HITACHI
Inspire the Next

Hitachi IT Operations Director Software Version 3.0.0-14 Release Notes

Contents

RN-91IOS020-15

About This Document

This document describes the revisions made to Hitachi IT Operations Director, software version 3.0.0-14. The document includes information that was not available at the time the technical documentation for this product was published, and a list of known problems and solutions.

Intended Audience

This document is intended for Hitachi Data Systems customers and authorized service partners who license and use Hitachi IT Operations Director.

Getting Help

For product tutorials and additional information, please refer to the self-service materials that are located on the IT Operations Software Portal:
http://www.itoperations.com
If you cannot locate the answer to your concern by referencing those materials, and if you purchased this product and have a current product support agreement, please visit the support Web site for current telephone numbers and other contact information: http://www.hds.com/services/support/
The Hitachi Data Systems Support Center staff is available 24 hours a day, seven days a week.

About This Release

These release notes apply to version 3.0.0-14 of Hitachi IT Operations Director.

Features and Enhancements

These functionalities are described in the IT Operations Director Help System.

In 3.0.0-08

Operating Systems for Network Access Control

IT Operations Director 3.0.0-08 supports the English version (only) of the following operating systems for Network Access Control:

- Microsoft® Windows Server® 2008 Standard
- Microsoft® Windows Server® 2008 Enterprise
- Microsoft® Windows Server® 2008 Standard without Hyper-V
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V
- Microsoft® Windows Server® 2008 R2 Standard
- Microsoft® Windows Server® 2008 R2 Enterprise
- Microsoft® Windows ® 7 Professional
- Microsoft® Windows ® 7 Enterprise
- Microsoft® Windows ® 7 Ultimate

German Operating System Internationalization support

On the German operating system, the English version of the IT Operations Director Manager and Agent components are supported. For precautionary information about running IT Operations Director on the German operating system, please see the Precautions section.

In 3.0.0-07

Antivirus Software

IT Operations Director 3.0.0-07 supports the following antivirus software:

- Symantec Endpoint Protection 12.1.

In 3.0.0-04

License Activation

The description of problem cause and associated workaround that is displayed in the license activation message has been improved.

Task Status

The message displayed in **Task Status** in the **Distribution** module has been improved to include the return code of the program execution in the **Task Status Details** dialog box in the **Task List**.

Collecting Host Names of Printers

IT Operations Director 3.0.0-04 supports the feature of collecting host names of printer that are discovered by SNMP authentication, by name resolution of MAC address, IP address, NETBIOS, DNS or hosts, instead of collecting the sysName, with the specification in the publishing options.

For details, refer to the IT Operations Director Usage Precautions section of this document.

VMware ESX Server

You can now install IT Operations Director 3.0.0-04 on the following Windows virtual machines:

- VMware ESX Server 3.0 or later.
- ESX and ESXi in VMware vSphere 4.
- ESXi in VMware vSphere 5.

Antivirus Software

IT Operations Director 3.0.0-04 supports the following antivirus software:

- McAfee SaaS Endpoint Protection 5.2
- VirusScan Enterprise 8.8

Improved Kaspersky Software

IT Operations Director is now able to collect Scan Engine Version, Virus Definition File Version, and Last Scanned Date information from the following software:

- Kaspersky Anti-Virus 6.0.4 for Windows Servers
- Kaspersky Anti-Virus 6.0.4 for Windows Servers 64bit
- Kaspersky Anti-Virus 6.0.4 for Windows Workstations
- Kaspersky Anti-Virus 6.0.4 for Windows Workstations 64bit

In 3.0.0-03

Operations Logs Collection

IT Operations Director 3.0.0-03 supports Internet Explorer 9, Firefox 4 or 5, and Windows Live Mail 2011 to be able to collect the Operations Logs relating to Web access, sending/receiving e-mail with attachments, and using FTP.

In 3.0.0-00

Network Access Control

IT Operations Director provides you with the option to control which computers can connect to the network with the Network Access Control feature; access can be based on criteria you specify, to protect your network from viruses and unauthorized users.

Windows Update Management

IT Operations Director provides you with the option to monitor the Windows Updates for the installed Microsoft Windows updates. If your site has a Product Support contract for Hitachi IT Operations Director, you can automatically obtain the latest Windows Update information in regular intervals.

Remote Control

IT Operations Director provides you with the remote access to manage and troubleshoot the end user's computers on the IT Operations management environment. Remote Control is a feature designed to assist the help desk personnel and system administrators. With this feature in your IT Operations Management environment, you can remotely access any computer, either with the IT Operations Director agent or through RFB protocol, distributed anywhere in your same office building or across geographical boundaries.

System Specification Changes

In 3.0.0-13

Firefox has been excluded from the supported Web browsers for operation logs

Firefox cannot be used to collect the following operation logs:

- Upload File
- Download File
- Send File
- Receive File
- Web Access

You can collect the above mentioned operation logs from the following Internet Explorer versions, only: Internet Explorer 6, 7, 8, and 9.

In 3.0.0-10

Update Tracked Date (from CSV)

When you perform **Update Tracked Date (from CSV)** on the management console, the update process can now complete successfully even when the CSV file has an empty row.

Import Software Search Conditions

In **Settings** > **Software Search Conditions,** the behavior of the **Import Software Search Conditions** menu has been changed as follows:

- When there are no records in a CSV file, an error message is displayed.
- When an empty row is included in a CSV file, the row is ignored.

The User Activity (USB Device Heavy User Top N) Report

When two conditions are met in a security policy (see the conditions below), the following operations are now not included in the report data:

The excluded operations:

- [Upload File]
- [Download File]
- [Send File]
- [Receive File]
- [Send Mail (Attachment File)]
- [Receive Mail (Attachment File)]
- [Save Attached File]

The security policy conditions:

1. In **Security policy** > **Operations Logs** > **Target Operations to be Logged**, the **[Select target operations]** is selected. In the subcategory of **[File Operation/Print Operation]** and **[Folder Operation]**, an item other than [Copy file], [Move file], [Rename file], [Create file], [Delete file], [Copy folder], [Move folder], [Rename folder], [Create folder], and [Delete folder] is **not** selected.
2. In a **Security policy**, all of the **[Suspicious Operations to be Notified]** settings are disabled.

In 3.0.0-08

Report Creation Condition Changes

The User Activity (Printer Heavy User Top N) report: The report creation condition has been changed so that the data for the User Activity (Printer Heavy User Top N) report is populated when a security policy meets either of the following conditions:

1. In **Operations Logs > Target Operations to be Logged > File Operation/Print Operation, [Print]** is enabled.
2. In **Operations Logs > Suspicious Operations to be Notified, [Large Number of Printing Jobs]** is enabled.

   Note: Previously, the report was created when any of the following conditions were met:
   1. In **Operations Logs > Target Operations to be Logged**, one or more sub-items are enabled in either the "**File Operation/Print Operation**" or "**Folder Operation**" categories.
   2. In **Operations Logs > Suspicious Operations to be Notified, [Large Number of Printing Jobs]** is enabled.
   3. In **Operations Logs, [Only operations that divulge information (recommended)]** is enabled.

The User Activity (USB Device Heavy User Top N) report: The report creation condition has been changed so that the data for the User Activity (USB Device Heavy User Top N) report is populated when a security policy meets either of the following conditions:

1. In **Operations Logs > Target Operations to be Logged**, one or more sub-items (except for **Print**) are enabled in either the "**File Operation/Print Operation**" or "**Folder Operation**" categories.
2. In **Operations Logs > Suspicious Operations to be Notified**, one or more item is selected in **Send/Receive E-mail with Attachments, Use Web/FTP Server**, or **Copy/Move the File to External Device**.
3. In **Operations Logs, [Only operations that divulge information (recommended)]** is enabled.

Note: Previously, the report was created when any of the following conditions were met:

1. In **Operations Logs > Target Operations to be Logged**, one or more sub-items are enabled in either the "**File Operation/Print Operation**" or "**Folder Operation**" categories.
2. In **Operations Logs > Suspicious Operations to be Notified**, one or more item is selected in **Send/Receive E-mail with Attachments, Use Web/FTP Server**, or **Copy/Move the File to External Device**.
3. In **Operations Logs, [Only operations that divulge information (recommended)]** is enabled.

System and Hardware Requirements

For a complete list of system and hardware requirements for this product, see the *Hitachi IT Operations Director Getting Started Guide.*

Fixed Problems

From 3.0.0-13 to 3.0.0-14

Summary	Description
Denial of Service (DoS) might occur.	The following problem has been corrected: Denial of Service (DoS) might occur. (CVE-ID: CVE-2014-0050) This problem occurred when IT Operations Director processed data in multipart format that contains an incorrect Content-Type.

From 3.0.0-10 to 3.0.0-13

Summary	Description
The IT Operations Director Agent Control service fails to start.	The following problem has been corrected: The IT Operations Director Agent Control service fails to start in the secondary system of a cluster configuration. This problem occurred when the IT Operations Director Agent Control service started in the secondary system of a cluster configuration.

Summary	Description
Windows Explorer might stop responding on an agent-installed machine during a file copy or move operation.	The following problem has been corrected: Windows Explorer might stop responding on an agent-installed machine when a copy or move operation is performed on a file that has a specific file name. This problem occurred when all of the following conditions were met: 1. The operating system is Windows Vista or later. 2. A file exists and the file name contains a single-byte left parenthesis "(" but the character is not closed with a single-byte right parenthesis ")", for example, "A(A)(A.doc". 3. A copy or move operation is performed on the file (or folder including the file) which meets Condition 2, and an existing file with the same file name is overwritten by the copied or moved file. 4. Any of the following security policies are assigned to the agent-installed machine: (a) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Only operations that divulge information (recommended)]** is selected. (b) **Operation Logs** are enabled. In the **Suspicious Operations to be Notified**, any of the following are selected: • Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device (c) In **Other Access Restrictions > External Device Restriction > USB Device**, the option **[Restrict reading/writing]** is enabled. [For version 3.0.0 to 3.0.0-07] (d) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any child item under **File Operation/Print Operation** or **Folder Operation** are selected. [For version 3.0.0-08 or later] (d) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any child item (except for **Print**) under **File Operation/Print Operation** or **Folder Operation** are selected.

Summary	Description
Windows Explorer might stop responding on an agent-installed machine.	The following problem has been corrected: Windows Explorer might stop responding on an agent-installed machine. This problem occurred when all of the following conditions were met: 1. The operating system is Windows 2000. 2. A file is opened in an application such as Microsoft Excel, or a file operation is performed in Windows Explorer. 3. Any of the following security policies are assigned to the agent-installed machine: (a) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Only operations that divulge information (recommended)]** is selected. (b) **Operation Logs** are enabled. In the **Suspicious Operations to be Notified**, any of the following are selected: • Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device (c) In **Other Access Restrictions > External Device Restriction > USB Device**, the option **[Restrict reading/writing]** is enabled. [For version 3.0.0-07 or before] (d) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any child item under **File Operation/Print Operation** or **Folder Operation** are selected. [For version 3.0.0-08 or later] (d) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any child item (except for **Print**) under **File Operation/Print Operation** or **Folder Operation** are selected.
Permission of a user account is elevated incorrectly.	The following problem has been corrected: Permission of a user account is elevated incorrectly.
Hitachi IT Operations Director does not work correctly after you change the directory of the database folder.	The following problem has been corrected: IT Operations Director does not work correctly after you change the directory of the database folder. This problem occurred when all of the following conditions were met: • You change the directory of the database folder. • The **Use Operation log** check box is selected. • The **Backup Operation logs automatically** check box is deselected (cleared).

Summary	Description
Internet Explorer might stop responding on an agent-installed machine.	The following problem has been corrected: Internet Explorer might stop responding on an agent-installed machine. This problem occurred when all of the following conditions were met: 1. Internet Explorer is started and a Web site is accessed. 2. Any of the following security policies are assigned to the agent-installed machine: (a) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Only operations that divulge information (recommended)]** is selected. (b) **Operation Logs** are enabled. In the **Suspicious Operations to be Notified**, any of the following are selected: • Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device [For version 3.0.0 to 3.0.0-07] (c) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any child item under **File Operation/Print Operation** or **Folder Operation** or **Web Access** are selected. [For version 3.0.0-08 or 3.0.0-09] (c) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any child item (except for **Print**)under **File Operation/Print Operation** or **Folder Operation** or **Web Access** are selected. [For version 3.0.0-10 or later] (c) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any of the following are selected: • Web Access (Upload) • Web Access (Download) • FTP (Send File) • FTP (Receive File) • Send Mail (Attachment File) • Receive Mail (Attachment File)

Summary	Description
Either agent registration or package creation fails.	The following problem has been corrected: When agent registration performed in the management server and package creation performed in the management window are done simultaneously, either operation fails. This problem occurred when the following operations were done simultaneously: 1. From Windows **Start** menu > **Hitachi IT Operations** > **Director Tools** > **Agent Registration**, an agent is registered. 2. Any of the following operations are performed in the management window: • A package is added in the **Package List** window. • An Agent Installer is created in the **Agent Configurations** window. • An update package is automatically created by the **Auto Enforce** function that has been set in the **Install Updates** settings of a security policy.
Incorrect inventory information might be reported.	The following problem has been corrected: Incorrect inventory information might be reported by an agent-installed machine or a machine for which Windows authentication is successful. The incorrect inventory information causes the following behaviors: 1. An update is not displayed in the **Installed Updates** list and the update is determined to be "Not Installed" for the machine. 2. The Windows Firewall status is determined to be "Disabled" for the machine and "Disabled" is displayed. 3. The Automatic Windows Update status is determined to be "Disabled" for the machine and "Disabled" is displayed. 4. An account is not displayed in the **Account Details**. This problem occurred when any of the following conditions were met: • The WMI service (service name: "Winmgmt") stops while the inventory information is being collected. • The Windows Firewall service (service name: "SharedAccess", "MpsSvc" in Vista or later) stops due to shutdown while the Windows Firewall status is being collected. • The Windows Automatic Updates service (service name: "wuauserv") stops due to shutdown while the Automatic Windows Update status is being collected. • The Workstation service (service name: "LanmanWorkstation") stops due to shutdown while the account information is being collected.

Summary	Description
The IT Operations Director Agent Control service might terminate abnormally.	The following problem has been corrected: The IT Operations Director Agent Control service might terminate abnormally. This problem occurred if you defined more than a certain amount of data for an asset custom field. The estimation of the amount of data that would exceed the limit of a custom field is described below. The estimated number decreases if you define a custom field in other languages or if you restrict Input Characters. • More than 70 items (each item consists of approximately 10 double-byte characters) are registered as the hierarchy or enumeration item for a custom field whose type is **Hierarchy** or **Enumeration**. • More than 30 fields (each field has a total of about 30 double-byte characters in **Item Name** and **Description**) are registered as a custom field.
The IT Operations Director Agent Control service might terminate abnormally when it starts.	The following problem has been corrected: The IT Operations Director Agent Control service might terminate abnormally when it starts. This problem occurred if you defined more than a certain amount of data for the **Remote Control Security Settings** of the default agent configuration. The estimation of the amount of data that would exceed the limit of the settings is described below. • More than 250 controllers (specified by IP address) are registered as **Allowed Controller**. • More than 30 users (each user consists of about 10 single-byte characters) are registered as **Allowed User**.
"pdsds.exe" may generate an application error.	The following problem has been corrected: "pdsds.exe" may generate an application error. This problem occurred, depending on the memory status, when launching the following windows: • Security > Device List • Assets > Department or Location List • Inventory > Device List

Summary	Description
Windows Explorer might terminate abnormally on an agent-installed machine during the folder operation.	The following problem has been corrected: Windows Explorer might terminate abnormally when the folder operation is performed on an agent-installed machine. This problem occurred when all of the following conditions were met: 1. Any of the following security policies are assigned to the agent-installed machine: (a) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Only operations that divulge information (recommended)]** is selected. (b) **Operation Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any child item under **File Operation/Print Operation** or **Folder Operation** are selected. (c) **Operation Logs** are enabled. In the **Suspicious Operations to be Notified**, any of the following are selected: • Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device (d) In **Other Access Restrictions > External Device Restriction > USB Device**, the option **[Restrict reading/writing]** is enabled. 2. The rename or move operation is performed to a very deeply rooted folder in Explorer.
The jdngsmcdevsr.exe process terminates abnormally on an agent-installed machine.	The following problem has been corrected: The jdngsmcdevsr.exe process terminates abnormally on an agent-installed machine. This problem occurred when all of the following conditions were met: 1. In **Security Policy > Other Access Restrictions > USB Device**, the **Restrict reading/writing** option and the **Allow registered USB device usage** option are enabled. 2. A USB device which is allowed to use is connected to an agent-installed machine. 3. A very deeply rooted folder is stored in the USB device.
The Warning dialog box might continue to be displayed in the management console.	The following problem has been corrected: The Warning dialog box might continue to be displayed in the management console. This problem occurred when a connection to the database failed during the completion of a task, such as a setting change, within the management console.
The software name might be incorrectly displayed.	The following problem has been corrected: Regarding some installed software, the software name might be incorrectly displayed in the **Software List** and the software might be repeatedly added to the list. This problem occurred when 1-byte NULL was added in the end of the registry value that stores the software information.

Summary	Description
The export might fail when you use an old version of a template.	The following problem has been corrected: When you export the Device List (Details) by using a template that you saved before you upgraded the management server, the export might fail. This problem occurred when all of the following conditions were met: • In version 2.5.0, when you export the Device List (Details), you save the items to be exported as a template. • In version 3.0.0 or later, you export the Device List (Details) by using the saved template.
The package distribution task might fail.	The following problem has been corrected: When distributing a package, the package might not be decompressed in an agent-installed machine and the task might fail. Also, an agent cannot be installed on a machine by executing the Agent Installer. This problem occurred when the following operations were performed simultaneously in different management consoles: 1. A distribution package is registered in the **Package List** window of the **Distribution** module. 2. The Agent Installer is created in the **Agent Configurations** window of the **Settings** module.
A user is not allowed to start the software.	The following problem has been corrected: A user is not allowed to start the software even though a group name is specified in **Approval User/Group Name** as the exception in the **Block Software** settings. This problem occurred when all of the following conditions were met: 1. In **Security Policy > Other Access Restrictions > Blocked Software**, software is registered. 2. A group name is entered in **Approval User/Group Name** as the exception to the software use. 3. There are about 60 or more groups to which the account of the user who started the software, belongs.

Summary	Description
Software is not blocked.	The following problem has been corrected: Software is not blocked when a user starts it if the software has no version information. This problem occurred when all of the following conditions were met: 1. In **Security Policy > Other Access Restrictions > Blocked Software**, software is registered. 2. There is no version information in the software. You can find that there is no version information in the software if the Properties window in Windows Explorer is as follows: [For Windows 2000/XP/2003] The Version tab does not exist in the Properties window. [For Windows Vista/2008/7] The value of File version is blank in the Details tab of the Properties window.
The MAC address of a device is removed.	The following problem has been corrected: When a Discovery from Active Directory is performed, the MAC address of a device is removed from the existing device information in the management window. This problem occurred when all of the following conditions were met: 1. The device information is collected only by the following methods: • ARP • ICMP • Active Directory 2. A Discovery from Active Directory is performed. 3. While the Discovery from Active Directory is being performed, the MAC address of the device cannot be collected, based on a number of possible causes; for example, the device is powered-off, it is temporarily disconnected from the network, or a network failure occurs.

Summary	Description
When a device is discovered, another asset that is identical to the device, is registered.	The following problem has been corrected: After you add a hardware asset by any of the following operations, and if you perform a discovery using SNMP to discover a device which is identical to the asset, then another hardware asset identical to the device is registered. • A hardware asset is added in the Assets window. • A hardware asset is imported. • A hardware asset is added by using the Analyzer Integration function. This problem occurred when all of the following conditions were met: 1. You add a hardware asset that meets all of the following conditions: • Host name is 16 or more characters long. • A lowercase letter is included in the first 15 characters of the host name. 2. After adding the asset, you perform a discovery using SNMP to a device which is identical with the asset.
The agent might not start.	The following problem has been corrected: After an agent is installed using the Agent Installer, and after you restart the OS, the agent might not start. This problem occurred when all of the following conditions were met: 1. You install an agent by using the Agent Installer. 2. You restart the OS immediately after you install an agent.
The operation logs related to a file or folder might not be output correctly.	The following problem has been corrected: After you copy a file or folder on an agent-installed machine, the operation logs for the file or folder might not be output correctly. This problem occurred when all of the following conditions were met: 1. The operating system is Windows Vista or later. 2. You copy a file or folder in the same folder.
The user name might be blank in the logs and events related to Print.	The following problem has been corrected: The user name for the following operation logs and events might be blank. Also, the corresponding data is not displayed in the **User Activity (Printer Heavy User Top N)** report: • Operation logs related to "printing" and "print-restriction" • Events related to suspicious operations that are "print-restriction" and "a large number of printing jobs" This problem occurred depending on the printer driver installed on an agent.

Summary	Description
Operation logs for printing might not be obtained and printing might not be restricted.	The following problem has been corrected: Operation logs for printing might not be obtained and printing might not be restricted. This problem occurred when all of the following conditions were met: 1. An agent-installed machine has a **computer name** that exceeds 15 characters. 2. A printer is installed on the agent-installed machine, and a printing operation for the printer is completed.
Operation logs for which the date is year 3001 or later are registered.	The following problem has been corrected: When an agent notifies the management server of the operation logs for which the date is year 3001 or later, these operation logs are registered in the management server. This problem occurred when an agent notified the management server of the operation logs dated year 3001 or later.
There is a problem in registering hardware asset information.	The following problem has been corrected: Either of the following symptoms occurs. Symptom (1): An invalid value can be registered for a custom field by importing hardware assets. Symptom (2): You may be unable to change the hardware asset information. A. Symptom (1) occurred when all of the following conditions were met: 1. A custom field for hardware assets is defined with the **Enumeration** type. 2. By importing hardware assets, you overwrite or update the value of the selection item for the custom field, but the imported value has not been defined as the selection items yet. B. Symptom (2) occurred when all of the following conditions were met: 1. A value that has not been defined as the selection items for the custom field is set for a hardware asset. 2. Any of the following operations are performed for the hardware asset: (a) Edit the hardware asset information (b) Change the hardware asset status (c) Edit the associated contracts (d) Edit the associated hardware assets (e) Edit the associated inventory information (f) Import the hardware asset

From 3.0.0-09 to 3.0.0-10

Summary	Description
Explorer might stop responding on an agent computer.	The following problem has been corrected: Explorer might stop responding on an agent computer. This problem occurred when any of the following security policies were applied to an agent computer: 1. **Operations Logs** are enabled. In the **Target Operations to be Logged**, the option **[Only operations that divulge information (recommended)]** is selected. 2. **Operations Logs** are enabled. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected and in the **Operation Classification**, any of the following are selected: • File Operation/Print Operation • Folder Operation In the subcategory displayed by expanding the **[File Operation/Print Operation]** and **[Folder Operation]**, one or more items (except for **Print**) is selected. 3. **Operations Logs** are enabled. In the **Suspicious Operations to be Notified**, any of the following are selected: • Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device 4. In **Other Access Restrictions** > **External Device Restriction** > **USB Device** > the option **[Restrict reading/writing]** is enabled.
When Discovery from IP Address Range is performed, the MAC address is removed from the device information of any device that has already been discovered by Network Access Control.	The following problem has been corrected: When Discovery from IP Address Range is performed, the MAC address is removed from the device information of any device that has already been discovered by Network Access Control. This problem occurred when all of the following conditions were met: 1. When Network Access Control discovers a device and discovery is performed for the device, the inventory information is obtained only by ICMP. 2. When Discovery from IP Address Range is performed to the above-mentioned device, the inventory information is obtained only by ICMP.

Summary	Description
Inventory information might not be obtained from a device that has already been discovered by Discovery from IP Address Range using Windows authentication.	The following problem has been corrected: The following pieces of inventory information might not be obtained from a device that has already been discovered by Discovery from IP Address Range using Windows authentication: • System Details - Network Details (Information about only a single network address can be obtained). • System Details - Computer Details - Processor. • Hardware Details - Processor Details. • Hardware Details - Hard Disk Details. • Hardware Details - Network Adapter Details (Information about only a single network adapter can be obtained). • Hardware Details - Keyboard Details. • Hardware Details - Mouse Details. This problem occurred when all of the following conditions were met: 1. Discovery from IP Address Range or inventory information collection is performed. 2. Windows authentication is successful. 3. The size of the inventory information collected is larger than 32000 bytes.
Even when you enable Network Access Control, an event might not be displayed in the Event List window.	The following problem has been corrected: The message "The network access control has started." might not be displayed in the **Event List** window even when you enable Network Access Control. This problem occurred when all of the following conditions were met: 1. The operating system of an agent PC is either Windows 7 or Windows Server 2008. 2. Multiple network adapters are connected to the agent PC. 3. Among the network adapters, there is a network adapter that is not connected to the network.
System and hardware information sent from an agent might not be reflected on the management server.	The following problem has been corrected: System and hardware information sent from an agent might not be reflected on the management server. This problem occurred when multiple devices such as a printer and a hard disk were connected to the agent PC.

Summary	Description
After clicking on the **# of Not Compliant Computers** link, the corresponding number of computers displayed is incorrect.	The following problem has been corrected: In **Security > Security Policy List >** the **Antivirus Software** tab, when you click on the **# of Not Compliant Computers** link, the **Computer Security Status > Device List** will display. However, computers that are not compliant with Antivirus Software are not correctly displayed in that **Device List** and the number of listed computers is not consistent with the number of the original **# of Not Compliant Computers** link that was clicked. This problem occurred when you on the **# of Not Compliant Computers** link in **Security > Security Policy List >** the **Antivirus Software** tab.
When you update tracked date of software licenses by using a CSV file, a database error occurs.	The following problem has been corrected: When you update the tracked date of software licenses by using a CSV file (the file has 257 or more items for which License Number is set), a database error occurs. This problem occurred when you updated the tracked date of software licenses by using a CSV file (the file has 257 or more items for which License Number is set) in the **Software License List** window.
Security assessment might be executed twice in succession, therefore causing a high processing load on the management server.	The following problem has been corrected: Security assessment might be executed twice in succession, therefore causing a high processing load on the management server, and more security assessment events are displayed. This problem occurred when all of the following conditions were met: 1. In **Device List > Edit Device Details**, any of the following items of devices are changed: • Department • Location • IP Address • Subnet Mask • Device Type • Operating System 2. Then, a security policy assigned to the devices is changed.
Package registration of a ZIP file might fail.	The following problem has been corrected: Package registration of a ZIP file might fail. This problem occurred when you tried to register a package selecting a ZIP file in which a lot of files are compressed, in **Package List > the Add Package**.

Summary	Description
Agent Control service stops.	The following problem has been corrected: The IT Operations Director Agent Control service stops when a device with a host name of 62 characters is discovered. This problem occurred when a device with a host name of 62 characters was discovered by either of the following operations: 1. Discovery from IP Address Range. 2. Discovery from Active Directory.
Device information might be inappropriately deleted from the Network Filter List.	The following problem has been corrected: Device information might be inappropriately deleted from the **Network Filter List**. This problem occurred when all of the following conditions were met: 1. Inventory information is received from a device (Device-1). 2. Inventory information is received from another device (Device-2) 3. During the process of updating the inventory information for Device-1, an error occurs because of insufficient processing resources. 4. After the error (3), the process of updating the inventory information for Device-2 is executed.
Device information is not updated and error events are triggered.	The following problem has been corrected: Device information is not updated and the following error events are triggered. • An error occurred while updating received files. (Event ID: 208) • Failed to update. Error occurred while updating received files. (Event ID: 210) This problem occurred when all of the following conditions were met: 1. From the **Edit Device Details** menu on the management console, you set the device information as follows: • PC or server is specified for **Device Type**. • Nothing (blank) is selected for **Operating System**. 2. Inventory information is received from the edited device.
The same device is registered twice with different host names; the one host name is FQDN and the other host name is not FQDN.	The following problem has been corrected: The same device is registered twice with different host names; one is FQDN and the other is not FQDN. This problem occurred when all of the following conditions were met: 1. A device that belongs to a domain is discovered and managed using SNMP authentication. 2. Hitachi IT Operations Director Agent is installed on the same device.

Summary	Description
Explorer might terminate abnormally on an agent computer.	The following problem has been corrected: Explorer might terminate abnormally on an agent computer. This problem occurred when either of the following items was changed in a security policy: • **Operations Logs** • **Other Access Restrictions > External Device Restriction > USB Device.**
Agent deployment won't complete.	The following problem has been corrected: When you perform an agent deployment to two devices (one device has an IP address set in the device information and the other device does not have an IP address set in the device information) at the same time, the agent deployment status for the device (that does not have an IP address in the device information) may remain "Deploying" indefinitely and the agent deployment for the device might not be completed. This problem occurred when an agent deployment was performed to two devices at the same time; one device has an IP address set in the device information and the other device does not have an IP address set in the device information.

From 3.0.0-08 to 3.0.0-09

Summary	Description
A subnet mask cannot be acquired from an agent computer.	The following problem has been corrected: When the subnet mask of "255.255.255.255" is configured on an agent computer, the agent cannot acquire the subnet mask. As a result, the subnet mask of the system details is not sent from the agent to the management server. This problem occurred when the subnet mask of "255.255.255.255" was configured on an agent computer.
An agent computer might have a high processing load.	The following problem has been corrected: The CPU usage of the jdngsmcdevsr.exe process might increase abnormally on an agent computer, therefore causing a high processing load on that agent computer. This problem occurred when all of the following conditions were met: 1. **Restrict Reading/Writing for USB device** is enabled in a security policy. 2. After Step 1, **Restrict Reading/Writing for USB device** is disabled once, and then enabled again. Or, after Step 1, the agent computer continues to run after 2:00 am.

Summary	Description
Discovery from the Active Directory cannot be executed.	The following problem has been corrected: When you attempt to perform a Discovery from the Active Directory, the progress bar remains at 0 percent and the discovery cannot be executed. This problem occurred when either of the following cases existed in the **Settings > the Active Directory settings** window: **Case 1:** This problem occurred when all of the following conditions were met: 1. Multiple domain information entries are specified for connecting to the Active Directory. 2. Different domain names are specified for the connection destinations. 3. The different domains do NOT have a hierarchical relationship with each other. **Case 2:** This problem occurred when all of the following conditions were met: 1. Multiple domain information entries are specified for connecting to the Active Directory. 2. Different domain names are specified for the connection destinations. 3. The different domains DO have a hierarchical relationship with each other. 4. All of the "Root OU" settings include the name of a domain that is hierarchically higher than the other domains and all of the "Root OU" settings consist of a "Domain name" and an "OU name."
The ioutils exportoplog command fails and produces an error message.	The following problem has been corrected: An attempt to execute the ioutils exportoplog command fails and the following error message is displayed: KDEX4086-E. This problem occurred when all of the following conditions were met: 1. The Operation Log file contains a character that is converted to a surrogate pair character in UTF-16 format. 2. The ioutils exportoplog command is executed.
When executing Discovery from the Active Directory, the last modified date and time is updated even though the inventory information has not actually been modified.	The following problem has been corrected: When executing Discovery from the Active Directory, the last modified date and time is updated even though the inventory information has not actually been modified. This problem occurred when all of the following conditions were met: 1. The Active Directory discovery target computers exist directly under a domain. 2. In the **Settings > the Active Directory settings** window, the **Get Department Hierarchy Information** box is selected. 3. Only a domain name is specified for the "Root OU" in the Active Directory connection information. 4. Discovery from the Active Directory is executed.

Summary	Description
An item that cannot be deleted from the Network Filter List is created.	The following problem has been corrected: An item that cannot be deleted from the **Network Filter List** is created. This problem occurred when all of the following conditions were met. 1. One of the following conditions applies: • Hitachi IT Operations Director Agent is installed on an agentless device. • The host name of an agentless device that was previously unable to be acquired has been acquired. • The MAC address of an agentless device that was previously unable to be acquired has been acquired. 2. The MAC address of a device is physically updated or deleted by a user.

From 3.0.0-07 to 3.0.0-08

Summary	Description
The agent policy update feature and the distribution feature won't work.	The following problem has been corrected: The agent policy update feature and the distribution feature won't work. This problem occurred when the following condition was met: The root directory of any drive was specified for the management server's Data Folder.
The jdngsmctfm.exe process might terminate abnormally.	The following problem has been corrected: When the Agent Monitor Control service starts on an agent computer, the jdngsmctfm.exe process might terminate abnormally (or terminate abnormally and then start repeatedly) and burden the agent computer with a large processing load. This problem occurred when all of the following conditions were met: **For Director software version 2.5.0:** 1. The Operations Logs are enabled in a security policy that is assigned to an agent computer. 2. The software is upgraded to 3.0.0 or later. **For Director software version 3.0.0:** 1. The Operations Logs are enabled in a security policy that is assigned to an agent computer and the security policy satisfies any of the following conditions: 1. In the **Target Operations to be Logged**, [**Only operations that divulge information (recommended)**] is selected. 2. In the **Target Operations to be Logged**, [**Select target operations**] is selected and any of the following are selected in the **Operation Classification**: • File Operation/Print Operation • Folder Operation • Web Access 3. In the **Suspicious Operations to be Notified**, any of the following are selected: • Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device 2. After the above settings are set, a user receives or sends attached files and the total number of files is more than 3,000.
Agent Control service might stop unexpectedly.	The following problem has been corrected: An invalid memory is referred to by the IT Operations Director Agent Control service and the service might stop unexpectedly. This problem occurred when inventory information was received from multiple agents at the same time.

Summary	Description
Device information and asset information of a node might be overwritten incorrectly, or a node might be registered as a different device and asset.	The following problem has been corrected: The device information and the asset information of a node might be overwritten incorrectly, or a node might be registered as a different device and asset. This problem occurred when there was insufficient memory on the management server during the process of registering the device information and the asset information of a node.
The distribution feature does not work.	The following problem has been corrected: The distribution feature does not work. This problem occurred when the root directory of any drive was specified for the management server's Data Folder.
Operations related to a database or Operations Logs fail.	The following problem has been corrected: The following operations fail in the management server: • Database backup • Database restore • Automatic backup of Operations Logs • Operation logs restore • Database upgrade This problem occurred in either case: **Case 1:** This problem occurred when all of the following conditions were met and setup was completed: 1. During a setup, the **Use Operations Log** check box is selected in the **Operations Log Settings** panel. 2. In the **Operations Log Settings** panel, your specification is either of the following case: a. A product of values that are specified in [**Number of managed nodes**] and [**Maximum restore period for Operations Logs**] is 143853 or more. For example, [**Number of managed nodes**] is 300 nodes and [**Maximum restore period for Operations Logs**] is 500 days. b. You specify 4773 or more nodes in [**Number of managed nodes**]. **Case 2:** This problem occurred when all of the following conditions were met: 1. The root directory of any drive was specified for the management server's Local Data Folder. 2. Automatic backup of the Operations Logs is enabled.
Cross-site scripting security issues exist.	The following problem has been corrected: Cross-site scripting security issues exist. This problem occurred when a script was wrongly performed across sites by an attack from a malicious third party.

Summary	Description
A vulnerability issue exists, which may cause a Web browser on a management console to terminate abnormally.	The following problem has been corrected: A vulnerability issue exists, which may cause a Web browser on a management console to terminate abnormally.
A device group with an incorrect name might be created unexpectedly.	The following problem has been corrected: A device group with an incorrect name might be created unexpectedly after "**Edit Device Details**" is performed. This problem occurred when all of the following conditions were met: 1. "**PC**" or "**Server**" is specified for the Device Type in the **Edit Device Details** dialog box. 2. **OK** is clicked.
During Daylight Savings Time, when you use a filter, data that does not match the condition is displayed.	The following problem has been corrected: During Daylight Savings Time, when you use a filter that specifies a relative date for a condition to search data, data that does not match the condition is displayed as the search result or data that matches the condition is not displayed as the search result. This problem occurred when all of the following conditions were met: 1. A region where Daylight Savings Time is used is specified for the time zone in the operating system on the management server. 2. The system clock on the management server is currently in Daylight Savings Time. 3. Data is searched using a filter that specifies a relative date.
When security is assessed, the Virus Definition File Version and the Scan Engine Version might be incorrectly assessed as "Problem."	The following problem has been corrected: When security is assessed, the **Virus Definition File Version** and the **Scan Engine Version** might be assessed as a "**Problem**" immediately, even if you have given several days in the **Update Time limit** for these items. This problem occurred when all of the following conditions were met: 1. 25 or more days are specified for **Update Time limit** for the **Virus Definition File Version** and the **Scan Engine Version** in a security policy. 2. Security is assessed.
The agent deployment status remains "Deploying" indefinitely and the agent deployment won't complete.	The following problem has been corrected: The agent deployment status remains "Deploying" indefinitely and the agent deployment won't complete. This problem occurred when all of the following conditions were met: 1. An IP address is not set in the device information of a device targeted for agent deployment. 2. The management server is not able to connect to the target device by host name while deploying an agent.

Summary	Description
An internal error occurs when displaying system details of a device, or exporting device details fails.	The following problem has been corrected: An internal error occurs when displaying the system details of a device in which a subnet mask is not set, or when the export of device details fails for a device for which a subnet mask is not set. This problem occurred when either of the following operations was performed to a device in which a subnet mask was not set: 1. In **Inventory > Device Inventory > Device List** or **Device List (Network)** or **Department List** or **Location List**, a device is selected and then the **System Details** tab is displayed. 2. In **Inventory > Device Inventory > Device List or Device List (Network)** or **Department List** or **Location List**, the **Export Device Details** menu is selected and then the item "**System Details - Network Details - IP Address/Subnet Mask**" is exported.
The "Internal Error" message is displayed in the Import Assets wizard.	The following problem has been corrected: If you export custom fields (data type: Date) in the **Assets** module to a CSV file and then import the CSV file from a Web browser where the date format of the browser locale is different from the date format of the management server locale, the "Internal Error" message is displayed in the **Cause** column in the **3. Confirm Settings** panel in the **Import Assets** wizard. This problem occurred when all of the following conditions were met: 1. The date format that is supported by the locale of the operating system for the management server and the date format that is supported by the locale of the Web browser for the management client are different. 2. You import custom fields (data type: Date).
The last date that archived logs can be restored is incorrectly changed to an earlier date.	The following problem has been corrected: The last date that archived logs can be restored is incorrectly changed to an earlier date; therefore displaying an earlier (incorrect) date as the last date that archived logs can be restored in the **Restore Archived Logs** dialog box. This problem occurred when all of the following conditions were met: 1. The management client is set in a time zone where Daylight Savings Time is used. 2. The **Operations Log List** is displayed when the management client's date is currently in Standard Time (not Daylight Savings Time). 3. In the **Restore Archived Logs** dialog box, the restorable period includes the days in Daylight Savings Time.
Overwrite-installation or uninstallation of the management server fails.	The following problem has been corrected: Overwrite-installation or uninstallation of the management server fails when the root directory of any drive was specified for the management server's Data Folder. This problem occurred when the root directory of any drive was specified for the management server's Data Folder.

Summary	Description
Communication to a device that is set to permit communication is still being blocked.	The following problem has been corrected: Communication to a device that specified as the **Exclusive Communication Destination for Access-Denied Devices** is blocked. This problem occurred when all of the following conditions were met: 1. Network Access Control is enabled. 2. With Network Access Control enabled, an upgrade-installation of Hitachi IT Operations Director is performed.
Operations Logs might not be collected on a file in a CD/DVD drive, or software activation might not be blocked on a CD/DVD drive.	The following problem has been corrected: Operations Logs might not be collected or software activation might not be blocked when a user performs a file operation or a program execution/termination on a CD/DVD drive on an agent computer. This problem occurred when all of the following conditions were met: 1. Any of following were enabled in a security policy: • In **Operations Logs > Target Operations to be Logged**, [**File Operation**] or [**Folder Operation**] is enabled. • In **Operations Logs > Target Operations to be Logged**, [**Program Execution/Termination**] is enabled. • In **Other Access Restrictions**, [**Blocked Software**] is enabled. 2. The agent computer is using a Windows 7/Windows Server 2008 R2 environment. 3. The CD format is CDFS. 4. The **Recording** tab is displayed in the **Properties** dialog box for the CD/DVD drive.
A security policy might not be applied to an agent computer.	The following problem has been corrected: When an agent computer receives a security policy when the computer starts, the security policy might not be applied to the computer. This problem occurred when the **Operations Logs** settings or the **Other Access Restrictions settings** are changed in the security policy.
Although Operations Logs are disabled, the Large Number of Printing Jobs event might be triggered.	The following problem has been corrected: Although Operations Logs are disabled, the Large Number of Printing Jobs event might be triggered for an agent computer. This problem occurred when all of the following conditions were met: 1. In the **Edit Security Policy** dialog box, **Operations Logs** are set to **Disabled** with the **Large Number of Printing Jobs** check box selected in **Suspicious Operations to be Notified**. 2. In the security policy **Other Access Restrictions**, **Printing Restriction** is enabled. 3. A user prints something on an agent computer that contains more pages than specified in **Large Number of Printing Jobs**.

Summary	Description
A device on which network access is not allowed might still be able to access the network.	The following problem has been corrected: A device on which network access is not allowed might still be able to access the network. This problem occurred when Network Access Control was manually uninstalled on an agent computer.
An agent might consume CPU resources when the IT Operations Director Network Monitor service is stopped.	The following problem has been corrected: An agent might consume CPU resources when the IT Operations Director Network Monitor service is stopped. This problem occurred when all of the following conditions were met: 1. Network Access Control is enabled on an agent computer. 2. The IT Operations Director Network Monitor service is stopped on the agent computer.
The message that is displayed when an agent deployment fails has been improved.	The following problem has been corrected: The message that is displayed when you perform an agent deployment after removing a discovery range has been improved; users can now better understand that the agent deployment failed because the discovery range has been removed. This problem occurred when all of the following conditions were met: 1. The discovery range you used when performing **Discovery from IP Address Range** is removed. 2. An agent deployment is performed.

From 3.0.0-06 to 3.0.0-07

Summary	Description
The Agent Monitor Control service might stop unexpectedly.	The following problem has been corrected: The Agent Monitor Control service might stop unexpectedly on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. Any of the following are enabled in a security policy: Operations Logs, Restrict Reading/Writing for USB device, Printing Restriction, or Blocked Software. 2. An IME other than the Windows Standard IME is used. 3. Either of the following operations is performed: • Disable all Operations Logs, Restrict Reading/Writing for USB device, Printing Restriction, and Blocked Software in a security policy. • Shut down an agent-installed computer.
The Agent Monitor Control service might stop unexpectedly (or incorrect Operations Logs might be uploaded to the management server).	The following problem has been corrected: The Agent Monitor Control service might stop unexpectedly on an agent-installed computer or incorrect Operations Logs might be uploaded to the management server. This problem occurred when all of the following conditions were met: 1. Any of the following are enabled in a security policy: Operations Logs, Restrict Reading/Writing for USB device, Printing Restriction, or Blocked Software. 2. After Step 1, the security policy settings are changed, but any of the following are still set to **Enabled**: Operations Logs, Restrict Reading/Writing for USB device, Printing Restriction, or Blocked Software.
When Discovery from IP Address Range using SNMP authentication is executed, an application error occurs.	The following problem has been corrected: When Discovery from IP Address Range using SNMP authentication is performed, an application error occurs and Discovery from IP Address is suspended. This problem occurred when either of the following conditions was met: • The data acquired by SNMP exceeds 512 bytes. • The sum total of data acquired by SNMP from one IP device exceeds 10 KB.

Summary	Description
If the connection with the database is temporarily disconnected, the scheduled execution of some features won't work.	The following problem has been corrected: If the connection with the database is temporarily disconnected, the scheduled execution of the following features won't work: - Discovery. - Assessing security status. - Updating support service information. - Creating and maintaining report data. - Backup of the Operations Log database. - Collecting end user information. - Analyzer Integration. This problem occurred when all of the following conditions were met: 1. The IT Operations Director Service has started. 2. The connection with the database is temporarily disconnected and then restored.
An "internal parameter error" occurs when a security policy is removed or updated.	The following problem has been corrected: An "internal parameter error" occurs when a security policy is removed or updated. This problem occurred when all of the following conditions were met: 1. With Hitachi IT Operations Director 2.5.0, a policy (except for the Default Policy) is updated after "Restore Default Settings" is performed in the **Edit Security Policy** dialog box. 2. The software is upgraded from Hitachi IT Operations Director 2.5.0 to 3.0.0. 3. The Default Policy or the security policy, which was updated in Step 1 is removed or updated.
Changed Network Access Control Settings are not reflected.	The following problem has been corrected: Changed Network Access Control Settings aren't reflected in Network Access Control. This problem occurred when the Network Access Control configuration file in an agent is corrupted.
Changed Network Access Control Settings might not be reflected.	The following problem has been corrected: Changed Network Access Control Settings might not be reflected in Network Access Control. This problem occurred when either of the following conditions were met: - Network Access Control is enabled or disabled. - Network Access Control Settings is changed.

Summary	Description
Cannot disable the Network Access Control.	The following problem has been corrected: If Network Access Control is enabled on an agent computer and if the specified management server's host name or IP address is changed for that same agent computer, you will no longer be able to disable Network Access Control on that agent computer. This problem occurred when the specified management server's host name or IP address is changed on an agent computer on which Network Access Control is enabled.
Cannot deploy an agent onto a computer where a user has not logged on to Windows.	The following problem has been corrected: An agent cannot be deployed onto a computer where a user has not logged on to Windows. This problem occurred when all of the following conditions were met: 1. The agent computer is using a Windows XP/2003 environment. 2. The agent has never been installed on the computer. 3. A user has not yet logged on to Windows. 4. An agent is deployed.
IP address and MAC address are not added to Network Filter List.	The following problem has been corrected: IP address and MAC address are not added to Network Filter List. This problem occurred when reading an internal file, that is output by Network Access Control, fails.
Cannot remove a device on which Network Access Control is enabled.	The following problem has been corrected: You can no longer remove a device on which Network Access Control has been enabled. This problem occurred when all of the following conditions were met: 1. "Disable Network Access Control" is performed to a device on which Network Access Control has been enabled. 2. Before the process of "Disable Network Access Control" from Step 1 is completed, "Enable Network Access Control" is performed to another device which is in the same network group as the device from Step 1.

Summary	Description
The output data in Export Device Details is different from the data that is displayed on the management console.	The following problem has been corrected: The output data in Export Device Details is different from the data that is displayed on the management console. - For [Screen Saver Startup Time]: The value that is increased by 60 times is output. - For [Password Strength] and [Password Never Expires]: An inverse value of the correct value is output. - For [Last Logged On User Name]: An empty string is output when the logged on user information does not exist. - For [Shared Folder]: A value is output as "Enabled" instead of the correct value of "Exist" and a value is output as "Disabled" instead of the correct value of "None." - For [Power On Password]: The values "Unknown" and "Not Implemented" are output as "Disabled" in the CSV file. This problem occurred when performing Export Device Details **in Inventory > Device Inventory > Device List** or **Device List (Network)** or **Department List or Location List**.
Cross-site scripting security issues exist.	The following problem has been corrected: Cross-site scripting security issues exist. This problem occurred when a script was wrongly performed across sites by an attack from a malicious third party.
The CPU usage for the Agent Monitor Control service might become higher than necessary.	The following problem has been corrected: The CPU usage for the Agent Monitor Control service might become higher than necessary on an agent-installed computer. This problem occurred when any of the following are enabled in a security policy: Operations Logs, Restrict Reading/Writing for USB device, Printing Restriction, or Blocked Software.
The device status of a managed device that is running might display as "Stop" on the management console during Daylight Savings Time.	The following problem has been corrected: The device status of a managed device that is running might display as "Stop" on the management console during Daylight Savings Time. This problem occurred when all of the following conditions were met: 1. A region where Daylight Savings Time has been introduced is specified for the time zone in the operating system for the management server. 2. During Daylight Savings Time, the management server collects information from managed devices at the interval specified in Agent Configuration.

Summary	Description
Before reaching the maximum disk storage capacity, old Operations Logs might be deleted.	The following problem has been corrected: Before reaching the maximum disk storage capacity (described in the **Setup > Operations Log Settings panel > Required capacity**), old Operations Logs might be deleted. This problem occurred when all of the following conditions were met: 1. During setup, the **Use Operations Log** box is checked and 765 or more nodes are specified for the number of managed nodes. 2. The management server receives Operations Logs from multiple agents. 3. The data size of the Operations Log database folder, which is specified in the Setup panel, is 64 GB or more.
The Remote Control Chat icon doesn't appear in the taskbar.	The following problem has been corrected: The Remote Control Chat icon doesn't appear in the taskbar. This problem occurred when all of the following conditions were met: 1. The agent PC is either the Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2 environment. 2. In the Chat settings, the **Start the chat server when Remote Control agent starts** option is ON. 3. In the Chat settings, the **Display Icon in Taskbar** option is ON. 4. The user logs off from the agent PC and logs on again immediately.
An application error might occur during a file transfer.	The following problem has been corrected: An application error might occur during a file transfer and it becomes impossible to execute the file transfer. This problem infrequently occurred when all of the following conditions were met: 1. The **Allow File Transfer** option is ON. 2. The log on operation is performed from an agent-installed computer.
An application error might occur when the Remote Control Agent starts.	The following problem has been corrected: An application error might occur when Remote Control Agent starts. This problem occurred when virtual memory becomes temporarily insufficient when starting Remote Control Agent.
Transferring clipboard data might be executed repeatedly between Remote Controller and an agent.	The following problem has been corrected: Transferring clipboard data might be executed repeatedly between Remote Controller and an agent when updating clipboard data. This problem occurred when updating clipboard data.

Summary	Description
An application error might occur during a Remote Control connection.	The following problem has been corrected: An application error might occur during a Remote Control connection. This problem occurred when all of the following conditions were met: 1. The Controller is connected with the Remote Control Agent, which is using the Windows Vista/2008/7/2008 R2 environment. 2. The agent-installed computer is using a "Windows Aero" mouse. 3. Virtual memory becomes temporarily insufficient.
An internal error occurs when saving a filter from a context menu in Network Filter List.	The following problem has been corrected: An internal error occurs when saving a filter from the Simple Filter context menu in the Network Filter List. This problem occurred when all of the following conditions were met: 1. In **Settings > Network Access Control > Network Filter Settings**, the hidden filters are shown from the "**>>**" button and the **Connection to Network** filter is selected from the Simple Filter. 2. The "**Save As...**" option is selected from the Simple Filter context menu and the new filter condition is saved with a new name.
An incorrect set of dates are displayed in the Report Duration field of Report Option.	The following problem has been corrected: An incorrect set of dates is displayed in the Report Duration field in the **Security Diagnosis Reports - Timeframe Diagnosis** option. This problem occurred when all of the following conditions were met: 1. The management server's time zone and the management client's time zone are different. 2. As a result of Step 1, the management client's time is ahead of the management server's time. 3. Either "Weekly," "Quarterly," or "Half-Yearly" is specified in the Report Option in **Reports > Security Diagnosis Reports > Timeframe Diagnosis**.
The header and value for the number of contracts might be displayed as off by a month.	The following problem has been corrected: The header and value for the number of contracts might be displayed as off by a month in the **Expired Contracts (next 3 months)** panel. This problem occurred when either of the following conditions were met: • If you use a Web browser that is set to English language, the header is displayed incorrectly off by one month. • The current month is different between the management client and the management server due to a time zone difference between them and the **Expired Contracts (next 3 months)** panel is displayed in **Assets > Dashboard**.

Summary	Description
Data is displayed incorrectly in the Managed Nodes Trend panel.	The following problem has been corrected: Data is displayed incorrectly in the **Managed Nodes Trend** panel. This problem occurred when all of the following conditions were met: 1. The management server's time zone and the management client's time zone are different. 2. As a result of Step 1, the management client's time is ahead of the management server's time. 3. The **Managed Nodes Trend** panel is displayed in **Inventory > Dashboard**.
The Approval Time to allow the use of blocked software is not registered properly.	The following problem has been corrected: The Approval Time to allow the use of blocked software is not registered properly. This problem occurred when all of the following conditions were met: 1. The management server's time zone and the management client's time zone are different. 2. The Approval Time to allow the use of blocked software is set in **Security Configuration Items > Other Access Restrictions**.
The start date and end date of restored Operations Logs aren't displayed on the activated range of the Time Chart.	The following problem has been corrected: The start date and end date of restored Operations Logs aren't displayed on the activated range of the Time Chart. This problem occurred when all of the following conditions were met: 1. The management client is set in a time zone where Daylight Savings Time is used. 2. The Operations Log List is displayed in either of the following case: **Case 1** a) For the Start Date or End Date of the data to restore, a Standard Time (not Daylight Savings Time) is specified. Then, the Operations Logs are restored. b) The Operations Log List is displayed when the management client's time zone is currently in Daylight Savings Time. **Case 2** a) For the Start Date or End Date of the data to restore, a Daylight Savings Time is specified. Then, The Operations Logs are restored. b) The Operations Log List is displayed when the management client's time zone is currently in Standard Time (not Daylight Savings Time). 3. The beginning date of the Operations Logs indicated by the Time Chart is the start date of the restored Operation Logs. Or the end date of Operations Logs indicated by Time Chart is the end date of the restored Operations Logs.

Summary	Description
The date and time displays incorrectly in the Description text box in the Event Detail dialog box.	The following problem has been corrected: The date and time displays incorrectly in the **Description** text box in the **Event Detail** dialog. This problem occurred when all of the following conditions were met: 1. A difference exists between the management server's time zone and the management client's time zone. 2. The **Event Detail** dialog box of an event (Event ID: 1020, 1033, or 1035) is displayed in the **Events > Event List**.
A Windows update that is eliminated from a security assessment might be listed incorrectly in the Event Detail dialog box.	The following problem has been corrected: A Windows update that is eliminated from a security assessment might be listed incorrectly in the **Event Detail** dialog box for the following event: **Severity**: Information. **Type**: Security. **Event #**: 63. **Description**: Update information has been added. This problem occurred when all of the following conditions were met: 1. A Windows update is published, which is applied to some or all of the following operating systems: - Windows Server 2003 for Itanium-based Systems. - Windows Server 2003 R2 for Itanium-based Systems. - Windows Server 2008 for Itanium-based Systems. - Windows Server 2008 R2 for Itanium-based Systems. 2. The latest support information is registered by any of the following operations: - The latest support information is registered from the Support site according to the specified schedule set in **Settings > General > Product Update**. - In **Security > Windows Update > Update List**, an offline update is performed from the **Action** menu. - The support information is registered by the updatesupportinfo (support information registration) command.

Summary	Description
The Cause and Workaround in the message (KDEX5010-W).	The description of Cause and Workaround was fixed in the message (KDEX5010-W), which is triggered when a Discovery from IP Address Range execution fails. This problem occurred when all of the following conditions were met: 1. Either of the following operation is performed to IP devices: - Discovery from IP Address Range. - Update Device Details. 2. The IT Operations Director Agentless Service is running while IP devices are processing either of the following requests: - Discovery from IP Address Range. - Update Device Details.
An incorrect year might be displayed in the Report Duration field of Report Option.	The following problem has been corrected: An incorrect year might be displayed in the Report Duration field in the **Report Option - Timeframe Diagnosis** option. This problem occurred in either case: **Case 1:** This problem occurred when all of the following conditions were met: 1. Either "Quarterly," "Half-Yearly," or "Yearly" is specified in **Report Option** in **Reports > Security Diagnosis Reports > Timeframe Diagnosis**. 2. Any month other than January is specified in **Select the start month of year** in **Settings > Reports > Duration and Start Date**. **Case 2:** This problem occurred when all of the following conditions were met: 1. Any report duration is specified in **Report Option** in **Reports > Asset Detail Reports > Hardware Assets**. 2. Any month other than January is specified in **Select the start month of year** in **Settings > Reports > Duration and Start Date**. **Note**: This problem also occurred in the **Hardware Assets Cost** report and the **Software License Cost** report.
A memory leak might occur in the IT Operations Director Agent Control service.	The following problem has been corrected: A memory leak might occur in the IT Operations Director Agent Control service. This problem occurred when any of the following conditions was met: - Hardware information is received from an agent. - Windows update information is received from an agent. - Operations such as **Update Device Details** and **Send User Notification** are performed to an agent.

Summary	Description
The system might become unstable upon a computer on which Network Access Control is enabled.	The following problem has been corrected: The system might become unstable on a computer upon which Network Access Control is enabled. This problem occurred when any of the following conditions were met: • Network Access Control is disabled. • From an agent computer upon which Network Access Control is enabled, **Administrator Tools > Setup** is launched and then the information in the **Connected managing server** field is changed. • A device upon which Network Access Control has been enabled is removed. • A database recreation is performed from the **Setup** panel in the management server. • A database restore is performed from the **Database Manager** panel.
The Network Access Control service might terminate unexpectedly.	The following problem has been corrected: The Network Access Control service might terminate unexpectedly. This problem occurred when any of the following conditions was met: • Network Access Control is disabled. • From an agent computer upon which Network Access Control is enabled, **Administrator Tools > Setup** is launched and then the setting in the connected management server is changed. • A device upon which Network Access Control has been enabled is removed. • A database recreation is performed from the **Setup** panel in the management server. • A database restore is performed from the **Database Manager** panel.
In the **Export Device Details > Select Export Columns** dialog box, the **Save Template** dialog box does not display as expected.	The following problem has been corrected: In the **Export Device Details > Select Export Columns** dialog box, if you select any template and change items to export, the **Save Template** dialog box does not display as expected. This problem occurred when performing **Export Device Details** in **Inventory > Device Inventory > Device List** or **Device List (Network)** or **Department List or Location List** and when either of the following conditions were met: • A template (**Installed Software Details** > any software is specified) is selected and then the software is removed. • A template (**Security Details > Windows Update Details > Installed Updates >** any update is specified) is selected and then the Windows update is removed.

Summary	Description
The agent process might crash on an agent-installed computer.	The following problem has been corrected: The agent process might crash on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. Operations Logs are enabled in a security policy. 2. Any one of the following acquisition conditions is specified: • An IP address is specified in the **Web Access** acquisition condition. • The **Private IP Address** option is selected in the **Web Access** acquisition condition. • An IP address is specified in the acquisition condition of the **Use Web/FTP Server** settings of **Suspicious Operations to be Notified**. • The **Private IP Address** option is selected in the acquisition condition of **Suspicious Operations to be Notified > Use Web/FTP Server**. 3. Internet Explorer 6 is installed on an agent-installed computer. 4. Any one of the following operations is performed: • Access to a Web page. • Web upload. • Web download. • FTP send. • FTP receive.
When exporting various lists, if UTF-16 is specified for Encoding, the characters are garbled.	The following problem has been corrected: When exporting various lists, if UTF-16 is specified for Encoding, characters will be garbled. This problem occurred when all of the following conditions were met: 1. When exporting, UTF-16 is specified for Encoding in the **Select Export Columns** dialog box. 2. A list is exported to a CSV file. **Note**: This problem does not occur in the **Export Device Details** menu in **Inventory > Device Inventory > Device List** or **Device List (Network)** or **Department List** or **Location List**.

From 3.0.0-04 to 3.0.0-06

Summary	Description
Agent information might not be updated.	The following problem has been corrected: Information about an agent might not be updated. This problem occurred when the management server receives connection requests from many agents at the same time.
Cross-site scripting security issues.	The following problem has been corrected: Cross-site scripting security issues.
The Autoplay feature of drives other than removable and permanent drives might be enabled.	The following problem has been corrected: The Autoplay feature of drives other than removable and permanent drives might be enabled on an agent-installed computer if the USB device reading and writing restriction is enabled. This problem occurred when all of the following conditions were met: 1. The Autoplay feature on drives other than removable drive and permanent drive is disabled in the Group Policy of Windows. 2. The Restrict Reading/Writing of USB Device option is enabled in a security policy.
The Setup console might not be launched or troubleshooting information might not be recorded.	The following problem has been corrected: The Setup console might not be launched or troubleshooting information might not be recorded. This problem occurred when the Hitachi IT Operations Director process is forcibly terminated.
Asset information is not updated and error events are triggered, even if end user information is entered from an agent-installed computer.	The following problem has been corrected: Even when end user information is entered from an agent-installed computer, the asset information is not updated and the following error events are triggered: • An error occurred while updating received files. (Event ID: 208) • Failed to update. Error occurred while updating received files. (Event ID: 210) This problem occurred when all of the following conditions were met: 1. From the management console, a custom field for hardware assets is added and the following settings are specified for that field: - For **Data Source**, **End User** is selected. - The **Entering item is mandatory** box is not checked. - For **Type**, **Date** is selected. 2. From an agent-installed computer, end user completes the form entry without specifying anything for the custom field (which is added in Step 1.)

Summary	Description
Changed Network Access Control Settings might not be reflected.	The following problem has been corrected: Even if Network Access Control Settings are changed, the change might not be reflected in Network Access Control. This problem occurred when Network Access Control Settings are changed.
A list display might return to the default.	The following problem has been corrected: For a list (for example, **Assets** > **Hardware Assets** > **Department List**), if you change displayed columns, column width, or column order, the list display might return to the default setting when the list is re-displayed. This problem occurred when all of the following conditions were met: 1. For various lists, the **Display Columns** setting is changed from the **Select Columns** dialog box or column width or order is changed, and then the list is used. 2. The operating system for the management server is restarted or the services for the management server are started by using the startservice command. 3. After Step 2, various lists (for example, **Assets** > **Hardware Assets** > **Department List**) are displayed for the first time.
Some data doesn't display, or the display returns to the default, in the **Settings** module.	The following problem has been corrected: Some data doesn't display, or the display returns to the default when any operation is performed in the **Settings** module. This problem occurred when either of the following conditions was met: **Occurrence Condition 1** Either of the following operations are performed in any screens under **Settings** > **Discovery**: - **Manage** or **Ignore** is executed after the columns (which are hidden by default in the **Display Columns** setting) are displayed on the list. - **Manage** or **Ignore** is executed after the list is sorted by any column. **Occurrence Condition 2** Either of the following operations are performed in **Settings** > **Agent** > **Agent Deployment**: - **Deploy Agent** or **Stop Deployment** is executed after the columns (which are hidden by default) are displayed on the list. - **Deploy Agent** or **Stop Deployment** is executed after the list is sorted by any column.

From 3.0.0-03 to 3.0.0-04

Summary	Description
Windows Explorer might crash on an agent-installed computer.	The following problem has been corrected: Windows Explorer might crash on an agent-installed computer. This problem occurred when Operations Logs are enabled in a security policy.
The information acquired from the Active Directory is not reflected in IT Operations Director.	The following problem has been corrected: The following information acquired from the Active Directory is not reflected in IT Operations Director: **Common Fields (Hardware Assets and Device Inventory)** and **Custom Fields (Hardware Assets)**. This problem occurred when all of the following conditions were met: 1. For any item in **Common Fields (Hardware Assets and Device Inventory)** or any custom-created item in **Custom Fields (Hardware Assets)**, the Active Directory is specified as a Data Source. 2. Devices are managed in IT Operations Director by the following management type: • Agent Management • Agentless Management (Administrative Share or SNMP) 3. The devices managed in IT Operations Director are also managed in the Active Directory. 4. Discovery is started in the Active Directory.
The Agent features won't work after converting a product license.	The following problem has been corrected: When a trial license is converted to the product version on the day of the trial's expiration, the Agent icon temporarily disappears on the agent-installed computers and the agent features won't work. This problem occurred when a trial license is converted to the product version on the day of license expiration.
A database access error might occur when working within the Web browser.	The following problem has been corrected: When multiple administrators are simultaneously working within a management console, a database access error might occur. This problem occurred when multiple administrators assigned security policies to managed computers at the same time. Note: This problem has occurred even if the security policies or managed computers differed by each administrator.

Summary	Description
A blocked file name is incorrectly displayed.	The following problem has been corrected: A blocked file name is incorrectly displayed in the **Edit Unauthorized Software** dialog box. The operation itself is successful; it is only the display that is incorrect. This problem occurred when all of the following conditions were met: 1. In a **Security Policy** > **Software Use**, multiple software applications with the same name and version are added as unauthorized software. 2. In the **Unauthorized Software** settings, **Auto Enforce** and **Block Activation** are enabled, and then a file name is set to block activation. Note: This problem also occurred when software was added from the **Add as Unauthorized Software** button in **Inventory** > **Software Inventory** > **Software List**. Caution: If a blocked file name of an unauthorized software application is still incorrectly displaying even after you apply this maintenance release version of Director, set the file name again according to the following steps: 1. Open the **Software Use** panel in a security policy. 2. Open the **Edit Unauthorized Software** dialog box and set a correct file name in the blocked file name field. **Note:** To review the blocked software as it is currently set, view the **Blocked Software List** in the **Other Access Restrictions** panel.
The connection for the management server and agents fails.	The following problem has been corrected: The connection for the management server and agents fails. This problem occurred when all of the following conditions were met: 1. After replacing the management server machine, the database is restored using backup data that was created on another machine. 2. Database Recreation is performed from the **Setup** panel. Note: This problem won't occur if Database Restore is performed after step 2.
Distributing a Windows update fails.	The following problem has been corrected: If a Windows Update File is registered for an update that was automatically added in the Update List, the update still isn't distributed. This problem occurred when a Windows Update File was registered in **Security** > **Windows Update** > **Update List**, for an update that was automatically added in the Update List.
The computer on which Network Access Control is enabled cannot communicate to the network.	The following problem has been corrected: The computer on which Network Access Control is enabled cannot communicate to the network. This problem occurred when Network Access Control was enabled on a computer that has two or more NICs.

Summary	Description
Remote Control connection might fail.	The following problem has been corrected: The Remote Control connection to an agent-installed computer might fail. This problem occurred depending on the memory that allocated during agent installation on the computer.
File distribution and software installation fails.	The following problem has been corrected: When a distribution task is executed to a PC on which an agent was installed by the Custom Installation process, a file is not distributed or software is not installed, even though the Task Status displays as Completed and Successful. This problem occurred when the agent installation path is 55 characters or longer.
An extra message might be displayed when a file is saved in Microsoft Excel.	The following problem has been corrected: When you attempt to overwrite a file in Microsoft Excel on an agent-installed computer, you may receive the following error message: "The file may have been changed by another user since you last saved it. In that case, what do you want to do?" This problem occurred when all of the following conditions were met: 1. Operations Logs are enabled in a security policy. 2. The operating system is Windows Vista or later. 3. Overwrite operation is repeated in Microsoft Excel.

Summary	Description
Network communication (of the operating system or applications) fails.	The following problem has been corrected: Network communication (of the operating system or applications) fails on an agent-installed computer if that agent-installed computer has not been restarted since Operations Logs have been disabled in a security policy. This problem occurred when all of the following conditions were met: If the Director software is version 2.5.0: 1. Operations Logs are enabled in a security policy that is assigned to an agent-installed computer. 2. Then Operations Logs are disabled in the security policy assigned to the agent-installed computer. 3. After the security policy (mentioned in Condition 2) is applied to an agent-installed computer, that computer is not restarted. If the Director software is version is 3.0.0: 1. Operations Logs are enabled in a security policy that is assigned to an agent-installed computer and the security policy satisfies any of the following conditions: a. Only operations that divulge information (recommended) is selected in the **Target Operations to be Logged** settings. b. Select target operations is selected in the **Target Operations to be Logged** settings and any of the following are selected in **Select target operations** > **Operation Classification**: • File Operation/Print Operation • Folder Operation • Web Access c. Any of the following are selected in the **Suspicious Operations to be Notified** settings: • Send/Receive E-mail with Attachments • Use Web/FTP Server • Copy/Move the File to External Device 2. Then either of the following settings is set in a security policy that is assigned to that agent-installed computer: a. Disable Operations Logs. b. Enable Operations Logs and set all the following settings in **Operations Logs** settings: • Deselect the **File Operation/Print Operation**, **Folder Operation**, and **Web Access** in the **Target Operations to be Logged** > **Operations Classification** settings. • Deselect **Send/Receive E-mail with Attachments**, **Use Web/FTP Server**, and **Copy/Move the File to External Device** in the **Suspicious Operations to be Notified** settings. 3. After the security policy (mentioned in Condition 2) is applied to an agent-installed computer, that computer is not restarted.

Summary	Description
The features of another software product that uses shell extension don't work properly.	The following problem has been corrected: The features of another software product that uses shell extension won't work properly on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. A software product that uses shell extension is installed on an agent-installed computer. 2. After Step 1, an agent is uninstalled.
Operations Logs are not uploaded to the management server.	The following problem has been corrected: The agent process crashes on an agent-installed computer and the Operations Logs are not uploaded to the management server. This problem occurred when all of the following conditions were met: 1. In a security policy (**Other Access Restrictions** > **USB Device**), the **Restrict Reading/Writing** option is enabled and the **Allow Registered USB Device Usage** checkbox is checked. 2. A registered USB device is connected to an agent-installed computer. 3. There is a file whose modified date and time is later than year 10000, on the USB device connected. This problem also occurred when all of the following conditions were met: 1. Operations Logs are enabled in a security policy. 2. A file operation is performed on a file whose modified (or created) date and time is later than year 10000.
The Agent Monitor Control service might hang up or crash on an agent-installed computer.	The following problem has been corrected: The Agent Monitor Control service might hang up or crash on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. Any of following are enabled in a security policy: **Operations Logs, Restrict Reading/Writing for USB device, Printing Restriction,** or **Blocked Software**. 2. An agent-installed computer is in operation while the system clock on that computer is currently showing a time that is after 2:00 AM.
The agent process might crash on an agent-installed computer.	The following problem has been corrected: The agent process might crash on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. Operations Logs are enabled in a security policy. 2. File operations are performed simultaneously on a large number of files in Windows Explorer.

Summary	Description
Memory usage of the Print Spooler service on an agent-installed computer keeps increasing.	The following problem has been corrected: Memory usage of the Print Spooler service on an agent-installed computer keeps increasing. This problem occurred when all of the following conditions were met: 1. **Printing Restriction** is enabled in the **Other Access Restriction** security policy. 2. A printer is registered on an agent-installed computer.
The CPU usage for the agent process might reach 100% on an agent-installed computer.	The following problem has been corrected: The CPU usage for the agent process might reach 100% on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. Operations Logs are enabled in a security policy. 2. Internet Explorer on an agent-installed computer is version 6. 3. An IP address is specified in the **Web Access log acquisition** condition. Or, an IP address is specified in the acquisition condition of **Use Web/FTP Server** settings of **Suspicious Operations to be Notified**. 4. Any one of the following operations is numerously performed at the same time: • Access to a Web page • Web upload • Web download • FTP send • FTP receive
The CPU usage for the agent process is high on an agent-installed computer.	The following problem has been corrected: The CPU usage for the agent process is high on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. In the security policy **Other Access Restrictions > USB Device**, **Restrict Reading/Writing** is enabled and **Allow Registered USB Device Usage** is selected. 2. There are several tens of thousands of files on the registered USB device. 3. Any of the following operations is performed: • An agent-installed computer is started while a registered USB device connected to the computer. • A registered USB device is connected to an agent-installed computer. • A file operation is performed within the connected registered USB device.

Summary	Description
An agentless management device only displays the IP address as the device details.	The following problem has been corrected: For a device whose management type is Agentless Management (Authentication Successful), only the IP address is displayed as the device details. This problem occurred when Discovery from IP Address Range is executed for a device whose operating system is not started.
The features of another file monitoring software product might not work properly.	The following problem has been corrected: The features of another file monitoring software product might not work properly on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. If the Director software is version 2.5.0: Operations Logs are enabled in a security policy that is assigned to an agent-installed computer. If the Director software is version is 3.0.0: Operations Logs are enabled in a security policy that is assigned to an agent-installed computer and the security policy satisfies any of the following conditions: • **Only operations that divulge information (recommended)** is selected in the **Target Operations to be Logged** settings. • **Select target operations** is selected in the **Target Operations to be Logged** settings and any **File Operation/Print Operation, Folder Operation** or **Web Access** is selected in the **Select target operations** > **Operation Classification**. • **Send/Receive E-mail with Attachments, Use Web/FTP Server,** or **Copy/Move the File to External Device** is selected in the **Suspicious Operations to be Notified** settings. 2. A software product made by another company that monitors files is installed. 3. Any of the following software applications are used: • Explorer • Internet Explorer • Firefox • Outlook • Outlook Express • Windows Mail • Windows Live Mail
There is no response from the Web server.	The following problem has been corrected: When a certain value in the header of the HTTP request is specified and a connection to the IT Operations Director Web server is established, the Web server did not respond.

From 3.0.0-01 to 3.0.0-03

Summary	Description
The IT Operations Director Agent Control service might not start.	The following problem has been corrected: The IT Operations Director Agent Control service might not start. This problem occurred when starting the IT Operations Director Agent Control service.
You might not be able to view device information.	The following problem has been corrected: If IT Operations Director detects a shutdown of an agent-installed computer that does not exist in the **Device Inventory** list, an error will occur. For example, you might not be able to view the **Device List** anymore. This problem occurred when Director detects a shutdown of an agent that does not exist in the **Inventory tab > Device Inventory > Device List/Device List (Network)/Department List/ Location List**.
The IT Operations Director Agent Control service might stop.	The following problem has been corrected: The IT Operations Director Agent Control service might stop when an invalid Operations Log file is sent from an agent. This problem occurred when an invalid Operations Log file was sent from an agent.
Registering a device or updating device details might fail.	The following problem has been corrected: The following actions might fail: • A device on which an agent is installed might not be registered on the management server. • Registering a USB device from any agent-installed computer might fail. • Updating device details might fail for any agent-installed computer. This problem occurred when there was an error during the connection process with an agent.
An agent might not be able to connect to the management server.	The following problem has been corrected: An agent might not connect with the management server, and information from the agent-installed computer might not be updated to the management server. This problem occurred if there was a Windows-managed damaged file on the agent-installed computer.

Summary	Description
Reading files from Internet Explorer add-ons might fail.	The following problem has been corrected: Reading files from Internet Explorer add-ons might fail on an agent-installed computer. This problem occurred when all of the following conditions were met: 1. A security policy in which Operations Logs are enabled is assigned to an agent-installed computer. 2. If the software version is 3.0.0, the assigned security policy satisfies any of the following conditions: • **Only operations that divulge information (recommended)** is selected from the **Target Operations to be Logged** settings. • **Select target operations** is selected from the **Target Operations to be Logged** settings. And **File Operation/Print Operation, Folder Operation** or **Web Access** is checked for the **Select target operations > Operation Classification**. • **Send/Receive E-mail with Attachments, Use Web/FTP Server, or Copy/Move the File to External Device** is selected from the **Suspicious Operations to be Notified** settings. 3. Any of the following Web browsers or E-mail applications are used on an agent-installed computer: • Internet Explorer • Firefox • Microsoft Outlook Express • Microsoft Outlook • Windows Mail • Windows Live Mail 4. A file-open operation is performed on the same file several times, on add-ons that are running on the application (mentioned in Condition 3).

Summary	Description
Discovery from IP Address, Agent Deployment, Update Device Details, or a periodic update of device information might fail.	The following problem has been corrected: **Discovery from IP Address, Agent Deployment, Update Device Details**, or a periodic update of device information might fail after you install **Network Access Control** on the management server. This problem occurred when all of the following conditions were met: 1. The operating system of the management server is any of the following: • Windows Server 2003 Standard Edition • Windows Server 2003 Enterprise Edition • Windows Server 2003 R2 Standard Edition • Windows Server 2003 R2 Enterprise Edition 2. Network Access Control is installed on the management server. 3. The Enable Network Access Control feature is enabled. 4. Any of the following are executed. • Discovery from IP Address • Agent Deployment • Update Device Details • Periodic update of device information
You might encounter problems working within the management console.	The following problem has been corrected: You might not be able to work within the management console when a database access error occurs. This problem occurred when all of the following conditions were met: • The management server's Operating System is Windows XP with Service Pack 2 or Service Pack 3. • There are more than 10 agent-installed computers (not started).
The IT Operations Director Agent Control service might stop - 1.	The following problem has been corrected: The IT Operations Director Agent Control service might stop when invalid system information is sent from an agent. This problem occurred when invalid system information was sent from an agent.
The IT Operations Director Agent Control service stops - 2.	The following problem has been corrected: The IT Operations Director Agent Control service stops when an IPv6 IP address is sent from an agent. This problem occurred when an IPv6 IP address was sent from an agent.
Acquiring Installed Software information consumes CPU resources.	The following problem has been corrected: Acquiring Installed Software information consumes CPU resources and takes time on an agent-installed computer. This problem occurred when an agent was acquiring security items.

Summary	Description
Task result might be listed as "Failed."	The following problem has been corrected: An agent might be listed a Package Distribution Task or an Uninstallation Task as "Failed" even if it was successful. This problem occurred when all of the following conditions were met: 1. Security items are being monitored. 2. The Package Distribution Task or Uninstallation Task is executed while security items are being monitored.
The USB files might not be listed.	The following problem has been corrected: The USB files might not be listed (from an agent to the management server). This problem occurred when a large number of files were stored in the USB device.
An agent-installed computer cannot communicate with the management server.	The following problem has been corrected: An agent-installed computer cannot communicate with the management server. This problem occurred when an error occurred in the connection process with the management server on an agent-installed computer.
The IT Operations Director Agent Service stops.	The following problem has been corrected: The IT Operations Director Agent Service stops on an agent-installed computer. This problem occurred when an agent-installed computer received an activation request and experienced an error during the processing of that request.
Downloading a file that is attached to a hardware asset fails.	The following problem has been corrected: When a file larger than 128 MB – and that is attached to a hardware asset as hardware information– is downloaded, the "session timeout" message is displayed and you get a corrupted file. This problem occurred when you downloaded a file larger than 128 MB that has been attached to a hardware asset.

Summary	Description
An agent cannot communicate with the management server after the security policy change.	The following problem has been corrected: An agent cannot communicate with the management server if the agent-installed computer has not been restarted since a security policy has been changed. This problem occurred when all of the following conditions were met: **If the Director software is version 2.5.0:** 1. Operations Logs are enabled in a security policy that is assigned to an agent-installed computer. 2. Then Operations Logs are disabled in the security policy assigned to the agent-installed computer. 3. After the security policy (mentioned in Condition 2) is applied to an agent-installed computer, that computer is not restarted. **If the Director software is version is 3.0.0:** 1. Operations Logs are enabled in a security policy that is assigned to an agent-installed computer and the security policy satisfies any of the following conditions: (a) **Only operations that divulge information (recommended)** is selected in the **Target Operations to be Logged** settings. (b) **Select target operations** is selected in the **Target Operations to be Logged** settings and any **File Operation/Print Operation, Folder Operation** or **Web Access** is checked in **Select target operations** > **Operation Classification**. (c) **Send/Receive E-mail with Attachments, Use Web/FTP Server,** or **Copy/Move the File to External Device** is selected in the **Suspicious Operations to be Notified** settings. 2. Then set either of the following settings in a security policy that is assigned to the agent-installed computer: (a) Disable Operations Logs. (b) Enable Operations Logs and set all the following settings in Operations Logs settings: • Uncheck **File Operation/Print Operation, Folder Operation**, and **Web Access** in the **Target Operations to be Logged** > **Operations Classification** settings. • For **Suspicious Operations to be Notified** settings, uncheck **Send/Receive E-mail with Attachments, Use Web/FTP Server**, and **Copy/Move the File to External Device.** 3. After the security policy (mentioned in Condition 2) is applied to an agent-installed computer, that computer is not restarted.
The IT Operations Director Web Container service might not start.	The following problem has been corrected: The IT Operations Director Web Container service might not start. This problem occurred when starting the IT Operations Director Web Container service.

Summary	Description
An agent fails to deploy.	The following problem has been corrected: The "Internal Error" message is displayed when you deploy an agent to a target computer in which Administrative Share is disabled and from a management console in which the Web browser language is English. Also, no information is displayed in the Agent Deployment list. This problem occurred when agents were deployed to a target computer in which Administrative Share was disabled and from the management console where the Web browser language is English.
New settings in the management server might not be reflected in the agents.	The following problem has been corrected: When you upgrade an agent by using the Agent Installer, the new management server settings with which the agent connects might not be reflected in the agents. This problem occurred when all of the following conditions were met: 1. In **Settings > Agent > Agent Configurations > Add/Edit Agent Configurations**, the settings of the management server for agents to connect with are changed. 2. An Agent Installer is created with the agent configuration. 3. The agent is upgraded using the Agent Installer in an agent-installed computer that connects with a management server which has not yet been changed as described in Step 1.
Installed Software details of an agent might not be correctly registered.	The following problem has been corrected: Installed Software details of an agent might not be correctly registered. This problem occurred when all of the following conditions were met: 1. For a device, Management Type is Agentless Management and Windows authentication has failed. 2. For the device mentioned in Condition 1, an agent is installed on the device or Windows authentication succeeds on the device.
Printer details might not be registered.	The following problem has been corrected: Printer details of a printer device might not be registered. This problem occurred when either of the following conditions was met: • A printer (whose host name was not acquired by Director or is a printer without host name) is discovered as a result of IP discovery and that printer is set as a managed node. • From the management console, any of the following items is edited manually for a printer that has already been registered. ○ Host name ○ IP address ○ Subnet mask ○ Operating system Then, when IP discovery is performed, Director cannot acquire the information that is edited manually.

Summary	Description
A device might incorrectly belong to the "Device Type: Unknown" group.	The following problem has been corrected: Although the device's operating system name is correctly displayed, the device might incorrectly belong to the group of "Device Type: Unknown." This problem occurred when all of the following conditions were met: 1. From the management console, for a device whose operating system information is not registered, the operating system information is set manually. 2. After Step 1, Director receives the information from the corresponding device.
Management server installation or setup might fail.	The following problem has been corrected: Management server installation or setup might fail. This problem occurred when any of the following conditions was met: • **Quick Installation** is executed. • In the **Setup > Operations Log Settings** panel, the Use Operations Log check box is selected or deselected. • Logical IP address is changed in the **Setup** > **Cluster Environment** panel.
You might not be able to edit the software license information.	The following problem has been corrected: You might not be able to edit the software license information. This problem occurred when all of the following conditions were met: 1. Display **Assets** > **Software Licenses** > **Software License List**. 2. In the above list, scroll down to view more than 200 software licenses (and license information). 3. Select multiple software licenses from the list and click Edit. A similar problem might occur when you attempt to perform **Action** menus options for the following lists: • **Security** > **Computer Security Status** > **Device List** or **Network List** or **Department List** or **Location List**. • **Inventory** > **Device Inventory** > **Device List** or **Device List (Network)** or **Department List** or **Location List**.
A device that is set as an Ignored Node is displaying on the list.	The following problem has been corrected: A device which has already been set as an Ignored Node is displayed in **Assets** > **Managed Software** > **Managed Software List** > **Installed Computers** tab. This problem occurred when all of the following conditions were met: 1. Software managed as **Managed Software** is installed on a device which is set to be an **Ignored Node**. 2. In **Assets** > **Managed Software** > **Managed Software List**, select a managed software mentioned in Step 1 and display the **Installed Computers** tab.

Summary	Description
From Firefox, updating version information of the add-on for IT Operations Director Agent fails and Operations logs cannot be collected.	The following problem has been corrected: When you upgrade the IT Operations Director Agent, the Firefox version information in the add-on for IT Operations Director Agent fails to reflect the update and the **Operations** logs in Firefox cannot be collected. This problem occurred when all of the following conditions were met: 1. **Operations Logs** are enabled in a security policy that is assigned to an agent-installed computer. 2. If the Director software version is 3.0.0 and the assigned security policy satisfies any of the following settings: • **Only operations that divulge information (recommended)** is selected in the **Target Operations to be Logged** settings. • **Select target operations** is selected for the **Target Operations to be Logged** settings. Then **File Operation/Print Operation, Folder Operation**, or **Web Access** is checked in **Select target operations > Operation Classification**. • **Send/Receive E-mail with Attachments, Use Web/FTP Server**, or **Copy/Move the File to External Device** is selected for the **Suspicious Operations to be Notified** settings. 3. Firefox 3.5 or 3.6 is used on the agent-installed computer. 4. You upgrade the IT Operations Director Agent.

Summary	Description
An item named "Unknown" is registered incorrectly.	The following problem has been corrected: **Department** and **Location** are fields in hardware assets. Although the item is named **Unknown** and therefore not allowed to be registered in the lower hierarchy of **Department** and **Location**, you can still register the item named **Unknown** in the highest hierarchy. This problem occurred when all of the following conditions were met: 1. Display **Settings** > **Assets** > **Asset Field Definitions**. 2. In the **Common Fields (Hardware Assets and Device Inventory)** table, click **Edit** for **Department** or **Location**. The **Edit Custom Fields** dialog box displays. 3. For the data type, **Hierarchy** is selected. Click **Edit** to open the **Edit Hierarchy** dialog box. 4. Add the item called **Unknown** to the highest hierarchy. Click **OK**. 5. In the **Edit Custom Fields** dialog box, click **OK**. A similar problem occurred if **Enumeration** is selected for the data type and you add **Unknown**. Moreover, a similar problem occurred in the following windows where you can open the **Edit Custom Fields** dialog box: • **Security** > **Computer Security Status** > **Department List** or **Location List** (in Navigation panel) > **Edit** icon**.** • **Assets** > **Hardware Assets** > **Department List** or **Location List** (in Navigation panel) > **Edit** icon**.** • **Assets** > **Hardware Assets** > **Department List** or **Location List** > **Add/Edit Hardware Asset** dialog box**.** • **Assets** > **Hardware Assets** > **Department List** or **Location List** > **Import Assets** wizard**.** • **Inventory** > **Device Inventory** > **Department List** or **Location List** (in Navigation panel) **> Edit** icon**.** • **Inventory** > **Device Inventory** > **Device List** or **Device List (Network)** or **Department List** or **Location List** > **Edit Device Details** dialog box**.** • **Settings** > **Discovery** > **Discovered Nodes** > **Edit Device Details** dialog box**.** • **Settings** > **Discovery** > **Managed Nodes** > **Edit Device Details** dialog box**.**
Exporting the Event List on and after Page 2 fails.	The following problem has been corrected: If the **Event List** is longer than one page, when you export the list only Page 1 is exported. This problem occurred when you export an **Event List**. Pages 2 or later in **Events** > **Events List** will not export.

Summary	Description
A computer on which Network Access Control is enabled might be temporarily unable to communicate.	The following problem has been corrected: A computer which has been blocked by Director's Network Access Control may temporarily unable to communicate with an Exclusive Communication Destination. An Exclusive Communication Destination is a special internet destination that has been defined by the administrator. Computers that have been blocked by Network Access Control are normally allowed to access Exclusive Communication Destinations. This problem occurred when the IP address of the device on which Network Access Control was enabled was specified on **Network Access Control** > **Network Access Control Settings** > **Exclusive Communication Destination for Access-Denied Devices** screen.
A Windows Update is listed incorrectly in the Events List.	The following problem has been corrected: A Windows Update is installed on an agent-installed computer but is listed incorrectly in the Events List as **New software has been discovered**: **Event #: 1004** **Description: New software has been discovered.** This problem occurred when software information for Windows Update was sent by an agent.
Windows Updates are included in the Fluctuation of Installed Software in Summary Reports.	The following problem has been corrected: Windows Updates are included in the target of the fluctuation in the **Fluctuation of Installed Software** in **Summary Reports**, even though they are not supposed to be included. This problem occurred when software information for Windows Updates was sent by an agent.
The latest Scanned Date/Time of Antivirus software might be incorrect.	The following problem has been corrected: The Date and Time of a Latest Scanned of an Antivirus software might be incorrect. This problem occurred when OfficeScan Corporate Edition 10.5 Patch1 was installed on an agent-installed computer.
The time required to execute the ioutils command might gradually increase.	The following problem has been corrected: The amount of time required to execute the data import and export command (the **ioutils** command) might gradually increase. This problem occurred when you executed the **ioutils** command.

Summary	Description
It might take a long time for a certain operation to be completed.	The following problem has been corrected: It might take a long time for a certain operation to be completed. This problem occurred when any of the following operations is executed: • Discovery from IP Address Range • Discovery from Active Directory • Agent Deployment • Update Device Details The problem occurred only when the information from an agent-less computer or a device other than a computer is updated with: • Allow or block Network Access • Distribute Updates The problem occurred only when Distribute Update is executed in the Security tab > Security Policies > Security Policy List > Windows Update tab: • Calculate Security Diagnosis Reports • Calculate Security Detail Reports • Calculate Inventory Detail Reports • Calculate Asset Detail Reports
An incorrect event might be displayed on the Event List.	The following problem has been corrected: The following event might be incorrectly displayed on the Event List on the management server: **Event #: 208** **Description: An error occurred while updating received files.** This problem occurred when all of the following conditions were met: 1. Any of the following notifications is sent by an agent: - Distribution result - The result of whether Network Access Control is installed - Event - Uninstallation 2. If you click **Ignore** or **Remove** for the device affected by Step 1 on the management server at the same time that the notification in Step 1 is sent.
An Uninstallation Task result might display as "Failed."	The following problem has been corrected: When software is uninstalled by the Uninstallation Task and requires a target computer in order to restart, the task result might display the uninstallation as "Failed", even though the software uninstallation was successful and the target computer was restarted. This problem occurred software was uninstall by the Uninstallation Task and that required a target computer to restart.

Summary	Description
The Event [The agent's operation has been stopped.] might be displayed on Event List.	The following problem has been corrected: When you install an agent, the following event might be displayed on the Event List in the management console. **Event #: 1003** **Description: The agent's operation has been stopped.** This problem occurred when an agent version was upgraded or the agent installation was overwritten by another installation.
A security policy might be incorrectly assigned to an agent.	The following problem has been corrected: A security policy might be incorrectly assigned to an agent. This problem occurred when all of the following conditions were met: 1. You create an Agent Installer. 2. You remove the Agent Configuration that was used in Step 1. 3. You register a new agent, using the Agent Installer created in Step 1.
Last Modified Date/Time might be updated incorrectly.	The following problem has been corrected: When you update device information for a device, the Last Modified Date/Time of another device that was added or updated before will be incorrect. This problem occurred when either of the following conditions was met: 1. After adding a device newly, you update the information of another device. 2. After the End User Form information of a device has been sent, you update the information of another device.
Department information acquired from an agent might not be reflected in the management server.	The following problem has been corrected: Department information acquired from an agent might not be reflected in the management server. This problem occurred when all of the following conditions were met: 1. In discovery settings for the Active Directory, you select the **Get Department Hierarchy Information** check box and perform the Active Directory discovery. 2. Later, the inventory information (including Department information) is received from an agent.

Summary	Description
The device status of a device with Network Access Control might not be updated from "Stop".	The following problem has been corrected: For a device whose Management Type is Agent Management (Network Access Control), the Device Status might not be updated from "Stop." This problem occurred when all of the following conditions were met: 1. When you enable Network Access Control for a device and it takes 10 minutes (or more) longer than the time for the Server Connection Interval set in Agent Configuration to reflect the result of the enabled Network Access Control to the management server. 2. If the agent did not communicate with the management server for 10 minutes (or more) longer than the time for the Server Connection Interval set in Agent Configuration because of a network failure.
The last Alive Confirmation Date/Time of a device which has not been started up might be falsely updated.	The following problem has been corrected: The **Last Alive Confirmation Date/Time** of a device which has not been started up might be falsely updated. This problem occurred when all of the following were met: 1. You discover devices by **Discovery from IP Address Range.** 2. You power OFF the discovered devices. 3. You execute **Discovery from IP Address Range** again.
The event [The network access control has stopped running.] might be falsely displayed.	The following problem has been corrected: The following event might be displayed even though the processing of the network access control has not stopped running. **Severity: Warning** **Type: Security** **Event #: 1082** **Description: The network access control has stopped running.** This problem occurred when the management server could not communicate with an agent of a Network Access Control enabled computer for 10 minutes (or more) longer than the time for the Server Connection Interval set in Agent Configuration because of a network failure.
Hardware assets might not be displayed in Department List or Location List.	The following problem has been corrected: When you select a department or location (in which assets exist) from navigation panel of Hardware Assets, assets might not be displayed to the Department List or Location List window. This problem occurred when you selected a department or location in which "\" is included in the department or location name.

Summary	Description
An "Internal Error" message might be triggered when you change a device to Ignored Node.	The following problem has been corrected: An "Internal Error" message might be triggered when you change a device to Ignored Node, if another administrator has just enabled Network Access Control for the same device. This problem occurred when you click **Ignore** in **Settings** > **Managed Nodes** for a device in which Network Access Control has been just enabled. Normally, it is impossible to click **Ignore** if a device is Network Access Control enabled. However, this problem might occur when another administrator enables Network Access Control at the same time that you click **Ignore**.
Nothing is displayed in the top and bottom of the list when you sort the Network Filter Settings list.	The following problem has been corrected: Nothing is displayed in the top and bottom of the list when you sort the Network Filter Settings list by the following items: - User Name - Manufacturer - Operating System - E-mail - Phone This problem occurred when items were added from the **Add Allow or Deny Network Access Permission** dialog box.

Summary	Description

Character strings are incorrectly added to the Notes.	The following problem has been corrected:
	Notes added to the **Add Notes** text box in the following dialog boxes are incorrectly added to the **Notes**:
	- The **Hardware Assets**
	  o The **Change Asset Status** dialog box
	  o The **Update Tracked Date (Directly)** dialog box
	  o The **Update Tracked Date (from CSV)** dialog box
	  o The **Change Asset Status (Planned)** dialog box
	- **Software Licenses**
	  o The **Change License Status** dialog box
	  o The **Update Tracked Date (Directly)** dialog box
	  o The **Update Tracked Date (from CSV)** dialog box
	  o The **Change License Status (Planned)** dialog box
	- **Contracts**
	  o The **Change Contract Status** dialog box
	- **Inventory > Device Inventory**
	  o The **Send User Notification** dialog box
	- **Security > Computer Security Status**
	  o The **Send User Notification** dialog box
	This problem occurred when the characters "\" or "$" were included in the character strings added in the **Add Notes** text box.

It takes time to display the Update Group list when you select an update group from navigation panel.	The following problem has been corrected: When you select an update group from the navigation panel of the Windows Update window, it takes time to display the Windows update list of the selected group. This problem occurred when all of the following conditions were met: 1. With Hitachi IT Operations Director 2.5.0, certain Windows updates are selected as Excluded updates or Mandatory updates in a security policy.* 2. You upgrade from Hitachi IT Operations Director 2.5.0 to Hitachi IT Operations Director 3.0.0. * The exact number at which it occurs can depend on the performance of the PC upon which Hitachi IT Operations Director is installed. However, it occurs when approximately more than 100 Windows updates are set as Excluded updates or Mandatory updates.

Summary	Description
The Deterrence Log of Operations Logs is collected incorrectly.	The following problem has been corrected: When **Printing Restriction, Blocked Software,** and **USB Device Restriction** are performed on an agent-installed computer, the **Deterrence Log** of the Operations Logs is collected incorrectly even though Operations Logs are disabled. This problem occurred when all of the following conditions were met: 1. The following settings are set in the security policy: o Operations Logs are enabled with the **Deterrence Log** (**Block Program Activation, Block Printing,** and **Block Attached External Device**) as a collecting target. o In the **Other Access Restriction** panel, **Printing Restriction, Blocked Software, or USB Device Restriction** is enabled. 2. After Step 1, you disable Operations Logs in the security policy and the agent-installed computer is not restarted. 3. After Step 2, **Printing Restriction, Blocked Software,** or **USB Device Restriction** is performed.
The registered Date/Time of software information might be incorrect.	The following problem has been corrected: The registered Data/Time of software information might be incorrect. This problem occurred when the software information was sent by an agent that was registered again after the software information was removed from the management console.

From 3.0.0 to 3.0.0-01

Summary	Description
Upgrading the database might fail.	The following problem has been corrected: Upgrading the database might fail when you upgrade IT Operations Director from version 2.5.0 to 3.0.0. This problem occurred when all of the following conditions were met: • In IT Operations Director 2.5.0, all of the following operations have been performed: ▪ In a security policy (**Other Access Restrictions** > **USB Device**), you enable both **Restrict Reading/Writing** and **Allow Registered USB Device Usage** at the same. ▪ From the computer to which the above security policy is assigned, you perform a device registration for a USB device on which approximately 15,000 or more files are stored. ▪ From the Assets window, you change the asset status of a registered USB device to a status other than "Unconfirmed." • You upgrade IT Operations Director to version 3.0.0.
Installing the agent fails.	The following problem has been corrected: Installing an IT Operations Director agent fails if the USB Graphics Windows Driver made by DisplayLink is installed on the target computer. This problem occurred when the USB Graphics Windows Driver made by DisplayLink is installed on the target computer.
The security status of the **Scan Engine Version** of **Antivirus Software** might not change to "Safe."	The following problem has been corrected: The security status of the Scan Engine Version of antivirus software might not change to "Safe." This problem occurred when all of the following conditions were met: • In a security policy, for **Antivirus Software**, the **Scan Engine Version** is set as security judgment target for OfficeScan Corporate Edition. • The antivirus software installed on the managed target computer has either: ▪ Been updated from OfficeScan Corporate Edition 8.0 to OfficeScan Corporate Edition 10.0 or 10.5. ▪ Both OfficeScan Corporate Edition 8.0 and OfficeScan Corporate Edition 10.0 or 10.5 installed.

Summary	Description
The IT Operations Director Agent features might stop when the trial license period expires.	Even if you change your license from a trial version to a product version, the license information of the product version might fail to notify the agents. Therefore the IT Operations Director Agent features stop when your trial license period expires. This problem occurred when all of the following conditions were met: 1. You move your license from a trial version to a product version. 2. After moving your license to a product version, you have not restarted the IT Operations Director services. 3. The trial license period expires.
Cannot detect the suspicious operation of sending an e-mail with attachments.	The following problem has been corrected: The act of sending an e-mail with attachments is not detected as a suspicious operation when the e-mail is sent, even if the act is set as a target of suspicious activity for monitoring. This problem occurred when all of the following conditions were met: 1. You set the following in a security policy: ▪ Operations Logs are enabled. ▪ **Suspicious Operations to be Notified** and **Send/Receive E-mail with Attachments** are enabled. ▪ In the **Suspicious Operation Condition** dialog box, when deciding which conditions to monitor, you enter a character string in **E-mail**, and select **Send E-mail** or **Send/Receive E-mail** for **User Action** and select **Do not monitor** for **Operation**. 2. On an agent-installed computer, you send an e-mail to multiple addresses. 3. Among the destination addresses specified in Step 2, there is at least one address that doesn't match a character string specified in **E-mail** in Step 1.

Summary	Description
Exporting the File List from a USB device might fail.	The following problem has been corrected: You might not be able to export the File List of a USB device. This problem occurs when you attempt to export a USB device's File List that contains a large amount of data. The condition of occurrence depends on the data volume (the volume of character strings of each item) of the File List you are trying to export. This problem occurs when there are approximately 10,000 items on a File List. However, it might also occur when there are less than 10,000 items on a File List, depending on the specifications of the management console machine. Moreover, a similar problem might occur when exporting the following lists: • Security > Computer Security Status > Device List or Network List or Department List or Location List • Assets > Hardware Assets > Department or Location List • Assets > Hardware Assets > Department or Location List > File List tab • Assets > Software Licenses > Software License List • Assets > Managed Software > Managed Software List • Assets > Contracts > Contract List • Inventory > Device Inventory > Device List or Device List(Network) or Department List or Location List • Inventory > Software Inventory > Software List • Inventory > Software Inventory > Software List > Installed Computers tab • Distribution > Packages > Package List • Distribution > Tasks > Task List • Settings > Discovery > Discovered Nodes • Settings > Discovery > Managed Nodes • Settings > Discovery > Ignored Nodes
The security status of **Scan Engine Version** and **Virus Definition File Version** of **Antivirus Software** incorrectly displays as "Safe."	The following problem has been corrected: Security status of **Scan Engine Version** and **Virus Definition File Version** of **Antivirus Software** incorrectly displays as "Safe." This problem occurred when all of the following conditions were met: 1. Either (or both) **Scan Engine Version** and **Virus Definition File Version** of **Antivirus Software** are set as a security judgment target in a security policy. 2. You update the **Scan Engine Version** or **Virus Definition File Version** of **Antivirus Software** for managed nodes. 3. The dates specified for the **Update Time limit** of **Scan Engine Version** and **Virus Definition File Version** in a security policy have already passed. 4. A security judgment is run on a node that uses a version older than the updated **Scan Engine Version** or **Virus Definition File Version**.

From 2.5.0-07 to 3.0.0

Summary	Description
Downloading files might fail with Internet Explorer 9.	The following problem has been corrected: When you download a file in Internet Explorer 9 on an agent-installed computer, the file might not be correctly saved in the designated save destination folder and file size might become 0 bytes. This problem occurred when all of the following conditions were met: • Operations Logs are enabled in a security policy. • A Hitachi IT Operations Director Agent is installed on the computer. • Protected mode is enabled in Internet Explorer 9. • You launch Internet Explorer 9 with standard user permissions. • The User Account Control (UAC) setting is enabled. • The designated save destination folder is under %USERPROFILE%, such as Desktop or My Documents.
Importing asset information fails	The following problem has been corrected: A system error occurs when you attempt to import asset information from a CSV file, if that asset information includes a custom field that has already been removed. This problem occurred when all of the following conditions were met: • In the Import Assets wizard, in the Step 2 tab (Map Fields), you specify a custom field to import from a CSV file and click Next. • From the time you start the Import Assets wizard until you click Next in the Step 2 tab, the custom field you set to import has been removed in a separate window.
A system error might occur in the Managed Software List window.	The following problem has been corrected: A system error might occur when you click the tab title portion of the Licensed Computers tab in Assets > Managed Software > Managed Software List. This problem occurred when all of the following conditions were met: • In the Licensed Computers tab, you display the Mode column. • You click the tab title portion of the Licensed Computers tab.
Display response becomes progressively slower.	The following problem has been corrected: The display response performance gradually decreases when working within Hitachi IT Operations Director for a couple of hours (or more). This problem occurred after logging in to Hitachi IT Operations Director and using the software for a couple of hours (or more).

Summary	Description
A memory leak might occur after editing a security policy.	The following problem has been corrected: A memory leak might occur after you edit a security policy or change the target computers to which you assign a policy. This problem occurred when all of the following conditions were met: • You change target computers to which you assign a security policy or you edit a security policy. • The target computer to which the policy is assigned to is powered off at a fixed time.
The Hitachi IT Operations Director service might stop.	The following problem has been corrected: When the device information is edited, the IT Operations Director Agent Control service might be stopped. This problem occurred when the system resources became insufficient during the processing of a task.
A memory leak might occur after the device information or the asset information is edited.	The following problem has been corrected: When device information or asset information associated with a device is edited, a memory leak might occur. This problem occurred when all of the following conditions were met: • The device information or asset information associated with a device is edited. • After the information is edited, the device belongs to the second or lower hierarchy in the Device List, Department List, Location List of the Device Inventory hierarchy.
CPU usage increases on an agent-installed computer.	The following problem has been corrected: CPU usage increases on an agent-installed computer on which the Trend Micro antivirus software is installed. This problem occurred when one of the following software applications was installed on an agent-installed computer: • ServerProtect for Windows NT/Netware5.7 (32bit/64bit) • ServerProtect for Windows NT/Netware5.8 (32bit/64bit)

Collecting Operations Logs or blocking software activation might fail.	The following problem has been corrected:
	The Hitachi IT Operations Director Agent service might become unresponsive and cause one of the following security policies to fail: Collecting Operations logs or blocking software activation or other restrictions.
	This problem occurred when all of the following conditions were met:
	• Any of the following security policies are enabled:
	  • Operations logs.
	  • Printing restriction.
	  • Restrict reading/writing of USB device.
	  • Blocked software.
	• The system clock on the agent-installed computer is currently showing a time that is after 2:00 AM.

Summary	Description
Affected programs might not work correctly.	The following problem has been corrected: A process might not work correctly on an agent-installed computer when a wrong return code is returned by the process. This problem occurred when all of the following conditions were met: • Operations Logs are enabled in a security policy. • A Hitachi IT Operations Director Agent is installed on the computer.
You might not be able to collect Operations logs for sending e-mail with attachments.	The following problem has been corrected: Operations Logs for sending e-mail with attachments might be collected with the attached file name garbled or collected incorrectly, or Operations logs for sending e-mail with attachments might not be collected at all. This problem occurred when all of the following conditions were met: • Operations logs are enabled in a security policy. • An e-mail is sent with many attachments from an agent-installed computer.

You might not be able to collect Operations logs for saving/sending/receiving e-mail with attachments.	The following problem has been corrected:
	Operations logs for saving, sending, and receiving e-mails with attachments might not be collected.
	This problem occurred when all of the following conditions were met:
	• Operations logs are enabled in a security policy.
	• Either:
	  • There are more than 110 e-mail-attached files that have already been received on an agent-installed computer.
	  • An e-mail with more than 110 files attached is received or sent.

Hardware Assets cannot be updated.	The following problem has been corrected: Even if you edit the hardware information of a device in the Inventory module, the update is not reflected in the Assets module (in the Asset Information tab, Device Inventory Details field). This problem occurred when the hardware information was edited in the Inventory module.
Windows Explorer might crash.	The following problem has been corrected: Windows Explorer might crash on an agent-installed computer. This problem occurred when the Operations log is enabled in a security policy.

Summary	Description
Connection target server changes might not be reflected in an agent.	The following problem has been corrected: In Agent Configuration in the Settings module, when you change the Server Name (where IT Operations Director is installed) to a wrong one and save the settings, then modify the Server Name to the correct one immediately, then save your changes, the updated server name might not be reflected to the agent side. This problem occurred when the Server Name (where IT Operations Director is installed) is changed in the Agent Configuration two times in a short period of time.

Known Problems

Summary	Description
File limit for information collection.	When the **Restrict Reading/Writing for USB device** is enabled in a security policy, the file information that can be collected from a registered USB device is limited to a maximum of 10,000 files per each device.
Operations may malfunction during discovery.	When discovery is executed, saving the discovery results will consume memory on the management client's computer. The larger the amount of devices that are discovered, the more memory will be required. If memory is insufficient on the computer, the following malfunctions in operations may occur: • Response time may become increasingly slow. • Web browser may become a white screen. To prevent this, do not leave the **Last Discovery Log** window open. If this problem occurs, it does NOT affect the discovery result. Just restart the Web browser and log in to Hitachi IT Operations Director to restore the operation.
A 64-bit machine is displayed in the 32-bit group.	When the device information of a 64-bit machine with a Windows Vista, Windows 7, or Windows Server 2008 operating system is modified, it might be displayed in the "32-bit" group of the **Device List** of the **Menu** area of the **Security** and **Inventory** modules. If this occurs, you can correct the display issue by accessing the **Action** menu, selecting the **Update Device Details** option, and obtaining the latest data.

Installation Notes

You need to activate the IT Operations Director license for the trial or purchased product. An **Activation Token** is required for this process. License activation information is available in the *Hitachi IT Operations Director Getting Started Guide*, in the Help, and by launching Help from each panel of the **License Activation** wizard.

Precautions

Usage Restriction on the German Operating System

When running the English version of IT Operations Director's Manager or Agent on the German operating system, the following restrictions exist:

i) German anti-virus software and German operating system patches (Windows updates) are not supported.

ii) The following Number representations that are unique to the German locale are not supported:

- A comma used as a decimal symbol.
- A period used as a digit grouping symbol.

iii) Network Access Control does not support the German version of Windows 7 and Windows Server 2008.

IT Operations Director 3.0.0-14 Component Version

IT Operations Director 3.0.0-14 consists of the following four components:

- Hitachi IT Operations Director 3.0.0-14
- Hitachi IT Operations Director Agent 3.0.0-14
- Hitachi IT Operations Director RC Manager 3.0.0-14
- Hitachi IT Operations Director NM Agent 3.0.0-14

Web Browsers and E-mail Software

Ensure that Web browsers and the e-mail software used by your organization are listed in the table below (so that Operations logs relating to **Web Access, E-mail with Attachments**, and **FTP** can be collected):

Supported Web Browser and E-mail Software	
Web Browsers	• Internet Explorer 6, 7, 8, 9
E-mail Software	• Microsoft Outlook Express 6 • Microsoft Outlook 2002, 2003, 2007, 2010 • Windows Mail 6 • Windows Live Mail 2009, 2011

Antivirus Software

Ensure that the antivirus software that is used by your organization is listed in the table below:

Supported Antivirus Software	
Symantec Corporation	• Symantec Antivirus Corporate Edition 10.0 (32-bit/64-bit), 10.1 (32-bit/64-bit), 10.2 (32-bit/64-bit) • Symantec Client Security 3.0 (32-bit/64-bit), 3.1 (32-bit/64-bit) • Symantec Endpoint Protection 11.0 (32-bit/64-bit), 12.1 (32-bit/64-bit) • Norton AntiVirus 2010 (32-bit/64-bit), 2011(32-bit/64-bit)
McAfee, Inc.	• McAfee Total Protection Service 5.0 • McAfee SaaS Endpoint Protection5.2 • McAfee VirusScan Enterprise 8.5i (32-bit/64-bit), 8.7i (32-bit/64-bit), 8.8 (32-bit/64-bit)
Trend Micro Incorporated	• OfficeScan Corporate Edition 8.0 (32-bit/64-bit), 10.0 (32-bit/64-bit), 10.5 (32-bit/64-bit) • ServerProtect for Microsoft Windows/NT NetWare 5.7 (32-bit/64-bit), 5.8 (32-bit/64-bit) • PC-cillin 2010 (32-bit/64-bit) • Titanium Internet Security 2011 (32-bit/64-bit) • Worry-Free Business Security - Standard 7.0 (32-bit/64-bit) • Worry-Free Business Security - Advanced 7.0 (32-bit/64-bit)
Microsoft Corporation	Forefront Client Security 1.5 (32-bit/64-bit)
Kaspersky Lab ZAO	• Kaspersky Anti-Virus for Windows Server 6.0.3 (32-bit/64-bit), 6.0.4 (32-bit/64-bit) • Kaspersky Anti-Virus for Windows Workstation 6.0.3 (32-bit/64-bit), 6.0.4 (32-bit/64-bit)
ESET, spol. s r. o.	ESET NOD32 Antivirus 4.0 (32-bit/64-bit), 4.2 (32-bit/64-bit)
Sophos Plc	• Sophos Endpoint Security and Data Protection 9.0 (32-bit/64-bit), 9.5 (32-bit/64-bit) • Sophos Security Suite small business solutions (32-bit/64-bit) 4.0 • Sophos Computer Security small business solutions (32-bit/64-bit) 4.0 • Sophos Anti-Virus small business solutions (32-bit/64-bit) 4.0
F-Secure Corporation	F-Secure Client Security 8.0 (32-bit/64-bit), 9.0 (32-bit/64-bit)

Port Numbers

Check the port numbers of the computers for installing IT Operations Director.

If another application uses the port numbers that IT Operations Director will use, then both applications will fail to work properly.

The available port numbers for IT Operations Director are from 31000 to 31012, and 31080.

To check the port numbers currently being used by an application.

1. Start all applications that will be used in the selected machine.
2. Start **Command** prompt.
3. Type **netstat –a | find "310"** and press **Enter** key.
4. Port numbers from 310 are displayed. (If port numbers from 310 is not used then nothing will be displayed.)

Installing/Uninstalling

For installing/uninstalling IT Operations Director, refer to the *Hitachi IT Operations Director Getting Started Guide.*

Refer to the table below for the list of precautions to be followed:

IT Operations Director Precautions	
Installation/Uninstallation	Terminate all Windows applications before installation/uninstallation. If you perform an installation/uninstallation while IT Operations Director is running, you will need to restart the operating system regardless of success or failure of the installation/uninstallation.
Installation folder path contains space	If the path for the installation folder contains a space and there is a file that has the name same as that of the path name before the space, the installation fails. For example, the installation folder path is "C:\Program Files\Hitachi\Director" and there is a file whose name is "Program" under the C drive, the installation fails. In this case, move the file to another directory or change the file name. If the file is unnecessary, delete it and then perform the installation.
Creating Agent environment using Remote Desktop Connection	• Remote Desktop Connection can be used for only installation, setup, uninstallation, and troubleshooting agents. • During the above mentioned process you must use "console session" instead of normal Remote Desktop Connection. To use "console session," specify the **/console** option as follows while starting the Remote Desktop Connection in the working terminal (client side): **mstsc.exe /console** Note: mstsc.exe is an executable file of the Remote Desktop Connection application. Only one user can use the "console session" connection at the same time.

Using Power ON by using Intel AMT	To use AMT, build the environment by using the following steps: a. Check the PC in which the IT Operations Director Agent is installed. Then make sure that DHCP is enabled for IP address assignment for both operating system and AMT. b. Install the Intel AMT driver on the PC that has IT Operations Director Agent installed. i. Configure the BIOS setup of AMT as follows in the PC that has IT Operations Director Agent installed. Specify "Small Business" for Provision Model. ii. Specify "Enable" for DHCP Mode. iii. Configure other settings such as user name and password of AMT. c. Register a DLL assembly for the AMT feature in both the PCs (one with IT Operations Director installed and the other with IT Operations Director Agent installed). To perform Assembly Registration, please refer to the following. i. Click **Start**, and then **Run**. ii. Type cmd and press **Enter**. The Command Prompt opens. iii. Use the cd command and move to Microsoft .NET Framework folder in which RegAsm.exe exists. Example: cd C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727 iv. Execute the Assembly Registration tool (Regasm.exe) as follows: **Using the default directory for installation** [Hitachi IT Operations Director] Example of executing the Assembly Registration tool: Regasm.exe /register "C:\Program Files\Hitachi\Director\mgr\bin\jdnagcamt.dll" [Hitachi IT Operations Director Agent] Example of executing the Assembly Registration tool: Regasm.exe /register /codebase "C:\Program Files\Hitachi\Director Agent\bin\jdngamt.dll" d. Perform the following operations in IT Operations Director and check whether the AMT setting is successfully applied. i. In the **AMT** tab, set the user ID and the password that you have already set in (Step: b-iii). ii. You can execute **Power ON** using Intel AMT if the value is shown in AMT Firmware Version in the **System** tab of the **Inventory** module.
Web Browsers	When you open or log in to the management console, a dialog box indicating **malformed request** or **unexpected error** displays and the management console might be displayed incorrectly. In this case, please delete the Temporary Internet Files in the Web browser. Please note that this symptom is most likely to occur after newly-installing or upgrading Hitachi IT Operations Director. To delete the Temporary Internet Files, complete the following steps: • **Microsoft Internet Explorer 6** 1. In Microsoft Internet Explorer, select **Tools** > **Internet Options**. The **Internet Options** dialog box is displayed.

	2. In the **Internet Options** dialog box, in the **General** tab, click **Delete Files** under **Temporary Internet Files.** The **Delete Files** dialog box displays. 3. In the **Delete Files** dialog box, select **Delete all offline content** and click **OK**. 4. In the **Internet Options** dialog box, click **OK**. • **Windows Internet Explorer 7** 1. In Microsoft Internet Explorer, select **Tools** > **Internet Options**. The **Internet Options** dialog box is displayed. 2. In the **Internet Options** dialog box, select **General** > **Browsing history** > **Delete**. The **Delete Browsing History** dialog box is displayed. 3. In the **Delete Browsing History** dialog box, select **Temporary Internet Files** > **Delete** files. The **Delete Files** dialog box is displayed. 4. In the **Delete Files** dialog box, click **Yes**. • **Windows Internet Explorer 8** 1. In Microsoft Internet Explorer, select **Safety** > **Delete Browsing History**. The **Delete Browsing History** dialog box is displayed. 2. In the **Delete Browsing History** dialog box, select the **Temporary Internet Files** check box, and click **Delete**. • **FireFox** 1. In FireFox, select **Tools** > **Clear Recent History**. The **Clear Recent History** dialog box is displayed. 2. In the **Clear Recent History** dialog box, click the button to the left of **Details**. In the displayed list, select the **Cache** check box, and click **Clear Now**. If this symptom still occurs, delete the Temporary Internet Files of the Web browser based on the applicable steps: • **Microsoft Internet Explorer 6** 1. In Microsoft Internet Explorer, select **Tools > Internet Options**. The **Internet Options** dialog box displays. 2. In the **Internet Options** dialog box, in the **General** tab, click **Settings** under **Temporary Internet Files**. The **Settings** dialog box displays. 3. In the **Settings** dialog box, click **View Files** in the **Temporary Internet Files** folder. 4. In a folder displayed in Explorer, check whether the following files exist. If they exist, delete all the files: - Director.jsp - kg.swf - KgMessage.swf - en_US_KgResource.swf - ja_JP_KgResource.swf - font_jaJP.swf • **Windows Internet Explorer 7 or 8** 1. In Microsoft Internet Explorer, select **Tools > Internet Options**. The **Internet Options** dialog box displays. 2. In the **Internet Options** dialog box, in the **General** tab,

	click **Settings** under **Browsing history**. The **Temporary Internet Files and History Settings** dialog box displays. 3. In the **Temporary Internet Files** and **History Settings** dialog box, click **View Files** in the **Temporary Internet Files**. 4. In a folder displayed in Explorer, check whether the following files exist. If they exist, delete all the files: - Director.jsp - kg.swf - KgMessage.swf - en_US_KgResource.swf - ja_JP_KgResource.swf - font_jaJP.swf
Management server replacement	When you replace the management server, follow the following steps to set up your new environment: 1. Back up your database. If you are enabling automatic backup for the Operations Logs, save the data that is stored in the "Operations log backup folder" to another location. 2. Replace the management server. If you are enabling automatic backup for Operations Logs, store the backup data that you saved in Step 1, to a folder in the new management server after replacement. 3. Install Hitachi IT Operations Director on the new management server after replacement. 4. Set up the management server. If you performed the **Quick Installation**, it is unnecessary to set up the management server. If you are enabling automatic backup for Operations Logs, specify the folder in which you stored the backup data in Step 2, for the "Operations log backup folder" field. 5. Restore the database that you backed up in Step 1. Activate your license (using the Activation Token that you already have). 6. The management server replacement is complete.

Changing the host name of the management server.	When you change the management server's host name in the following environment, complete the steps below. If you perform a Database Upgrade without completing the steps below, the Database Upgrade will fail. Environment conditions: • The management server is not cluster configuration. • The management server's host name is changed. • The software is upgraded from Hitachi IT Operations Director V3.0.0-03 or before. Steps to complete: 1. Click **Start** > **Hitachi IT Operations** > **Director Command** and execute the **stopservice** command to stop the service. 2. Open the "HiRDB.ini" file with a text editor (it is stored in the <Hitachi IT Operations Director installation folder>\mgr\db\CONF\emb folder). 3. Change the value for [PDHOST] written in the "HiRDB.ini" file as follows: [Before change] PDHOST=<host name> [After change] PDHOST=127.0.0.1 4. Execute the **startservice** command in **Director Command** and start the service.
Installation environment.	The management sever does not support Terminal Server. Network Access Control cannot be enabled on a Terminal Server.

IT Operations Director Usage Precautions

1. When you turn on pop-up blocker in a Web browser, then any pop-up window in IT Operations Director might not launch. To work around this problem, add the address of IT Operations Director to **Allowed sites** in **Pop-up Blocker Settings** dialog box of a Web browser. The following steps describe how to set **Pop-up Blocker Settings** in **Microsoft Internet Explorer**.
    i. In **Microsoft Internet Explorer**, select **Tools** – **Internet Options.**
    ii. In **Internet Options** dialog box, select **Privacy** tab and click **Settings** button to display **Pop-up Blocker Settings** dialog box.
    iii. In the **Pop-up Blocker Settings** dialog, enter a host name or IP address (of the machine on which IT Operations Director is installed) in the text field of **Address of Web site to allow.** Then, click **Add**.

2. Do not log in twice into IT Operations Director at the same time from the same client PC (desktop). Otherwise, this attempt to log in twice might disable one of the sessions with IT Operations Director.
3. IT Operations Director does not support **Back** and **Refresh** button of a browser. To move back/forward and to refresh the screen, use the relevant button of IT Operations Director.
4. You cannot execute **Power ON** using Intel AMT in the following environments because AMT does not work.
    i. When LAN and wireless LAN are connected to the same subnet.
    ii. When PC is stopped in the wireless LAN environment.
    iii. When PC on battery power is stopped.
5. IT Operations Director Agent and Agentless computers (with Windows 7/Windows Server 2008 R2) cannot collect information about the free space, capacity and file system of the drive in which **BitLocker Drive Encryption** is enabled.
6. IT Operations Director Agent and Agentless computers (with Windows 7) cannot collect information about the software that is installed by Windows XP Mode.
7. IT Operations Director Agent (with Windows 7) cannot block software activation that is installed by Windows XP Mode, restrict external device usage, restrict printing, and acquire operations logs under Windows XP mode.
8. While using an agent computer with Windows 7/Windows Server 2008 R2, the agent icon is always hidden in the task tray and it is visible only while displaying a balloon hint. Specify **Show icon and notifications** while customizing the taskbar display for the IT Operations Director Agent icon.
9. When you enable or disable **Operations Logs** or change the settings of **External Device Restriction** in a security policy, please reboot the computer where the IT Operations Director Agent is installed. Otherwise, the changed settings may not be effective, and Operations Logs may not be collected when **Operations Logs** are changed to "Enabled," and the change of **External Device Restriction** settings may not become effective.
10. In an agent computer with OS x64 and VMware Server installed, if you enable **Operations Logs**, then the guest operating system of the VMware Server may not run. To avoid such a situation, do not enable **Operations Logs**.
11. When Operations Logs or Printing Restrictions in Other Access Restrictions are enabled in a security policy on an agent-installed computer, you might not be able to access another computer by host name from Windows Explorer.

This problem occurs when all of the following conditions are met:

1. Operations Logs or Printing Restrictions in Other Access Restrictions are enabled in a security policy.
2. The operations were logged on a computer on which an IT Operations Director Agent is installed.
3. Both computers (access source and destination) are Windows Vista or later.
4. A shared printer is already registered to the access source computer.

Perform one of these procedures to avoid the problem:

- Access the destination computer by IP address rather than host name.
- Reduce the number of the shared printers registered on the access source computer.
- Remove the shared printers registered on the access source computer.
- Register the credentials (user names and password) of the destination computer to the Credential Manager in Windows.

12. The color of each item in the legend might not be displayed when you print out reports.

13. When you uninstall and then re-install Hitachi IT Operations Director before your trial license's expiration date, the IT Operations Director Service and the IT Operations Director Agent Control service won't start. To start the services, execute the **startservice** command after installation.
14. When you enable and disable Network Access Control for the same device repeatedly within a short period of time, enabling Network Access Control might fail. If this happens, wait a few minutes and try to enable Network Access Control again.
15. In **Hardware Assets** > **USB Device** > **File List** tab, the file information might be incorrectly displayed when the USB device meets any of the following conditions:

    1. File system is encrypted.
    2. File system is password protected.
    3. There is a floppy disk drive or optical disk drive.
16. The **getlogs** command uses a folder that is set for the user environment variables TEMP, as a temporary folder. If the **KDEX4041-E** message is triggered when you execute the **getlogs** command, make sure that there is enough space in this folder.
17. The application error **netsh.exe** might occur in a device in which Network Access Control is enabled when all of the following conditions are met:
    1. **Network Access Control** is enabled for the device from the management console.
    2. The operating system of the device in which Network Access Control is enabled is Windows XP (Service Pack 2 or before).
    3. The Windows Update (KB843048) is not applied to the device in which **Network Access Control** is enabled.

    If this symptom occurs, install the Windows update (KB843048) or Windows XP Service Pack 3.
18. When the Root Certificate of an agent-installed computer is not the latest, an error (**Event source: crypt32, Event ID: 8**) might be triggered to that computer's event logs. To resolve this, take either of the following actions:
    - Enable communication from an agent-installed computer to Microsoft Corporation's Windows Update Web site.
    - Disable the automatic update of Root Certificates of trusted root certificate authorities (for directions, see Microsoft Corporation's Web site).
19. The screen might flicker or just not display during installation of Hitachi IT Operations Director Agent.
20. During an agent uninstallation, the progress bar might not show any progress (or it might take a long time for a restart confirmation dialog box to display) after the 0% progress is displayed. However, do not restart or shutdown the computer during this time; wait until the Hitachi IT Operations Director Agent dialog box is displayed.

21. When you duplicate (using VMWare or hard disk copy) an agent-installed virtual environment or an agent-installed master computer's environment, be sure to execute the following command **with administrator permission** on the master computer before duplicating:
    <Hitachi IT Operations Director Agent Installation Folder>\bin\resetnid.vbs /nodeid

22. When you upgrade Hitachi IT Operations Director to 3.0.0, the following symptom might occur:
    - It takes time to display the **Security Policy Settings** dialog box or the **Server Busy** message is displayed, when you access the **View Policy** menu.
    - The Server Busy message is displayed when you take any action selecting more than 10,000 updates in the **Update List** window.
    - When scrolling down the Update List, the "Unexpected error occurred while accessing database" message is triggered.

    Conditions

    This problem occurs when all of the following conditions are met:

    i. With Hitachi IT Operations Director 2.5.0, certain Windows updates are set as **Excluded** or **Mandatory** in a security policy.*

    ii. Hitachi IT Operations Director 2.5.0 is upgraded to Hitachi IT Operations Director 3.0.0.

    * Whether this problem occurs depends on the performance of the PC on which Hitachi IT Operations Director is installed. However, it occurs when approximately more than 100 Windows updates are set as **Excluded** or **Mandatory**.

Workaround

Use either of the following methods as a workaround:

Workaround 1: This method prevents this symptom from occurring.

Perform the following steps before and after upgrading Hitachi IT Operations Director to 3.0.0:

i. Before upgrading Hitachi IT Operations Director to 3.0.0, cancel the selection of the **Excluded** or **Mandatory** for all of the security policies.
ii. Upgrade Hitachi IT Operations Director to 3.0.0.
iii. After the upgrade, set **Excluded** or **Mandatory** updates for Windows updates again in each security policy.
    a. In the **Security** tab, create an Update Group with any name.
    b. Add the **Excluded** or **Mandatory** updates to the Update Group that you created in (a).
    c. Edit a security policy and select the Update Group for **Excluded Update Group** or **Mandatory Update Group**.
    d. Perform steps **a-c** for all security policies.

Workaround 2: This method works around the symptom once it has already occurred.

Perform the following steps after upgrading Hitachi IT Operations Director to 3.0.0:

i. Upgrade Hitachi IT Operations Director to 3.0.0.
ii. When the symptom occurs, perform **Step iii**.
iii. Set **Excluded** or **Mandatory** updates for Windows updates again in the security policy.
    a. In the **Security** tab > **Windows Update** > **Update Group** > and choose a certain group. Choose **Action** > **Remove Windows Update** and remove all the updates that belong to the selected update group.*
    b. In the Update List, add **Excluded** or **Mandatory** updates again to the update group of (a).
    c. Perform steps **a** and **b** for all update groups.

*** Precaution for removing update programs**

- Remove less than 1,000 updates at one time.
- Depending on the performance of the PC, it takes approximately ten minutes to delete 1,000 updates.
- An error might occur when you attempt to remove too many updates at one time.

23. When you operate the following steps in Internet Explorer 9, an internal error may occur or you cannot continue working within the management console:

    1. Click Browse in the following wizard screen and open the file selection dialog box:

        - Import Assets
        - Install Software
        - File Distribution

    2. Then, work within the management console of IT Operations Director keeping the file selection dialog box opened.

        Note: Be sure to close the file selection dialog box before working within the management console of IT Operations Director.

24. When you close the window by clicking the Close button from the Web browser in Internet Explorer 9, the following error message might appear in the Web browser and subsequently launch the login screen again, "A problem with this webpage caused Internet Explorer to close and reopen the tab." To avoid this, do not close the window while opening the following windows:
    - The Getting Started Wizard.
    - Import Assets.
    - Install Software.
    - File Distribution.
    - Uninstall Software.
    - The window opened by "Restore Archived Logs."
    - The window opened by "Remote Control."
    - The window opened by "Export."
    - The preview screen in "Send User Notification."
    - The window opened by "Open new window" in the Reports module.
    - The Help window.

25. There might be a discrepancy between the number of suspicious operations (each day) displayed in the **Security** > **Suspicious Operations** panel and the number of suspicious operations displayed in the **Operations Log List** (which is accessed from the anchor). In this case, cross-check the suspicious operations of that day by viewing the **Events** module, and check the Operations Logs of each corresponding computer (the operation source) in the **Operations Log List** or check the Operations Logs before and after that day in the Operations Log List.

    This problem occurs in any of the following cases:

    - There is a time lag in sending suspicious operations notifications to the management server from the agent. Time lags can occur due to an agent-installed computer shutting down or due to network connection problems.

    - The system clocks on the agent-installed computer and the management server don't coincide. Operations Logs might be recognized as occurring before or after the date that notification can be sent to the management server.

    - Operations Logs are enabled, but the Operations Logs for that day are not restored.

26. While opening multiple tabs in a module (for example, the **Security, Assets, Inventory, Distribution, Event, Reports** or **Settings** module), if you successively perform the operations of changing a tab and clicking Refresh, either of the following screens messages might appear:

    - A blank list is displayed.
    - The "Unhealthy request" error message is displayed.

    If this occurs, close the corresponding tab and open it again.

27. When performing Discovery from IP Address Range, if the information for identifying the device cannot be collected, the message, "SNMP: NG (No Credential)" might display for that device.

28. When performing Discovery from IP Address Range and the discovery includes a loopback and broadcast addresses, the loopback and broadcast addresses might be discovered even they shouldn't be. To avoid this, exclude loopback addresses and broadcast addresses from the discovery range.

29. Special network devices that are Linux-based, such as BIG-IP, might be discovered as servers (Linux). After checking the **Device Details** of the discovered device, you can change the device type if needed.

30. When **Restrict Reading/Writing for USB Device** is enabled in a security policy, the device might be detected more than once by the operating system if USB device restriction occurred after the device has already been detected, causing the restriction message to appear repeatedly. To resolve this, disconnect the (restricted) USB device from the machine.

31. When Operations Logs are enabled and a computer's Power ON is specified as a target operation to be logged, the Operations Logs of a computer's power ON will be collected at the time of agent overwrite installation.

32. The Autoplay feature of any removable and permanent drive is disabled if the USB device reading and writing restriction is enabled in a security policy. In addition, the settings of the Autoplay feature won't be changed even if the USB device reading and writing restriction is disabled in a security policy or if an agent is uninstalled. The Autoplay feature of removable drive and permanent drive remain disabled.

33. The **Printer Identification Information Change** feature

    When obtaining information by SNMP, Director collects the sysName from a device as the management name (: host name) and uses it to identify that device. Devices that do not support host names or devices in which host names are not set, are identified by their MAC address or IP address.

    If more than one device has the same sysName, Director manages them as identical devices. In such an environment, the option to collect other names for devices instead of the sysName is useful. By the following method described here, you can collect a name (which can be obtained by name resolution such as NETBIOS, DNS and hosts) or MAC address or IP address, as a host name.

    The following describes how to apply this feature and the related usage precautions.

    Note: The feature does not apply to the Active Directory discovery feature. This feature does apply to:
    - Discovery from IP Address Range.
    - Periodic device information collecting for agentless devices.
    - Latest device information obtaining for agentless devices.

Method

In the following configuration file for customizing, add a row with the key name "Agent_LessPrHostnameSwitch". Specify "IpResolve" for the value. Save the file.

File name: jdn_manager_config.conf
Storage location: <Hitachi IT Operations Director installation folder>\mgr\conf
(By the default, it is C:\Program Files\Hitachi\Director\mgr\conf)

```
-----
#
# property
#
# Example:
# Port_Manager=31000
Agent_LessPrHostnameSwitch=IpResolve
-----
```

< Details of the "Agent_LessPrHostnameSwitch" key >
Specification of "Agent_LessPrHostnameSwitch"

Setting	Description
IpResolve	• Does not use sysName as a host name of printer. • Uses sysName as a host name of SNMP devices (excluding printer). • If sysName cannot be obtained, name resolution of IP address is tried for all SNMP devices (including printer). If name resolution is resolved, the obtained name is used as host name. If not resolved, a host name is generated based on MAC address or IP address.
Key is not set. (default)	• As normal specification (sysName is used as a host name of printer.)
Values other than IpResolve (Null character is included.)	

Options for checking whether the feature was applied

Option One: If name resolution of IP address is not resolved.

After Discovery from IP Address Range is done, check the following:

1. In the **Discovered Nodes** tab, each printer (name is MACxxxxxxxxxxx or IPnnnnnnnnnnn) has been added to the list.
2. If there is already a printer (which was already identified by sysName and was set to "Managed") in the list, a printer discovered in this discovery is identified as same as the existing printer if the discovered printer has the same MAC address or IP

address as the existing printer. At that time, its host name is changed to MACxxxxxxxxxxx or IPnnnnnnnnnnn.

Option Two: If name resolution of IP address is resolved.

After Discovery from IP Address Range is done, check the following:

1. In the **Discovered Nodes** tab, each printer (name is <name resolution result>) has been added to the list.
2. If there is already a printer (which was already identified by sysName and was set to "Managed") on the list, the existing printer remains in the list. And a printer (name is <name resolution result>) discovered in this discovery has been added. In this case, delete the device information and the asset information of the existing printer, and then set the newly discovered printer to Managed. If you want to inherit the asset information that was already set for the existing printer, change the associated device information of the existing printer asset, and then delete the unnecessary printer asset information. It is possible to check whether the assets are the same by sorting the list by MAC address or IP address.

Notes

- It is not recommended to specify any key other than Agent_LessPrHostnameSwitch in jdn_manager_config.conf.
- If you return the setting in Agent_LessPrHostnameSwitch to the default, even if multiple printers that have the same sysName are discovered, they are managed as an identical device. For this reason, if you manage devices individually, be careful not to return the settings to the default.
- This configuration file keeps the setting value even after overwrite-installation. It is unnecessary to specify the settings after upgrade installation.

34. When the date information (*) is manually registered from a management console, its "date and time" information is registered into a database, as [00:00:00] on the specified date in the management client's time zone.

    For this reason, keep in mind that the date of the previous day may display, if the management console is used in multiple time zone environments.

    Moreover, in an environment where Daylight Savings Time is used, if a date of Daylight Savings Time is registered during Standard Time (not Daylight Savings Time), the date is actually registered as the previous day's date.

Therefore, in an environment where Daylight Savings Time is used, check whether the date is reflected as you intended it to be on the management console, after you register the date information.

***** Applies to all items that display dates on the management console.

Main items are:

- [Security]: [Update List] >[Release Date].
- [Assets]: [Last Tracked Date], [Planned Date], [Contract Start Date], [Contract End Date], and [Contract date].
- [Inventory]: [Installation Date].
- [Distribution]: [Execution Schedule].
- [Settings]: [Network Filter List] > [Start Date/Time] and [End Date/Time].
- Overall management console: Date and time or a period that can be specified by a filter.

35. When **Restrict Reading/Writing for USB device** is enabled in a security policy, the feature of restricting USB devices becomes disabled temporarily on the agent-installed computer while the **Register USB Device** dialog is displayed on that computer.

36. For best performance, we recommend you use different PCs for Director's management server and management console.

    When using the same PC for the management server and management console, the performance of the management console can be affected by the management server's processing load.

37. When you attempt to enable Network Access Control on a Windows XP or Windows Server 2003 computer that is in a region where Daylight Savings Time is used, the **File version conflict** dialog box may be displayed on the computer's desktop. In that case, please click the **Yes to all** button and continue the process.

    Note: The process of enabling Network Access Control is incomplete while the dialog box is displayed on the target computer. If the Network Access Control status remains **Starting management** on the management console indefinitely, please check if the same dialog box is displayed on the target computer's desktop.

38. Do not remove a discovery range that you have already used when performing **Discovery from IP Address Range**, until there are no agentless-managed devices in that discovery range. Otherwise, deploying agents may fail. When you remove a discovery range, please add the discovery range again and perform **Discovery from IP Address Range** again and rediscover the devices.

39. When you specify SNMP for credentials and perform **Discovery from IP Address Range**, the following inventory information may be unable to be obtained from a device even if SNMP authentication succeeded in the device:

    - **System Details - Network Details** (Information about only a single network address can be obtained)
    - **System Details - Printer Details**
    - **Hardware Details - Processor Details**
    - **Hardware Details - Hard Disk Details**
    - **Hardware Details - Network Adapter Details** (Information about only a single network adapter can be obtained)
    - **Hardware Details - Keyboard Details**
    - **Hardware Details - Mouse Details**

    When you enable Network Access Control, please register all the IP addresses of such devices (The above inventory details are not obtainable) to the **Network Filter List**, specifying **Permit**. At this time, register only IP address without entering MAC address.

40. A printer that has the functionality of a router may be discovered as a Network Device. In this case, check the device information of the discovered device, and modify device type if necessary.

41. When a MAC address is obtained by SNMP during **Discovery from IP Address Range** and the MAC address is not in the valid format, an error event occurs and the device details may be unable to be obtained from the device. To avoid this, exclude such a device from the discovery range and recreate a discovery range.

42. Windows Firewall is disabled or stopped on a device where Network Access Control is enabled. If the Windows Firewall or the firewall feature from another security product is enabled, communication to a device that is specified as the **Exclusive Communication Destination for Access-Denied Devices** might be blocked. To avoid this, disable the Windows Firewall or the firewall feature by another security product.

43. The Routing and Remote Access service is used in a device on which Network Access Control is enabled. Therefore, do not disable or stop Windows Role Service named "Routing and Remote Access". Also, when you disable Network Access Control, stop the Routing and Remote Access service.

44. The print monitoring is executed on an agent computer if any of the following are enabled in a security policy:

    - In **Operations Logs** > **Target Operations to be Logged** > **File Operation/Print Operation**, **Print** is enabled.
    - In **Operations Logs** > **Suspicious Operations to be Notified**, **Large Number of Printing Jobs** is enabled.
    - In **Other Access Restrictions**, **Blocked Software** is enabled.

    As a result, if there is a network shared printer on the agent computer, it would put a load on a printer server or the network. If this problem occurs, disable the above-mentioned three settings in a security policy.

45. If you have a dialog box open for longer than 60 minutes, without clicking **OK**, a timeout will occur; if this happens, any changes made to the settings in the said windows will not be saved.

46. A maximum file size of 2GB can be registered as an attached file through the following windows:
    - **Assets > Hardware Assets > Department List** or **Location List** > **Add/Edit Hardware Asset** dialog box.
    - **Assets > Software Licenses > Software License List > Add/Edit Software License** dialog box.
    - **Assets > Contracts > Contract List > Add/Edit Contract** dialog box.

47. In **Reports > Security Diagnosis Reports > Timeframe Diagnosis > Comments**, the number of devices displayed in the **Comments** column is the TOTAL number of problematic computers that were tallied during the indicated timeframe.

48. When **Operations Logs** are enabled and when either of the following software is installed on an agent computer, Internet Explorer may terminate abnormally or a site using the software may not be displayed correctly on the agent computer:
    - Oracle JInitiator made by Oracle Corporation.
    - Java Runtime 1.3.1_02 to 1.4.0_01 made by Oracle Corporation.

    This symptom may occur when **Operations Logs** are enabled and any of the following security policies is applied to an agent computer:

        1. In the **Target Operations to be Logged,** the **[Only operations that divulge information (recommended)]** option is selected.
        2. In the **Target Operations to be Logged,** the **[Select target operations]** option is selected. In the subcategory of **[File Operation/Print Operation],** any of the following items are selected:

- [Upload File]
- [Download File]
- [Send File]
- [Receive File]
- [Send Mail (Attachment File)]
- [Receive Mail (Attachment File)]

3. In the **Suspicious Operations to be Notified**, any of the following are selected:
   - [Send/Receive E-mail with Attachments]
   - [Use Web/FTP Server]
   - [Copy/Move the File to External Device]

   Regarding the symptom that occurs in the environment in which Oracle JInitiator or Java Runtime are installed, the problem may be caused by Oracle JInitiator or Java Runtime. If you are going to use the **Operations Logs**, we request that you consider upgrading Oracle JInitiator and Java Runtime.

49. Do not turn back the system time on all computers that configure the IT Operations Director system while you are running IT Operations Director. Otherwise, some functions which keep the order based on time might be affected.

50. When you view a Website by using Internet Explorer in an environment in which an agent and Symantec Endpoint Protection made by Symantec Corporation are installed, the CPU usage of iexplore.exe remains high. In this case, either it takes time to load the Website, or the Website is not correctly displayed.

    This symptom may occur when all of the following conditions are met:

    1. **Operation Logs** are enabled, and a security policy that meets any of the following conditions is assigned to an agent-installed machine:
       a. In the **Target Operations to be Logged**, the option **[Only operations that divulge information (recommended)]** is selected.
       b. In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any of the following are selected:
          - File Operation/Print Operation
          - Folder Operation
          - Web Access
       c. In the **Suspicious Operations to be Notified**, any of the following are selected:
          - Send/Receive E-mail with Attachments

- Use Web/FTP Server
- Copy/Move the File to External Device

2. Internet Explorer version is 9.
3. Internet Explorer Protected Mode is enabled.
4. A user with a standard user right starts Internet Explorer.
5. User Account Control (UAC) is enabled.
6. Symantec Endpoint Protection is installed on an agent-installed machine and the version is 11.
7. Symantec Endpoint Protection's File System Auto-Protect is enabled.

To work around this symptom, upgrade Symantec Endpoint Protection to version 12 or later, or assign a security policy which does not meet the Condition 1 on an agent-installed machine, and then restart the agent-installed machine.

51. To use the External Device Restriction feature of Other Access Restrictions, the service "Portable Device Enumerator Service" must be running on an agent-installed machine. If this service is not running, the operations may become unstable. For example, the use of a device is not suppressed or it continues to be suppressed.

    This symptom may occur when all of the following conditions are met:

    1. The operating system is Windows Vista or later.
    2. "Portable Device Enumerator Service" is not running.
    3. In **Security Policy > Other Access Restrictions > External Device Restriction > the Windows Vista/2008/7** tab, any of the following settings are enabled, and the security policy is (or was) applied to an agent-installed machine:
        - CD/DVD Drive > Restrict writing
        - FD Drive > Restrict reading/writing
        - Removable Disk > Restrict reading/writing

    To work around this symptom, check the Startup Type of the "Portable Device Enumerator Service". If the setting is Disabled, set it to Manual or Automatic, and then restart the agent-installed machine.

52. An agent registers the add-on for Agent in Internet Explorer in order to collect operation logs for Web access. If the add-on is set to Disable in the add-ons settings of Internet Explorer, the Web access logs cannot be obtained. In Internet Explorer 9, when an add-on is registered, a confirmation message asking whether to enable the add-on is displayed. To avoid the behavior of displaying the message, perform the following steps and then restart Internet Explorer.
    1. Log on to the agent-installed machine as a user with administrator privileges, type "gpedit.msc" in Run, and start Group Policy Editor.

2. Open the Add-on List settings in the following location:
   Local Group Policy Editor > Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Features > Add-on Management > Add-on List.
3. In the Add-on List dialog, select Enable. In the activated Options, click Display in the Add-on List.
4. Add the following settings for each operating system:
   <For Windows 7 or Windows Server 2008 R2>
   Value name: {90CA397B-DA51-47EB-9299-0B7041857FCB}
   Value: 1
   <For Windows Vista or Windows Server 2008>
   Name of item to be added: {90CA397B-DA51-47EB-9299-0B7041857FCB}
   Value of item to be added:1

If the add-on is set to Disable, perform the following steps:

1. Perform the steps as described above.
2. In Internet Explorer > Tools > Internet Options > Programs > Manage Add-ons, change the setting for Hitachi IT Operations Director Agent to Enable.

53. Surrogate pair characters are not supported. When surrogate pair characters are used, the following symptoms occur.
    1. When surrogate pair characters are entered in the management console and the entered data is registered or updated in the management console, the management console does not respond. In this case, close the management console.
    2. If the device's system information containing surrogate pair characters is updated and saved in the **Edit Device Details** dialog, then the surrogate pair characters are garbled.
    3. If Organization information that contains surrogate pair characters exceeding 256 characters (each surrogate-pair character is counted as two characters) in Active Directory is reflected into the Department information, the characters after the 256th character are truncated and are reflected into the Department information.
    4. When surrogate pair characters are included in the administrator name on a computer, the administrator information of the computer cannot be acquired from Active Directory.
    5. When surrogate pair characters are included in the name of the directory for containing the files the getlogs command will create, the error indicating that the specified output directory is invalid or not found occurs.
    6. When you attempt to display surrogate pair characters in the management console, some of the characters might appear garbled.

54. In **Inventory > Device Inventory > Device List > Installed Software Details** tab, when you clear the Show Windows Updates check box, all of the contents of the list may sometimes not be displayed. In this case, refresh the displayed information by clicking the update icon on the tab.

55. In the Windows Server 2003 environment on which an agent is installed, when the Operation Logs function is enabled, TCP/IP communications of 32-bit applications fail. Even after the operating system restarts, communications still fail. This symptom occurs when all of the following conditions are met on an agent-installed machine:
    1. The operating system is any of the following:
        - Windows Server 2003 x64 Edition with no Service Pack
        - Windows Server 2003 x64 Edition Service Pack 1
        - Windows Server 2003 R2 x64 Edition with no Service Pack
    2. **Operation Logs** are enabled, and a security policy that meets any of the following conditions is assigned to an agent-installed machine:
        (a) In the **Target Operations to be Logged**, the option **[Only operations that divulge information (recommended)]** is selected.
        (b) In the **Target Operations to be Logged**, the option **[Select target operations]** is selected, and in the **Operation Classification**, any of the following are selected:
            - Web Access (Upload)
            - Web Access (Download)
            - FTP (Send File)
            - FTP (Receive File)
            - Send Mail (Attachment File)
            - Receive Mail (Attachment File)
            - Save Attached File

        (c) In the **Suspicious Operations to be Notified**, any of the following are selected:
            - Send/Receive E-mail with Attachments
            - Use Web/FTP Server
            - Copy/Move the File to External Device

    To work around this symptom, apply the Service Pack 2 or later for the operating system to the computer, and then assign the corresponding security policy.
    When this symptom occurs, log on to the computer as a user with administrator privileges, execute the following OS command from the Command Prompt window, and then reset the Winsock catalogue to the default configuration.
    "netsh winsock reset catalog"
    Because the above mentioned command cannot be executed on the Windows Server 2003 x64 Edition with no Service Pack, install SP1 or

later on the computer and then execute the command. In addition, after you execute the above command, re-install a third-party "Winsock layered service providers" (which had been installed on the computer before the Operation Logs function was enabled).

56. The horizontal scroll bar may appear in the legend for the chart in the management window, and the contents of the legend may be blocked. To avoid this problem, change the width of the management window and then refresh the display.

57. Limit the number of system and operation administrators to 10. If multiple users perform operations in the management window simultaneously, a message might appear that prompts the user to repeat the operation or it might take time to display the view.

58. When you upgrade this product (by installing it over the previous version of this product), the Import status that was displayed in the **Background Task** panel of the **Home** module is not inherited. The Import status is updated when you perform an import after the upgrade.

59. If the version information of an executable file of the software is corrupted or inconsistent, the software may not be blocked when a user starts it, even though the file name which you registered in the **Blocked Software List** matches "the full file name" or "the original file name" of the software.

60. After you restore data, database maintenance will be performed when the management server starts. Database maintenance may take an hour or more. Therefore, operation performed in the management window may be delayed immediately after data is restored, or operation may not start at the time specified in the schedule and it may be delayed.

61. If you restore backup data while any the following operations are being performed, these operations will be performed again when the management server starts after data is restored.
    - Discovery from an IP address range
    - Active Directory discovery
    - Agent deployment
    - Update device details
      (Only when this operation is performed on an agentless computer or a device other than a computer.)
    - Distribute updates
      (Only when this operation is performed by launching the **Distribute Updates** menu on the **Windows Update** tab in **Security > Security Policy List**.)
    - Calculate Security Diagnosis Report
    - Calculate Security Detail Report

- Calculate Inventory Detail Report
- Calculate Asset Detail Report
- Restore archived logs

Therefore, operation performed in the management window may be delayed immediately after data is restored, or operation may not start at the time specified in the schedule and it may be delayed.

62. If you specify two or more judgment conditions with the same software name and version to configure the Target Software in the **Mandatory Software** settings of a security policy, the number of **[# of Not Compliant Computers]** (which is displayed in **Security Policies > Security Policy List > the Software Use** tab) may not match the actual number of computers that are not compliant with the security policy. We recommend that you do not specify judgment conditions with the same software name and version in the **Mandatory Software** settings.

63. If you specify two or more judgment conditions with the same software name and version to configure the Target Software in the **Unauthorized Software** settings of a security policy, the number of **[# of Not Compliant Computers]** (which is displayed in **Security Policies > Security Policy List > the Software Use** tab) may not match the actual number of computers that are not compliant with the security policy. We recommend that you do not specify judgment conditions with the same software name and version in the **Unauthorized Software** settings.

64. When you discover a network using Windows authentication in an environment where the discovery-target computers do not have a common account, and the discovery needs to use different credentials to discover the target computers, the account of a discovery-target computer may get locked.
    This problem occurs when all of the following conditions are met:
    1. Windows authentication is set for the discovery range.
    2. The account lockout policy is enabled on a discovery-target computer.
    3. The authentication fails with the credential information in the discovery-target computer in 2.
       This condition applies to the environment where a common account used by the discovery-target computers does not exist and the discovery needs to use different credentials to discover the target computers.
    4. The network discovery is performed.

    When you discover a network using Windows authentication for a discovery-target computer in which the account lockout policy is enabled, divide the discovery range or remove unnecessary credentials

so that the number of credentials to be used for the authentication is less than the value specified for the account lockout threshold.

65. In the management window, the number of characters in the text area where multiple lines are allowed includes a newline by treating it as two characters, in addition to the actual number of characters that a user enters.

66. In the [Send User Notification], [Deny Network Access], and [Edit Other Language Message] windows that users can enter a text, the font information is converted to the number of characters, and is added to the actual number of characters that a user enters. The estimated number of characters of font information to be added is as follows:
    - 189 characters per line
    - 7 characters per part where bold, italic, or underline is used
    - 92 characters per part where a font is changed in the middle of the line
    - 38 characters and the number of characters of URL per part where a hyperlink is used

67. If multiple administrators update the settings in the dialog box at the same time, the settings entered by an administrator who last updated is saved. The settings entered by other administrators who updated at the same time will not be saved.

68. When a failover occurs during cluster system operation, the status and result of an import are not displayed in the following windows. In this case, import items again.
    - [Home] > [Background Task]
    - [Settings] > [Assets] > [Last Import Log]

Documentation

In addition to the Help, IT Operations Director ships with the *Hitachi IT Operations Director Getting Started Guide (MK-90IOS011-01).*

This document contains pre-installation and post-installation guidelines and instructions. This is your starting point for using IT Operations Director.

Copyright and License Information

Java is a registered trademark of Oracle and/or its affiliates.

Kaspersky is a registered trademark of Kaspersky Lab in the United States.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Mac and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Microsoft is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Microsoft, and Hyper-V are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft, and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetShield and VirusScan are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries.

Norton AntiVirus is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

OfficeScan is a trademark of Trend Micro Incorporated and is registered in various jurisdictions worldwide.

Pentium is a trademark of Intel Corporation in the United States and other countries.

RSA is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries.

RealPlayer is registered trademark of RealNetworks, Inc.

ServerProtect is a trademark of Trend Micro Incorporated, registered in the U.S. and is a trademark in other countries.

Sophos Anti-Virus is a registered trademark of Sophos Plc.

Symantec is a U.S. registered trademark of Symantec Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows NT is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows Server is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows Vista is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

This product includes software developed by the Apache Software Foundation (http://www.apache.org).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by IAIK of Graz University of Technology.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/ This product includes software developed by Ralf S. Engelschall for use in the mod_ssl project (http://www.modssl.org/).

Hitachi IT Operations Director includes RSA BSAFE Cryptographic software from RSA Security Inc.

All other trademarks, service marks, and company names are properties of their respective owners.