Fujitsu Software Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V2.9.0

First Step Guide

CA92344-5429-04
March 2024

Preface

Purpose

This manual is for those using the following operation and management software for the first time. This software manages and operates ICT devices such as servers, storages, and switches as well as facility devices such as PDUs in an integrated way.

- Fujitsu Software Infrastructure Manager
- Fujitsu Software Infrastructure Manager for PRIMEFLEX (hereinafter referred to as "ISM for PRIMEFLEX")

Hereinafter, the two products above will be referred to as "ISM."

This manual describes the minimum amount of preparation and operations required for using ISM.

For a description on the use of each function, refer to the following manuals.

Product Manuals

Manual Name	Description
Fujitsu Software Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V2.9.0 First Step Guide	This manual is for those using this product for the first time. This manual summarizes the procedures for the use of this product, the product system, and licensing. In this manual, it is referred to as "First Step Guide."
Fujitsu Software Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V2.9.0 User's Guide	This manual describes the functions of this product, the installation procedure, and procedures for operation. It allows you to quickly grasp all functions and all operations of this product. In this manual, it is referred to as "User's Guide."
Fujitsu Software Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V2.9.0 Operating Procedures	This manual describes the installation procedure and usages for the operations of this product. In this manual, it is referred to as "Operating Procedures."
Fujitsu Software Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V2.9.0 Glossary	This document defines the terms that you need to understand in order to use this product. In this manual, it is referred to as "Glossary."

Intended Readers

This manual is intended for readers who are using ISM for the first time. To read this manual, you must know the following.

- An understanding of how to use hardware
- An understanding of how to use OSes
- An understanding of networks

Notation in this Manual

Notation

Keyboard

Keystrokes that represent nonprintable characters are displayed as key icons such as [Enter] or [F1]. For example, [Enter] means press the key labeled "Enter." [Ctrl]+[B] means hold down the key labeled "Ctrl" or "Control" and then press the B key.

Symbols

Items that require particular attention are indicated by the following symbols.

Point

Describes the content of an important point.

Note

Describes an item that requires your attention.

Variables: <xxx>

Represents variables that require replacement by numerical values or text strings in accordance with your usage environment.

Example: <IP address>

Using PDF applications (Adobe Reader, etc.)

Depending on the specifications of the PDF application you are using, issues (extra spaces and line breaks, missing spaces, line breaks, and hyphens in line breaks) may occur when you perform the following operations.

- Saving to a text file
- Copying and pasting text

High Risk Activity

The Customer acknowledges and agrees that the Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. The Customer shall not use the Product without securing the sufficient safety required for the High Safety Required Use. In addition, Fujitsu (or other affiliate's name) shall not be liable against the Customer and/or any third party for any claims or damages arising in connection with the High Safety Required Use of the Product.

To Use This Product Safely

This document contains important information required for using this product safely and correctly. Read this manual carefully before using the product. In addition, to use the product safely, the customer must understand the related products (hardware and software) before using the product. Be sure to use the product by following the precautions on the related products. Be sure to keep this manual in a safe and convenient location for quick reference during use of the product.

Modifications

The customer may not modify this software or perform reverse engineering through decompiling or disassembly.

Disclaimers

Fujitsu Limited assumes no responsibility for any claims for losses, damages or other liabilities arising from the use of this product. The contents of this document are subject to change without notice.

Trademarks

Copyright

Modification History

Edition	Issue Date	Modification Overview	Section	
01	September 2023	First edition	-	-
02	December 2023 Major reorganization of the manual or modification of contents	Added precaution for Power Capping	1.2 Product System and Licenses	Note for Table: "Supported functions for each Operation Mode"
		Modified description due to changes in ISM Backup/Restore specifications	2.1.1 Design the ISM Installation Environment	Operation Modes and the range of estimated disk resources
			3.2 Backing up ISM-VA	-
		Added supported versions of ServerView Suite Update DVD	2.5.1 Prepare Firmware Data for a Firmware Update	Firmware data to be prepared (When updating PRIMERGY)
		Modified description of MIB handling	3.1.3 Set up an MIB File	-
03	January 2024 Major reorganization of the manual or modification of contents	Modified the configuration and descriptions on Backup/ Restoration of ISM	3.1.1 Apply Patches to ISM-VA	"Note"
			3.1.2 Upgrade ISM-VA	"Note"
			3.2 Backup and Restoration of ISM	-
04	March 2024 Modification for ISM 2.9.0.020 patch application	Changed images due to support for displaying the power status on the node list screen	1.1.1 Optimizing Operations Through the Integrated Management of Infrastructure Operations (Node Management)	Figure "Displaying a node list"
			2.2 Logging in to the ISM Graphical User Interface and Screen Layout	Screen layout and main name
			2.3.2 Manage Nodes	Step 2
			2.4.1 Monitor the Changes in Node Statuses	Step 3
			2.4.2 Monitor CPU/Memory Availability and Temperature	Step 2
	March 2024 Major reorganization of the	Added "power status" in the default monitoring items when a node is registered	2.4 Procedures for Using Monitoring	Table "Default monitoring items for when a node is registered"

Edition	Issue Date	Modification Overview	Section	
	manual or modification of contents			

Contents

Chapter 1 Overview....1
1.1 Operation Modes and Functions....1
1.1.1 Optimizing Operations Through the Integrated Management of Infrastructure Operations (Node Management)....2
1.1.2 Integrated Monitoring for the Status of Multiple Nodes (Monitoring)....2
1.1.3 Simplification of Firmware Updates (Firmware Management)....4
1.1.4 Copying and Applying Settings to Multiple Nodes (Profile Management)....5
1.1.5 Displaying a Network Map (Network Management)....6
1.1.6 Automation and Integrated Management of Logs (Log Management)....8
1.1.7 Managing a Virtual Platform (Virtualized Platform Expansion)....9
1.2 Product System and Licenses....10

Chapter 2 Required Preparations and Procedures for Using ISM....14
2.1 ISM Installation Workflow....14
2.1.1 Design the ISM Installation Environment....15
2.1.2 Install ISM-VA....16
2.1.3 Set up the ISM-VA Environment....18
2.1.4 Register Licenses....20
2.1.5 Register Users....21
2.1.6 Allocate Virtual Disks....21
2.2 Logging in to the ISM Graphical User Interface and Screen Layout....22
2.3 Procedures for Using Node Management....25
2.3.1 Register Nodes....25
2.3.2 Manage Nodes....27
2.4 Procedures for Using Monitoring....29
2.4.1 Monitor the Changes in Node Statuses....30
2.4.2 Monitor CPU/Memory Availability and Temperature....32
2.4.3 Notify Monitoring Statuses....34
2.4.3.1 Set up a mail server (SMTP server)....35
2.4.3.2 Set mail notification as the alarm notification method (Action)....35
2.4.3.3 Set alarm notification methods and notification targets (Alarm Settings)....38
2.5 Procedures for Using Firmware Management....42
2.5.1 Prepare Firmware Data for a Firmware Update....43
2.5.2 Import Firmware Data into ISM....44
2.5.3 Update Firmware....45

Chapter 3 Maintaining ISM....49
3.1 Update ISM....49
3.1.1 Apply Patches to ISM-VA....49
3.1.2 Upgrade ISM-VA....55
3.1.3 Set up an MIB File....56
3.2 Backup and Restoration of ISM....57
3.3 Collection of Maintenance Data....58
3.3.1 Collect Maintenance Data with the GUI....58
3.3.2 Collect Maintenance Data Using a Command....61
3.3.3 Collect Maintenance Data for Virtual Resource Management....62

Chapter 1 Overview

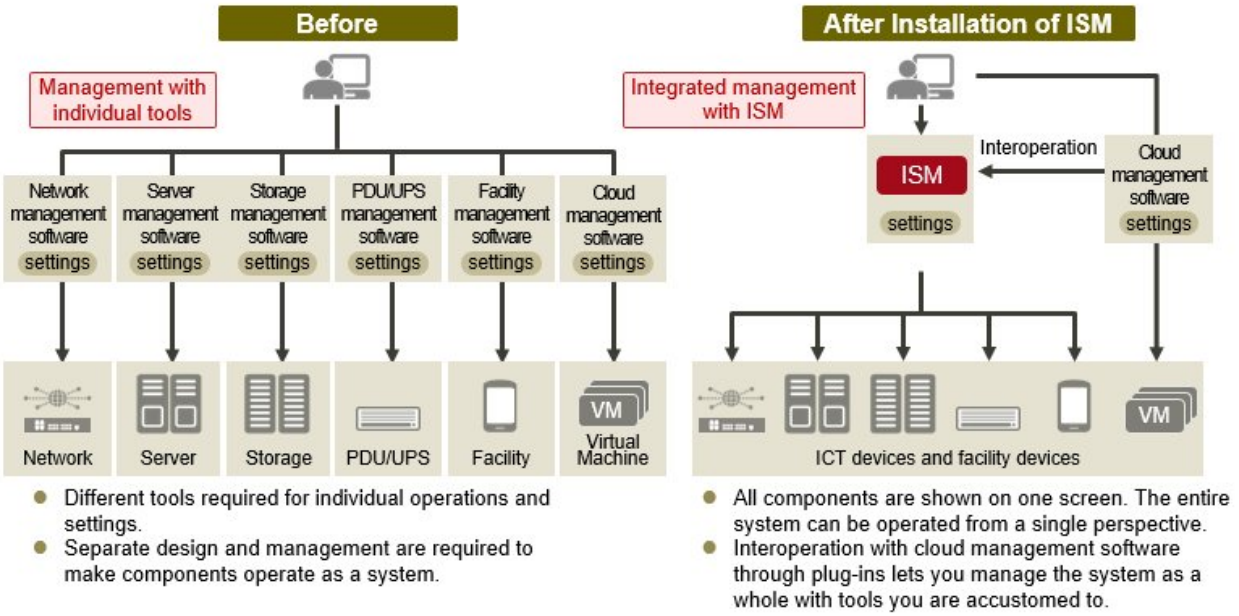
ISM is a software package that manages and operates ICT devices such as servers and storages, as well as facility devices in an integrated way.

This chapter describes the functions that can be used with each license as well as the functions that can be used in different ISM Operation Modes.

Purpose of ISM

By installing ISM, multiple and various types of ICT devices can be managed in an integrated way. With this software, you can monitor the status of all the ICT devices in a data center or a machine room. You can also execute batch firmware updates for multiple devices and configure servers automatically. It can reduce costs of operation management and increase the operation quality.

Figure 1.1 Integrated operation and management through installation of ISM



1.1 Operation Modes and Functions

This section describes an overview of the ISM functions for each Operation Mode.

ISM Operation Modes

ISM can be used in three different modes depending on how you want to use the software. In this manual, these modes are referred to as "Operation Modes."

An icon is displayed for the corresponding mode in the description for each function. The icons that correspond to each mode are as follows.

Operation Mode	Icon	Description
Essential mode	Essential	Can be used for monitoring the status of servers, storages, and switches as well as firmware management.
Advanced mode	Advanced	Can be used for the management, operation, and maintenance of servers, storages, switches, and other facility devices, in addition to the functions that can be used in Essential mode.
Advanced for PRIMEFLEX mode	Advanced for PRIMEFLEX	Can be used for the creation, expansion, management, and maintenance of clusters for virtual platforms, in addition to the functions that can be used in Advanced mode.

Operation Mode	Icon	Description
		Power Capping cannot be used in Advanced for PRIMEFLEX mode.

The Operation Mode is determined by the products that are purchased (media and licenses). For details on products, modes, and the difference between modes, refer to "1.2 Product System and Licenses."

1.1.1 Optimizing Operations Through the Integrated Management of Infrastructure Operations (Node Management)

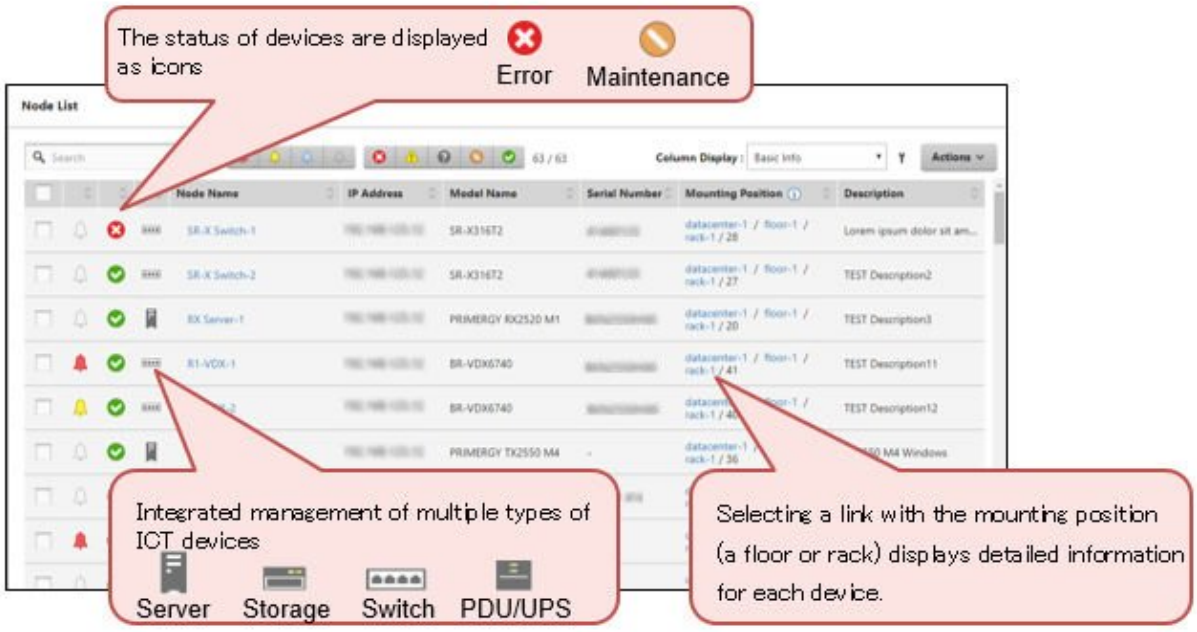
Essential Advanced Advanced for PRIMEFLEX

ICT and facility devices that are operated and managed in an ISM environment are called "nodes."

With ISM, you can register a batch of nodes to be managed by specifying and discovering nodes that are connected to a network by using an IP address range. This will allow you to make node registration work more efficient.

You can manage node information (node names, serial numbers, IP addresses, etc.) in the same format for any type of node after a node is registered (Figure 1.2 Displaying a node list).

Figure 1.2 Displaying a node list



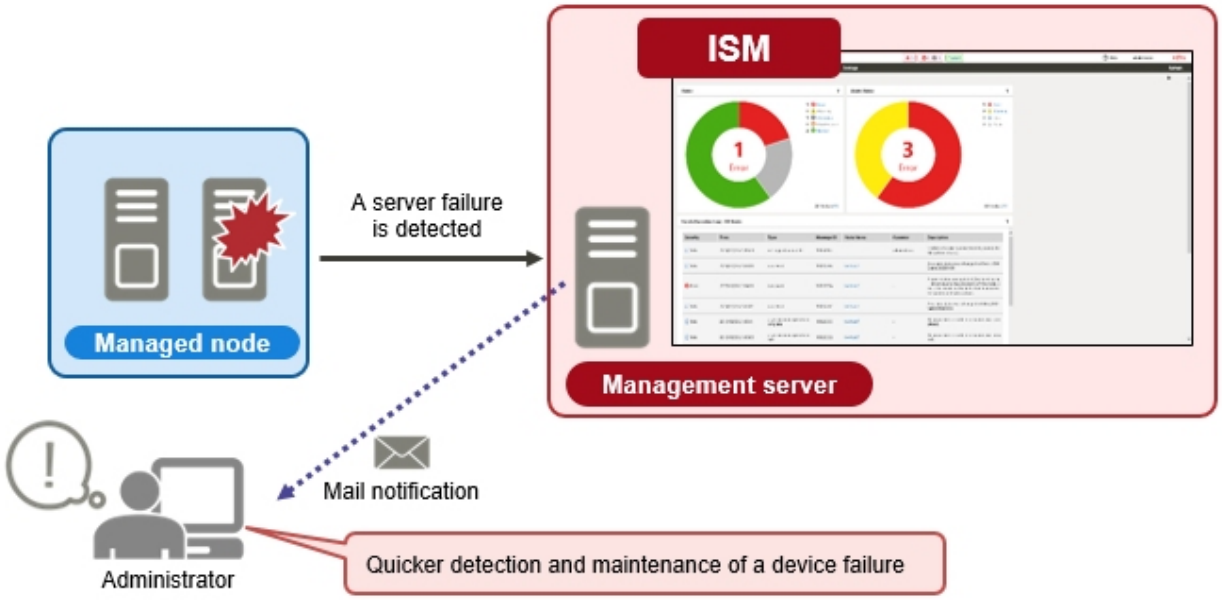
1.1.2 Integrated Monitoring for the Status of Multiple Nodes (Monitoring)

Essential Advanced Advanced for PRIMEFLEX

With ISM, you can monitor the power status, the availability of CPU, memory, and disk space, intake temperature, as well as events (SNMP traps) due to failures at the same time for all registered nodes.

You can send mail to an administrator when an event has occurred such as a device failure. It is also possible to perform other operations in addition to sending mail such as sending/forwarding SNMP traps, sending logs to Syslog servers, and automatic execution of scripts. By using these functions, you can handle events quickly and minimize time-outs.

Figure 1.3 Image of Monitoring



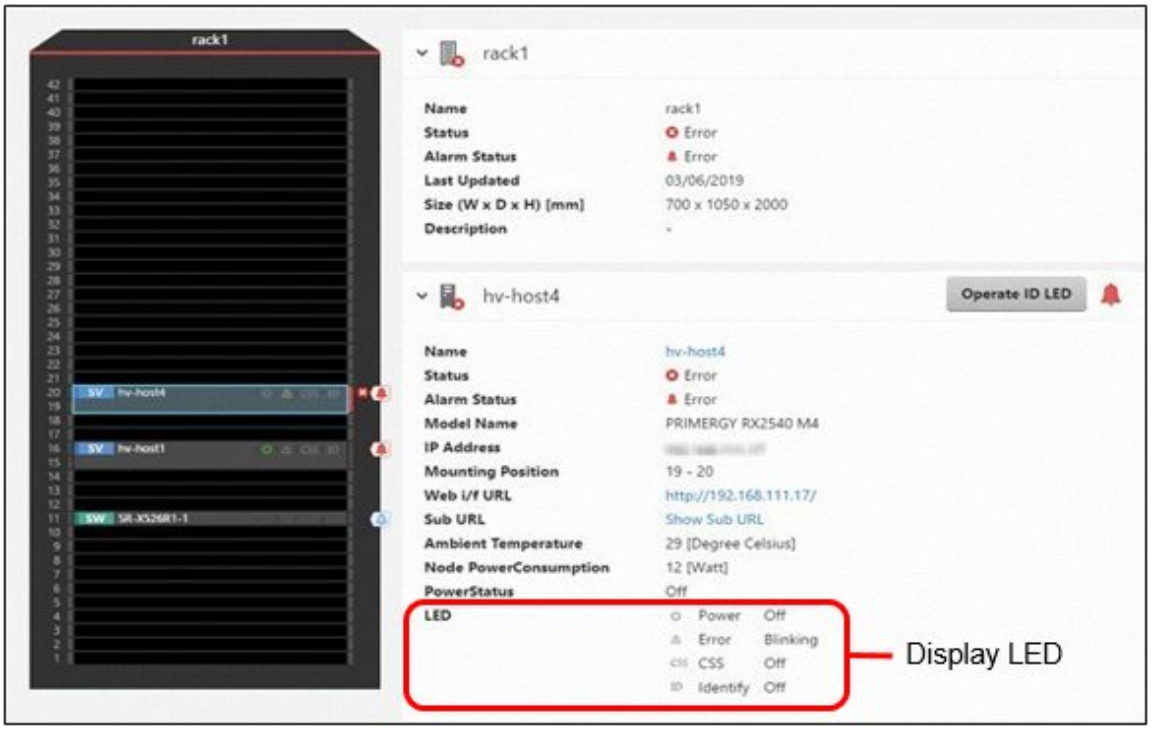
Displaying the mounting position in a rack

Advanced | Advanced for PRIMEFLEX

In Advanced mode and Advanced for PRIMEFLEX mode, you can display the status of devices mounted on a server rack on the screen.

There are some devices that have LEDs that display the status on the front of the device and this can also be displayed on a screen in ISM. By using this function, you can locate the position of a device that is failing in a rack as if you were standing in front of the server rack (Figure 1.4 Displaying the mounting position in a rack).

Figure 1.4 Displaying the mounting position in a rack

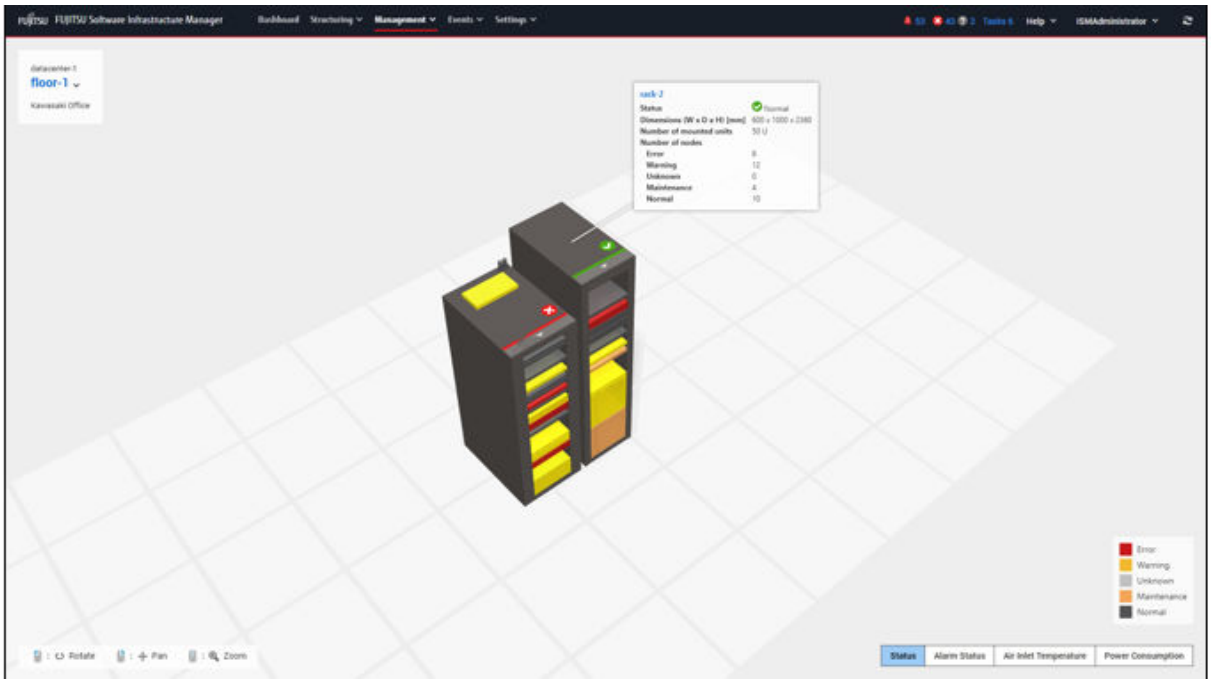


Displaying 3D view

Advanced | Advanced for PRIMEFLEX

In Advanced mode and Advanced for PRIMEFLEX mode, the overall status of data centers and server rooms can be viewed similar to that of server racks on a screen in ISM (Figure 1.5 Displaying 3D view). You can confirm information on the operation of devices, SNMP traps being received, the severity of detected events, intake temperature, and power consumption on the same screen in ISM. By using this function, you can grasp the relationship between the status and position of devices.

Figure 1.5 Displaying 3D view



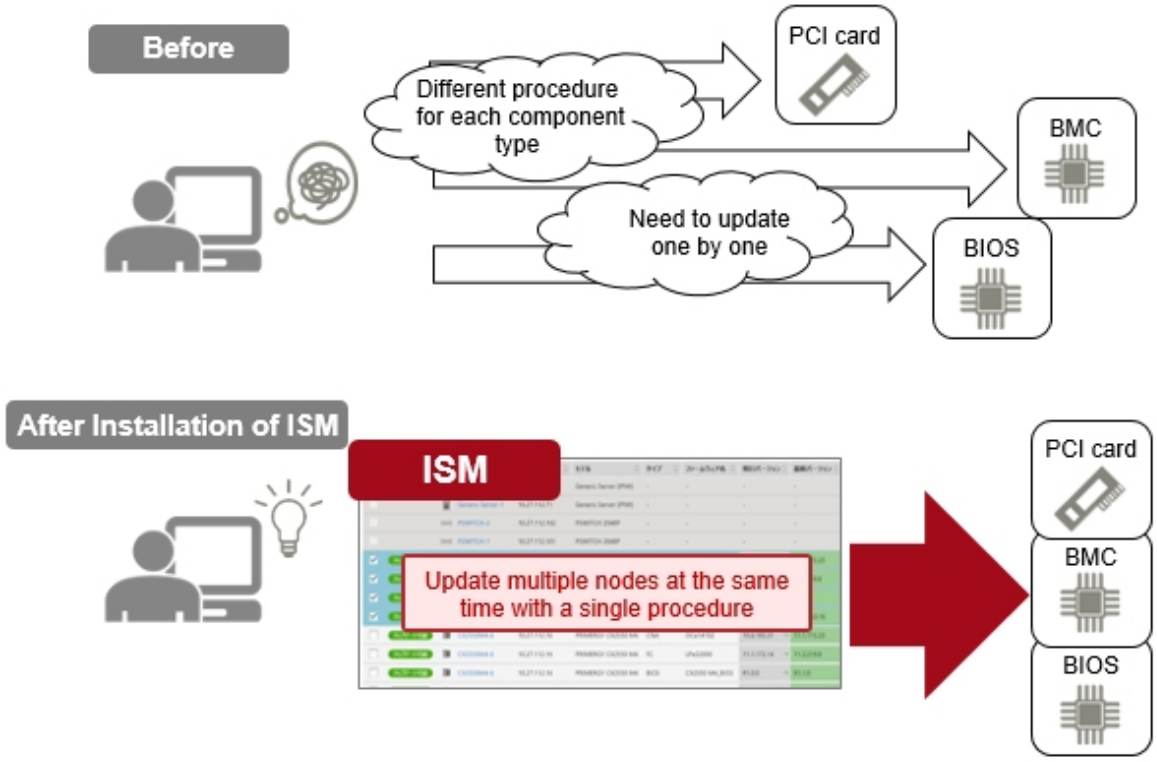
1.1.3 Simplification of Firmware Updates (Firmware Management)

Essential | Advanced | Advanced for PRIMEFLEX

In ISM, you can confirm the firmware version of multiple nodes on one management screen regardless of the type of device.

You can also update the firmware for multiple nodes and components that needed to be updated individually in the past, and you can update the firmware for these at the same time.

Figure 1.6 Image of Firmware Management



1.1.4 Copying and Applying Settings to Multiple Nodes (Profile Management)

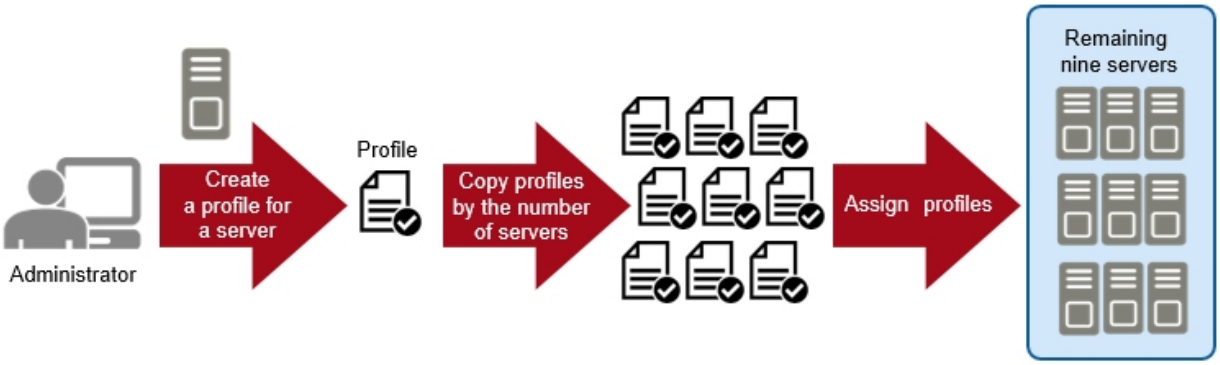
Advanced | Advanced for PRIMEFLEX

In ISM, you can set up (settings for installing a device, OS installation, and make registrations to management software) a series of devices to start operations.

In this type of setup, settings are organized into a settings file and saved as a "profile," and then the "profile" is assigned to the devices. You can copy and reuse this profile on multiple devices.

For example, if you must apply the same settings to 10 new devices, you can apply the settings to the remaining nine devices (Figure 1.7 Example of applying the same settings to multiple devices) by creating only one profile.

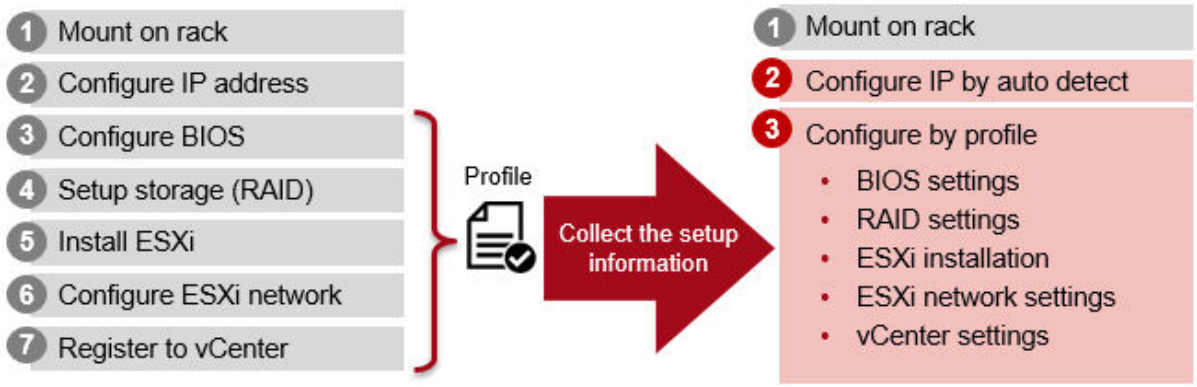
Figure 1.7 Example of applying the same settings to multiple devices



It is also possible to change part of a profile when you must have different settings for different devices.

You can also save parameters as profiles when installing OSes on servers.

Figure 1.8 Example of deploying VMware ESXi servers



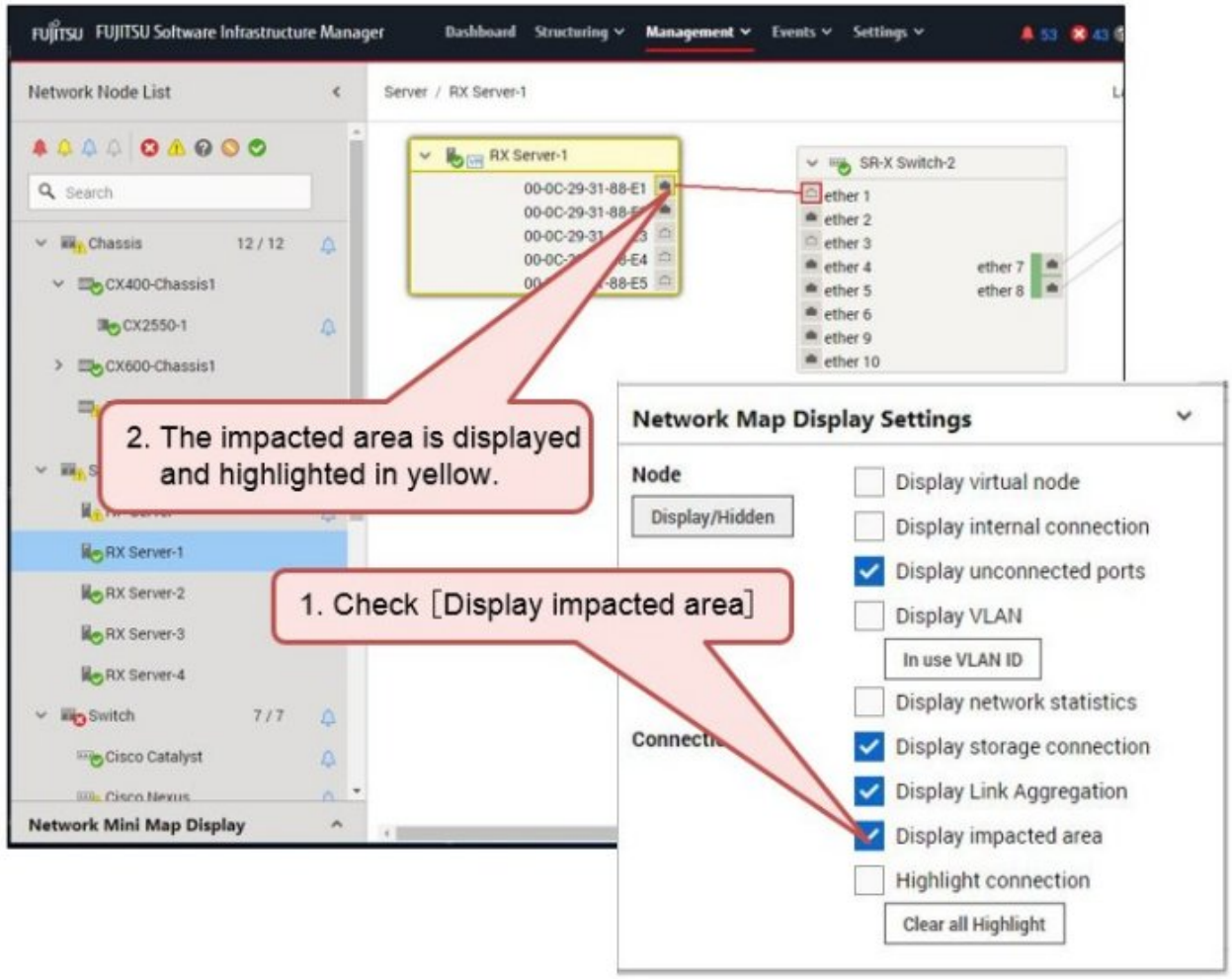
1.1.5 Displaying a Network Map (Network Management)

Advanced | Advanced for PRIMEFLEX

In ISM, you can graphically display virtual network connections (network maps) in addition to physical connections. By using this function, you can easily see the influence of a stopped device or virtual server.

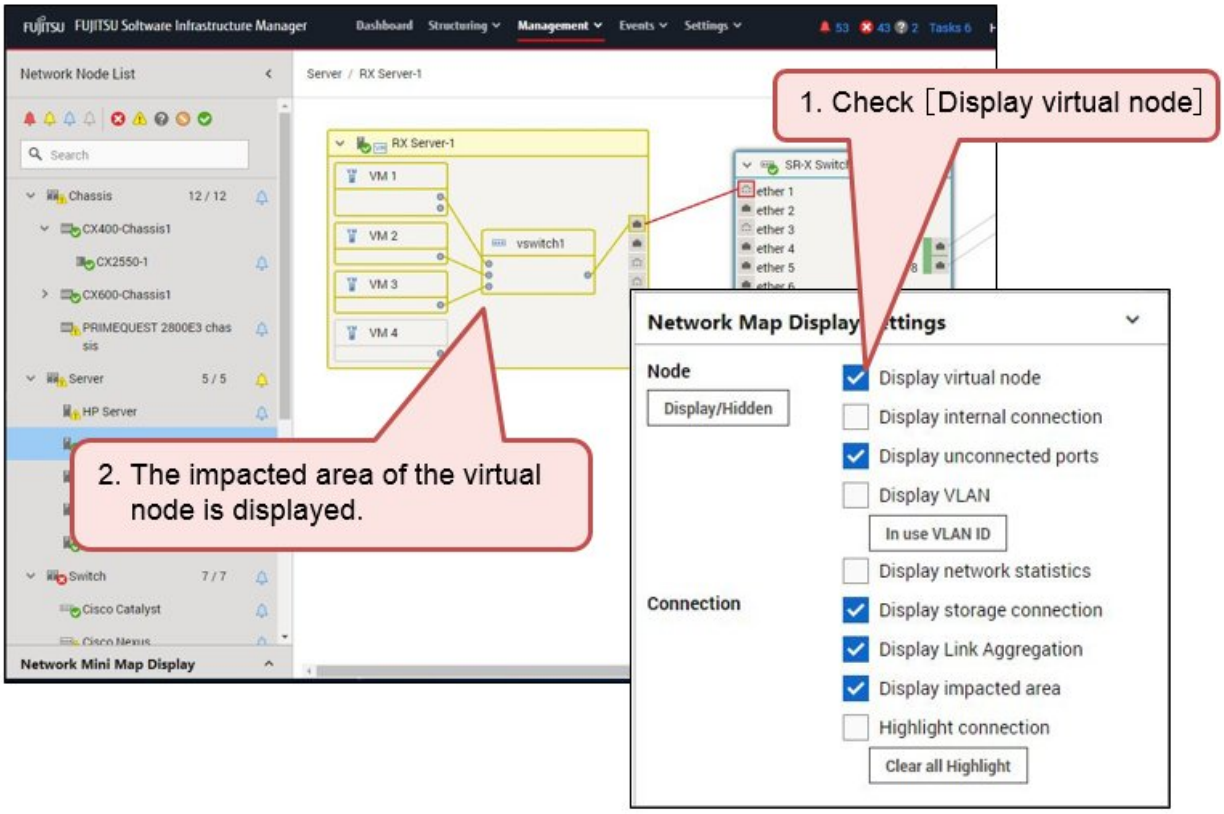
You can confirm the impacted area which is highlighted in yellow when you select the [Display impacted area] checkbox on a network map (Figure 1.9 Image of physical connections on a Network Map).

Figure 1.9 Image of physical connections on a Network Map



You can also confirm the impacted area for virtual machines, virtual switches, virtual routers, and CNA ports when you select the [Display virtual node] checkbox (Figure 1.10 Image of virtual nodes displayed on a Network Map).

Figure 1.10 Image of virtual nodes displayed on a Network Map

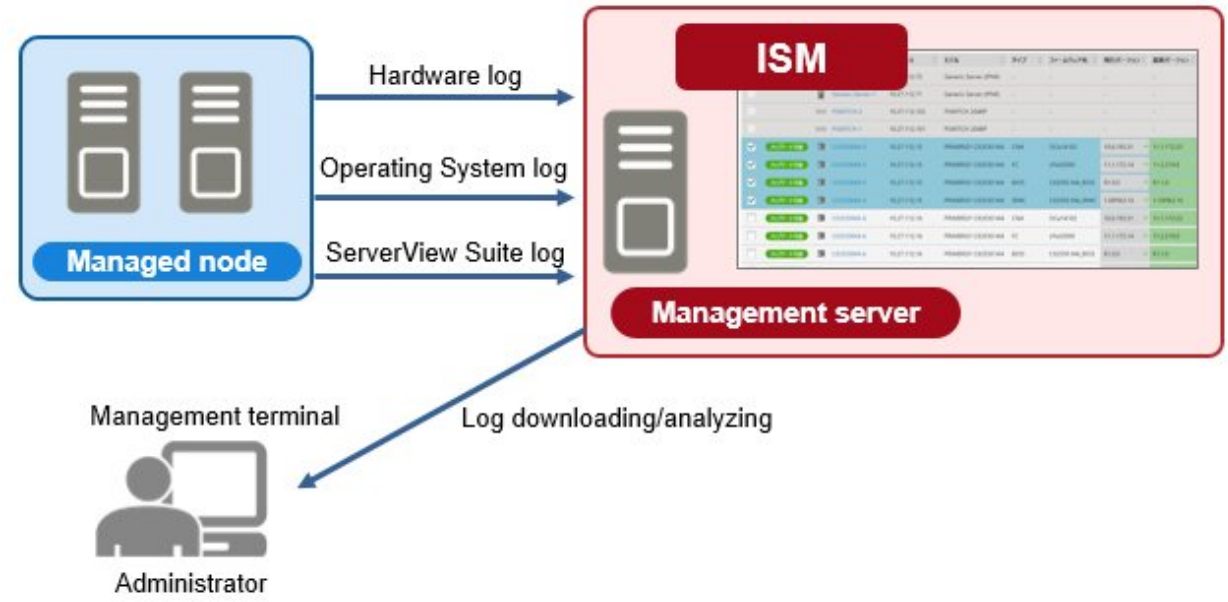


1.1.6 Automation and Integrated Management of Logs (Log Management)

Advanced | Advanced for PRIMEFLEX

With ISM, you can collect different types of logs (hardware logs, operating system logs, and ServerView Suite logs) for managed nodes at the same time and collect logs automatically according to a specified schedule. You can manage different types of logs in an integrated manner and generation management for retained logs is more efficient. You can also search by keywords in logs for assistance in investigations when an error has occurred on a managed node.

Figure 1.11 Image of Log Management



1.1.7 Managing a Virtual Platform (Virtualized Platform Expansion)

Advanced for PRIMEFLEX

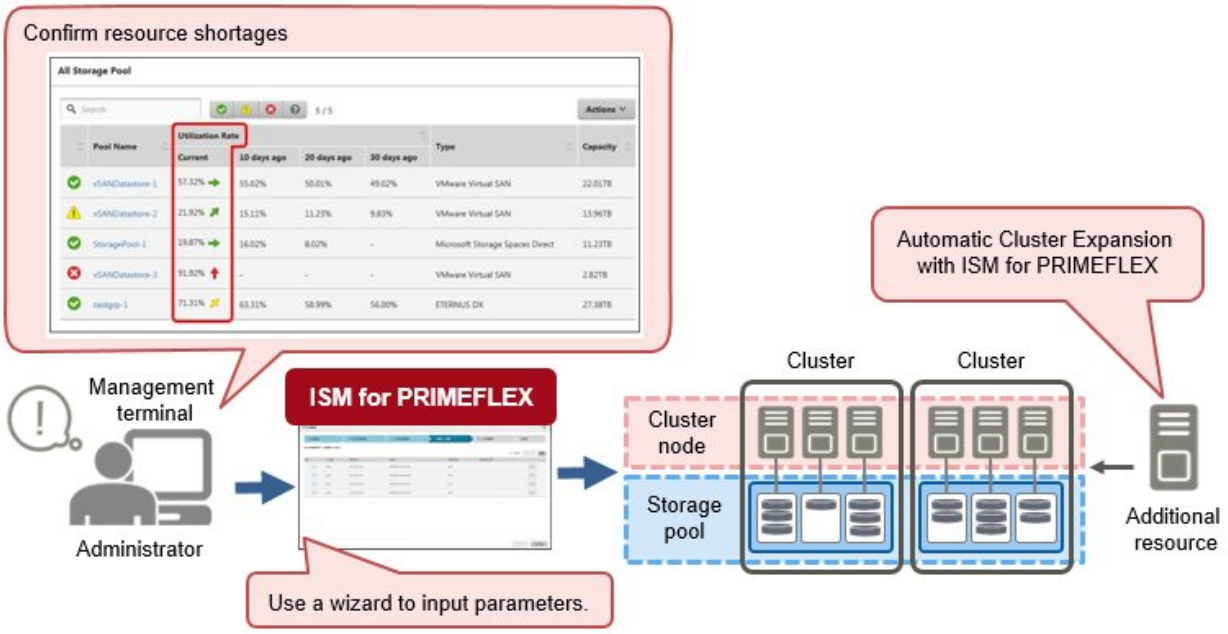
ISM for PRIMEFLEX is included in the four following Fujitsu Integrated System PRIMEFLEX products:

- PRIMEFLEX HS
- PRIMEFLEX for VMware vSAN
- PRIMEFLEX for Microsoft Storage Spaces Direct
- PRIMEFLEX for Microsoft Azure Stack HCI

With ISM for PRIMEFLEX, it is easy to expand the resources for a cluster that has been configured in a virtual storage environment (Software Defined Storage).

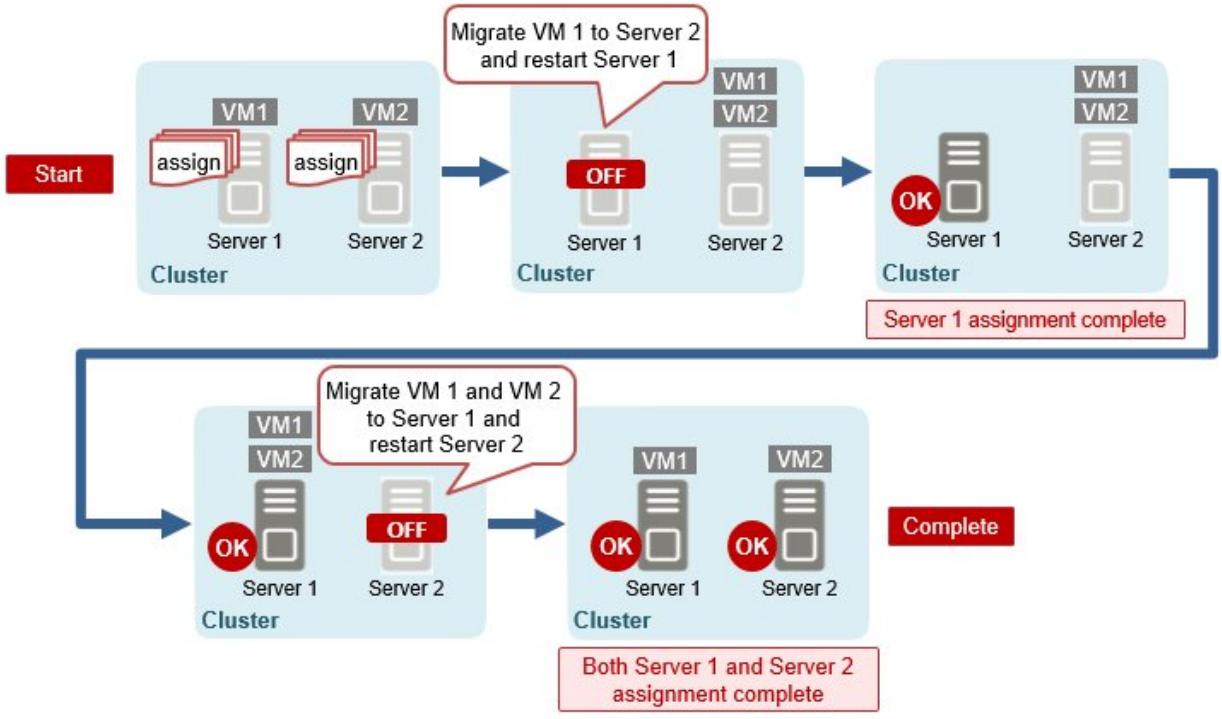
You can confirm the availability and insufficiency of resources from a screen in ISM as seen in "Figure 1.12 Image of adding a resource with ISM for PRIMEFLEX."
This function reduces the workload of the administrator by automating the procedure from OS installation to cluster expansion by linking with ISM's Profile Management when resources are insufficient.

Figure 1.12 Image of adding a resource with ISM for PRIMEFLEX



It is easier to manage the operation of a virtual platform because the firmware of cluster nodes is updated without stopping operations as seen in "Figure 1.13 Image of Rolling Update."

Figure 1.13 Image of Rolling Update



1.2 Product System and Licenses

The product system for ISM is composed of the following, and the functions that can be used vary depending on the license.

- Media packs

  This is the ISM installation media. ISM is provided as a virtual appliance that has been packaged into software that serves as the operating platform for virtual machines. You must select a media pack according to the hypervisor that operates ISM (virtual appliance).

- Server licenses

  These licenses unlock the use of functions in ISM. The functions that can be used (Operation Modes) are different depending on whether or not a server license is registered and the type of server license it is. Prepare the necessary server license for the functions (Operation Mode) that you need.

  A server license is required for ISM (each virtual appliance).

  Prepare node licenses according to the server license mode.

- Node licenses

  A license granting permission for the maximum number of nodes that can be managed in ISM. A node license is required to monitor/operate nodes in ISM. Prepare the appropriate node license according to the increase in the number of managed nodes.

  Prepare node licenses according to the Operation Mode of the server license. Only one type of node license can be registered with ISM.

Point

- Hereafter, the virtual appliance in which ISM is packaged will be referred to as "ISM-VA."
- The Operation Mode of the server license and the node license must match.

ISM product systems and Operation Modes

ISM product system	Operation Mode		
	Essential	Advanced	Advanced for PRIMEFLEX
Media packs	- Infrastructure Manager for Red Hat Enterprise Linux KVM Media Pack V2 - Infrastructure Manager for vSphere Media Pack V2 - Infrastructure Manager for Windows Server Hyper-V Media Pack V2		- Infrastructure Manager for PRIMEFLEX Media Pack (ESXi) V2 - Infrastructure Manager for PRIMEFLEX Media Pack (Hyper-V) V2
Server licenses	No license registration	Infrastructure Manager Advanced Edition Server License V2	Infrastructure Manager Advanced Edition for PRIMEFLEX Server License V2
Node licenses [Note]	Up to a maximum of 1000 nodes can be registered without a license	Infrastructure Manager Node License V2 Up to 1000 nodes can be registered by license registration	Infrastructure Manager for PRIMEFLEX Node License V2 Up to 1000 nodes can be registered by license registration

[Note]: Node licenses are counted differently depending on the device that is registered. For details, contact your local Fujitsu customer service partner.

Supported functions for each Operation Mode

Note: Y = Supported, N = Not supported

Function	Operation Mode		
	Essential	Advanced	Advanced for PRIMEFLEX
Node Management	Y [Note 1]	Y	Y
Monitoring	Y [Note 2]	Y	Y
Firmware Management	Y [Note 3]	Y	Y
Profile Management	N	Y	Y

Function		Operation Mode		
		Essential	Advanced	Advanced for PRIMEFLEX
Log Management		N	Y	Y
Network Management		N	Y	Y
Power Capping [Note 4]		N	Y	N
Virtual Resource Management [Note 5]		N	Y	Y
Backup/Restore Hardware Settings [Note 6]		N	Y	Y
Packet Analysis of Virtual Network [Note 7]		N	Y	Y
Expansion functions for virtualized platform	Cluster Management	N	Y	Y
	Cluster Creation	N	N	Y
	Cluster Expansion	N	N	Y
	Rolling Update	N	N	Y
	Node Disconnection/ Reintegration [Note 8]	N	N	Y
	Cluster Stop [Note 9]	N	N	Y
Backup/restoration of ISM [Note 10]		Y	Y	Y

[Note 1]: To use Management of Cloud Management Software, an Advanced or Advanced for PRIMEFLEX server license is required. For information, refer to "2.13.6 Management of Cloud Management Software" in "User's Guide."

[Note 2]: To use the following features, an Advanced or Advanced for PRIMEFLEX server license is required.

- Displaying the mounting position in a rack or displaying 3D view for a node

  For information, refer to "1.1.2 Integrated Monitoring for the Status of Multiple Nodes (Monitoring)."

- Setting a monitoring policy

  For information, refer to "Hardware settings when registering discovered nodes" in "2.2.1.6 Discovery of nodes" in "User's Guide."

- Anomaly Detection (monitoring behavior or status that is not normal)

  For information, refer to " 2.3.6 Anomaly Detection" in "User's Guide."

[Note 3]: To manage firmware versions (Firmware Baseline), an Advanced or Advanced for PRIMEFLEX server license is required.

For information, refer to "2.6.5 Firmware Baseline" in "User's Guide."

[Note 4]: For information on this function, refer to "2.8 Power Capping" in "User's Guide." Note that this function will no longer be available after V2.10.0 (launch in 2H of CY2024)

[Note 5]: For information on this function, refer to "2.9 Virtual Resource Management" in "User's Guide."

[Note 6]: For information on this function, refer to "2.10 Backup/Restore Hardware Settings" in "User's Guide."

[Note 7]: For information on this function, refer to "2.11 Packet Analysis of Virtual Network" in "User's Guide."

[Note 8]: For information on this function, refer to "2.12.5 Node Disconnection/Reintegration" in "User's Guide."

[Note 9]: For information on this function, refer to "2.12.8 Cluster Stop" in "User's Guide."

[Note 10]: For information on this function, refer to "4.4 Backup/restoration of ISM" in "User's Guide."

Note

- Be sure to use the correct set of media packs and server/node licenses for the same product. You cannot use an ISM for PRIMEFLEX server/node license if you are using an ISM media pack. The same is also true for the opposite.
- Devices that support Operation Modes and functions may vary. For details, contact your local Fujitsu customer service partner.

- When the Operation Mode is Essential mode, the ISM REST API is not supported. Operation when using the REST API is not guaranteed.

Chapter 2 Required Preparations and Procedures for Using ISM

This chapter describes the preparations and procedures for using the functions in Essential mode after installing ISM. For information on all of the functions in ISM, refer to "User's Guide."

The overview of the content described in this chapter is shown in "Figure 2.1 Overview of the functions that can be used in Essential mode."

Figure 2.1 Overview of the functions that can be used in Essential mode

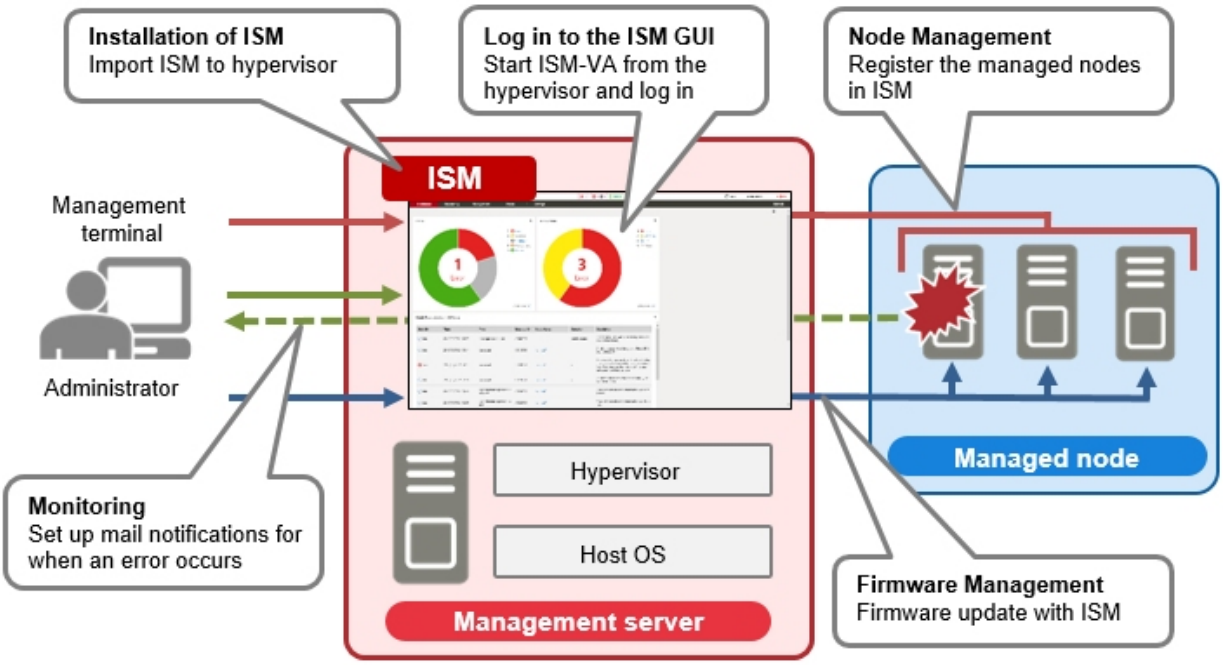


Table 2.1 Reference for the procedures and functions that can be used in Essential mode

Function	Reference
Node Management	2.3 Procedures for Using Node Management
Monitoring	2.4 Procedures for Using Monitoring
Firmware Management	2.5 Procedures for Using Firmware Management

Point

- You must install ISM to use ISM. For the installation workflow, refer to "2.1 ISM Installation Workflow."
- The procedure in the "Table 2.1 Reference for the procedures and functions that can be used in Essential mode" describes how to use ISM using the graphical user interface (GUI) in a web browser. For details on how to log in to the ISM GUI and screen layout, refer to "2.2 Logging in to the ISM Graphical User Interface and Screen Layout."

2.1 ISM Installation Workflow

The installation workflow for ISM is performed as follows.

1. Prepare a management server
2. Prepare a Host OS and hypervisor

3. Design the ISM installation environment
4. Install ISM-VA
5. Set up the ISM-VA environment
6. Register licenses
7. Register users
8. Allocate virtual disks

The following describes an overview of "3. Design the ISM installation environment" to "8. Allocate virtual disks."

2.1.1 Design the ISM Installation Environment

To operate ISM smoothly, you must perform the following before installing ISM.

- Estimating disk resources

  Estimate the disk resources needed for the purpose of a disk resource. The range of estimated disk resources will be different depending on the Operation Mode.

  Table 2.2 Operation Modes and the range of estimated disk resources

Purpose of disk resources	Operation Mode	
	Essential	Advanced Advanced for PRIMEFLEX
Storage for files when logs are retrieved, archived, and downloaded with Log Management	N	Y
Importing the DVD image used for the OS installation for Profile Management	N	Y
Importing firmware used by Firmware Management	Y	Y
Importing the ServerView Suite DVD image used by Profile Management and Firmware Management	Y	Y
Backup and restoration of ISM	Y	Y
Storage for collected logs for an investigation when trouble occurs	Y	Y
Collecting maintenance data for a failure investigation	Y	Y

  Note: Y = Required, N = Not required

- Designing a network

  Design a network environment according to the network environment that ISM will connect to and your operation requirements.

- Setting node names

  Specify the node names of the devices to be registered and managed by ISM. It is recommended that you set up naming conventions for node names in advance so that it is easier to recognize the purpose of nodes in ISM operations.

- Designing users

  Specify the users that will log in to ISM. Privileges are set for each operation in ISM and are defined as ISM user roles. Design the associations between users and user roles according to your security requirements.

For details on installation design, refer to "3.2 Installation Design for ISM" in "User's Guide."

2.1.2 Install ISM-VA

The ISM software is supplied with the Fujitsu Software Infrastructure Manager Media Pack for each product.

Install ISM-VA with the procedure depending on the hypervisor on which the ISM-VA is to be installed.

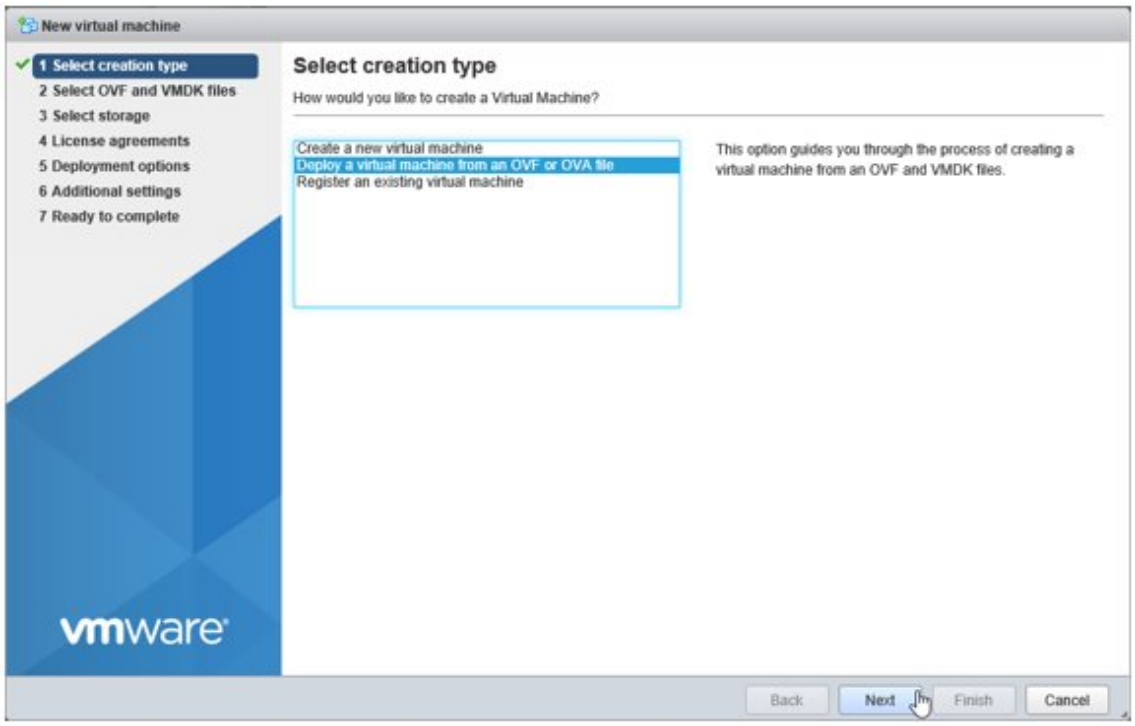
ISM-VA is installed by using the importing function of the hypervisor.

As an example, this section describes the procedure for installing ISM-VA on a VMware vSphere Hypervisor (VMware ESXi 6.5 or later).

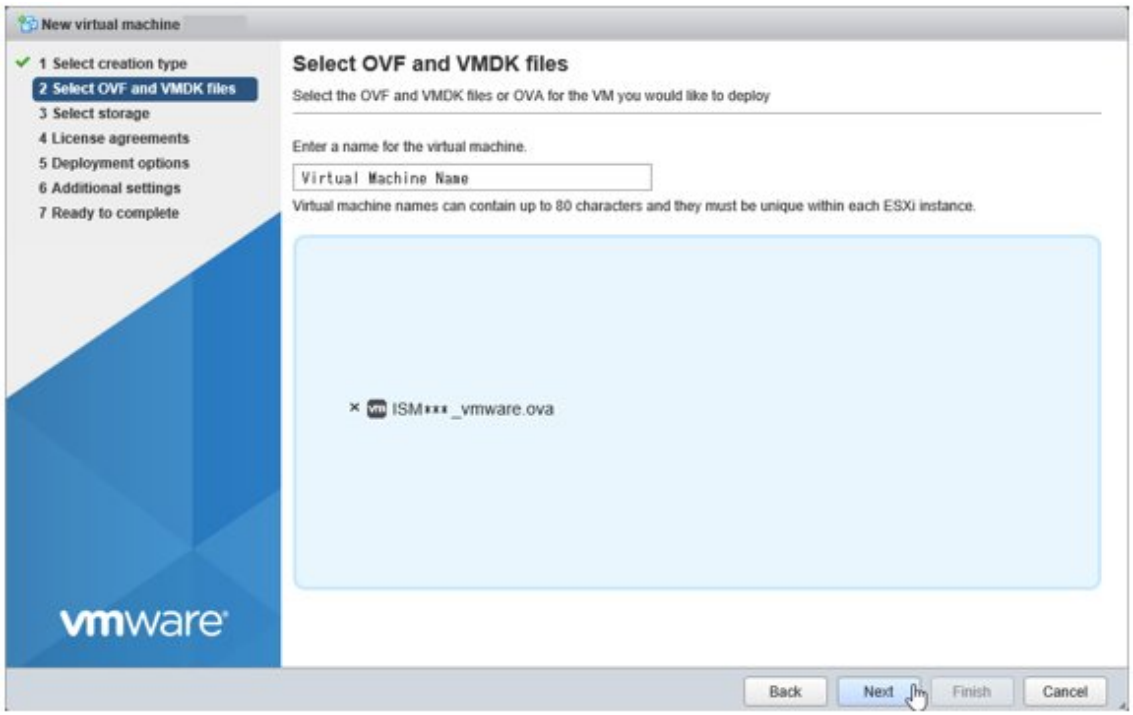
For other installation procedures, refer to "3.3 Installation of ISM-VA" in "User's Guide."

1. Start the vSphere Client (HTML 5), right-click on the [Host] of the navigator, and then select [Create/Register VM].

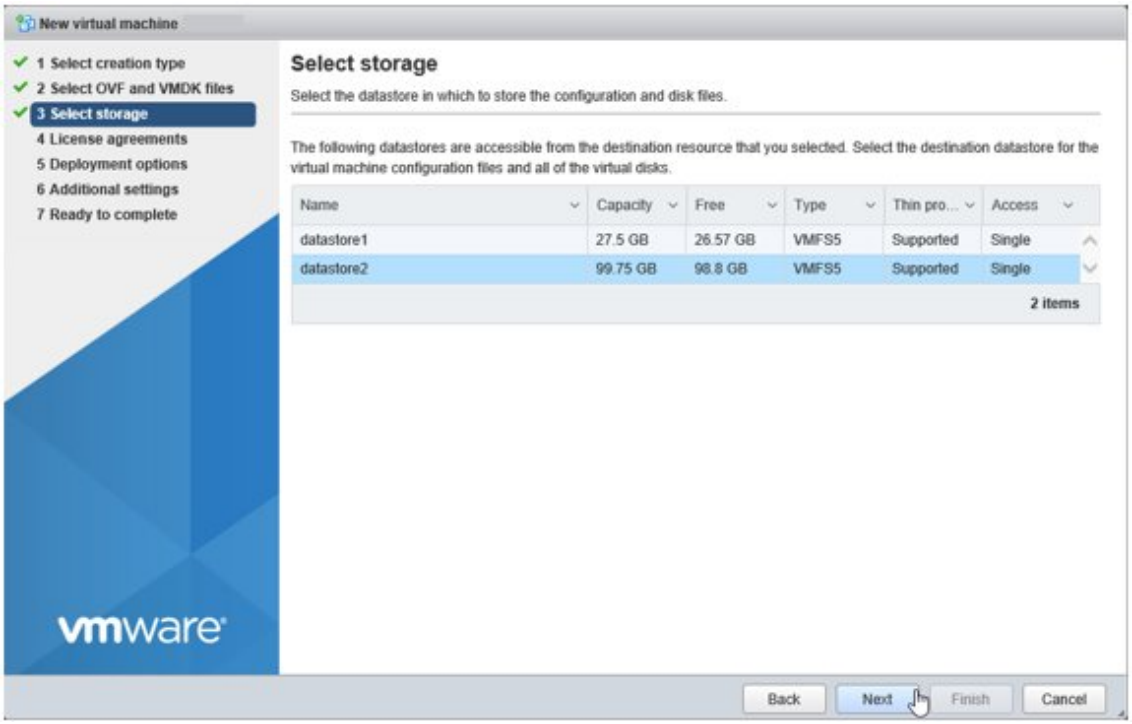
2. On the "Select creation type" screen, select [Deploy a virtual machine from an OVF or OVA file] and then select [Next].



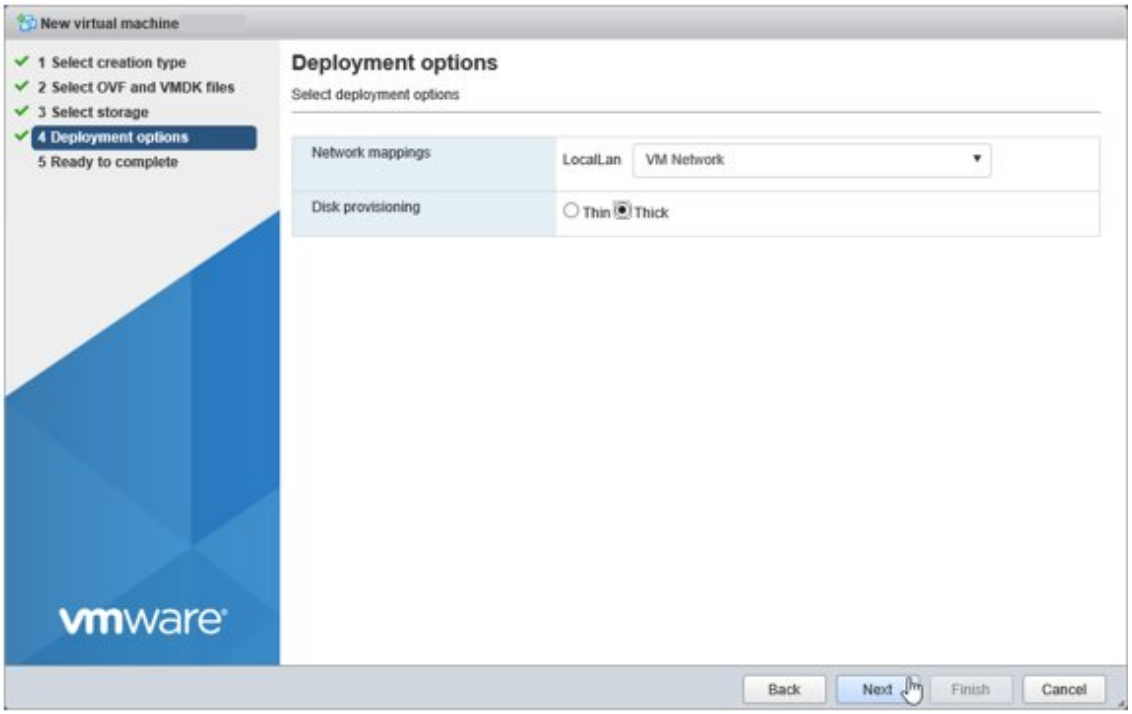
3. On the "Select OVF and VMDK files" screen, specify an arbitrary name for the virtual machine, then set deployment for the ovf file and the vmdk file included on the DVD, and then select [Next].



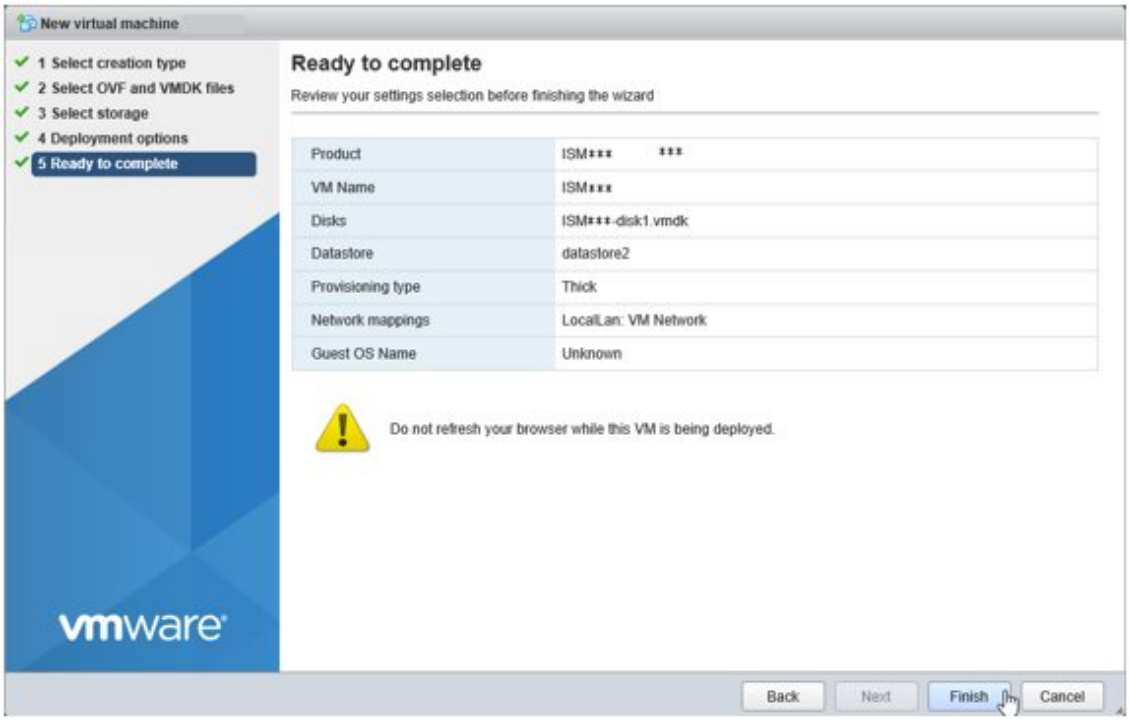
4. On the "Select storage" screen, select the datastore to deploy to, and then select [Next].



5. On the "Deployment options" screen, select the network being used. Select "Thick" for Disk provisioning and then select [Next].



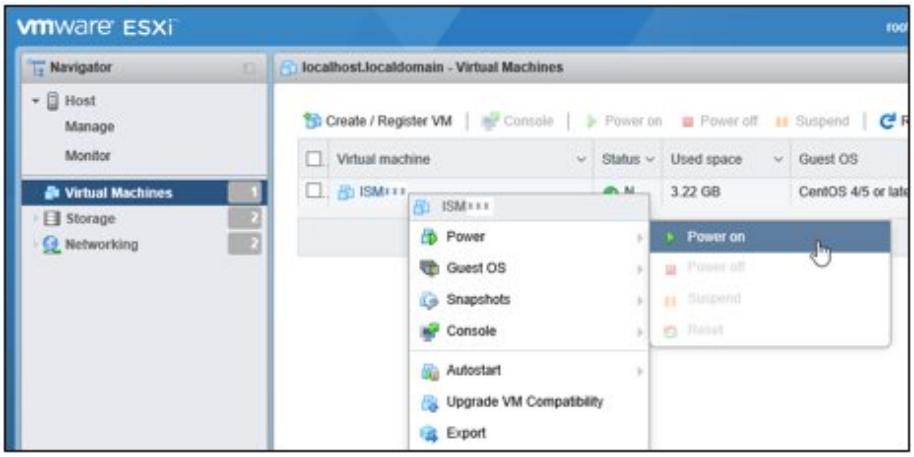
6. On the "Ready to complete" screen, confirm the settings, and then select [Finish] to complete deployment.



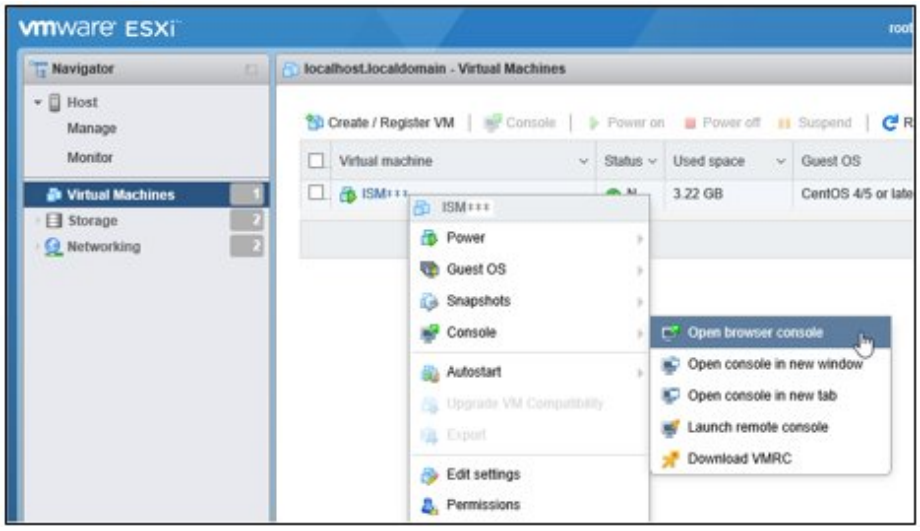
2.1.3 Set up the ISM-VA Environment

Start ISM-VA with the following procedure.

1. In vSphere Client (HTML 5), right-click on the installed ISM-VA, and then select [Power on].



2. Right-click on the installed ISM-VA, and then select [Open browser console] or other console.



Point

The following message may be displayed when starting ISM-VA, but the ISM-VA settings are optimized to operate on VMware ESXi 6.5/6.7, so this is not a problem.

```
The configured guest OS (CentOS 4/5 or later (64-bit)) for this virtual machine does not match the guest that is currently running (CentOS 7 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimizations.
```

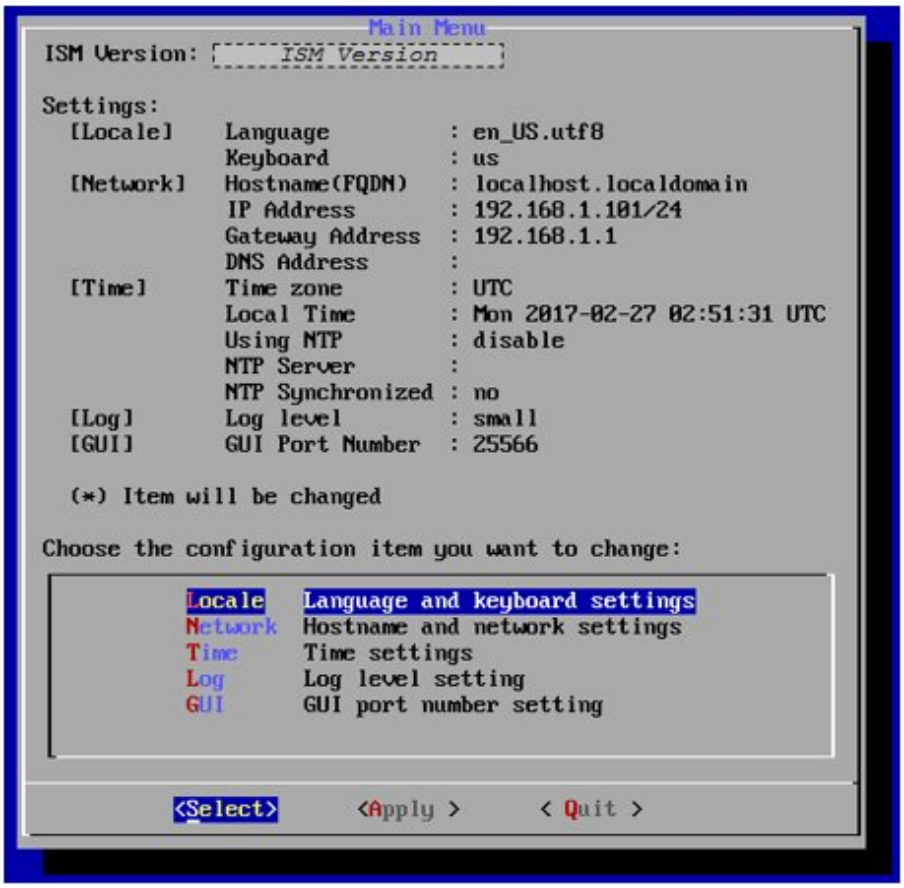
After you start ISM-VA, perform the initial setup for ISM-VA. You can set up ISM-VA by using the console basic setting menu or by using a command. This section describes how to set up ISM-VA by using the basic setting menu. To perform basic settings using a command, refer to "3.4.2.2 Initial setup using the ismadm command" in "User's Guide."

1. Use the administrator account and the default password to log in to the console.
   - Administrator account: administrator
   - Default password: admin
2. Execute the following command to start the basic setting menu.

```
# ismsetup
```

The first time you log in from the hypervisor console, the menu is displayed automatically.

The screen below is displayed.



3. Execute the ISM-VA settings.

   On the basic setting menu, the following items can be set.

   - Locale
   - Network
   - NTP server
   - Log level
   - Web GUI port number

   You must set "Network" according to the network environment that ISM will connect to. Set the IP address for ISM-VA in "Network."

   ISM will still operate correctly with the default settings for the other items, however you should set up ISM-VA according to your operation requirements. For details on the basic settings menu, refer to "4.2 ISM-VA Basic Settings Menu" in "User's Guide."

2.1.4 Register Licenses

You must register the appropriate license for Advanced mode or Advanced for PRIMEFLEX mode when you install ISM. You do not need to register a license for Essential mode.

For the appropriate media and license for an Operation Mode, refer to "1.2 Product System and Licenses."

You can register a license from the console or from the GUI in a web browser. This section describes how to register a license from the GUI.

To register a license from the console, refer to "4.8 License Settings" in "User's Guide."

1. Start the ISM GUI in a web browser.

   URL: https://<ISM-VA IP address>:25566

2. From the GUI, log in as an administrator.

   Password (default): admin

   The "Fujitsu End User Software License Agreement" screen is displayed.

3. Check the content, and then check [Above contents are correct.].

4. Select the [Agree] button.

5. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [General].

   For details on the screen layout of the GUI, refer to "2.2 Logging in to the ISM Graphical User Interface and Screen Layout."

6. From the menu on the left side of the screen, select [License].

7. From the [Actions] button, select [Register].

   The "Register License" screen is displayed.

8. Use the following procedure to register the license key.

   a. Specify the license key in the entry field.

   b. Select the [Add] button to add entry fields if adding other license keys.

   c. Repeat Step a to b and register all licenses, then select the [Apply] button.

9. From the [Actions] button, select [Restart ISM-VA] to restart ISM-VA.

2.1.5 Register Users

Register the users that you designed in "2.1.1 Design the ISM Installation Environment." Use the following procedure to register users.

1. Start the ISM GUI in a web browser.

2. From the GUI, log in as an administrator.

3. From the Global Navigation Menu on the GUI of ISM, select [Settings] - [Users].
   For details on the screen layout of the GUI, refer to "2.2 Logging in to the ISM Graphical User Interface and Screen Layout."

4. From the menu on the left side of the screen, select [Users].

5. From the [Actions] button, select [Add].
   The "Add User" screen is displayed.

6. Enter the user information, and select the [Apply] button.

7. Repeat Step 5 and 6 for each user to be registered.

2.1.6 Allocate Virtual Disks

Allocate the virtual disks to ISM-VA (virtual machines) via the hypervisor. Create the virtual disks so that they are within the capacity of the disk resources that was estimated in "2.1.1 Design the ISM Installation Environment."

Allocate virtual disks to be used for ISM-VA disk resources (system space) and disk resources for each user (user space). For details on system space and user space, refer to "3.2.1 Disk Resource Estimation" in "User's Guide."

To allocate virtual disks for system space and user space, refer to the following in "User's Guide."

- System space: "3.7.1 Allocation of Virtual Disks to ISM-VA"
- User space: "3.7.2 Allocation of Virtual Disks to User Groups"

2.2 Logging in to the ISM Graphical User Interface and Screen Layout

ISM provides a graphical user interface (GUI) that can be used in a web browser.

Point

In addition to a GUI, other user interfaces are provided such as FTP, SSH, and REST API. For information on user interfaces, refer to "2.1 User Interface" in "User's Guide."

Login, screen layout, and item names are as follows.

Logging in to ISM

Log in to the ISM GUI after starting ISM-VA from the hypervisor.

Figure 2.2 Login screen of ISM GUI

Item	Content
URL	https://<ISM-VA IP address>:25566
User Name	administrator (default)
Password	admin (default)

Point

The actions of ISM users are restricted according to privileges called "user roles." The user with the default values above is a special user (an ISM administrator) that belongs to the Administrator group and has the Administrator role which allows the user to manage ISM in its entirety.

For details, refer to "2.13.1 User Management" in "User's Guide."

When Multi-Factor Authentication (MFA) is enabled, the following screen is displayed with the following QR code.

Scan the QR code from a device that has a multi-factor authentication client application installed, such as Google Authenticator, and then enter the displayed code in the "Authorization Code" column of the ISM GUI.

Figure 2.3 Login Screen of ISM GUI when Multi-Factor Authentication is enabled (on first login)

Item	Description
Authentication Code	Enter the code generated by scanning the QR code or the emergency codes.
QR Code	QR code for generating an authentication code.
Setup Key	Use when the QR code cannot be scanned. You can set the set up key in a multi-factor authentication client application to generate the authentication code.
Emergency Codes	Code that can be used instead of the authentication code. If the device that scans the QR code is broken or is lost, you can log in by entering the emergency codes instead of the authentication code.

Write down Setup Key and Emergency Codes. They are displayed only once, so be sure to keep them safe.

Select the check box for confirmation, and log in.

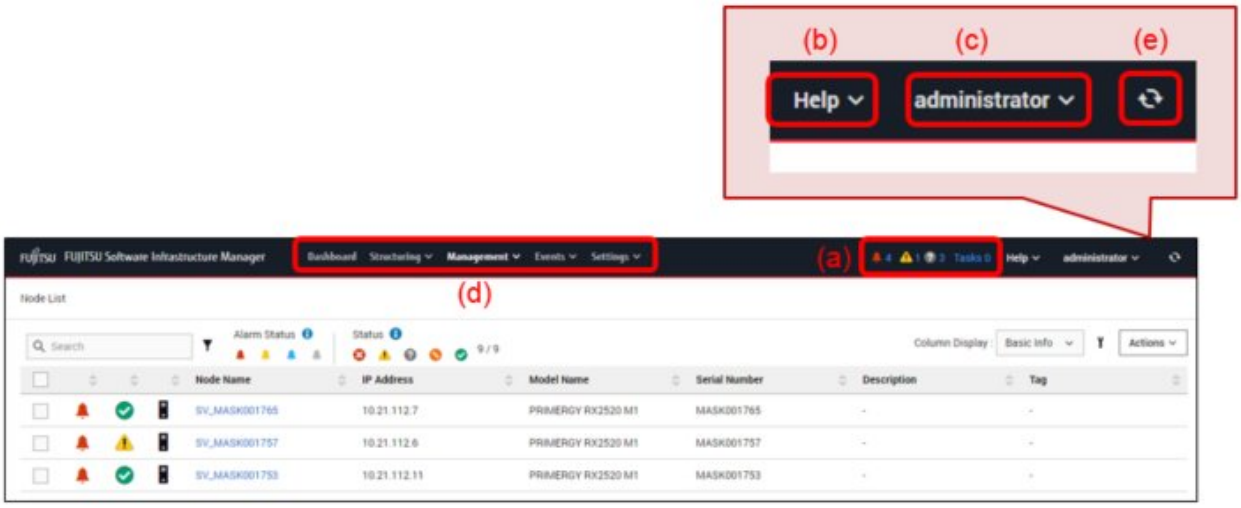
For subsequent Multi-Factor Authentication logins, enter the code displayed in the multi-factor authentication client application to log in.

Figure 2.4 Login screen of ISM GUI when Multi-Factor Authentication is enabled (second and subsequent logins)

Point

- ISM supports the multi-factor authentication client applications that comply with RFC 6238.
  Google Authenticator (iOS, Android) is recommended.
- For information about Multi-Factor Authentication provided by ISM, refer to "2.13.1 User Management" in "User's Guide."

Screen layout and item names



(a) Alarm status, status, task icon

Displays the number of nodes with an "Error" status and the number of currently running tasks.

(b) Help

Displays help and guidance.

(c) User name

You can view the user name that is logged in.

In order to log out from ISM, move the mouse pointer over the user name and select [Log out].

Select [Language] to change the settings for the displayed Language, Date Format, and Time Zone on the GUI.

(d) Global Navigation Menu

This menu is for accessing different screens in ISM.

(e) [Refresh] button

Selecting this button refreshes the entire screen.

2.3 Procedures for Using Node Management

Node Management is a function for registering and managing nodes in ISM.

2.3.1 Register Nodes

To manage nodes in ISM, nodes must first be registered with ISM.

There are two ways to register nodes:

- Use discovery to register a node on a network

  Specify an IP address range and discover nodes that can be registered. You can register discovered nodes in any order.

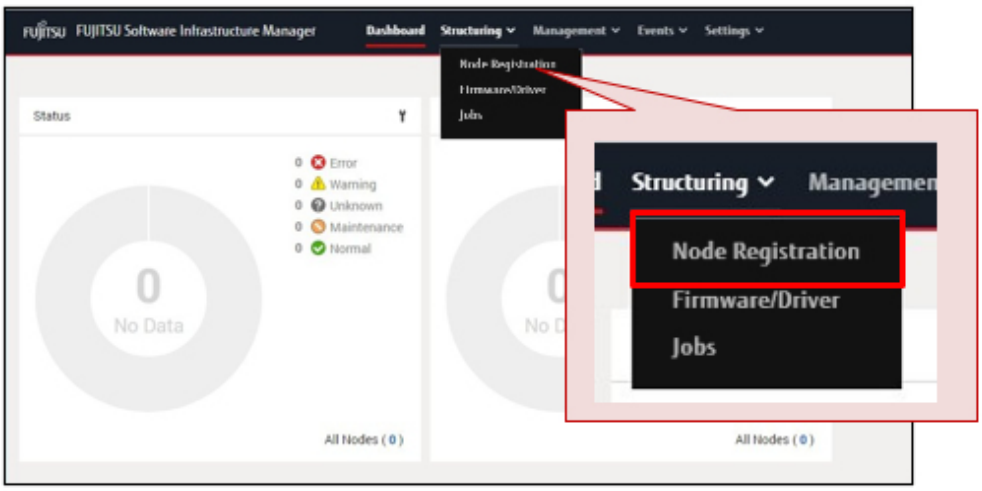
- Register a node directly

  You can register a node by specifying a single IP address.

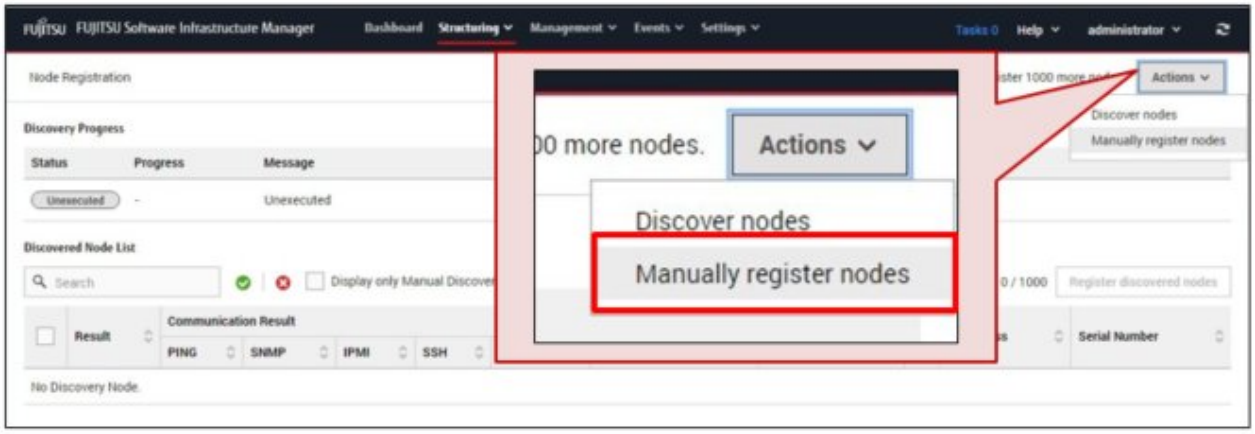
For details, refer to "Chapter 3 Register/Set/Delete a Managed Node" in "Operating Procedures."

The following shows how to register a node directly. As an example, this section describes the procedure for registering a server.

1. From the Global Navigation Menu, select [Structuring] - [Node Registration].



2. From the [Actions] button on the "Node Registration" screen, select [Manually register nodes].



3. Follow the "Node Manual Registration" wizard and enter the setting items to register the server.

   For a description on the setting items, select [⑦] in the upper-right of the wizard, and refer to the help screen.

4. From the Global Navigation Menu, select [Management] - [Nodes] to confirm that the server is registered.

   After the server is registered, the server is displayed on the "Node List" screen.

Point

It may take time to display the node list depending on the number of nodes registered in ISM.

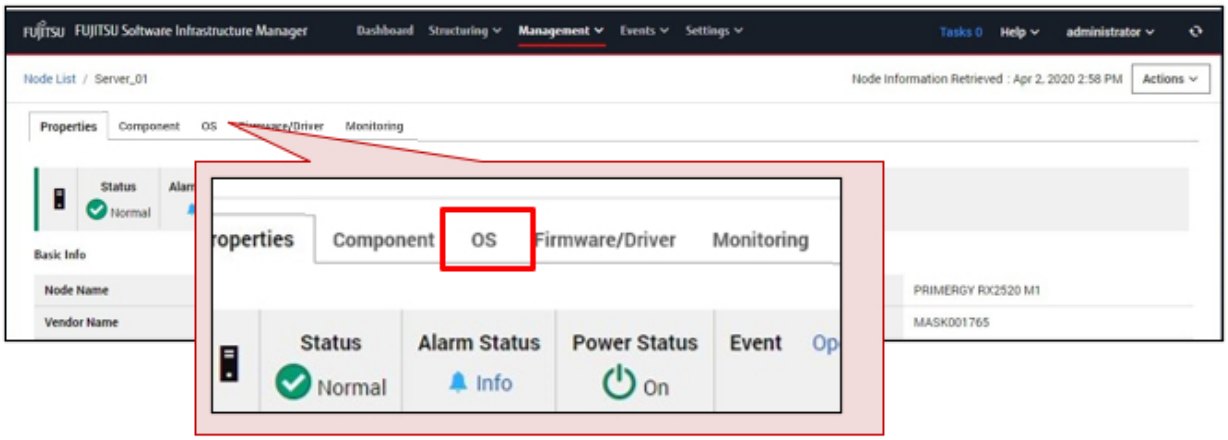
This finishes the server registration.

If an OS is installed on the target server, execute the following procedure to set the OS information in ISM.

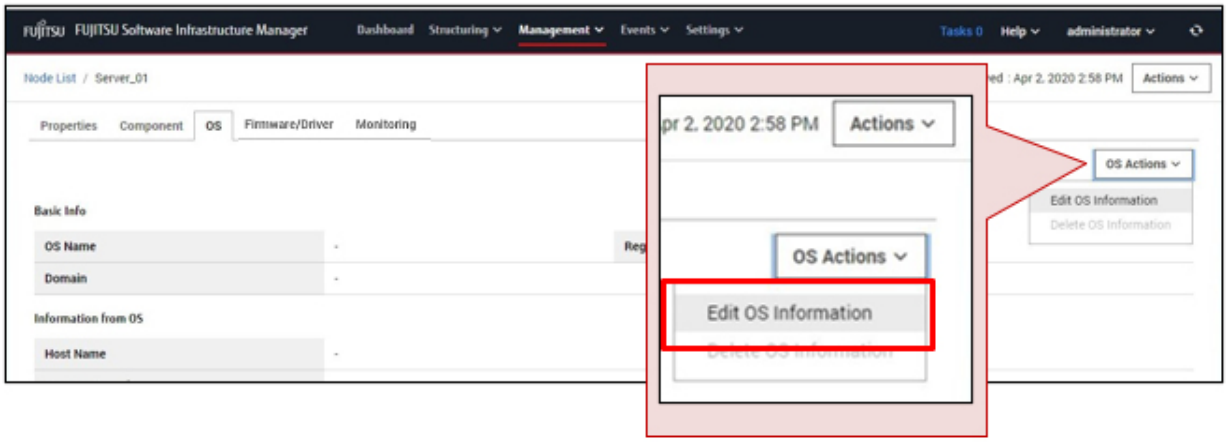
If an OS is not installed on the target server, use the following procedure to set the OS information in ISM after you have installed an OS.

5. From the Global Navigation Menu, select [Management] - [Nodes], and select the target server from the "Node List" screen.

6. On the Details of Node screen, select the [OS] tab.



7. From the [OS Actions] button on the upper-right of the screen, select [Edit OS Information].



8. On the "Edit OS Information" screen, set the OS information.

   For a description on the setting items, select [⑦] on the upper-right of the screen, and refer to the help screen.

9. After entering the OS information, select the [Apply] button.

   This finishes OS information editing. After the OS information is edited, the OS information for the server can be retrieved.

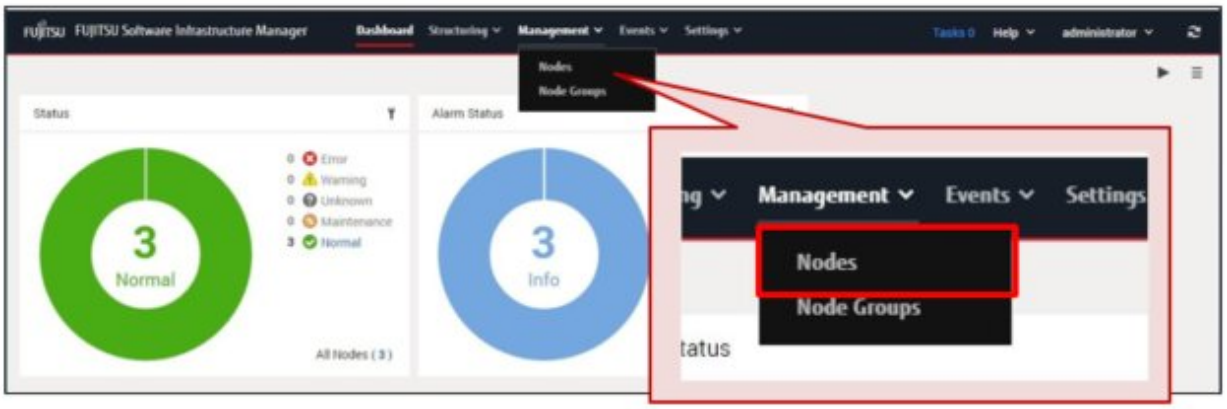
2.3.2 Manage Nodes

Information such as node names and IP addresses that have been set for nodes, model names for nodes, and serial numbers are displayed in a node list. By using this function, you can manage different kinds of devices in an integrated way.

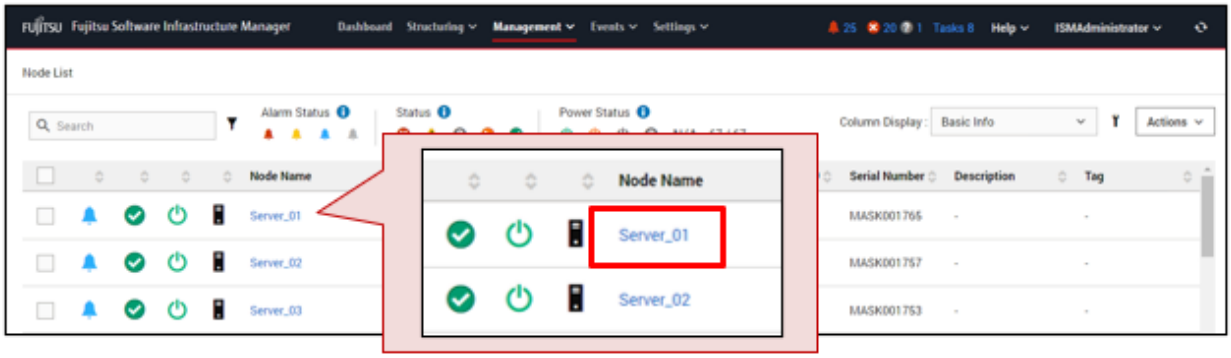
You can also refer to detailed node information for each node from the node list.

The following shows how to refer to detailed node information.

1. From the Global Navigation Menu, select [Management] - [Nodes].



2. On the "Node List" screen, select the node name.



3. On the Details of Node screen, select the tab that has the information you want to confirm.

Point

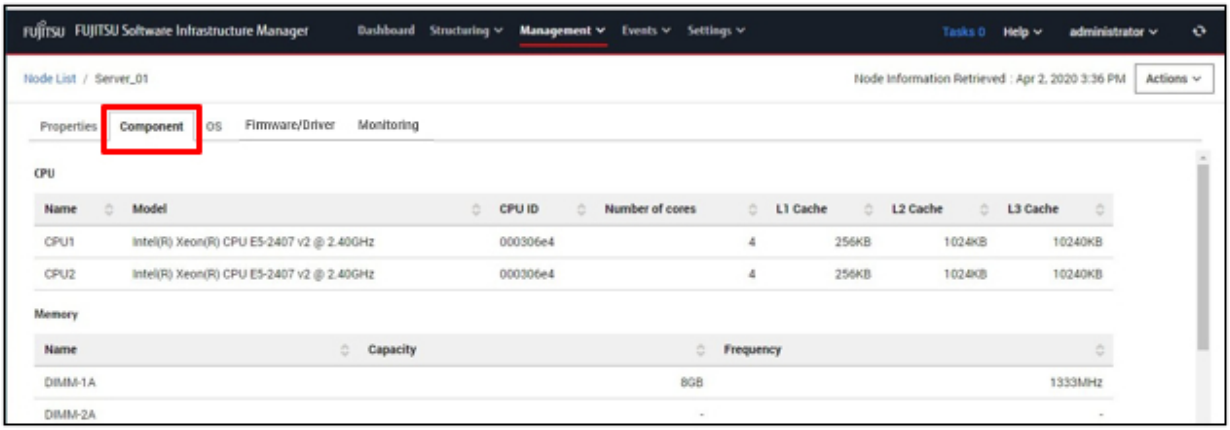
On the Details of Node screen, information is separated into tabs.

The tabs displayed differ depending on the type of device.

The following shows a screen sample when the target node is a server.

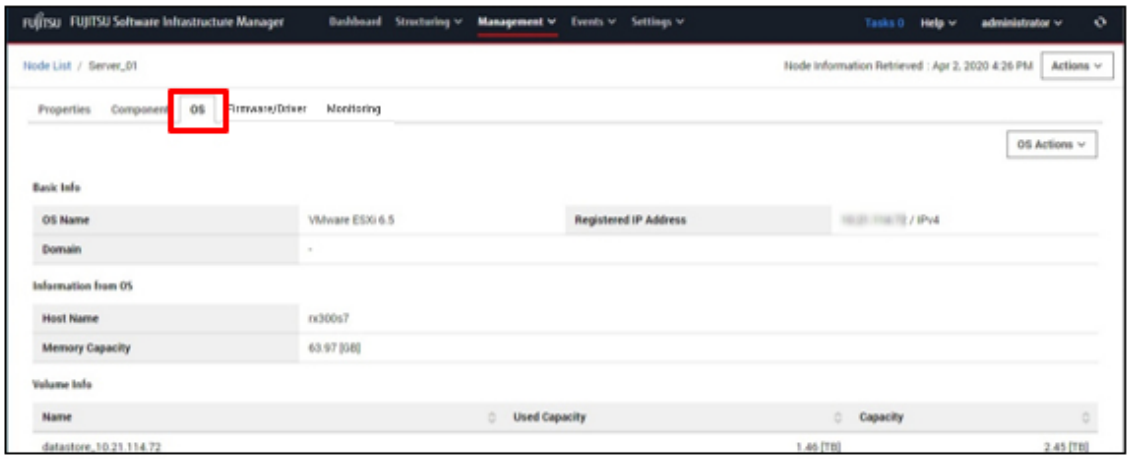
- To confirm information for the CPU and memory installed on the server

  Select the [Component] tab.



- To confirm information for the OS that is installed on the server

  Select the [OS] tab.



Point

For other operations involving node management, refer to the following chapters in "Operating Procedures."

- "Chapter 3 Register/Set/Delete a Managed Node"
- "Chapter 6 Other Functions to Manage/Operate Nodes"

2.4 Procedures for Using Monitoring

Monitoring is a function that can be used for the following purposes.

- Receiving event notifications (SNMP traps) from nodes as well as monitoring changes in statuses
- Periodically recording CPU/memory availability and sensor values such as CPU temperature/intake temperature as well as making comparisons with specified threshold values
- Issuing external alarm notifications for event notifications and monitoring results

The following items are set as the default monitoring items when a node is registered.

Table 2.3 Default monitoring items for when a node is registered

Default monitoring items	Description
Overall status	The overall status value of the managed node is monitored.
Power consumption	The power consumption of the managed device as well as each individual component are monitored.
Temperature information	The temperature inside chassis, air inlets, and other locations are monitored.
Statuses of the various LEDs	Power LEDs, CSS LEDs, Identify LEDs, and Error LEDs are monitored. This is only applicable for PRIMERGY.
Power status	The power status is monitored.

Note

The details for items that can actually be managed differ depending on the type of device.

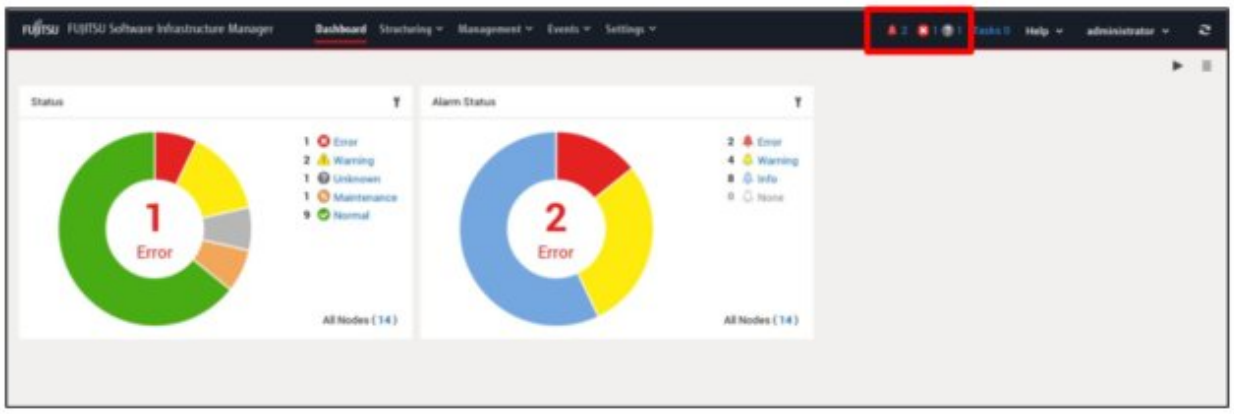
2.4.1 Monitor the Changes in Node Statuses

You can receive event notifications (SNMP traps) from nodes. You can also monitor the changes in node statuses.

The following shows how to confirm the change in status for a node.

This procedure describes how to confirm the status of a node when a severe error has occurred in a node.

1. On the ISM GUI, confirm whether an error has occurred.



An icon that indicates that an error has occurred is displayed on the upper-middle part of the screen.

Icon	Description
	An Error level alarm status. This icon indicates that a node has notified ISM that a severe error (CRITICAL level SNMP trap) has occurred on the node.
	An Error level status. This icon indicates that the status of a managed node is an Error level status.
	A Warning level alarm status. This icon indicates that a node has notified ISM that a MAJOR or MINOR level SNMP trap has occurred on the node.
	An Unknown level status. This icon indicates that an error has occurred on the node and the status cannot be confirmed.

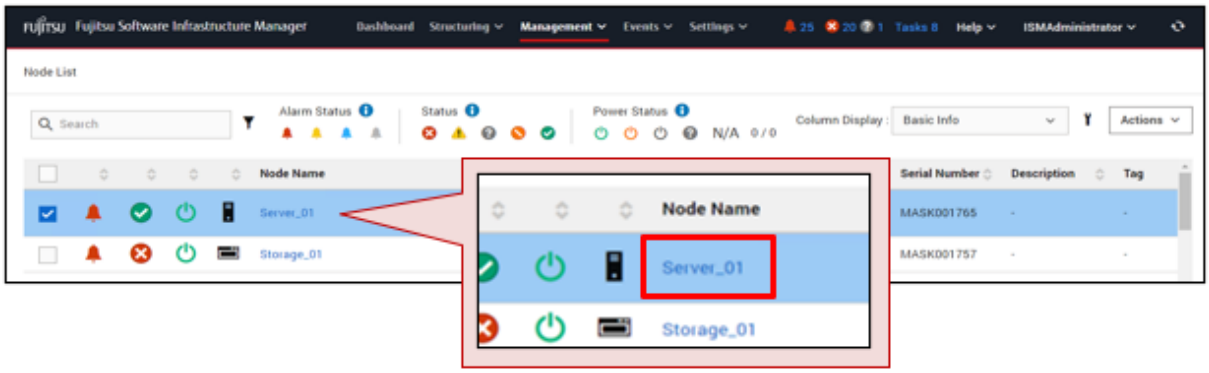
The number to the right of these icons indicate the number of nodes in which an error has occurred. These icons are not displayed when an Error level or Warning level error has not occurred.

2. Select the icon that you want to confirm the errors for.

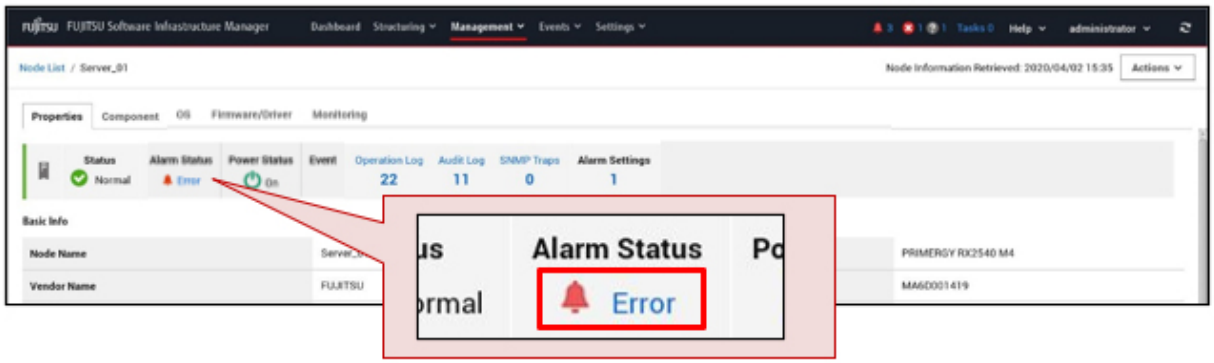
   A list of nodes in which an error has occurred is displayed.

3. From the list of nodes that have errors, select the node name that you want to confirm the error status for.

   The following is an example of a node list in which an Error level alarm status has occurred.



4. On the Details of Node screen, select the "Error" alarm status on the [Properties] tab to confirm related events when an error has occurred.

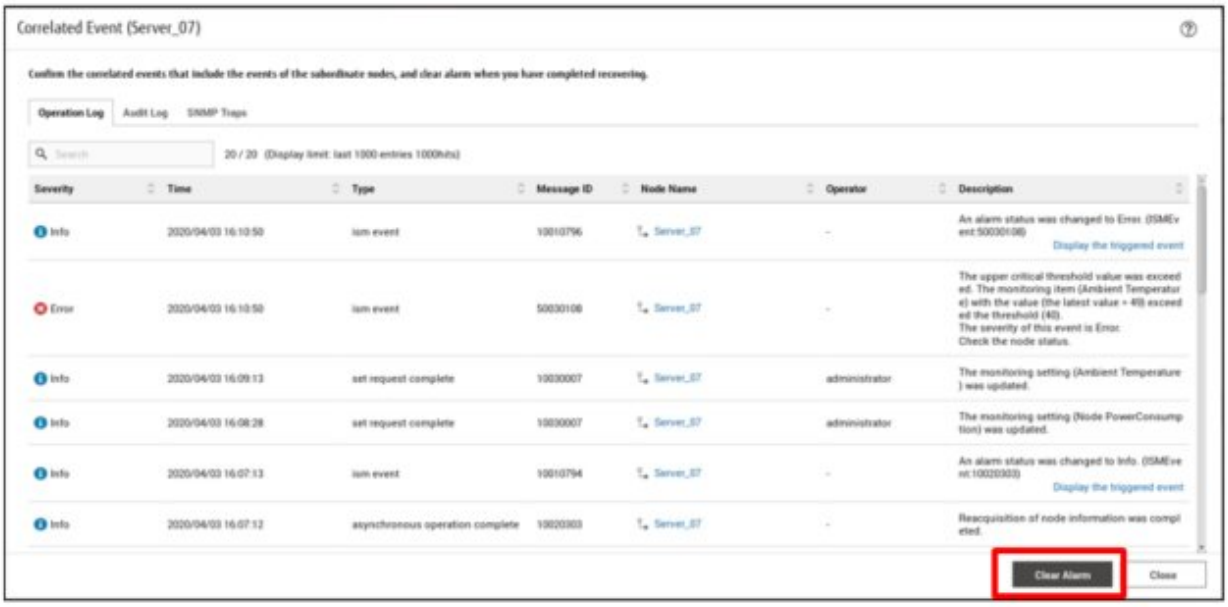


5. On the "Correlated Event" screen, confirm related events by selecting the tabs ([Operation Log] tab, [Audit Log] tab, or the [SNMP Traps] tab).

   You can investigate the cause of the Error level alarm status.

6. Clear the alarm when the error is resolved.

   Select the [Clear Alarm] button.

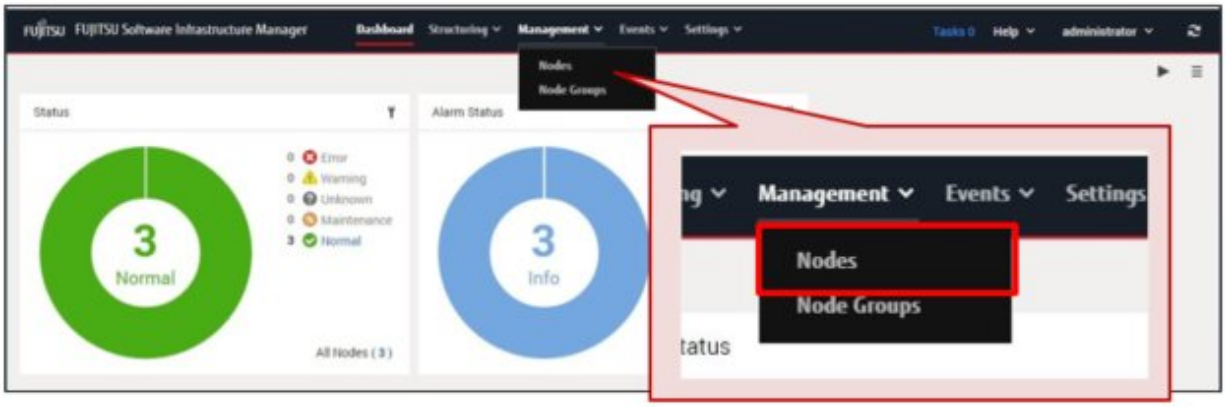


2.4.2 Monitor CPU/Memory Availability and Temperature

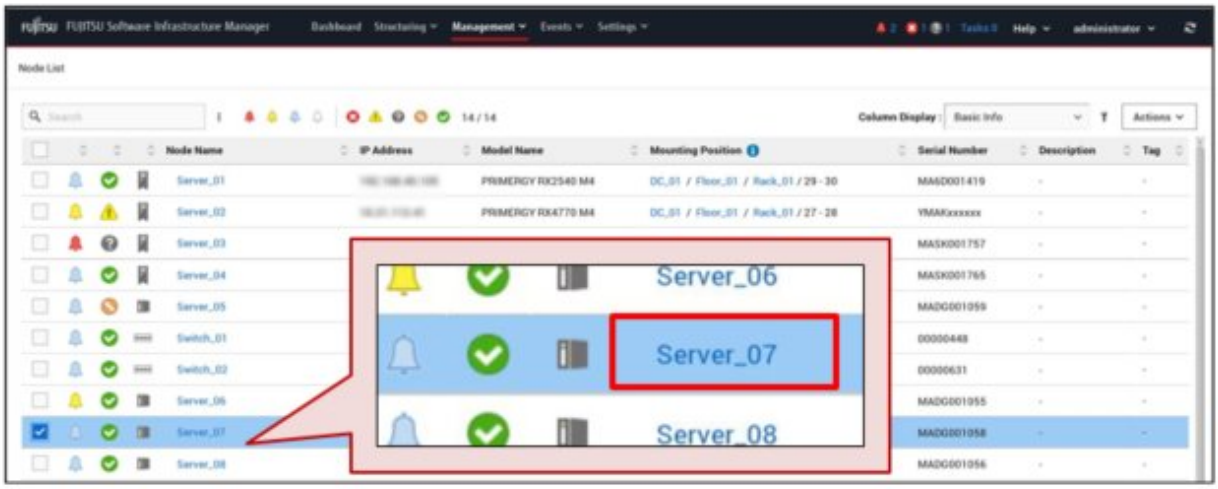
You can periodically record CPU/memory availability and sensor values such as CPU temperature/intake temperature as well as make comparisons with specified threshold values.

As an example, this section describes how to confirm the CPU/memory availability and temperature of a server.

1. From the Global Navigation Menu, select [Management] - [Nodes].

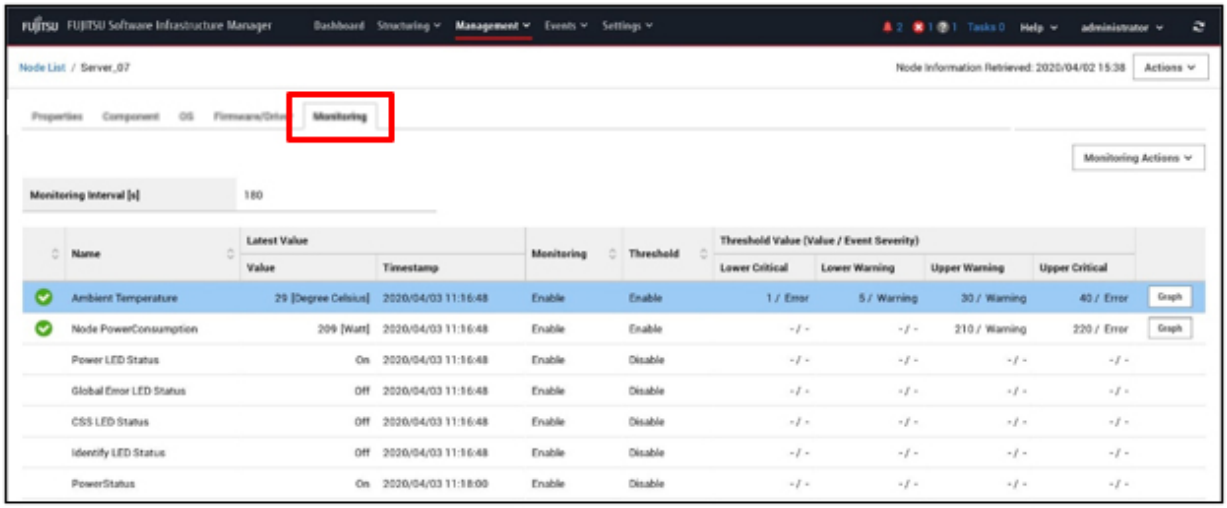


2. On the "Node List" screen, select the node name.



3. On the Details of Node screen, select the [Monitoring] tab.

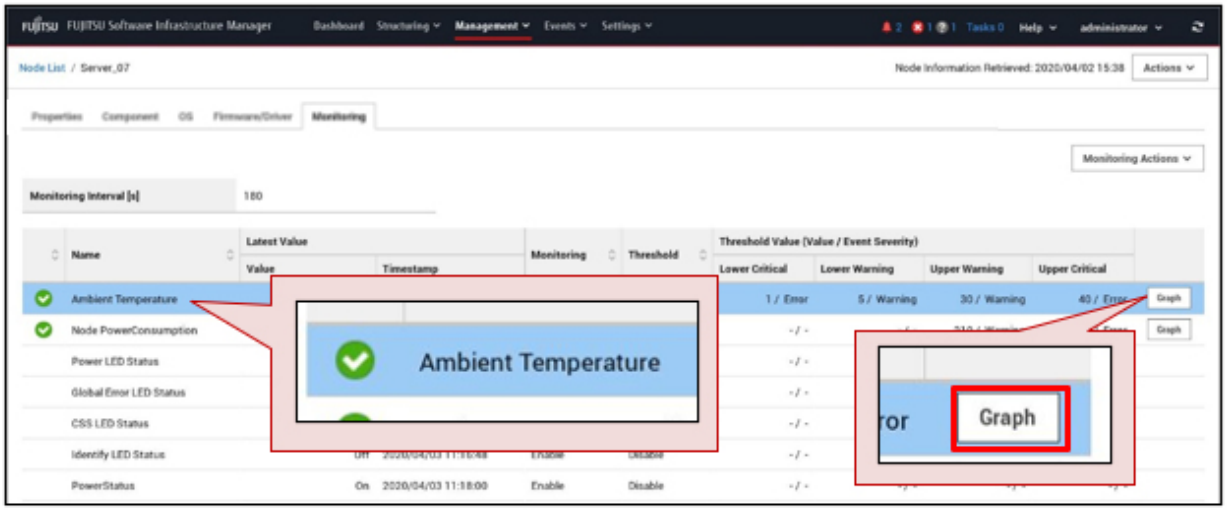
   The items to be monitored for the node are displayed.



   Selecting the [Graph] button displays the information recorded for each monitoring interval in a graph. In the graph, the threshold values are also displayed so you can identify the date and time a threshold was exceeded.

   Example: To confirm the ambient temperature in a graph

a. Select the [Graph] button in the row for the item to display in the graph (here, the ambient temperature: "Ambient Temperature").



b. On the "Monitoring Item Graph" screen, check the graph to identify the date and time the threshold value was exceeded.

2.4.3 Notify Monitoring Statuses

You can issue external alarm notifications for event notifications and monitoring results.

This section describes the setting procedure for alarm actions that provide mail notification when an error has occurred for "Table 2.3 Default monitoring items for when a node is registered."

The workflow for the setting procedure is as follows.

1. Set up the mail server (SMTP server) so that ISM can send mail.

   Refer to "2.4.3.1 Set up a mail server (SMTP server)."

2. Set up the method (action) in which notifications are made externally from ISM

   In this procedure, set up a specified mail address so that mail notification with a specific subject can be sent.

   Refer to "2.4.3.2 Set mail notification as the alarm notification method (Action)."

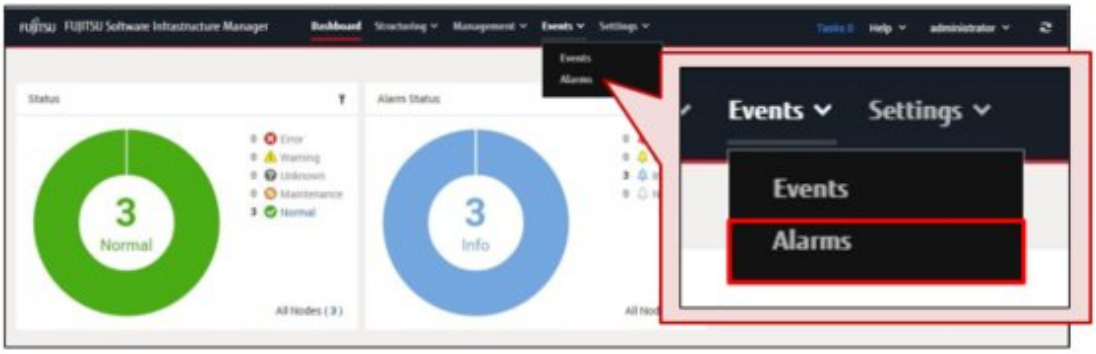
3. Set up the notification method (action) configured above and the notification targets.

   Refer to "2.4.3.3 Set alarm notification methods and notification targets (Alarm Settings)."

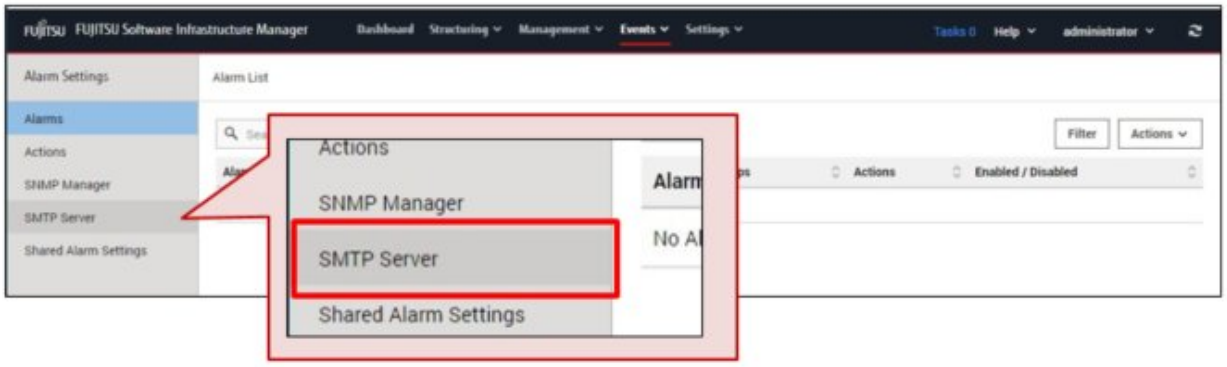
2.4.3.1 Set up a mail server (SMTP server)

You must set up a mail server (SMTP server) if mail notifications are going to be received for errors and changes in the statuses of managed nodes.

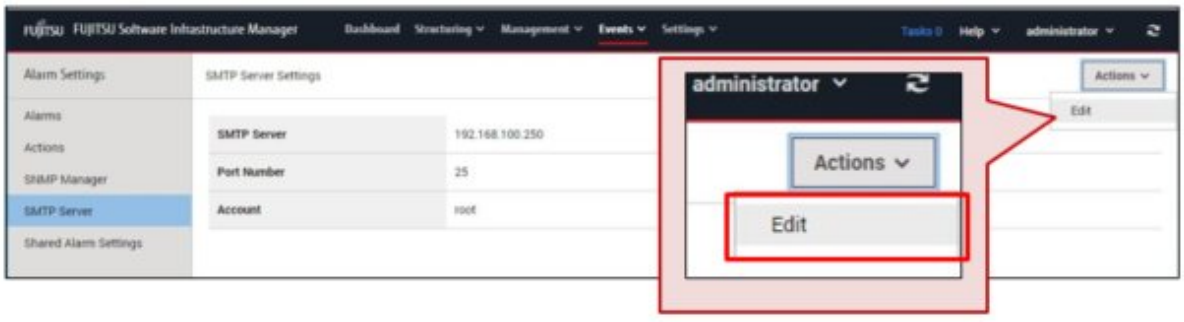
1. From the Global Navigation Menu, select [Events] - [Alarms].



2. From the menu on the left side of the screen, select [SMTP Server].



3. From the [Actions] button on the "SMTP Server Settings" screen, select [Edit].



4. Enter the setting items on the "SMTP Server Settings" screen, and then select the [Apply] button.

   For a description on the setting items, select [⑦] on the upper-right of the screen, and refer to the help screen.

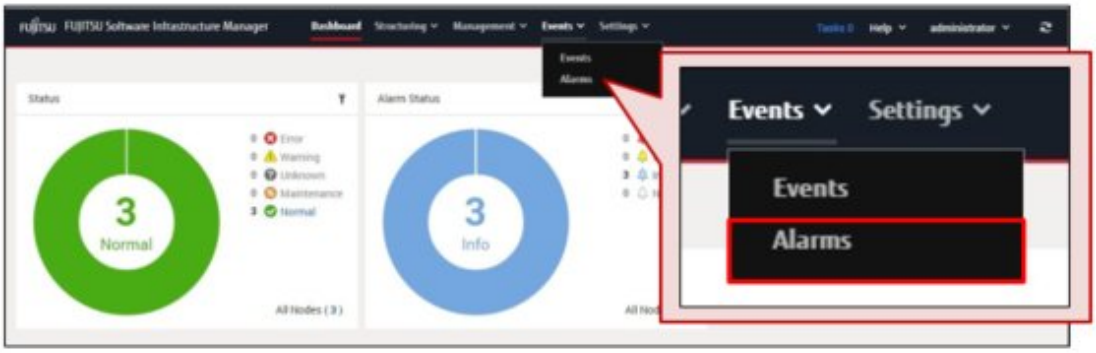
2.4.3.2 Set mail notification as the alarm notification method (Action)

Set up the method (action) in which notifications are made externally from ISM when an error has occurred for monitoring items. As an example, this section describes how to set up an action that sends mail.

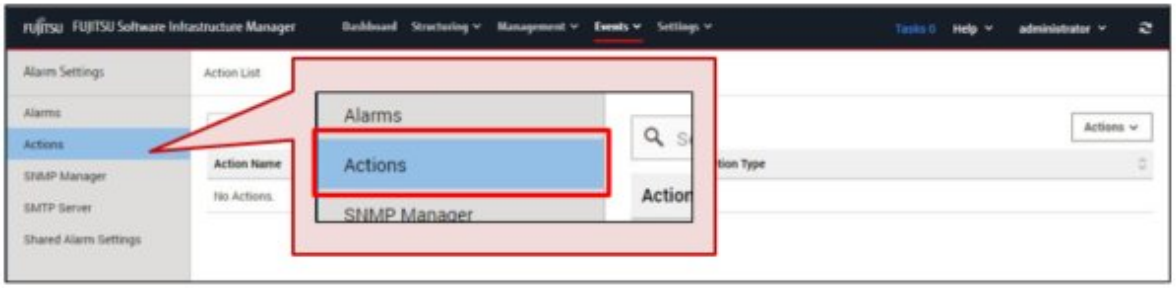
Point

For details on other types of notification methods (actions), refer to "2.3.3 Action Settings" in "User's Guide."

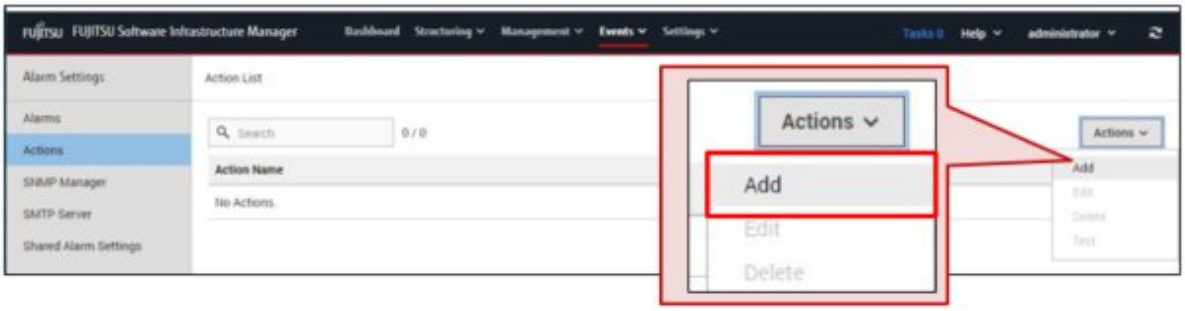
1. From the Global Navigation Menu, select [Events] - [Alarms].



2. From the menu on the left side of the screen, select [Actions].

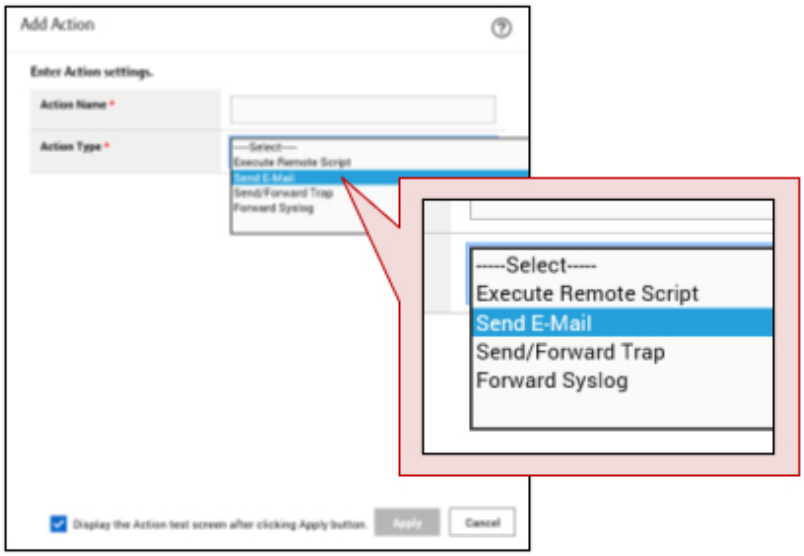


3. From the [Actions] button on the "Action List" screen, select [Add].



4. Set [Action Name] on the "Add Action" screen, and then select "Send E-Mail" in [Action Type].

   In this example, [Action Name] is set as "Mail Report."



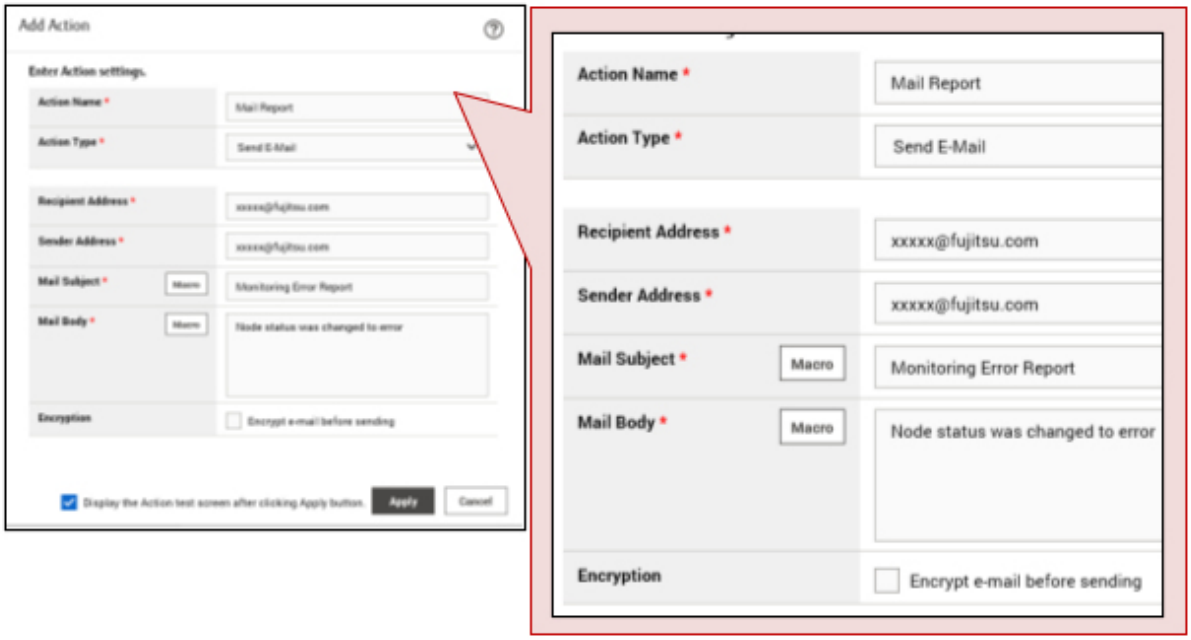
5. After entering Recipient Address, Mail Subject, etc. on the "Add Action" screen, select the [Apply] button.

   For a description on the setting items, select [⑦] on the upper-right of the screen, and refer to the help screen.

   As an example, the following content is set for mail notifications when an error has occurred for a default monitoring item.

   - Mail Subject: "Monitoring Error Report"
   - Mail Body: "Node status was changed to error"

   In "Recipient Address," enter the mail address of the administrator that will receive the mail notification.



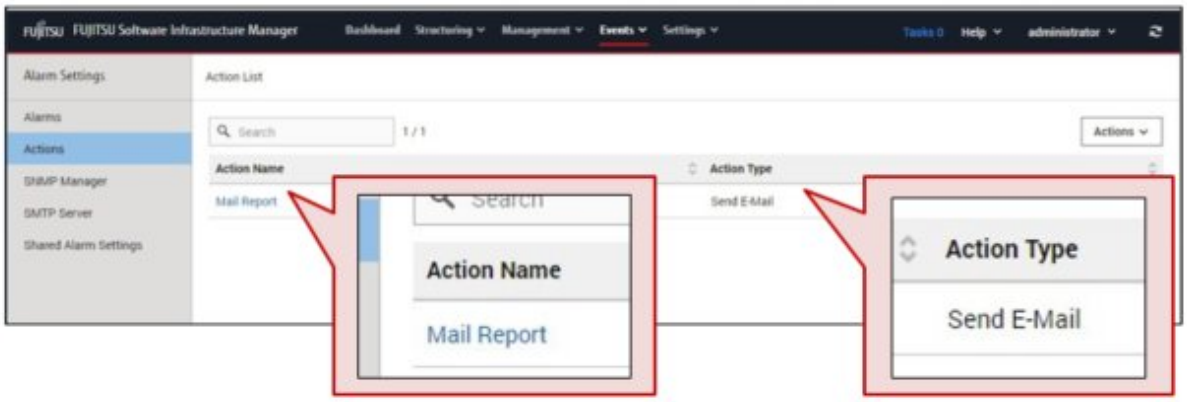
Point

You can confirm whether the set action is executed correctly.

Select the [Display the Action test screen after clicking Apply button.] check box on the bottom part of the "Add Action" screen. Since the screen will be displayed after the action is applied, perform the test.

After action is added, the set action is displayed on the "Action List" screen.

Here, you can confirm the "Action Name" and "Action Type" set in Step 4.



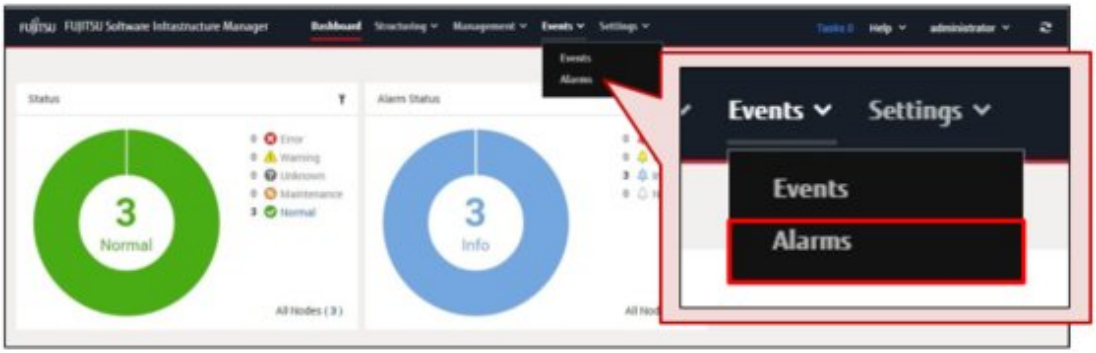
2.4.3.3 Set alarm notification methods and notification targets (Alarm Settings)

You can define created alarm notification methods (actions) and notification targets (type and event), and set alarms.

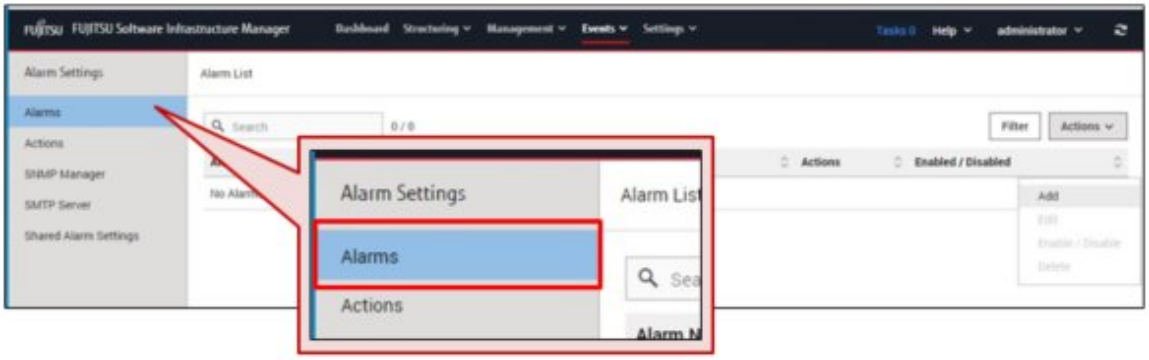
As an example, this section describes "Error Event" as the definition of an alarm and is configured to the following settings.

Item	Description
Notification target	The error or event in ISM (the error that has occurred in a default monitoring item)
Notification method	The action created in "2.4.3.2 Set mail notification as the alarm notification method (Action)" (Action Name: "Mail Report")

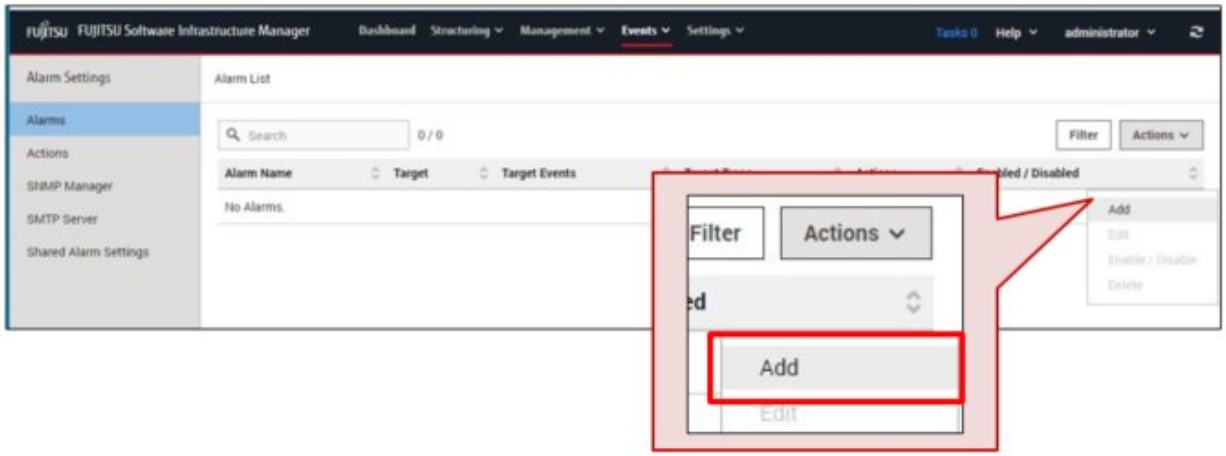
1. From the Global Navigation Menu, select [Events] - [Alarms].



2. From the menu on the left side of the screen, select [Alarms].

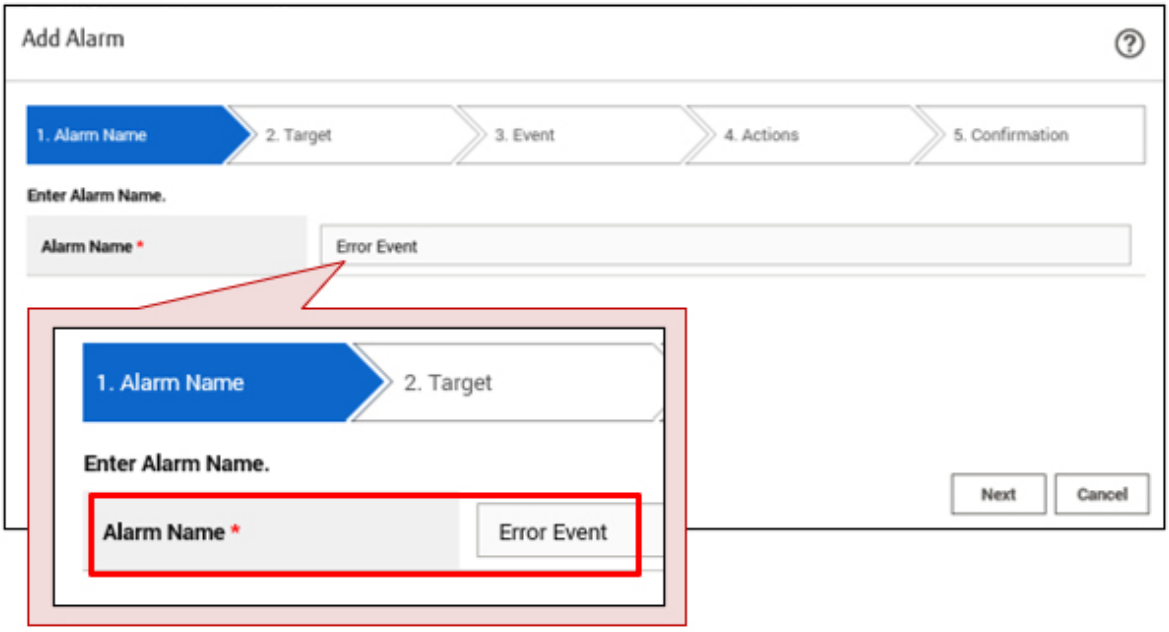


3. From the [Actions] button on the "Alarm List" screen, select [Add].



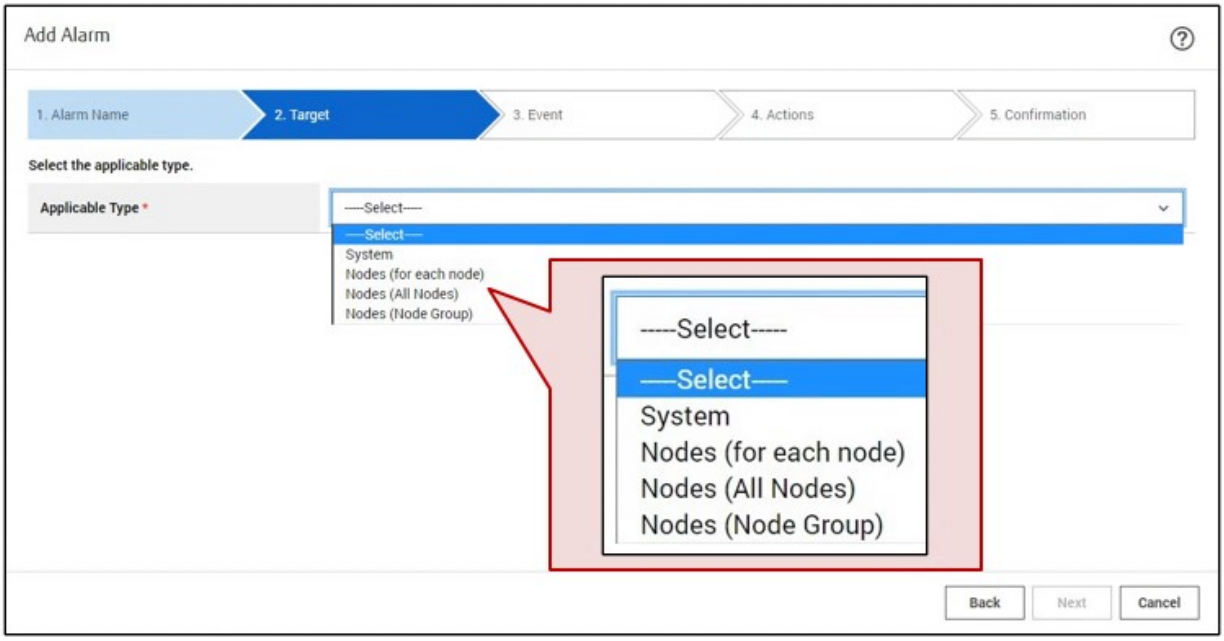
4. Enter the alarm name ("1. Alarm Name" screen in the "Add Alarm" wizard).

   In this example, the alarm name is set as "Error Event."



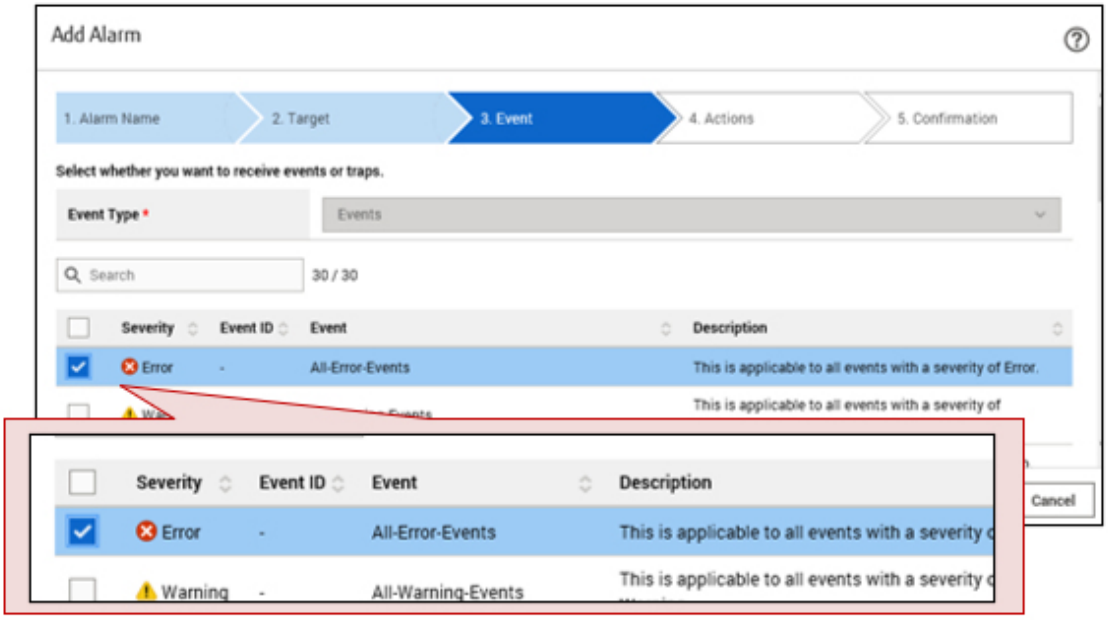
5. Set the target for alarm notification ("2. Target" screen in the "Add Alarm" wizard).

   In this example, the target for alarm notification is set to "System."
   Errors and events in ISM are the target.



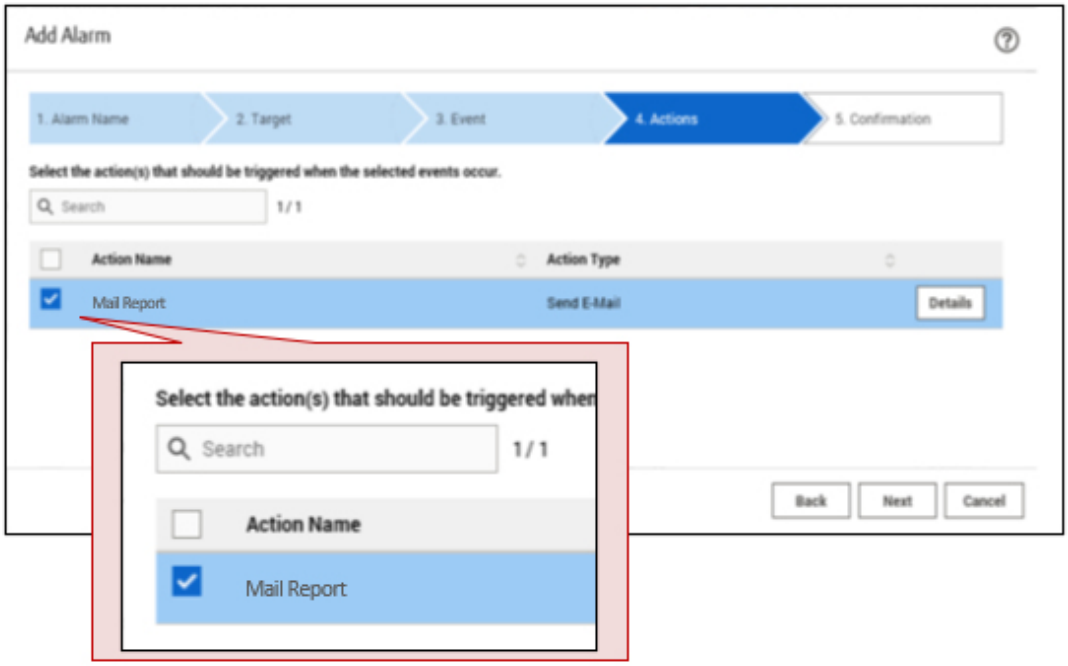
6. Select the checkbox for an event from the event list ("3. Event" screen in the "Add Alarm" wizard).

   In this example, the row in which "Severity" is "Error" and "Event Type" is "All-Error-Events" is selected.

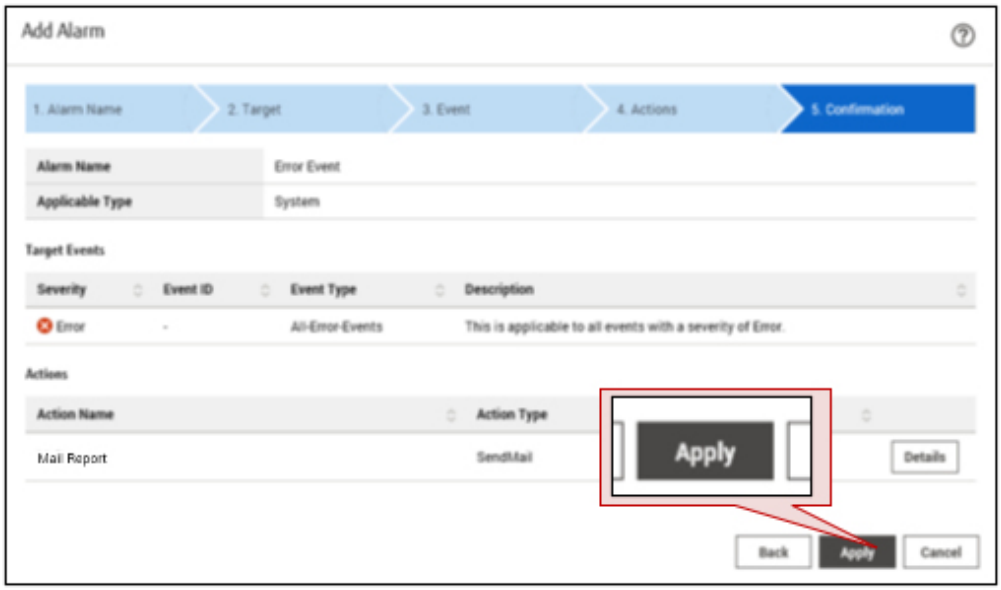


7. Select the action name from the defined action list ("4. Actions" screen in the "Add Alarm" wizard).

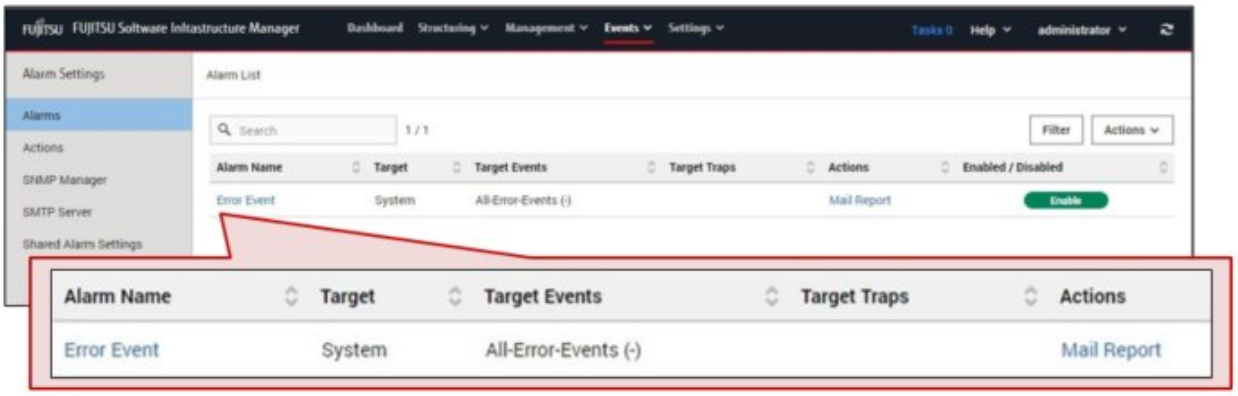
   In this example, the action name ("Mail Report") created in "2.4.3.2 Set mail notification as the alarm notification method (Action)" is selected.



8. Confirm the content, and then select the [Apply] button ("5. Confirmation" screen in the "Add Alarm" wizard).



After alarm addition is finished, the set alarm will be displayed on the "Alarm List" screen.



This finishes the alarm settings.

2.5 Procedures for Using Firmware Management

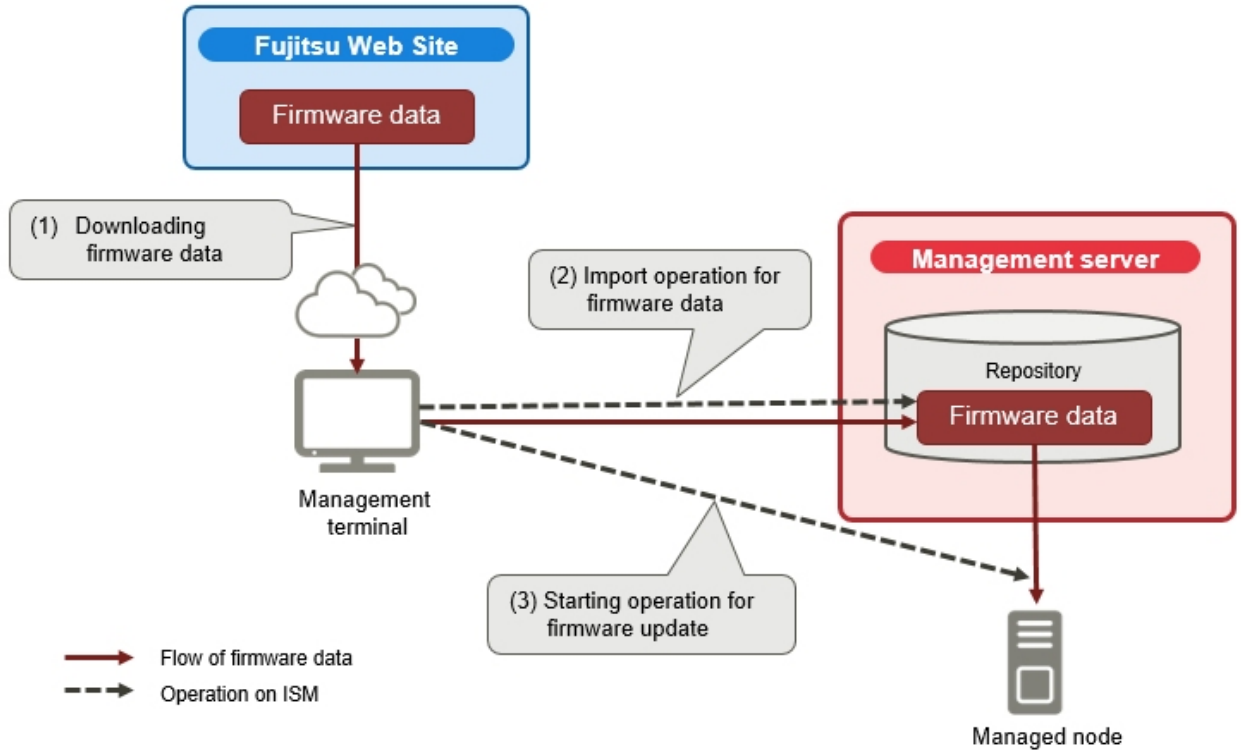
Firmware Management is a function that operates firmware updates for multiple managed nodes together and manages versions of the firmware in an integrated manner.

By using Firmware Management, you can reduce the amount of maintenance work for managed nodes.

When updating firmware, you must import the firmware data into ISM in advance. The workflow for firmware updates is as follows.

1. Download the firmware data from the FUJITSU website ((1) in the figure below).
2. Forward the firmware data that was downloaded to the repository on ISM-VA ((2) in the figure below).
3. ISM will use the firmware data that was put into the repository to update the firmware of the target node ((3) in the figure below).

Figure 2.5 Image of Firmware Management



This section describes the procedure from firmware data preparation to the execution of the firmware update for the PRIMERGY BIOS/iRMC.

The workflow for the procedure is as follows.

1. Prepare the firmware data for the firmware update.

   Refer to "2.5.1 Prepare Firmware Data for a Firmware Update."

2. Import the firmware data into ISM for the firmware update.

   Refer to "2.5.2 Import Firmware Data into ISM."

3. Update the firmware.

   Refer to "2.5.3 Update Firmware."

2.5.1 Prepare Firmware Data for a Firmware Update

Obtain the latest firmware data to apply to a managed node.

There are two ways to store the firmware data that is applied to managed nodes in the repository:

- Import a firmware data ISO image file from the provided DVD into the repository
- Import the firmware data for each node from the FUJITSU website into the repository

The firmware data for the PRIMERGY BIOS/iRMC can be found in the locations listed in the chart below.

Prepare the DVD and the firmware data listed in the chart below. If the data is in DVD format, prepare the appropriate ISO image files.

Table 2.4 Firmware data to be prepared (When updating PRIMERGY)

Target firmware	Firmware Type (sort)	Firmware data to be used/Location from which to obtain
iRMC of PRIMERGY	iRMC	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website

Target firmware	Firmware Type (sort)	Firmware data to be used/Location from which to obtain
		https://support.ts.fujitsu.com/ [Note 2]
BIOS of PRIMERGY	BIOS	ServerView Suite Update DVD (11.15.09 version or later) [Note 1] Or the firmware data that can be downloaded from the following website https://support.ts.fujitsu.com/ [Note 2]

[Note 1]: To obtain the ServerView Suite Update DVD image, refer to the following website:
https://support.ts.fujitsu.com/IndexDownload.asp?lng=com&SoftwareGUID=

ISM supports the versions of 11 (11.15.09 or later), 12, 13, 14 (except 14.21.09), 15, and 16 of the ServerView Suite Update DVD.

[Note 2]: Download Flash File.

Point

The firmware data to be used depends on the firmware update target.

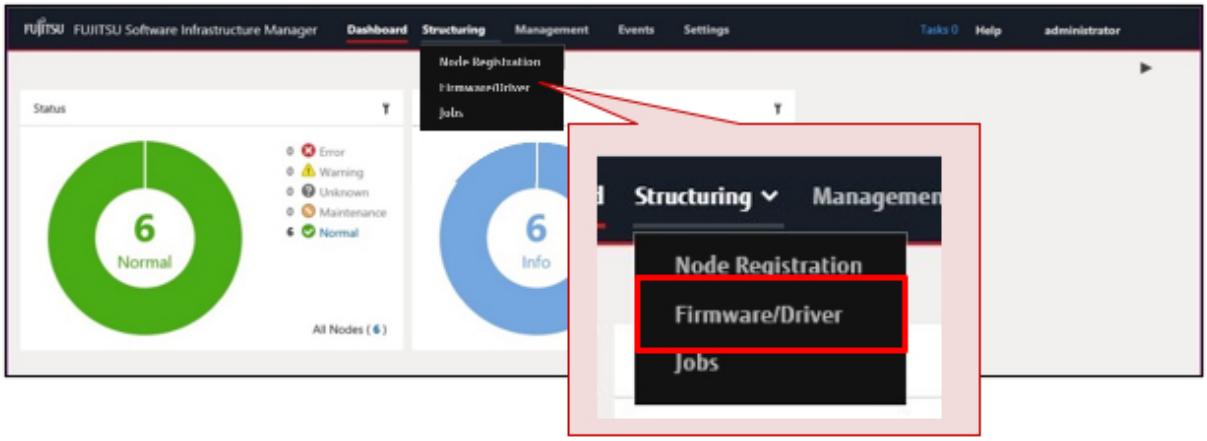
For details on firmware data preparation for firmware other than the firmware in the "Table 2.4 Firmware data to be prepared (When updating PRIMERGY)," refer to "2.13.2.1 Storing and deleting firmware data" in "User's Guide."

2.5.2 Import Firmware Data into ISM

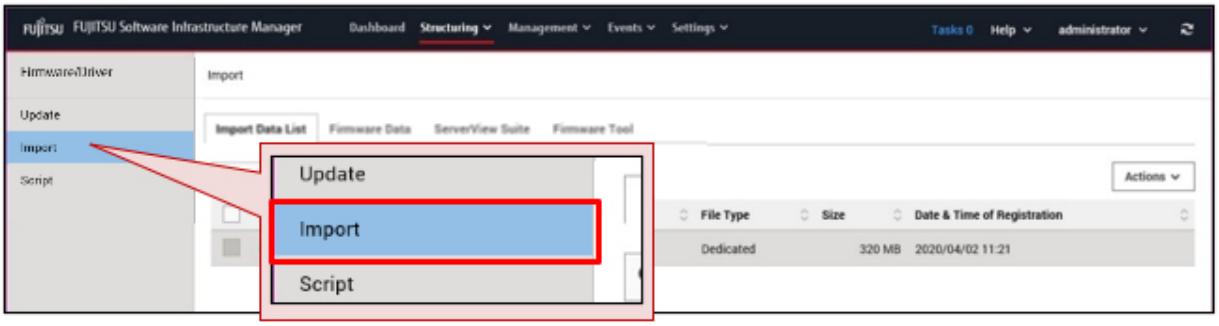
This section describes the procedure to import firmware data that was prepared in "2.5.1 Prepare Firmware Data for a Firmware Update."

This is the procedure for importing firmware data from the DVD.

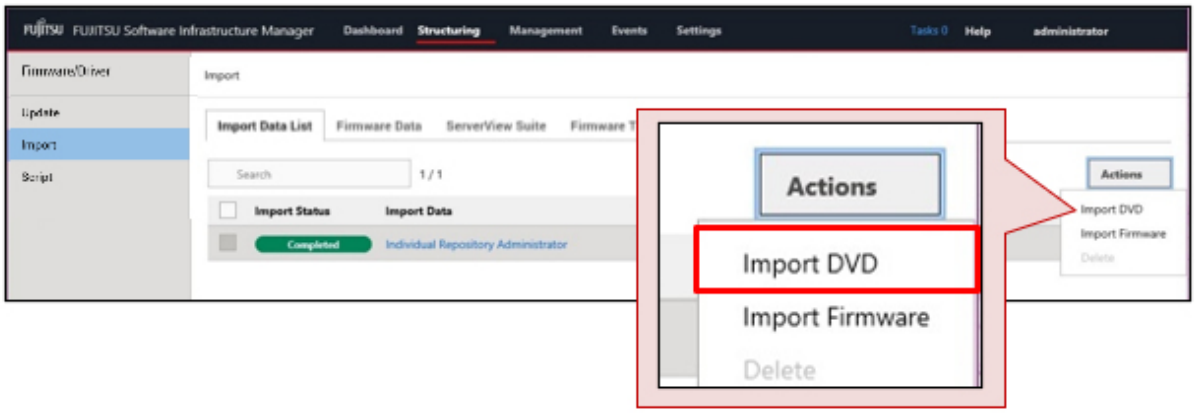
1. From the Global Navigation Menu, select [Structuring] - [Firmware/Driver].



2. From the menu on the left side of the screen, select [Import].



3. From the [Actions] button on the [Import Data List] tab, select [Import DVD].



4. Enter the items to select the firmware data on the "Import DVD Image (ISO)" screen, and then select the [Apply] button.

   For a description on the setting items, select [⑦] on the upper-right of the screen, and refer to the help screen.

   The firmware data is imported from the DVD.

Point

DVD import may take some time to complete. After starting the import, the operations are registered as ISM tasks. Confirm the current status of the task on the "Tasks" screen.

When you select [Tasks] from the top of the Global Navigation Menu, a list of tasks is displayed.

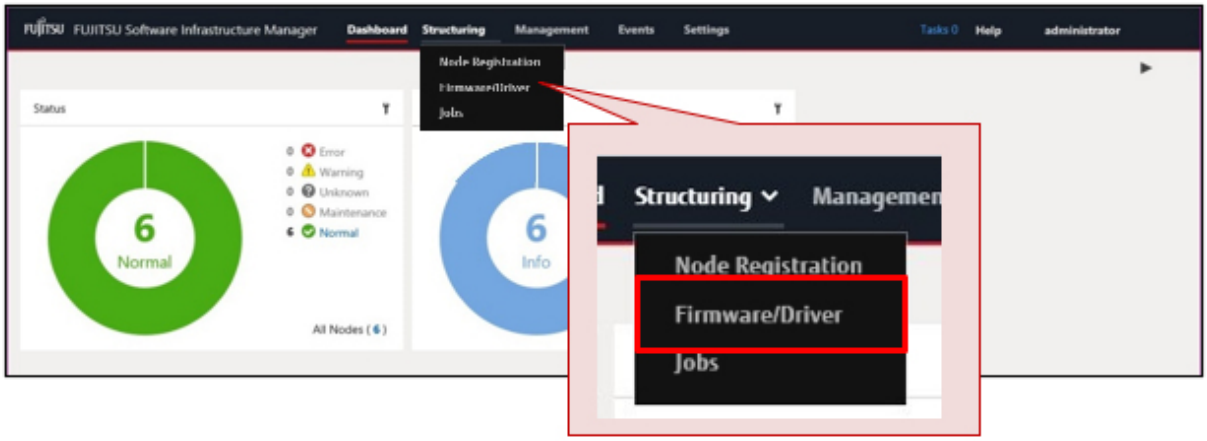
2.5.3 Update Firmware

This section describes the procedure for updating the PRIMERGY BIOS/iRMC using the firmware data that was imported in "2.5.2 Import Firmware Data into ISM."

Note

Do not perform operations that interrupt nodes that are updating (such as turning the power off).

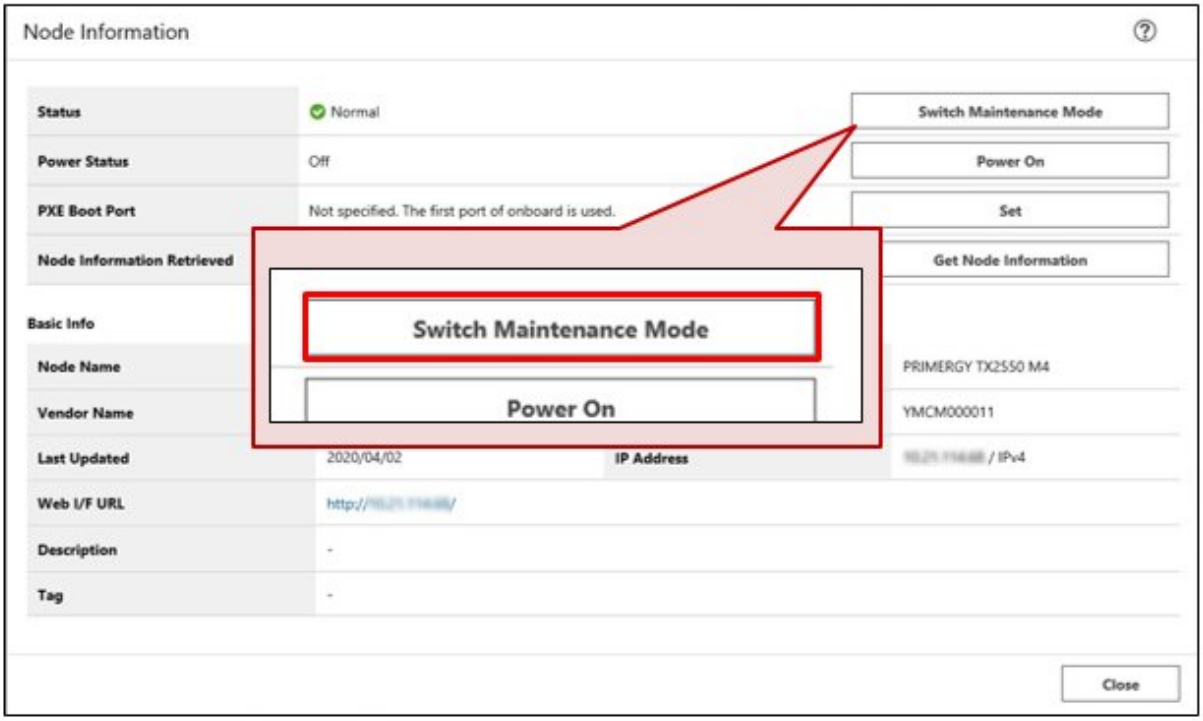
1. From the Global Navigation Menu, select [Structuring] - [Firmware/Driver].



2. Set the node to be updated to Maintenance Mode.

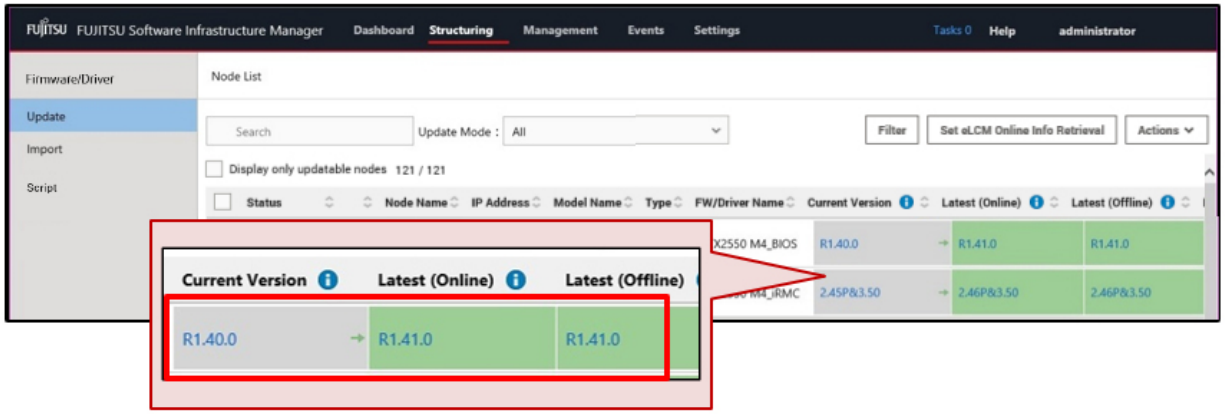
   a. On the "Node List" screen, select the node name.

   b. On the "Node Information" screen, select the [Switch Maintenance Mode] button.



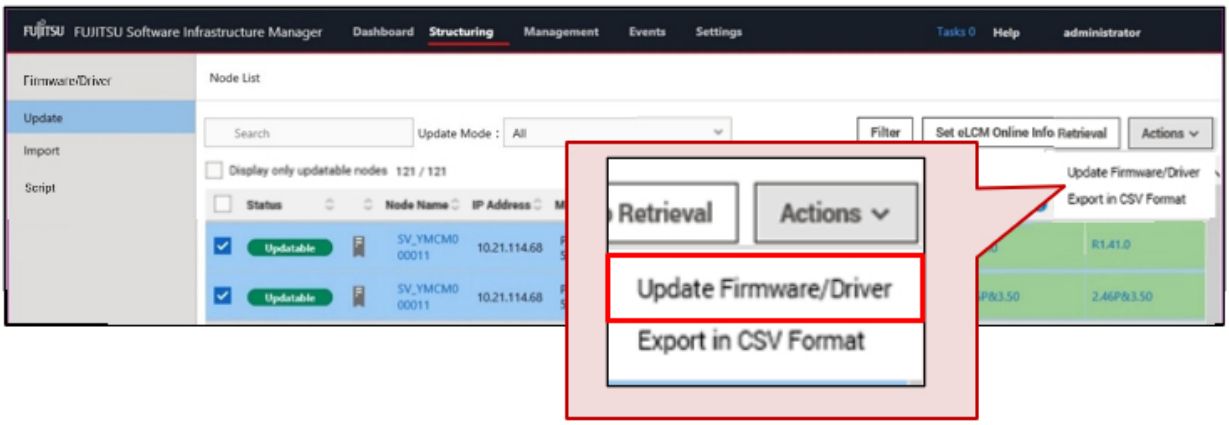
3. On the "Node List" screen, confirm the "Current Version" and the "Latest Version" for the node to be updated.

   "Updatable" is displayed in [Status] for nodes that can be updated (there is a difference between "Current Version" and "Latest Version," the firmware data for "Latest Version" has been imported to ISM).



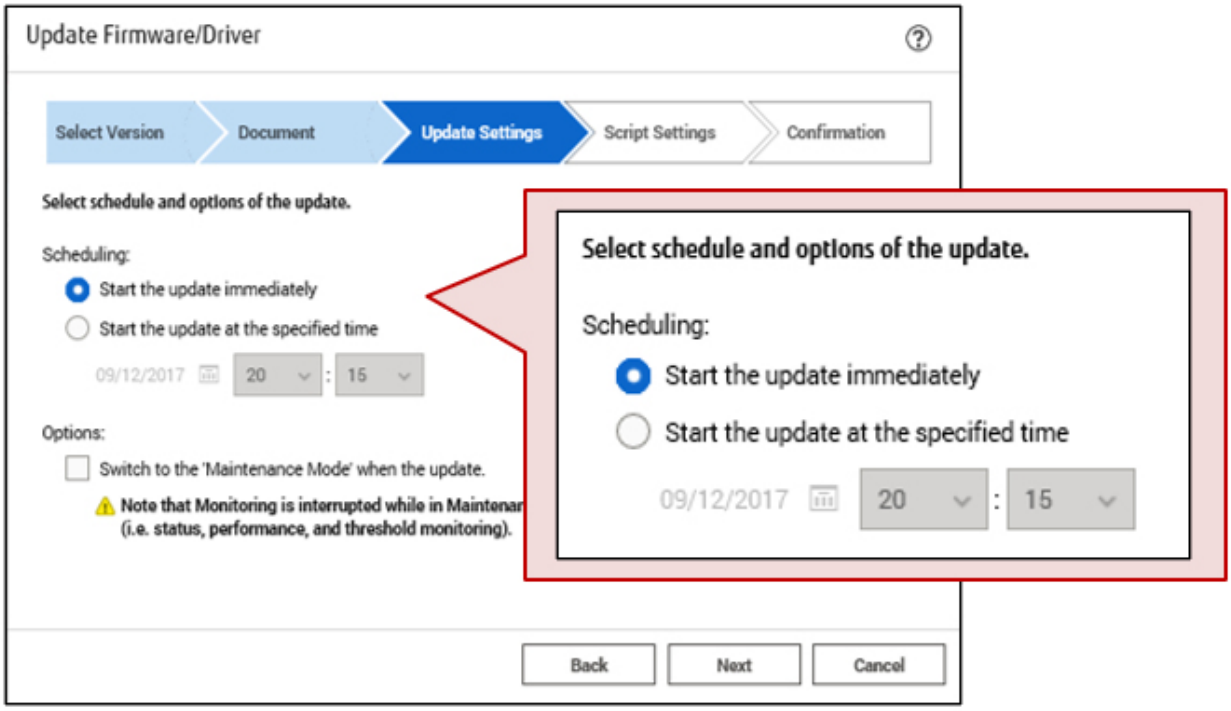
4. Select the checkbox for the node to be updated, and then from the [Actions] button, select [Update Firmware/Driver].

   You can select multiple nodes.



5. Follow the "Update Firmware/Driver" wizard and execute the operations according to the instructions on the screen.

   You can schedule a firmware update in "Update Settings" screen in the "Update Firmware/Driver" wizard.



   - If specifying a date and time for firmware updates

     Select [Start the update at the specified time], and specify the date and time for execution.

     Check the operation status on the "Jobs" screen since it is registered as an ISM job.

     The job ID is displayed in the "List of Jobs" field in the result confirmation dialog box displayed after execution. The job list is displayed when you select [Structuring] - [Jobs] from the Global Navigation Menu. Identify the job based on its job ID.

   - If you selected [Start the update immediately] and the firmware was updated

     After starting the update, since the task is registered as a "Task" in ISM, confirm its current status on the "Tasks" screen. After executing the update, the "Task Details" field in the dialog box for confirmation of the result displays the task ID.

     The following tasks types are registered under Firmware Update tasks.

- Online Update: Updating firmware
- Offline Update: Updating firmware (Offline mode)

When you select [Tasks] from the top of the Global Navigation Menu, a list of tasks is displayed. Identify the appropriate task by its task ID and task type.

6. After confirming that the task is complete, turn off Maintenance Mode for the target node.

This finishes the server firmware update.

Chapter 3 Maintaining ISM

This chapter describes how to handle common problems in ISM, backup the ISM environment in case of trouble during operation, and the countermeasures for errors that may occur with ISM functions.

Point

- A console (a command-line interface for operating ISM-VA) is used for ISM maintenance operations. For details, refer to "User's Guide."
- Only ISM administrators can perform maintenance operations.

3.1 Update ISM

If you need patches, upgrades, or MIB files for ISM, contact your local Fujitsu customer service partner.

3.1.1 Apply Patches to ISM-VA

This section describes the procedure to transfer a patch file (ISM280_xxx_Sxxxxxxxx-xx.tar.gz) to "/Administrator/ftp" for ISM-VA and to apply the patch.

You can upload a patch file to ISM-VA from a management terminal using the ISM GUI. After uploading the file, you can then apply the patch by using the console.

Note

- Before applying patches, back up (export) with a hypervisor, where ISM is running.
- If you have upgraded to ISM 2.9.0 from ISM 2.7.0.030 and earlier and you have not used the system update command, you cannot use Log Management after applying the patch.

  You must execute the command after restarting ISM-VA to be able to use Log Management. Refer to Step 12 and Step 13 for details on running the system update command.
- ISM-VA disk space is used for system updates. For disk space requirements, refer to "System updates after applying a patch or upgrade" in "1.3.1 Requirements for Hypervisor to Run ISM-VA (Virtual Machines)" in "User's Guide."

Point

The following is an overview of the patch process.

1. (Step 1 - 3): Determine the amount of disk space required to apply the patch.
2. (Step 4 - 11): Procedure to apply the patch.
3. (Step 12 - 13): Procedure to update the system.

1. Confirm the amount of disk space required for when the patch is applied.

   a. Log in to ISM-VA from the console as an administrator and execute the following command.

   ```
   # apply-update
   ```

   One of the following messages is displayed. (The sentences after the * are not actually displayed on the screen.)
   If (Message 3) is displayed, Steps b to d are not needed.

   (Message 1)

```
Ready to start System update.

Number of total node logs: 75416                          *Number of node logs for all nodes
Disk size required for system updates: 31.1MB             *Amount of disk space required
Size of available space: 20.8MB                           *Current available disk space
Not Enough hard disk space for system update without deleting Node Log.
If system update without deleting Node Log, after selection “0: Cancel System Update” please
free at least an additional 31.1MB of disk space on ‘/’ .
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
menu below.

1: System Update (Delete Node Log)
0: Cancel System Update
Please select one of the mode:
```

Point

If "Disk size required for system updates" appears in the message, the node logs must be deleted during the system update due to lack of disk space.
If you want to keep past node logs, execute one of the following.

- Confirm the amount of space in "Size of available space" (Current available disk space) and free up memory until you have the amount of space mentioned in "Disk size required for system updates."
- Refer to "2.5.6 Downloading Node Logs" in "User's Guide" to download node logs beforehand.

(Message 2)

```
Ready to start System update

Number of total node logs: 27364                        *Number of node logs for all nodes
Time of System update depends on the number of Node log.
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
menu below.
"Delete Node Log" contributes to shortening of System upgrade.

1: System Update (Delete Node Log)
2: System Update (Node Log Undeleted)
0: Cancel System Update
Please select one of the mode:
```

(Message 3)

```
Your system is up to date.
```

b. Confirm the number (Number of node logs for all nodes registered in ISM) in the "Number of total node logs" row.

c. Select "0: Cancel System Update" to close the message.

d. Calculate the required disk space using the following formula.

   <Number confirmed in Step b> x 500 Bytes

2. Log in to ISM-VA from the console as an administrator, check the system space (entire ISM-VA), and free disk space for the Administrator user group.

```
# ismadm volume show -disk
```

To determine the amount of free disk space in the system (entire ISM-VA), see "Avail" in the "/" mount location.

If you have allocated virtual disks to the Administrator user group, also check the free disk space in the Administrator user group.

Refer to "Avail" in the "'RepositoryRoot'/Administrator" mount location for free disk space for the Administrator user group.

3. Add the disks required for when the patch is applied.

   Determine how much disk space is required to apply the patch based on the disk space calculated in Step 1 and the size of the patch file.

   - If no virtual disk is allocated to the Administrator user group

     Free space required for the system (entire ISM-VA):

     The total of the "capacity calculated in Step 1" and the "capacity approximately six times the patch size"

   - If virtual disks are allocated to the Administrator user group

     - Free space required for the system (entire ISM-VA):

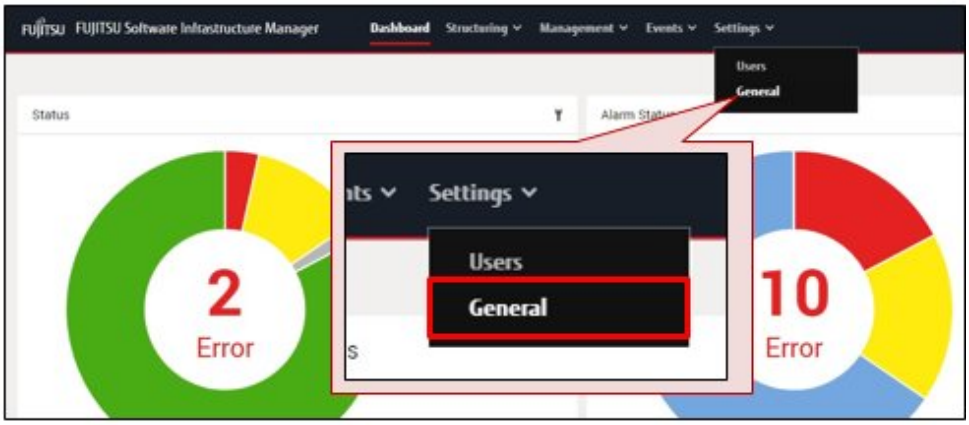
       "About three times the patch size"

     - Administrator user group requires:

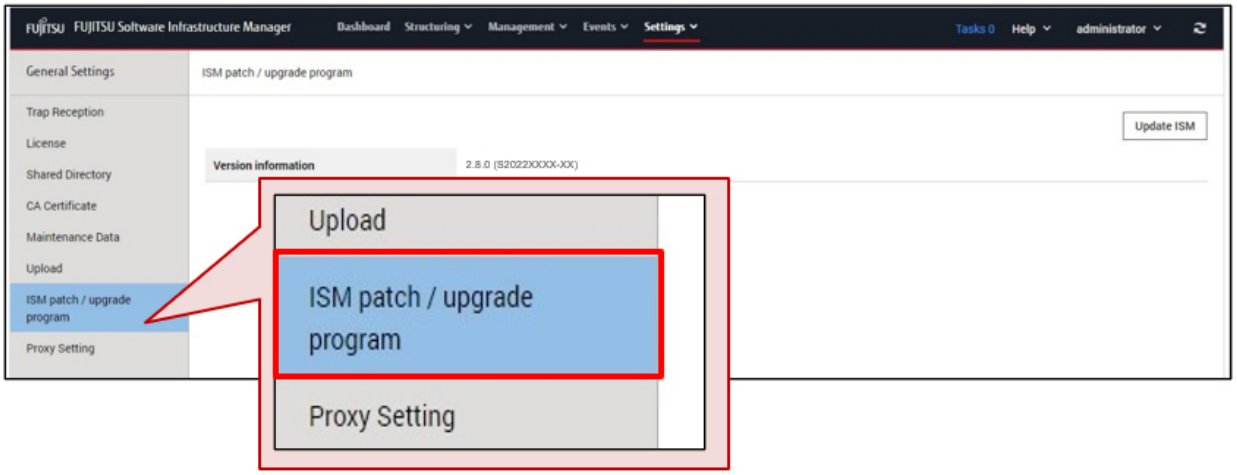
       The total of the "capacity calculated in Step 1" and the "capacity around three times the patch size"

   If you run out of space, add virtual disks for both the system (entire ISM-VA) and the Administrator user group. Refer to "3.7 Allocation of Virtual Disks" and "4.6 Management of Virtual Disks" in "User's Guide" to add virtual disks.

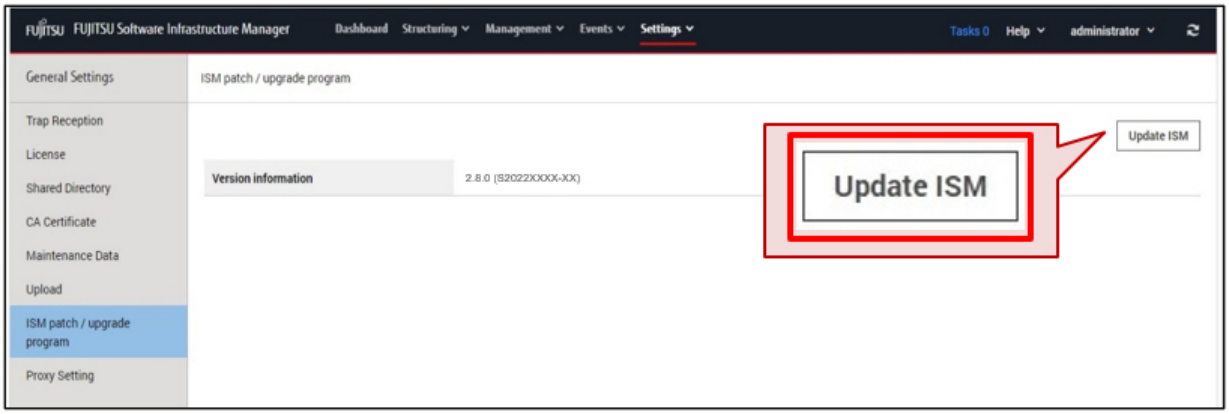
4. From the Global Navigation Menu, select [Settings] - [General].



5. From the menu on the left side of the screen, select [ISM patch / upgrade program].

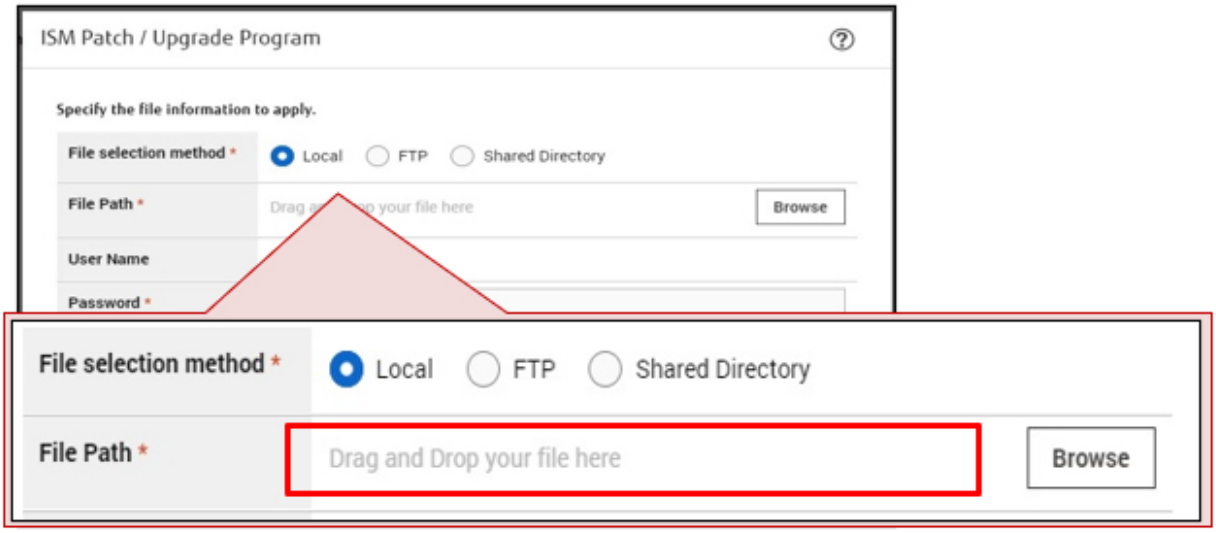


6. Select the [Update ISM] button.

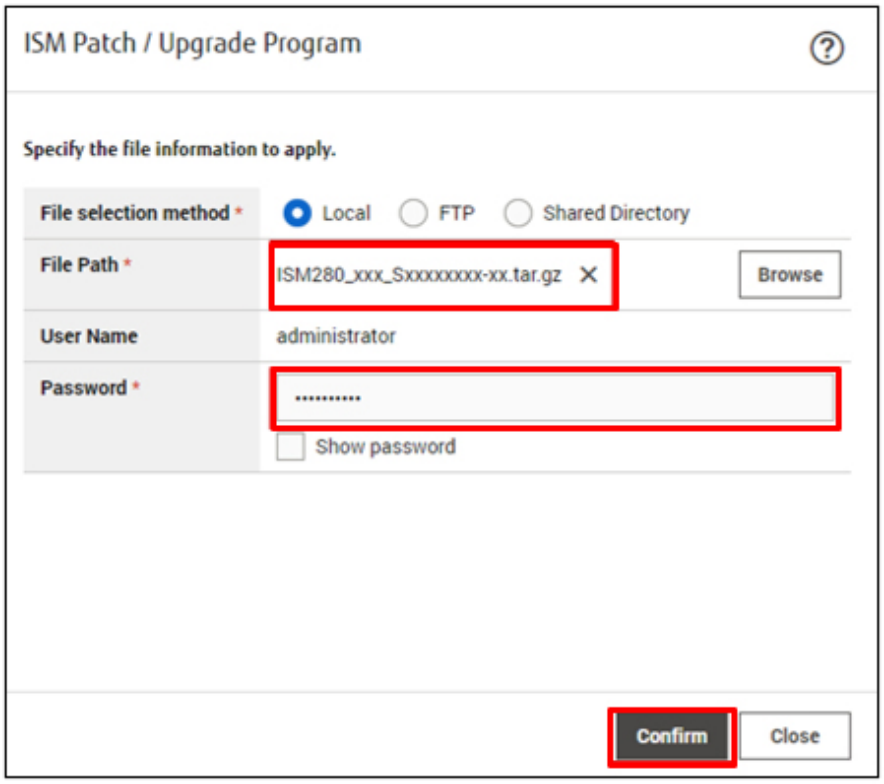


The "ISM Patch / Upgrade Program" screen is displayed.

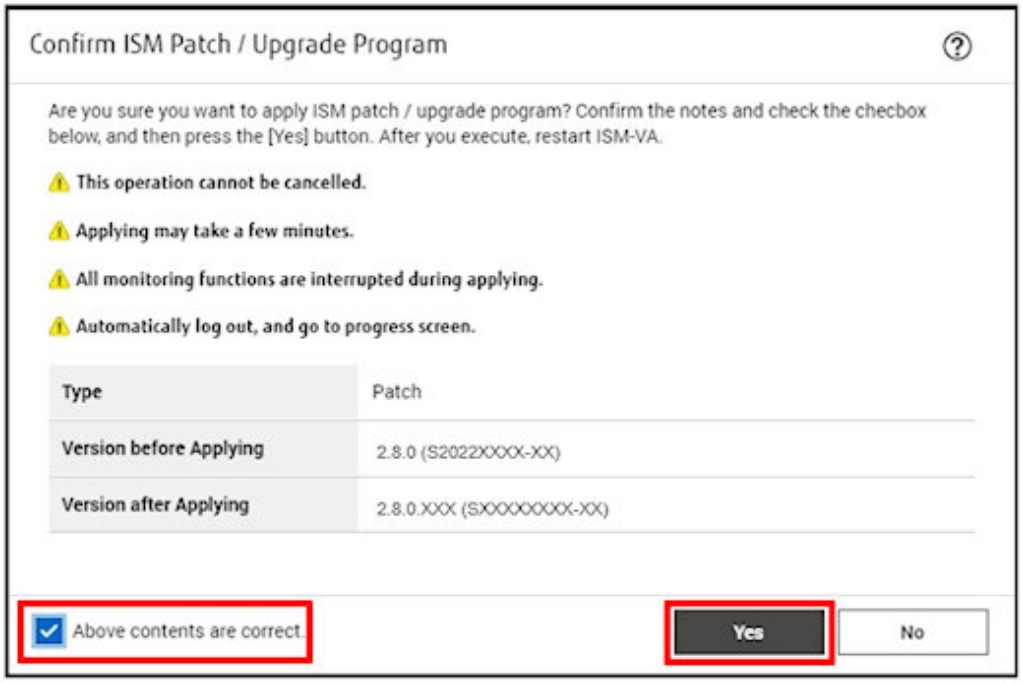
7. Select "Local" from [File selection method] and drag and drop the file to upload to the GUI of ISM.



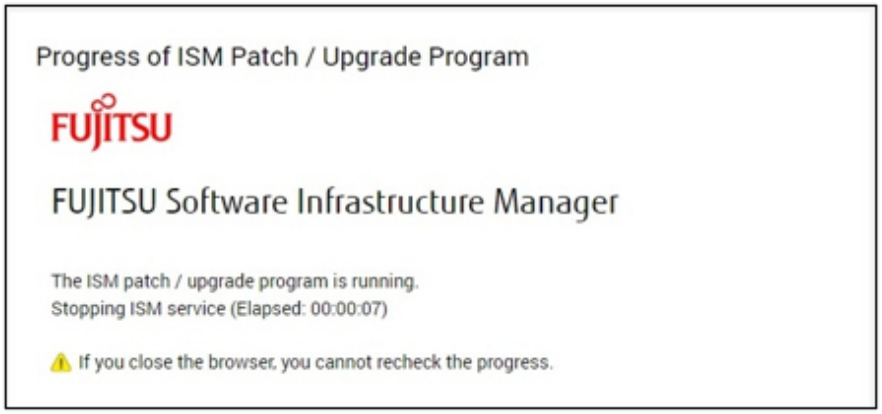
8. Enter your login password in [Password] and select the [Confirm] button.



9. Check the display contents, select the [Above contents are correct] checkbox and select the [Yes] button.

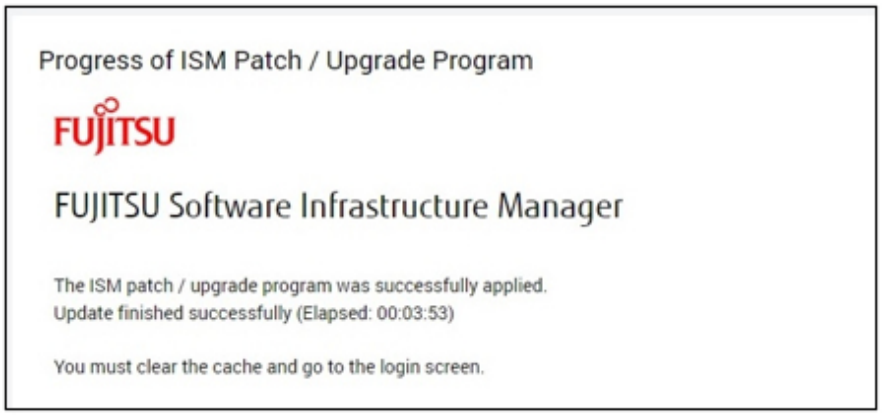


The ISM patch is applied.

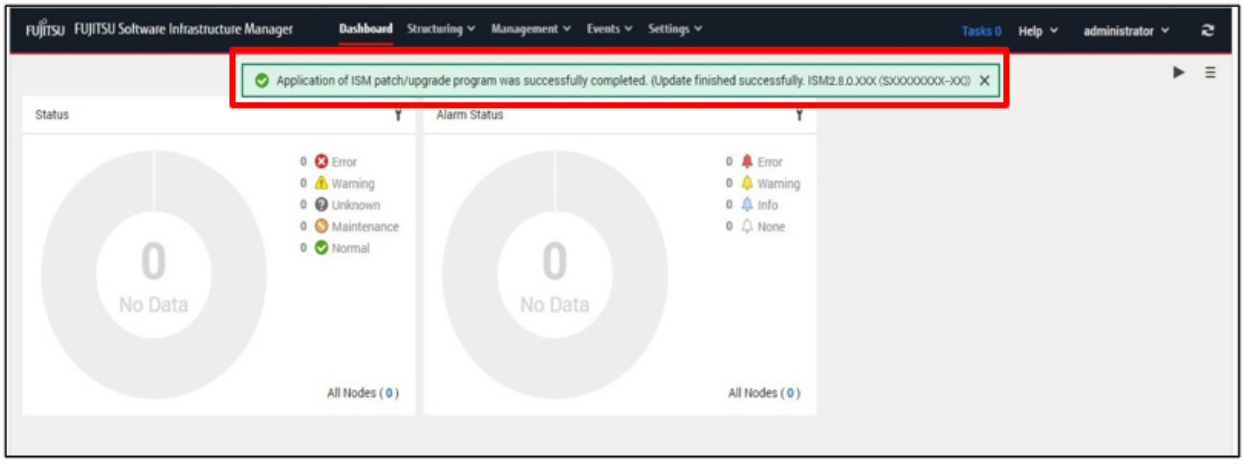


10. Wait until application of the patch is completed.

    After application of the patch is completed, clear the cache, and go to the login screen.



11. After logging into ISM, confirm that the patch is applied.



12. Log in to ISM-VA from the console as an administrator and execute the following command.

```
# apply-update
```

    If the following message is displayed, the system is already up to date. The procedures below are not required.

```
Your system is up to date.
```

If the following message is displayed, you must update the system.

- If there is enough disk space required to save node logs

```
Ready to start System update

Number of total node logs: 27364
Time of System update depends on the number of Node log.
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
menu below.
"Delete Node Log" contributes to shortening of System upgrade.

1: System Update (Delete Node Log)
2: System Update (Node Log Undeleted)
0: Cancel System Update
Please select one of the mode:
```

- If there is not enough disk space required to save node logs

```
Ready to start System update.

Number of total node logs: 75416
Disk size required for system updates: 31.1MB
Size of available space: 20.8MB
Not Enough hard disk space for system update without deleting Node Log.
If system update without deleting Node Log, after selection “0: Cancel System Update” please
free at least an additional 31.1MB of disk space on ‘/’ .
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the
menu below.

1: System Update (Delete Node Log)
0: Cancel System Update
Please select one of the mode:
```

For more details, refer to "4.17 Application of Patches" in "User's Guide."

The system update process continues in the background.

Note

- Do not turn off ISM-VA during a system update. In the unlikely event that ISM-VA is rebooted, restore to a version of ISM-VA that was backed up before the patch was applied.
- During a system update, if you perform an operation that uses a lot of system space, such as a DVD import, the system update may fail. In this case, perform the system update again.

13. From the Global Navigation Menu on the ISM GUI, select [Events] - [Events].
On the [Operation Log] tab, confirm that a log with the message ID "10140003" is output.

    The system update is complete if the "10140003" log is output.

    Point

    The system update failed if the "50140050" log is output.

    Collect maintenance data for ISM and contact your local Fujitsu customer service partner.

    This finishes the procedure for applying the patches to ISM-VA.

3.1.2 Upgrade ISM-VA

You can upload an upgrade file to ISM-VA from a management terminal using the ISM GUI and perform the upgrade.

Note

- If you want to upgrade from V1.0 - V1.5 to V2.9, contact your local Fujitsu customer service partner.
- Before upgrading, back up (export) with a hypervisor, where ISM is running.
- If you have upgraded from ISM 2.7.0.030, you cannot use Log Management.

  You must execute the command after restarting ISM-VA to be able to use Log Management. For details on executing the command, refer to "4.18 Upgrade of ISM-VA" in "User's Guide."
- ISM-VA disk space is used for system updates. For disk space requirements, refer to "System updates after applying a patch or upgrade" in "1.3.1 Requirements for Hypervisor to Run ISM-VA (Virtual Machines)" in "User's Guide."

1. Calculate the amount of disk space required for when the patch is applied.
   a. From the Global Navigation Menu on the ISM GUI, select [Management] - [Nodes].
   b. Select the node name on the "Node List" screen.
   c. On the Details of Node screen, select the [Properties] tab, and check the number of logs displayed in "Node Logs."
   d. Add up the number of Node Logs for all nodes registered with ISM and use the following formula to calculate the required disk space.

      ```
      <Number of Node Logs for all nodes> x 500 bytes
      ```
2. For the rest of the procedures, execute from Step 2 in "3.1.1 Apply Patches to ISM-VA."

   Read "patch" as "upgrade

3.1.3 Set up an MIB File

MIB is public information regarding the status of network devices managed with SNMP, and is standardized as MIB-II, which is published as RFC 1213. An MIB file is a text-based file that defines this public information. To send and receive SNMP traps, the receiving side is required to save an MIB file provided by the device side.

Add/update the MIB file in the following cases.

- If you want to add a new MIB file to receive SNMP traps from the hardware supplied from a vender other than Fujitsu such as ISM unsupported Fujitsu devices, Cisco switches, or HP servers.
  For the latest information on products supported by ISM V2.9.0, refer to "Support Matrix."
  https://support.ts.fujitsu.com/index.asp
  Select [Select a new Product] on the above site and enter "Infrastructure Manager" in [Product Search:].
  Select [DOWNLOADS] and select the target operating system.
  The reference procedures are subject to change without notice.
- If you want to update an MIB file already registered in ISM to execute a firmware update.

You can upload an MIB file to ISM-VA from a management terminal using the ISM GUI. After uploading the file, you can register the MIB file by using the console.

1. Upload the MIB file to ISM-VA from a management terminal using the ISM GUI.
   a. From the Global Navigation on the ISM GUI, select [Settings] - [General].
   b. From the menu on the left side of the screen, select [Upload].
   c. Select a root directory from the list.
   d. From the [Actions] button, select [Upload File].

      On the "Upload File" screen, select the following.

      - File Type: MIB file
      - Upload Target Path: /Administrator/ftp/mibs

e. Select the [Apply] button.

2. From the console as an ISM administrator, log in to ISM-VA.
3. Execute MIB file registration command.

```
# ismadm mib import
```

Point

You can display and delete the MIB files registered on ISM-VA by using the following commands.

- Display MIB files

```
# ismadm mib show
```

- Delete MIB files

```
# ismadm mib delete -file <MIB file name>
```

3.2 Backup and Restoration of ISM

You can back up the ISM settings and node registration data and restore them as necessary in case the ISM setting data is damaged due to a problem or the setting data is lost due to an operation error.

The following methods can be used to back up/restore ISM:

- Backup/restoration of ISM using the ISM-VA management command

  For the procedure for backups, refer to "8.1.1.2 Back up ISM using the command" in "Operating Procedures."
  For the procedure for restorations, refer to "8.1.2.2 Restore ISM using the command" in "Operating Procedures."

- Backup/restoration of ISM using the GUI (ISM 2.9.0.010 or later)

  For the procedure on backups, refer to "8.1.1.1 Back up ISM using the GUI " in "Operating Procedures."
  For the procedure on restorations, refer to "8.1.2.1 Restore ISM using the GUI" in "Operating Procedures."

- Backup/restoration of ISM using the REST API (ISM 2.9.0.010 or later)

  Refer to "REST API Reference Manual."

Point

When migrating a server with ISM, backup/restoration of the entire ISM-VA using a hypervisor is effective.

ISM-VA is running as a virtual machine. You can migrate the server using the export/import functions of the hypervisor where ISM-VA (virtual machine) is running. However, the source and the destination of hypervisors must be the same.

ISM-VA can operate on the following hypervisors:

- Windows Server
- Azure Stack HCI OS
- VMware ESXi
- Red Hat Enterprise Linux with KVM installed
- SUSE Linux Enterprise Server with KVM installed
- Nutanix AHV

3.3 Collection of Maintenance Data

You can collect maintenance data required for investigations when a failure has occurred in ISM.

There are two ways to collect the maintenance data of ISM, one is using the GUI and the other is using a command.

You can collect a vc-support log from vCenter if vCenter is registered in the cloud management software in ISM when Virtual Resource Management maintenance data is required.

3.3.1 Collect Maintenance Data with the GUI

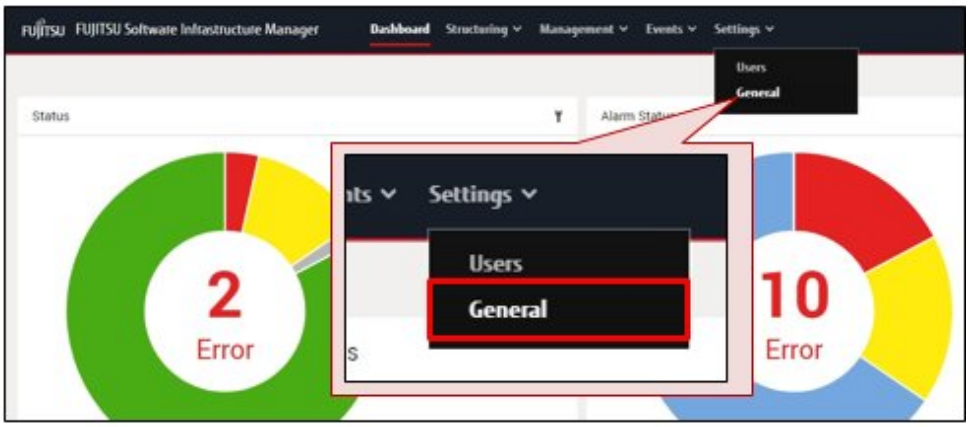
Log in to the ISM GUI to collect and download the maintenance data with the following procedure.

Collect maintenance data

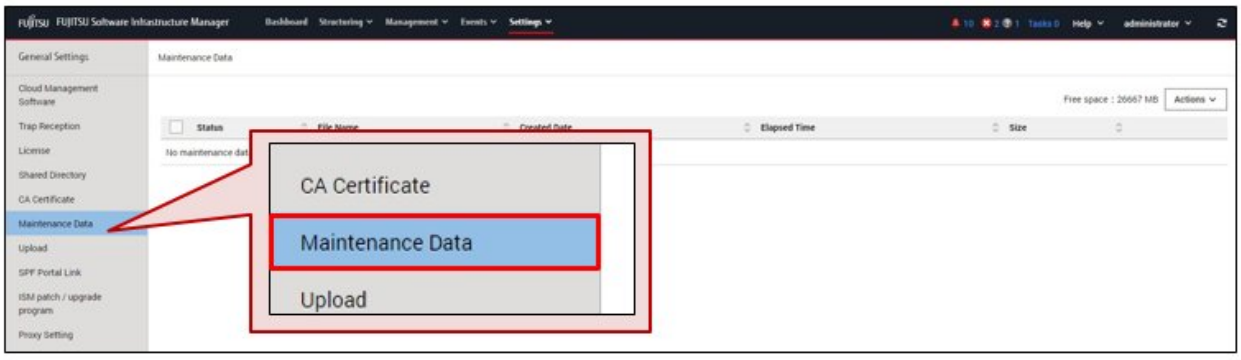
Note

Batch collection of maintenance data takes several hours to complete and requires large amounts of free disk space. For details, refer to "3.2.1.5 Estimation of required disk space for maintenance data" in "User's Guide."

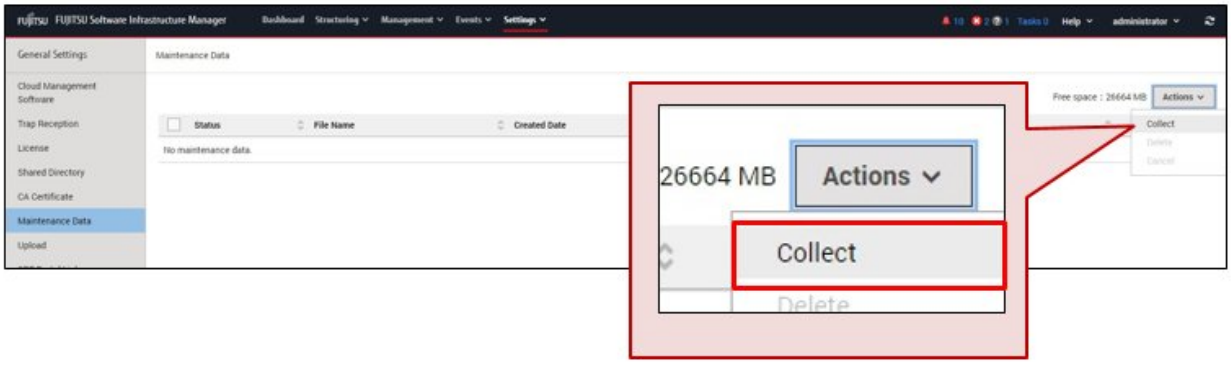
1. From the Global Navigation Menu, select [Settings] - [General].



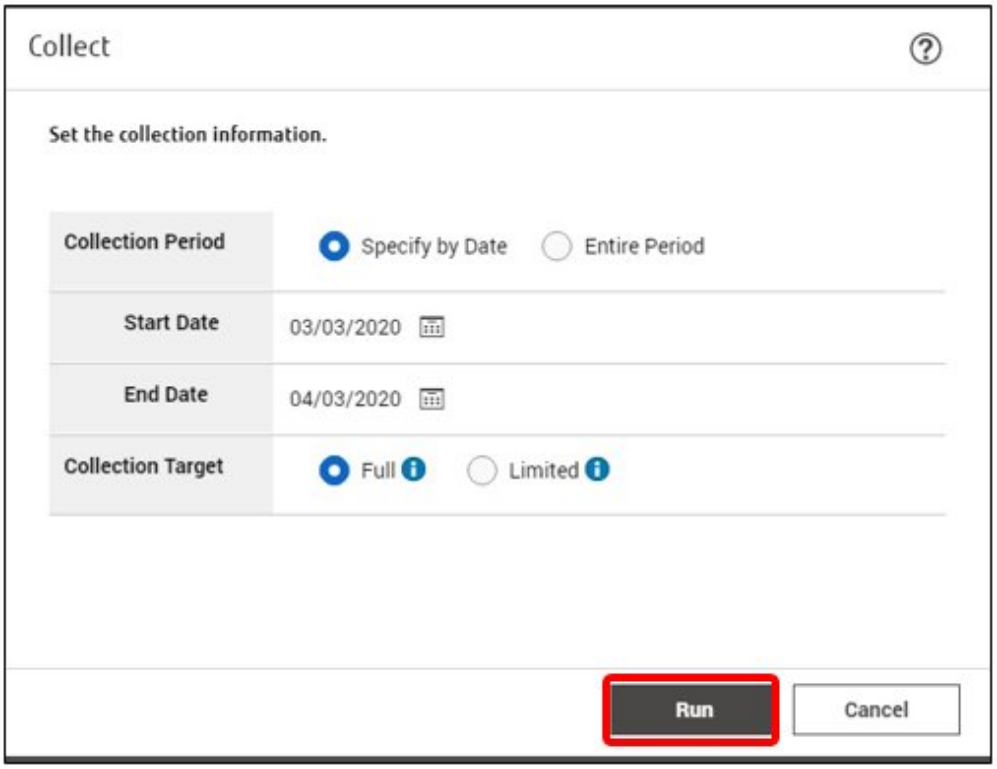
2. From the menu on the left side of the screen, select [Maintenance Data].



3. From the [Actions] button on the "Maintenance Data" screen, select [Collect].

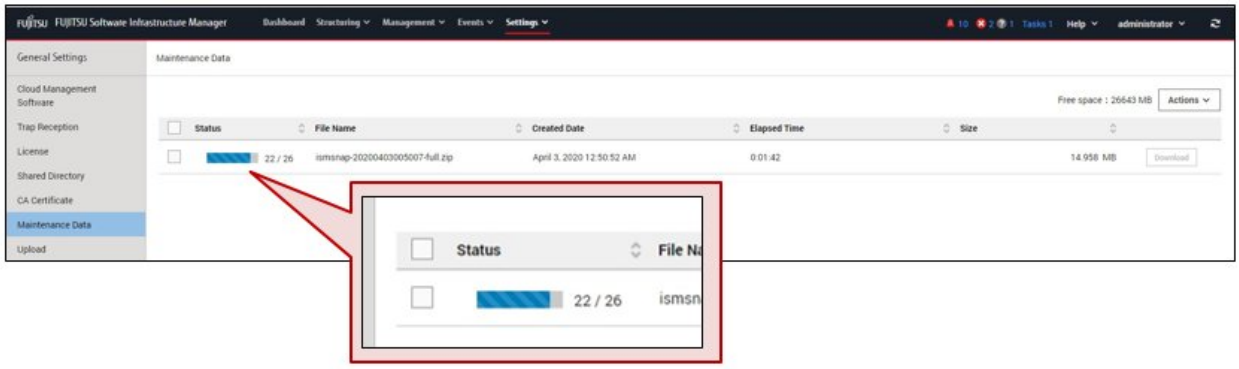


4. Select Collection Period and Collection Target on the "Collect" screen, and then select the [Run] button.



- Collection Period
  - Entire period
  - Specify by Date: Specify Start Date and End Date for collection
- Collection Target
  - Full: Collection of ISM RAS Logs, ISM-VA Operation System Logs, and database information together
  - Limited: Collection of ISM RAS Logs only

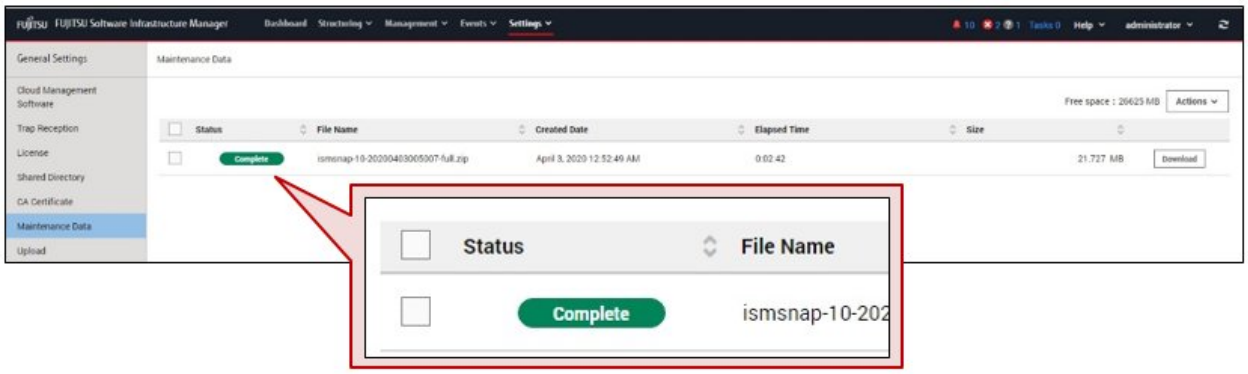
Collection starts and the progress of the collection is displayed in the [Status] column.



To refresh the displayed progress, select the [Refresh] button on the upper-right of the screen on the ISM GUI.

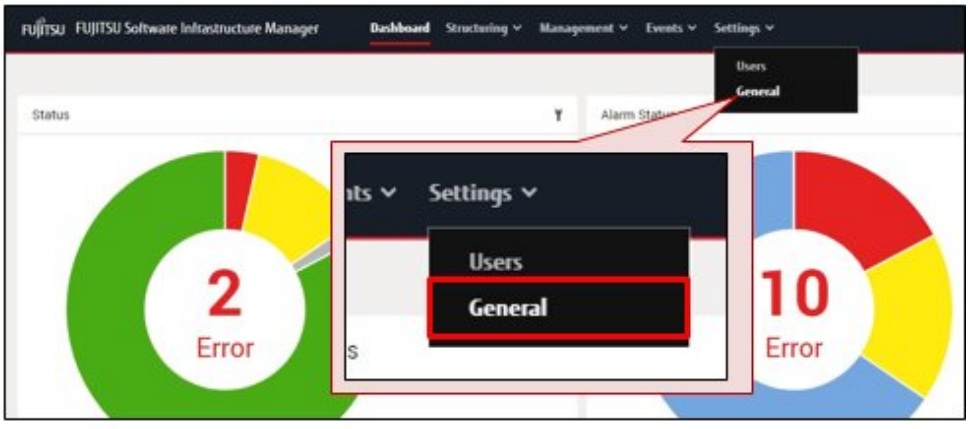
The progress can also be checked from the "Task" screen. The task type is "Collecting Maintenance Data."

When the collection is complete, the Status icon becomes "Complete" and you can download the data.

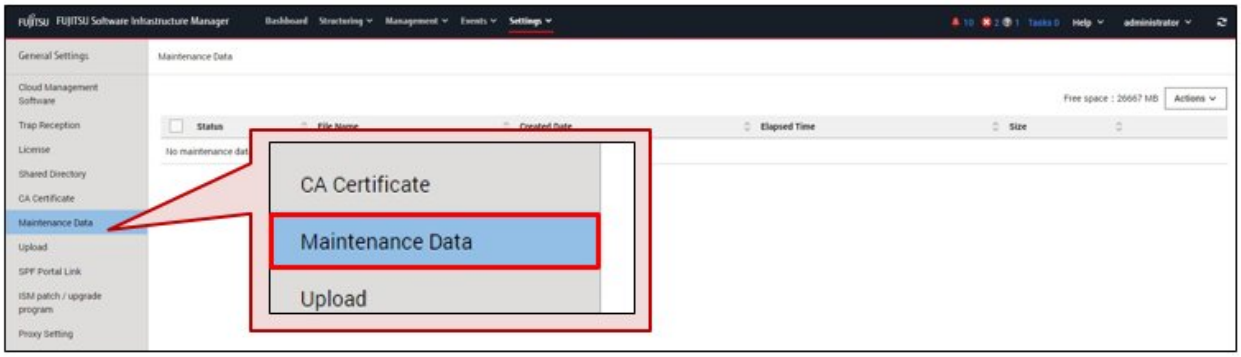


Download maintenance data

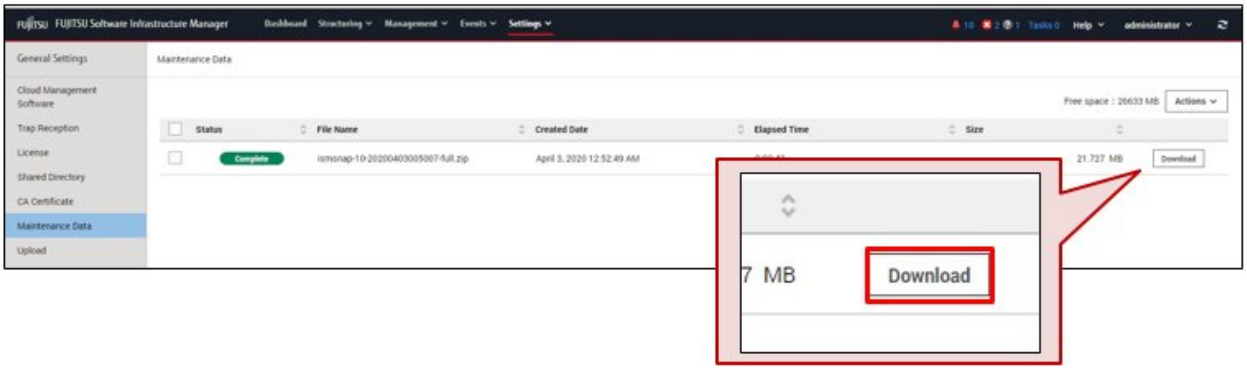
1. From the Global Navigation Menu, select [Settings] - [General].



2. From the menu on the left side of the screen, select [Maintenance Data].



3. On the "Maintenance Data" screen, select the [Download] button of the maintenance data that you want to collect.



4. Download the maintenance data according to the download confirmation of the browser.

Note

- The maintenance data collected from the "Maintenance Data" screen in GUI of ISM are retained in the following directory and only the maintenance data under this directory will be displayed.

  Maintenance Data storage directory: /Administrator/transfer

  The maintenance data retained in the FTP communication directory of ISM-VA, "/Administrator/ftp," are not displayed on the "Maintenance Data" screen.

- The maintenance data will be retained for five generations. If it exceeds five generations, it will be deleted automatically from the oldest creation date and time.

- The maintenance data will be deleted automatically 5 weeks after collected.

3.3.2 Collect Maintenance Data Using a Command

Use the ISM-VA commands to collect ISM maintenance data.

Note

Batch collection of maintenance data takes several hours to complete and requires large amounts of free disk space. For details, refer to "3.2.1.5 Estimation of required disk space for maintenance data" in "User's Guide."

1. After starting ISM-VA, log in to ISM-VA from the console as an ISM administrator.

2. Collect the ISM maintenance data.

   The following are part of some examples. Refer to "8.2.2 Collect Maintenance Data to Execute the Command" in "Operating Procedures."

   - For the batch collection of ISM RAS Logs, ISM-VA Operating System Logs, and database information with a collection period (2021/12/10 to 2022/1/10) specified.

     ```
     # ismadm system snap -dir /Administrator/ftp -full -from 20211210 -to 20220110
     snap start
     Your snap has been generated and saved in:
      /Administrator/ftp/ismsnap-20220110175808-20211210-20220110-full.zip
     ```

   - For the batch collection information of ISM RAS Logs, ISM-VA Operating System Logs, database information, collected statistics information by Anomaly Detection and Packet Analysis of Virtual Network (collection period required).

     A collection period (2022/05/18 to 2022/05/19) is specified.

     ```
     # ismadm system snap -dir /Administrator/ftp -full -extstats -from 20220518 -to 20220519
     snap start
     Your snap has been generated and saved in:
      /Administrator/ftp/ismsnap-20220519072513-20220518-20220519-full-extstats.zip
     ```

   Point

   - "-dir" specifies the output destination path. You can retrieve maintenance data collected by FTP access by specifying the file transfer area described in "2.1.2 FTP Access" in "User's Guide."
   - To specify the period of maintenance data to be collected, specify the collection start date and collection end date by adding the "-from" and "-to" options. Specify the date in "YYYYMMDD" format. If you specify the period of maintenance data to be collected, the collection start date and collection end date are added to the file name. The collection start date and collection end date are set based on the time zone set in ISM-VA.

     If no period is specified, maintenance data is collected for the entire period.

3. Access FTP as an ISM administrator from a management terminal, and download the collected maintenance data.

Note

The five latest files are stored in the maintenance data created in the directory where the maintenance data is stored. Use the FTP client software and manually delete maintenance data that are no longer required.

3.3.3 Collect Maintenance Data for Virtual Resource Management

You can collect a vc-support log from vCenter if vCenter is registered in the cloud management software in ISM. For details, refer to "To collect ESX/ESXi and vCenter Server diagnostic data" from the following URL.

https://kb.vmware.com/s/article/2032892

In the log collection procedure in the URL above, when selecting the ESXi hosts to export logs to, select all the vSAN cluster ESXi hosts where an error has occurred.