

Hitachi, Ltd.

Contents

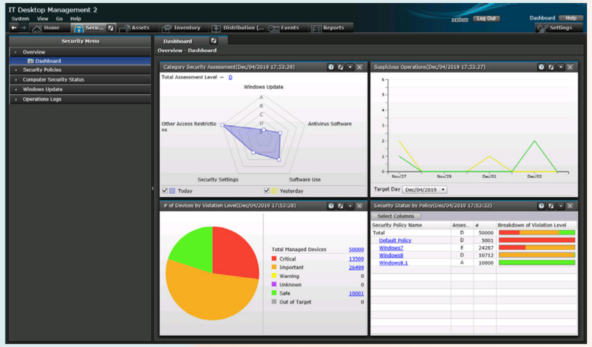
- Overview of JP1/IT Desktop Management 2
- What you can do
- Example of a system configuration
- Support for safe use
- List of features

Overview of JP1/IT Desktop Management 2

HITACHI

Properly manage a diverse array of IT assets and protect them from security risks

In a diverse IT environment that includes PCs, servers, virtual desktops, thin clients, and smart devices, you can automatically collect and centrally manage software information, hardware information, security information, operation logs, and more.

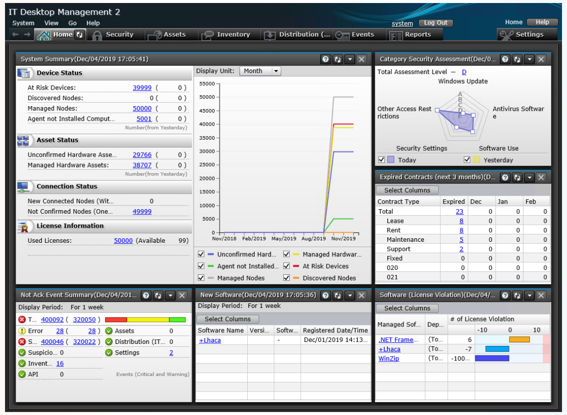


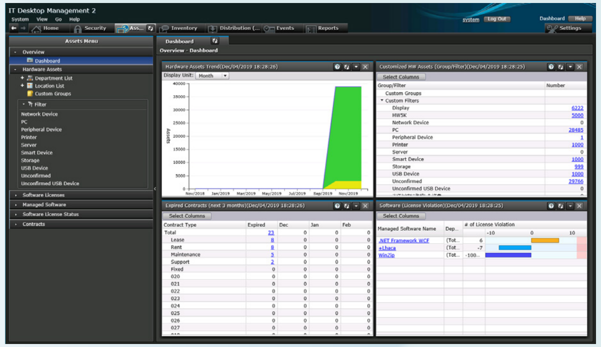
IT Desktop Management 2
Security Menu
Dashboard
Category Security Assessment
Suspicious Operations
# of Devices by Violation Level
Security Status by Policy

Security management

Understand the status of security measures

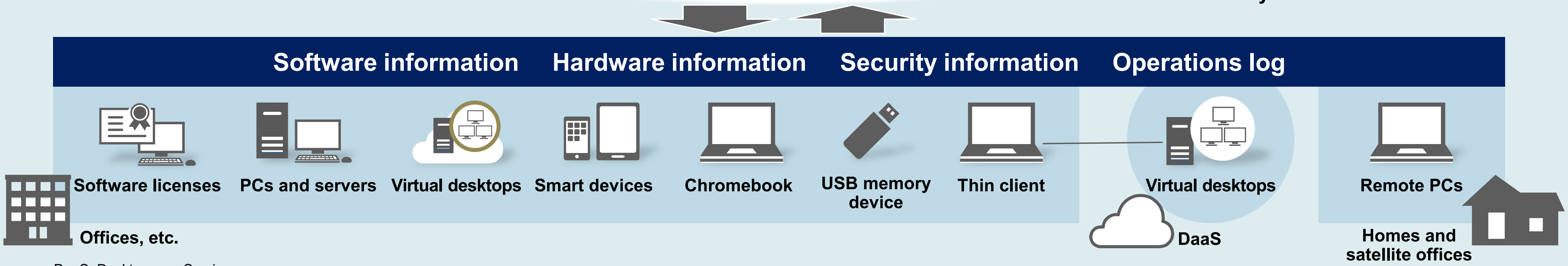
Home module





Asset management

Collect and centrally manage the latest information about your IT assets



DaaS: Desktop as a Service

What you can do >
Security management >
Asset management >

HITACHI

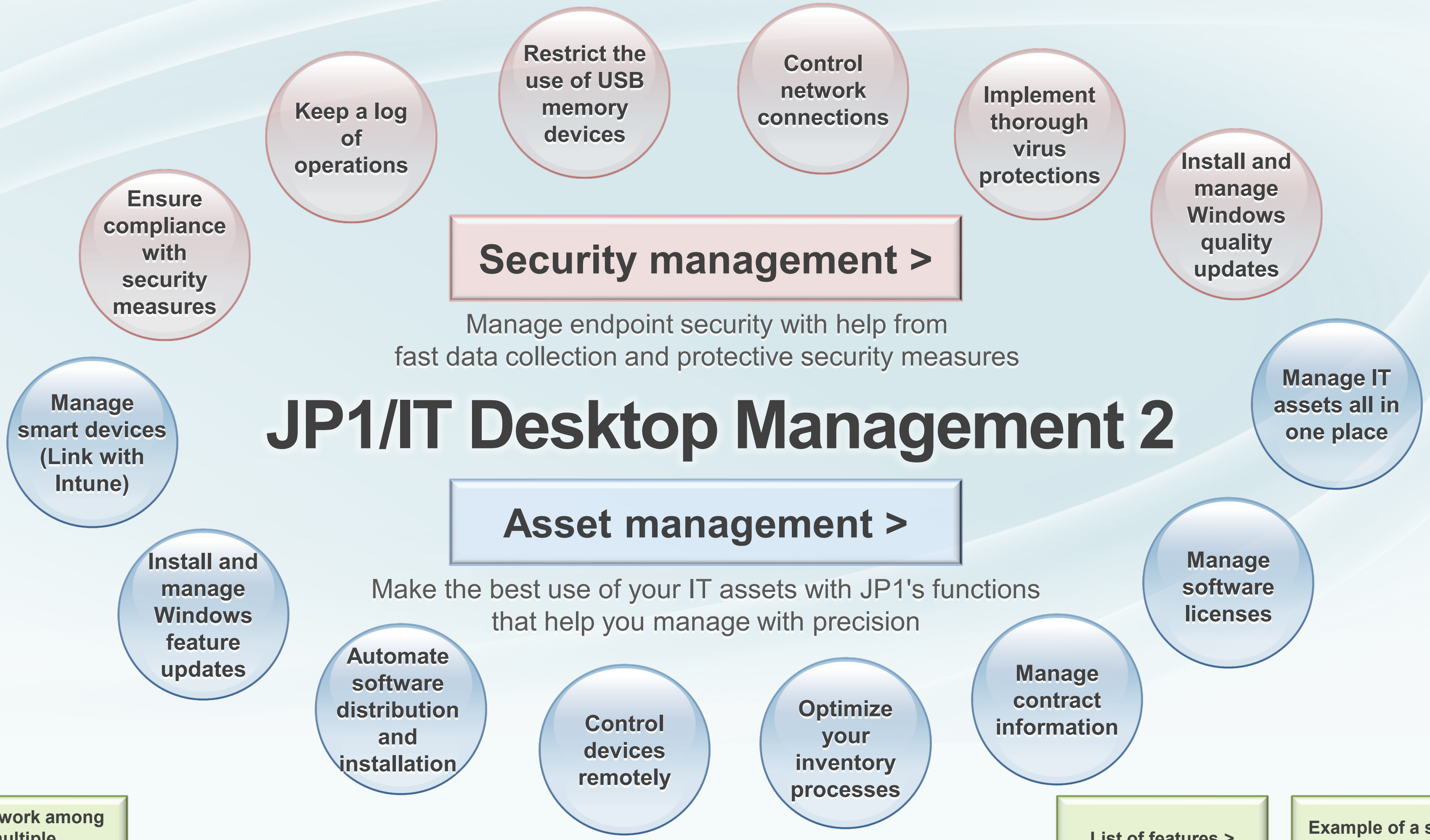
What you can do

- What you can do with JP1/IT Desktop Management 2
- Understand the current status of your system
- Security management
- Asset management
- Divide work among multiple administrators

What you can do with JP1/IT Desktop Management 2

HITACHI

Protect your diverse collection of IT assets with JP1's easy-to-use interface and rich selection of functions



Ensure compliance with security measures

Keep a log of operations

Restrict the use of USB memory devices

Control network connections

Implement thorough virus protections

Install and manage Windows quality updates

Security management >

Manage endpoint security with help from fast data collection and protective security measures

JP1/IT Desktop Management 2

Asset management >

Make the best use of your IT assets with JP1's functions that help you manage with precision

Manage smart devices (Link with Intune)

Install and manage Windows feature updates

Automate software distribution and installation

Control devices remotely

Optimize your inventory processes

Manage contract information

Manage software licenses

Manage IT assets all in one place

Intune: Microsoft Intune

Understand the current status of your system >

Divide work among multiple administrators >

List of features >

Example of a system configuration >

Products required for the main functions in this brochure >

Understand the current status of your system:
View important events and changes from the previous day

Automatically collect information about PCs and other devices connected to the network. The Home module of IT Desktop Management 2 shows a summary of the information you need to review on a daily basis. Simply by checking the Home module, which appears just after you log in, you can check the overall status and any issues that need to be addressed, including important events and any changes from the previous day.

☑ How has the system changed since yesterday?

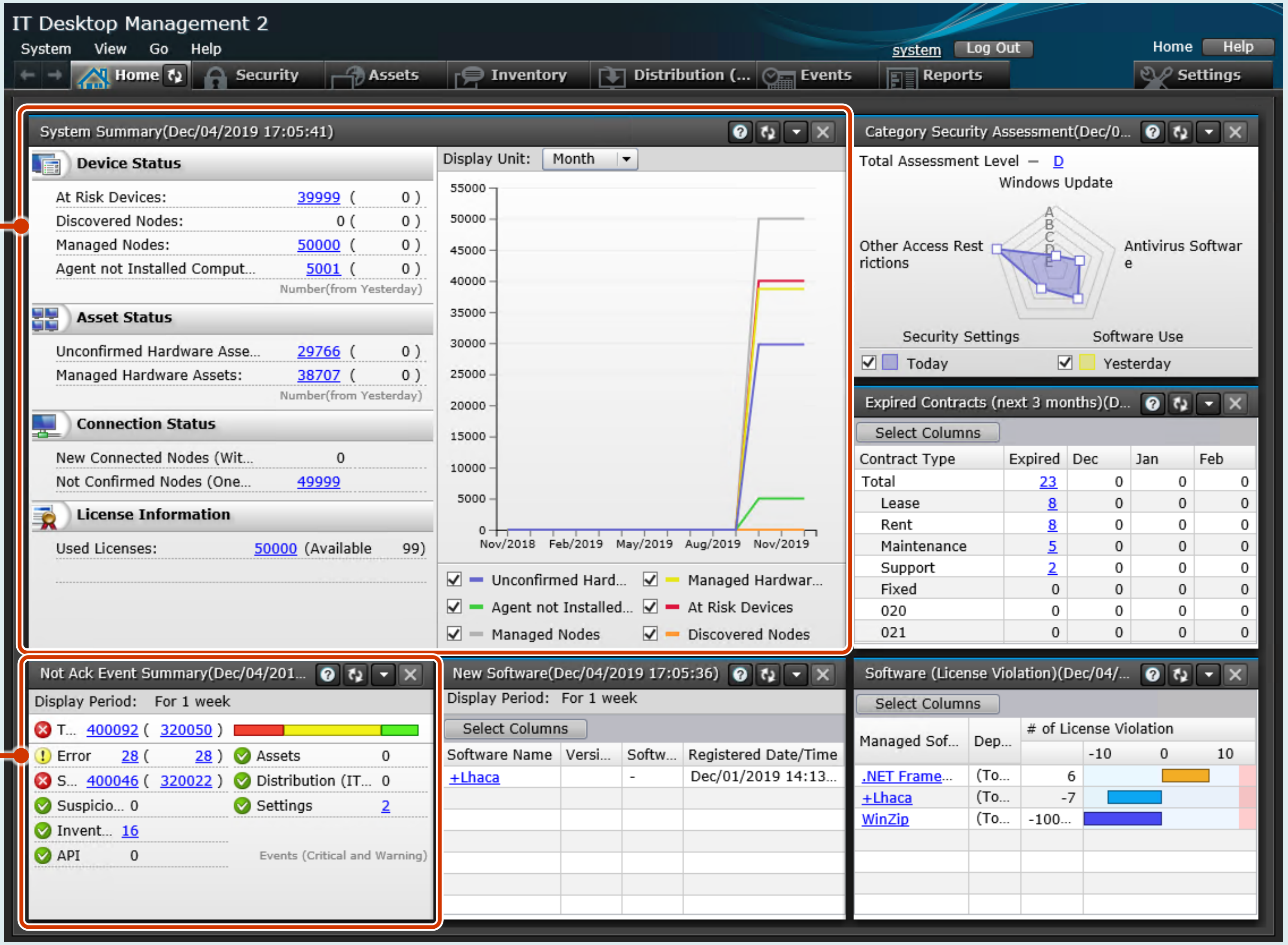
By checking the System Summary, you can see how the system has changed from the previous day and answer questions like the following:

- ☑ Are any PCs at risk?
- ☑ Have any new PCs or other devices been connected to the system?
- ☑ Are there any devices whose operating status has not been confirmed for an extended period of time?
- ☑ What is the overall status of the system and what are some general trends?

Verify that no unexpected changes have occurred, and ensure that your system remains safe. If you do find a problem, you can get the details simply by clicking the relevant link. These features help you resolve problems more smoothly.

☑ Did any important events occur?

All of the events that have occurred in the system are aggregated and displayed in one location, allowing you to determine how many events of a certain type have occurred. Click the corresponding link to see details about a particular event type.



System Summary(Dec/04/2019 17:05:41)

Device Status

At Risk Devices:	39999	(0)
Discovered Nodes:	0	(0)
Managed Nodes:	50000	(0)
Agent not Installed Comput...	5001	(0)

Number(from Yesterday)

Asset Status

Unconfirmed Hardware Asse...	29766	(0)
Managed Hardware Assets:	38707	(0)

Number(from Yesterday)

Connection Status

New Connected Nodes (Wit...	0
Not Confirmed Nodes (One...	49999

License Information

Used Licenses: 50000 (Available 99)

Display Unit: Month

Category Security Assessment(Dec/0...

Total Assessment Level – D

Expired Contracts (next 3 months)(D...

Select Columns

Contract Type	Expired	Dec	Jan	Feb
Total	23	0	0	0
Lease	8	0	0	0
Rent	8	0	0	0
Maintenance	5	0	0	0
Support	2	0	0	0
Fixed	0	0	0	0
020	0	0	0	0
021	0	0	0	0

Not Ack Event Summary(Dec/04/201...

Display Period: For 1 week

T...	400092 (320050)			
Error	28 (28)		Assets	0
S...	400046 (320022)		Distribution (IT...	0
Suspicio...	0		Settings	2
Invent...	16			
API	0			

Events (Critical and Warning)

New Software(Dec/04/2019 17:05:36)

Display Period: For 1 week

Select Columns

Software Name	Versi...	Softw...	Registered Date/Time
+Lhaca		-	Dec/01/2019 14:13...

Software (License Violation)(Dec/04/...

Select Columns

Managed Sof...	Dep...	# of License Violation
.NET Frame...	(To...	6
+Lhaca	(To...	-7
WinZip	(To...	-100...

Home module

Understand the current status of your system:
Check the status of update programs, unnecessary software installations, and license violations

HITACHI

Check the Home module to see the status of Windows quality updates and other security measures, and to check for problems such as the installation of unnecessary software and software license violations.

☑ Are security measures such as Windows quality updates being implemented appropriately?

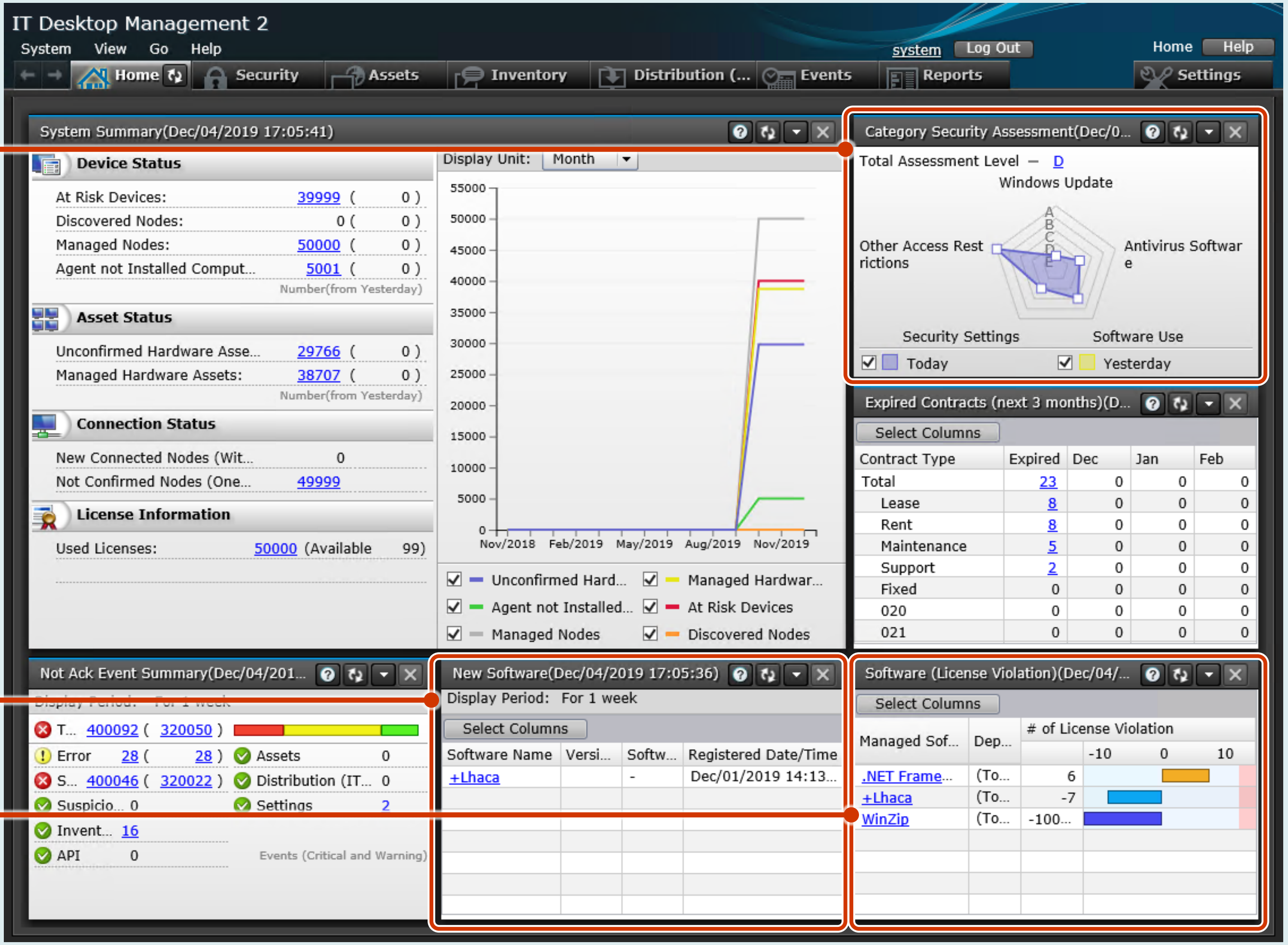
Comprehensively evaluate your system's security by checking the status of security measures, broken down into categories such as Windows quality updates, virus protections, and security settings.

☑ Were any attempts made to install unnecessary software?

JP1 detects when any new programs or Windows apps are installed on monitored PCs. You can periodically check this area to see whether software that is not required for work has been installed.

☑ Are there any software license violations?

For each of the software programs you manage, you can check whether actual usage exceeds the number of licenses you own.



System Summary(Dec/04/2019 17:05:41)

Device Status

At Risk Devices:	39999	(0)
Discovered Nodes:	0	(0)
Managed Nodes:	50000	(0)
Agent not Installed Comput...	5001	(0)

Number(from Yesterday)

Asset Status

Unconfirmed Hardware Asse...	29766	(0)
Managed Hardware Assets:	38707	(0)

Number(from Yesterday)

Connection Status

New Connected Nodes (Wit...	0
Not Confirmed Nodes (One...	49999

License Information

Used Licenses: 50000 (Available 99)

☑ Unconfirmed Hard... ☑ Managed Hardwar...
☑ Agent not Installed... ☑ At Risk Devices
☑ Managed Nodes ☑ Discovered Nodes

Category Security Assessment(Dec/0...

Total Assessment Level – D

Windows Update / Antivirus Software / Software Use / Security Settings / Other Access Restrictions

☑ Today ☑ Yesterday

Expired Contracts (next 3 months)(D...

Contract Type	Expired	Dec	Jan	Feb
Total	23	0	0	0
Lease	8	0	0	0
Rent	8	0	0	0
Maintenance	5	0	0	0
Support	2	0	0	0
Fixed	0	0	0	0
020	0	0	0	0
021	0	0	0	0

Not Ack Event Summary(Dec/04/201...

Display Period: For 1 week

T...	400092 (320050)			
Error	28 (28)		Assets	0
S...	400046 (320022)		Distribution (IT...	0
Suspicio...	0		Settings	2
Invent...	16			
API	0			

Events (Critical and Warning)

New Software(Dec/04/2019 17:05:36)

Display Period: For 1 week

Software Name	Versi...	Softw...	Registered Date/Time
+Lhaca		-	Dec/01/2019 14:13...

Software (License Violation)(Dec/04/...

Managed Sof...	Dep...	# of License Violation
.NET Frame...	(To...	6
+Lhaca	(To...	-7
WinZip	(To...	-100...

Home module

What you can do >

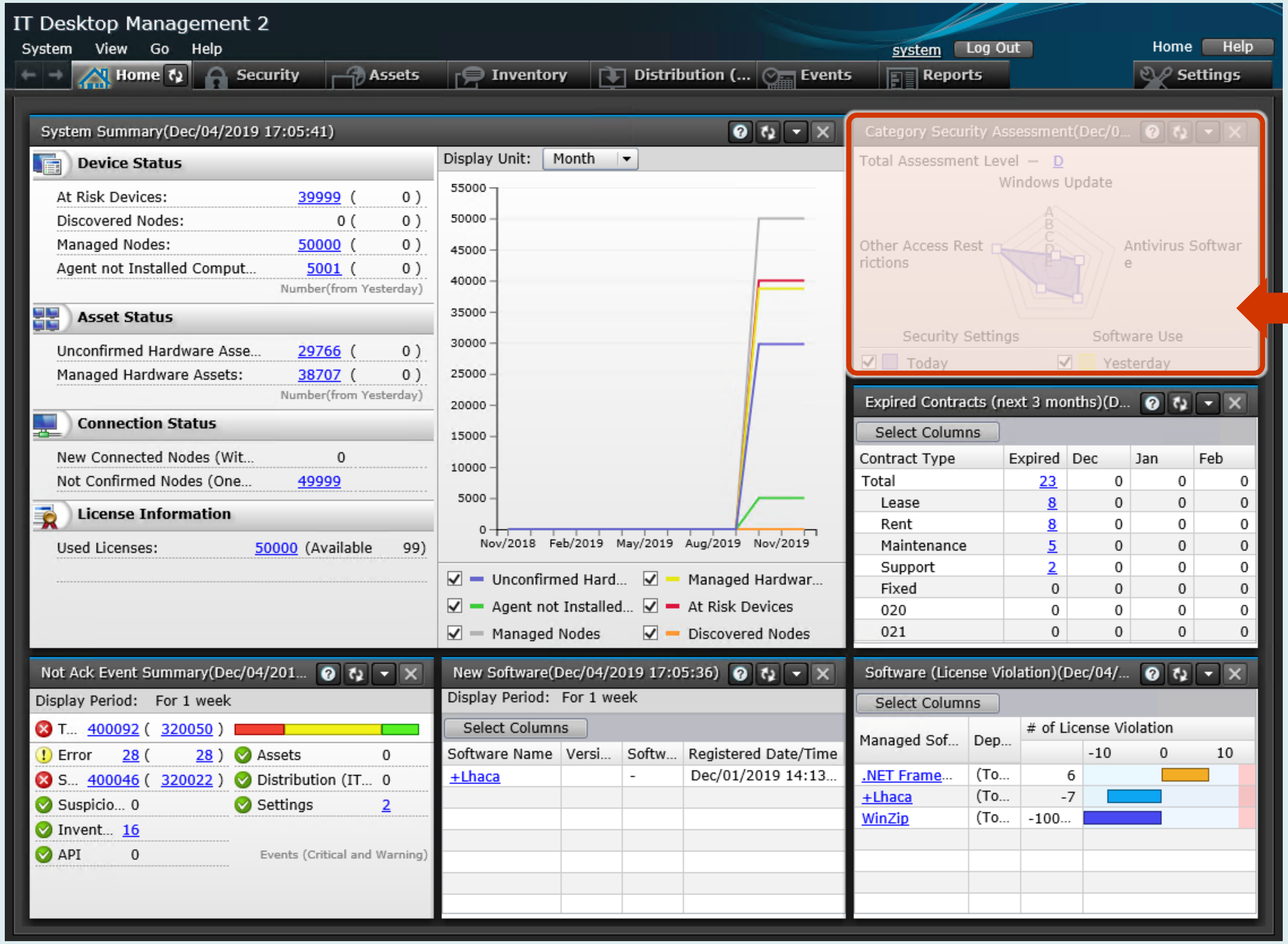
Security management >

Asset management >

Understand the current status of your system:
Customize the Home module

HITACHI

The Home module summarizes and organizes information into small panels. You can customize the appearance by choosing the information that you want to see each day from the 19 available panels.


IT Desktop Management 2
System View Go Help
system Log Out
Home Help
Home Security Assets Inventory Distribution (... Events Reports Settings

System Summary(Dec/04/2019 17:05:41)

Device Status

At Risk Devices:	39999	(0)
Discovered Nodes:	0	(0)
Managed Nodes:	50000	(0)
Agent not Installed Comput...	5001	(0)

Number(from Yesterday)

Asset Status

Unconfirmed Hardware Asse...	29766	(0)
Managed Hardware Assets:	38707	(0)

Number(from Yesterday)

Connection Status

New Connected Nodes (Wit...	0
Not Confirmed Nodes (One...	49999

License Information

Used Licenses: 50000 (Available 99)

Display Unit: Month

☑ Unconfirmed Hard... ☑ Managed Hardwar...
☑ Agent not Installed... ☑ At Risk Devices
☑ Managed Nodes ☑ Discovered Nodes

Category Security Assessment(Dec/0...

Total Assessment Level – D

☑ Today ☑ Yesterday

Expired Contracts (next 3 months)(D...

Select Columns

Contract Type	Expired	Dec	Jan	Feb
Total	23	0	0	0
Lease	8	0	0	0
Rent	8	0	0	0
Maintenance	5	0	0	0
Support	2	0	0	0
Fixed	0	0	0	0
020	0	0	0	0
021	0	0	0	0

Not Ack Event Summary(Dec/04/201...

Display Period: For 1 week

T...	400092 (320050)		
Error	28 (28)	Assets	0
S...	400046 (320022)	Distribution (IT...	0
Suspicio...	0	Settings	2
Invent...	16		
API	0		

Events (Critical and Warning)

New Software(Dec/04/2019 17:05:36)

Display Period: For 1 week

Select Columns

Software Name	Versi...	Softw...	Registered Date/Time
+Lhaca		-	Dec/01/2019 14:13...

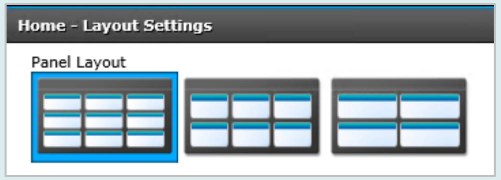
Software (License Violation)(Dec/04/...

Select Columns

Managed Sof...	Dep...	# of License Violation
.NET Frame...	(To...	6
+Lhaca	(To...	-7
WinZip	(To...	-100...

Home module

Choose from three available layouts

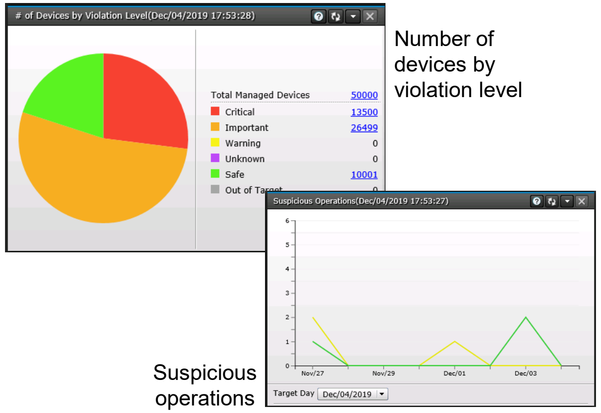


Home - Layout Settings

Panel Layout

Customize the module's appearance to display the summaries you want to check.

☑ Are there any PCs for which security measures need to be implemented?



# of Devices by Violation Level(Dec/04/2019 17:53:28)

Total Managed Devices	50000
🟥 Critical	13500
🟧 Important	26499
🟨 Warning	0
🟪 Unknown	0
🟩 Safe	10001
⬜ Out of Target	0

Suspicious Operations(Dec/04/2019 17:53:27)

Target Day Dec/04/2019

Number of devices by violation level

Suspicious operations

☑ Were any suspicious operations performed, such as those that might have transferred important data outside the company?

Security management

Have you experienced any of these issues?

HITACHI

☑ Need to determine whether security risks to the company are being effectively mitigated?

Ensure compliance with security measures p. 9

With JP1/IT Desktop Management 2, you can collect information from managed PCs, such as information about security vulnerabilities, prohibited operations, and information leakage. JP1 helps you form a clear picture as to whether the security risks facing your company are being effectively mitigated.

☑ Need to eliminate the risk of information leaks from day-to-day operations?

Keep a log of operations p. 12

Operations that allow someone to obtain internal company information, potentially disclosing such information to parties outside the company, pose a risk of information leakage. Examples of such operations include uploading data to an external website, sending email, and copying data to a USB memory device. JP1 identifies these types of operations as "suspicious operations" and notifies administrators, who can then trace the operations by examining the operations logs.

☑ Need to prevent data from being easily transferred onto USB memory devices and taken outside the company?

Restrict the use of USB memory devices p. 16

With JP1, you can permit the use of only USB memory devices owned by the company, prohibiting the use of all other USB memory devices. In other words, if someone inserts an unauthorized USB memory device, use of the device will be disabled. This feature limits the ability of USB memory devices to act as a pathway for information to leak outside the company. JP1 also allows you to check a list of the files stored on each USB memory device that you are managing.

☑ Need to prevent people from connecting PCs deemed unsafe to the company network?

Control network connections p. 17

You can use JP1 to quarantine PCs that are deemed unsafe and PCs infected by malware. You can also automate the process for verifying that all appropriate security measures have been implemented on a particular managed PC before that PC is allowed access to the network.

☑ Need to identify at-risk PCs that require antivirus software updates?

Implement thorough virus protections p. 18

As JP1 allows you to verify that all required security measures have been implemented, if an unsafe PC is found, you can send a message to the user of that PC to request that the necessary security measures be applied. Furthermore, if there are PCs that are at risk because their antivirus software is not up to date, you can distribute and install the latest version of that software on these PCs.

☑ Need to identify PCs for which the necessary Windows quality updates have not been installed?

Install and manage Windows quality updates p. 19

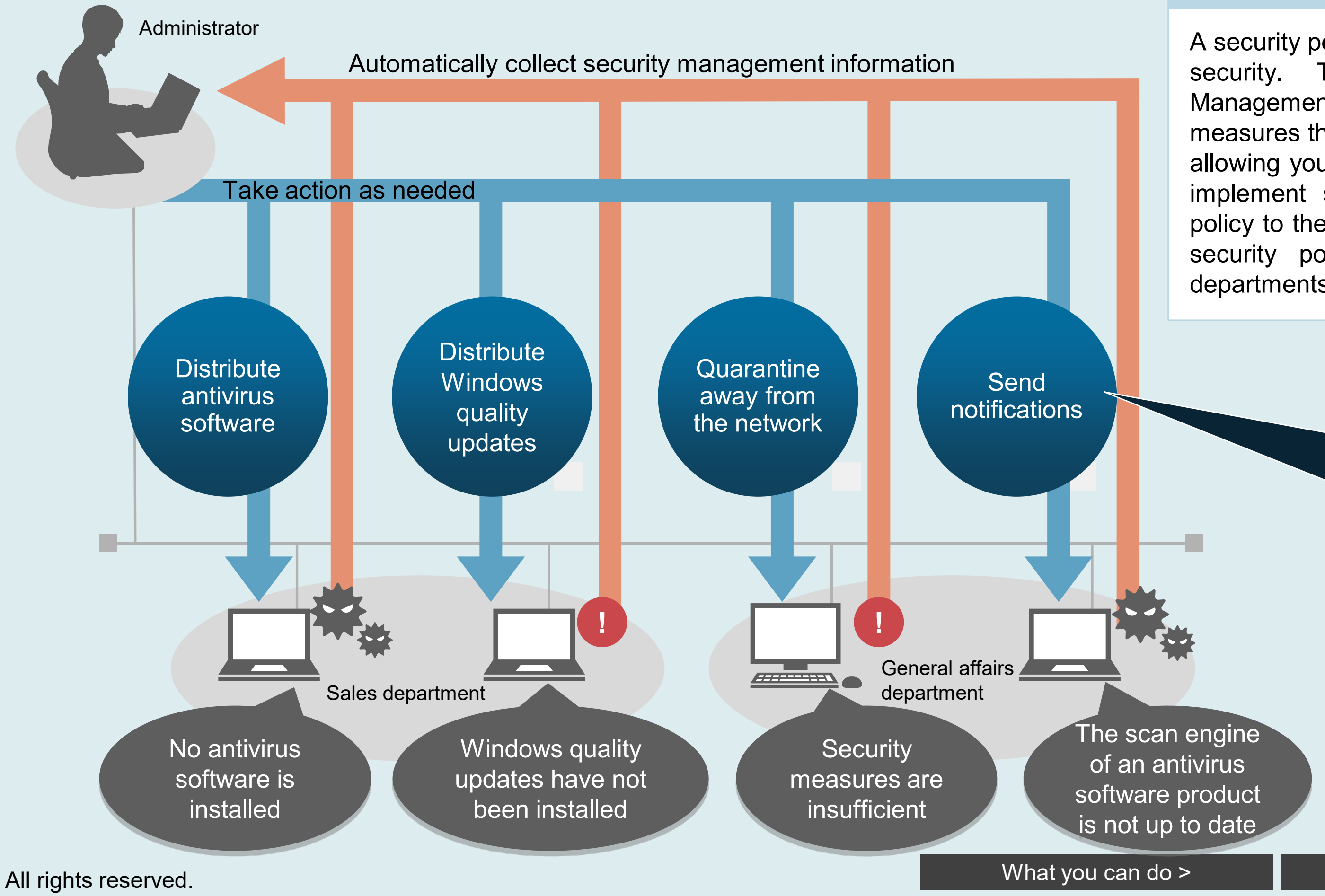
When the automatic Windows quality update function is disabled, JP1 can automatically enable it so that the latest Windows quality updates are installed. If there is a specific Windows quality update that you do not want to install, you can select which Windows quality updates are to be distributed and installed.

Ensure compliance with security measures: Check the status of security measures and take the necessary action

Check the security status of individual PCs, and take the appropriate action depending on what you find.

Examples

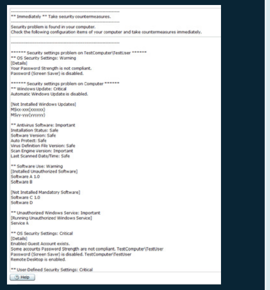
- ●Distribute and install antivirus software and other required software
- ●Check for and install the latest Windows quality updates as necessary
- ●Quarantine unsafe devices away from the network
- ●Send messages to request the implementation of security measures


Administrator
Automatically collect security management information
Take action as needed
Distribute antivirus software
Distribute Windows quality updates
Quarantine away from the network
Send notifications
Sales department
General affairs department
No antivirus software is installed
Windows quality updates have not been installed
Security measures are insufficient
The scan engine of an antivirus software product is not up to date

What is a security policy?

A security policy is an organization's policy for ensuring information security. The security policy provided by JP1/IT Desktop Management 2 - Manager comes with a number of security measures that need to be implemented on PCs already configured, allowing you to start managing your system immediately. You can implement security measures simply by applying this security policy to the PCs you manage. You can also change the provided security policy to create customized policies for individual departments or PCs.

Send notifications



```
------------------------------------------------------------
** Immediately ** Take security countermeasures.
------------------------------------------------------------
Security problem is found in your computer.
Check the following configuration items of your computer and take countermeasures immediately.

------------------------------------------------------------

****** Security settings problem on TestComputer\TestUser ******
** OS Security Settings: Warning
[Details]
Your Password Strength is not compliant.
Password (Screen Saver) is disabled.

****** Security settings problem on Computer ******
** Windows Update: Critical
Automatic Windows Update is disabled.

[Not Installed Windows Updates]
MSxx-xxx(xxxxxx)
MSyy-yyy(yyyyyy)

** Antivirus Software: Important
Installation Status: Safe
Software Version: Safe
Auto Protect: Safe
Virus Definition File Version: Safe
Scan Engine Version: Important
Last Scanned Date/Time: Safe

** Software Use: Warning
[Installed Unauthorized Software]
Software A 1.0
Software B

[Not Installed Mandatory Software]
Software C 1.0
Software D

** Unauthorized Windows Service: Important
[Running Unauthorized Windows Service]
Service A

** OS Security Settings: Critical
[Details]
Enabled Guest Account exists.
Some accounts Password Strength are not compliant. TestComputer\TestUser
Password (Screen Saver) is disabled. TestComputer\TestUser
Remote Desktop is enabled.

** User-Defined Security Settings: Critical
```

Freely customize notification messages

Ensure compliance with security measures: Detect information leakage risks

Detect operations that attempt to obtain files from PCs, and notify administrators of such operations.

Examples

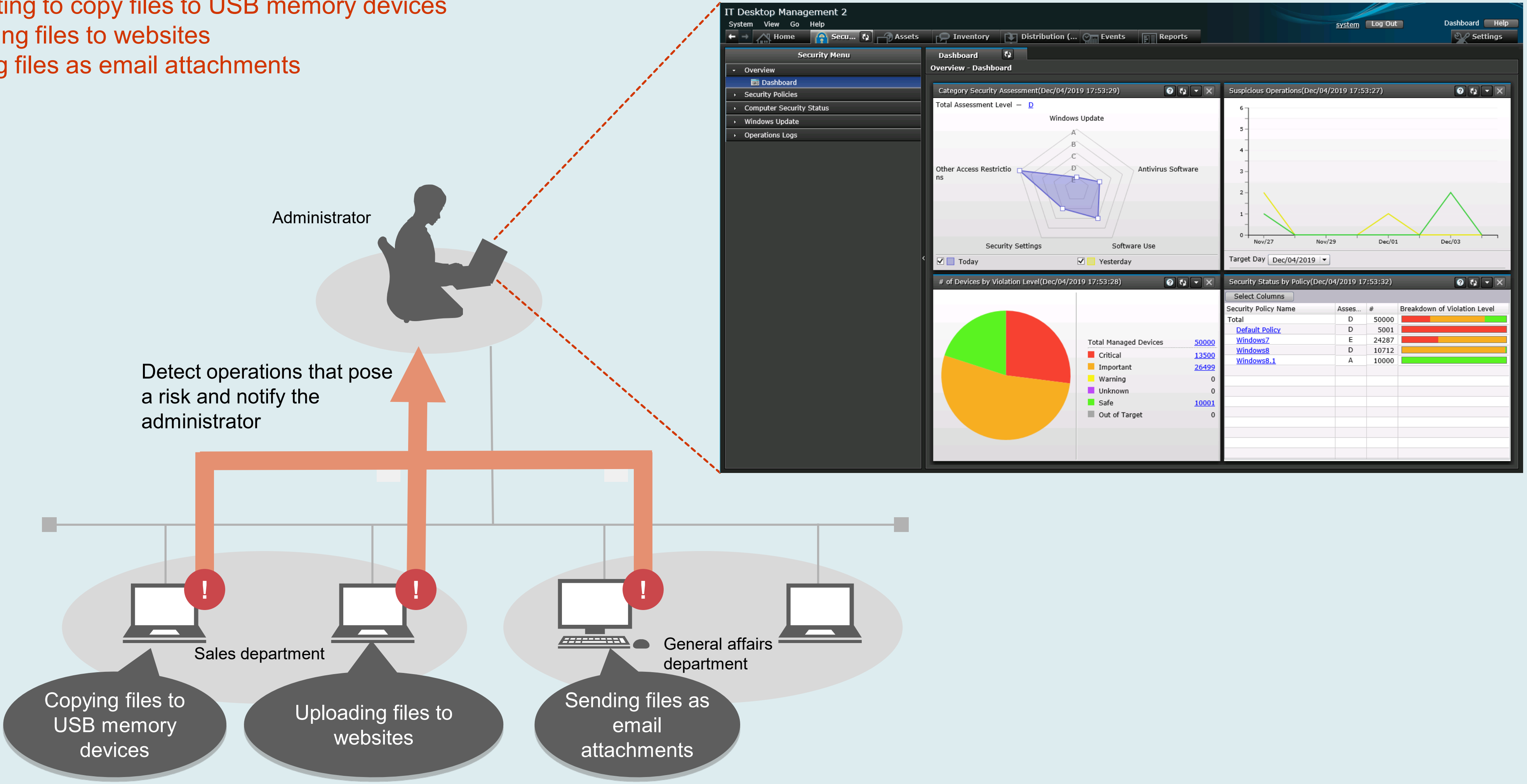
Detect and send notifications about operations such as the following:

●Attempting to copy files to USB memory devices

●Uploading files to websites

●Sending files as email attachments

Security module (Dashboard)



Administrator

Detect operations that pose a risk and notify the administrator

Sales department

General affairs department

Copying files to USB memory devices

Uploading files to websites

Sending files as email attachments

IT Desktop Management 2

Overview - Dashboard

Category Security Assessment(Dec/04/2019 17:53:29)

Total Assessment Level — D

Suspicious Operations(Dec/04/2019 17:53:27)

Target Day Dec/04/2019

# of Devices by Violation Level(Dec/04/2019 17:53:28)

Total Managed Devices	50000
🟥 Critical	13500
🟧 Important	26499
🟨 Warning	0
🟪 Unknown	0
🟩 Safe	10001
⬜ Out of Target	0

Security Status by Policy(Dec/04/2019 17:53:32)

Select Columns

Security Policy Name	Asses...	#	Breakdown of Violation Level
Total	D	50000	
Default Policy	D	5001	
Windows7	E	24287	
Windows8	D	10712	
Windows8.1	A	10000	

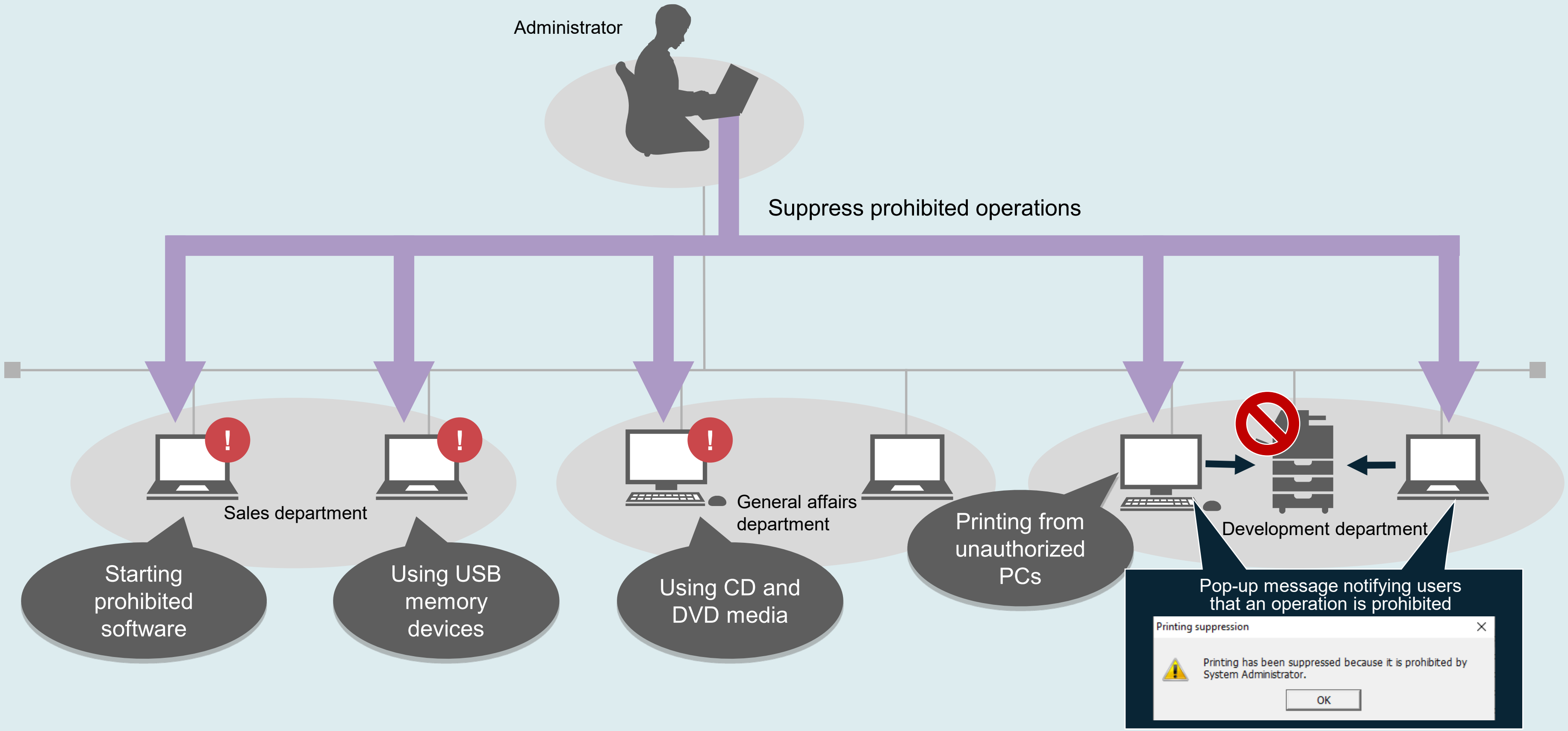
Ensure compliance with security measures: Suppress prohibited operations

HITACHI

You can specify operations that are to be prohibited and use pop-up messages to notify users who try to perform these operations.

Examples

- ●Suppress printing from unauthorized PCs
- ●Suppress the startup of prohibited software
- ●Suppress the use of USB memory devices
- ●Suppress the use of CD and DVD media


Administrator
Suppress prohibited operations
Sales department
General affairs department
Development department
Starting prohibited software
Using USB memory devices
Using CD and DVD media
Printing from unauthorized PCs

Pop-up message notifying users that an operation is prohibited

Printing suppression

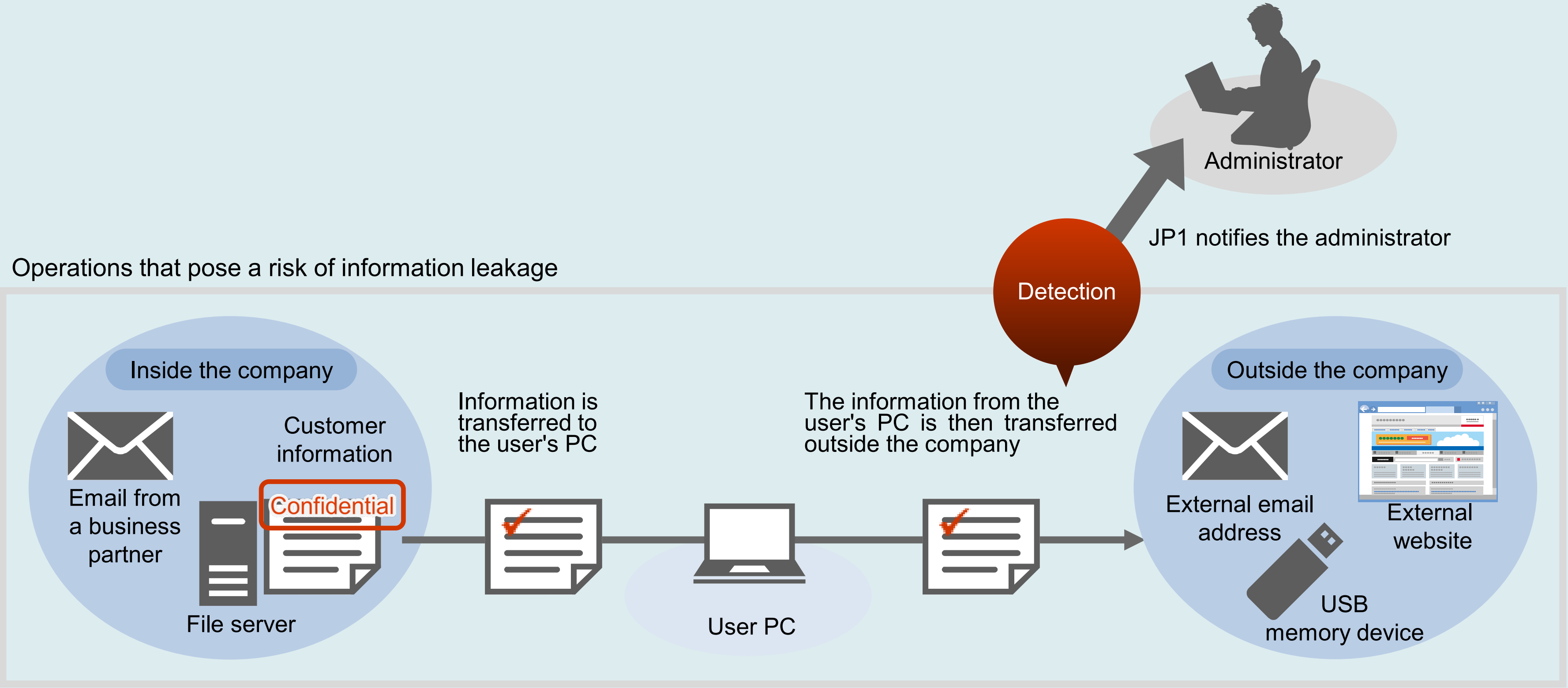
Printing has been suppressed because it is prohibited by System Administrator.

OK

Keep a log of operations:

Detect operations that pose a risk of information leakage and notify the administrator

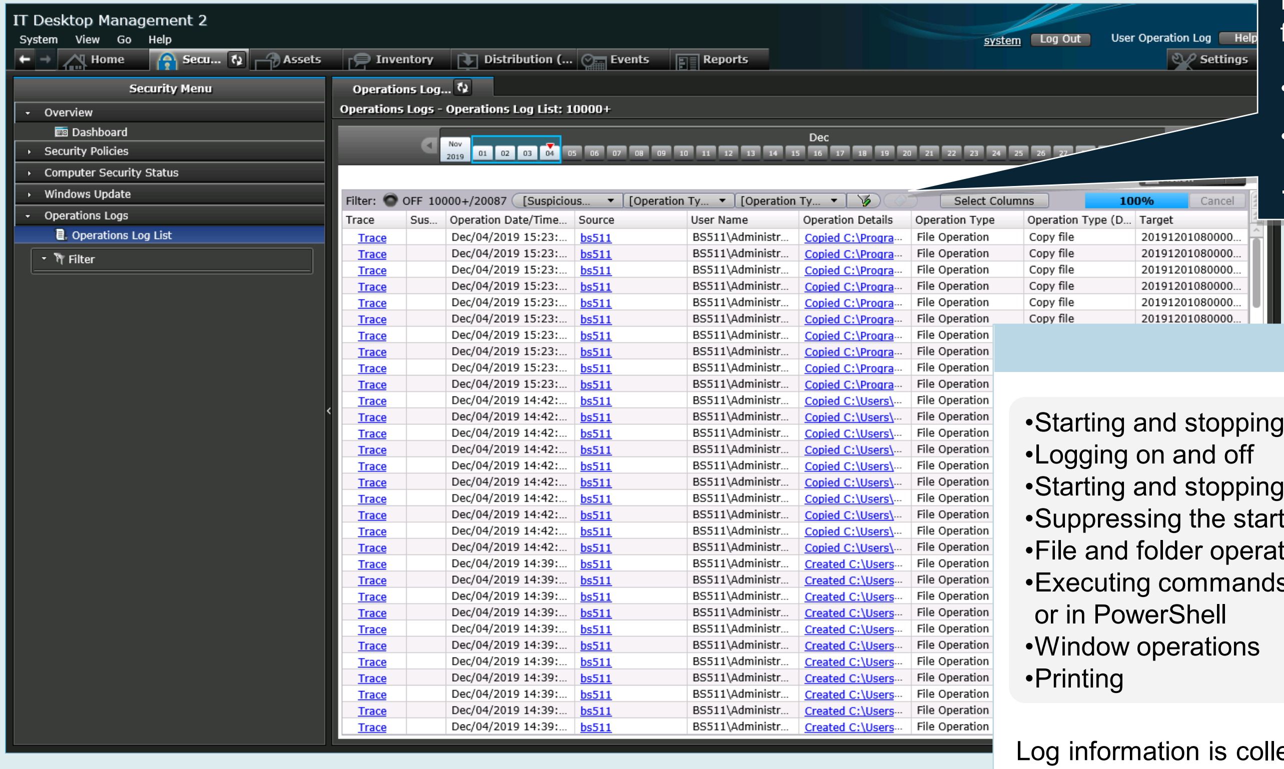
Monitor company files and files received from certain email addresses, websites, or other sources. Operations to transfer monitored files outside the company can be detected as suspicious operations. You can even record and manage operations that are performed while a PC is disconnected from the network, ensuring that no suspicious activity escapes your attention.


Administrator
JP1 notifies the administrator
Detection
Operations that pose a risk of information leakage
Inside the company
Email from a business partner
Customer information
Confidential
File server
Information is transferred to the user's PC
User PC
The information from the user's PC is then transferred outside the company
Outside the company
External email address
External website
USB memory device

Keep a log of operations:
Filter for operations that pose a risk of information leakage

Check the operations log more efficiently by filtering to show only operations that might leak information.

Security module (Operations Log List)



Operations Logs - Operations Log List: 10000+

Filter: ● OFF 10000+/20087 [Suspicious... ▼ [Operation Ty... ▼ [Operation Ty... ▼

Trace	Sus...	Operation Date/Time...	Source	User Name	Operation Details	Operation Type	Operation Type (D...	Target
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation	Copy file	20191201080000...
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation	Copy file	20191201080000...
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation	Copy file	20191201080000...
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation	Copy file	20191201080000...
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation	Copy file	20191201080000...
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation	Copy file	20191201080000...
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation		
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation		
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation		
Trace		Dec/04/2019 15:23:...	bs511	BS511\Administr...	Copied C:\Progra...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:42:...	bs511	BS511\Administr...	Copied C:\Users\...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		
Trace		Dec/04/2019 14:39:...	bs511	BS511\Administr...	Created C:\Users...	File Operation		

In the Operations Log List window, specify conditions to filter for specific log entries, such as the following:

- Log entries generated when a user operated on a file whose file name contained the word "customer"
- Entries from the operations log of a specific PC

...etc.

Operations for which log information can be collected

- •Starting and stopping PCs
- •Logging on and off
- •Starting and stopping processes
- •Suppressing the startup of programs
- •File and folder operations*1
- •Executing commands from a command prompt or in PowerShell
- •Window operations
- •Printing
- •Suppressing printing operations
- •Connecting and removing external media devices
- •Blocking externally connected devices
- •Web access (uploading and downloading data)*2
- •FTP operations (sending and receiving files)*2
- •Sending and receiving emails with attachments*2
- •Saving attachments from emails*2

Log information is collected only about operations for which there is a risk of information being leaked, helping to minimize the size of the database that stores log data.

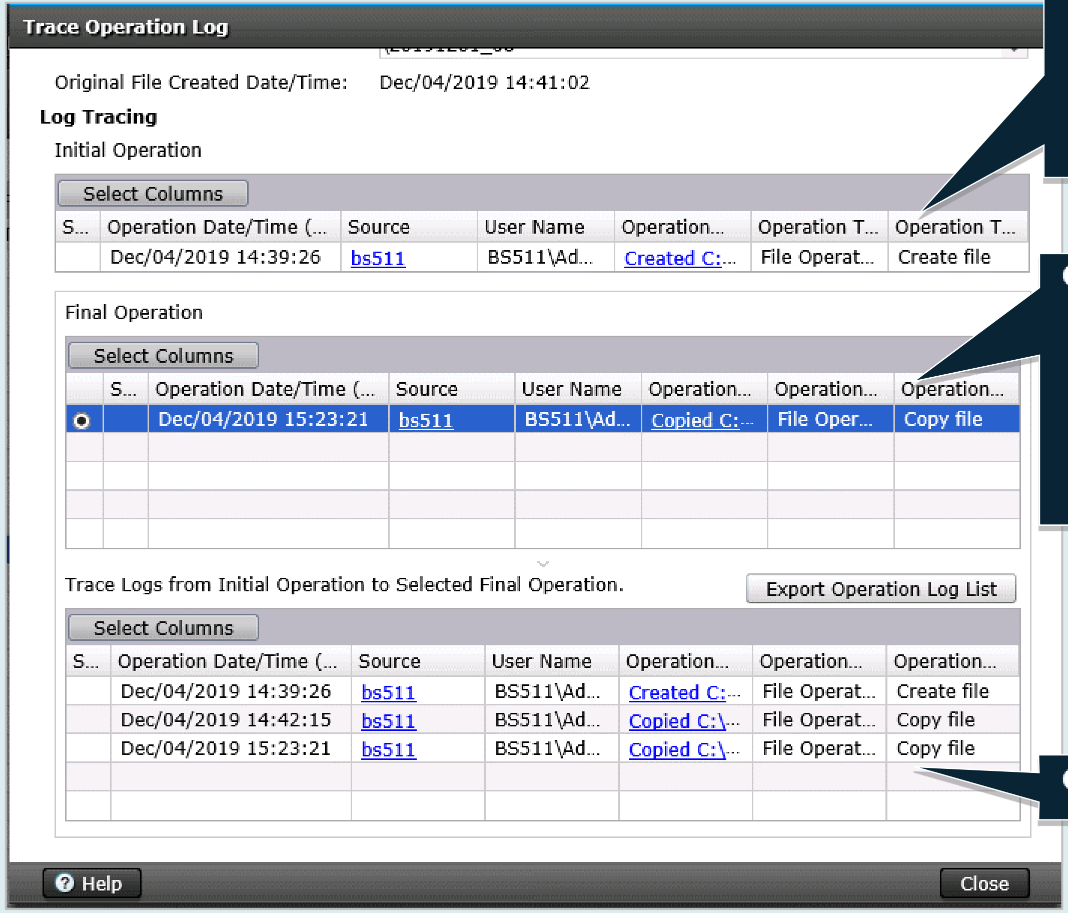
*1 Refers to operations in Windows Explorer and does not include operations performed in other software (such as Microsoft Office programs).

*2 For information on the browser (Microsoft Edge and Google Chrome) and email software (such as Outlook) for which operations log information can be obtained, see the applicable JP1 product manual.

Keep a log of operations: Trace suspicious operations

You can trace operations that pose a risk of information leaks in the Trace Operation Log dialog box. This dialog box provides information that includes when the operation was performed, who performed the operation, the source from which the file was obtained, how the file was obtained, and how the file was transferred outside the company.

Trace Operation Log dialog box



Trace Operation Log

Original File Created Date/Time: Dec/04/2019 14:41:02

Log Tracing

Initial Operation

S...	Operation Date/Time (...	Source	User Name	Operation...	Operation T...	Operation T...
	Dec/04/2019 14:39:26	bs511	BS511\Ad...	Created C:...	File Operat...	Create file

Final Operation

	S...	Operation Date/Time (...	Source	User Name	Operation...	Operation...	Operation...
○		Dec/04/2019 15:23:21	bs511	BS511\Ad...	Copied C:...	File Oper...	Copy file

Trace Logs from Initial Operation to Selected Final Operation.

S...	Operation Date/Time (...	Source	User Name	Operation...	Operation...	Operation...
	Dec/04/2019 14:39:26	bs511	BS511\Ad...	Created C:...	File Operat...	Create file
	Dec/04/2019 14:42:15	bs511	BS511\Ad...	Copied C:\...	File Operat...	Copy file
	Dec/04/2019 15:23:21	bs511	BS511\Ad...	Copied C:\...	File Operat...	Copy file

❶ How the file in question first appeared on the user's PC

- When was the file obtained?
- Who obtained the file?
- Where did the file come from?
- How was the file obtained?

❷ Last operation performed on the file on the user's PC (the file obtained in ❶)

- Deleting the file
- Transferring the file off the PC, or sending the file as an email attachment
- Copying, moving, or renaming the file

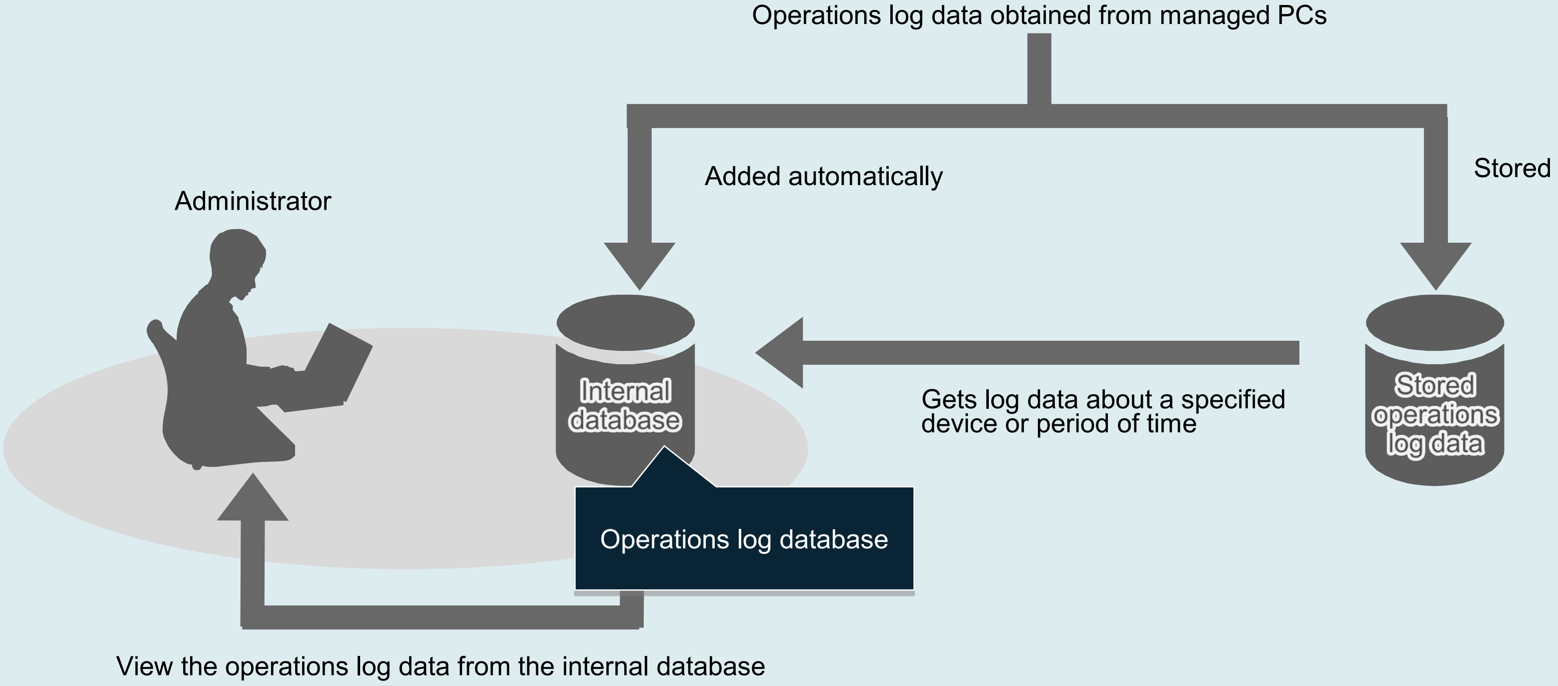
...etc.

❸ History of operations from ❶ to ❷

Keep a log of operations: Work with large amounts of operations log data from a single management server

HITACHI

JP1/IT Desktop Management 2 - Manager's internal database allows you to use a single management server for all of the functions you need, such as for storing, loading, and referencing large amounts of operations log data.


Operations log data obtained from managed PCs
Added automatically
Stored
Administrator
Internal database
Stored operations log data
Gets log data about a specified device or period of time
Operations log database
View the operations log data from the internal database

The internal database (operations log database) can hold a maximum of 30 to 500 days' worth of data.
1 to 300 days' worth of data is automatically added to this database.
For example, if the database can hold a maximum of 500 days' worth of data and 300 days' worth of data is automatically added, you can add up to 200 days' worth of data about specified devices or periods of time.

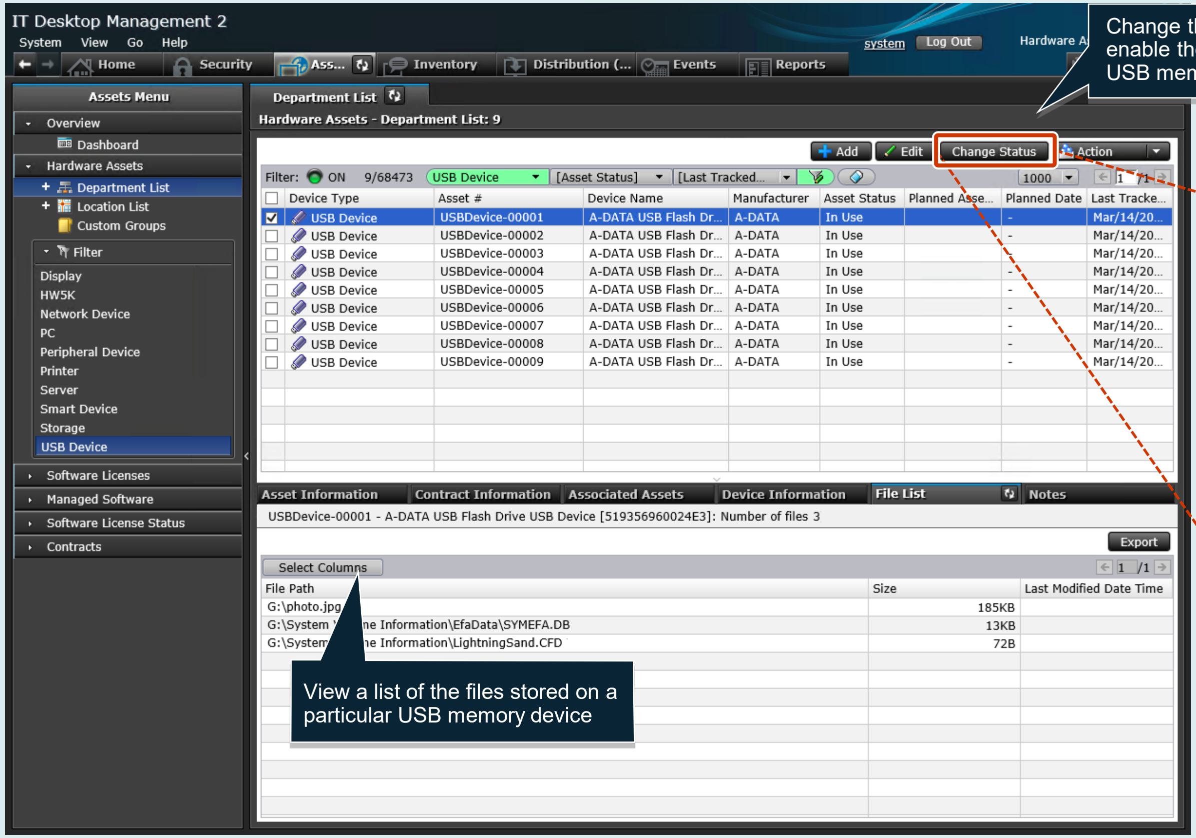
Restrict the use of USB memory devices

HITACHI

You can either prohibit the use of USB memory devices completely or permit the use of only devices that have been registered.* This function allows administrators to identify whenever an unapproved USB memory device is connected to a managed PC. Registered USB memory devices are kept in a list for easy verification, and you can use this list when you want to enable devices to make them immediately usable. To reduce the likelihood of information leaks, you can limit the USB memory devices that can be used throughout the company to approved devices only, or limit the use of a particular USB memory device to certain departments or sites.

Assets module (Department List)

*You can register any USB memory device that has a unique device instance ID.



Hardware Assets - Department List: 9

Filter: ON 9/68473 USB Device [Asset Status] [Last Tracked... 1000 1 /1

☐	Device Type	Asset #	Device Name	Manufacturer	Asset Status	Planned Asse...	Planned Date	Last Tracke...
☑	USB Device	USBDevice-00001	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00002	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00003	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00004	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00005	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00006	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00007	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00008	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...
☐	USB Device	USBDevice-00009	A-DATA USB Flash Dr...	A-DATA	In Use		-	Mar/14/20...

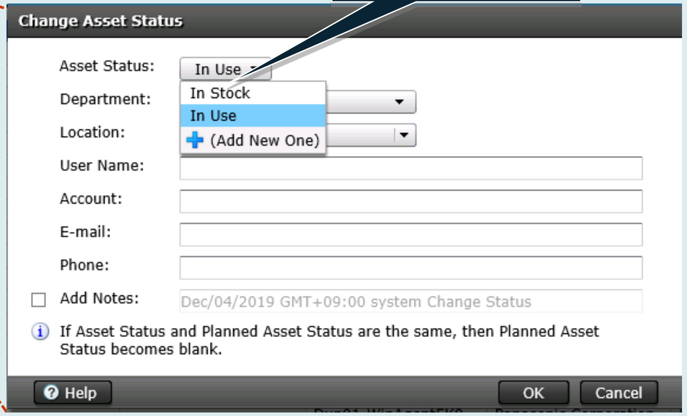
USBDevice-00001 - A-DATA USB Flash Drive USB Device [519356960024E3]: Number of files 3

File Path	Size	Last Modified Date Time
G:\photo.jpg	185KB	
G:\System ...ne Information\EfaData\SYMEFA.DB	13KB	
G:\System ...ne Information\LightningSand.CFD	72B	

Change the settings to enable the use of a USB memory device

View a list of the files stored on a particular USB memory device

Enable a device by changing its status to "In Use"



Asset Status: In Use

Department:

Location:

User Name:

Account:

E-mail:

Phone:

☐ Add Notes: Dec/04/2019 GMT+09:00 system Change Status

If Asset Status and Planned Asset Status are the same, then Planned Asset Status becomes blank.

Change Asset Status dialog box

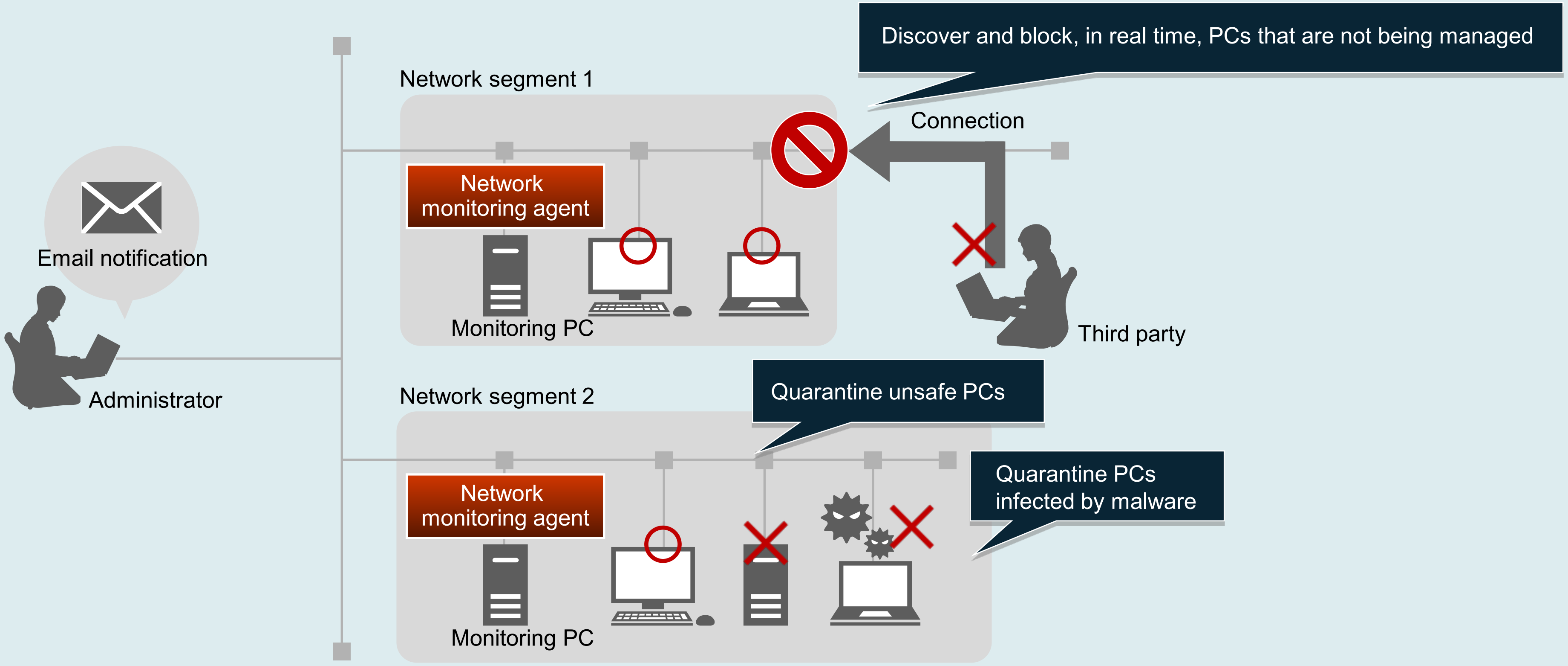
You can collect information about the files stored on any USB memory device that has a unique device instance ID. This helps when you want to check whether a device contains any data that must not be transferred outside the company. By getting a clear understanding of how data makes its way outside, you can take whatever measures are necessary to prevent information from leaking via USB memory devices.

Security management

Control network connections

HITACHI

When a PC that you are not managing attempts to connect to a network segment including another PC that is monitoring the network, the new PC is identified as a new device and can be blocked. In addition, PCs that are deemed unsafe and PCs infected by malware can be automatically quarantined. JP1 can send an email to the administrator whenever a PC is blocked or quarantined.



Discover and block, in real time, PCs that are not being managed

Quarantine unsafe PCs

Quarantine PCs infected by malware

Tips

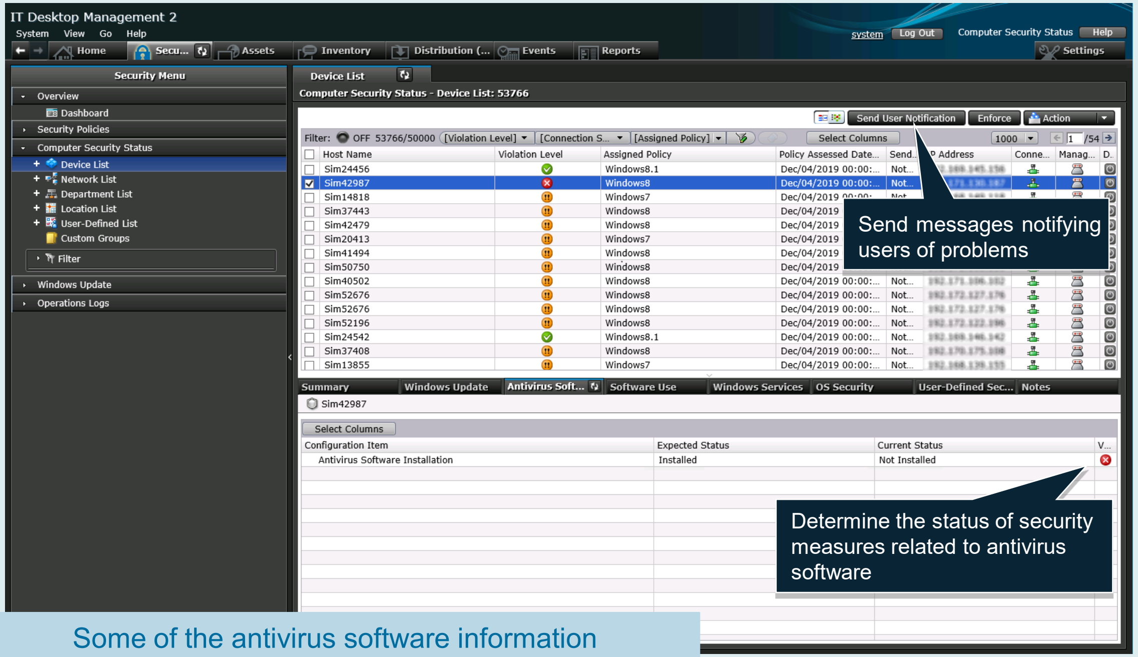
- ●After an unsafe PC is quarantined, the necessary security measures can be applied to that PC either automatically or manually. The PC is then reassessed and, if it is deemed secure, it is automatically granted permission to reconnect to the network.
- ●You can also configure the system so that PCs that you are not managing are not actually blocked from the network. Instead, a notification is simply sent to the administrator whenever JP1 detects that such a PC has connected to the network.
- ●By linking JP1 with Microsoft Intune and Microsoft Defender, you can automatically quarantine unsafe devices that have been infected by malware.

Security management

Implement thorough virus protections

You can check whether there are any problems with security measures related to antivirus software, and distribute and install the newest versions of antivirus software products on PCs where such products are not up to date.

Security module (Device List)



Computer Security Status - Device List: 53766

Filter: OFF 53766/50000 [Violation Level] [Connection S... [Assigned Policy] 1000 1 /54

	Host Name	Violation Level	Assigned Policy	Policy Assessed Date...	Send...	IP Address	Conne...	Manag...	D...
□	Sim24456	✓	Windows8.1	Dec/04/2019 00:00:...	Not...	[redacted]			
☑	Sim42987	✗	Windows8	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim14818	!!	Windows7	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim37443	!!	Windows8	Dec/04/2019					
□	Sim42479	!!	Windows8	Dec/04/2019					
□	Sim20413	!!	Windows7	Dec/04/2019					
□	Sim41494	!!	Windows8	Dec/04/2019					
□	Sim50750	!!	Windows8	Dec/04/2019					
□	Sim40502	!!	Windows8	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim52676	!!	Windows8	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim52676	!!	Windows8	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim52196	!!	Windows8	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim24542	✓	Windows8.1	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim37408	!!	Windows8	Dec/04/2019 00:00:...	Not...	[redacted]			
□	Sim13855	!!	Windows7	Dec/04/2019 00:00:...	Not...	[redacted]			

Summary | Windows Update | Antivirus Soft... | Software Use | Windows Services | OS Security | User-Defined Sec... | Notes

Sim42987

Select Columns

Configuration Item	Expected Status	Current Status	V...
Antivirus Software Installation	Installed	Not Installed	✗

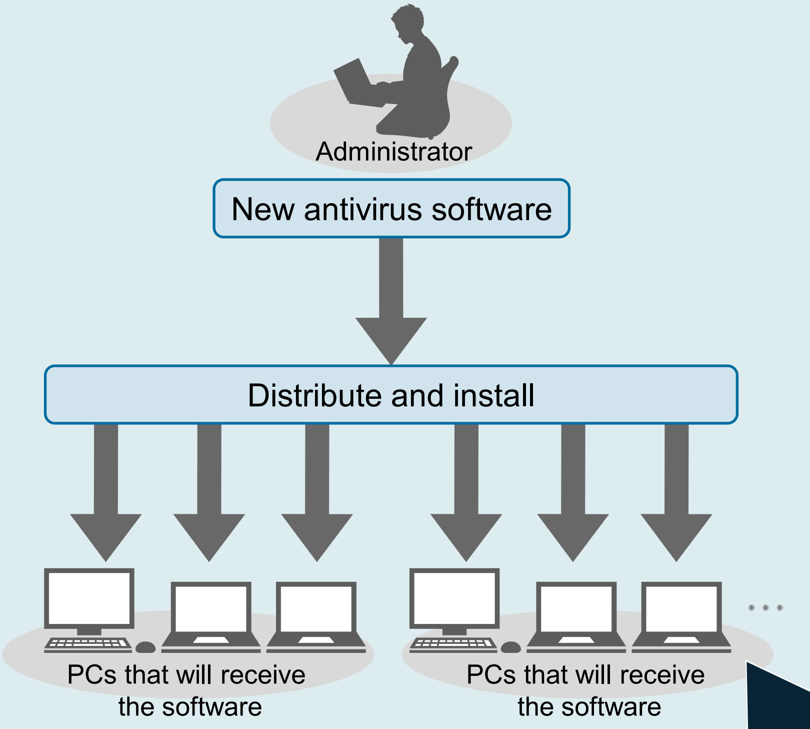
Send messages notifying users of problems

Determine the status of security measures related to antivirus software

Some of the antivirus software information that can be checked

- Whether a product is installed
- Product version
- Scan engine version
- Version of the virus definition file
- Date and time of the last scan

Note: Depending on the antivirus software, some types of information cannot be collected. For details, see the applicable JP1 product manual.

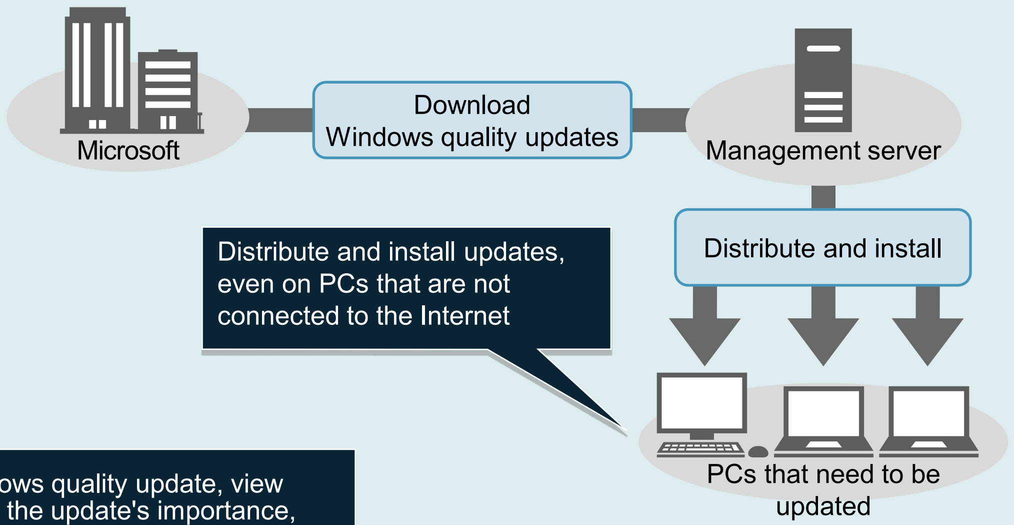

Administrator
New antivirus software
Distribute and install
PCs that will receive the software
PCs that will receive the software
...

During installation, automatically power on PCs that are not running, and then power them off after installation is complete*

* To automatically power on a PC, the PC must support Wake-on-LAN or Intel AMT (Active Management Technology).

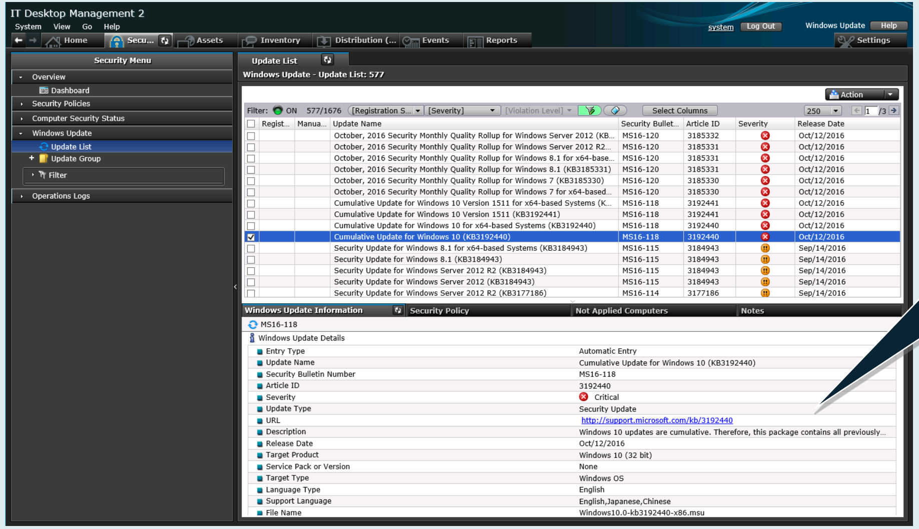
Install and manage Windows quality updates

Windows quality updates can be distributed and installed on PCs that you are managing. As long as the management server is connected to the Internet, the entire process can be automated.
You can manually distribute and install individual Windows quality updates, an indispensable option when there is an urgent update that needs to be installed right away.



Distribute and install updates, even on PCs that are not connected to the Internet

Security module (Update List)



Windows Update - Update List: 577

Filter: ● ON 577/1676 [Registration S... [Severity] [Violation Level] 250 1 /3

	Regist...	Manua...	Update Name	Security Bullet...	Article ID	Severity	Release Date
□			October, 2016 Security Monthly Quality Rollup for Windows Server 2012 (KB...	MS16-120	3185332	✖	Oct/12/2016
□			October, 2016 Security Monthly Quality Rollup for Windows Server 2012 R2...	MS16-120	3185331	✖	Oct/12/2016
□			October, 2016 Security Monthly Quality Rollup for Windows 8.1 for x64-base...	MS16-120	3185331	✖	Oct/12/2016
□			October, 2016 Security Monthly Quality Rollup for Windows 8.1 (KB3185331)	MS16-120	3185331	✖	Oct/12/2016
□			October, 2016 Security Monthly Quality Rollup for Windows 7 (KB3185330)	MS16-120	3185330	✖	Oct/12/2016
□			October, 2016 Security Monthly Quality Rollup for Windows 7 for x64-based...	MS16-120	3185330	✖	Oct/12/2016
□			Cumulative Update for Windows 10 Version 1511 for x64-based Systems (K...	MS16-118	3192441	✖	Oct/12/2016
□			Cumulative Update for Windows 10 Version 1511 (KB3192441)	MS16-118	3192441	✖	Oct/12/2016
□			Cumulative Update for Windows 10 for x64-based Systems (KB3192440)	MS16-118	3192440	✖	Oct/12/2016
☑			Cumulative Update for Windows 10 (KB3192440)	MS16-118	3192440	✖	Oct/12/2016
□			Security Update for Windows 8.1 for x64-based Systems (KB3184943)	MS16-115	3184943	‼	Sep/14/2016
□			Security Update for Windows 8.1 (KB3184943)	MS16-115	3184943	‼	Sep/14/2016
□			Security Update for Windows Server 2012 R2 (KB3184943)	MS16-115	3184943	‼	Sep/14/2016
□			Security Update for Windows Server 2012 (KB3184943)	MS16-115	3184943	‼	Sep/14/2016
□			Security Update for Windows Server 2012 R2 (KB3177186)	MS16-114	3177186	‼	Sep/14/2016

Windows Update Information | Security Policy | Not Applied Computers | Notes

MS16-118

Windows Update Details

Entry Type	Automatic Entry
Update Name	Cumulative Update for Windows 10 (KB3192440)
Security Bulletin Number	MS16-118
Article ID	3192440
Severity	✖ Critical
Update Type	Security Update
URL	http://support.microsoft.com/kb/3192440
Description	Windows 10 updates are cumulative. Therefore, this package contains all previously...
Release Date	Oct/12/2016
Target Product	Windows 10 (32 bit)
Service Pack or Version	None
Target Type	Windows OS
Language Type	English
Support Language	English,Japanese,Chinese
File Name	Windows10.0-kb3192440-x86.msu

For each Windows quality update, view details such as the update's importance, a link to a description of the update, and the site from which you can download the update

As new Windows quality updates become available, they are automatically added to the update list.

Note: Automatic distribution of Windows quality updates requires a subscription to JP1 support services. It takes approximately two weeks from when Windows quality updates first become available until the time that they can be automatically distributed. The types of Windows quality updates that can be automatically distributed include important updates and security updates. Service packs and updates to other software (such as Microsoft Office) are not included.

Have you experienced any of these issues?

HITACHI

☑ Need to accurately keep track of what software is installed, and how many PCs and devices you are managing?

Manage IT assets all in one place p. 21

With JP1, you can automatically collect information about hardware devices and software programs over the network. In addition to on-premises devices connected to the network, you can also manage notebook computers that are only occasionally connected to the network, as well as notebook computers, thin clients, and smart devices that are taken off-premises for remote work. Even contract-related information (such as the contract type and period) can be registered and managed in association with the relevant IT assets.

☑ Need to check whether you have enough licenses for your software?

Manage software licenses p. 24

JP1 can automatically identify what software is installed on managed PCs and then incorporate this information to show you the number of licenses you own, the number of licenses in use, and the number of licenses still available. You can check this data to make sure you are not using any software programs in excess of the licenses that you have purchased. JP1 also allows you to identify the PCs on which a program has been installed but to which no license has been allocated.

☑ Need to be able to easily search through a large number of contracts?

Manage contract information p. 25

JP1 allows you to manage contract information (contract type, start and end dates, status, etc.) in association with managed IT assets. Actual contract documents can be scanned and the resulting electronic data can then be saved as an attachment to the contract information. This means that, instead of having to search for physical documents, you can quickly and easily check the contents of a contract from JP1.

☑ Need to optimize the way you take stock of your IT assets?

Optimize your inventory processes p. 26

JP1 can be used to collect information about the types of devices being used at your company, including PCs and servers. You can keep data about your IT assets up to date simply by registering new devices and maintaining information about persons managing existing devices. You can also output this information to a list that can be used when checking for actual devices, making inventory processes more efficient.

☑ Need to address problems that occur on PCs without having to be on-site?

Control devices remotely p. 27

When a problem occurs on a PC at a remote site, you can solve the problem remotely from the convenience of your own desk. Remote connectivity allows you to send and receive required data to and from PCs. You can even record a video of your remote operations to use later when explaining the process to other users.

☑ Need to frequently distribute and install software on your company's PCs and servers?

Automate software distribution and installation p. 29

You can use JP1 to automatically distribute and install software on your company's remote PCs and servers. JP1 provides a wide array of functions that allow you to distribute software to only a specific subset of PCs (for example, PCs belonging to a particular department) and to specify the date and time when software is to be distributed and installed. With these and many other detailed settings, JP1 allows you to customize your software distribution operations.

☑ Need to apply Windows feature updates without interrupting your operations?

Install and manage Windows feature updates p. 30

You can use JP1 to postpone the application of Windows 11 feature updates or to disable automatic updates. This prevents your OSs from being updated automatically, thereby lightening the load on the network when an update is distributed and allowing you to control the timing of updates. As a result, you can apply OS updates in a planned manner with a minimum impact on business operations, even in a large-scale environment.

☑ Need to ensure the proper management of smart devices used in your company?

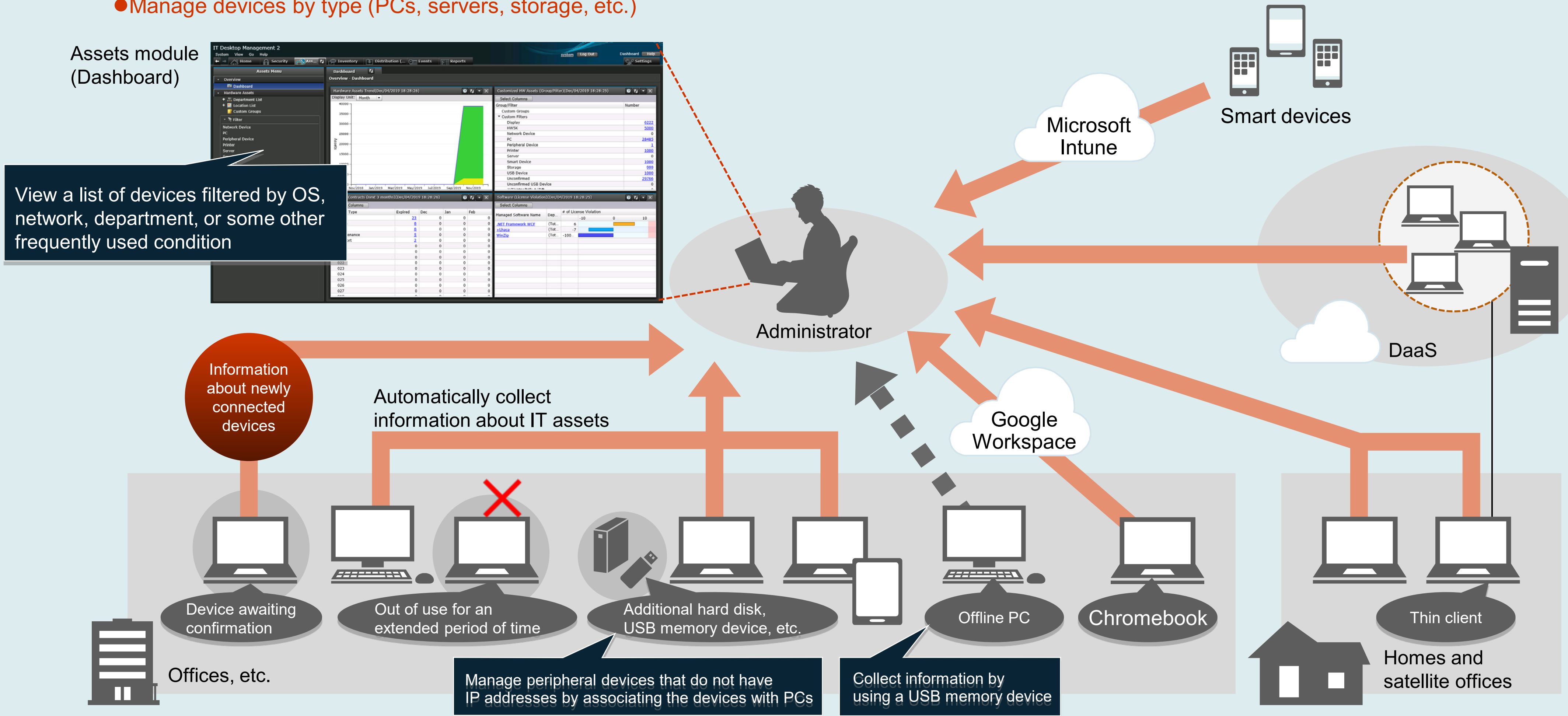
Manage smart devices p. 31

JP1 allows you to collect information from smart devices (such as smartphones and tablets) and manage them together with other devices such as computers and servers. If a smart device is lost, the administrator can lock or initialize the device to mitigate risks.

Manage IT assets all in one place: Manage devices

You can collect all types of information about a device, from its specifications (such as its operating system, memory, and hard disk capacity) to network information (such as its IP address and MAC address). You can even collect information about a PC's users and associated department. Based on this information, JP1 can identify whenever someone connects an unknown device to the network and then inform the administrator that a new device needs to be confirmed.

Examples
- ●Identify PCs that have been disconnected from the network for an extended period of time
- ●Manage devices by type (PCs, servers, storage, etc.)


Assets module
(Dashboard)
IT Desktop Management 2
Administrator
Microsoft Intune
Smart devices
DaaS
Information about newly connected devices
Automatically collect information about IT assets
Google Workspace
Device awaiting confirmation
Out of use for an extended period of time
Additional hard disk, USB memory device, etc.
Offline PC
Chromebook
Thin client
Offices, etc.
Homes and satellite offices

View a list of devices filtered by OS, network, department, or some other frequently used condition

Manage peripheral devices that do not have IP addresses by associating the devices with PCs

Collect information by using a USB memory device

What you can do >
Security management >
Asset management >

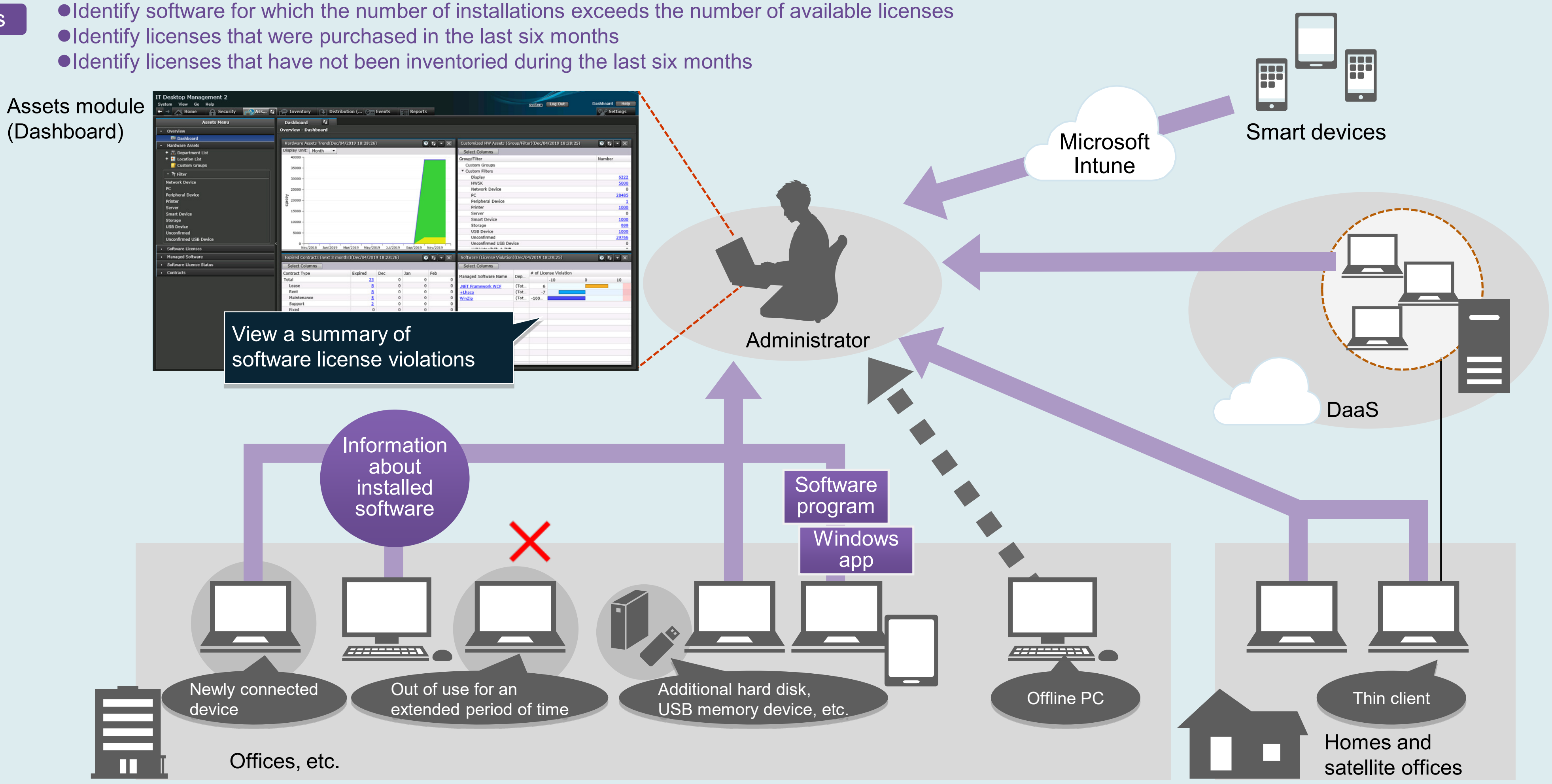
Manage IT assets all in one place:
Manage software

HITACHI

You can use JP1 to collect information about installed programs and Windows apps, including their names, their versions, and when they were installed. After collecting this information, if you discover a program or an app that you want to prohibit, you can do so easily from the list of installed programs and apps. JP1 can also be used to automatically aggregate data about software license use, such as the number of times a program has been installed and the number of licenses you own for that program. You can use this information to make sure that your licenses are being used properly.

Examples

- Identify software for which the number of installations exceeds the number of available licenses
- Identify licenses that were purchased in the last six months
- Identify licenses that have not been inventoried during the last six months



Group/Filter	Number
Custom Groups	
Custom Filters	
Display	6222
HW5K	5000
Network Device	0
PC	28485
Peripheral Device	1
Printer	1000
Server	0
Smart Device	1000
Storage	999
USB Device	1000
Unconfirmed	29766
Unconfirmed USB Device	0

Contract Type	Expired	Dec	Jan	Feb
Total	23	0	0	0
Lease	8	0	0	0
Rent	8	0	0	0
Maintenance	5	0	0	0
Support	2	0	0	0
Fixed	0	0	0	0

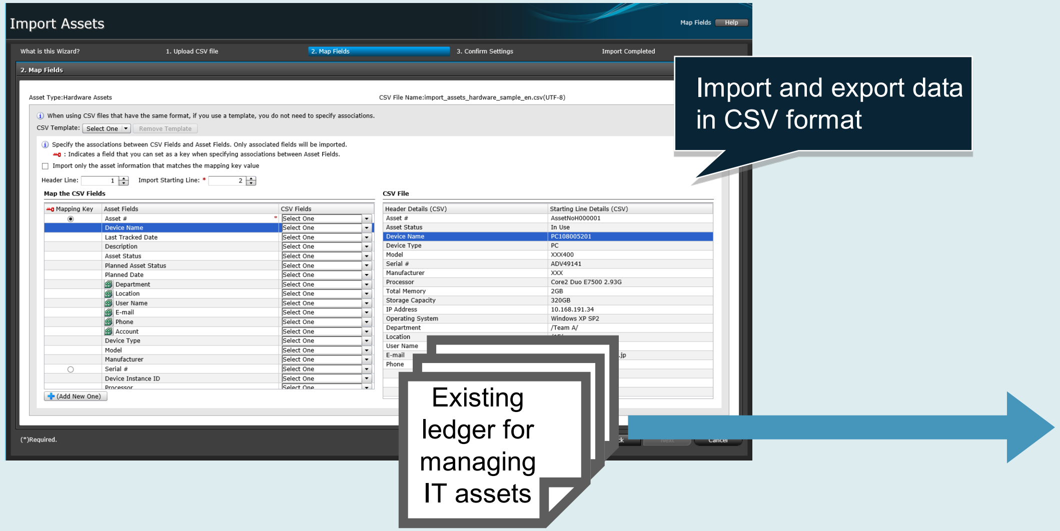
Managed Software Name	Dep...	# of License Violation
.NET Framework WCF	(Tot...	6
+Lhaca	(Tot...	-7
WinZip	(Tot...	-100...

Manage IT assets all in one place:
Centrally manage IT assets and contract information

HITACHI

If you already have a ledger for managing your IT assets or a ledger for recording contract information (the names and contact information of vendors you have contracted with), you can easily import it into JP1 by using the Import Assets wizard. The imported information can then be used in combination with data that JP1 automatically collects, such as information about devices, software, and contracts (contract type, contract period, etc.).

Import Assets wizard



2. Map Fields

Asset Type:Hardware Assets

CSV File Name:import_assets_hardware_sample_en.csv(UTF-8)

When using CSV files that have the same format, if you use a template, you do not need to specify associations.

CSV Template: Select One

Specify the associations between CSV Fields and Asset Fields. Only associated fields will be imported.

: Indicates a field that you can set as a key when specifying associations between Asset Fields.

□ Import only the asset information that matches the mapping key value

Header Line: 1 Import Starting Line: * 2

Map the CSV Fields

Mapping Key	Asset Fields	CSV Fields
●	Asset # *	Select One
	Device Name	Select One
	Last Tracked Date	Select One
	Description	Select One
	Asset Status	Select One
	Planned Asset Status	Select One
	Planned Date	Select One
	Department	Select One
	Location	Select One
	User Name	Select One
	E-mail	Select One
	Phone	Select One
	Account	Select One
	Device Type	Select One
	Model	Select One
	Manufacturer	Select One
○	Serial #	Select One
	Device Instance ID	Select One
	Processor	Select One

CSV File

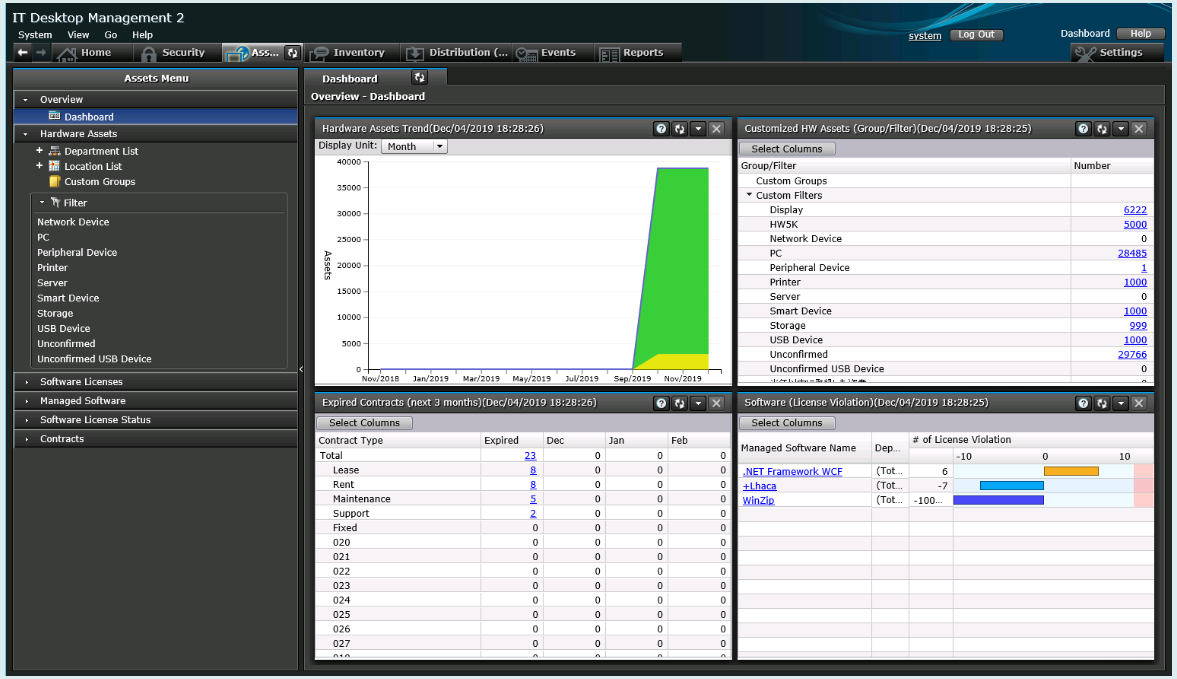
Header Details (CSV)	Starting Line Details (CSV)
Asset #	AssetNoH000001
Asset Status	In Use
Device Name	PC108005201
Device Type	PC
Model	XXX400
Serial #	ADV49141
Manufacturer	XXX
Processor	Core2 Duo E7500 2.93G
Total Memory	2GB
Storage Capacity	320GB
IP Address	10.168.191.34
Operating System	Windows XP SP2
Department	/Team A/
Location	
User Name	
E-mail	.jp
Phone	

(*)Required.

Import and export data in CSV format

Existing ledger for managing IT assets

Assets module (Dashboard)



Hardware Assets Trend(Dec/04/2019 18:28:26)

Customized HW Assets (Group/Filter)(Dec/04/2019 18:28:25)

Group/Filter	Number
Custom Groups	
Custom Filters	
Display	6222
HW5K	5000
Network Device	0
PC	28485
Peripheral Device	1
Printer	1000
Server	0
Smart Device	1000
Storage	999
USB Device	1000
Unconfirmed	29766
Unconfirmed USB Device	0

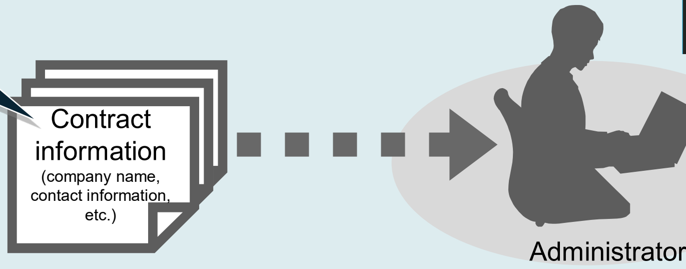
Expired Contracts (next 3 months)(Dec/04/2019 18:28:26)

Contract Type	Expired	Dec	Jan	Feb
Total	23	0	0	0
Lease	8	0	0	0
Rent	8	0	0	0
Maintenance	5	0	0	0
Support	2	0	0	0
Fixed	0	0	0	0
020	0	0	0	0
021	0	0	0	0
022	0	0	0	0
023	0	0	0	0
024	0	0	0	0
025	0	0	0	0
026	0	0	0	0
027	0	0	0	0

Software (License Violation)(Dec/04/2019 18:28:25)

Managed Software Name	Dep...	# of License Violation
.NET Framework WCF	(Tot...	6
+Lhaca	(Tot...	-7
WinZip	(Tot...	-100...

Centrally manage contract information as well

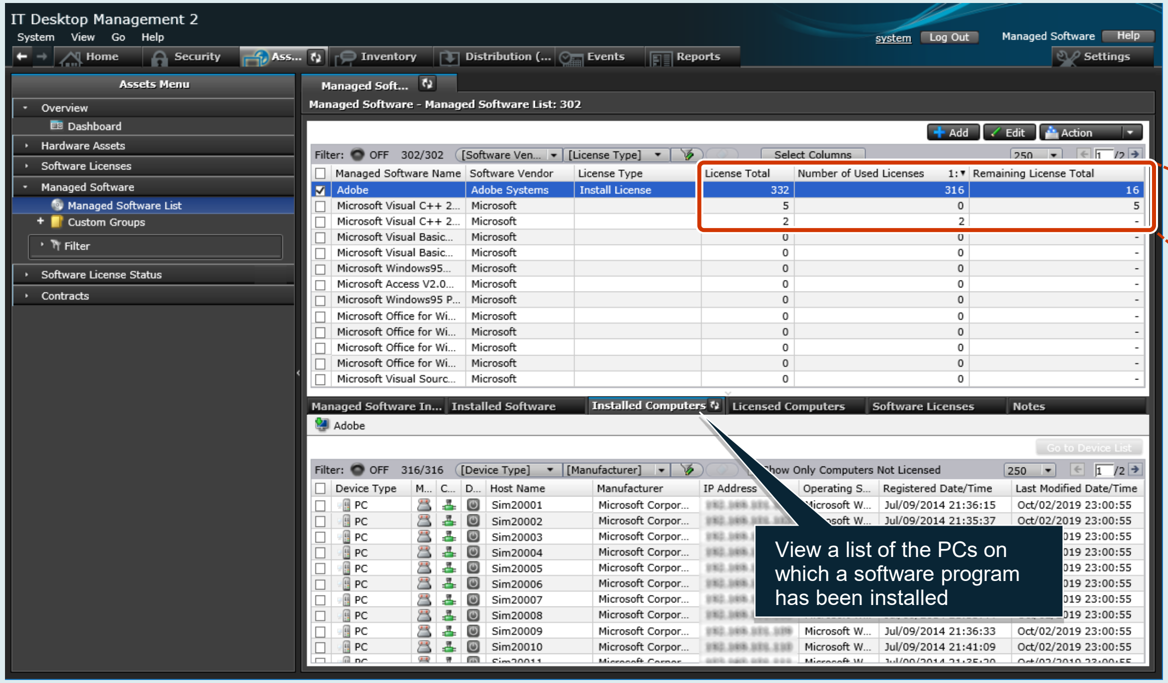


Contract information
(company name, contact information, etc.)

Manage software licenses

With JP1, you can determine the number of software licenses that have been allocated, the PCs to which they have been allocated, the number of times the software has actually been installed, and the PCs on which the software has been installed. If software has been installed on a PC that has not been allocated a license, you can inform the user of that PC that, as a rule, permission to use any software must be obtained via the proper procedures before users are allowed to install that software. This monitoring ability helps prevent both unapproved installations and license violations.

Assets module (Managed Software List)



Managed Software - Managed Software List: 302

Filter: OFF 302/302 [Software Ven...] [License Type] 250 1 /2

	Managed Software Name	Software Vendor	License Type	License Total	Number of Used Licenses 1:▼	Remaining License Total
☑	Adobe	Adobe Systems	Install License	332	316	16
□	Microsoft Visual C++ 2...	Microsoft		5	0	5
□	Microsoft Visual C++ 2...	Microsoft		2	2	-
□	Microsoft Visual Basic...	Microsoft		0	0	-
□	Microsoft Visual Basic...	Microsoft		0	0	-
□	Microsoft Windows95...	Microsoft		0	0	-
□	Microsoft Access V2.0...	Microsoft		0	0	-
□	Microsoft Windows95 P...	Microsoft		0	0	-
□	Microsoft Office for Wi...	Microsoft		0	0	-
□	Microsoft Office for Wi...	Microsoft		0	0	-
□	Microsoft Office for Wi...	Microsoft		0	0	-
□	Microsoft Office for Wi...	Microsoft		0	0	-
□	Microsoft Visual Sourc...	Microsoft		0	0	-

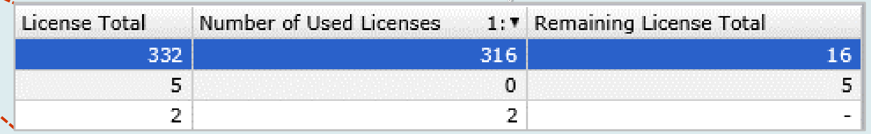
Adobe

Filter: OFF 316/316 [Device Type] [Manufacturer] □ Show Only Computers Not Licensed 250 1 /2

□	Device Type	M...	C...	D...	Host Name	Manufacturer	IP Address	Operating S...	Registered Date/Time	Last Modified Date/Time
□	PC				Sim20001	Microsoft Corpor...	[redacted]	Microsoft W...	Jul/09/2014 21:36:15	Oct/02/2019 23:00:55
□	PC				Sim20002	Microsoft Corpor...	[redacted]	soft W...	Jul/09/2014 21:35:37	Oct/02/2019 23:00:55
□	PC				Sim20003	Microsoft Corpor...	[redacted]			019 23:00:55
□	PC				Sim20004	Microsoft Corpor...	[redacted]			019 23:00:55
□	PC				Sim20005	Microsoft Corpor...	[redacted]			019 23:00:55
□	PC				Sim20006	Microsoft Corpor...	[redacted]			019 23:00:55
□	PC				Sim20007	Microsoft Corpor...	[redacted]			019 23:00:55
□	PC				Sim20008	Microsoft Corpor...	[redacted]			019 23:00:55
□	PC				Sim20009	Microsoft Corpor...	[redacted]	Microsoft W...	Jul/09/2014 21:36:33	Oct/02/2019 23:00:55
□	PC				Sim20010	Microsoft Corpor...	[redacted]	Microsoft W...	Jul/09/2014 21:41:09	Oct/02/2019 23:00:55

View a list of the PCs on which a software program has been installed

For each software program, check the number of licenses you own, how many are being used, and how many have not been allocated



License Total	Number of Used Licenses 1:▼	Remaining License Total
332	316	16
5	0	5
2	2	-

Tips

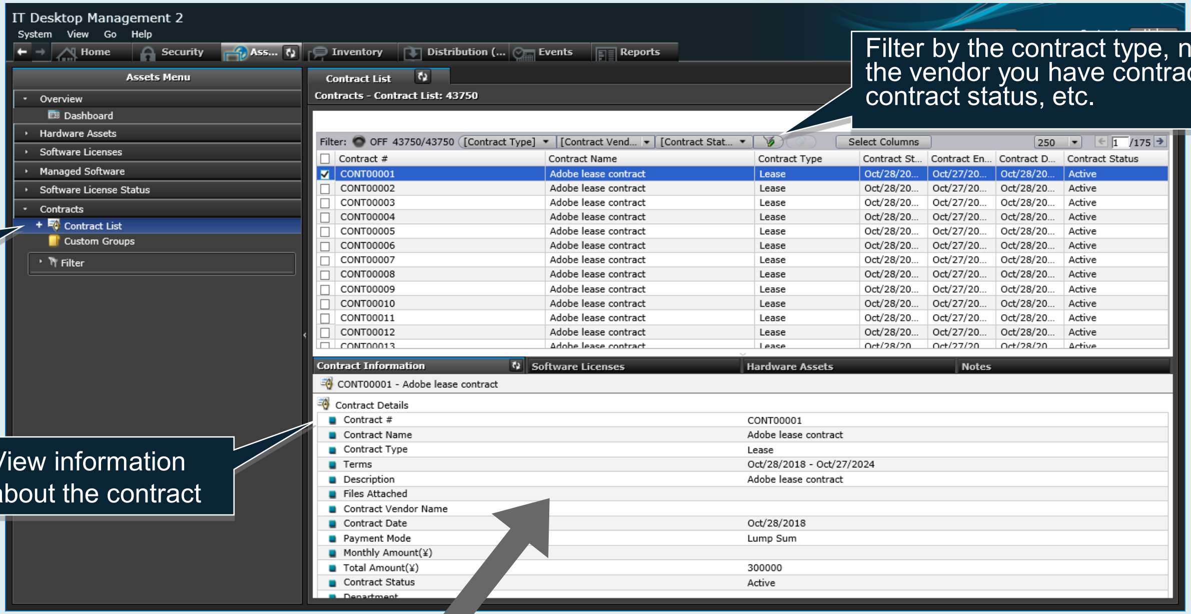
- ●Licenses for Microsoft Office products can be managed as either product licenses or volume licenses. Managing licenses as volume licenses is done by grouping individual licenses by product ID.*
- ●JP1 automatically calculates the number of software licenses that are currently in use and then compares this number with the number of licenses you own to determine whether you have a license surplus or deficit. All of this information can be viewed in a report.

* Some Microsoft Office products cannot be managed by product ID.

Manage contract information

You can manage support service contracts, rental agreements, lease agreements, and other types of contracts by registering information about each contract and associating it with information about the relevant assets. JP1 helps you identify contracts whose expiration dates are drawing near, allowing you to take action before contracts expire.

Assets module (Contract List)



Contracts - Contract List: 43750

Filter: OFF 43750/43750 [Contract Type] [Contract Vend... [Contract Stat... Select Columns 250 1 /175

	Contract #	Contract Name	Contract Type	Contract St...	Contract En...	Contract D...	Contract Status
☑	CONT00001	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00002	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00003	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00004	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00005	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00006	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00007	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00008	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00009	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00010	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00011	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00012	Adobe lease contract	Lease	Oct/28/20...	Oct/27/20...	Oct/28/20...	Active
□	CONT00013	Adobe lease contract	Lease	Oct/28/20	Oct/27/20	Oct/28/20	Active

CONT00001 - Adobe lease contract

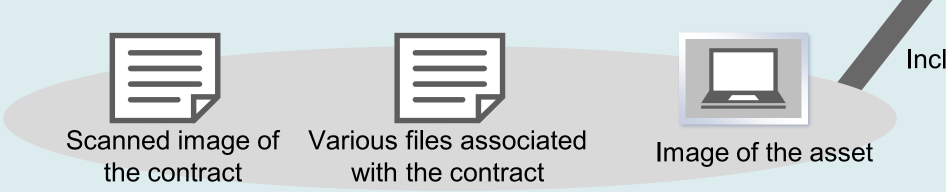
Contract Details

Contract #	CONT00001
Contract Name	Adobe lease contract
Contract Type	Lease
Terms	Oct/28/2018 - Oct/27/2024
Description	Adobe lease contract
Files Attached	
Contract Vendor Name	
Contract Date	Oct/28/2018
Payment Mode	Lump Sum
Monthly Amount(¥)	
Total Amount(¥)	300000
Contract Status	Active
Department	

Filter by the contract type, name of the vendor you have contracted with, contract status, etc.

Manage information about software contracts and more in a list

View information about the contract



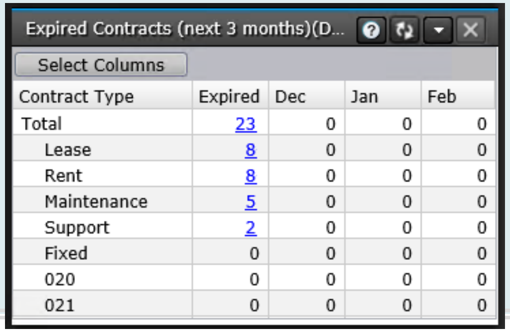
Scanned image of the contract

Various files associated with the contract

Image of the asset

Include multiple attachments, regardless of the type of data

Home module (panel showing expired contracts and those that expire in the next three months)



Contract Type	Expired	Dec	Jan	Feb
Total	23	0	0	0
Lease	8	0	0	0
Rent	8	0	0	0
Maintenance	5	0	0	0
Support	2	0	0	0
Fixed	0	0	0	0
020	0	0	0	0
021	0	0	0	0

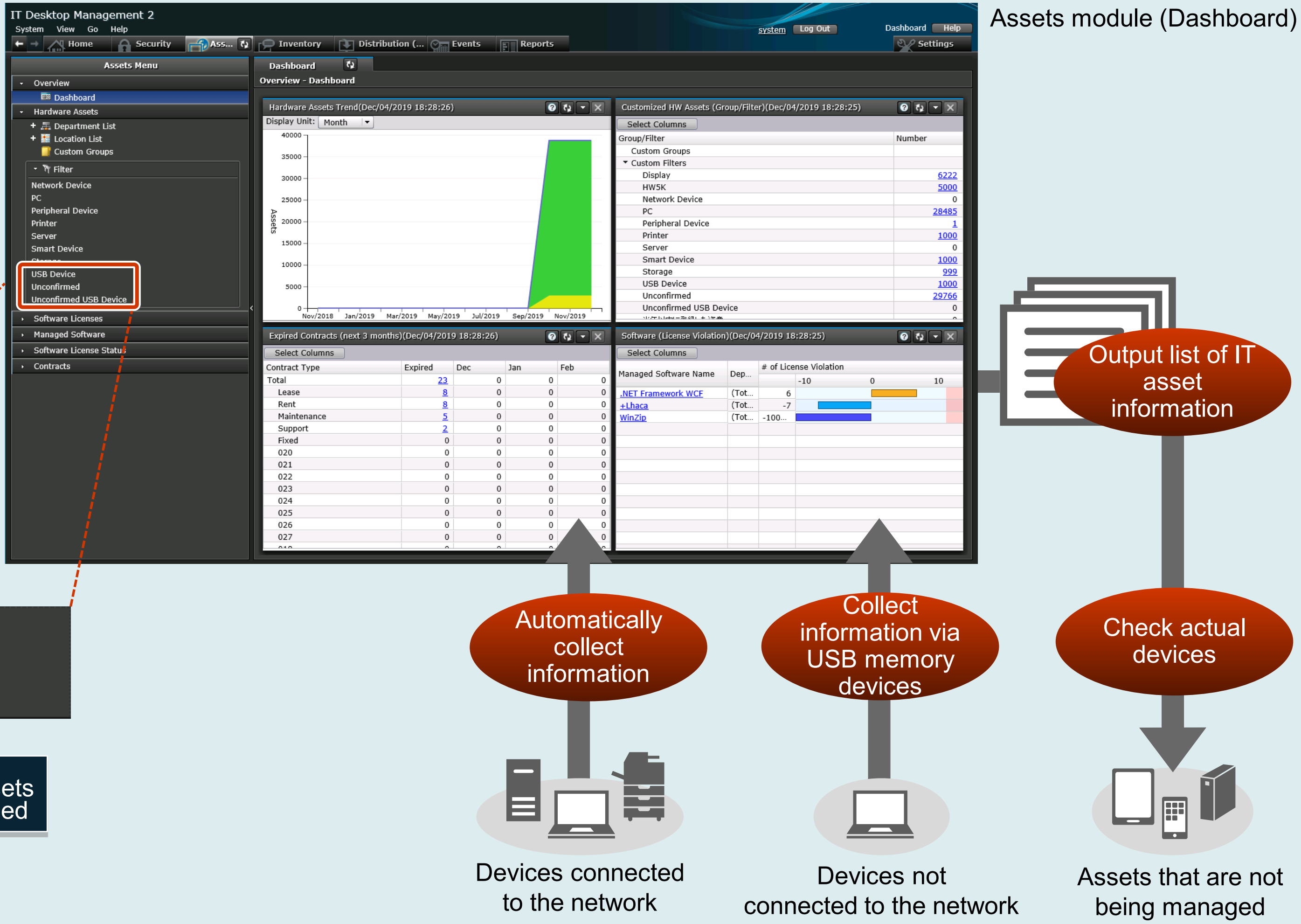
Tips

- ●By configuring the Home module to display contract expiration dates, you can easily check which contracts are set to expire in the near future.
- ●Contract expiration dates are also included in the summary reports that are created on a daily, weekly, and monthly basis, helping to ensure that contracts are renewed before they expire.

Asset management

Optimize your inventory processes

Even if the person managing a PC or other device changes (for example, because the department moves to a new location or the device is now managed by another department), you can still confirm the existence of that device as long as it is connected to the network. Based on information such as the device's IP address, you can easily identify the device's location, helping you take stock of your assets more efficiently.



Assets module (Dashboard)

Customized HW Assets (Group/Filter)(Dec/04/2019 18:28:25)

Group/Filter	Number
Custom Groups	
Custom Filters	
Display	6222
HW5K	5000
Network Device	0
PC	28485
Peripheral Device	1
Printer	1000
Server	0
Smart Device	1000
Storage	999
USB Device	1000
Unconfirmed	29766
Unconfirmed USB Device	0

Expired Contracts (next 3 months)(Dec/04/2019 18:28:26)

Contract Type	Expired	Dec	Jan	Feb
Total	23	0	0	0
Lease	8	0	0	0
Rent	8	0	0	0
Maintenance	5	0	0	0
Support	2	0	0	0
Fixed	0	0	0	0
020	0	0	0	0
021	0	0	0	0
022	0	0	0	0
023	0	0	0	0
024	0	0	0	0
025	0	0	0	0
026	0	0	0	0
027	0	0	0	0

Software (License Violation)(Dec/04/2019 18:28:25)

Managed Software Name	Dep...	# of License Violation
.NET Framework WCF	(Tot...	6
+Lhaca	(Tot...	-7
WinZip	(Tot...	-100...

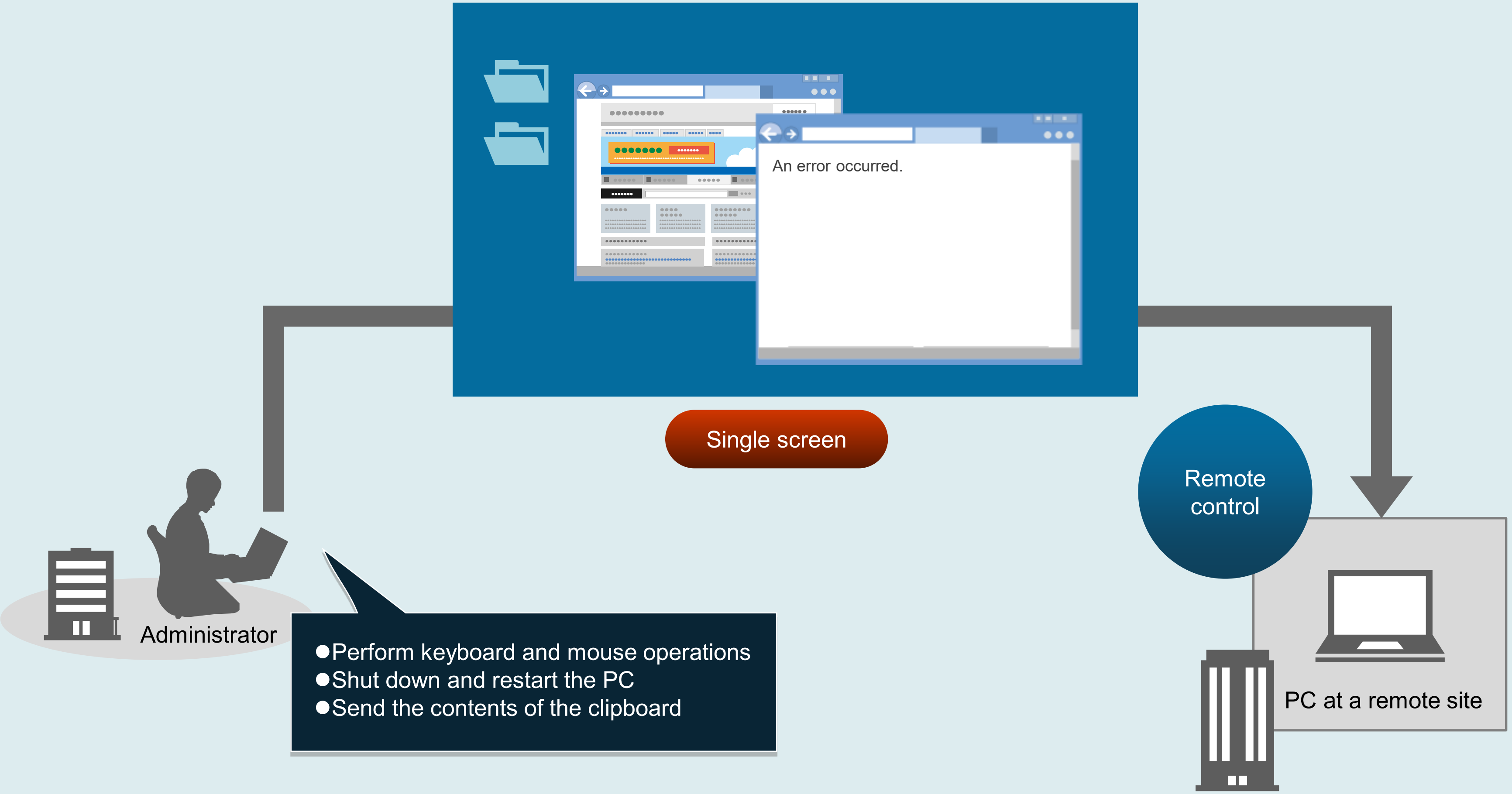
USB Device
Unconfirmed
Unconfirmed USB Device

Filter to display only assets that need to be inventoried

Control devices remotely:
Perform operations on remote PCs

HITACHI

Administrators can connect to a remote PC and view its desktop from their own PCs. By doing so, administrators are able to operate remote PCs in exactly the same way as if they were operating their own PCs.

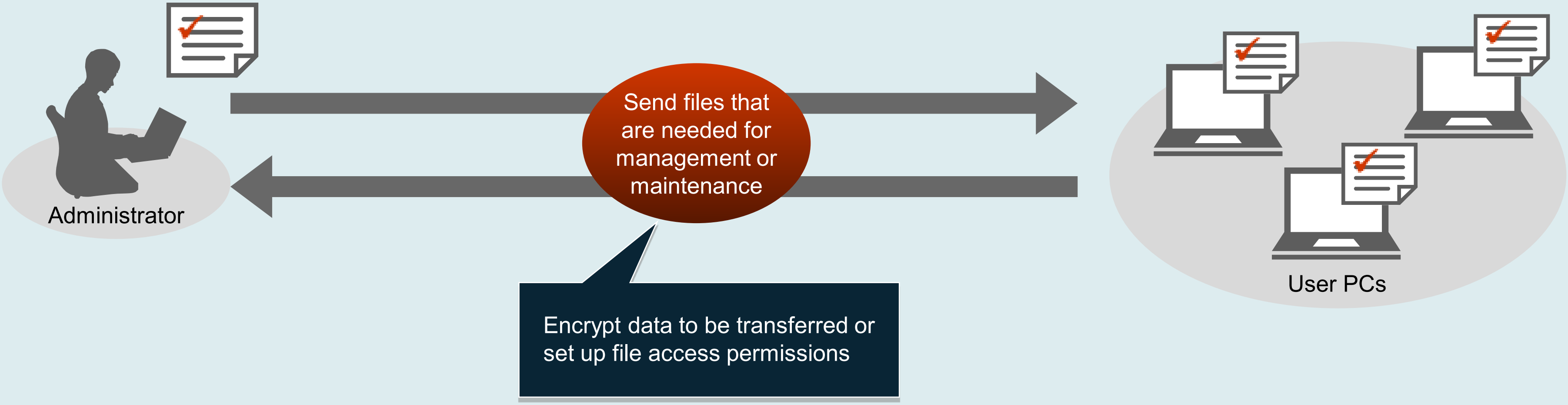


An error occurred.

- Perform keyboard and mouse operations
- Shut down and restart the PC
- Send the contents of the clipboard

Control devices remotely: Transfer files

By using standard Windows Explorer operations, you can view the files on a remote computer that are needed for management or maintenance and send files by using drag-and-drop operations. Moreover, you can connect to multiple computers and send files to all of them at the same time. These features can be useful when you want to collect and analyze the log files from multiple PCs on which a problem has occurred, or when you want to send data to multiple PCs.


Administrator
Send files that are needed for management or maintenance
User PCs
Encrypt data to be transferred or set up file access permissions

Tips

- In addition to recording and playing back a video of your operations, you can also communicate (via chat) with the user of the remote computer in real time.
- To ensure that your company's PCs do not become subject to illicit remote operations, you can dictate which PCs and users are permitted to perform remote operations.
- When the remote PC supports AMT*, the optical drive on the administrator's PC can be used as if it were a drive on the remote PC.

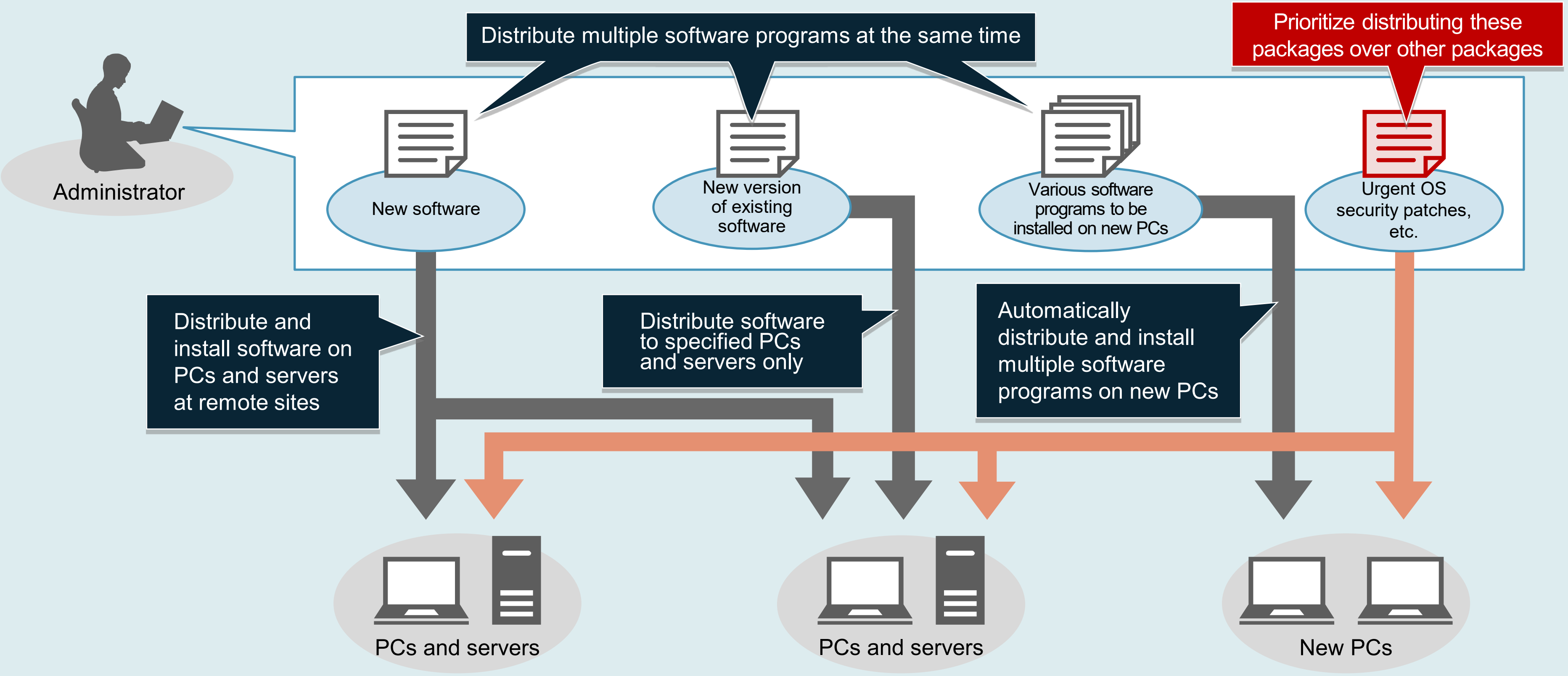
* For information on the versions of AMT that are supported by JP1, see the applicable JP1 product manual.

Asset management

Automate software distribution and installation

HITACHI

JP1 helps you efficiently distribute and install software programs (prepared by an administrator) on your company's PCs and servers, even those at remote sites. Use this feature to upgrade any software program to its latest version on multiple PCs in a single step, install software onto new PCs, and more.


Distribute multiple software programs at the same time
Prioritize distributing these packages over other packages
Administrator
New software
New version of existing software
Various software programs to be installed on new PCs
Urgent OS security patches, etc.
Distribute and install software on PCs and servers at remote sites
Distribute software to specified PCs and servers only
Automatically distribute and install multiple software programs on new PCs
PCs and servers
PCs and servers
New PCs

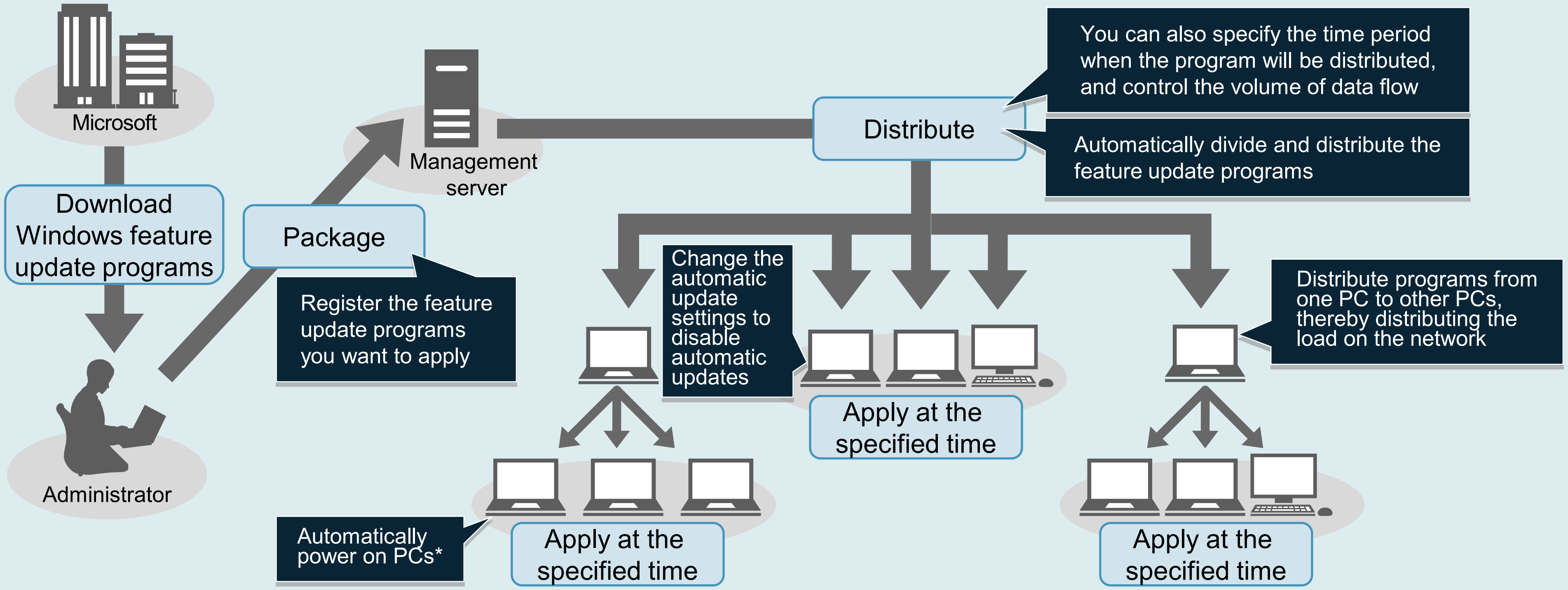
Tip

When you want to send a software program or file to multiple PCs and servers, you can reduce the overall size of the data to be sent, or split large files so that they can be sent at specified intervals. These techniques can reduce the load on your network.

Install and manage Windows feature updates

HITACHI

When a Windows feature update program is downloaded to the administrator's PC, you can distribute the update to multiple PCs according to a plan that places minimal load on the network. You can then apply the update in a batch operation, on a date and time that you specify in advance. In this way, you can control the application of Windows feature updates to PCs within your company.



Download Windows feature update programs

Package

Register the feature update programs you want to apply

Distribute

You can also specify the time period when the program will be distributed, and control the volume of data flow

Automatically divide and distribute the feature update programs

Change the automatic update settings to disable automatic updates

Distribute programs from one PC to other PCs, thereby distributing the load on the network

Apply at the specified time

Apply at the specified time

Apply at the specified time

Automatically power on PCs*

* To automatically power on a PC, the PC must support Wake-on-LAN or Intel AMT (Active Management Technology).

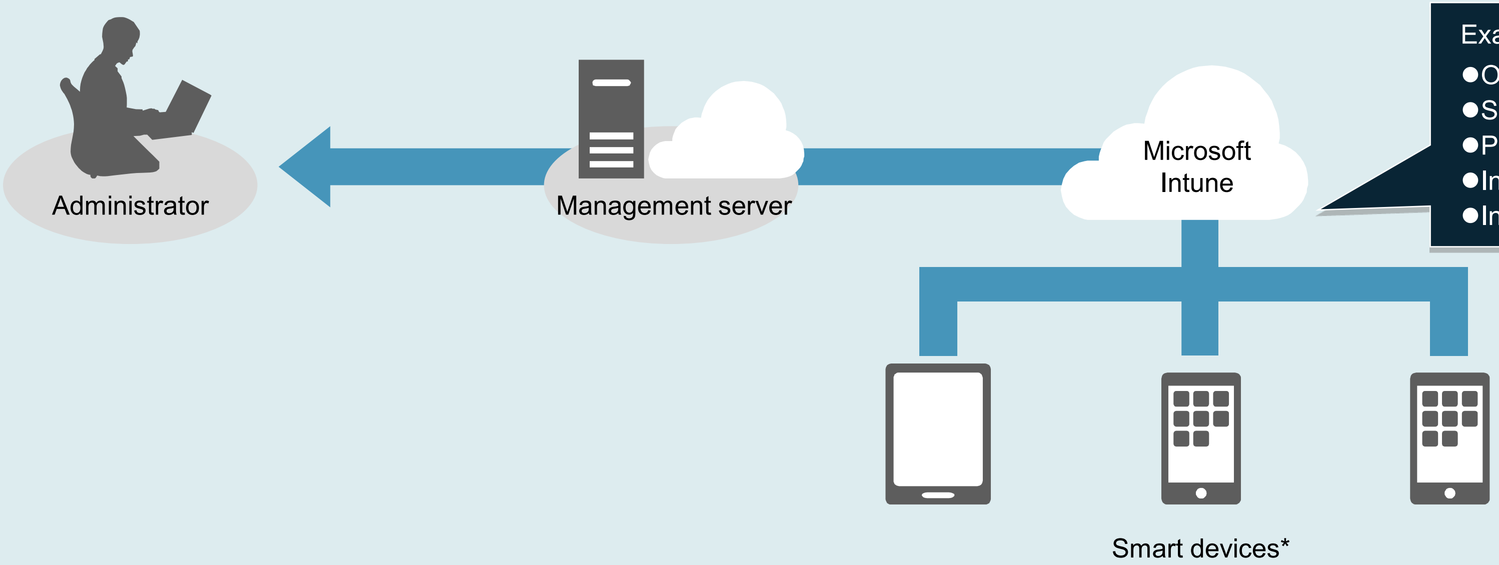
Tip

You can output, to a CSV file, information about the application statuses of Windows feature update programs for PCs within your company.
This allows you to easily check the application statuses in list form.

Manage smart devices:
Collect information about and control smart devices

■Collect information about smart devices

By linking with Microsoft Intune, JP1 can collection information about smart devices, such as their OS, serial number, and contract phone number. You can manage this information from the same window that you use to manage PCs and servers.

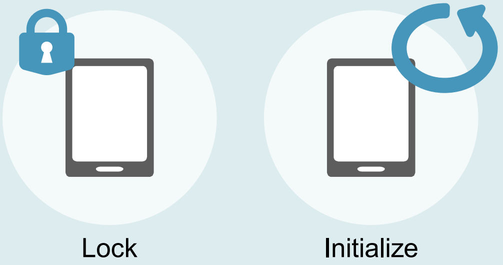


Examples of information that can be collected:
- ●OS
- ●Serial number
- ●Phone number
- ●Installed apps
- ●Internal storage capacity of the device

*JP1 can be used to manage devices running iOS, iPadOS, Android, or Windows.

■Protect smart devices

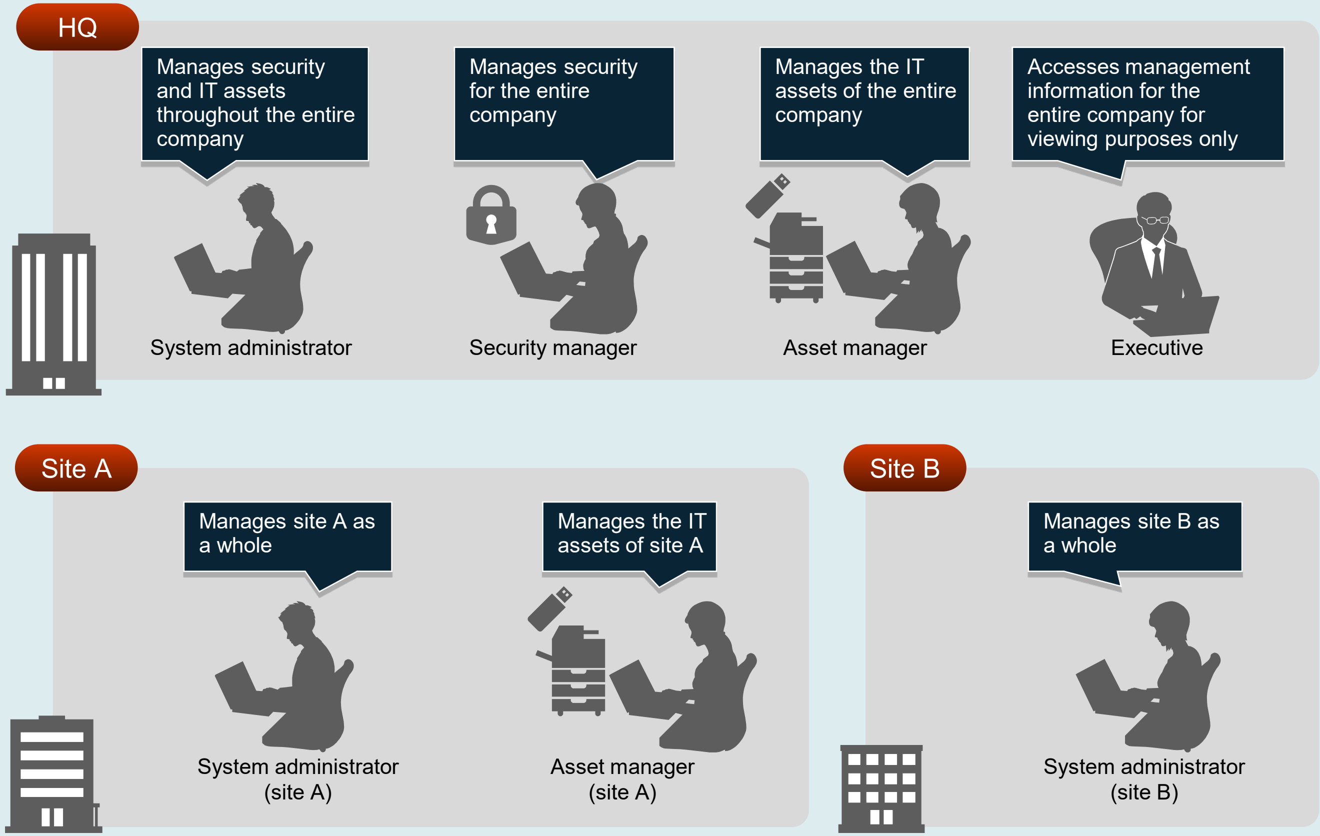
When smart devices are used for work, you inevitably incur some risks. JP1's functions for controlling smart devices help you mitigate these risks. For example, when someone loses a smart device, you can ensure that anyone who happens to pick up the lost device will not be able to use it, such as by locking the device or initializing it to prevent information leaks.



Divide work among multiple administrators:
Set the management scope for each type of user

HITACHI

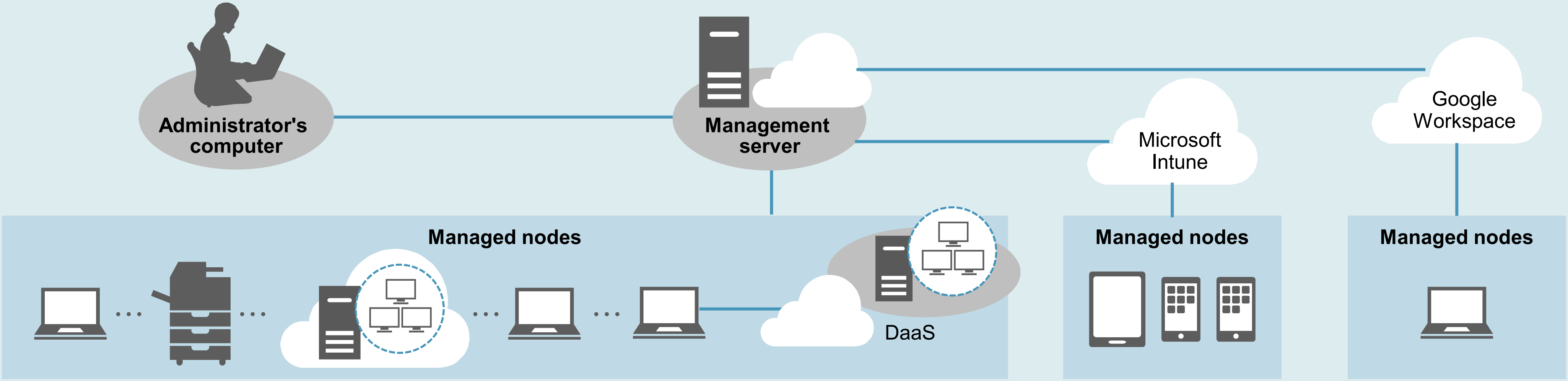
When you need to manage a large number of devices or devices located at different sites, you might want to divide management responsibilities among multiple administrators, and JP1 lets you do just that. You can even help your administrators work more efficiently by providing them with customized windows that show only the information that they need for the departments or operations that they are managing. You can define what each type of administrator can manage by configuring view permissions and update permissions. For example, you might grant a general administrator permission to view and update any information across the entire company, but grant the administrator at a single site permissions that relate only to his or her local IT assets.


HQ
Manages security and IT assets throughout the entire company
System administrator
Manages security for the entire company
Security manager
Manages the IT assets of the entire company
Asset manager
Accesses management information for the entire company for viewing purposes only
Executive
Site A
Manages site A as a whole
System administrator (site A)
Manages the IT assets of site A
Asset manager (site A)
Site B
Manages site B as a whole
System administrator (site B)

Example of a system configuration

- **Example of a system configuration**

Example of a system configuration



■ Administrator's computer

A web browser (Microsoft Edge, Firefox, or Google Chrome) must be installed.

DaaS: Desktop as a Service

■ Management server

Supported OSs:
Windows Server 2022, Windows Server 2019, and Windows Server 2016
Required hard drive space:
For the program: 2.5 GB or more
For data storage: 20 GB or more
(If you want to collect the operations log and revision history archive, more space is required. For details, see the applicable JP1 product manual.)
CPU:
2.0 GHz processor or faster
RAM:
2.0 GB or more
(This is the amount of RAM required by JP1 and does not include the amount of RAM required by the OS or other applications.)

■ Managed nodes

Supported OSs for managed nodes:

- Windows 11, Windows 10, Windows 8.1, Windows 8, and Windows 7
- Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2
- macOS 15, macOS 14, macOS 13, macOS 12, macOS 11, macOS 10.15, macOS 10.14, macOS 10.13, and macOS 10.12
- OS X 10.11, and OS X 10.10
- Red Hat Enterprise Linux® 9, Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 6, and Red Hat Enterprise Linux 5
- Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, and Oracle Linux 6
- CentOS 8, CentOS 7, and CentOS 6
- AIX 7.3, AIX 7.2, AIX 7.1, and AIX 6.1
- HP-UX 11iV3
- Solaris 11, and Solaris 10

Prerequisite OS for smart devices: iOS, iPadOS, Android, or Windows
Prerequisite OS for Chromebook devices: ChromeOS, ChromeOS Flex

Note:

- macOS, OS X, Red Hat® Enterprise Linux® 7, 6, and 5, Oracle Linux 7 and 6, CentOS, AIX, HP-UX, and Solaris are supported for JP1 V12. The sales period for JP1 V12 products is until the end of September 2026, and the support period is until the end of September 2034.
- The above system configuration is an example that uses JP1/IT Desktop Management 2 - Manager. To manage smart devices, you will also need Microsoft Intune. For details about system configurations, see the applicable JP1 product manual.
- For details about supported OSs and the corresponding product versions, visit the JP1 website. In some cases, an OS might be supported for a certain product, but individual functions within that product might not be available in that OS.

Support for safe use

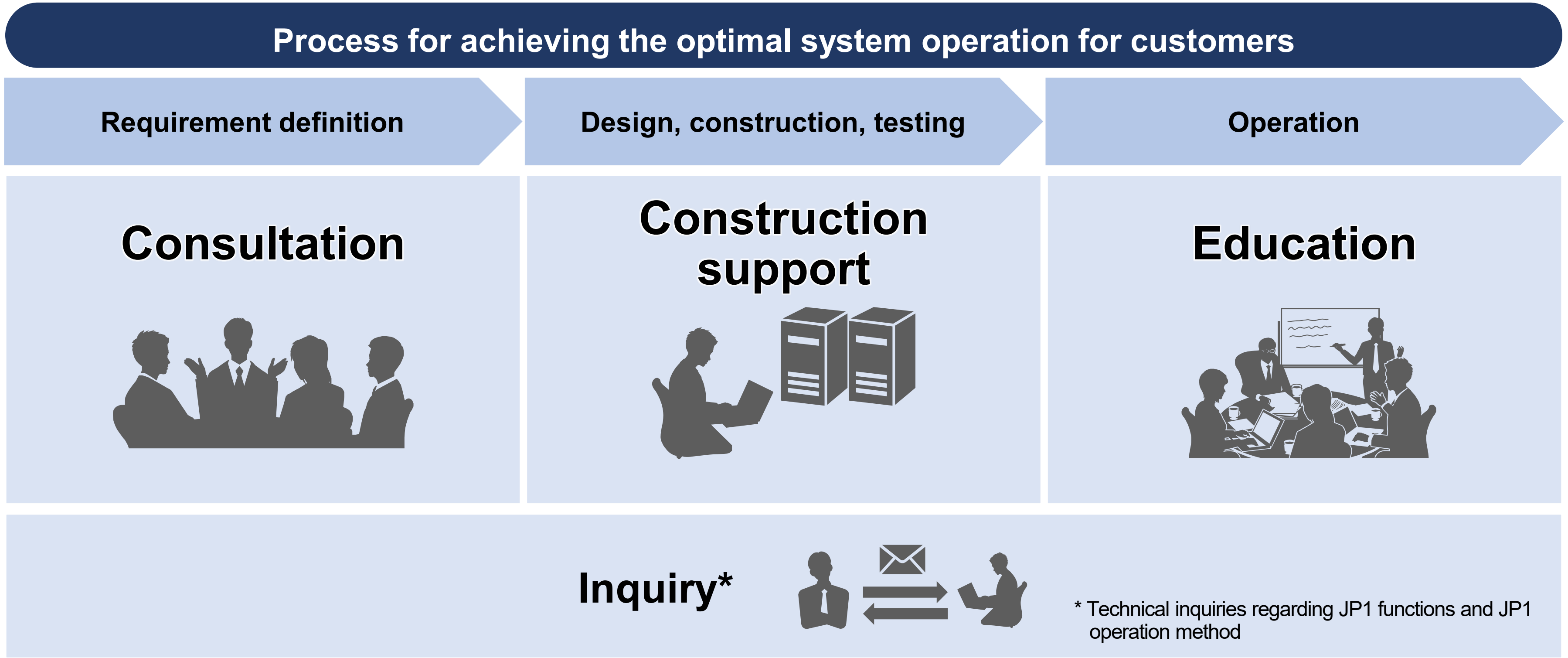
- JP1 professionals assist customers
- One-stop problem resolution at an early stage
- Long-term use with peace of mind and guaranteed compatibility with preceding versions
- Global use with peace of mind
- Reliable quality for customers

JP1 professionals assist customers

HITACHI

We can achieve the optimal system operation for our customers.

JP1 professionals can derive a system operation method suitable for the customer's requirements, system scale, and environment, and help achieve a network management system.



Process for achieving the optimal system operation for customers

Requirement definition	Design, construction, testing	Operation
Consultation	**Construction support**	**Education**

Inquiry*

* Technical inquiries regarding JP1 functions and JP1 operation method

By involving JP1 professionals, you can clarify system operation requirements, shorten the examination and implementation period, and smoothly hand over to the operation team.

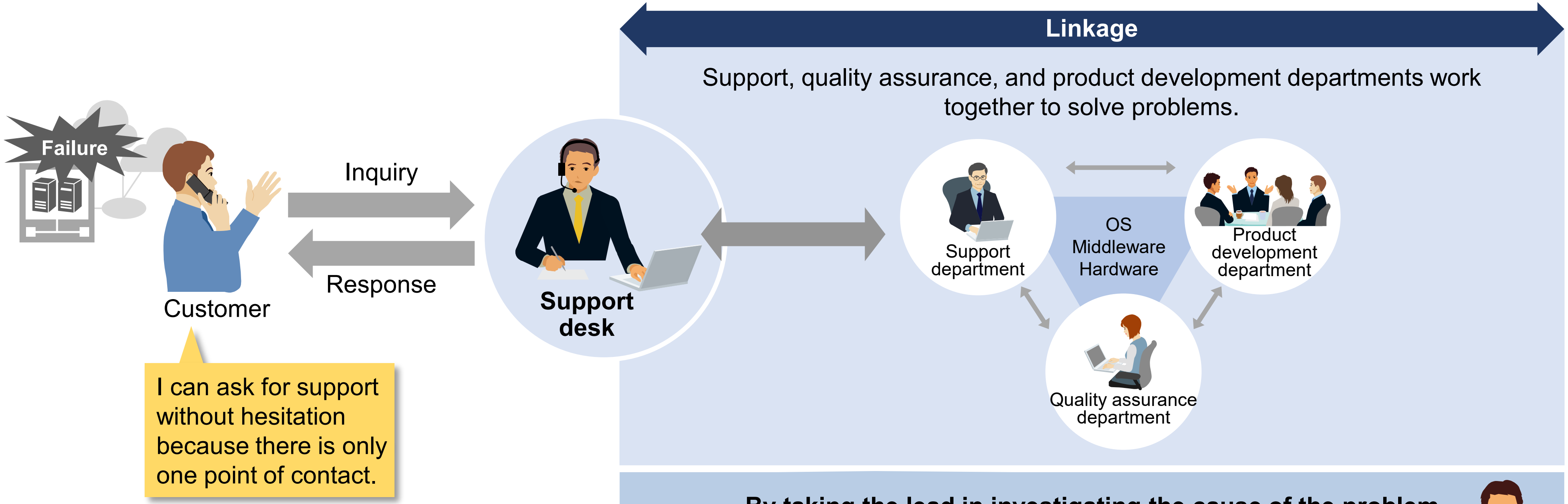
JP1 professionals are engineers who have a specified level of JP1 skills and have been certified based on the JP1 Engineer Qualification System.

One-stop problem resolution at an early stage

We provide one-stop support to solve problems quickly.
This reduces the burden on customers of a problem occurs.

We provide support for early stage resolution of complex problems, which can involve multiple elements such as operating systems and middleware.

One-stop support resolves problems quickly, prevents recurrence, and ensures stable operation of customer systems



Failure

Customer

Inquiry

Response

Support desk

I can ask for support without hesitation because there is only one point of contact.

Linkage

Support, quality assurance, and product development departments work together to solve problems.

Support department

OS
Middleware
Hardware

Product development department

Quality assurance department

By taking the lead in investigating the cause of the problem and implementing countermeasures,
Hitachi prevents the customer's problems from dragging on.

Long-term use with peace of mind and guaranteed compatibility with preceding versions

HITACHI

You can use JP1 for a long time and expand your business systems without worry.

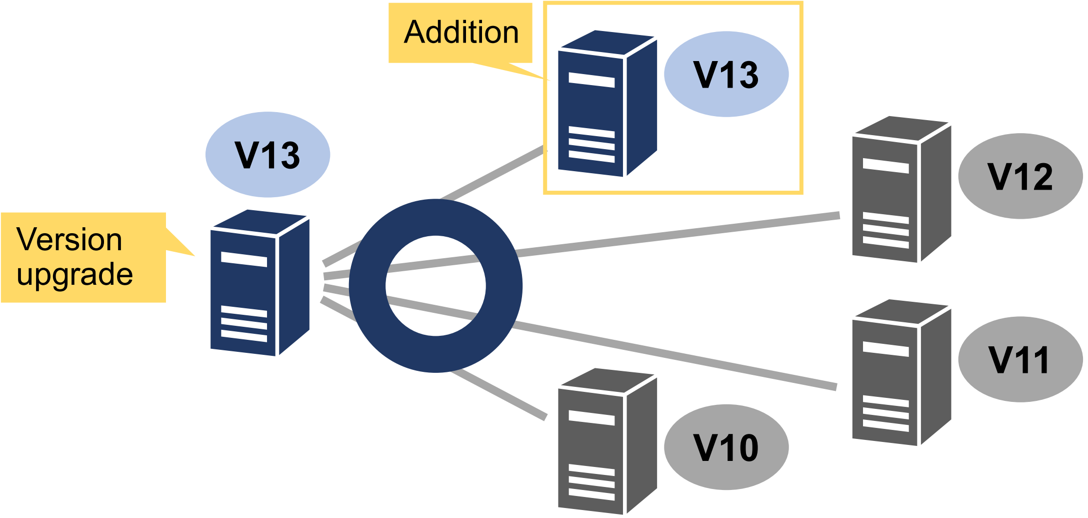
We provide continuous support even when the customer's system has a long life cycle.
JP1 ensures compatibility between versions, allowing for gradual system expansion.

Long-term support for the life cycle of customer systems

At least 10 years of support is guaranteed

with the same version

Flexible support for business system expansion



Guaranteed compatibility with the preceding three major versions.
You can operate your system even if it contains different JP1 versions.

Even if you upgrade JP1, interface compatibility is maintained.
Therefore, you can use the linked products, services, user programs without modification.

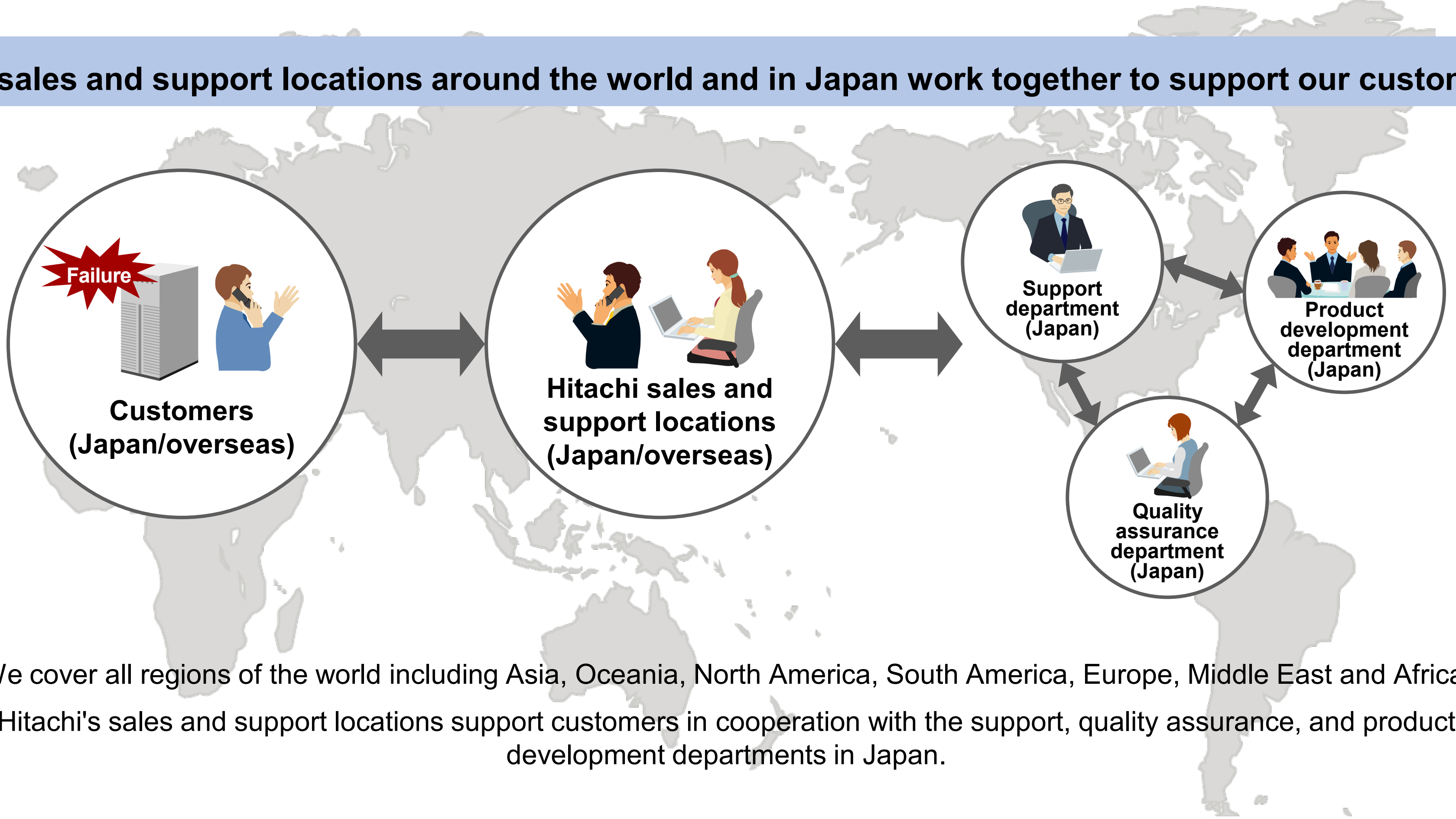
What you can do >
Security management >
Asset management >

Global use with peace of mind

You can use JP1 with peace of mind around the world.

We support our customers with sales and support locations covering all regions of the world.

Our sales and support locations around the world and in Japan work together to support our customers


Failure
Customers (Japan/overseas)
Hitachi sales and support locations (Japan/overseas)
Support department (Japan)
Product development department (Japan)
Quality assurance department (Japan)

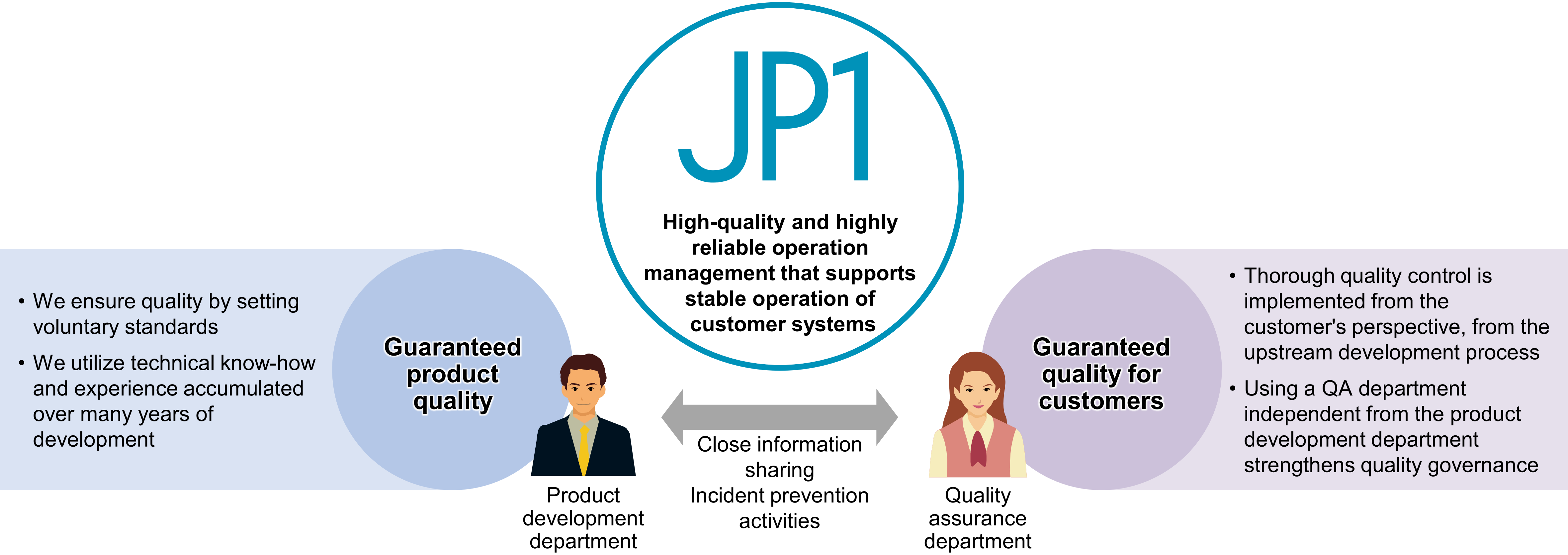
We cover all regions of the world including Asia, Oceania, North America, South America, Europe, Middle East and Africa.

Hitachi's sales and support locations support customers in cooperation with the support, quality assurance, and product development departments in Japan.

Reliable quality for customers

Achieve stable operation of mission-critical systems!

We have established a system to maintain high quality and high reliability so that customers can use our products with peace of mind.



JP1

High-quality and highly reliable operation management that supports stable operation of customer systems

- We ensure quality by setting voluntary standards
- We utilize technical know-how and experience accumulated over many years of development

Guaranteed product quality

Product development department

Close information sharing
Incident prevention activities

Quality assurance department

Guaranteed quality for customers

- Thorough quality control is implemented from the customer's perspective, from the upstream development process
- Using a QA department independent from the product development department strengthens quality governance

List of features

- **List of features**

List of features (1/3)

Category	Subcategory	Features
Deployment	Deployment support	• Deployment support via a wizard • Push distribution for agents (remote installation)*1 • Web application servers and internal databases
	Current status during deployment	• Home module • Current diagnosis reports
Operation	Operation support	Home module: Identify changes in the system as compared to the previous day, and build a customized Home module by choosing from 19 panels
		Discover new devices
		Agentless operations*2
		Use commands to apply changes to group information in a batch
	Database management	Perform database maintenance tasks (backup, restoration, reorganization) via the GUI
	Event display	• Device-related events (new hardware or software, changes to security settings, etc.) • Security-related events (security assessments, suppression of prohibited operations, etc.) • Asset-related events (new assets, new software licenses, etc.) • Distribution events (file distribution, software installation) • Configuration-related events (device discovery, agent deployment, etc.) • Events related to suspicious operations • Error events (error information)
	Registration of management accounts	• Set up permissions (system administrator permissions, user management permissions, view permissions) • Set up permissions by task type (restrict permissions that can be assigned to security management tasks, asset management tasks, device management tasks, and other task types) • Set up management scopes (restrict the types of management information that can be viewed by each department)
	Automated backup	Automatically back up operations logs to specified folders
Security management	Security policy items	■ Check the status of updates • Check whether automated updates are enabled or disabled in accordance with your company's regulations • Check whether the necessary quality updates and feature updates have been applied
		■ Check the statuses of antivirus software products • Check antivirus software information (product and scan engine version, definition file version, resident settings, date of last virus scan, etc.)
		■ Check the statuses of software programs being used • Check whether prohibited programs or Windows apps are installed • Make sure required programs and Windows apps are installed
Security management	Security policy items	■ Check the security settings of services • Check whether prohibited services are running
		■ Check the OS security settings • Check whether any guest accounts are enabled • Check for accounts that have weak passwords • Check for accounts that have passwords that do not expire • Check whether the number of days since a password was changed exceeds the number of allowable days • Check whether automatic logon is enabled • Check whether power-on passwords are set • Check whether password-protected screensavers are set up • Check whether the screensaver starts after a specified amount of time passes • Check whether a shared folder is set up • Check whether an administrative share is set up • Check whether unlimited anonymous access is enabled • Check whether Firewall is enabled • Check whether DCOM is enabled • Check whether the remote desktop functionality is enabled
		■ Create policies for assessing security that include conditions other than those that JP1 provides as security settings
		■ Settings to suppress printing • Suppress printing operations • Set up password protection for printing operations ■ Settings to suppress operations that use various devices • Suppress the use of USB memory devices (prohibit the use of unregistered USB memory devices) • Suppress the use of internal CD/DVD drives • Suppress the use of internal floppy disk drives • Suppress the use of IEEE 1394 devices • Suppress the use of internal SD card slots • Suppress the use of Bluetooth devices • Suppress the use of Windows Portable Devices • Suppress the use of imaging devices ■ Settings to suppress software startup • Suppress the startup of specified software programs (allow startup only by approved users or during specified periods)
Security management	Security policy items	■ Settings related to operations logs • Collect logs about the following operations: Starting and stopping PCs, logging on and off, starting and stopping processes, file and folder operations*3, executing commands from a command prompt or in PowerShell, printing, connecting and removing external media devices, window operations, suppressing the startup of programs, suppressing printing operations, blocking externally connected devices, web access (uploading and downloading data)*4, FTP operations (sending and receiving files)*4, sending and receiving emails with attachments*4, saving attachments from emails*4 • Collect logs about suspicious operations only
	Support for creating security policies	• Default policy (security check) • Recommended policy (enhanced security)
		Edit security policies
	Security policy assignment	• Automatically assign the default policy • Assign a unique security policy to each group • Assign a unique security policy to each PC
	Handling security policy violations	• Send notifications to users • Control network connections • Forcibly change security settings • Suppress operations • Collect log of suppressed operations
	Automatic security policy updates	• Automatically check whether virus definition files are up to date • Automatically check whether all Windows updates have been installed*5
	Checking the security status	■ Dashboard • Number of devices by violation level ("Safe", "Important", "Warning", or "Critical") • Security assessment by category (assess the security status by using levels A to E) • Security assessment by policy • Status of suspicious operations
		List security policies, display the security statuses of devices
	Quality updates	View a list of updates, automatically collect information about updates*5, create update groups, create packages for distributing updates, import and export a list of updates
	Operations logs	View a list of operations logs, trace operations in the operations logs, perform operations on stored log files
	Controlling devices that connect to the network	• Detect when new devices are connected to the network (permit or deny a connection) • Control connections for each network segment • Control connections for each device • Allow connections from blocked devices to specific devices • Re-allow connections from PCs that are deemed secure • Quarantine PCs infected by malware*6

*1 For information on the requirements for using push distribution for agents, see the applicable JP1 product manual.
*2 For information on the requirements and the available functions when using an agentless configuration, see the applicable JP1 product manual.
*3 Refers to operations in Windows Explorer and does not include operations performed in other software (such as Microsoft Office programs).
*4 For information on the browser (Microsoft Edge and Google Chrome) and email software (such as Outlook) for which operations log information can be obtained, see the applicable JP1 product manual.
*5 This feature requires a subscription to JP1 support services.
*6 This feature requires Microsoft Intune. In addition, Microsoft Defender is required as the antivirus software product.

What you can do >   Security management >   Asset management >

List of features (2/3)

Category	Subcategory	Features
Asset management	Managing hardware assets	• Asset information (such as adding, editing, or deleting information; changing the status; updating the inventory date; adding management items; and importing from or exporting to CSV files) • Contract information • Associated assets (monitors, hard disks, printers, USB memory devices, etc.) • Device information (automatically collected on a regular basis)
	Managing software licenses	• Software license information (such as adding, editing, or deleting information; changing the status; updating the inventory date; and importing from or exporting to CSV files) • Contract information • Computers to which licenses are to be allocated
	Managing software	• Information about managed software (such as adding, editing, or deleting information; and importing from or exporting to CSV files) • Installed software programs*6 • Computers on which a software program has been installed*6 • Computers to which software licenses have been allocated • Software licenses
	Managing USB memory devices	• Suppress the use of unapproved USB memory devices • Suppress the use of USB memory devices on specific PCs • Check the use history of a USB memory device • Get information about the files stored on a USB memory device
	Managing contracts	• Contract information (such as adding, editing, or deleting information; changing the status; and importing from and exporting to CSV files) • Software programs associated with a contract • Hardware devices associated with a contract
	Checking asset information	■ Dashboard • Trends in the number of hardware assets • Hardware assets (filtered display, display for each custom group) • Software programs (up to 100 programs) for which the number of remaining licenses is low • Information about contracts expiring in the next three months

Category	Subcategory	Features
Device management	Collection of device information and software information	• Automatically collect information on a regular basis • Collect the most recent information • Collect device information from managed computers that are offline • Export information to CSV files
	Device information	• System information (computer name, serial number, CPU, RAM, free space, name of the last user who logged on, OS and service pack, IP address, domain, etc.) • Hardware information (CPU, RAM, disk drives, etc.) • Information about installed programs and Windows apps (such as the names, versions, and installation dates of programs and apps; and the product keys and license types of Microsoft Office products) • Security information (information about Windows updates, antivirus software, and the security settings of services and of the OS) • Collect and manage the history of revisions made to device information
	Software information	List of computers on which a particular software program is installed*6
	Confirmation of device statuses	■ Dashboard • Customized device inventory (filtered display, custom group display) • Number of devices by OS • New software • Trends in managed nodes (separate display for nodes with agents installed and for nodes without agents installed)
	Remote control	• Keyboard and mouse operations • Remote maintenance operations that use optical media*7 • Send and receive files • Encrypt transferred data and set file access permissions • Send files to multiple computers at once • Issue a connection request from computers to controllers • Create and play back video recordings of remote operations • Use chat • Shut down and restart computers • Transfer clipboard contents

Category	Subcategory	Features
Software distribution	Distribution tasks	• Software to be installed*8 • Files • Windows updates • Uninstallation of installed software*8
	Defining execution schedules	• Execution at a specified date and time • Execution at user login • Execution at next startup • Automatic startup of the target computer • Automatic distribution of software to newly added devices
	Distributing and installing software	• Perform various operations by executing commands • Issue messages before and after execution • Control the transfer interval based on network availability • Execute distribution tasks in accordance with security policies • Distribute and install software to nodes in a defined group • Distribute and install packages in order of priority • Distribute and install software to offline PCs • Enable users to install software (pull distribution)
	Setting installation conditions	• Check the system conditions (hard drive space and RAM) • Check software-related conditions (required software programs and their versions) • Specify the installation method (interactive GUI or background) • Restart the PC after installation • Specify whether to display dialog boxes during processing • Set up actions to be executed before and after installation, and when installation ends in an error • Specify information such as company name and owner name • Incorporate user responses into the processing for installation via script files
	Distributing network load	• Control the distribution flow rate • Establish relay computers • Split packages to be distributed • Use multicast distribution
Reporting	Summary reports	• Daily summary reports • Weekly summary reports • Monthly summary reports

*6 You can also check which Windows apps are installed.
*7 This feature is available when the remote PC supports AMT. For information about supported versions, see the applicable JP1 product manual.
*8 For information on the requirements for installing and uninstalling software, see the applicable JP1 product manual.

What you can do >
Security management >
Asset management >

List of features (3/3)

HITACHI

Category	Subcategory	Features
Reporting (cont.)	Security diagnosis reports	■ Security assessment using five security levels, comparison with previous month's assessment results, explanations, topics, etc. • Current diagnosis report • Timeframe diagnosis
	Security details	• Status of violation levels • Status of security settings (Windows updates, passwords, etc.) • Status of antivirus software • Installation status of prohibited software (top 10 prohibited software programs that are installed) • Installation status of Windows updates (top 10 Windows updates that are not yet installed) • Installation status of required software (top 10 required software programs that are not yet installed) • Other access restrictions (top 10 software programs whose startup was suppressed per user) • User activity (top 10 users who use USB memory devices)
	Inventory details	• Device management status (breakdown of and trends in the number of managed PCs) • Green IT (status of power-saving settings)
	Asset details	• Hardware assets (changes and trends in the number of hardware assets) • Cost of hardware assets (cost trends) • Cost of software licenses (cost trends) • Software for which there are license violations (ranking of software programs with the highest number of license violations) • Software for which there is a surplus of licenses (ranking of software programs with the highest number of unused licenses)
	Output reports	Output CSV files
		Specify the scope of data items to be aggregated (department, device type, location, network, security policy)
Smart device manage-ment[*9]	-	• Check the overall status (smart device status, used storage space, available storage space, etc.) • Control devices (locking/initializing smart devices)
Chromebook device manage-ment[*10]	-	Import device information
Useful features	-	• Power devices on and off[*11] • Email event notifications to administrators • Send notifications to users • Forcibly change security settings • Configure VPN clients in a batch • Transfer management of software licenses • Password-protect agent settings • Execute commands to start or stop services on the management server, import or export various types of information, collect troubleshooting information, etc.
Other features	Linkage with Active Directory	Import device information
	Linkage with other JP1 products	Perform login authentication and manage permissions by using the Base component[*12]
	Cluster software support	Windows Server Failover Clustering
	Virtualization support[*13]	Support for various virtualization environment
	Device management over the Internet[*14]	• Manage security, assets, and devices • Distribute software
	Other	• Configure multi-tenancy • Use management relay servers to distribute management and create a management hierarchy • Remotely collect files from managed PCs

[*9] This feature requires Microsoft Intune.
[*10] This feature requires Google Workspace.
[*11] To automatically power on a PC, the PC must support Wake-on-LAN or Intel AMT.
[*12] Such as the Base component of JP1/Integrated Management 3 - Manager or JP1/Automatic Job Management System 3 - Manager.
[*13] For notes and other information on supported versions, please contact us.
[*14] For more information about the available functions, see the applicable JP1 product manual.

What you can do > | Security management > | Asset management >

Products required for the main functions in this brochure

Product names
JP1/IT Desktop Management 2 - Manager JP1/IT Desktop Management 2 - Additional License for Linux

Note:

- JP1 support services are available under a separate contract.
- These products are also available through the purchase of subscriptions, which allow you to use products and support services for a period of one year.

Third-party product names and trademarks

HITACHI

Note: In this brochure, *JP1/IT Desktop Management 2* is used to refer collectively to the products listed above in "Products required for the main functions in this brochure".

•Copyright, patent, trademark, and other intellectual property rights related to the "TMEng.dll" file are owned exclusively by Trend Micro Incorporated.

•Adobe is an either registered trademark or trademark of Adobe in the United States and/or other countries.
•AIX is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.
•Android, Chrome, Chromebook, ChromeOS, ChromeOS Flex, Google, Google Chrome, and Google Workspace are trademarks of Google LLC.
•The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc.
•Intel® is a trademark of Intel Corporation or its subsidiaries.
•iPadOS, macOS, and OS X are trademarks of Apple Inc., registered in the U.S. and other countries and regions.
•Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.
•Microsoft, Access, Microsoft Edge, Microsoft Intune, Outlook, Visual Basic, Visual C++, Windows, and Windows Server are trademarks of the Microsoft group of companies.
•Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates.
•Red Hat, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the United States and other countries.
•Other company, product or service names may be trademarks or registered trademarks of others.

- Product specifications are subject to change for the purpose of improvement without prior notice.
- The colors of actual product screens may appear to be slightly different from those in the screenshots shown in this document.
- Microsoft product screenshots are used with permission from Microsoft.
- This document uses the following units of measurement: 1 kilobyte (KB) = 1,024 bytes; 1 megabyte (MB) = 1,048,576 bytes; 1 gigabyte (GB) = 1,073,741,824 bytes; and 1 terabyte (TB) = 1,099,511,627,776 bytes.
- If you plan to export any of these products, please check all restrictions (for example, those stipulated by Japan's Foreign Exchange and Foreign Trade Law and the export control laws and regulations of the United States), and carry out all required procedures.
  If you require more information or clarification, please contact your Hitachi sales representative.
- For the most recent information on the support status of a JP1 product, including supported operating environments, please visit the JP1 website.

END

Integrated Operations Management

Asset and distribution management

Introducing JP1/IT Desktop Management 2

- Protecting your increasingly diverse IT assets -

Hitachi, Ltd.