FUJITSU Software
Systemwalker Operation Manager

Installation Guide

UNIX/Windows(R)

J2X1-8181-04ENZ0(00)
February 2022

Preface

Purpose of This Document

This document describes the Systemwalker Operation Manager installation procedure.

Intended Readers

This document is intended for system administrators who install Systemwalker Operation Manager or perform operation design of Systemwalker Operation Manager.

This document assumes you are familiar with how to work with operating system(s) and GUIs.

Abbreviations and Generic Terms Used

- The term "Windows Server 2019 " is used to refer to all of the following products:
  - Microsoft(R) Windows Server(R) 2019 Standard (x64)
  - Microsoft(R) Windows Server(R) 2019 Datacenter (x64)
- The term "Windows Server 2016" is used to refer to all of the following products:
  - Microsoft(R) Windows Server(R) 2016 Standard (x64)
  - Microsoft(R) Windows Server(R) 2016 Datacenter (x64)
- The term "Server Core" is used to refer to all of the following products:
  - Microsoft(R) Windows Server(R) 2019 Standard Server Core
  - Microsoft(R) Windows Server(R) 2019 Datacenter Server Core
  - Microsoft(R) Windows Server(R) 2016 Standard Server Core
  - Microsoft(R) Windows Server(R) 2016 Datacenter Server Core
- The term "Windows(R) 10" is used to refer to all of the following products:
  - Windows(R) 10 Home (x64)
  - Windows(R) 10 Pro (x64)
  - Windows(R) 10 Enterprise (x64)
- The term "Windows(R) 8.1" is used to refer to all of the following products:
  - Windows(R) 8.1 (x64)
  - Windows(R) 8.1 Pro (x64)
  - Windows(R) 8.1 Enterprise (x64)
- Windows Internet Explorer(R) is abbreviated as "Internet Explorer".
- Versions of Systemwalker Operation Manager that run on all of the following operating systems are referred to as "Windows versions of Systemwalker Operation Manager" or simply "Windows versions":
  - Windows
  - 64-bit versions of Windows, except Itanium
- Articles specific to the version of Systemwalker Operation Manager that runs on 32-bit versions of Windows are referred to as "Windows x86 version".
- Articles specific to the version of Systemwalker Operation Manager that runs on Itanium-compatible versions of Windows are referred to as "Windows for Itanium version".

- Articles specific to the version of Systemwalker Operation Manager that runs on 64-bit versions of Windows, except Itanium, are referred to as "Windows x64 version".
- Server Core, Windows Server 2019, and Windows Server 2016 may be abbreviated as "Windows servers".
- Oracle Solaris may be referred to as Solaris, Solaris Operating System or Solaris OS.
- Versions of Systemwalker Operation Manager that run on Solaris are referred to as "Solaris versions of Systemwalker Operation Manager" or simply "Solaris versions".
- Articles specific to the version of Systemwalker Operation Manager that runs on 32-bit versions of Solaris are referred to as "Solaris 32-bit version".
- Articles specific to the version of Systemwalker Operation Manager that runs on 64-bit versions of Solaris are referred to as "Solaris 64-bit version".
- Versions of Systemwalker Operation Manager that run on HP-UX are referred to as "HP-UX versions of Systemwalker Operation Manager" or simply "HP-UX versions".
- Versions of Systemwalker Operation Manager that run on AIX are referred to as "AIX versions of Systemwalker Operation Manager" or simply "AIX versions".
- Articles specific to the version of Systemwalker Operation Manager that runs on 64-bit versions of Linux, except Itanium, are referred to as "Linux x64 version" or simply "Linux versions".
- Articles specific to the version of Systemwalker Operation Manager that runs on 32-bit versions of Linux are referred to as "Linux x86 version".
- Articles specific to the version of Systemwalker Operation Manager that runs on Itanium-compatible version of Linux are referred to as "Linux for Itanium version".
- Solaris, HP-UX, AIX, Linux and Linux for Itanium versions of Systemwalker Operation Manager are referred to collectively as "UNIX versions of Systemwalker Operation Manager" or simply "UNIX versions".
- Solaris, HP-UX, AIX and Linux may be referred to as "UNIX servers".
- Systemwalker Operation Manager Standard Edition may be abbreviated as "SE".
- Systemwalker Operation Manager Enterprise Edition may be abbreviated as "EE".
- Standard Edition may be abbreviated as "SE" and Enterprise Edition may be abbreviated as "EE".
- Arcserve(R) Backup for Windows is abbreviated as "Arcserve".
- Microsoft(R)-Mail that is provided as a standard feature with Windows NT(R) is abbreviated as "MS-Mail".

Export Restriction

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Trademarks

APC and PowerChute are trademarks or registered trademarks of Schneider Electric IT Corporation.

All products, service name, company name and logo of Arcserve are registered trademark or trademark of Arcserve (USA), LLC.

HP-UX is a registered trademark of Hewlett-Packard Development Company.

AIX and HACMP are trademarks or registered trademarks of International Business Machines Corporation in the United States.

Intel and Itanium are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

MC/ServiceGuard is a registered trademark of Hewlett-Packard Development Company, or L.P.

Microsoft, Windows, Windows Server and Azure, or the name and the product name of other Microsoft product are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Red Hat are registered trademarks of Red Hat, Inc. in the U.S. and other countries.

Linux(R) is a registered trademark of Linus Torvalds in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle Corporation or its subsidiaries in the U.S. and/or other countries.

R/3, SAP and all SAP trade name that are presented are registered trademarks or trademarks of SAP SE in Germany and in several other countries.

UNIX is a registered trademark of The Open Group.

VMware and the VMware logo are registered trademarks or trademarks of VMware in the United States and/or other jurisdictions.

Amazon Web Services, Amazon Elastic Compute Cloud, Amazon CloudWatch and AWS Lambda are trademarks of Amazon.com, Inc. or its affiliated company in the United States and/or other countries.

Short Mail is a registered trademark of NTT DoCoMo, Inc.

In addition, company name and product name may appear in this document are trademarks or registered trademarks of their respective owners.

The use of screenshots follows the guidelines of Microsoft Corporation.

Contents

Chapter 1 Installation of Systemwalker Operation Manager

This chapter explains how to install Systemwalker Operation Manager.

1.1 List of Functions to be Installed

Systemwalker Operation Manager provides server and client functions. The following lists functions to be installed on the server and client.

List of functions to be installed on the server

Installation option	Function name	OS supported	Restrictions (Note 1)
Server (basic)	Calendar	Common	A
	Power control	Common (Note 2)	A
	Starting Services and Applications	Common (Note 3)	A
	Jobscheduler	Common	A
	Job Execution Control	Common	A
	Event Monitoring	Windows system only	A
	Action Management	Windows system only	A
	Backup Linking	Windows system only	A
	Task Linking	Common	A
	Master Schedule Management	Common (Note 4)	A
	Web Console/Web API	Common (Note 5)	A
	Web Console Operation Guide	Common	A
Document	Help	Windows system only	B

Note 1:

A: These functions are always installed. In the Windows system, the entire server functions can be installed if Server Functions of Systemwalker Operation Manager is selected during system installation.

B: Optional functions (Initial values are installed.)

C: Optional functions (No initial values are installed.)

Note 2:

The Power Supply Control using the power control device is available on Windows versions only.

Note 3:

The application startup function only is available on UNIX version.

Note 4:

Windows, Solaris, Linux, HP-UX, and AIX versions are provided only for EE version.

Note 5:

Web API are provided only for Windows and Linux version.

Information

The version/level of Systemwalker Operation Manager to be installed can be confirmed by F3crfver command or swpkginfo command. For details on these commands, see the *Systemwalker Operation Manager Reference Guide*.

List of functions to be installed on a client

Installation option	Function name	OS supported	Restrictions (Note 1)
Operation Manager client	Systemwalker Operation Manager client	Common	A
Action Execution (Voice Notification)	Event Monitoring and Action Management	Windows system only	C (Note 2)
Client (Task Linking)	Client Task Linking	Common	C
Master Schedule Management	Master Schedule Management	Common (Note 3)	B
Document	Help	Common	B

Note 1:

A: Can be installed if **Client Functions of Systemwalker Operation Manager** is selected.

B: Optional functions (Initial values are installed.)

C: Optional functions (No initial values are installed.)

Note 2:

Only some of the functions, such as Audio Notification, are optional.

Note 3:

Windows, Solaris, Linux, HP-UX, and AIX versions are provided only for EE version.

In order to monitor a job net from Systemwalker Centric Manager, you must install the Systemwalker Operation Manager client functions on the Operation Management Server where Systemwalker Centric Manager has been installed.

Information

You can confirm the version/level of installed Systemwalker Operation Manager by selecting **About Systemwalker Operation Manager** from the **Help** menu of the **Systemwalker Operation Manager** window. Moreover, it can be checked also by the F3crfver command. For details on this command, see the *Systemwalker Operation Manager Reference Guide*.

1.2 Tasks from Installation Through Operation

The following shows the standard procedure from installation through operation of Systemwalker Operation Manager.

1. Installation

   Install Systemwalker Operation Manager. For details, see "1.3 Installation in the Windows System", "1.4 Installation in the UNIX System" or "1.5 Silent Installation".

2. Definition of the operating environment and Security Definitions

   Define the operating environment and the security definitions of Systemwalker Operation Manager. For details, see "Chapter 2 Definition of Operating Environment of Systemwalker Operation Manager".

3. Configuration and Operation of Jobs

   Configure and run jobs using Systemwalker Operation Manager.

   For details, refer to the *Systemwalker Operation Manager User's Guide*.

1.3 Installation in the Windows System

This section explains how to install Systemwalker Operation Manager server/clients.

Before starting the system installation, check the following points and take any required actions.

Referring to the related documents

The Release Note and other documents on the Systemwalker Operation Manager product media provide basic notes on Systemwalker Operation Manager. Refer to these files as they have important information you should have.

Checking the operating environment

Check both the hardware and software resources required for operating Systemwalker Operation Manager. Refer to the *Systemwalker Operation Manager Technical Guide* for those resources.

1.3.1 Notes Prior to Installation

Be aware of the following when installing Systemwalker Operation Manager.

Shutdown of services and jobs

All of Systemwalker Operation Manager services are stopped automatically when the system is installed. If it coexists with Systemwalker Centric Manager in the same environment, the Systemwalker Centric Manager services are also stopped. Ensure that none of Systemwalker Operation Manager jobs are running before system installation. Then, start Systemwalker upgrade installation or reinstallation.

However, those services may fail to stop or those services are not stopped. If this happens, cancel the current installation and stop services manually before starting to install again.

Stopping Systemwalker products

Stop the following Systemwalker product before starting the installation.

- Systemwalker Operation Manager V13.8.0 or later
- Systemwalker Centric Manager V13.4.0 or later

Refer to the manual of each product for how to stop the product.

Note that the Web server used by each product must also be stopped.

Port numbers

Refer to "Appendix C Listing of Port Numbers" for information on the port numbers used by Systemwalker Operation Manager. Add a port number to "<*system directory*>\system32\drivers\etc\services" according to a function to use.

If the port number has already been used, add a different port number that has not been used on any servers.

Note that some port numbers are added automatically to the services file when Systemwalker Operation Manager is installed. If the applicable port number has already been written, it will not be added.

Refer to "2.2.2 Changing Port Numbers" for information on how to change the port number.

Note

Web Console and Web API port numbers

If the port used by the Web server is already being used elsewhere on the system where the product will be installed, the following message is displayed during installation:

```
Web server setup failed.
```

If this message is output, follow the procedure outlined in the *Systemwalker Operation Manager Message Guide* or "Changing the port number of the Web Console/Web API function" in "2.2.2 Changing Port Numbers", and set up the Web server again.

Installing upgrades

- Before installing the upgrade, stop any Systemwalker Operation Manager clients, Systemwalker Operation Manager Environment Setup clients, Master Schedule Management Environment Setup clients, Multi-server Monitoring clients, Jobscheduler Info Printout clients, Master Schedule Management monitor clients or Task Link clients that may be running.

  If any of those clients are active, you may fail to install the upgrades.

- If an update pack has been applied to a server or client, that update pack must be removed before any upgrade can be installed. Refer to the update pack user guide (README.TXT) provided with the relevant update pack for the removal procedure.

- If V13.3.0 or later UNIX client has been installed, upgrade installation to Windows x86 cannot be performed. Uninstall the client before installing the Windows x86 client.

- The user restriction definitions will be inherited after the upgrade installation as well.

Installing the Redistributable package

When Systemwalker Operation Manager is installed, the following Redistributable package will be installed automatically if it has not already been installed on the system.

- Installation type: Server
  Microsoft Visual C++ 2015-2019 Redistributable

- Installation type: Client
  Microsoft Visual C++ 2015 Redistributable

However, if a package newer than Redistributable package has already been installed, the Redistributable package will not be installed.

Note that the Redistributable package is required to operate Systemwalker Operation Manager, and therefore should not be uninstalled if Systemwalker Operation Manager is already installed. If uninstalled, the Redistributable package must be manually installed.

Installing and uninstalling the .NET Framework

One of the following versions of .NET Framework is required for installing, using, or uninstalling the Operation Manager client function:

- .NET Framework 2.0

- .NET Framework 3.x

- .NET Framework 4.x

Since the .NET Framework is available as part of operating system functions, use one of the following procedures to install the .NET Framework before installing the Operation Manager client function.

Windows Server 2016 / Windows Server 2019:

Select **Control Panel** >> **Programs and Features** >> **Turn Windows features on or off**. In the **Add Roles and Features** Wizard of the **Server Manager** window that is displayed, select the server where Systemwalker Operation Manager is installed from **Server Selection** of the menu, and then select **Features**. From the feature list displayed, select **.NET Framework 3.x Features** or **.NET Framework 4.x Features** to add the feature. This operation is not required if one of the checkboxes has already been selected.

Windows(R) 8.1 or later:

Select **Control Panel** >> **Programs** >> **Programs and Features** >> **Turn Windows features on or off**. In the **Windows Features** window that is displayed, select **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** or **.NET Framework 4.5 (Advanced Services)**. This operation is not required if one of the checkboxes has already been selected.

To uninstall .NET Framework, use the same window as was displayed during installation and perform the uninstallation (function deletion) process.

Refer to "Uninstalling the Operation Manager client function and the .NET Framework" in "1.6.3 Systemwalker Uninstallation from the Windows System" for notes on uninstalling the Operation Manager client function and the .NET Framework.

Note

Notes on installing and uninstalling the .NET Framework

- When using a redistributable package, follow the terms of use in the download site of the Microsoft .NET Framework Redistributable package.
- If you mistakenly installed the .NET Framework after the Operation Manager client function was installed, you will need to manually specify the settings that are normally entered automatically when the client function is installed.

  In this case, after the .NET Framework has been installed, execute the following command from the command prompt with administrator privileges:

  ```
  <Windows directory>\Microsoft.NET\Framework\v2.0.50727\regasm.exe <Operation Manager
  installation directory>\mpwalker.jm\bin\Fujitsu.OPMGR.Forms.Interop.dll /tlb<Operation Manager
  installation directory>\mpwalker.jm\bin\com.Fujitsu.OPMGR.Forms.Interop.tlb
  ```

- If you mistakenly uninstalled the .NET Framework despite using the Operation Manager client function, you will need to reinstall the .NET Framework in order to use the Operation Manager client function.
- .NET Framework 2.0 is installed automatically when either .NET Framework 3.0 or .NET Framework 3.5.1 is installed.
- To check if .NET Framework 2.0 is included with more recent versions than .NET Framework 3.5.1, refer to the Microsoft Corporation website.

Specifying a directory containing a space as the installation directory

- If Systemwalker Operation Manager is installed in the directory that contains a space, such as "C:\Program Files", short file name creation (in 8.3 format) must be enabled in the operating system settings beforehand. It is not possible to install Systemwalker Operation Manager in the directory that contains a space if short names are disabled.
- If Systemwalker Operation Manager is to coexist with Systemwalker Centric Manager, only the following can be specified as the installation directory that contains a space:
  - C:\Program Files
- Specify the NTFS format disk for the installation directory.

User restriction definitions for new installation

When a new installation is performed, the user restriction definition is enabled (*1).

*1: The option **Restrict so that only users included in the swadmin group can start demand jobs, start jobnet Job execution control attributes or use Jobscheduler command functions.** in the **Define Operation Manager Shared Parameter** window is selected.

Users need to be registered to the swadmin group to submit a demand job, start a job net with the Job Execution Control attribute, and run Jobscheduler commands.

This setting can be changed after the installation.

Refer to "2.4.5 Define User Restrictions" for information on the user restriction definitions.

1.3.2 Tasks Prior to Installation

This section explains the tasks that must be performed prior to installation.

Reading the software ReadMe files

The software ReadMe files provide basic notes about Systemwalker Operation Manager. Be sure to read these files before installation.

Backing up existing environments

Make a backup copy of the existing environments in case of installation failure although they are transitioned automatically during upgrading or reinstallation.

For the detailed backup procedure, see the following

- "Chapter 3 Backing Up or Restoring Operation Environment"

Checking the system installation environment

Confirm the following items regarding the system environment at the installation destination.

Server service

When you install Systemwalker Operation Manager, the Server service must be running beforehand. Ensure that the Server service has already started.

Windows Modules Installer service

When installing Systemwalker Operation Manager, confirm that one of the following options is set for **Startup type** in **Windows Modules Installer Properties** beforehand.

- **Manual**
- **Automatic**
- **Automatic (Delayed Start)**

Use of DHCP

If you have used the DHCP server to dynamically assign an IP address to the server machine, you cannot start Systemwalker Operation Manager's server functions. Ensure that the DHCP is not used. However, you can use the Systemwalker Operation Manager's client functions even in the environment where the DHCP server is used.

Primary domain controller

When installing on a backup domain controller, confirm that the primary domain controller is running.

Network drive connection

Ensure that the destination drive or directory is NOT connected to the network as a separate drive within the same system. You must disconnect the drive or directory before installation. If connected, you may fail to install the server functions.

Active programs

Before installing Systemwalker, shut down all of currently active applications. Also, shut down the following programs before installation.

- Resident programs (permanently running programs) including virus detection programs
- Screen savers

Deciding the installation method

You can select one of the following methods to install Systemwalker Operation Manager in the system. Decide in which method you will install your Systemwalker Operation Manager.

a. Local installation

   You can directly install Systemwalker on a PC with a drive by using the product media.

b. Network installation

   You can install Systemwalker on a network-connected PC if the drive has been set as the shared disk.

Preventing depletion of the desktop heap

To prevent depletion of the desktop heap when using Windows Server 2008 or later, modify the registry and expand the size of the desktop heap.

Change the third parameter of the registry indicated below (SharedSection) to "3072".

- Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems
- Name: Windows
- Value: Third parameter of SharedSection
  - Before (example in Windows Server 2012)

    ```
    SharedSection=1024,20480,768
    ```

  - After (example in Windows Server 2012)

    ```
    SharedSection=1024,20480,3072 (*1)
    ```

*1: If the value of the third parameter of SharedSection is greater than 3072, do not change it.

Configuring firewall settings

In the firewall settings, allow connection with the port number/protocol to be used by Systemwalker Operation Manager. Refer to the operating system manuals for information on how to allow the required connection (port) for the firewall function. Refer to "C.1 Listing of Port Numbers" for information on the ports that Systemwalker Operation Manager uses.

Note

Using the mjrmtjob command

It is necessary to set the port numbers for the firewall to execute a job on a remote machine using the mjrmtjob command and to use the remote machine environment where the firewall function is used. On the remote machine, allow the port numbers listed in "Remote machine (port numbers that should accept external server access)".

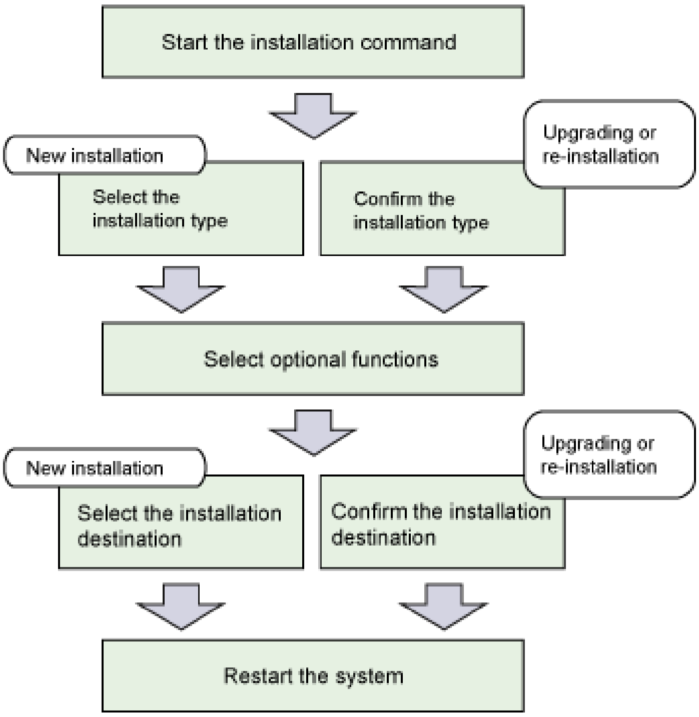
You need a remote machine license to use the mjrmtjob command to execute jobs on a remote machine.

1.3.3 Installation Procedure

Installation is performed by a user belonging to the local Administrators group.

If the installation environment is a domain controller, log on as a user belonging to the built-in local Administrators group.

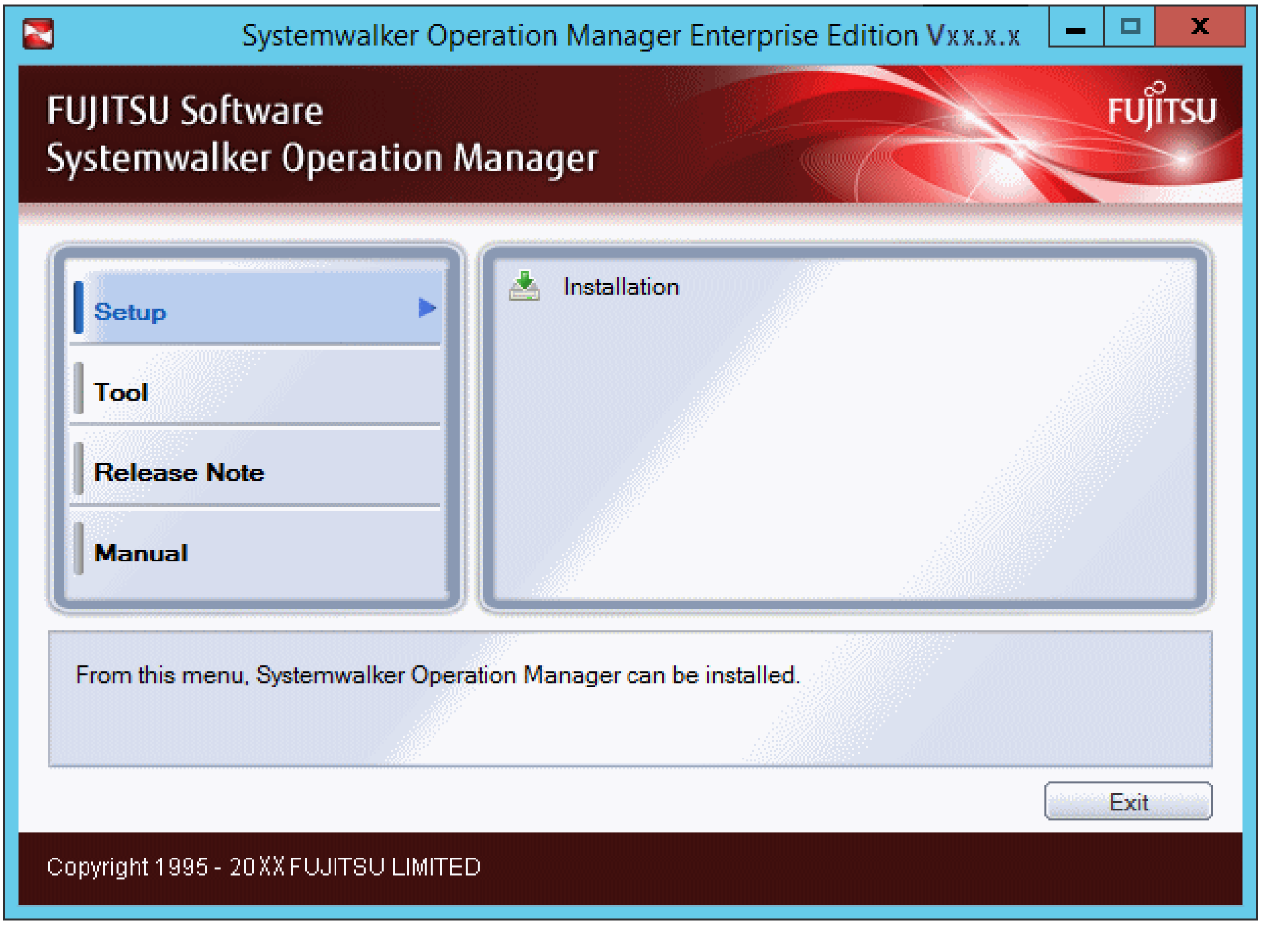
Use the following procedure to install Systemwalker Operation Manager.


Start the installation command
New installation
Select the installation type
Upgrading or re-installation
Confirm the installation type
Select optional functions
New installation
Select the installation destination
Upgrading or re-installation
Confirm the installation destination
Restart the system

1) Activate the installation command.

For environments other than Server Core

When you insert the Systemwalker Operation Manager product media into its drive, the following menu appears automatically.


Systemwalker Operation Manager Enterprise Edition Vxx.x.x
FUJITSU Software
Systemwalker Operation Manager
FUJITSU
Setup
Tool
Release Note
Manual
Installation
Exit

From this menu, Systemwalker Operation Manager can be installed.

Copyright 1995 - 20XX FUJITSU LIMITED

If the Installer does not start automatically, execute the following command from the product media:

```
<drive> \SwSetup.exe
```

Information

When using a directory to which the product media has been copied for installation

Follow the procedure below:

1. Execute the subst command to assign the directory to which the product media has been copied to a virtual drive.

   Example of assigning the directory to virtual drive Z:

   subst Z: *<full path of directory to which product media was copied>*

2. Execute swsetup.exe under the virtual drive assigned in 1.

Execute the subst command and swsetup.exe, from a command prompt launched via **Run as administrator**.

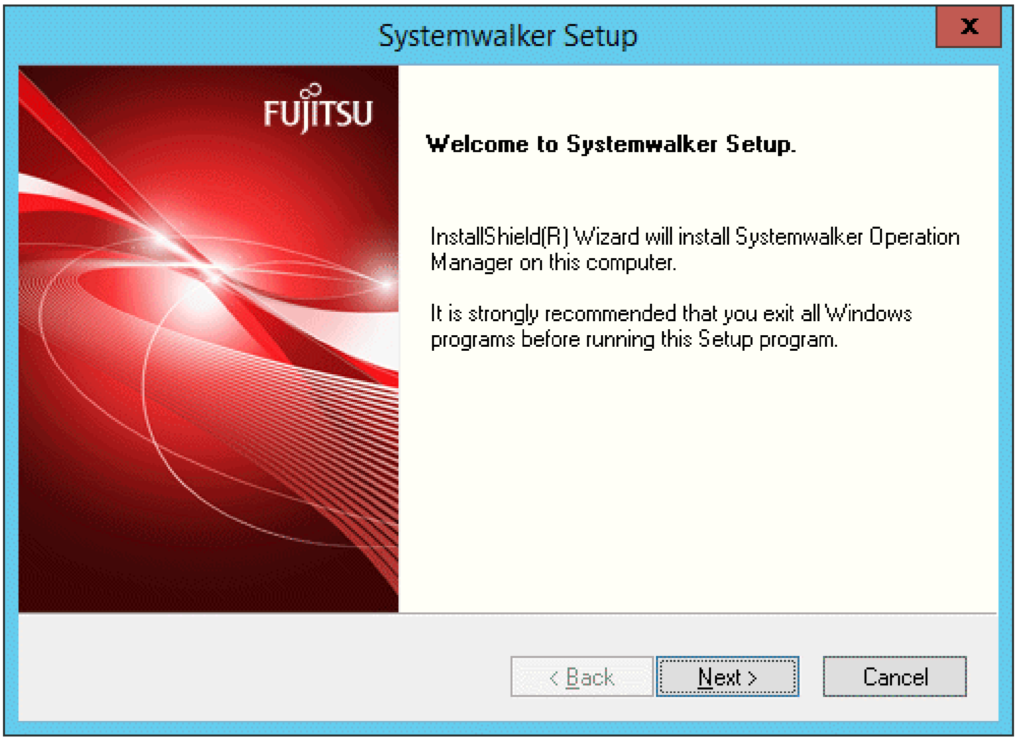
[Windows x86]

Click **Installation** to display the window shown below. Then, click **Next**.

[Windows x64]

If installing a server, click **Installation(Server)** to display the window shown below. Then, click **Next**.

If installing a client, click **Installation(Client)** to display the window shown below. Then, click **Next**.


Systemwalker Setup

Welcome to Systemwalker Setup.

InstallShield(R) Wizard will install Systemwalker Operation Manager on this computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Server Core environments

Execute the following command from the command prompt:

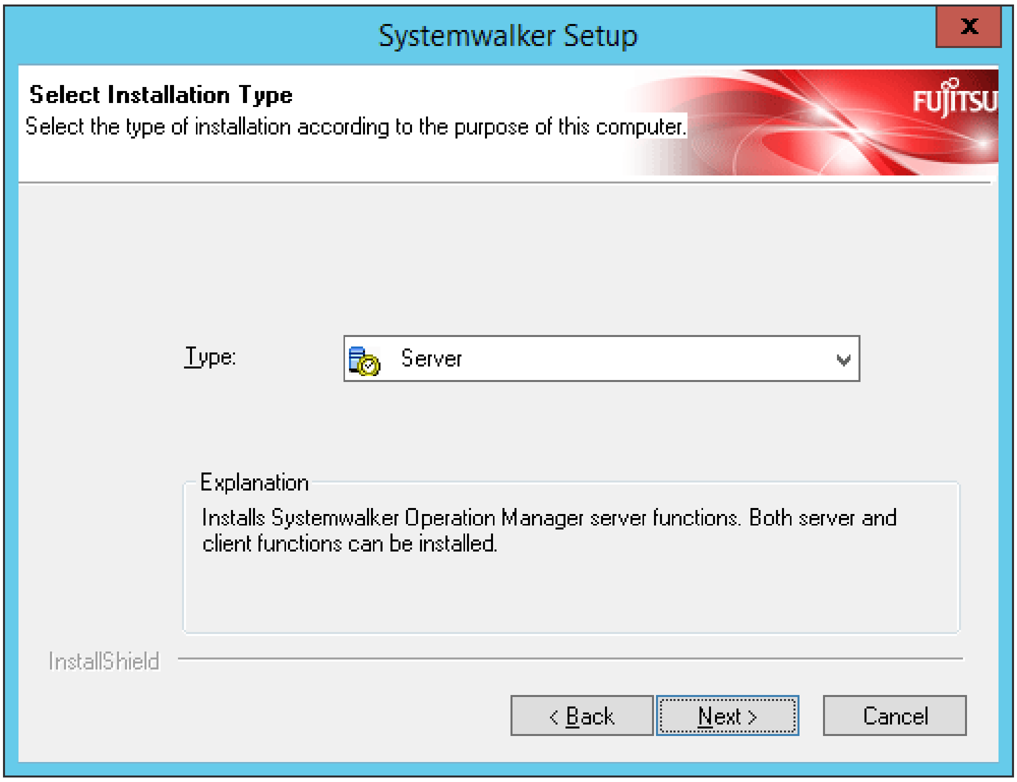
```
<drive>\MAIN\win32\setup.exe
```

Refer to "setup Systemwalker Operation Manager Installation Command" in the *Systemwalker Operation Manager Reference Guide* for information on commands.

After this command is executed, the **Systemwalker Setup** window will be displayed. Click **Next**. The displayed window is the same as the **Systemwalker Setup** window that is output in non-Server Core environments.

2) Select an installation type.

When the following window appears, select **Server** or **Client** and click **Next**.



Systemwalker Setup

Select Installation Type

Select the type of installation according to the purpose of this computer.

Type: Server

Explanation

Installs Systemwalker Operation Manager server functions. Both server and client functions can be installed.

- **Performing upgrade installations or reinstallations**

  Messages in the windows displayed may vary. Note that the installation type cannot be changed.

- **Server Core environments**

  The only installation type that can be selected is **Server**.

- **Windows x64**

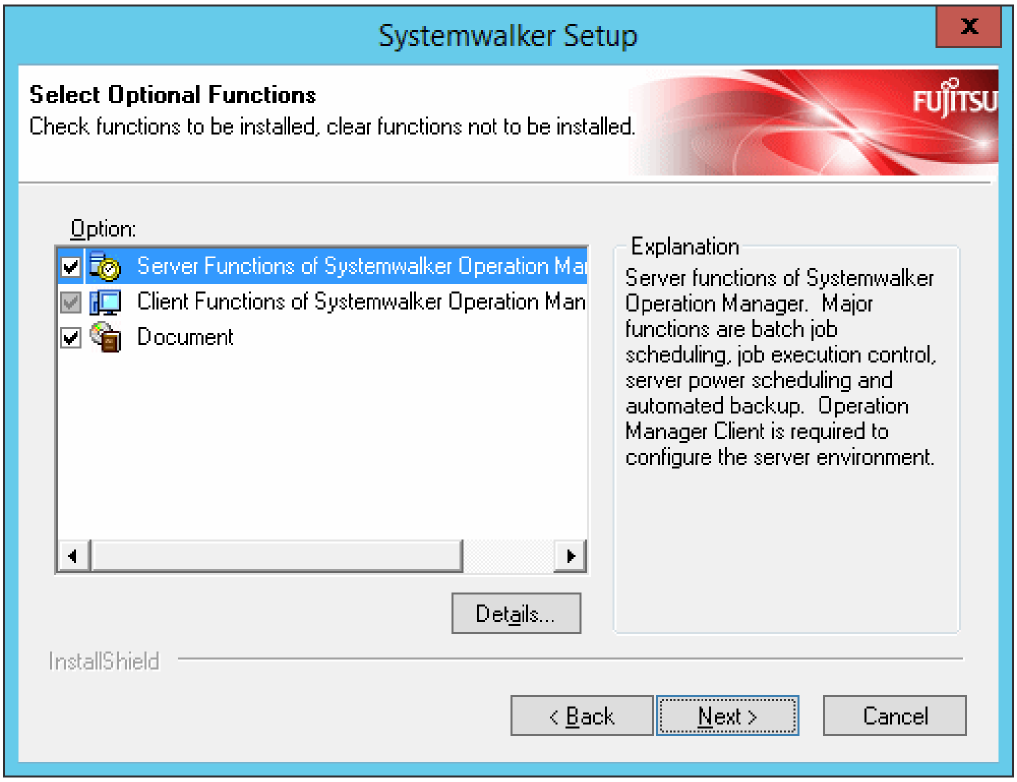
  If **Installation(Server)** was selected, the only installation type that can be selected is **Server**.

  If **Installation(Client)** was selected, the only installation type that can be selected is **Client**.

3) Select optional functions.

If you have selected **Server**, the following window appears. Select the functions you want to install and click **Next**.

If you have selected **Client**, the options window may vary.



Select Optional Functions

Check functions to be installed, clear functions not to be installed.

Option:

☑ Server Functions of Systemwalker Operation Ma

☑ Client Functions of Systemwalker Operation Man

☑ Document

Explanation

Server functions of Systemwalker Operation Manager. Major functions are batch job scheduling, job execution control, server power scheduling and automated backup. Operation Manager Client is required to configure the server environment.

- Configuring environment settings for server functions

  For configuring the environment settings of server functions, the Operation Manager client function must be installed. Select the **Client Functions of Systemwalker Operation Manager** check box.

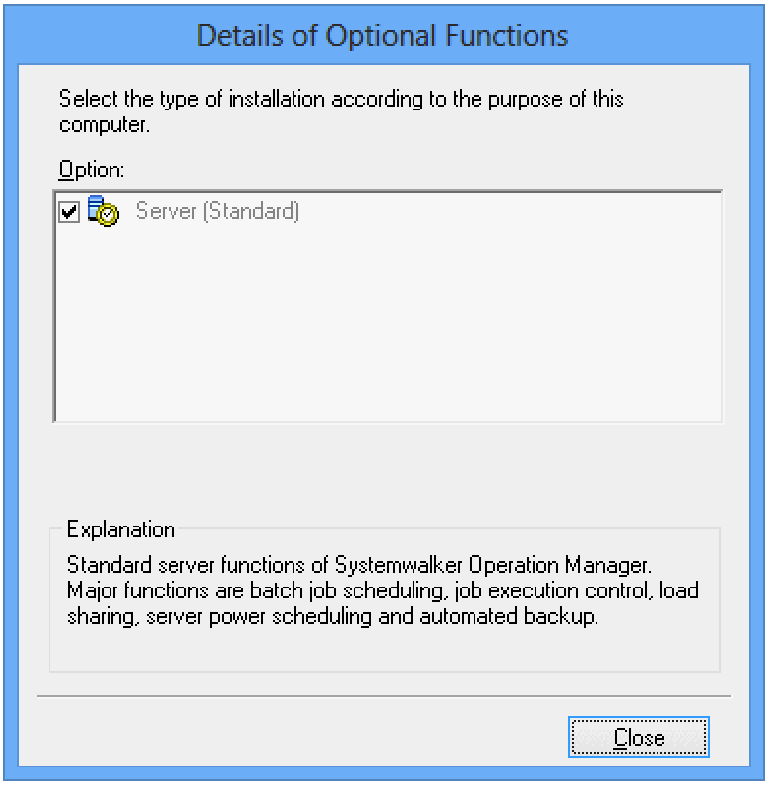
- Performing upgrade installations

  It is not possible to clear the selection of a previously installed item. If the server functions or the client functions were not previously installed, they can be installed now.

- Server Core environments

  Only **Server Functions of Systemwalker Operation Manager** can be selected as an optional function. **Client Functions of Systemwalker Operation Manager** and **Document** cannot be used, even if selected.

Select **Server Functions of Systemwalker Operation Manager** and click **Details**, and the following window will appear.



Select the type of installation according to the purpose of this computer.

Option:

☑ Server (Standard)

Explanation

Standard server functions of Systemwalker Operation Manager. Major functions are batch job scheduling, job execution control, load sharing, server power scheduling and automated backup.

The detailed installation functions are displayed and you can select the desired ones. For the configuration of each function, see "1.1 List of Functions to be Installed".

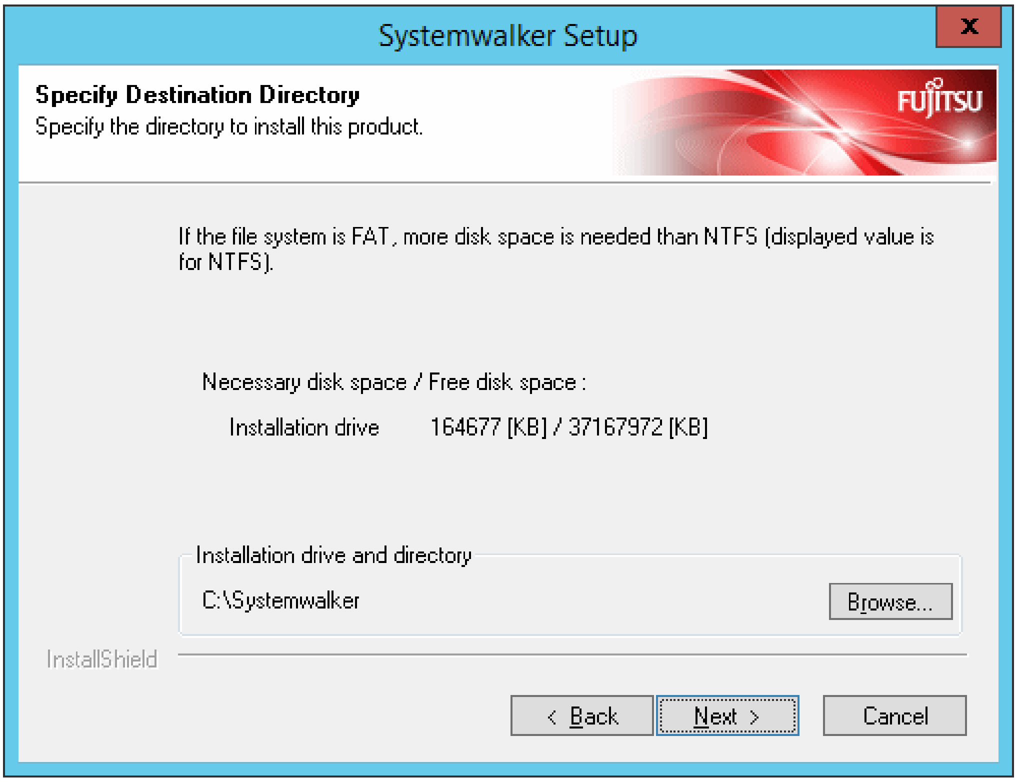
Select the functions you want to install, and click **Close**.

The followings are notes for this window.

- During upgrading, you cannot unselect the previously installed options. However, you can install the server or client functions you have not installed yet.
- If you do not click the **Details** button, the default setup is installed. For the default setup, see "1.1 List of Functions to be Installed".

4) Select the installation directory.

The following shows the window where you can specify the **Installation drive and directory**. Specify the directory and click **Next**.



Systemwalker Setup

Specify Destination Directory

Specify the directory to install this product.

If the file system is FAT, more disk space is needed than NTFS (displayed value is for NTFS).

Necessary disk space / Free disk space :

Installation drive 164677 [KB] / 37167972 [KB]

Installation drive and directory

C:\Systemwalker

When you do this, the amount of space required for installation and the amount of available space are shown. Specify a drive with adequate free space.

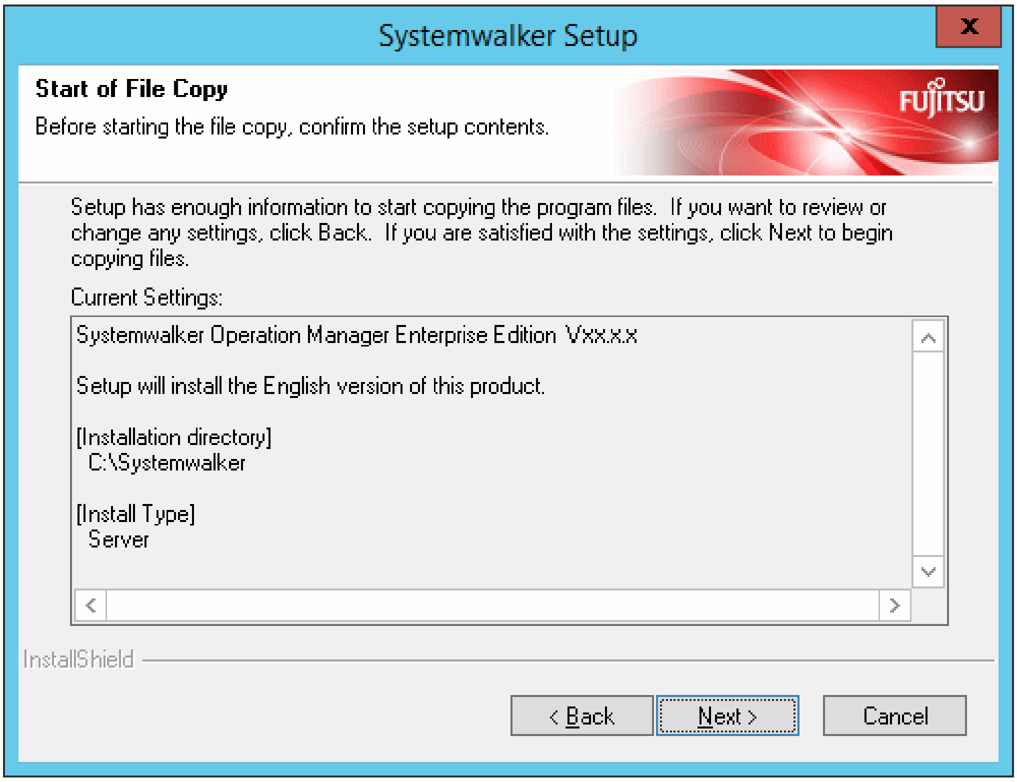
The installation directory name can be made up of up to 74 alphanumeric characters.

- **Performing upgrade installations or reinstallations**

  The windows displayed may vary. Note that the installation destination cannot be changed.

5) Check the setup information.

When your entry is complete, the following window appears. When your setup is correct, click **Next**.



Start of File Copy

Before starting the file copy, confirm the setup contents.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Systemwalker Operation Manager Enterprise Edition  Vxx.x.x

Setup will install the English version of this product.

[Installation directory]
  C:\Systemwalker

[Install Type]
  Server
```

6) Restart the system.

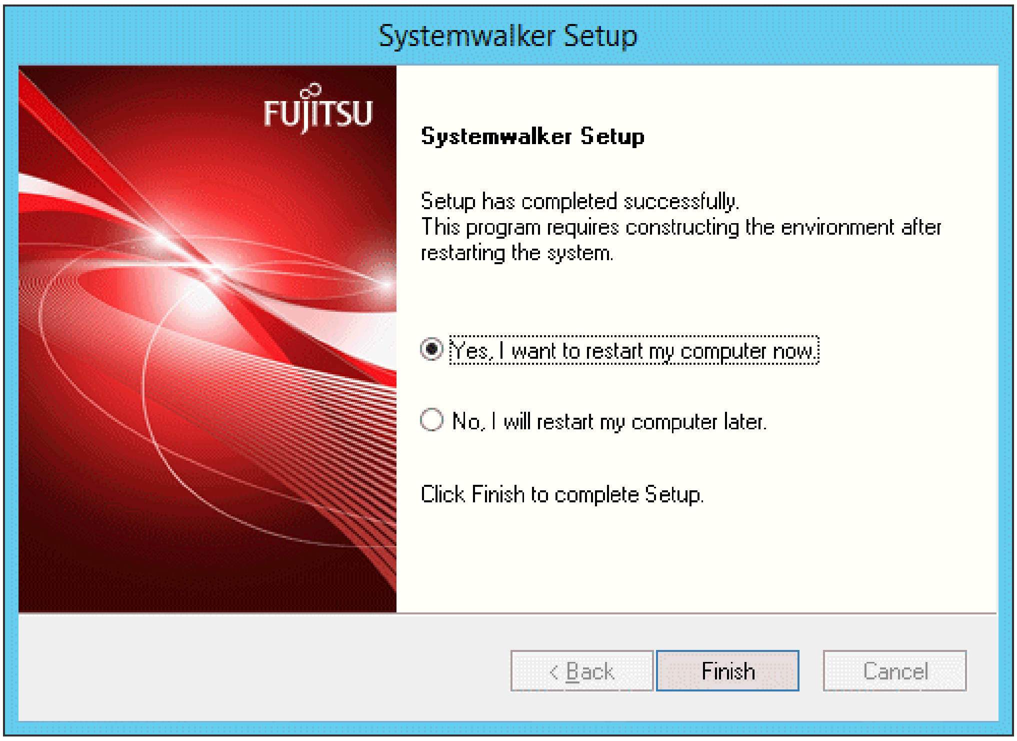
The system will have to be restarted if any of the following conditions are met:

- If Systemwalker Centric Manager has been installed
- If the installation is not a new installation
- If the Microsoft Visual C++ Redistributable package has been installed, the existing version is earlier than the version that is bundled with the product, and the conditions that require a restart are met

If the system does not have to be restarted, the following message will be displayed:

```
Click Finish to complete Setup.
```

If the system has to be restarted, the following window will be displayed when the installation completes, so click the Finish button.



Systemwalker Setup

Systemwalker Setup

Setup has completed successfully.
This program requires constructing the environment after restarting the system.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Click Finish to complete Setup.

To operate Systemwalker Operation Manager, first, you must input the license key and then you must define the operating environment of Systemwalker Operation Manager and configure and run your jobs. Refer to the following documents for these operations.

- Defining the operating environment

  "Chapter 2 Definition of Operating Environment of Systemwalker Operation Manager" in this guide

- Configuring and running jobs

  Systemwalker Operation Manager User's Guide

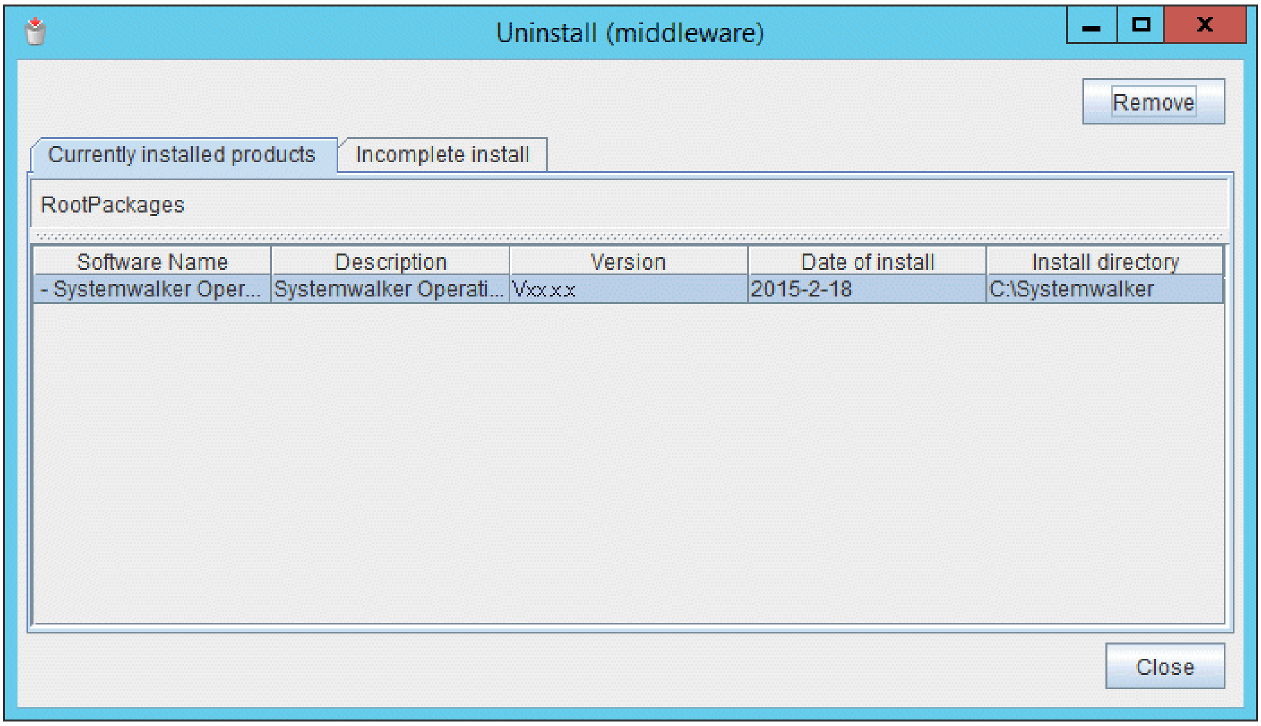
Information

Checking the installed products (Environments other than Server Core)

Follow the procedure below to check the installed products.

1. Select **Start** or **Apps** >> **Fujitsu** >> **Uninstall (middleware)**.

The **Uninstall (middleware)** window opens, and a list of installed product names is displayed.



Software Name	Description	Version	Date of install	Install directory
- Systemwalker Oper...	Systemwalker Operati...	Vxx.x.x	2015-2-18	C:\Systemwalker

1. Click **Close** to close the window.

If the installation ends with an error, the product information will be displayed in the **Incomplete install** tab. After removing the cause of the error, delete the product information from the **Incomplete install** tab as required.

1.3.4 Notes After Installation

This section provides important notes to take into account after the installation has completed.

"FJQSS (Information Collection Tool)" and "Uninstall (middleware)"

When Systemwalker Operation Manager is installed, the following menus are created (unless there are other Fujitsu middleware products installed):

- **Start** or **Apps** >> **FJQSS (Information Collection Tool)**
- **Start** or **Apps** >> **Fujitsu** >> **Uninstall (middleware)**

FJQSS (Information Collection Tool) is a tool that is built into Systemwalker Operation Manager, and it is used to collect investigation information required when a problem occurs.

For details on FJQSS (Information Collection Tool), refer to the manual that is displayed on selecting **Start** or **Apps** >> **FJQSS (Information Collection Tool)** >> **FJQSS User's Guide**.

"Uninstall (middleware)" is a tool that is commonly used in the Fujitsu middleware products. It manages information for Fujitsu middleware products and starts the uninstaller of products that are installed. The tool can manage not only information for FJQSS (Information Collection Tool) that is built into Systemwalker Operation Manager, but also other Fujitsu middleware products information.

Refer to "1.6.3 Systemwalker Uninstallation from the Windows System" for details on uninstalling Systemwalker Operation Manager.

NetBIOS over TCP/IP

When you use Systemwalker Operation Manager as a domain user, you must enable the 'NetBIOS over TCP/IP'. In Windows Server 2012 or later or Windows(R) 8.1 or later, **Default** or **Enable NetBIOS over TCP/IP** must be selected in the NetBIOS settings.

Follow the procedure below to select **Default** or **Enable NetBIOS over TCP/IP** if neither is set.

1. Open Local Area Connection Properties by following the procedures below.

   To open the properties, select Ethernet from Network and Sharing Center on Control Panel.

2. After selecting Internet Protocol (TCP/IP), click Properties to open the Properties window.
3. Click Advanced to open the TCP/IP Advanced Settings window.
4. Click Enable NetBIOS over TCP/IP on the WINS tab.

Server service

When you use Systemwalker Operation Manager do not shut down the Server service. The Server service is started automatically when you install the operating system.

Event log [Windows version]

If the Windows event log cannot be written due to insufficient capacity, Systemwalker Operation Manager may not function normally. Review the event log settings using the following setting example as a reference:

1. Start the Windows Event Viewer and open the Application properties window.
2. Set Overwrite events as needed for When maximum log event log size is reached.

IPv6 single stack environment

It is not possible to build a Systemwalker Operation Manager Web server in an IPv6 single stack environment.

Windows Defender

When Systemwalker Operation Manager is installed, the following information may be recorded in the Windows Defender history as " "Unknown" in the Alert level" but these messages can be safely ignored. The following information is included in the Resource column of the history, for items relating to the Systemwalker Operation Manager client program:

- service:
  - F3CVSERV
  - MpAosfX
  - Mpinst (*1)

    *1: Recorded temporarily during installation.
- runkey:
  - mpaosfac

1.3.5 Tasks after Installation

Perform the following tasks after installation.

Continuous Execution mode for network jobs

If you have reinstalled Systemwalker Operation Manager in an environment where the Continuous Execution mode is enabled by the "jmmode" command, reissue the "jmmode" command to enable the Continuous Execution mode.

1.4 Installation in the UNIX System

This section explains how to install Systemwalker Operation Manager in the UNIX server.

Before starting the system installation, check the following points and take required actions given.

Referring to the related documents

The software ReadMe files and other documents on the Systemwalker Operation Manager product media provide basic notes on Systemwalker Operation Manager. Refer to these files.

Checking the operating environment

Check both the hardware and software resources required for operating Systemwalker Operation Manager. Refer to the *Systemwalker Operation Manager Technical Guide* for those resources.

1.4.1 Notes Prior to Installation

This section provides important notes to take into account before installation.

Stopping daemons

All of Systemwalker Operation Manager daemons are stopped automatically when the system is installed. If it coexists with Systemwalker Centric Manager in the same environment, the Systemwalker Centric Manager daemons are also stopped automatically.

Stopping Systemwalker products

Stop the following Systemwalker product before starting the installation.

- Systemwalker Operation Manager V13.8.0 or later
- Systemwalker Centric Manager V13.4.0 or later

Refer to the manual of each product for how to stop the product.

Note that the Web server used by each product must also be stopped.

Port numbers

Refer to "Appendix C Listing of Port Numbers" for information on the port numbers used by Systemwalker Operation Manager. Add a port number to /etc/services according to a function to use. If the port number has already been used, add a different port that has not been used on any servers.

Note that some port numbers are added automatically to the services file when Systemwalker Operation Manager is installed. If the applicable port number has already been written, it will not be added.

Refer to "2.2.2 Changing Port Numbers" for information on how to change the port number.

Note

Web Console and Web API port numbers

If the port used by the Web server is already being used elsewhere on the system where the product will be installed, the following message is displayed during installation:

```
Web server setup failed.
```

If this message is output, follow the procedure outlined in the *Systemwalker Operation Manager Message Guide* or "Changing the port number of the Web Console /Web API function" in "2.2.2 Changing Port Numbers", and set up the Web server again.

Upgrade installations

- If a cumulative patch for PC clients has been applied to a client in the Solaris version, that patch must be removed before any upgrade can be installed. Refer to the PC client cumulative patch application procedure guide (README.TXT) provided with the relevant patch for the removal procedure.
- The user restriction definitions will be inherited after the upgrade installation as well.

Setting of /etc/hosts (For Solaris/Linux)

In the Red Hat Linux and Solaris 11 or later systems, 127.0.0.1 is set as an IP address for the local host name in the /etc/hosts field by default. This can lead to the following issues:

- If the Systemwalker Operation Manager server is installed on this server, the server setup may fail.
- If you connect a Systemwalker Operation Manager client or Multi-server Monitoring clients to the server under this condition, it may not be monitored correctly.
- If a network job is executed for another server from this server, it will take longer than expected to execute network jobs.
- If a network job is executed for another server from this server, the network job may end abnormally.

Therefore, the IP address for the host name of localhost configured in the /etc/hosts file during installation must be an address that can be connected from the client and from the execution server.

An example of /etc/hosts file settings is shown below:

[Before]

```
127.0.0.1 <host name> localhost
```

[After]

```
127.0.0.1 localhost
xxx.xxx.xxx.xxx <host name>
```

Note: xxx.xxx.xxx.xxx is the IP address for <*host name*> (localhost).

Installation in Non-Global Zone[Solaris]

When installing Systemwalker Operation Manager in the Non-Global Zone, take the following notes.

- One or more logical network interfaces must be assigned from the Global Zone.
- The "Directory Inheritance" of the Zone function cannot be used in the Systemwalker installation directory and in the following directories:

  All directories locating under /opt
  All directories locating under /etc
  All directories locating under /var
  All directories locating under /usr

- The Systemwalker installation directory and the following directories cannot be shared by another Zone.

  /opt
  /etc
  /var
  /usr

User restriction definitions for new installation

When a new installation is performed, the user restriction definition is enabled (*1).

*1: The option **Restrict so that only users included in the swadmin group can start demand jobs, start jobnet Job execution control attributes or use Jobscheduler command functions.** in the **Define Operation Manager Shared Parameter** window is selected.

Users need to be registered to the swadmin group to submit a demand job, start a job net with the Job Execution Control attribute, and run Jobscheduler commands.

This setting can be changed after the installation.

Refer to "2.4.5 Define User Restrictions" for information on the user restriction definitions.

1.4.2 Tasks Prior to Installation

This section explains the tasks that must be performed prior to installation.

Backing up existing environments

If you are upgrading or reinstalling, back up your existing environment in case installation fails.

For the detailed backup procedure, see the following.

- "Chapter 3 Backing Up or Restoring Operation Environment"

Shutdown of jobs

Ensure that all of Systemwalker Operation Manager jobs have stopped. Then, start Systemwalker upgrade installation or reinstallation.

Installation in single-user mode [Solaris/Linux]

To install in single-user mode, perform the installation with the /opt directory and the target installation directory mounted.

Configuring firewall settings

For the port number/protocol used by Systemwalker Operation Manager, allow communication in the firewall settings. For information on how to allow necessary communication (ports) to the firewall function, refer to the OS documentation. Refer to "C.1 Listing of Port Numbers" for information on the ports that Systemwalker Operation Manager uses.

Note

Using the mjrmtjob command

It is necessary to set the port numbers for the firewall to execute a job on a remote machine using the mjrmtjob command and to use the remote machine environment where the firewall function is used. On the remote machine, allow the port numbers listed in "Remote machine (port numbers that should accept external server access)".

You need a remote machine license to use the mjrmtjob command to execute jobs on a remote machine.

1.4.3 Installation Procedure

The standard installation procedure is shown in the following two steps.

- Installation in Solaris (Global Zone), HP-UX, AIX, or Linux
- Installation in Solaris (Non-Global Zone)

Note that the screenshots used in this section are those for the Linux version.

Installation in Solaris (Global Zone), HP-UX, AIX, or Linux

The following shows the installation procedures of Systemwalker Operation Manager in Solaris (Global Zone), HP-UX, AIX, or Linux.

1) Log in as the superuser.

Log in at the console of the computer where you install Systemwalker Operation Manager.

2) Mount the file system.

Mount the required file system as shown in the following example.

```
# mount -F ufs /dev/dsk/c?t?d?s? /<mount point> (Note) or
# mountall -l
```

Note:

The command varies depending on the operating system and the machine environment. For details of commands, see the manual for the operating system in use.

3) Mount the Systemwalker Operation Manager product media.

Mount the Systemwalker Operation Manager product media on its drive. Check the correct drive device name as it may vary depending on the environment you use.

The command varies depending on the operation system and the machine environment. An example for each operating system is shown below.

Solaris

```
# /usr/sbin/mount -F hsfs -o ro /dev/.../cdrom]
```

Note: It is recommended that you specify an HSFS file system.

HP-UX

```
# /usr/sbin/pfs_mount -t rrip -x unix /dev/.../cdrom
```

AIX

```
# /usr/sbin/mount -r -v "cdrfs" /dev/.../cdrom
```

Linux

```
# /bin/mount -t iso9660 -r /dev/.../cdrom
```

Note: It is recommended that specify an ISO 9660 file system.

The device name (/dev/...) may differ depending on the system. If there is no mount point (/cdrom or /mnt/cdrom), create one in advance.

Note

Mounting the product media

The product media has been created in UDF Bridge format. You can therefore mount it as an HSFS file system (Solaris), ISO 9660 file system (Linux), or UDF file system. However, mounting it as a UDF file system may result in the revocation of execution permission for files to be executed. In this case, the installer will not run or there will be other issues.

Note that, depending on the operating system, the mount specifications will be as follows:

- If you mount the product media automatically or without specifying a file system option in the mount command, it will be mounted as a UDF file system and you will not be able to execute its commands.

You can check the mount options for the mounted product media by executing the mount command without any arguments. To check the type of file system, specify the -v option in the arguments.

4) Execute the installation command.

Issue the Systemwalker Operation Manager installation command. The following gives an example.

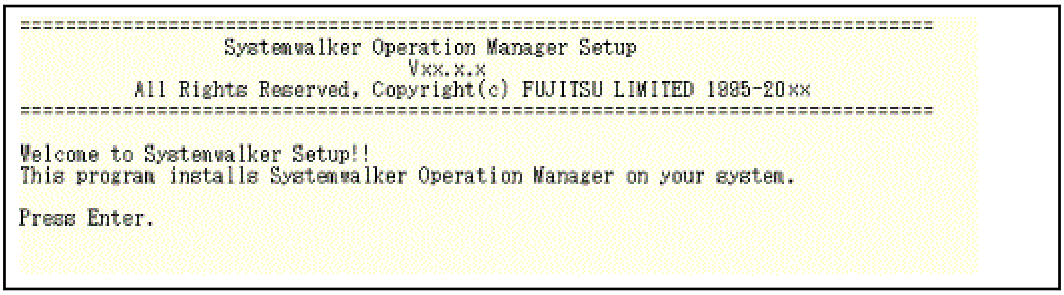
```
# /<mount point>/Solaris/unx/swsetup
```

Note:

The command varies depending on the operating system.

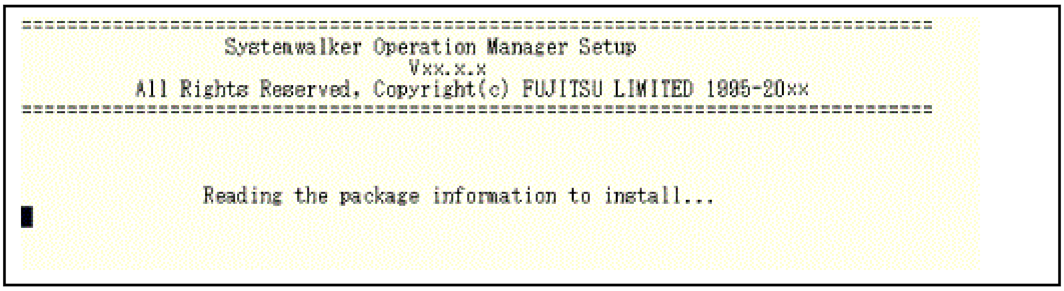
Solaris version: /<*mount point*>/Solaris/unx/swsetup
HP-UX/AIX version: /<*mount point*>/unx/swsetup
Linux version: /<*mount point*>/Linux/unx/swsetup

Executing the command displays the following window. Press the **Enter** key.



```
================================================================================
                  Systemwalker Operation Manager Setup
                                Vxx.x.x
          All Rights Reserved, Copyright(c) FUJITSU LIMITED 1995-20xx
================================================================================

Welcome to Systemwalker Setup!!
This program installs Systemwalker Operation Manager on your system.

Press Enter.
```

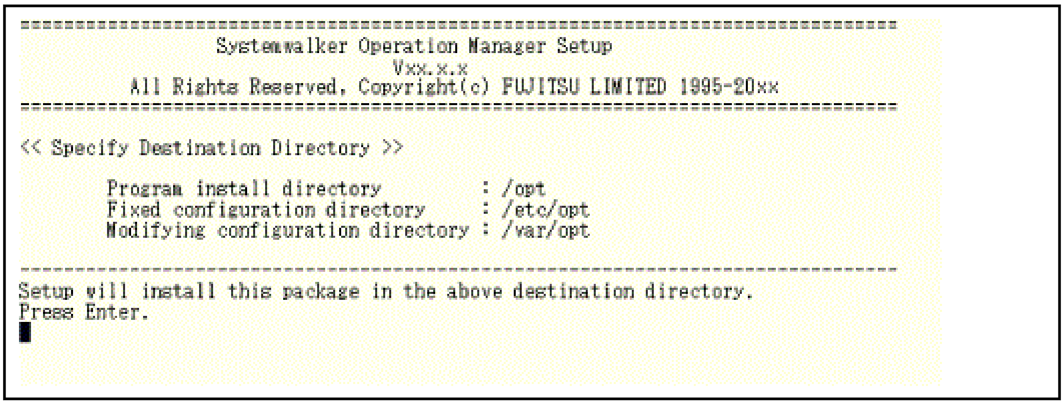
Pressing the **Enter** key displays the following window.



```
================================================================================
                  Systemwalker Operation Manager Setup
                                Vxx.x.x
          All Rights Reserved, Copyright(c) FUJITSU LIMITED 1995-20xx
================================================================================



                Reading the package information to install...
█
```

5) Check the installation destination directory.

When the following window appears, check the directory, and press the **Enter** key.



```
================================================================================
                  Systemwalker Operation Manager Setup
                                Vxx.x.x
          All Rights Reserved, Copyright(c) FUJITSU LIMITED 1995-20xx
================================================================================

<< Specify Destination Directory >>

        Program install directory         : /opt
        Fixed configuration directory     : /etc/opt
        Modifying configuration directory : /var/opt

--------------------------------------------------------------------------------
Setup will install this package in the above destination directory.
Press Enter.
█
```

Remark 1:

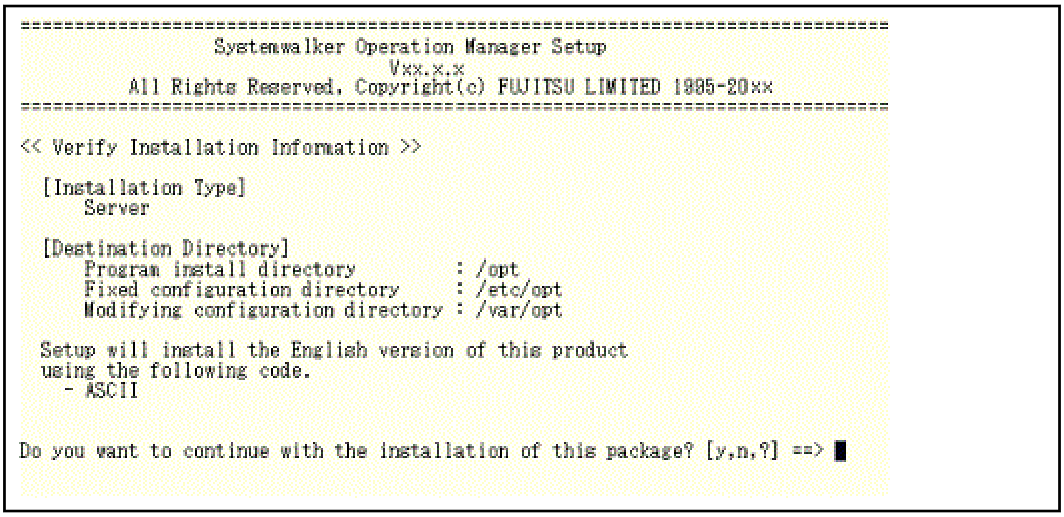
This window does not appear during an upgrade installation or reinstallation.

Remark 2:

For Solaris version, the installation directory can be changed. To change it, enter "y" and press the **Enter** key, and in the next window, enter the directory name you want to change to, using alphanumeric characters. Then, in the window to reconfirm the installation directory, if you want to change again, enter "y", or if you do not change, enter "n" or press the **Enter** key.

6) Check the setup information.

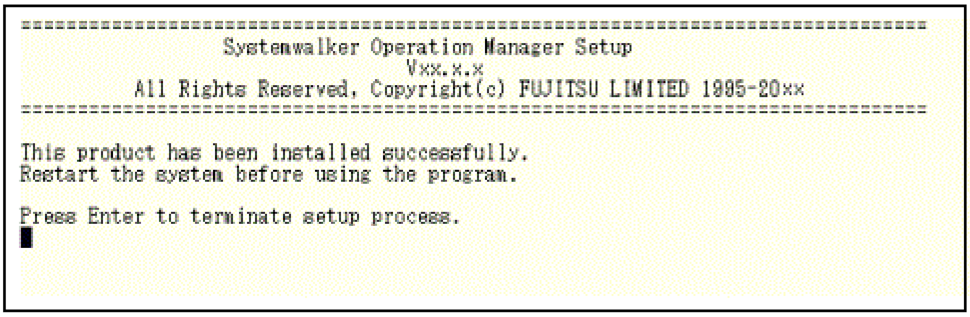
When your entry is complete, the following setup confirmation window appears. When your setup is correct, respond with "y".



```
================================================================================
                  Systemwalker Operation Manager Setup
                                Vxx.x.x
          All Rights Reserved, Copyright(c) FUJITSU LIMITED 1995-20xx
================================================================================

<< Verify Installation Information >>

  [Installation Type]
      Server

  [Destination Directory]
      Program install directory         : /opt
      Fixed configuration directory     : /etc/opt
      Modifying configuration directory : /var/opt

  Setup will install the English version of this product
  using the following code.
    - ASCII

Do you want to continue with the installation of this package? [y,n,?] ==>
```

7) Complete the installation.

After the installation has completed normally, the following window appears. Press the Enter key.



```
================================================================================
                  Systemwalker Operation Manager Setup
                                Vxx.x.x
          All Rights Reserved, Copyright(c) FUJITSU LIMITED 1995-20xx
================================================================================

This product has been installed successfully.
Restart the system before using the program.

Press Enter to terminate setup process.
```

Systemwalker has been installed.

8) Edit the /etc/rc.shutdown file (AIX version only).

For AIX version, define the following line in the /etc/rc.shutdown file.

```
/opt/systemwalker/bin/poperationmgr -s
```

If /etc/rc.shutdown does not exist, create it with the following content and assign appropriate access permissions (such as 0755) to the file so that it can be executed:

```
#!/bin/sh

/opt/systemwalker/bin/poperationmgr -s
```

If you do not define it, you may fail normal shutdown of Systemwalker Operation Manager. Furthermore, you cannot start Systemwalker Operation Manager normally at the restart of the operating system to cause a problem in operation. To restart the operating system, use the shutdown command, not the reboot command.

9) Restart the system.

To use Systemwalker Operation Manager, issue the following command to restart the system.

```
# cd / [RETURN]
# /usr/sbin/shutdown -y -i6 -g0 (Note)
```

Note:

The command varies depending on the operating system.

Solaris version: /usr/sbin/shutdown -y -i6 -g0
HP-UX version: /usr/sbin/shutdown -y -r now
AIX version: /usr/sbin/shutdown -r now
Linux version: /sbin/shutdown -r now

Installation in Solaris (Non-Global Zone)

The following shows the installation procedure of Systemwalker Operation Manager in Solaris (Non-Global Zone).

1) Log in the Global Zone.

Log in the Global Zone as the Administrator (root) user.

2) Mount the Systemwalker Operation Manager product media.

Mount the Systemwalker Operation Manager product media on its drive. If you are NOT using the volume management daemon, mount the system drive. Check the correct drive device name as it may vary depending on the environment you use. The following gives an example of mounting.

```
# mount -F hsfs /dev/dsk/<device name> <destination directory>
```

3) Copy the product media contents to the Global Zone disk.

Specify "/PKG" as the destination of copy.

```
# cp -rfp /<mount point>/* /PKG
```

4) Create a Non-Global Zone to be installed.

Create a Non-Global Zone to be installed. If you have already configured the Zone, you can skip this step.

For Zone creation details, see the related Solaris manual.

5) Shut down the Non-Global Zone to be installed.

Shut down the Non-Global Zone you have created in Step 4 or you have already created earlier by issuing the following command. Specify "SWZONE" as the name of Non-Global Zone to be installed.

```
# /usr/sbin/zoneadm -z SWZONE halt
```

6) Set up the Zone to allow reference to the copied product media contents from the Non-Global Zone.

Issue the following commands to allow referencing to the product media contents you copied in Step 3 from any Non-Global Zone.

```
# zonecfg -z SWZONE
zonecfg:SWZONE> add fs----- Enter "add fs".
zonecfg:SWZONE:fs> set dir=/SWPKG----- Enter "set dir=/SWPKG".
zonecfg:SWZONE:fs> set special=/PKG----- Enter "set special=/PKG".
zonecfg:SWZONE:fs> set type=lofs----- Enter "set type=lofs".
zonecfg:SWZONE:fs> set options=ro----- Enter "set options=ro".
zonecfg:SWZONE:fs> end----- Enter "end".
zonecfg:SWZONE> commit----- Enter "commit".
zonecfg:SWZONE> exit----- Enter "exit".
```

Once specified, the product media contents copied in the Global Zone can be referred to as the read-only file system from the /SWPKG directory of Non-Global Zone after the next startup of Non-Global Zone.

7) Log in the Non-Global Zone and install the Systemwalker system.

From the directory of Non-Global Zone which you can refer to, install the Systemwalker system in the same way as for the Global Zone or Linux.

```
# /SWPKG/unx/swsetup
```

The remaining steps are the same as those in Step 4) and subsequent steps that are explained in the previous section "Installation procedure in Solaris (Global Zone)."

If you need not refer to the Global Zone directories from the Non-Global Zone due to some reasons, you can release the setup by issuing the following commands. In such case, you must perform the operations only after shutdown of Non-Global Zone.

```
# zonecfg -z SWZONE
zonecfg:SWZONE> remove fs dir=/SWPKG
zonecfg:SWZONE> commit
zonecfg:SWZONE> exit
```

Information

Checking the installed products

Follow the procedure below to check the installed products.

1. Execute the following command:

   ```
   /opt/FJSVcir/cimanager.sh -c
   ```

   The Uninstall (middleware) tool will start and a list of product names will be displayed.

2. To refer to the details of the product information, enter the applicable product number.

   ```
   Loading Uninstaller...

   Installed software
   1. Systemwalker Operation Manager Enterprise Edition  <Vxx.x.x>

   Enter the number of the software to be uninstalled.
   [number,q]
   =>1

   <Product information>


   Uninstallation starts. Continue?
   [y,b,q]
   =>q
   ```

3. Enter "q" to terminate, and enter 'b' to go back to the previous information.

   Note that if you enter "y", the selected product will be uninstalled.

1.4.4 Notes After Installation

This section provides important notes to take into account after the installation has completed.

IPv6 single stack environment

It is not possible to build a Systemwalker Operation Manager Web server in an IPv6 single stack environment.

1.4.5 Tasks after Installation

Perform the following tasks after installation.

Continuous Execution mode for network jobs

If you have reinstalled Systemwalker Operation Manager in an environment where you have enabled the Continuous Execution mode by the "jmmode" command, reissue the "jmmode" command to enable the Continuous Execution mode.

1.5 Silent Installation

You can use the "Silent Installation" to install Systemwalker Operation Manager without entering the installation operator's name. The required information is automatically read from the "installation information files" you have created in advance. You can create these files using the Installation Support functions.

The advantages of Silent Installation are:

- You can create the installation information at each point.
- You can group the PCs for Systemwalker installation, and easily install Systemwalker appropriate to the user environment.

This section explains how to use the Silent Installation in the following steps.

- Creating an Installation Information File
- Performing the Silent Installation

Before starting the system installation, check the following points and take required actions given.

Referring to the related documents

The software ReadMe files and other documents on the Systemwalker Operation Manager product media provide basic notes on Systemwalker Operation Manager. Refer to these files as they have important information you should have.

Checking the operating environment

Check both the hardware and software resources required for operating Systemwalker Operation Manager. Refer to the *Systemwalker Operation Manager Technical Guide* for those resources.

1.5.1 Creating an Installation Information File

The installation information file contains all information required for Systemwalker installation such as the installation type and the destination directory.

You can create the installation information file on the Windows PC using the Installation Support functions as follows.

1. Insert the Systemwalker Operation Manager product media into the drive of the Windows PC where you create the Silent Installation information file. Create an installation information file using the product media of Systemwalker you want to install.
2. The Setup window will appear.
   - If creating an installation information file for server/client types and PC clients running on Windows, perform the following operations:
     a. If using Windows x86 media

        Click Installation Support Tool to start creating an environment for silent installation.

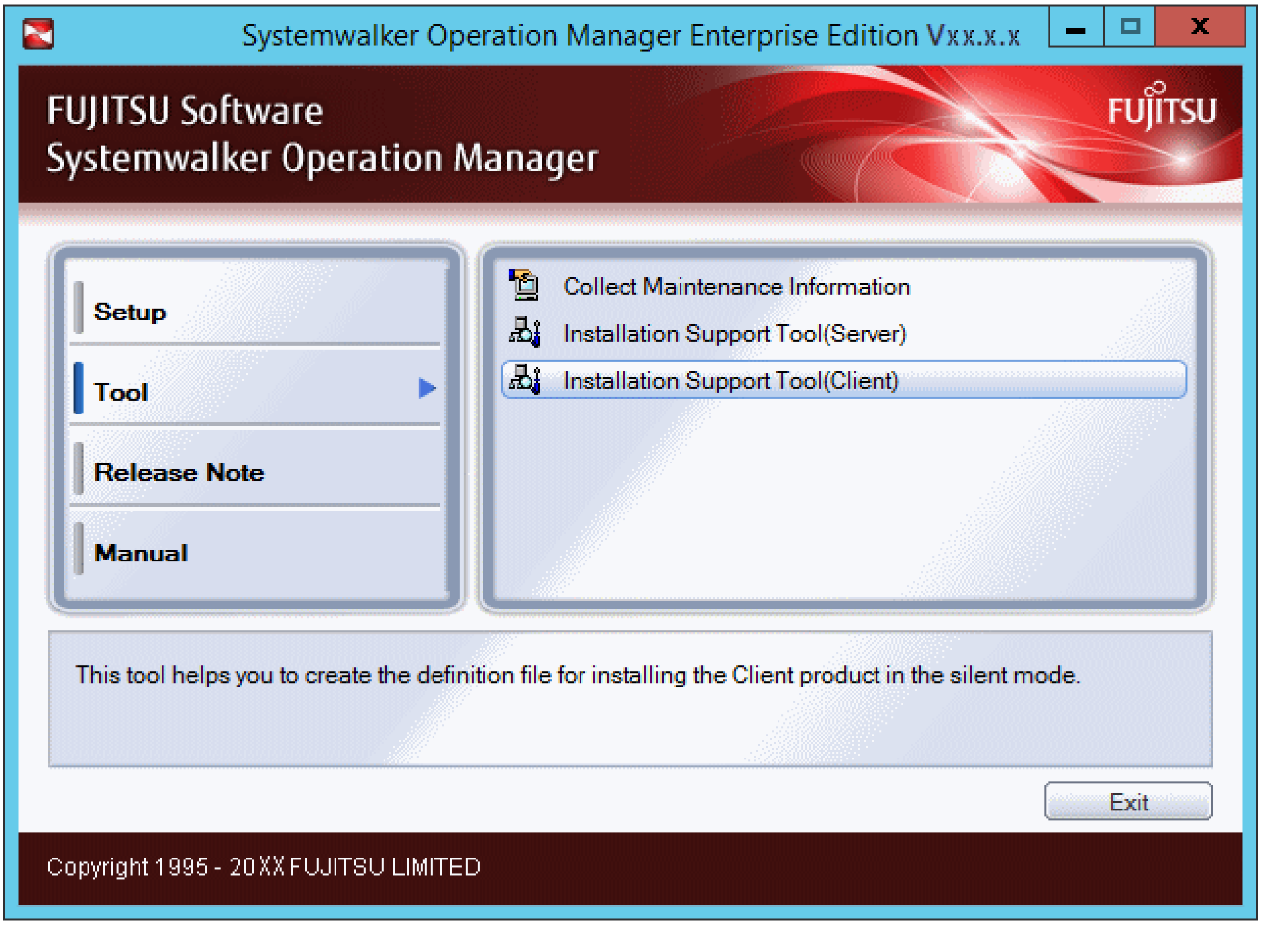
     b. If using Windows x64 media

        - If creating an installation information file for the server

        Click Installation Support Tool(Server) to start creating an environment for silent installation.

        - If creating an installation information file for the client

Click **Installation Support Tool(Client)** to start creating an environment for silent installation.



Systemwalker Operation Manager Enterprise Edition Vx.x.x.x

FUJITSU Software Systemwalker Operation Manager

This tool helps you to create the definition file for installing the Client product in the silent mode.

Copyright 1995 - 20XX FUJITSU LIMITED

FUJITSU
Setup
Tool
Release Note
Manual
Collect Maintenance Information
Installation Support Tool(Server)
Installation Support Tool(Client)
Exit

- When creating an installation information file for server types running on UNIX:

  Click **Terminates the Window** to close the **Setup** window.

  Issue the following command to start creating an environment for Silent Installation.

  Solaris

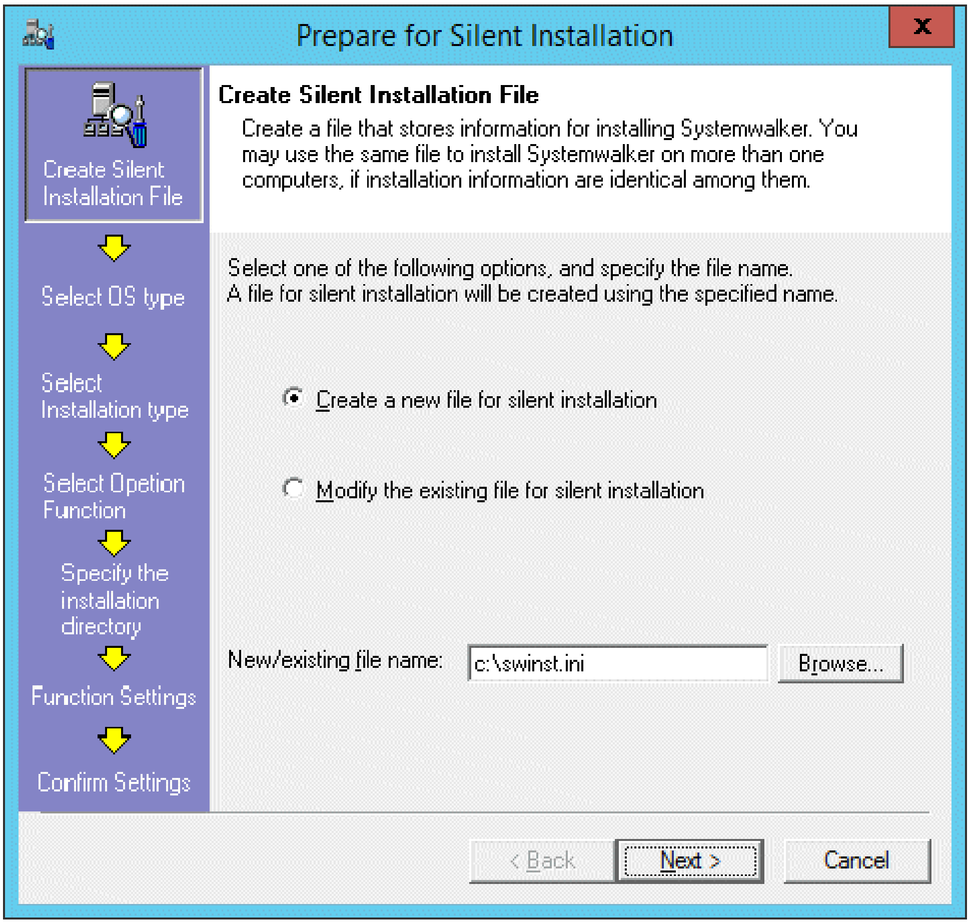
  ```
  <drive>\Solaris\tool_unx\sscmd\mkinst.exe
  ```

  Linux

  ```
  <drive>\Linux\tool_unx\sscmd\mkinst.exe
  ```

3. The **Create a Silent Installation File** window will appear.

   Select to create a new information file or to use an existing file, enter the installation information file name, and click **Next**.



Create Silent Installation File

Create a file that stores information for installing Systemwalker. You may use the same file to install Systemwalker on more than one computers, if installation information are identical among them.

Select one of the following options, and specify the file name.
A file for silent installation will be created using the specified name.

● Create a new file for silent installation

○ Modify the existing file for silent installation

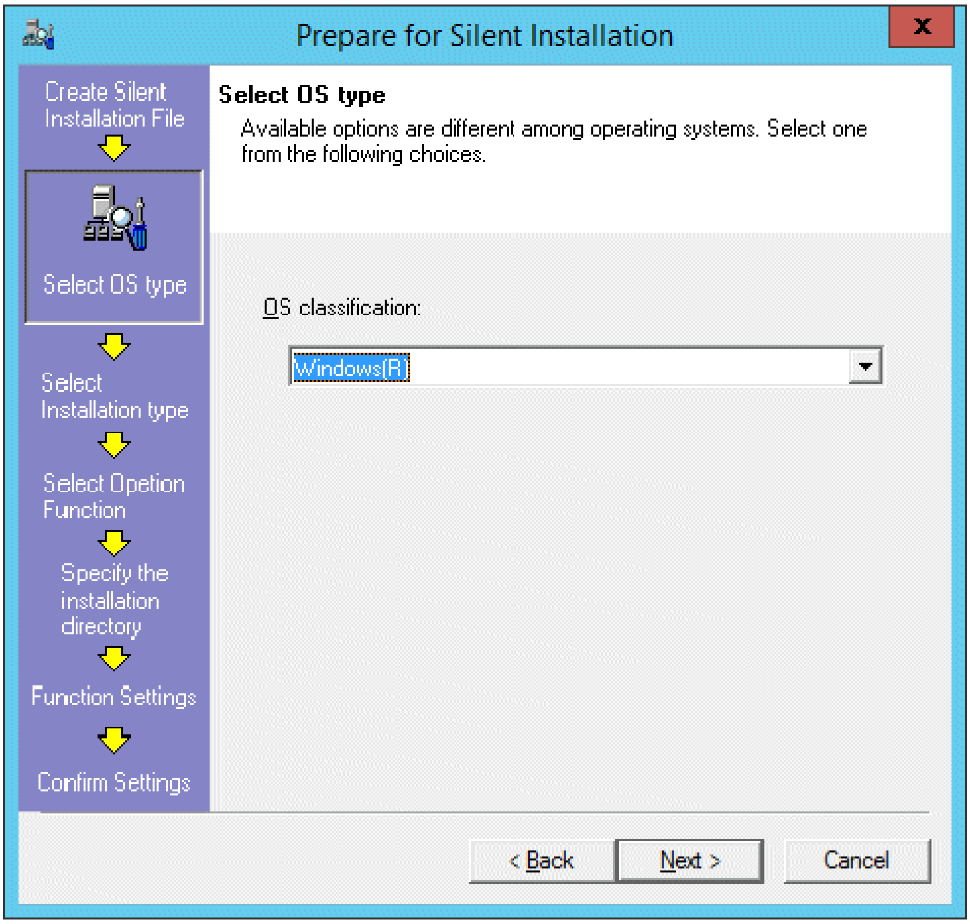
New/existing file name: c:\swinst.ini

Information

If the existing information is changed, the preset information is displayed in the subsequent windows.

4. The **Select an OS Type** window will appear.

   Select a Silent installation destination OS, and click **Next**.



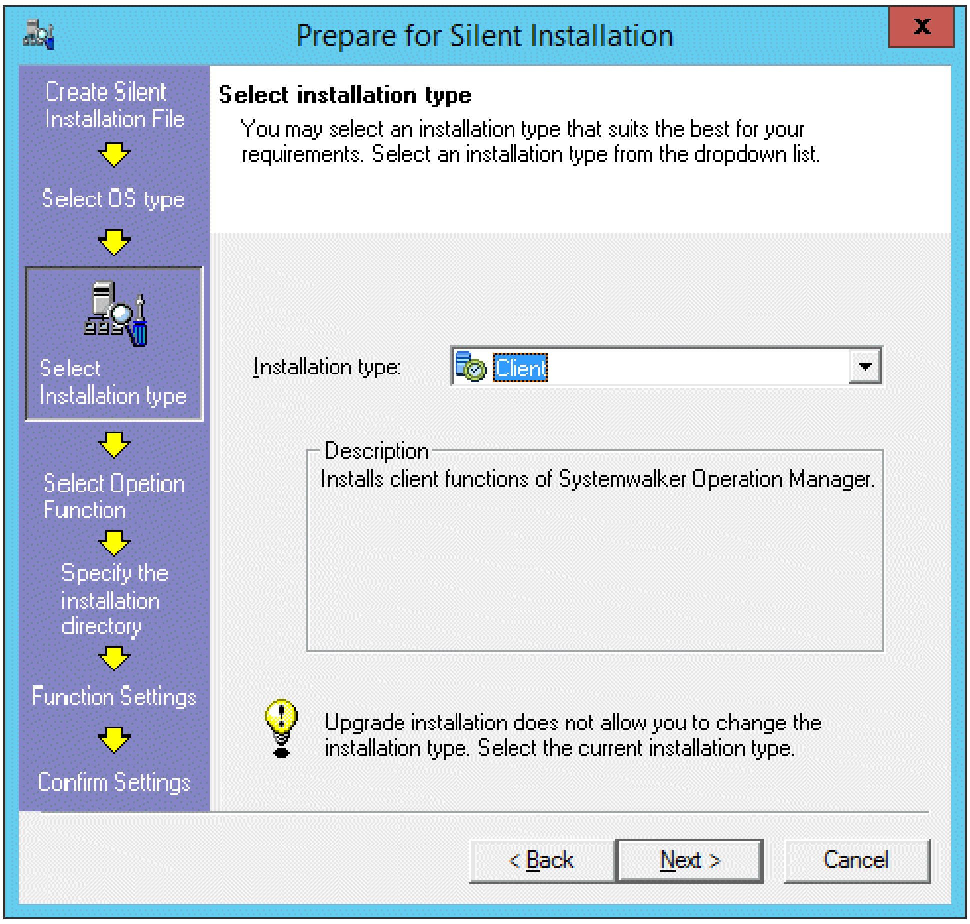
Select OS type

Available options are different among operating systems. Select one from the following choices.

OS classification: Windows(R)

5. The **Select Installation Type** window will appear.

   Select the installation type, and click **Next**.



Select installation type

You may select an installation type that suits the best for your requirements. Select an installation type from the dropdown list.

Installation type: Client

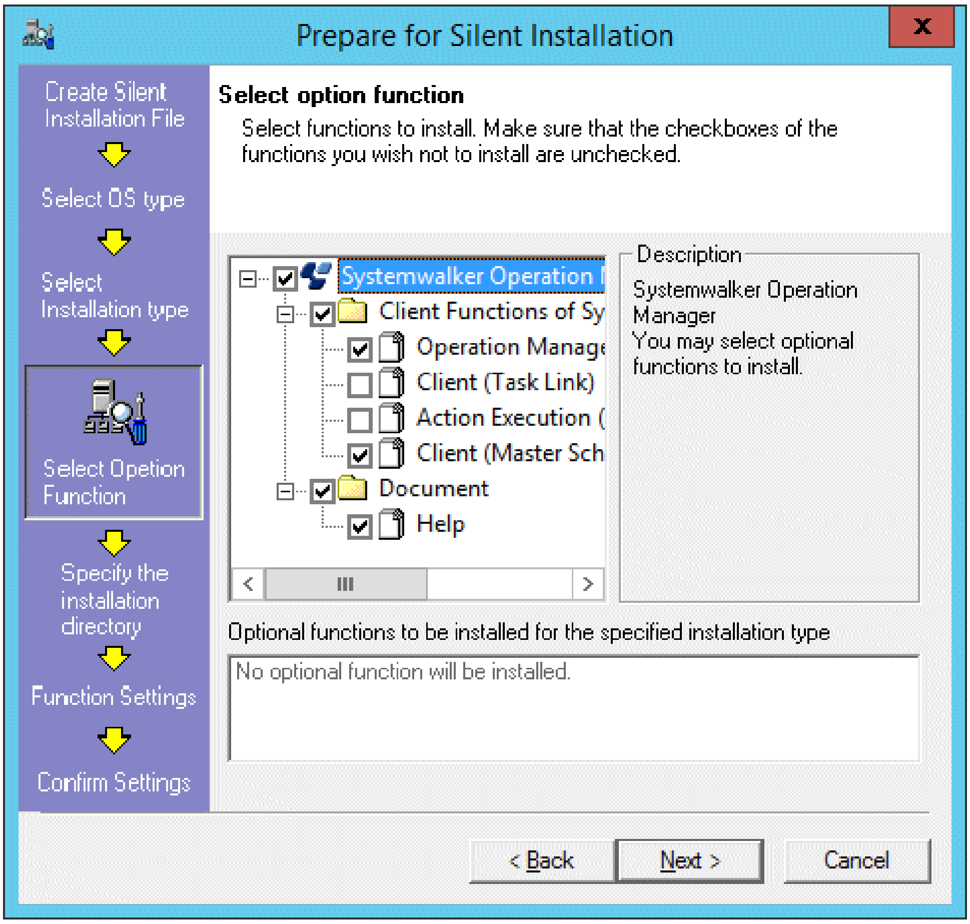
Description

Installs client functions of Systemwalker Operation Manager.

Upgrade installation does not allow you to change the installation type. Select the current installation type.

6. The **Select Option Function** window will appear.

   Select the functions you want to install, and click **Next**.



Prepare for Silent Installation

Select option function

Select functions to install. Make sure that the checkboxes of the functions you wish not to install are unchecked.

- ☑ Systemwalker Operation M
  - ☑ Client Functions of Sy
    - ☑ Operation Manage
    - □ Client (Task Link)
    - □ Action Execution (
    - ☑ Client (Master Sch
  - ☑ Document
    - ☑ Help

Description

Systemwalker Operation Manager
You may select optional functions to install.

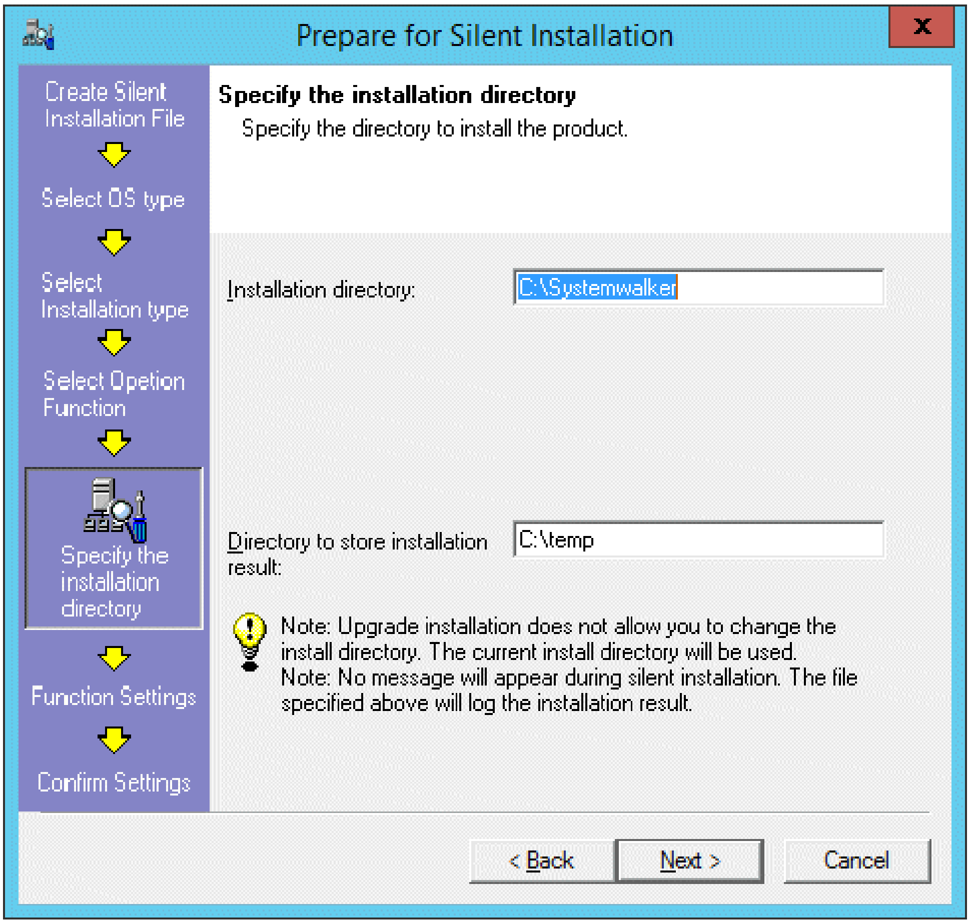
Optional functions to be installed for the specified installation type

No optional function will be installed.

7. The Specify the **Installation Directory** window will appear.

   a. If Windows(R) is selected in **Select OS type**:

      Specify the **Installation directory**, and click **Next**.



Specify the installation directory

Specify the directory to install the product.

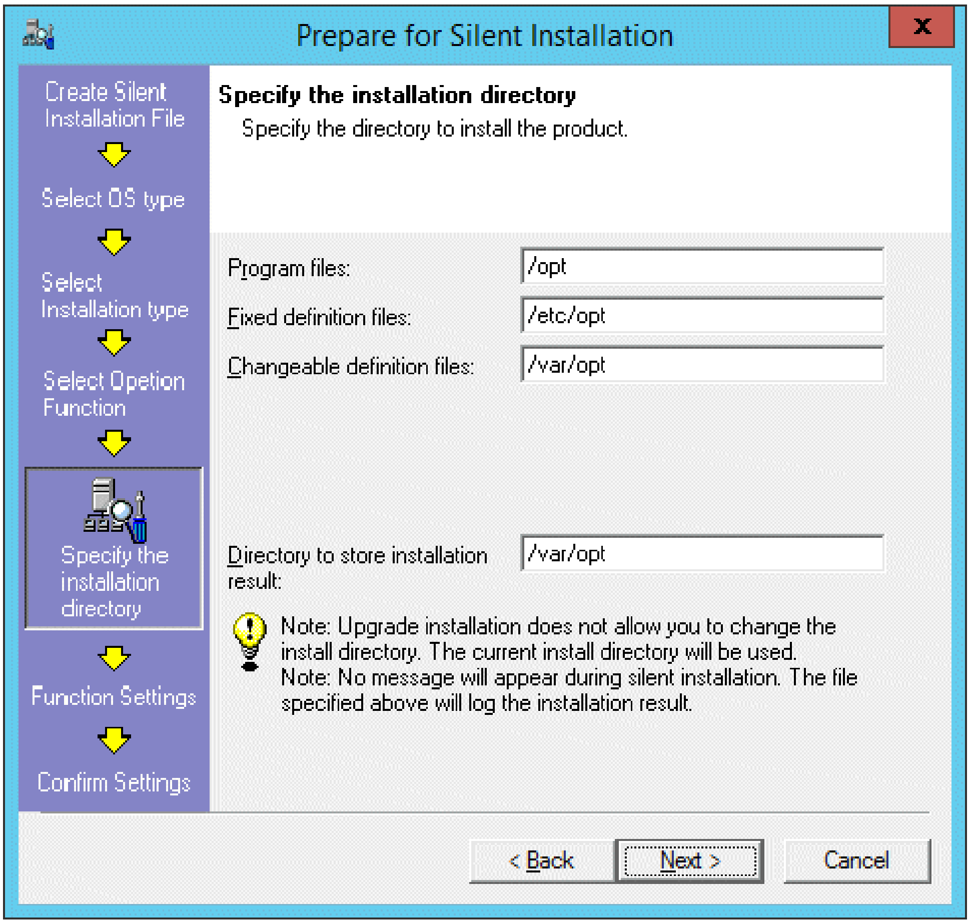
Installation directory: C:\Systemwalker

Directory to store installation result: C:\temp

Note: Upgrade installation does not allow you to change the install directory. The current install directory will be used.
Note: No message will appear during silent installation. The file specified above will log the installation result.

b. If an operating system other than Windows(R) is selected in **Select OS type**:

Specify the **Program files**, the location of **Fixed definition files** and the **Changeable definition files**, and click **Next**. In Linux, you cannot change an installation destination.



Specify the installation directory

Specify the directory to install the product.

Program files: /opt

Fixed definition files: /etc/opt

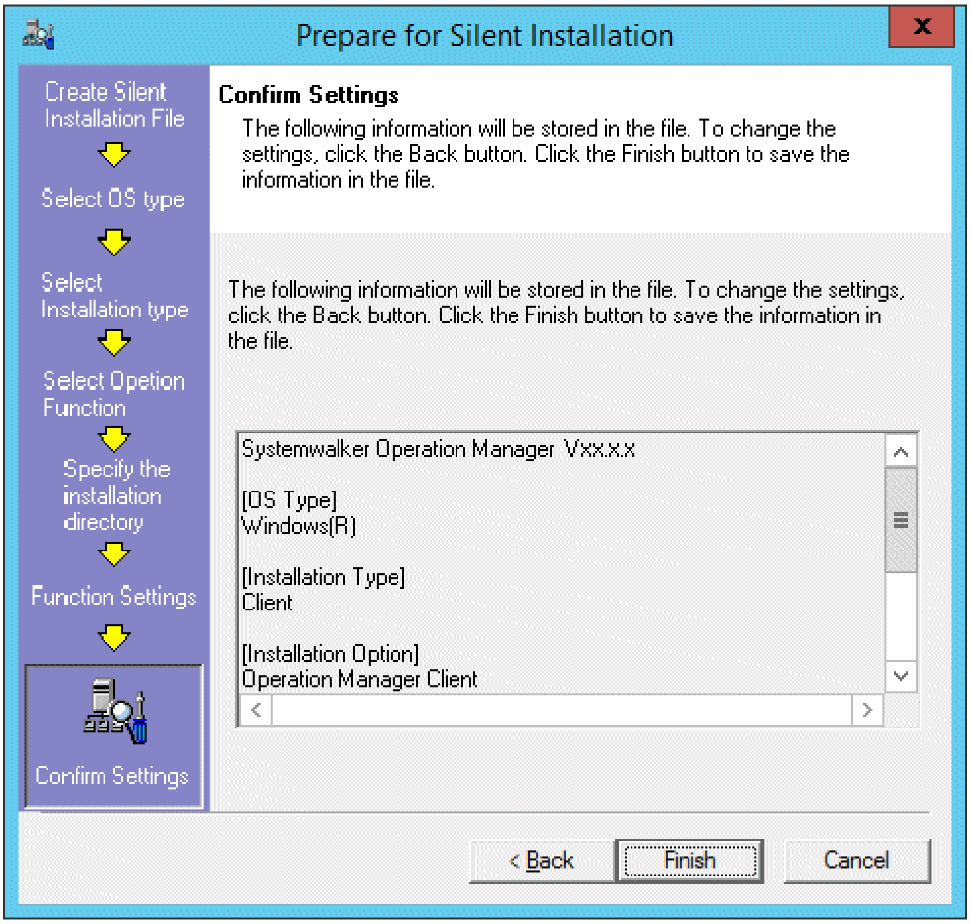
Changeable definition files: /var/opt

Directory to store installation result: /var/opt

Note: Upgrade installation does not allow you to change the install directory. The current install directory will be used.
Note: No message will appear during silent installation. The file specified above will log the installation result.

8. The following **Confirmation Settings** window will appear.

   Confirm your installation information, and click **Finish**.



Prepare for Silent Installation
Create Silent Installation File
Select OS type
Select Installation type
Select Opetion Function
Specify the installation directory
Function Settings
Confirm Settings

Confirm Settings

The following information will be stored in the file. To change the settings, click the Back button. Click the Finish button to save the information in the file.

The following information will be stored in the file. To change the settings, click the Back button. Click the Finish button to save the information in the file.

```
Systemwalker Operation Manager Vxx.x.x

[OS Type]
Windows(R)

[Installation Type]
Client

[Installation Option]
Operation Manager Client
```

Server Core environments

In Server Core environments, the installation support tool cannot be started. This means that the installation information file cannot be created.

Create the installation information file on another Windows computer (other than Server Core computers), and use FTP or some other method to transfer the file to the Server Core computer where the installation will be performed.

1.5.2 Performing the Silent Installation

Use the installation information file you have created for Silent Installation. The following explains how to perform the Silent Installation using this file. Install Systemwalker appropriate to the user environment.

Installation in the UNIX system

The following explains how to install Systemwalker Operation Manager in the UNIX system.

1. Log in as the superuser.

2. Copy the created installation information file to the PC where you want to install Systemwalker.

3. Mount the installation product media.

   Insert the installation product media into its drive. If the volume management daemon is not active, mount the drive. Check the correct drive device name as it may vary depending on the environment you use.

4. Issue the Silent Installation command as follows.

   Solaris

```
# <mount point>/Solaris/tool_unx/sscmd/swsilent.sh -i /work/swinst.ini -y
```

Linux

```
# <mount point>/Linux/tool_unx/sscmd/swsilent.sh -i /work/swinst.ini -y
```

```
swinst.ini: Instillation information file
```

For more information of the swsilent.sh command, refer to the *Systemwalker Operation Manager Reference Guide*.

The installation result is output with the following file names to a destination specified when the installation information file is created. Check the file as required.

Normal termination: swinst.success
Abnormal termination: swinst.err

When installing Systemwalker in Windows via network connection

The following explains the Silent Installation procedure via the network connection.

At the PC you use for Systemwalker installation

1. Mount the installation product media.
2. In Explorer, set the drive with the product media as a shared drive. (network drive A).
3. Copy the created installation information file to any location on the PC which you use for installation, and set the sharing at the destination. (network drive B)

At the PC where you install Systemwalker

1. Log on as a user belonging to the local Administrators group.
2. Using either of the following methods, connect network drive A and network drive B of the "PC you use for Systemwalker installation" to the network.
   - Run the "net use" command from a command prompt with Administrator privileges to map a network drive.
   - Use Explorer to map a network drive.
3. Issue the Silent Installation command as follows.

   Windows x86

   ```
   <network drive A> \MAIN\tool\sscmd\swsilent -i <network drive B>
   \<file name> -y (Note)
   ```

   Windows x64

   For server:

   ```
   <network drive A>:\MAIN\tool\sscmd\swsilent -i <network drive B>\<file name> -y
   (*1)
   ```

   For client:

   ```
   <network drive A>\Client\tool\sscmd\swsilent -i <network drive B>\<file name> -y
   (*1)
   ```

   ```
   File name: Installation information file
   ```

   ```
   *1: A UNC path cannot be specified for <network drive B>.
   ```

   For more information on the swsilent command, refer to the *Systemwalker Operation Manager Reference Guide*.

The installation result is output with the following file names to a destination specified when the installation information file is created. Check the file as required.

Normal termination: swinst.success
Abnormal termination: swinst.err

When installing Systemwalker in Windows during logon

The following explains the installation procedure by using the logon script under the domain environment.

At the PC you use for Systemwalker installation

The computer that is used for the installation work means a domain controller.

Specify a share name and installation information file using the full path name and alphanumeric characters.

1. Mount the installation product media.
2. In Explorer, set the drive with the product media as a shared drive.

   Set any name as the Share Name.

3. Copy the created installation information file to any location of the computer used for the installation work. Set the sharing of copied installation information file by using the Explorer. For the shared name, you can specify any name.

   The logon script template is stored in the following directory:

   Windows x86

   ```
   <CD-ROM drive>\MAIN\tool\sscmd\logonscr_japan.bat
   ```

   Windows x64

   For server:

   ```
   <drive>\MAIN\tool\sscmd\logonscr_japan.bat
   ```

   For client:

   ```
   <drive>\Client\tool\sscmd\logonscr_japan.bat
   ```

   For the method of setting the logon script, see the manual of your operating system.

At the PC where you install Systemwalker

The installation target computers should belong to the domain managed by the above mentioned computer used for the installation work (domain controller).

Log on the domain of PDC (the PC where you have created the installation information file) as the user belonging to the local Administrators group.

The preset logon script will be executed and the installation will start.

The installation result is output with the following file names to a destination specified when the installation information file is created. Check the file as required.

Normal termination: swinst.success
Abnormal termination: swinst.err

Note

When Systemwalker Operation Manager is installed on a Windows system, under certain conditions, it will start automatically upon the completion of the installation process.

If any of the following conditions are met, Systemwalker Operation Manager will not be started automatically when the installation completes:

- If Systemwalker Centric Manager has been installed
- If the installation is not a new installation
- If the Microsoft Visual C++ Redistributable package has been installed, the existing version is earlier than the version that is bundled with the product, and the conditions that require a restart are met

1.6 Uninstallation

This section explains how to uninstall Systemwalker Operation Manager.

1.6.1 Notes Prior to Uninstallation

To uninstall, log in as a user with administrator privileges.

Take the notes below into account when performing uninstallation.

User resources

When you uninstall Systemwalker Operation Manager, all files including user resources are deleted. To keep those resources, you must back them up before starting uninstallation. For the backup procedure details, see "3.1 Backup".

Uninstalling Systemwalker products

If any Systemwalker products are uninstalled from a system where the following product is installed, some files will still remain on the system after the uninstallation. Do not delete these files because they are used by Systemwalker common functions.

- Systemwalker Operation Manager V13.8.0 or later

Coexisting with Systemwalker Centric Manager

If you uninstall either of Systemwalker from the system where both Systemwalker Operation Manager and Systemwalker Centric Manager have been installed, part of Systemwalker files remains. Never delete those files as they are used by the remaining Systemwalker.

EE

Uninstallation from cluster system

If you are operating Systemwalker Operation Manager in the cluster configuration, you must shut down the cluster service for which Systemwalker Operation Manager is registered before its uninstallation. For the uninstallation details, refer to the *Systemwalker Operation Manager Cluster Setup Guide*.

Uninstalling the Redistributable package

The following Redistributable package will not be uninstalled automatically when Systemwalker Operation Manager is uninstalled. If required, perform the uninstallation manually.

- Installation type: Server
  Microsoft Visual C++ 2015-2019 Redistributable
- Installation type: Client
  Microsoft Visual C++ 2015 Redistributable

When updates have been applied

If there are updates that have already been applied to Systemwalker Operation Manager, remove the applied updates before the uninstallation.

Also, update the update application management registry configuration file after the uninstallation.

The procedure is as follows. Use the UpdateAdvisor (middleware) commands.

1. Execute the uam showup command and the uam remove -i <*update number*> command to remove all the updates applied to Systemwalker Operation Manager.

   Check the [Notes] section in the applicable patch information file for each update before removing it.

2. Uninstall Systemwalker Operation Manager.

3. Execute the uam setup -C <*update application management registry configuration file*> command to update the update application management registry configuration file.

1.6.2 Tasks Prior to Uninstallation

Perform the following tasks prior to uninstallation.

Stopping Systemwalker products

Before uninstalling, stop the following Systemwalker products.

- Systemwalker Operation Manager V13.8.0 or later

1.6.3 Systemwalker Uninstallation from the Windows System

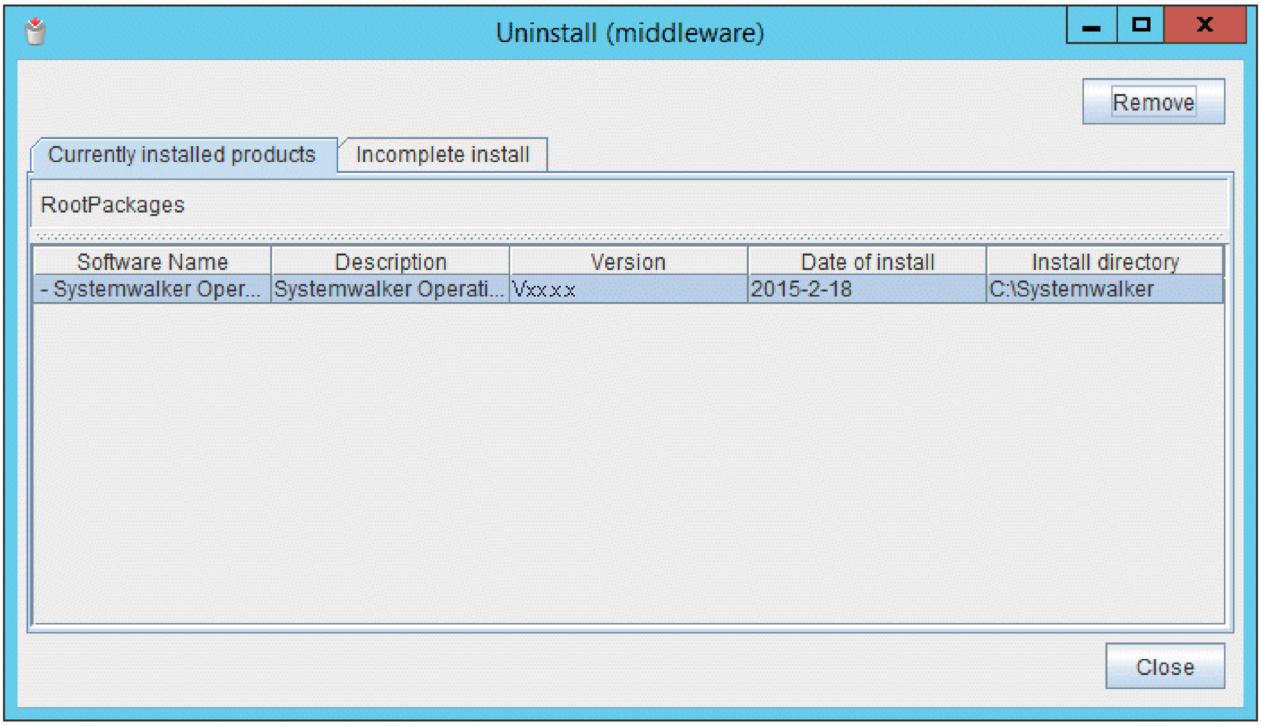
Explains the procedure of uninstalling Systemwalker Operation Manager.

Environments other than Server Core

To remove Systemwalker Operation Manager, follow the procedure below from the **Uninstall (middleware)** window.

1. Select **Start** or **Apps** >> **Fujitsu** >> **Uninstall (middleware)**.

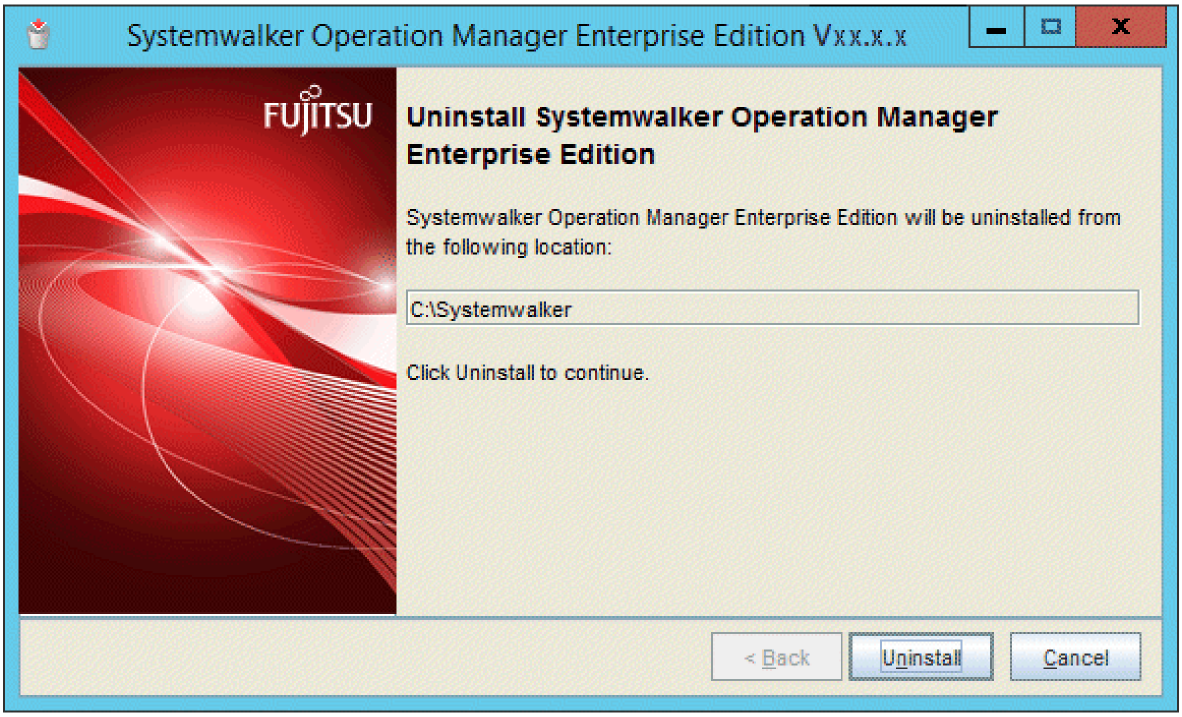
   The **Uninstall (middleware)** window will be displayed.



Software Name	Description	Version	Date of install	Install directory
- Systemwalker Oper...	Systemwalker Operati...	Vxx.x.x	2015-2-18	C:\Systemwalker

2. Select **Systemwalker Operation Manager** from **Software Name**, and click **Delete**.

   The **Systemwalker Operation Manager** uninstallation wizard will be displayed.



Systemwalker Operation Manager Enterprise Edition Vxx.x.x

Uninstall Systemwalker Operation Manager Enterprise Edition

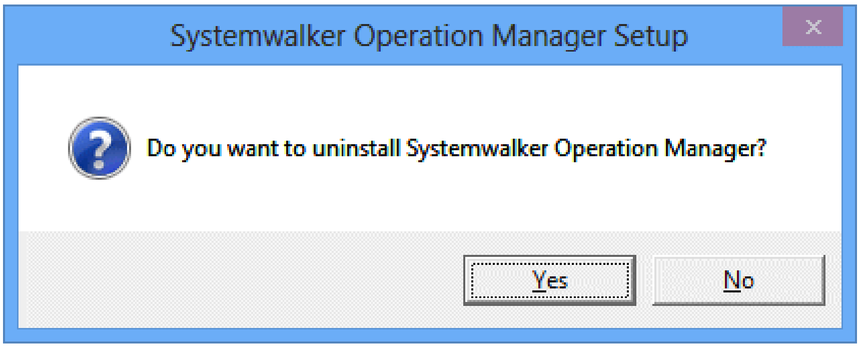
Systemwalker Operation Manager Enterprise Edition will be uninstalled from the following location:

C:\Systemwalker

Click Uninstall to continue.

3. Click **Uninstall**.

4. The **Systemwalker Operation Manager Setup** window will be displayed. Click **Yes**.



Systemwalker Operation Manager Setup

Do you want to uninstall Systemwalker Operation Manager?

5. When uninstallation completes, restart the operating system.

   Some files are deleted only when the operating system is restarted, so restart it to fully complete uninstallation.

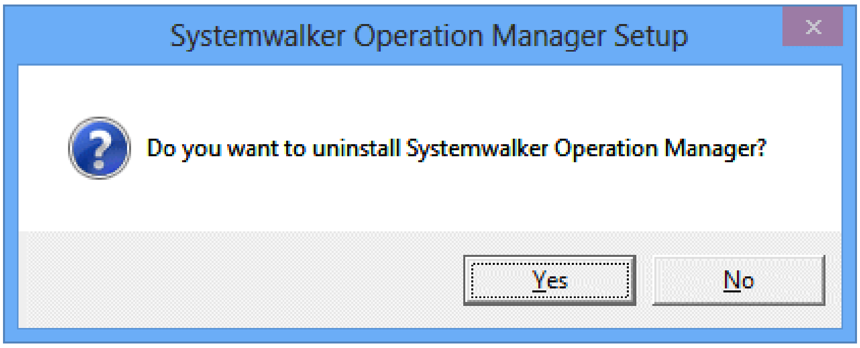
Server Core environments

To uninstall Systemwalker Operation Manager from a Server Core environment, follow the procedure below.

1. Execute the following command from the command prompt:

```
<Systemwalker Operation Manager installation directory>\MPWALKER.JM\jmunins
\swuset.exe
```

When this command is executed, the following window will be displayed, then click the **Yes** button.



Systemwalker Operation Manager Setup

Do you want to uninstall Systemwalker Operation Manager?

Refer to "swuset Systemwalker Operation Manager Uninstallation Command" in the *Systemwalker Operation Manager Reference Guide* for details on the command.

2. When uninstallation completes, restart the operating system.

   Some files are deleted only when the operating system is restarted, so restart it to fully complete uninstallation.

Uninstalling the Operation Manager client function and the .NET Framework

To uninstall the Operation Manager client function and the .NET Framework, first uninstall the Operation Manager client function and then uninstall the .NET Framework.

If the .NET Framework is mistakenly uninstalled before uninstalling the Operation Manager client function, reinstall the .NET Framework, uninstall the Operation Manager client and then uninstall the .NET Framework.

Refer to "Installing and uninstalling the .NET Framework" in "1.3.1 Notes Prior to Installation" for information on how to uninstall the .NET Framework.

Note

Current directory for uninstallation

The uninstallation may fail if the current directory is a directory below the Systemwalker Operation Manager installation directory. Move to another directory before executing the uninstallation.

Service shutdown during uninstallation

All Systemwalker Operation Manager services are stopped automatically when Systemwalker is uninstalled. If it coexists with Systemwalker Centric Manager in the same environment, the Systemwalker Centric Manager services are also stopped automatically.

However, those services may fail to stop or those services are not stopped. If it has occurred, cancel the uninstallation and manually stop those services. Then, restart uninstallation.

1.6.3.1 Notes After Uninstallation

This section provides important notes to take into account after the uninstallation has completed.

Files remaining without deleting

The following file is not deleted if you uninstall. If you do not need this file for the troubleshooting, delete it.

```
%SystemRoot%\mpjmuins.log
```

Note: %SystemRoot%: Installation directory for Windows Operating system

"FJQSS (Information Collection Tool)" and "Uninstall (middleware)"

If there are no Fujitsu middleware products other than Systemwalker Operation Manager, FJQSS (Information Collection Tool) will automatically be uninstalled when Systemwalker Operation Manager is uninstalled.

However, the Uninstall (middleware) tool will not be removed even if Systemwalker Operation Manager is uninstalled. The Uninstall (middleware) tool manages the information about other Fujitsu middleware products as well as Systemwalker Operation Manager. Do not uninstall this tool unless absolutely necessary. If you need to uninstall this tool, use the following procedure:

Uninstallation procedure

1. Start the Uninstall (middleware) tool, and ensure that no other Fujitsu middleware products exist.

   Select **Start** or **Apps** >> **Fujitsu** >> **Uninstall (middleware)** to display the **Uninstall (middleware)** window. Ensure that no other Fujitsu middleware products exist.

2. Execute the following uninstallation command:

   ```
   %SystemDrive%\FujitsuF4CR\bin\cirremove.exe
   ```

   When "This software is a common tool of Fujitsu products. Are you sure you want to remove it? [y/n]:" is displayed, enter "y" to continue with the uninstallation process. The product is then uninstalled.

If you mistakenly uninstall the Uninstall (middleware) tool, reinstall it using the following procedure:

Installation procedure

1. Log in to the machine where you need to perform the installation by using a user name belonging to the Administrators group, or switch to an account with administrator privileges.

2. Insert the Systemwalker Operation Manager product media into the drive, and execute the following installation command:

   Windows x86

   ```
   <drive>\MAIN\win32\CIR\cirinst.exe
   ```

   Windows x64

   For server:

   ```
   <drive>\MAIN\win32\CIR\cirinst.exe
   ```

   For client:

   ```
   <drive>\Client\win32\CIR\cirinst.exe
   ```

1.6.4 Systemwalker Uninstallation from the UNIX System

Uninstall the Systemwalker Operation Manager server.

Uninstallation procedure

1. Execute the following command:

   ```
   /opt/FJSVcir/cimanager.sh -c
   ```

   The Uninstall (middleware) tool will start and a list of product names will be displayed.

   ```
   Loading Uninstaller...

   Installed software
   1. Systemwalker Operation Manager Enterprise Edition  Vx.x.x

   Enter the number of the software to be uninstalled.
   [number,q]
   =>
   ```

2. Enter the number to the left of "Systemwalker Operation Manager", and press Enter.

   The Systemwalker Operation Manager uninstallation wizard will start.

```
Loading Uninstall (middleware)...

Installed software
1. Systemwalker Operation Manager Enterprise Edition  Vx.x.x

Enter the number of the software to be uninstalled.
[number,q]
=>1

The rest has been omitted



Uninstallation (middleware) will terminate.
```

Note

Current directory during Systemwalker uninstallation

If the current directory is under "opt/systemwalker," you cannot delete the "/opt/systemwalker" during Systemwalker uninstallation. Move the current directory to another location and execute the above command again.

Daemon shutdown during uninstallation

All Systemwalker Operation Manager daemons are stopped automatically when Systemwalker is uninstalled. If it coexists with Systemwalker Centric Manager in the same environment, the Systemwalker Centric Manager daemons are also stopped automatically.

/etc/rc.shutdown file (AIX version only)

From the /etc/rc.shutdown file, delete the following line added when Systemwalker was installed.

```
/opt/systemwalker/bin/poperationmgr -s
```

If you do not delete the line above, you will fail restart of the OS, disabling normal start of the system.

1.6.4.1 Notes After Uninstallation

This section provides important notes to take into account after the uninstallation has completed.

"FJQSS (Information Collection Tool)" and "Uninstall (middleware)"

If there are no Fujitsu middleware products other than Systemwalker Operation Manager, FJQSS (Information Collection Tool) will automatically be uninstalled when Systemwalker Operation Manager is uninstalled.

However, the Uninstall (middleware) tool will not be removed even if Systemwalker Operation Manager is uninstalled. The Uninstall (middleware) tool manages the information about other Fujitsu middleware products as well as Systemwalker Operation Manager. Do not uninstall this tool unless absolutely necessary. If you need to uninstall this tool, use the following procedure:

Uninstallation procedure

1. Execute the command below to start the Uninstall (middleware) tool. Ensure that no other Fujitsu middleware products exist.

   ```
   /opt/FJSVcir/cir/bin/cimanager.sh -c
   ```

2. Execute the following uninstallation command:

```
# /opt/FJSVcir/bin/cirremove.sh
```

When "This software is a common tool of Fujitsu products. Are you sure you want to remove it? [y/n]:" is displayed, enter "y" to continue with the uninstallation process. The product is then uninstalled.

If you mistakenly uninstall the Uninstall (middleware) tool, reinstall it using the following procedure:

Installation procedure

1. Log in to the machine where you need to perform the installation as superuser, or switch to an account with administrator privileges.
2. Insert the Systemwalker Operation Manager product media into the drive, and execute the following installation command:

   Linux (Red Hat Enterprise Linux 7)

   ```
   # <mount point>/Linux/RHEL7/unx/pkg/CIR/cirinst.sh
   ```

   Linux (Red Hat Enterprise Linux 8)

   ```
   # <mount point>/Linux/RHEL8/unx/pkg/CIR/cirinst.sh
   ```

   Solaris

   ```
   # <mount point>/Solaris/unx/pkg/CIR/cirinst.sh
   ```

Chapter 2 Definition of Operating Environment of Systemwalker Operation Manager

This chapter describes how to define the Systemwalker Operation Manager Operating Environment.

2.1 Outline of Operating Environment Definition

This section outlines the operating environment definition of Systemwalker Operation Manager.

System Definitions

Definitions about the system required to start using Systemwalker Operation Manager-

- Defining hosts in the "hosts" file

  Hosts should be defined in the "hosts" file when the Systemwalker Operation Manager client is used, when the Systemwalker Operation Manager Web Console is used, when network jobs are operated between servers and when the Systemwalker Operation Manager server is used in an IPv4/IPv6 dual stack environment.

- Changing Port Numbers

  The port numbers will need to be changed if they are being used by another product.

- Tuning system parameters [UNIX]

  For the UNIX version, the system parameters need to be tuned in order to ensure that Systemwalker Operation Manager runs stably.

Security Definitions

These definitions are required to operate Systemwalker Operation Manager securely. The definition items are as follows:

- Extended User Management function [UNIX]
- Access control
- Restricting execution users
- Audit log output

Common Systemwalker Operation Manager Definitions

Before defining environments specific to the Systemwalker Operation Manager functions, you need to define the environments that are common to the Systemwalker Operation Manager functions. The following items are defined:

- Monitored Hosts in Systemwalker Operation Manager
- Users
- Users (When using Extended User Management function) [UNIX]
- User restrictions
- Audit Log Output
- Encrypted communications (HTTPS communications) for the Web Console/Web API.
- This is required if using the Web Console/Web API.

EE

Definition of Multi-Subsystem Operations

Systemwalker Operation Manager Enterprise Edition supports a single server to operate multi-subsystems (Jobscheduler functions and Job Execution Control functions). This definition is required if you operate multi-subsystems. The following lists the required definition items.

- Creating a subsystem environment

- Assigning subsystem port numbers

You can also define the multi-subsystem operating environment after you have completed the operating environment setup explained in this chapter.

Definition of Power Control

In order to enable the power to the server to be turned on in response to a user logging in to a client, register the command for the power control function as a startup program on the client.

Definition of Jobscheduler

You need to define the following environments for the Jobscheduler.

- Defining Startup Parameters
- Defining a Message Table [Windows]
- Defining a Monitoring Permitted Host

Definition of Job Execution Control

You need to define the following environments for the Job Execution Control functions.

- Defining the System Operating Information
- Defining a Trust Host
- Defining the Job Owner Information [Windows]
- Defining the user control list for job execution [UNIX]

Definition of Event Monitoring [Windows]

You need to define the following environments for Event Monitoring.

- Defining the Event Monitoring environments (monitored log files)
- Defining the action execution environments (mail, Short Mail, and COM port)

Definition of Task Link

You need to define the following operating environments for Task Link.

- Defining a Password Management Book
- Definition for Task Link with Clients
- Defining the Host Information

Definitions when linking with Systemwalker Centric Manager

When monitoring the Jobscheduler by using Systemwalker Centric Manager's system monitoring functions, you must install Systemwalker Operation Manager's client functions in Systemwalker Centric Manager. Then, you must define the event logs to be output by the Jobscheduler in Systemwalker Centric Manager.

Definitions when constructing the existing environment on another server

After extracting the environment definition data and registration information from the currently operating server, you need to distribute them to another server.

Definition for maintenance

For maintenance of Systemwalker Operation Manager, you must complete the followings.

- Defining the Process Monitoring function
- Controlling the generation of maintenance information

Definitions when linking with Cloud Service to perform distributed execution by using Auto Scaling

By the notie from cloud service, you need to define ones that you can increase or decrease the execution server count of the host group according to the workload and resource usage.

2.1.1 Systemwalker Operation Manager Environment Setup Window

Most of the system operating environment can be defined from the **Systemwalker Operation Manager Environment Setup** window. The following explains how to open and use the **Systemwalker Operation Manager Environment Setup** window.

Only the system administrators (the users belonging to the Administrators group [Windows], the superuser [UNIX]), or the Operation Manager users having the administrative authority (when the Extended User Management function is valid in the UNIX system) can use the **Systemwalker Operation Manager Environment Setup** window. The **Systemwalker Operation Manager Environment Setup** window cannot be used if a user ID that does not have administrator privileges is specified in the **Systemwalker Operation Manager Environment Setup [Login]** window.

Note

Refer to "Support for Client and Server Connection" in the *Systemwalker Operation Manager Technical Guide* for details about the range of supported connections.

How to open the window

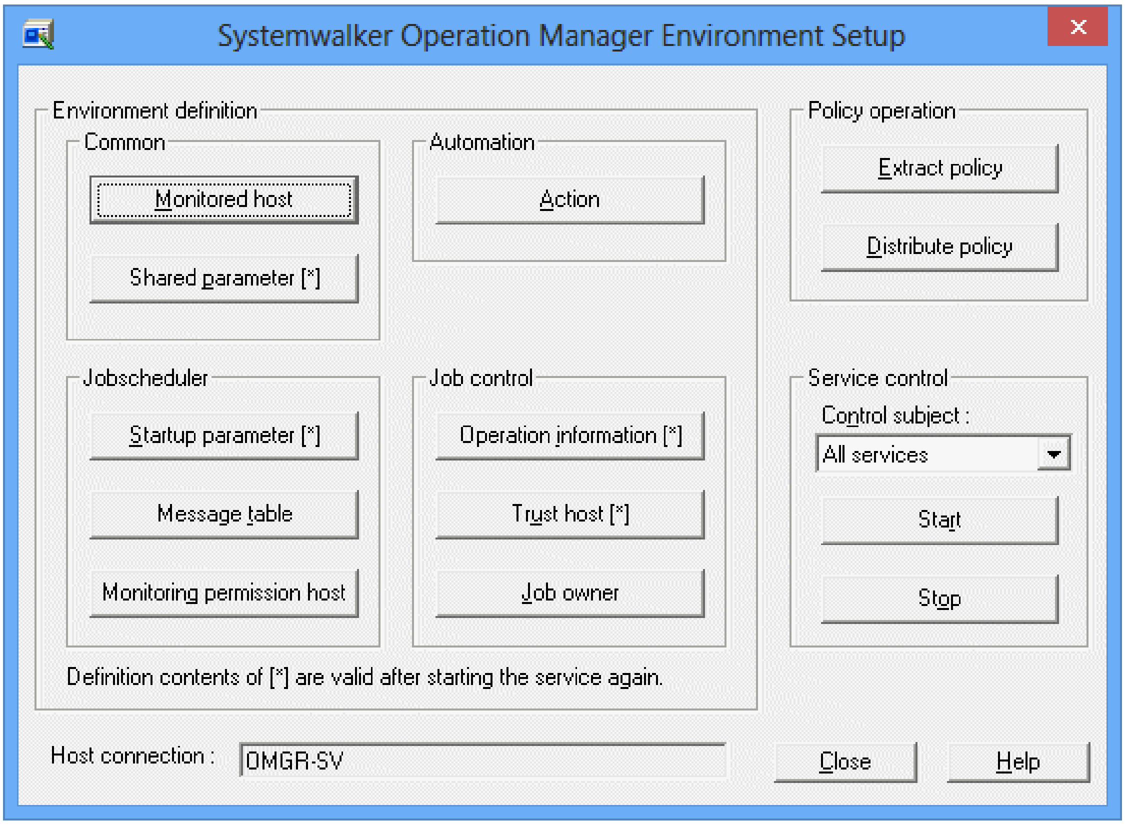
Select **Start** or **Apps** >> **Systemwalker Operation Manager** >> click **Environment Setup**. When the **Environment Setup [Login]** window appears, enter the destination connection and other required information, and click **Login.** (Note)

EE

Note:

When multi-subsystems are running on the server, the **Specify Subsystem Connection** window appears after the **Environment Setup [Login]** window. Select the destination subsystem number and click **OK**, and the **Systemwalker Operation Manager Environment Setup** window will appear.

Systemwalker Operation Manager Environment Setup window



Control subject : All services

Definition contents of [*] are valid after starting the service again.

Host connection : OMGR-SV

Common:

This explains the buttons used when defining common environments in Systemwalker Operation Manager.

Monitored host:

Opens the **Select Monitored Host Configuration** window.

Shared parameter:

Opens the **Define Operation Manager Shared Parameter** window.

Automation:

This explains the buttons used when defining the environment for the automation function.

Action [Windows]:

Opens the **Action Environment Setup** dialog box.

Jobscheduler:

This explains the buttons used when defining the environment for Jobscheduler functions.

Startup parameter:

Opens the **Define Jobscheduler Startup Parameters** window.

Message table [Windows]:

Opens the **Define Message Table** window.

Monitoring permission host:

Opens the **Define Monitoring Permission Host** window.

Job control:

This explains the buttons used when defining the environment for the Job Execution Control functions.

Operation information:

Opens the **Define Operating Information** window.

Trust host:

Opens the Define Trust Host window.

Job owner [Windows]:

Opens the Define Job Owner Information window.

Policy operation:

This explains the buttons for policy operation.

Extract policy:

Opens the Extract Policy window.

Distribute policy:

Opens the Systemwalker Operation Manager Distribution [Login] window.

[Windows]

Service control:

This explains the buttons used for service control.

Control subject:

This allows you to select a service to be started and stopped from a combo box. For details, see the Systemwalker Operation Manager Online Help.

Start:

Starts the selected services to be controlled. If services are already active, they are stopped first, then restarted.

Stop:

Stops the selected services from being controlled.

[UNIX]

Daemon control:

This explains the buttons used for daemon control.

Control subject:

This allows you to select a daemon or daemons to be started and stopped from a combo box. For details, see the *Systemwalker Operation Manager Online Help*.

Start:

Starts the selected daemons to be controlled. If daemons are already active, they are stopped first, then restarted.

Stop:

Stops the selected daemons from being controlled.

2.2 System Definitions

This section explains how to define the entire system of Systemwalker Operation Manager.

2.2.1 Defining the hosts File

The following explains how to define hosts in the "hosts" file.

Outline

Before using a Systemwalker Operation Manager's client, you must define the host name and IP address of the connected server machine in the "hosts" file stored on the client machine.

To use the Systemwalker Operation Manager Web Console, the host names and IP addresses of the hosts being monitored must be defined in the "hosts" file for the environment where the Web server is running.

In operations where network jobs are operated between servers, it is necessary to ensure that the IP address of the schedule server can be resolved from its host name. For this reason, register the host name and IP address of the schedule server machine in the "hosts" file on the execution server.

To use a Systemwalker Operation Manager server in an IPv4/IPv6 dual stack environment, define both the IPv4 and IPv6 addresses corresponding to the host name of the local host in the "hosts" file on the server.

Definition procedures

Edit the "**hosts**" file locating under the "<*System root*>\system32\drivers\etc" directory or the "etc" directory by using an editor, such as Notepad.

Note

/etc/hosts setting (Solaris/Linux versions)

With the default of the Red Hat type Linux or Solaris 11 or later, "127.0.0.1" is set in the /etc/hosts file as the IP address of the hostname of the local host. This can lead to the following issues:

- If a Systemwalker Operation Manager client or multi-server monitoring client is connected, it may not be possible to correctly monitor a server with this setting.
- If a network job is executed for another server from this server, it will take longer than expected to execute network jobs.
- If a network job is executed for another server from this server, the network job may end abnormally.

Therefore, the IP address for the host name of localhost configured in the /etc/hosts file during installation must be an address that can be connected from the client and from the execution server.

An example of /etc/hosts file settings is shown below:

[Before]

```
127.0.0.1 <host name> localhost
```

[After]

```
127.0.0.1 localhost
xxx.xxx.xxx.xxx <host name>
```

```
Note: xxx.xxx.xxx.xxx is the IP address for <host name> (localhost).
```

Notes

- Systemwalker Operation Manager can run in an environment where a WINS server is used.
- If you have used the DHCP server to dynamically assign an IP address to the server machine, you cannot start the Systemwalker Operation Manager's server functions. Make sure that the DHCP is not used. However, you can use the Systemwalker Operation Manager's client functions even in the environment where the DHCP server is used.

2.2.2 Changing Port Numbers

The following explains how to change port numbers for Systemwalker Operation Manager.

Initial values of port numbers

Systemwalker Operation Manager has the default port numbers (initial values assigned to ports) used by each Systemwalker Operation Manager function. For the default port numbers, see "C.1 Listing of Port Numbers".

If any of the following default port numbers is already used for another product, you must change it to an unused port number.

Definition procedure

You can change the port numbers used by Systemwalker Operation Manager in the following steps.

Changing a port number other than that of the Web Console/Web API function

1. Using an editor such as vi and Notepad, open the services file on the machine where the Systemwalker Operation Manager server and clients have been installed.
2. Specify both the service name of the function you wish to change and a new port number you use in the services file. If this service name is already written in the services file, change its port number only.

   Note that service names defined in the services file are case sensitive.
3. Restart Systemwalker Operation Manager.

Note

Notes for changing port numbers

When changing port numbers, note the following:

- The storage location of **services** file varies depending on the activated operating system (OS) as follows.

  If Windows Server is used:

  ```
  (System root) \system32\drivers\etc\services
  ```

  If UNIX server is used:

  ```
  /etc/services
  ```

- The port number for "mjsnet" is always required for communication when network jobs are executed between servers. If you change the port numbers for "mjsnet," they must be unique for all servers connected to the network.

  If any of the following occurs, you must define port numbers in the **services** file on all servers to be linked by the network job function.

  - The "mjsnet" port number other than "9327/tcp" has been defined in the **services** file on any of servers linked by the network job function.
  - A Windows server in SystemWalker/OperationMGRV5.0L30 or earlier is included in a server linked by the network job function.

EE GEE

Refer to "2.5.2 Assigning Subsystem Port Numbers" for information on port numbers when starting multiple subsystems.

Changing the port number of the Web Console/Web API function

1. Close all browsers displaying the Web Console. Also, do not send the request of Web API.
2. Log in as system administrator (user belonging to the Administrator group or superuser).
3. Execute the poperationmgr command to stop Systemwalker Operation Manager.
4. Execute the command below to output the Web server port definition file required for changing port numbers.

   [Windows]

   ```
   <Systemwalker Operation Manager installation directory>\MPWALKER.JM\mpjmweb\bin
   \mpowebconfig.bat -o <file name>
   ```

   [Solaris/Linux]

   ```
   /opt/FJSVjmweb/bin/mpowebconfig -o <file name>
   ```
5. Edit the Web server port definition file that was output, and change the relevant port number.

   Refer to the Reference Guide for information on the Web server port definition file.

6. Execute the command below for the changes to the edited Web server port definition file to take effect.

   [Windows]

   ```
   <Systemwalker Operation Manager installation directory>\MPWALKER.JM\mpjmweb\bin
   \mpowebconfig.bat -i <file name>
   ```

   [Solaris/Linux]

   ```
   /opt/FJSVjmweb/bin/mpowebconfig -i <file name>
   ```

7. Execute mpowebsetup (Web server setup command) with the -u option specified to remove the Web server settings.
8. Execute mpowebsetup (Web server setup command) without any option to set up the Web server.
9. Execute the soperationmgr command to start Systemwalker Operation Manager.

After the port number changes are complete, the Web server port definition file can be deleted if no longer required.

2.2.3 Tuning System Parameters [UNIX]

To run Systemwalker Operation Manager for UNIX version in stable condition, you must tune system parameters. Refer to the following table for the system parameters that need to be tuned, and their values. For some parameters, a value will be added to the preset value (the default value), while for others a value will be compared with the preset value and whichever is larger (the maximum) will be set. (When a value is added, refer also to the upper limit allowed by the system.) The "Type" column in the following table indicates which type each parameter is.

For more information on how to set system parameters, see the documents for respective operating systems.

With Solaris

Solaris 10 or later has the concept of projects. Systemwalker Operation Manager operates under the following projects.

- "system" project

  The project where the daemon and others existing in the initial OS environment operate

- "user.root" project

  The project which process gets operated during the initial OS setup environment with the root privilege.

Tuning system parameters

[Shared memory]

Parameter	Description	OS default value	Value	Type	Privilege
project.max-shm-memory	Maximum size of shared memory segment	The size of the physical memory of the OS (in bytes) / 4	70000 x the number of subsystems used (Note 1)	Addition	Privilege level

Note 1:

This is for EE version. For SE version, place 1 at "the number of subsystems in use".

If jobs that use shared memory are started from Systemwalker Operation Manager, it is necessary to set values for project.max-shm-memory for the system and user.root projects in the /etc/project file, taking the size of the shared memory used by the job process into consideration.

[Message Queue]

Parameter	Description	OS default value	Value	Type	Privilege
process.max-msg-qbytes	Maximum number of bytes of messages in queue	64 (KB)	(privileged, the number of simultaneously started job nets (Note 1) x 200 (Note 2), deny)	Maximum	Privilege level
project.max-msg-ids	Number of message queue identifiers	128	(privileged, 4 x the number of subsystems used (Note 3), deny)	Addition	Privilege level

Note 1:

When you use jobs having Job Execution Control attributes, add the number of simultaneously started jobs as well.

Note 2:

200 is a standard value. It changes depending on the host name and the path length to the output file.
Set an appropriate value after performing sufficient verification.

Note 3:

This is for EE version. For SE version, place 1 at "the number of subsystems in use".

[Semaphore]

Parameter	Description	OS default value	Value	Type	Privilege
project.max-sem-ids	Number of semaphore identifiers	128	2	Addition	Privilege level
process.max-sem-ops	Number of semaphore operations allowed per semop call	512	2	Maximum	Privilege level
process.max-sem-nsems	Number of semaphores per semaphore identifier	512	1	Maximum	Privilege level

[Stack Size]

Parameter	Description	OS default value	Value	Type	Privilege
process.max-stack-size	Maximum stack memory segment size that can be used by processes	8388608 (bytes)	2000000 (bytes) (*1)	Maximum	Basic level

*1: When operating Systemwalker Operation Manager only, you can use the default values only without any problem. When operating it together with other products, tune the system parameters according to the maximum values of other products.

Setting system parameters

Edit the /etc/project file to change system parameters.

Before setting any system parameters, check the default values and the upper limits of the values that can be set. Examples showing how to edit and check the settings are provided below.

```
# projects -l
```

Example showing how to edit /etc/project

This example sets the number of simultaneously started job nets to 80 and the number of subsystems in use to 5. The system has the 1G-byte physical memory.

```
system:0::::project.max-msg-ids=(privileged,148,deny);process.max-msg-
qbytes=(privileged,65536,deny);project.max-sem-ids=(privileged,
130,deny);process.max-sem-ops=(privileged,512,deny);process.max-sem-
nsems=(privileged,512,deny);project.max-shm-memory=(privileged,
268785456,deny);process.max-stack-size=(basic,8388608,deny)

user.root:1::::project.max-msg-ids=(privileged,148,deny);process.max-msg-
qbytes=(privileged,65536,deny);project.max-sem-ids=(privileged,
130,deny);process.max-sem-ops=(privileged,512,deny);process.max-sem-
nsems=(privileged,512,deny);project.max-shm-memory=(privileged,
268785456,deny);process.max-stack-size=(basic,8388608,deny)
noproject:2::::
default:3::::
group.staff:10::::
```

Checking system parameters

After performing the above settings, the following command can be used to check the information that has been set.

```
# projects -l
```

Confirmation command execution example

```
# projects -l
system
projid : 0
comment: ""
users : (none)
groups : (none)
attribs: project.max-msg-ids=(privileged,148,deny)
process.max-msg-qbytes=(privileged,65536,deny)
project.max-sem-ids=(privileged,130,deny)
process.max-sem-ops=(privileged,512,deny)
process.max-sem-nsems=(privileged,512,deny)
project.max-shm-memory=(privileged,268785456,deny)
process.max-stack-size=(basic,8388608,deny)
user.root
projid : 1
comment: ""
users : (none)
groups : (none)
attribs: project.max-msg-ids=(privileged,148,deny)
process.max-msg-qbytes=(privileged,65536,deny)
```

```
project.max-sem-ids=(privileged,130,deny)
process.max-sem-ops=(privileged,512,deny)
process.max-sem-nsems=(privileged,512,deny)
project.max-shm-memory=(privileged,268785456,deny)
process.max-stack-size=(basic,8388608,deny)
noproject
projid : 2
comment: ""
users : (none)
groups : (none)
attribs:
default
projid : 3
comment: ""
users : (none)
groups : (none)
attribs:
group.staff
projid : 10
comment: ""
users : (none)
groups : (none)
attribs:
```

Linux

Tuning system parameters

[Message Queue]

Parameter	Description	Value	Type
kernel.msgmnb	Maximum number of bytes of messages in queue	the number of simultaneously started job nets (Note 1) x 200 (Note 2)	Maximum
kernel.msgmni	Number of message queue identifiers	4 x the number of subsystems in use (Note 3)	Addition

Note 1:

When you use jobs having Job Execution Control attributes, add the number of simultaneously started jobs as well.

Note 2:

200 is a standard value. It changes depending on the host name and the path length to the output file.
Set an appropriate value after performing sufficient verification.

Note 3:

This is for EE version. For SE version, place 1 at "the number of subsystems in use".

EE

When operating multiple subsystems in Linux versions, the number of message queues is four times the number of subsystems. Therefore, it exceeds the maximum number of message queues that can be used. This may prevent the subsystems from starting.

If this happens, add the following settings to the /etc/sysctl.conf file to increase the maximum number of message queues that can be used. Restart the system after editing the file.

```
kernel.msgmni = 4x the number of subsystems used
```

[Semaphore]

Specify semaphore values for each parameter as shown in the following table.

```
kernel.sem = para1 para2 para3 para4
```

Parameter	Description	Value	Type
para1	Maximum number of semaphores for each semaphore identifier	1	Maximum
Para2	Number of semaphores in entire system	2	Addition
Para3	Maximum number of operators for each semaphore call	2	Maximum
Para4	Number of semaphore identifiers in entire system	2	Addition

Tuning procedure (Red Hat Enterprise Linux 7 or later)

1. Use the following command to check the values of the parameters in the above table that have been set in the current system:

```
#/sbin/sysctl -a
```

2. Compare the current settings with those in the above table (under "Tuning system parameters"), then calculate an appropriate setting based on the Maximum and Addition type of each parameter.

3. Cleate new file in /etc/sysctl.d/.

   Example:

```
vim /etc/sysctl.d/customo.conf
```

4. Edit the records for tuning the system parameters in /etc/sysctl.conf as shown in the following example

   Example: When three subsystems are used and the number of simultaneously started job nets is set to 50:

```

kernel.sem=1100 38151 200 3309

kernel.msgmni=28
kernel.shmmax=4000000000
kernel.shmmni=25512
```

5. Save the setting file.

6. Use one of the following two methods to enable the above settings.

   Method 1: Reboot the system to apply the settings

```
# cd /
# /sbin/shutdown -r now
```

   Method 2: Use /sbin/sysctl -p to apply the settings (Above 3.)

```
# /sbin/sysctl -p /etc/sysctl.d/custom.conf
```

If this command is used, there is no need to reboot the system.

7. The output of the following command can be used to confirm that the new system parameter settings have been applied:

```
# /sbin/sysctl -a
```

Confirmation example

```
:
(Omitted)

:
kernel.sem = 1100 38151 200 3309
kernel.msgmnb = 65536
kernel.msgmni = 28
kernel.msgmax = 65536
kernel.shmmni = 25512
kernel.shmall = 2097152
kernel.shmmax = 4000000000
:
(Omitted)
:
```

With HP-UX

Tuning system parameters

[Message Queue]

- IPF version of HP-UX 11i V2

Parameter	Description	Value	Type
msgtql	Number of message headers	the number of simultaneously started job nets (Note 1) x 4	Addition
msgmnb	Maximum number of bytes of messages in queue	the number of simultaneously started job nets (Note 1) x 200 (Note 2)	Maximum
msgseg	Number of message segments	The number of simultaneously started job nets (Note 1) x 200 (Note 2) /The value of msgssz	Addition
msgmap	Number of entries in message map	The value of msgtql + 2 (Note 3)	Maximum
msgmni	Number of message queue identifiers	4 x the number of subsystems in use (Note 4)	Addition

- IPF version of HP-UX 11i V3

Parameter	Description	Value	Type
msgtql	Number of message headers	The number of job nets running	Addition

Parameter	Description	Value	Type
		simultaneously (Note 1) x 4	
msgmnb	Maximum number of bytes in a queue	The number of job nets running simultaneously (Note 1) x 200 (Note 2)	Maximum
msgmbs	Maximum size of the message queue (MB)	The number of job nets running simultaneously (Note 1) x 200 (Note 2)/ 1,000,000	Maximum
msgmni	Number of message queue identifiers	4 x the number of subsystems used (Note 4)	Addition

Note 1:

When you use job nets with Job Execution Control attributes, add the number of simultaneously started jobs as well.

Note 2:

200 is a standard value. It changes depending on the host name and the path length to the output file.
Set an appropriate value after performing sufficient verification.

Note 3:

Find the value of msgtql, and then make calculation based on that value.

Note 4:

This is for EE version. For SE version, place 1 at "the number of subsystems in use".

Tuning procedure

Use a system manager or similar tool to change the kernel parameters and recreate the kernel.

2.2.4 Setting Up SELinux

The following explains the settings required for Linux environments where the SELinux (Security-Enhanced Linux) function is enabled.

When a security violation message for the application to be executed as a job appears in the log output by SELinux

If the application to be executed as a job is the one with which domain transfer occurs, a security violation message to a file under the Systemwalker Operation Manager directory may appear in the log output by SELinux, depending on the privileges set for the domain where the application operates.

This security violation message is output as standard output or standard error output of this application is written in the file that Systemwalker Operation Manager manages. To suppress this message, it is necessary to grant 'sw_fjsvmjs_spool_t' that is the access right for the Systemwalker Operation Manager files to the domain where the application operates.

Describing the SELinux policy file

Describe the following content in the SELinux policy file:

```
allow <domain> sw_fjsvmjs_spool_t:file { write getattr };
```

The following example shows how to grant access rights to the sample_t domain:

```
allow sample_t sw_fjsvmjs_spool_t:file { write getattr };
```

In addition to the above case, the application executed from Systemwalker Operation Manager may output a security violation message. Under normal condition, when executing an application by logging on to the console, etc., that application operates in the unconfined_t domain. On the other hand, when executing an application from Systemwalker Operation Manager, that application operates in the initrc_t domain that is inherited from the Systemwalker Operation Manager daemon. Due to this difference, a security violation message may appear depending on the behavior of the job.

To resolve security violations, grant necessary access rights to the application based on the information in the log output by SELinux.

An example of granting access rights is shown below. In the actual environment, determine to which domain and what access rights should be granted according to the message that appears.

Example of granting access rights to the hostname_t domain

```
allow hostname_t self:capability { dac_override };
```

See

Refer to the Linux online manuals, etc. for how to grant access rights of the SELinux function.

When login failure to the FTP server to be used for Task Link or access failure to the file to be transferred occurs

Enabling SELinux may cause login failure to the FTP server to be used for Task Link or access failure to the file to be transferred.

This problem occurs since the access rights for the login directory, file to be transferred and storage directory have not been granted to the SELinux domain (example: the ftpd_t domain) where the FTP server belongs. To remove this problem, these access rights need to be granted to the SELinux domain where the FTP server belongs.

An example of granting access rights is shown below. In the actual environment, determine to which domain and what access rights should be granted according to the message that appears.

Example of granting access rights to the ftpd_t domain

```
allow ftpd_t chkpwd_t:process { siginh noatsecure rlimitinh };
allow ftpd_t home_root_t:dir search;
allow ftpd_t user_home_dir_t:dir { read search open };
```

Example of command execution that allows FTP to read/write the files under user's home directory

```
# setsebool -P ftp_home_dir on
```

See

Refer to the Linux online manuals, etc. for how to grant access rights of the SELinux function.

2.3 Security Definitions

This section describes the security functions provided by Systemwalker Operation Manager. Enter the definitions for these functions when it is necessary to improve the security of a system.

Extended User Management function [UNIX]

This function sets up user IDs that are separate from the user IDs registered with the operating system, and manages the users who can access Systemwalker Operation Manager.

See "2.4.3 Defining Users (When using Extended User Management Function) [UNIX]" for details.

Access control

This function controls access to projects.

Refer to "Setting up Access Permissions for Projects" in the *Systemwalker Operation Manager User's Guide* for details on the definition method. See "Appendix E Usage Restrictions Based on Access Rights" for a list of the menu items, operations, commands and APIs that can be used with different access rights. For Web API, refer to the each API of "Web API [Windows] [Linux] " in the *Systemwalker Operation Manager Reference Guide.*

It is also possible to restrict the users who can access Systemwalker Operation Manager directories and files.

See "2.4.5 Define User Restrictions" for details on the definition.

Restricting execution users

This function registers the users who are allowed to execute jobs.

[Windows]

Specify **Execute jobs under the respective job owner's authority** in the **Options** sheet of the **Define Operating Information** window. Then, click the **Define Job Owner's Information** button to display the **Define Job Owner's Information** window and register only those users who are permitted to execute jobs.

See "2.8.1 Defining the System Operating Information" and "2.8.3 Defining the Job Owner Information [Windows]" for details.

[UNIX]

Register the users who are permitted to execute jobs in the user control list for job execution. See "2.8.4 Defining the User Control List for Job Execution [UNIX]" for details on how to define this function.

Audit log output

This function outputs a record of the operations performed on Systemwalker Operation Manager to an audit log file.

See "2.4.6 Defining Audit Log Output" for details on how to define this function.

2.4 Common Systemwalker Operation Manager Definitions

Before defining environments specific to the Systemwalker Operation Manager functions, you need to define the environments that are common to the Systemwalker Operation Manager functions.

This section provides an overview of the definitions common to all functions, and explains how to specify those definitions.

2.4.1 Defining the Monitored Host in Systemwalker Operation Manager

To monitor and operate on multiple servers from the Systemwalker Operation Manager client, the multi-server monitoring client or the Web Console, the host names of the monitored servers must be defined in the **Select Monitored Host Configuration** window and the **Monitored Host Configuration** window.

Use the following procedure to define Systemwalker Operation Manager's Monitored Host.

Definition procedure

1. Display the **Select Monitored Host Configuration** window.

   In the **Systemwalker Operation Manager Environment Setup** window, click **Monitored Host**. The **Select Monitored Host Configuration** window appears.

2. Display the **Monitored Host Configuration** window.

   In Systemwalker Operation Manager, you can register multiple Monitored Host configurations.

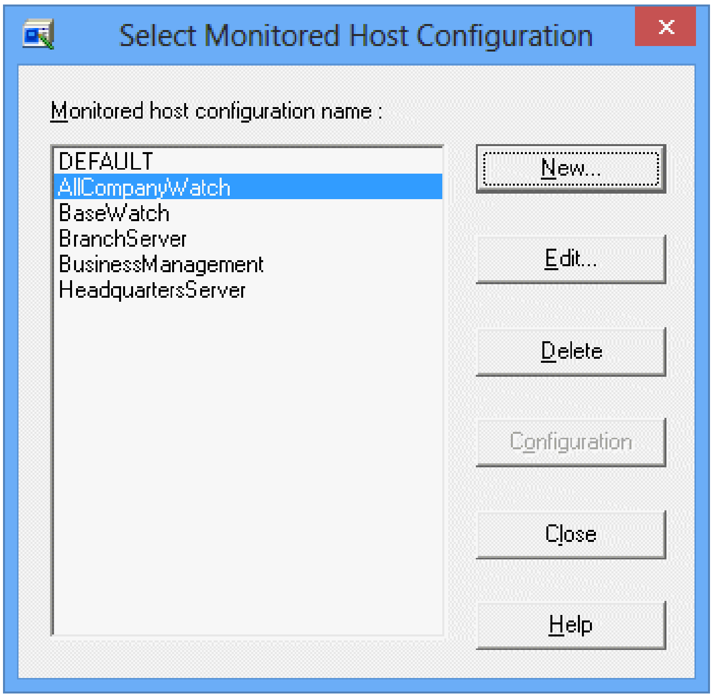
   Select Monitored Host from the **Select Monitored Host Configuration** window, and click **Edit**. To create new monitored host configuration, click **New**.

If you click **Edit**, the **Monitored Host Configuration** window for the selected monitoring host appears. If you click **New**, the **Monitored Host Configuration** window where only local host is defined appears.

Note

The monitored host definitions are used when the multi-server monitoring client or the Systemwalker Operation Manager Web Console is used. However, refer to the notes in "2.4.2 Defining Users" for information on user authentication for monitored hosts.

Select Monitored Host Configuration window



New button:

Displays the **Monitored Host Configuration** window where only local host is defined.

Edit button:

Displays the **Monitored Host Configuration** window for the monitored host configuration selected from the list of Monitored host configuration name.

Delete button:

Deletes the monitored host configuration selected from the list of Monitored Host Configuration name. You cannot delete the DEFAULT Monitored Host.

Configuration button [Windows]:

Reads the default Monitored Host information of Systemwalker Operation Manager from the configuration information database of the Operation Management Server where Systemwalker Centric Manager has been installed. On the computer where the **Systemwalker Operation Manager Environment Setup** window is running, Systemwalker Centric Manager must have been installed.

1. Define a folder.

   With the multi-server monitoring client and the Web Console, the servers that will be monitored or operated on can be grouped into folders and managed in a tree structure. To do so, select the root folder or any folder from the **Monitored Host Configuration** window, right-click for the pop-up menu, and click the **Add folder**. The **Folder Properties** window appears. Enter a folder display name and click **OK**. The entered folder display name will be registered.

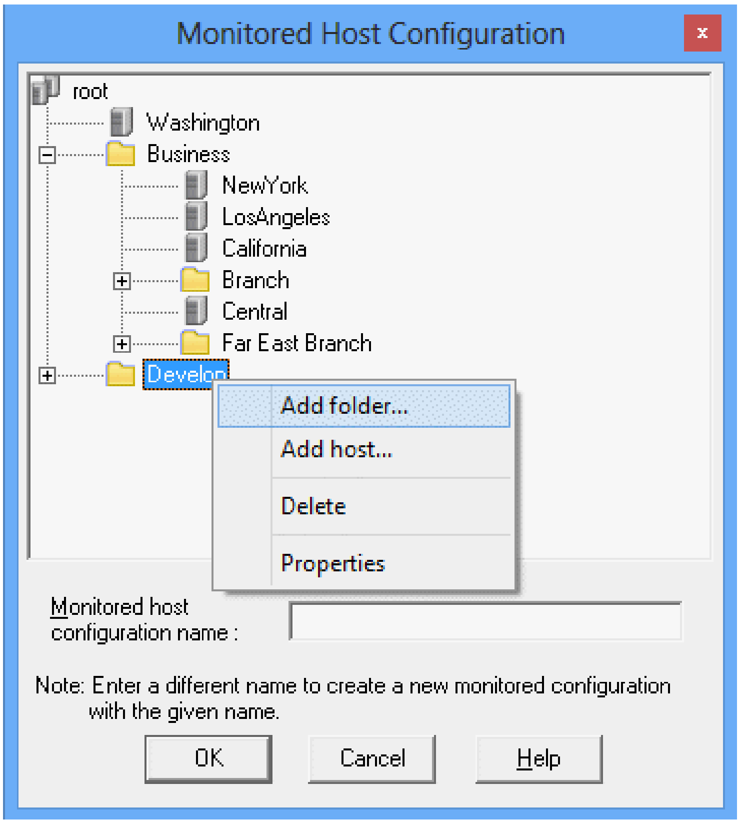
2. Define the host information for monitoring servers.

   Select the folder that you want to define in the **Monitored Host Configuration** window, right-click for the pop-up menu, and click **Add host**. The **Host Properties** window appears. Enter host information and click **OK**. The entered information (host information) will be registered.

3. Register monitored host configuration.

   In the **Monitored Host Configuration** window, specify **Monitored host configuration name**, and click **OK**. If you specify a new name, a new Monitored Host definition is added. If you specify an existing name, it is overwritten.

Monitored Host Configuration window



Note: Enter a different name to create a new monitored configuration with the given name.

Pop-up menu

You can select the following options from the shortcut menu (the popup menu displayed when you right-click).

Add folder:

Adds a new folder under the selected folder. When you click this menu, the **Folder Properties** window appears.

Add host:

Adds a new host under the selected folder. When you click this menu, the **Host Properties** window appears.

Delete:

Deletes the selected folder or host.

When you delete a folder, all information under that folder is deleted.

Properties:

Changes the property information of the selected folder or host. When you select a folder, the **Folder Properties** window appears. When you select a host, the **Host Properties** window appears.

Monitored host configuration name:

Specifies a Monitored Host definition name of up to 24 characters. The following characters can be used for specification.

- Alphanumeric characters, - hyphens (-), and underscores (_)

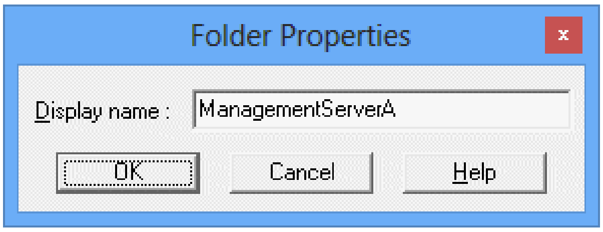
If you call it by pressing the **Edit** button in the **Select Monitored Host Configuration** window, the selected monitored host configuration name is displayed.

Information

The omgrmonitor command outputs the basic tree information of Systemwalker Centric Manager to a CSV format file, and reads it as the monitored host information of Systemwalker Operation Manager. Also, this command can output an already stored monitored host information to a CSV format file, and register the modified file as the monitoring host information again.

For the omgrmonitor command details, refer to the *Systemwalker Operation Manager Reference Guide*.

Folder Properties window

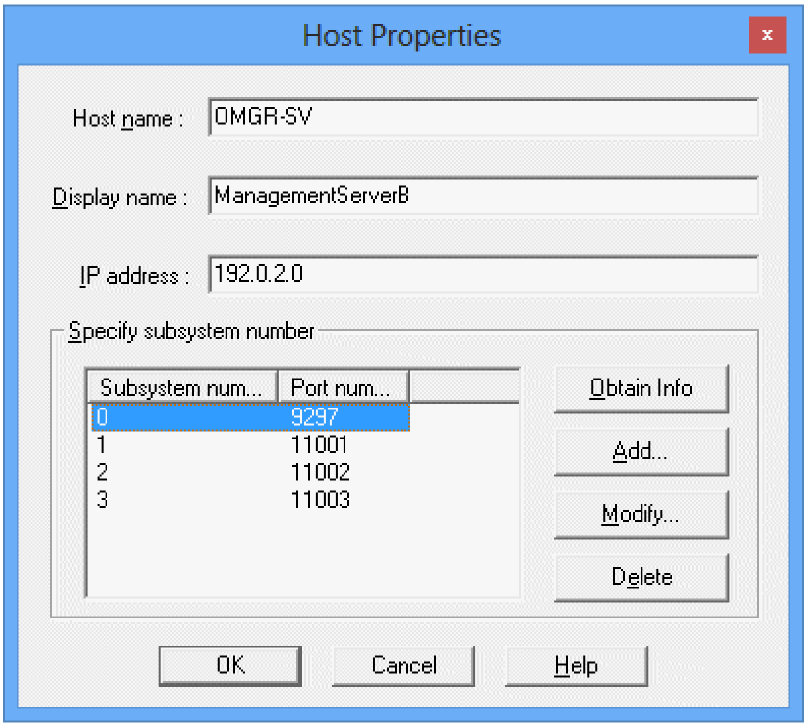


Display name : ManagementServerA

Display name:

Specifies a display name of up to 128 bytes. This is always required.

Host Properties window



Host name : OMGR-SV

Display name : ManagementServerB

IP address : 192.0.2.0

Specify subsystem number

Subsystem num...	Port num...
0	9297
1	11001
2	11002
3	11003

Host name:

Specifies the name of a host you want to define as a monitoring target server (DNS name) of up to 128 bytes.

It must be in the "host-name" or "host-name.domain-name" format. This is always required.

Display name:

Specifies a host name you wish to display using up to 128 characters. This can be omitted. The host name is set by default. This name is displayed in the tree.

IP address:

Specifies an IP address of a host you want to define as a monitoring target server. This can be omitted. If omitted, the name resolution is done on the server (that is, the IP address is mapped using the host name) when you click **OK** for registration. However, if the communication fails with the IP address evaluated by name resolution on the server, you need to manually set the IP address to allow connection from the client. If this setup is incomplete, the Jobscheduler and other screens may not be seen from the Systemwalker Operation Manager client.

If you need to explicitly define an IP address to allow communication from the client, see the following Reference Information "When you need to consider the IP address for connection from the client."

Subsystem number/Port number:

Shows subsystem and port numbers of monitored servers.

Subsystem number 0 and port number 9297 are displayed in the initial status. One or more numbers must always be specified. If multi-subsystems are NOT operated, subsystem number 0 is shown.

Obtain Info button:

Displays the **Enter Password of Connected Host** window when pressed. When the user ID and password for the administrator of the destination host are entered, information about the subsystem number and port number for the destination host is acquired automatically and added to the list.

Add button:

Displays the **Add/Change Subsystem Information** window. You can add subsystem and port numbers.

Modify button:

Displays the **Add/Change Subsystem Information** window. You can change subsystem number and port number selected on the list.

Delete button:

Deletes the subsystem information selected on the list.

Note

If you select a server from the **Connected host name** combo box of the **Systemwalker Operation Manager** window, you are connected to the host having the IP address you have specified in the **Host Properties** window.

Information

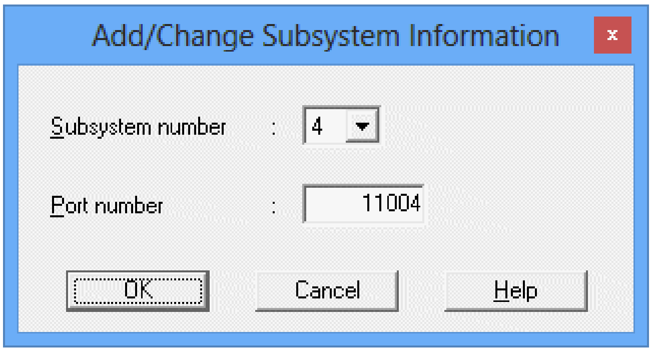
Reference Information: When you need to consider the IP address for connection from the client

The communication from the client may fail if you use the IP address evaluated by name resolution on the Systemwalker Operation Manager server. It may occur if:

- Multiple network cards have been installed, or
- Network Address Translation (NAT) has been installed in the network between the server and client.

In such conditions, you must explicitly define the IP address of the server which may be connected from clients in the **Host Properties** window.

Add/Change Subsystem Information window



Subsystem number:

Specifies a subsystem number. You can use 0 to 9 for specification.

Port number:

Specifies a port number of the subsystem you have selected in the **Subsystem number** field. The port number can be an integer of 1024 (a well-known number or larger) to 65535.

Note

Notes for IPv4/IPv6 dual stack environments

There are some notes to take into account for connecting clients and connection destination servers, in cases where the Systemwalker Operation Manager client and the connection destination server are both in an IPv4/IPv6 dual stack environment.

For the client to correctly identify the connection destination server, you must match the host name indicating the connection destination server and the content of the IP address definition with a. and b. below:

a. hosts file of the OS operated by the client

b. Monitored host definitions defined in the connection destination server (DEFAULT definition of the **Monitored Host Configuration** window)

Note that you must also match the version (IPv4/IPv6) of the IP address to be specified.

Systemwalker Operation Manager prioritizes the use of IPv4 addresses. For this reason, if you do not define the host name or IP address of the connection destination server in a. above, you must specify an IPv4 address as the IP address of b.

Information

Monitored host definitions when performing multi-server monitoring

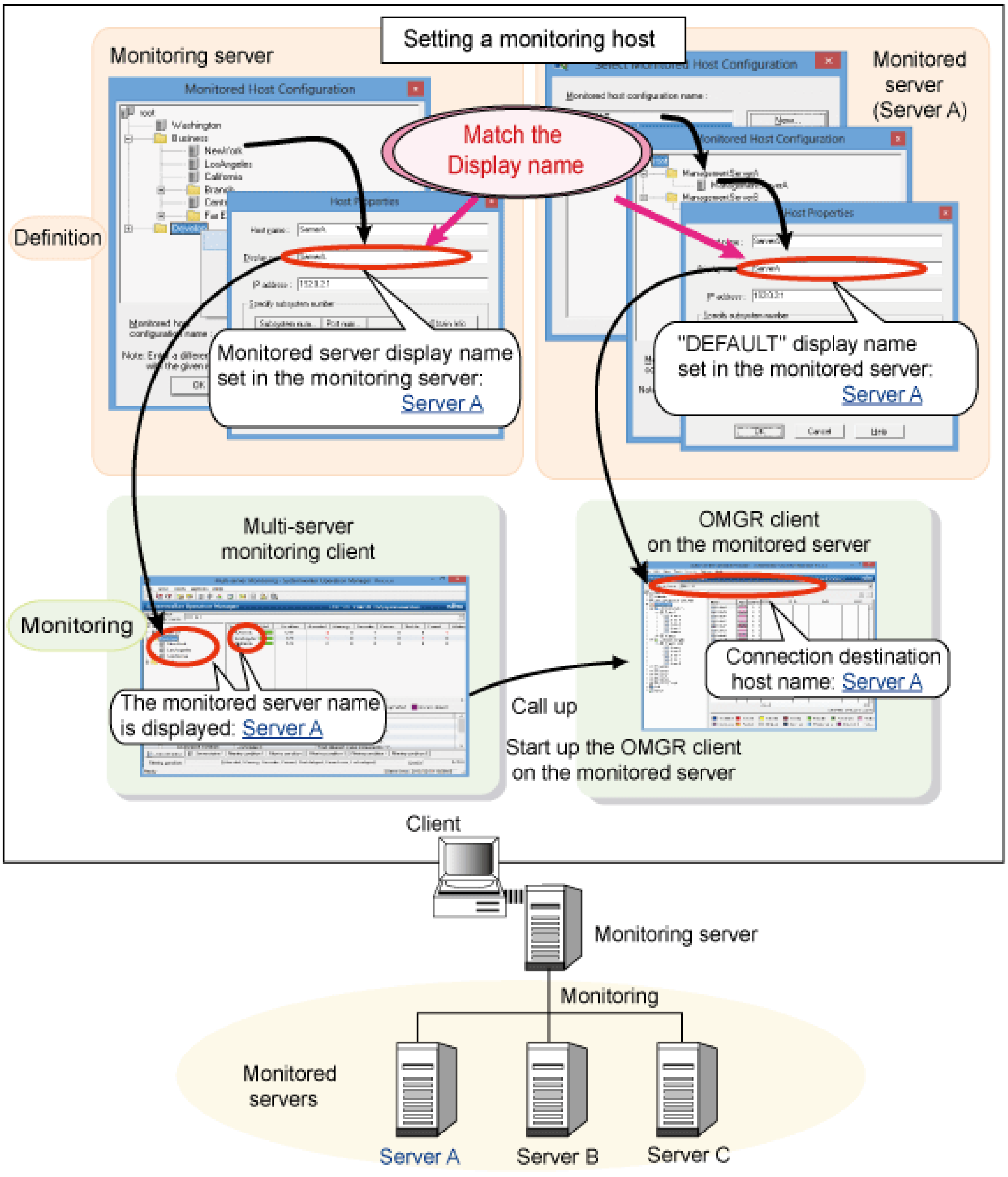
When the Systemwalker Operation Manager client on the monitored server is started from the multi-server monitoring client, the names of the servers (monitored server names) displayed in both windows below may be different:

- Name of the monitored server on the multi-server monitoring client's **Multi-server Monitoring** window
- Name of the server displayed as **Connected host name:** in the monitored server's **Systemwalker Operation Manager** window

If you wish to make the server names the same, you must match the display names in the respective definitions below:

- **Display name** in the **Host Properties** window of the monitored server, which is defined in the **Monitored Host Configuration** window of the monitoring server

- **Display name**, which is defined in the **Host Properties** window opened from the **Monitored Host Configuration** window, as the "DEFAULT" for the monitored server


Setting a monitoring host
Monitoring server
Monitored server (Server A)
Monitored Host Configuration
Host Properties
Match the Display name
Definition
Monitored server display name set in the monitoring server: Server A
"DEFAULT" display name set in the monitored server: Server A
Multi-server monitoring client
OMGR client on the monitored server
Monitoring
The monitored server name is displayed: Server A
Connection destination host name: Server A
Call up
Start up the OMGR client on the monitored server
Client
Monitoring server
Monitoring
Monitored servers
Server A
Server B
Server C

OMGR client: Systemwalker Operation Manager client

2.4.2 Defining Users

You must define users to allow using each Systemwalker Operation Manager function. The users who have been registered in the OS can use the Systemwalker Operation Manager functions.

For UNIX version, the users who have been registered in the Extended User Management function can use the Systemwalker Operation Manager functions. When you use the Extended User Management function, define users by seeing "2.4.3 Defining Users (When using Extended User Management Function) [UNIX]".

Also, with a user managed by OpenLDAP, you can use Systemwalker Operation Manager. When using a OpenLDAP, define users by referring to "2.4.4 Defining Users (When Using the LDAP) [UNIX]".

This section describes how to define users when the users who have been registered in the OS use the Systemwalker Operation Manager functions.

Outline

The following outlines how to define users.

1. Consider the users required for Systemwalker Operation Manager operation you use.

   Determine the users by referring to "2.4.2.1 User Control in Systemwalker Operation Manager" and "2.4.2.2 Job Execution Privileges"

2. Register users.

   Register users who can schedule, execute, and operate jobs. Use the OS functions to register those users.

Point

To allow general users to use projects when Systemwalker Operation Manager is operating, the system administrator should set up access rights for general users by referring to "Setting Access Rights for Projects" in the *Systemwalker Operation Manager User's Guide*.

Note

- If a general user logs in to the monitoring server from a multi-server monitoring client, the authentication processing for the monitored server will be performed using the user ID and password for the user that logged in to the monitoring server. Accordingly, to obtain information from the monitored server, register the same user ID and password on the monitored server (as was used to log in to the monitoring server).

- In multi-server monitoring, when some monitored servers are running an old version of Operation Manager, there may be some servers where the Extended User Management function or the user management function using a Systemwalker authentication repository is enabled and other servers where these functions are disabled. Even in such cases, servers can be monitored by setting up the same user ID and password (as for the user that logs in to the monitoring server) on each of the monitored servers.

- The Systemwalker Operation Manager Web Console performs authentication processing with monitored hosts by using the user ID and password that were used to log in to the Web Console. Accordingly, register users on the monitored hosts with the same user ID and password as the user that logs in to the Web Console.

- On the Systemwalker Operation Manager Web Console, when some monitored hosts are running an old version of Operation Manager, there may be some servers where the Extended User Management function or the user management function using a Systemwalker authentication repository is enabled and other servers where these functions are disabled. Even in such cases, hosts can be monitored by setting up the same user ID and password (as for the user that logs in to the Web Console) on each of the monitored hosts.

2.4.2.1 User Control in Systemwalker Operation Manager

The following explains how to control users in Systemwalker Operation Manager.

Installation

Perform the installation procedure as either a user belonging to the Administrators group (for the Windows) or a user with superuser privileges (for the UNIX).

Registering/deleting projects

Only the system administrator (the user belonging to the Administrators group in the Windows system or the superuser in the UNIX system) can register and delete projects.

Project owner

Only the system administrator (the user belonging to the Administrators group in the Windows system or the superuser in the UNIX system) can change the project's owner.

Setting access privileges to projects

Only the system administrator (the user belonging to the Administrators group in the Windows system or the superuser in the UNIX system) can register the users who can access to projects. The users must be assigned the following access privileges.

Windows system:

Select the group and user names from the domain or the list registered in the computer.

UNIX system:

Select the group and user names from the list registered in the computer.

Refer to "Setting up Access Permissions for Projects" in the *Systemwalker Operation Manager User's Guide* for details.

Monitoring/operating projects

The system administrator (the user belonging to the Administrators group in the Windows system or the superuser in the UNIX system) and the users who have been assigned the access privileges to a project can monitor and operate job nets, jobs or groups of the project.

Registering/changing job nets or groups

The system administrator, the project owner, or users having the update right and change right of a project can register and change job nets and groups of the project.

User restriction

Only the user registered in the swadmin group can start on-demand jobs, start job nets having Job Execution Control attributes, and execute Jobscheduler commands. For details, see "2.4.5 Define User Restrictions".

Command/API execution users

The user who has logged in the Systemwalker Operation Manager server can issue and execute Operation Manager's commands and API which operate on this server.

Web API execution users [Windows][Solaris]

The Web API running on the Systemwalker Operation Manager server is executed with user permissions that specified in the credentials.

Note

Notes on Solaris 10 or later

Solaris 10 or later provides the function to authorize job execution of each process separately. If you have limited the job execution in units of processes, even the user having the root privileges may be limited in his/her job execution.

For example, if you specify to suppress the process startup for files to be read when the shell is started, any operation from the shell is suppressed. In such case, the process is suppressed to start up even when a command provided by the Systemwalker Operation Manager is executed. Therefore, no user can execute jobs regardless of his/her command execution privileges.

2.4.2.2 Job Execution Privileges

The following explains the user privileges required to execute jobs in Systemwalker Operation Manager.

User privileges for job execution

The users having the following privileges can execute jobs in Systemwalker Operation Manager.

If the Execute job under the respective job owner's authority option is specified in the Windows system or if UNIX system is used:

Job type	Execution method	Specification of execution user	Privileges
Scheduled jobs	Started when job net startup conditions are satisfied or when operated.	Specified	Job execution user
Scheduled jobs	Started when job net startup conditions are satisfied or when operated.	Not specified	Project owner
On-demand jobs	Executed by the qsub command (Note 1)	Specified by "-cu" option	The user specified by "-cu" option
On-demand jobs	Executed by the qsub command (Note 1)	Not specified	The user who has logged in the Operation Manager server
On-demand jobs	Submitted from **Edit/ Submit Job Data** window	Cannot be specified.	The user who has logged in the Operation Manager server

```
Note 1) Also effective if the job submission API is used.
```

If the Execute job under the respective job owner's authority option is NOT specified in the Windows system:

Job type	Execution method	Specification of execution user	Privileges
Scheduled jobs	Started when job net startup conditions are satisfied or when operated.	Privileges for job execution are not changed even if specified.	Logon account of Job Execution Control services
On-demand jobs	Executed by the qsub command (Note 1)	Privileges for job execution are not changed even if specified.	Logon account of Job Execution Control services
On-demand jobs	Submitted from **Edit/ Submit Job Data** window	Cannot be specified.	Logon account of Job Execution Control services

```
Note 1) Also effective if the job submission API is used.
```

User privileges required for network jobs and Distributed Execution function

The account of network jobs and Distributed Execution function is inherited from the job submitting server to the destination server as follows.

If the job submitting server runs in the Windows system and if the Execute job under the respective job owner's authority option is specified:

Jobs are executed by the user having the privileges explained in "User privileges for job execution". Ensure that the following settings are the same on the server that submits the job and the server that receives the job, according to the operating system for the server that receives the job.

[If the server that receives the job is running the Windows version]

- Account and password

[If the server that receives the job is running the UNIX version]

- Account

If the following conditions are satisfied, jobs are executed under system administrator (superuser) privileges.

- The server that receives the job is running the UNIX version
- The executing user or project owner at the job submitting server belongs to the Windows Administrators group
-

If the job submitting server runs in the Windows system and if the Execute job under the respective job owner's authority option is NOT specified:

Jobs are executed by the logon account of Job Execution Control services.

The account of the executing user or project owner at the job submitting server needs to be registered in the destination server.

If the job submitting server runs in the Windows system, the Job Execution Control service logon account of the job submitting server and the job execution service logon account of the destination server must be the same.

When both of the following conditions are met, the submitted jobs are executed by the user having the system administrator (superuser) privileges.

- The job submitting server runs in the UNIX system.
- The executing user or project owner at the job submitting server belongs to the Windows Administrators group.

If the job submitting server runs in the UNIX system:

If the job submission server runs in the UNIX system, jobs are executed by the user having the privileges explained in "User privileges for job execution".

If the destination server runs in the Windows system, jobs are executed by the Job Execution Control service logon account. The account must match between the job submitting server and the destination server. Also, you must NOT specify the **Execute job under the respective job owner's authority** option. If it is specified, jobs are terminated abnormally.

Note

If the job submitting server is running in a UNIX system and the destination server is running in a Windows system, do not specify the **Execute jobs under the respective job owner's authority** option in the **Options** sheet of the **Define Operating Information** window. Otherwise, the job will terminate abnormally.

Point

If you specify an execution user to execute a job when using network jobs with the Distributed Execution function, the job will only be executed if the specified user has been registered as an OS user in both the job submitting server and the execution server.

Network jobs [UNIX]

		Job execution server	
		User is registered	User is not registered
Job submitting server	User is registered	Y	N
	User is not registered	Y	N

```
Y: The job is executed normally.
N: The job is NOT executed because an error occurs when the job execution request is
processed.
```

Network jobs [Windows] with the Distributed Execution function

		Job execution server	
		User is registered	User is not registered
Job submitting server	User is registered	Y	N
	User is not registered	N	N

```
Y: The job is executed normally.
N: The job is NOT executed because an error occurs when the job execution request is
processed.
```

2.4.3 Defining Users (When using Extended User Management Function) [UNIX]

This section describes how to define users when using the Extended User Management function.

Users registered and managed in Systemwalker Operation Manager using the Extended User Management function are hereinafter referred to as Operation Manager users, while users managed on operating systems are referred to as OS users.

Extended User Management function

For the UNIX version, the users who have been registered in Systemwalker Operation Manager can use its functions by using the Extended User Management function.

The Operation Manager user will be provided with administrator or non-administrator properties. The Operation Manager user registered as an administrator will have privileges to Systemwalker Operation Manager same as those of the conventional system administrator when performing operation from a client. The Operation Manager user with administrator's privileges can perform tasks which have been conventionally allowed only to the system administrator, such as project registration and Systemwalker Operation Manager environment setup.

However, you can execute commands on the server by the user privileges registered in the operating system even from a client. Registration of the Operation Manager user requires an OS user associated with the Operation Manager user (multiple Operation Manager users can be associated with one OS user). In addition, you must specify an OS user as an owner of the project and a user who can execute jobs.

Notice, you can not specify the user managed with LDAP as OS user associated with the Operation Manager user.

Overview of user definition when using the Extended User Management function

This section describes an overview of user definition when using the Extended User Management function

1. Consider the users required for Systemwalker Operation Manager operation you use. Consider the users by referring to "2.4.3.1 User Management of the Extended User Management Function" and "2.4.2.2 Job Execution Privileges".

2. Register an OS user if necessary. Use the operating system functions to register their users.

3. Define the Extended User Management function.

    1. Register an Operation Manager user and his/her password, if necessary.

       When distributing Operation Manager user information using the Policy Data Distribution function, you do not need to register the user in the policy data distribution destination server.

    2. Execute the command of the Extended User Management function to enable the Extended User Management function.

       You must also set it in the policy data distribution destination server.

3. Set the password for the "root" user (administrator).

   You must set it in the policy data distribution destination server.

For more information, see "2.4.3.2 Defining the Extended User Management Function".

4. Extract and distribute policy data, if necessary. For more information, see "2.13.3 Extracting/Distributing Policy Data when Using the Extended User Management Function [UNIX]".

Point

To allow general users to use projects when Systemwalker Operation Manager is operating, the system administrator should set up access rights for users without administrator privileges (such as general users) by referring to "Setting Access Rights for Projects" in the *Systemwalker Operation Manager User's Guide*.

Note

Users with administrator privileges

In Systemwalker Operation Manager, "Users with administrator privileges" refers to the users below.

- System administrators (users belonging to the Administrators group in the Windows system or superusers in the UNIX system)
- Operation Manager users having the Administrator's privileges if the Extended User Management function is valid in the UNIX version

2.4.3.1 User Management of the Extended User Management Function

This section explains how to control users by the Extended User Management function.

If the Extended User Management function is valid, only the Operation Manager user can operate the function from the Systemwalker Operation Manager client. The following explains the user management if the Extended User Management function is enabled.

Log into the Systemwalker Operation Manager server

If the Extended User Management function is enabled, you must log in the Systemwalker Operation Manager server as the Operation Manager user from each Systemwalker Operation Manager client.

If the Extended User Management function is disabled, log into it as an OS user.

Registering/deleting projects

If you log in as the Operation Manager user with administrator privileges, you can register or delete projects. The Operation Manager user without administrator privileges cannot register or delete projects.

Project owner

Be sure to specify an OS user as the owner of a project. You can specify either of a system administrator (superuser) or ordinary user.

If you log in as the Operation Manager user with administrator privileges, you can change the owner of the project. The Operation Manager user without administrator privileges cannot change the owner of the project.

Setting access privileges to projects

If you log in as an Operation Manager user, the user name displayed in the **Set Permissions** window is the Operation Manager user, not the OS user. Registration of users who can access projects is allowed only to the Operation Manager user with administrator privileges. To register them, select some from user names registered as the Operation Manager user.

Refer to "Setting up Access Permissions for Projects" in the *Systemwalker Operation Manager User's Guide* for details.

Monitoring/operating projects

The Operation Manager user with administrator privileges has the update right to all projects. The Operation Manager user without administrator privileges can operate projects to which their access privileges have been set.

Registering/changing job nets or groups

The Operation Manager user with administrator privileges or Operation Manager user with the update right and change right to projects can register and change job nets or groups from a client.

User restriction

Only the OS user associated with the Operation Manager users registered in the swadmin group can start on-demand jobs, start job nets having Job Execution Control attributes, and execute Jobscheduler commands. For details, see "2.4.5 Define User Restrictions"

Job execution user

Be sure to specify the OS user as the job execution user.

Command/API execution users

When executing commands provided by Operation Manager on the server, only the system administrator (superuser) can conventionally execute commands/API requiring system administrator privileges.

Conventionally, ordinary users can execute commands/API which are available to them and not restricted by the access privileges to projects.

For commands which are accessible to ordinary users and executed only when they have access privileges to projects, refer to the *Systemwalker Operation Manager Reference Guide*.

Web API execution users[Linux]

Specify the Operation Manager user in the authentication information of Web API.

2.4.3.2 Defining the Extended User Management Function

You must define the Operation Manager users to allow using each Systemwalker Operation Manager function.

Outline

Register the Operation Manager user and enable the Extended User Management function.

In addition, set a password for a user name, "root".

Note

Understanding "root"

The user name "root" in the Extended User Management function is registered by default as an Operation Manager user with administrator privileges. You cannot delete it.

Definition procedure

You must execute the following commands using the system administrator (superuser) privileges on the Systemwalker Operation Manager server.

For more information on the commands included in the procedure below, see the *Systemwalker Operation Manager Reference Guide - Security Command"*.

1. Register an Operation Manager user.

    1. Register an Operation Manager user using the **mpadduser** command.

        Select **administrator** or **non-administrator** as an attribute, and specify an OS user to associate with it.

        The following shows users who can be associated with Systemwalker Operation administrator or non-administrator.

Operation Manager user	OS user to be associated with
Administrator	System administrator (superuser)
Non-administrator	Ordinary users (other than superuser)

The OS user to be associated with the Operation Manager user must have been registered on the operating system. You cannot use the mpadduser command for registering the OS user.

2. Set a password using the **mpsetpasswd** command.

2. Enabling or disabling the Extended User Management function

   Issue the **mpsetusermode** command to enable the Extended User Management function.

   When the Extended User Management function is disabled, the operation is allowed only to the OS users even if Operation Manager users have been registered.

3. Register a password for "root".

   Set a password for "root" using the **mpsetpasswd** command.

To view the list of the registered Operation Manager users, use the mpusers command. To modify the registered Operation Manager user attributes, use the mpmoduser command, and to delete them, use the mpdeluser command, Use the mpusermode command to confirm if the Extended User Management function is enabled or not.

2.4.3.3 Extended User Management Function Setup Examples

This section shows the Extended User Management function setup examples.

Operation Manager user registration example

Assume that you have set the Operation Manager users as follows.

Operation Manager user	OS user	Privileges
root (Note)	root (system administrator)	Administrator
swroot	root (system administrator)	Administrator
swuser1	user (ordinary user)	Non-administrator
swuser2	user (ordinary user)	Non-administrator
swuser3	user (ordinary user)	Non-administrator
swguest	guest (ordinary user)	Non-administrator

Note 1:

The user name "root" is registered as an Operation Manager user with administrator privileges by default.
You cannot delete it. When using the user name "root", you must set a password.

When registering an Operation Manager user with administrator privileges, you must associate the OS user of the system administrator with it. When registering an Operation Manager user with non-administrator privileges, you must associate the OS user of the ordinary user with it.

Access privileges setup example

The Operation Manager user with administrator privileges has the update right to all projects as the Systemwalker Operation Manager administrator.

The Operation Manager user without administrator privileges can operate only projects to which their access privileges have been set based on the privileges they have.

The Operation Manager user with administrator privileges must set the access privileges of Operation Manager user without the administrator privileges, if necessary.

As privileges, the update right, Change right, operation right, and reference right are provided; the update right includes the Change right, operation right and reference right, and the Change right and operation right includes the reference right. The order of privilege strength is as follows.

```
Update right > change right / operation right > reference right
```

Assume that you set the access privileges as follows.

Project	Project owner	Access privileges to be set
Management project	root	Not set
user project	user	swuser1: Update right swuser2: Change right swuser3: Operation right
guest project	guest	swguest: Reference right swuser1: Reference right

Access privileges of the Operation Manager user

If you register Operation Manager users and set the access privileges as shown above, the Operation Manager users' access privileges to the projects are as follows.

Operation Manager user	Displayed project	Access privileges
root swroot	Management project	Update right
	user project	Update right
	guest project	Update right
swuser1	user project	Update right
	guest project	Reference right
swuser2	user project	Change right
swuser3	user project	Operation right
swguest	guest project	Reference right

Access privileges of the OS user

When the OS user is the system administrator, he/she has the update right to all projects. If the OS user is the general user and the project owner, he or she has the Update right to his/her own projects.

If the OS user is an ordinary user but not the project owner, he or she has the highest level of privileges out of the access privileges of multiple Operation Manager users who have been associated with the OS user (Update right > Change right / Operation right > Reference right).

Note if an OS user that executes commands or APIs has been associated with multiple Operation Manager users and both change rights and operation rights have been set up, then the OS user will have both rights.

If you register the Operation Manager users and set the access privileges as shown above, the associated OS user's access privileges to the projects are as follows.

OS user	Project	Access privileges to projects when executing command	Description
root	Management project	Update right	The "root" OS user is the system administrator, and so has update rights for all projects.
	user project	Update right	
	guest project	Update right	
user	user project	Update right	For the "user" project, "swuser1" has update rights, "swuser2" has operation rights and "swuser3" has change rights, and so the OS user "user" will have update rights to the "user" project.
	guest project	Reference right	For the "guest" project, "swuser1" has reference rights, and so the OS user "user" will have reference rights to the "guest" project.
guest	guest project	Update right	The OS user "guest" is the owner of the "guest" project and so has update rights to the "guest" project.

2.4.4 Defining Users (When Using the LDAP) [UNIX]

This section explains the managing user when using the OpenLDAP.

Beginning with, the user and the group managed by OpenLDAP are called LDAP user and LDAP group, respectively.

If you use the Extended User Management Function, you cannot use this LDAP function. Also, if the Systemwalker Centric Manager V15.3.0 or earlier is installed in the same server, you cannot use this LDAP function.

LDAP user/LDAP group

The available LDAP user and LDAP group are as below.

- The string length and character type of user name and group name must be within available OS user and OS group.
- The user and group of same with OS user and OS group are OS cannot exit.

Creating swadmin group on the OpenLDAP

When the user definition is enabled, if you use Systemwalker Operation Manager by the users registered in the OpenLDAP, you need to belong to the swadmin group. Also, if you use the user registered in the OpenLDAP from multiple Systemwalker

Operation Manager environment, it is recommended to create swadmin group on the OpenLDAP and belong to it, donot to belong to the swadmin group in the each Systenwalker Operation Management environment.

For the detail, refer to the "2.4.5 Define User Restrictions"

Provides procedures for creating swadmin group on the OpenLDAP.

Systemwalker Operation Manager is not installed

Provides procedures for creating swadmin group on the OpenLDAP before Systemwalker Operation Manager is installed.

1. If the swadmin group exist in the installation environment of the Systemwalker Operation Manager, delete it.
2. Create swadmin group on the OpenLDAP.
3. In the installation environment of the Systemwalker Operation Manager, make sure the swadmin group on the OpenLDAP can see them by the "getent group" command.
4. Install the Systemwalker Operation Manager.
5. Add local user of OS and the user registered on the OpenLDAP to the swadmin group on the OpenLDAP.

Systemwalker Operation Manager is installed

Provides procedures for creating swadmin group on the OpenLDAP when Systemwalker Operation Manager is already installed.

1. Back up the Systemwalker Operation Manager.
2. Uninstall the Systemwalker Operation Manager.
3. In the above environment, delete swadmin group.
4. Create swadmin group on the OpenLDAP.
5. In the above environment, make sure the swadmin group on the OpenLDAP can see them by the "getent group" command.
6. Install the Systemwalker Operation Manager.
7. Restore the Systemwalker Operation Manager information that backed-up.
8. Change the group of output directory for the Audit log to the swadmin group on the OpenLDAP.
9. Start the Systemwalker Operation Manager.
10. Add local user of OS and the user registered on the OpenLDAP to the swadmin group on the OpenLDAP.

Information

Monitored host definitions when performing multi-server monitoring

If you use the SSSD(System Security Services Daemon), you can get the LDAP user/group by gentent command to specify "enumerate = True" in the sssd.conf. For the detail, refer to the OS manuals

Defining the PAM authentication

If you use the Systemwalker Operation Manager by the user of OpenLDAP management, you need to create settings file of the PAM authentication in advance. This setting allows the PAM authentication to be executed by the access privilege checking of the user.

Create /etc/pam.d/omgr_check_user file and describe the followings.

[Linux]

```
auth sufficient pam_sss.so
auth required pam_unix.so
```

```
account sufficient pam_sss.so
account required pam_unix.so
```

-

[Solris]

```
auth requisite pam_authtok_get.so.1
auth required pam_dhkeys.so.1
auth required pam_unix_cred.so.1
auth binding pam_unix_auth.so.1 server_policy
auth required pam_ldap.so.1

account requisite pam_roles.so.1
account binding pam_unix_account.so.1 server_policy
account required pam_ldap.so.1
```

-

Set the permissions for the omgr_check_user file as below.

Owner	root
Group	root
Permissions	0644

If there are error settings, the user authentication fail to execute.

If there are no /etc/pam.d/omgr_check_user file, the PAM authentication is not executed.

Note

Solaris 11

In the Solaris 11, the "root" is default, not the "user account" but "role", so you cannot login to the system as root. If you connect to the each client (Note) of the Systemwalker Operation Manager, and each server of the Systemwalker Operation Manager from the Web console, you must execute rolemod command and change the root from the "role" to the "user account".

For the detail of rolemod command, refer to the following.

http://docs.oracle.com/cd/E26924_01/html/E25887/rbactask-4.html#rbactask-20

Note:

Systemwalker Operation Manager client/ Multiple monitoring client/ Print Jobscheduler Info clients/ Master Schedule Management environment setup client/ Master Schedule Management status monitoring client/ environment setup client

Using Systemwalker Operation Manager by the LDAP user

You can use the Systemwalker Operation Manager to login by the user of LDAP management.

Note

If you set /sbin/nologin to the login shell, it is not an authentication error.

2.4.5 Define User Restrictions

Systemwalker Operation Manager allows you to set any user who can access to the resources used by services/daemons and limits the Systemwalker Operation Manager users.

When the user definition is enabled, only the users registered in the swadmin group, users who belong to the Administrators group, and the superuser are enabled for the following:

- Starting demand jobs
- Starting job nets that have the Job Execution Control attribute
- Using Jobscheduler command functions

For a new installation of Systemwalker Operation Manager V17.0.0 or later, this definition is enabled by default. Refer to "How to disable the user restriction definition" for information on how to disable it.

Also, refer to "How to enable the user restriction definition" for information on how to enable the definition setting from a disabled status.

Note

You can use this option to limit the Systemwalker Operation Manager users only when you are using the file system of NTFS. You cannot use this option when you are using FAT, so disable the user restriction definition. [Windows]

How to disable the user restriction definition

1. Log in as system administrator (user belonging to the Administrators group or superuser).
2. Audit log file settings

   [Windows]

   1. Add "read" and "write" access rights for the Users group to the audit log output destination directory.
   2. Delete the swadmin group from the access permission entries for the audit log output destination directory.

   [UNIX]

   Change the access right for the audit log output destination directory to 777, and the owner to the sys group. The following is an example where the audit log output destination directory is /var/opt/FJSVftlo/audit (by default):

   ```
   # cd /var/opt/FJSVftlo

   # chmod 777 audit

   # chgrp sys audit
   ```

3. Display the **Define Operation Manager Shared Parameter** window

   The **Define Operation Manager Shared Parameter** window is displayed by clicking **Shared parameter** in the **Systemwalker Operation Manager Environment Setup** window.

4. Disable the user restriction definition

   Clear the option **Restrict so that only users included in the swadmin group can start demand jobs, start jobnet Job execution control attributes or use Jobscheduler command functions**.

5. Restart the service/daemon

   If **OK** is clicked in the **Define Operation Manager Shared Parameter** window, the restart confirmation dialog box is displayed. If **OK** is clicked in the dialog box, the following services or daemons restart as below:

   [Windows]

   Job Execution Control, Jobscheduler, Task Link services restart. If running multi-subsystem operation, all the subsystems and Task Link services restart.

   [UNIX]

   Job Execution Control and Jobscheduler daemons restart. If running multi-subsystem operation, all the subsystems restart.

How to enable the user restriction definition

The user restriction definition is inherited from the older version when upgrade installation is performed. Refer to the following procedure for information on how to enable the setting when it was disabled in the older version.

Creating the swadmin group

The swadmin group is required to restrict the users who can submit on-demand jobs, start job nets with the job execution control attribute or use the Jobscheduler commands.

- Windows:

  The swadmin group is created automatically during installation of the Systemwalker Operation Manager server. Once the swadmin group is created, it is NOT deleted even when the user restriction is canceled from the **Define Operation Manager Shared Parameter** window.

- UNIX version:

  The swadmin group is created automatically during installation of the Systemwalker Operation Manager server.

  Register all of the users who are permitted to use the Jobscheduler and Job Execution Control commands in the swadmin group.

Configuration in the Define Operation Manager Shared Parameter window

1. Display the **Define Operation Manager Shared Parameter** window

   The **Define Operation Manager Shared Parameter** window is displayed by clicking **Shared parameter** in the **Systemwalker Operation Manager Environment Setup** window.

2. Enable the user restrictions definition

   Check the option **Restrict so that only users included in the swadmin group can start demand jobs, start jobnet Job execution control attributes or use Jobscheduler command functions**.

3. Restart the service/daemon

   If **OK** is clicked in the **Define Operation Manager Shared Parameter** window, the restart confirmation dialog box is displayed. If **OK** is clicked in the dialog box, the following services or daemons restart as below:

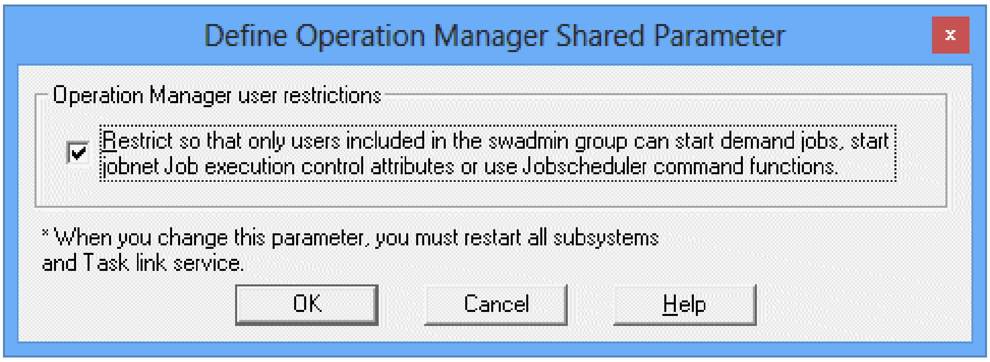
   [Windows]

   Job Execution Control, Jobscheduler, Task Link services restart. If running multi-subsystem operation, all the subsystems and Task Link services restart.

   [UNIX]

   Job Execution Control and Jobscheduler daemons restart. If running multi-subsystem operation, all the subsystems restart.

Define Operation Manager Shared Parameter window



Define Operation Manager Shared Parameter

Operation Manager user restrictions

☑ Restrict so that only users included in the swadmin group can start demand jobs, start jobnet Job execution control attributes or use Jobscheduler command functions.

* When you change this parameter, you must restart all subsystems and Task link service.

Operation Manager user restrictions:

Specify this option to allow only users of swadmin group, those of Administrators group and the superuser to start on-demand jobs, start job nets having Job Execution Control attributes, and use Jobscheduler commands.

Protecting audit log files

To protect audit log files, make security definitions, and then use the following procedure to set up access rights for the output destination directory.

Note

Make these settings again if the output destination directory for audit log files is changed.

[Windows]

1. Log in as a user that belongs to the Administrators group.
2. Delete the "full control" access rights to the audit log output destination directory for the "Everyone" user group.
3. Add "full control" access rights to the audit log output destination directory for the "swadmin" group.

[UNIX]

1. Log in as a superuser.
2. Change the ownership rights to the audit log output destination directory to the "swadmin" group.

   Example: # chgrp swadmin /var/opt/FJSVftlo/audit

3. Change the access rights to the audit log output destination directory.

   Example: # chmod 770 /var/opt/FJSVftlo/audit

The commands in this example assume the default settings are used for the audit log output destination directory.

Notes on the user restriction definition

- Access privileges to resources used by services/daemons

  [Windows]

  You can start some Systemwalker Operation Manager services only when you have access privileges to those resources. To do so, you must set the "full control" to the Administrators group to use the following resources of Systemwalker Operation Manager servers.

  Installation destination directory and subordinate files specified during installation

  - Calendar information directory (*Systemwalker Operation Manager installation directory*\MpWalker.JM\mpjmcal\caldb)
  - Database directory of Jobscheduler (The initial value is the *Systemwalker Operation Manager installation directory*\MpWalker.JM\mpjobsch\jobdb) and subordinate files

  [UNIX]

  Each daemon of Systemwalker Operation Manager uses the following resources, and the access privileges to those resources are set depending on the selection of the **Operation Manager user restrictions** check box option. Never change these access privileges. If changed, Systemwalker Operation Manager may not operate normally.

  - Solaris version and Linux version

    - Resources under the system installation directory

    - Resources under the database directory (/var/opt/*package name*)

  - HP-UX version and AIX version

    - Resources under the system installation directory

The access privileges that differ from those specified during system installation may be used when you check the **Operation Manager user restrictions** option, and an error message may be output when you issue the pkgchk command.

- **When using the Extended User Management function [UNIX]**

  If the Extended User Management function is enabled, OS users that are associated with Operation Manager users will be subject to the definitions in "Define user restrictions".

  If the Extended User Management function and the user restriction definition are enabled, the access rights are determined as below:

  1. The associated OS user is checked for belongingness to the swadmin group.
  2. If the belongingness to the swadmin group is confirmed, the OS user is checked for possession of the access privileges to projects.
  3. When the OS user's access privileges is confirmed, he/she can use this option to submit on-demand jobs, start job nets having Job Execution Control attributes, and issue Jobscheduler commands.

- **Submitting jobs [Windows]**

  If the user restriction definition is enabled and a domain user belonging to the swadmin groups is specified as the following users below, the specified domain user needs to be registered in the **Define Job Owner's Information** window to submit a job normally.

  - Schedule jobs: The project owner or the execution user for the job
  - On-demand jobs: The login user
  - The qsub command: The execution user for the job
  - Job submission API: The execution user for the job

2.4.6 Defining Audit Log Output

Overview

Make definitions for saving records of operations that have been performed on Systemwalker Operation Manager.

How to define audit logs

When Systemwalker Operation Manager is installed, audit logs are set up so that they are output.

The default settings for the output destination for audit logs and the number of days for storing audit logs are as follows:

- Output destination for audit logs

  [Windows]

  ```
  Systemwalker Operation Manager installation directory\MPWALKER.JM
  \mpcmtool\audit
  ```

  [UNIX]

  ```
  /var/opt/FJSVftlo/audit/
  ```

- Number of days for storing audit logs

  31 days

To make audit log output settings by changing the default output destination or number of storage days, refer to "Changing audit log output settings".

To not output audit logs, cancel audit log output by referring to "Canceling audit log output".

To manage audit logs centrally on the Operation Management Server by collecting logs from each server using the Systemwalker Centric Manager audit log management function, the settings for the audit log management function must be changed. Change the settings by referring to "Changing the settings for Systemwalker Centric Manager audit log management function".

Changing audit log output settings

If the output destination or number of storage days for audit logs is changed, make sure that there is sufficient disk capacity, taking the size of the audit log files into account. This section describes how to change the settings for audit log output under the following headings:

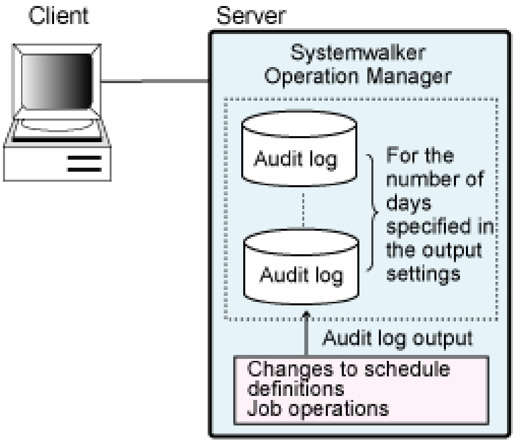
- Deciding the output destination and number of storage days for audit logs
- Estimating the size of audit log files
- Output settings for audit logs
- Protecting audit log files
- Checking the settings for audit log output

Deciding the output destination and number of storage days for audit logs

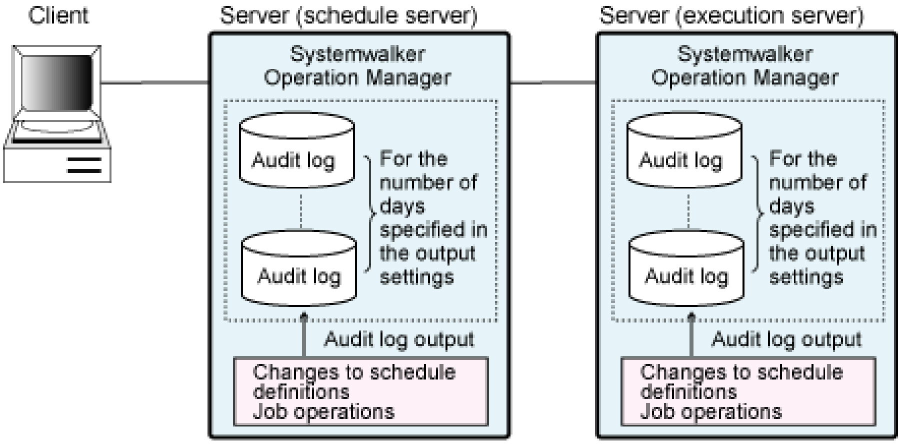
Decide the output destination and number of storage days for audit logs by considering the nature of the business and the operation mode of Systemwalker Operation Manager. The maximum number of days that can be set for storing audit logs is either 999 or infinite ("unlimit").

Note that audit log files are only held for the specified number of days, so it is recommended that audit log files be backed up regularly if necessary.

■ Operating Systemwalker Operation Manager on a single server


Client
Server
Systemwalker Operation Manager
Audit log
Audit log
For the number of days specified in the output settings
Audit log output
Changes to schedule definitions
Job operations

■ Operating Systemwalker Operation Manager on multiple servers


Client
Server (schedule server)
Server (execution server)
Systemwalker Operation Manager
Audit log
Audit log
For the number of days specified in the output settings
Audit log output
Changes to schedule definitions
Job operations
Systemwalker Operation Manager
Audit log
Audit log
For the number of days specified in the output settings
Audit log output
Changes to schedule definitions
Job operations

Estimating the size of audit log files

Estimate the size of the audit log files for the output destination and the number of storage days that have been decided. Review the output destination and the number of storage days if there is not enough disk space on the output destination.

Refer to "Hardware Resources" in the *Systemwalker Operation Manager Technical Guide* for information about formulas for estimating the size of audit log files.

Output settings for audit logs

Use the following procedure to change the output settings for audit logs according to the output destination and the number of storage days that have been decided.

1. Stop the Systemwalker Operation Manager service or daemon.

2. Make audit log output settings.

   Execute the mpsetlogsend_omgr audit log setup command on the Systemwalker Operation Manager server as the system administrator. Change the output destination and the number of storage days by specifying command options.

   [Windows]

   ```
   Systemwalker installation directory\MPWALKER.JM\bin
   \mpsetlogsend_omgr -f <output file name> -k {<number of storage
   days>|unlimit}
   ```

   [UNIX]

   ```
   /usr/bin/mpsetlogsend_omgr -f <output file name> -k {<number of
   storage days>|unlimit}
   ```

   For details on the mpsetlogsend_omgr command, refer to the *Systemwalker Operation Manager Reference Guide*.

3. Start the Systemwalker Operation Manager service or daemon.

Protecting audit log files

To protect audit log files, refer to "2.4.5 Define User Restrictions".

Checking the settings for audit log output

To check the audit log output settings after they have been made, execute the mpsetlogsend_omgr command without specifying any options.

Refer to the *Systemwalker Operation Manager Reference Guide* for details on what needs to be checked.

Canceling audit log output

To cancel audit log output, execute the following command and then restart Systemwalker Operation Manager.

[Windows]

```
Systemwalker installation directory\MPWALKER.JM\bin\mpsetlogsend_omgr -d
```

[UNIX]

```
/usr/bin/mpsetlogsend_omgr -d
```

To restart audit log output once it has been canceled, perform the procedure described in "Output settings for audit logs" again.

Changing the settings for Systemwalker Centric Manager audit log management function

If a Systemwalker Centric Manager Operation Management Server, Asset Management Server, Section Management Server, Job Server or Operation Management Client has been installed on a Systemwalker Operation Manager server, Systemwalker Operation Manager audit logs can be collected on the Operation Management Server by using the audit log management function on the Operation Management Server. Refer to the *Systemwalker Centric Manager Solution Guide - Security* for details on the audit log management function.

Changing the output destination for Systemwalker Operation Manager audit logs

To change the output destination for Systemwalker Operation Manager audit logs, use the following procedure.

Note that this procedure varies depending on the version and level of Systemwalker Centric Manager that has been installed.

If Systemwalker Centric Manager V13.2.0 or later has been installed

1. Execute the following command on the Systemwalker Operation Manager server where the output destination is to be changed.

   [Windows]

   ```
   Systemwalker installation directory\MPWALKER.JM\bin
   \mpsetlogsend_omgr -f <output file name > -k {<number of storage days>|
   unlimit}
   ```

   [UNIX]

   ```
   /usr/bin/mpsetlogsend_omgr -f <output file name> -k {<number of storage
   days>|unlimit}
   ```

   For more information on how to use the mpatmlog command, refer to the *Systemwalker Centric Manager Reference Guide*.

2. Apply the changes to the output destination settings.

   To apply the new settings after the output destination for audit logs has been changed, restart Systemwalker Operation Manager on the server where the changes have been made.

3. Collect audit logs from the server where the collection settings have been changed to the Operation Management Server.

   Collect audit logs by executing the following command on the Operation Management Server, in order to collect all the information (existing before the audit log output destination was changed) on the Operation Management Server.

   [Windows]

   ```
   Systemwalker installation directory\mpwalker.dm\bin\mpatmlog -H <target
   server name>
   ```

   [UNIX]

   ```
   /opt/systemwalker/bin/mpatmlog -H <target server name>
   ```

   Refer to the *Systemwalker Centric Manager Reference Guide* for details on how to use the mpatmlog command.

   Also, once collection of existing audit logs to the Operation Management Server has completed, delete the audit logs stored in the old output destination (existing before the settings were changed) if they are no longer required.

4. Update the audit log collection settings.

   Update the collection destination settings by executing the Systemwalker Operation Manager audit log setup command. Perform this operation on the Systemwalker Operation Manager server where the settings have been changed.

   ```
   mpsetlogsend_omgr -y
   ```

If Systemwalker Centric Manager V13.1.0 has been installed

Information for collecting Systemwalker Operation Manager audit logs can be registered by executing the mpatmlogapdef command with the following options specified. Refer to the *Systemwalker Centric Manager Reference Guide* for details on the mpatmlogapdef command.

To set up log collection for the first time:

- ADD option
- -A option (log identifier)

  OMGRLog
- -M option

  ASC
- -L option (name of the log file to be collected)

  audit log output file name*
- -F option (date format definition file name)

  [Windows]

  ```
  Systemwalker installation directory\mpwalker.dm\MpAtm\fmt
  \mpatmcmgroplog.fmt
  ```

  [Solaris/Linux]

  ```
  /etc/opt/FJSVmpatm/fmt/mpatmcmgroplog.fmt
  ```

A settings example is shown below.

[Windows]

In this example, Systemwalker Centric Manager V13.1.0 has been installed, and the Systemwalker installation directory is "C:\WIN32APP" and the name of the output file for audit logs is "C:\WIN32APP\mpwalker.jm\mpcmtool\audit \mp_omgr_audit".

```
mpatmlogapdef ADD -A OMGRLog -M ASC -L "C:\WIN32APP\mpwalker.jm
\mpcmtool\audit\mp_omgr_audit*" -F C:\WIN32APP\mpwalker.dm\MpAtm\fmt
\mpatmcmgroplog.fmt
```

[Solaris/Linux]

In this example, Systemwalker Centric Manager V13.1.0 has been installed and the name of the output file for audit logs is "/var/opt/FJSVftlo/audit/mp_omgr_audit".

```
/opt/systemwalker/bin/mpatmlogapdef ADD -A OMGRLog -M ASC -L "/var/opt/
FJSVftlo/audit/mp_omgr_audit*" -F /etc/opt/FJSVmpatm/fmt/
mpatmcmgroplog.fmt
```

To cancel log collection:

- REP option
- -A option (log identifier)

  OMGRLog
- -E option

  NO

A settings example is shown below.

[Windows]

```
mpatmlogapdef REP -A OMGRLog -E NO
```

[Solaris/Linux]

```
/opt/systemwalker/bin/mpatmlogapdef REP -A OMGRLog -E NO
```

Changing the collection settings

To cancel or restart log collection for Systemwalker Operation Manager, perform the following procedure on the Systemwalker Operation Manager server.

Note that this procedure varies depending on the version and level of Systemwalker Centric Manager that has been installed.

If Systemwalker Centric Manager V13.2.0 or later has been installed

```
mpsetlogsend_omgr {-y|-n}
```

To cancel audit log collection, specify "-n" as an option for the mpsetlogsend_omgr command. Alternatively, to change the settings so that audit logs are collected if they are not currently being collected, specify the "-y" option.

If Systemwalker Centric Manager V13.1.0 has been installed

Information for collecting Systemwalker Operation Manager audit logs can be changed by executing the mpatmlogapdef command with the following options specified. Refer to the *Systemwalker Centric Manager Reference Guide* for details on the mpatmlogapdef command.

To change the log collection destination (where log collection settings for Systemwalker Operation Manager have already been registered):

- REP option
- -A option (log identifier)

  OMGRLog
- -L option (name of the log file to be collected)

  audit log output file name*

A settings example is shown below.

[Windows]

In this example, the name of the output file for audit logs is "C:\WIN32APP\mpwalker.jm\mpcmtool\audit\mp_omgr_audit".

```
mpatmlogapdef REP -A OMGRLog -L "C:\WI32APP\mpwalker.jm\mpcmtool
\audit\mp_omgr_audit*"
```

[Solaris/Linux]

In this example, the name of the output file for audit logs is "/var/opt/FJSVftlo/audit/mp_omgr_audit".

```
/opt/systemwalker/bin/mpatmlogapdef REP -A OMGRLog -L "/var/opt/FJSVftlo/
audit/mp_omgr_audit*"
```

To cancel log collection:

- REP option
- -A option (log identifier)

  OMGRLog
- -E option

  NO

A settings example is shown below.

[Windows]

```
mpatmlogapdef REP -A OMGRLog -E NO
```

[Solaris/Linux]

```
/opt/systemwalker/bin/mpatmlogapdef REP -A OMGRLog -E NO
```

To restart log collection (where log collection settings for Systemwalker Operation Manager have already been registered):

- REP option
- -A option (log identifier)

  OMGRLog
- -E option

  YES

A settings example is shown below.

[Windows]

```
mpatmlogapdef REP -A OMGRLog -E YES
```

[Solaris/Linux]

```
/opt/systemwalker/bin/mpatmlogapdef REP -A OMGRLog -E YES
```

Note

When both Systemwalker Operation Manager and Systemwalker Centric Manager coexist on the same Linux server [UNIX]

If Systemwalker Operation Manager coexists with Systemwalker Centric Manager on Linux 64, audit logs for the ACL manager may be output to two separate files, subject to the conditions indicated in the following table:

- Conditions

		Centric Manager	
		V13.4.0 or later (Linux x86 version)	V13.4.0 or later (Linux x64 version)
Operation Manager	V13.2.0 to V13.3.1	No problem	Audit logs for the ACL manager are output to two separate files, regardless of the order in which Centric Manager and Operation Manager were installed
	V13.8.0 or later (Linux x86 version)	No problem	Audit logs for the ACL manager are output to two separate files if Centric Manager was installed after Operation Manager.
	V13.8.0 or later (Linux x64 version)	Audit logs for the ACL manager are output to two separate files if Centric Manager was installed after Operation Manager.	No problem

- Output file name

  Audit logs are output to the following two files:

  - The output destination displayed by the mpsetlogsend_omgr command (audit log setup command)
  - Files where "_acl" has been added before the date component of the file name above

Example)

If the output destination indicated by the mpsetlogsend_omgr command (audit log setup command) is "/var/opt/FJSVftlo/audit/log/mp_omgr_auditYYMMDD.log", audit logs will be output to the following two files:

- /var/opt/FJSVftlo/audit/log/mp_omgr_auditYYMMDD.log
- /var/opt/FJSVftlo/audit/log/mp_omgr_audit_aclYYMMDD.log

The files where "_acl" has been added to the file name are not displayed in the execution results of the mpsetlogsend_omgr command (audit log setup command) but the audit log output ON/OFF settings, storage period and collection targets are the same for both files.

2.4.7 Definitions for Encrypted Communications (HTTPS Communications) for the Web Console/ Web API

In order to perform HTTPS communications, a certificate/key management environment must be created using the following procedure. Refer to the *Systemwalker Operation Manage Reference Guide* for details on the commands being used.

1. Create a certificate/key management environment

Create directories to execute a certificate/key management when using SSL.

Create directories to manage a certificate/private key management with using the commands provided by the operating system.

The following example shows how to create.

[Windows]

```
mkdir d:\mpahso\sslcert          Administration directory
mkdir d:\mpahso\sslcert\cert     Certificate management directory
```

[Solaris]

```
# mkdir /export/home/mpahso/sslcert          Administration directory
# mkdir /export/home/mpahso/sslcert/cert     Certificate management directory
```

2. Create private keys and obtain certificates

Obtain certificates by requesting the certificate authority to issue a certificate.

Create a CSR (Certificate Signing Request) and private key at the same time

Create a CSR to request the certificate authority to issue a certificate.

When the following command is executed, a private key is created and then CSR (Certificate Signing Request) is created.

The following example shows how to create. You must specify the -config option when the CSR (Certificate Signing Request) is created (openssl req sub command).

[Windows]

```
c:\Systemwalker\MPWALKER.JM\mpahs\bin\openssl.exe genrsa -aes256 -out d:\mpahso\sslcert
\server.key 2048
(The execution result is as below.)
Generating RSA private key, 2048 bit long modulus
......+++
...........++
e is 65537 (0x10001)
Enter pass phrase for server.key: (Note)
Verifying - Enter pass phrase for server.key: (Note)
```

```
c:\Systemwalker\MPWALKER.JM\mpahs\bin\openssl.exe req -new -key d:\mpahso\sslcert
\server.key -out d:\mpahso\sslcert\server.csr -config c:\Systemwalker\MPWALKER.JM\mpahs
```

```
\conf\openssl.cnf -subj "/C=JP/ST=Shizuoka/L=Shizuoka-shi/O=fujitsu/OU=4-1f/
CN=www.example.com"
(The execution result is as below.)
Enter pass phrase for server.key: (Note)
```

[UNIX]

```
# /opt/FJSVftlo/mpahs/oss/openssl/bin/openssl genrsa -aes256 -out /export/home/mpahso/
sslcert/server.key 2048
(The execution result is as below.)
Generating RSA private key, 2048 bit long modulus
......+++
...........++
e is 65537 (0x10001)
Enter pass phrase for server.key: (Note)
Verifying - Enter pass phrase for server.key: (Note)
```

```
# /opt/FJSVftlo/mpahs/oss/openssl/bin/openssl req -new -key /export/home/mpahso/sslcert/
server.key -out /export/home/mpahso/sslcert/server.csr -config /opt/FJSVftlo/mpahs/oss/
openssl/ssl/openssl.cnf -subj "/C=JP/ST=Shizuoka/L=Shizuoka-shi/O=fujitsu/OU=4-1f/
CN=www.example.com"
(The execution result is as below.)
Enter pass phrase for server.key: (Note)
```

Note: If this string is output, enter the passphrase as a single-byte alphanumeric string of 128 bytes or less. In addition, input characters are not echoed back. The passphrase entered in this command is also used in the "4. Register the passphrase".

Make a request for a certificate to be issued

Send the created CSR to the certificate authority to request that a site certificate be issued.

Follow the request method used by the certificate authority.

Obtain certificates

Obtain a certificate signed by the certificate authority as PEM format (Base64 encoding data).

The certificates of PEM format is like the following data format.

```
-----BEGIN CERTIFICATE-----
(The certificates data that Base64 encoded)
-----END CERTIFICATE-----
```

Floow the obtain method used by the certificate authority.

3. Deploy the certificate

After obtaining the certificate, put them with the certificate management environment.

Deploy the certificate to the directory that created when the certificate/key management environment is builed.

Deploy any certificate of the certificate authority that issued the certificate (Site or client certificates) for use in operations.

Deploy the site certificate

Deploy the site certificate (server.pem) issued by the certificate authority to the certificate/key management environment.

[Windows]

```
move server.pem d:\mpahso\sslcert\cert
```

[UNIX]

```
# mv server.pem /export/home/mpahso/sslcert/cert
```

After registering the site certificate issued, check the certificate's expiry date to confirm when the certificate will need to be updated. The expiry date can be checked using the openssl x509 command.

Note

The expiration dates for site and certificate authority certificates (issuing authority certificate)

The site and certificate authority certificates (issuing authority certificate) have expiration dates. If they expire and the operation of Web console/Web API is continued, the warning messages is displayed during SSL communication from the client. Check the expiration dates for certificate by the openssl x509 comman and obtain new certificate and register it before they expire. After registering, restart Systemwalker Operation Manger.

The following example is how to check the expiration dates for certificate.

[Windows]

```
Systemwalker Operation Manager installation directory\MPWALKER.JM\mpahs\bin\openssl.exe
x509 -noout -dates -in d:\mpahso\sslcert\cert\server.pem
```

[UNIX]

```
# /opt/FJSVftlo/mpahs/oss/openssl/bin/openssl x509 -noout -dates -in /export/home/mpahso/
sslcert/cert/server.pem
```

Deploy the root CA certificate and Intermediate CA certificate

After obtaining root CA certificate, check fingerprints before rgistering. The fingerprints information of the root CA certificate is provided in a safe manner.

Check that fingerprints match to output root CA certificate obtained from the certificate authority.

In addition, the fingerprints is hash value from a portion of the certificate, and if the certificatehe is fake or tampered, it will be different value.

As the value will be different depending on the algorithm used to calculate, compare the computed fingerprints using the same algorithm.

The following example displays the fingerprint of the root CA certificate obtained from a certificate authority. Select the option [-sha1|-sha256|-md5] that matches the fingerprint information provided by the certificate authority and compare it with the displayed value.

[Windows]

Execution example if the root CA certificate for the certificate authority is stored in the d:\mpahso\sslcert\server-root-ca.pem.

```
c:\Systemwalker\MPWALKER.JM\mpahs\bin\openssl.exe x509 [-sha1|-sha256|-md5] -fingerprint -
noout -in d:\mpahso\sslcert\server-root-ca.pem
```

```
-md5 option:       MD5 Fingerprint=40 79 98 2F 37 12 31 7C AE E7 B4 AB 78 C8 A2 28
-sha1 option:        SHA1 Fingerprint=07 28 BE 26 94 89 6D F9 ... << (20 bytes is displayed
in hexadecimal.)
-sha256 option:      SHA256 Fingerprint=F7 16 00 6E A1 6E A2 14 ... << (32 bytes is
displayed in hexadecimal.)
```

[UNIX]

Execution example if the root CA certificate for the certificate authority is stored in the /export/home/mpahso/sslcert/server-root-ca.pem

```
# /opt/FJSVftlo/mpahs/oss/openssl/bin/openssl x509 [-sha1|-sha256|-md5] -fingerprint -
noout -in /export/home/mpahso/sslcert/server-root-ca.pem
```

```
-md5 option:       MD5 Fingerprint=40 79 98 2F 37 12 31 7C AE E7 B4 AB 78 C8 A2 28
-sha1 option:     SHA1 Fingerprint=07 28 BE 26 94 89 6D F9 ... << (20 bytes is displayed in
hexadecimal.)
```

```
-sha256 option:    SHA256 Fingerprint=F7 16 00 6E A1 6E A2 14 ... << (32 bytes is displayed
in hexadecimal.)
```

In addition to the root CA and site certificates of the certificate authority, some certificate authorities provide intermediate CA certificates, so check with each certificate authority to obtain an intermediate CA certificate.

The intermediate CA certificate is merged into the site certificate file and used.

Although merging the root CA certificate is not required, it is recommended that you operate with a pem file that contains the root CA certificate.

Example merging the intermediate CA certificate (server-chain-ca.pem), the root CA certificate (server-root-ca.pem) into the site certificate

[Windows]

```
type server-chain-ca.pem >> d:\mpahso\sslcert\cert\server.pem
type server-root-ca.pem >> d:\mpahso\sslcert\cert\server.pem
type d:\mpahso\sslcert\cert\server.pem
-----BEGIN CERTIFICATE-----
... (The site certificate data) ...
 -----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (The intermediate CA certificate data) ...
 -----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (The root CA certificate data) ...
-----END CERTIFICATE-----
```

[UNIX]

```
# cat server-chain-ca.pem >> /export/home/mpahso/sslcert/cert/server.pem
# cat server-root-ca.pem >> /export/home/mpahso/sslcert/cert/server.pem
# cat /export/home/mpahso/sslcert/cert/server.pem
-----BEGIN CERTIFICATE-----
... ((The site certificate data) ...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (The intermediate CA certificate data) ...
 -----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (The root CA certificate data) ...
-----END CERTIFICATE-----
```

Set the key exchange parameter

When DHE is used for key exchange, the parameter length must be set to 2048 bits or more as a security measure.

Merge the recommended parameters (2048 bit) from RFC 3526 into the site certificate.

Merge the following PEM format parameters, including the hyphens.

```
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEA///////////JD9qiIWjCNMTGYouA3BzRKQJOCIpnzHQCC76mOxOb
IlFKCHmONATd75UZs806QxswKwpt8l8UN0/hNW1tUcJF5IW1dmJefsb0TELppjft
awv/XLb0Brft7jhr+1qJn6WunyQRfEsf5kkoZlHs5Fs9wgB8uKFjvwWY2kg2HFXT
mmkWP6j9JM9fg2VdI9yjrZYcYvNWIIVSu57VKQdwlpZtZww1Tkq8mATxdGwIyhgh
fDKQXkYuNs474553LBgOhgObJ4Oi7Aeij7XFXfBvTFLJ3ivL9pVYFxg5lUl86pVq
5RXSJhiY+gUQFXKOWoqsqmj//////////wIBAg==
-----END DH PARAMETERS-----
```

4. Register the passphrase

Register the passphrase in the passphrase management file.

By specifying the passphrase and the passphrase management file with the ahsregistupin command, the passphrase will be encrypted and registered in the passphrase management file.

Example for register the passphrase

[Windows]

In this example, the passphrase (Interactive Input) is encrypted and registered in the d:\mpahso\sslcert\upinfile passphrase management file.

```
c:\systemwalker\MPWALKER.JM\mpahs\bin\ahsregistupin.exe -f d:\mpahso\sslcert\upinfile
```

[UNIX]

In this example, the passphrase (Interactive Input) is encrypted and registered in the /export/home/mpahso/sslcert/upinfile passphrase management file.

```
/opt/FJSVftlo/mpahs/bin/ahsregistupin -f /export/home/mpahso/sslcert/upinfile
```

5. Configure the environment definition file (httpd.conf)

Configure the Web server environment definition file "httpd.conf" to use SSL encryption.

The file "httpd.conf" is stored in the following directory:

[Windows]

```
<Systemwalker Operation Manager installation directory>\mpwalker.jm\mpahs\conf\httpd.conf
```

[UNIX]

```
/opt/FJSVftlo/mpahs/conf/httpd.conf
```

Definition examples of the environment definition file are shown below.

[Windows]

If performing SSL operations with the following settings:

- SSL protocol version: "TLSv1.2 TLSv1.3"
- Passphrase management file: "d:\mpahso\sslcert\upinfile"
- Site certificate: "d:\mpahso\sslcert\cert\server.pem"
- Site private key: "d:\mpahso\sslcert\server.key"

[Example of how to edit httpd.conf]

```
ServerAdmin webmaster@main.example.com
ServerName  main.example.com
SSLEngine      On
SSLHonorCipherOrder On
SSLProtocol    TLSv1.2 +TLSv1.3
SSLCertificateFile     d:\mpahso\sslcert\cert\server.pem
SSLCertificateKeyFile  d:\mpahso\sslcert\server.key

SSLUserPINFile  d:\mpahso\sslcert\upinfile
SSLCipherSuite  ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-
CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-
POLY1305
SSLCipherSuite TLSv1.3
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

[UNIX] [Linux]

If performing SSL operations with the following settings:

- SSL protocol version: "TLSv1.2 TLSv1.3""

- Passphrase management file: " export/home/mpahso/sslcert/upinfile"

- Site certificate: " /export/home/mpahso/sslcert/cert/server.pem"

- Site private key: " /export/home/mpahso/sslcert/server.key"

[Example of how to edit httpd.conf]

```
ServerAdmin webmaster@main.example.com
ServerName  main.example.com
SSLEngine      On
SSLHonorCipherOrder On
SSLProtocol    TLSv1.2 +TLSv1.3
SSLCertificateFile     /export/home/mpahso/sslcert/cert/server.pem
SSLCertificateKeyFile  /export/home/mpahso/sslcert/server.key

SSLUserPINFile  /export/home/mpahso/sslcert/upinfile
SSLCipherSuite  ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-
CHACHA20-POLY1305:
DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305
SSLCipherSuite TLSv1.3
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256
```

Note

Note that "httpd.conf" is excluded when backup and restoration are performed, or when migration assets are backed up and restored. Therefore, the same settings must be configured again if you restore the environment from the backup or restore the migration assets.

2.4.7.1 How to Back up and Restore the Certificate/Key Management Environment

This section explains how to back up and restore the certificate/key management environment.

Back up existing resources (private keys and certificates)

Back up the resources specified in the target directive (Note) of the environment definition file (httpd.conf) to the directory for back-up.

Restore private keys and certificates

Restore the back-up resources to the pass specified in the target directive (Note) of the environment definition file (httpd.conf).

Note: the target directive

- Site certificate: (The file specified in the SSLCertificateFile directive)

- Site private key: (The file specified in the SSLCertificateKeyFile directive)

- Passphrase management file: (The file specified in the SSLUserPINFile directive)

EE

2.5 Definition of Multi-Subsystem Operations

This section explains the definition required for multi-subsystem operations.

Note

- The number of Systemwalker Operation Manager service processes increases according to the number of subsystems, increasing the risk of the desktop heap being depleted. Adjust the size of the desktop heap if, as a result of the desktop heap being exhausted, the service fails to start or jobs terminate abnormally with exception code 0xC0000142. There is no particular method for estimating an appropriate value for the size of the desktop heap, so increase the size gradually in units of 256 KB or 512 KB.

- If you operate subsystems in the Windows system, you must change the shutdown exit according to your application. For the modification of shutdown exit, refer to the *Systemwalker Operation Manager Reference Guide*.

EE

2.5.1 Creating a Subsystem Environment

Outline

To start multi-subsystems on a single Systemwalker Operation Manager server, you must create a multi-subsystem operating environment.

Operation procedure

Issue the following command on the server where you wish to operate multi-subsystems. To do so, log in as the superuser or as the user belonging to the Administrators group who has the privileges of "Function as part of the operating system."

[Windows system]

```
createsubsystem.exe -sys subsystem-number
```

[UNIX system]

```
createsubsystem.sh -sys subsystem-number
```

Note 1:

This command is stored in the following directory:

Windows: System installation directory \MpWalker.JM\bin
Solaris version: /opt/FJSVJMCMN/bin
Linux version: /opt/FJSVJMCMN/bin
HP-UX version: /opt/FHPJMCMN/bin
AIX version: /usr/FAIXJMCMN/bin

Note 2:

The "subsystem-number" can be an integer of 1 to 9.

When you issue the **createsubsystem** command, the Jobscheduler database directory used by subsystems and the Job Execution Control spool directory will be created. If you are using the Windows system, the information you have specified in the **Spool directory** on the **Cluster settings** sheet of the **Define Operating Information** window is NOT copied when the Job Execution Control spool directory is created.

The database directory and the spool directory to be used by subsystem 0 are created automatically during installation of Systemwalker Operation Manager.

For the **createsubsystem** command details, refer to the *Systemwalker Operation Manager Reference Guide*.

EE

2.5.2 Assigning Subsystem Port Numbers

Outline

Before starting multi-subsystems on a single Systemwalker Operation Manager server, you must assign port numbers to subsystems used by Jobscheduler in the **services** file.

Also, before submitting jobs by linking Systemwalker Operation Manager servers for multiple-subsystem operations, you must assign the port numbers for network jobs in addition to the subsystem port numbers used by the Jobscheduler. Make sure that the same number of port numbers for Jobscheduler and port numbers of network jobs are required on all of Systemwalker Operation Manager servers to be linked.

The following defines the port number definition procedure.

Note

The port numbers of network jobs are not required when the following combination of schedule server and execution server is used.

Schedule server

V10.0L10/5.2 or after with operated with multiple subsystems.

Execution server

V5.0L30/5.2 or after with operated with subsystem 0.

Definition procedure

1. Open the **services** file.

   Using an editor such as "vi" or Notepad, open the **services** file on the computer where the Systemwalker Operation Manager server has been installed.

   The storage location of the **services** file varies depending on the activated operating system (OS) as follows.

   If Windows server is used:

   ```
   (System root) \system32\drivers\etc\services
   ```

   If UNIX server is used:

   ```
   /etc/services
   ```

2. Assign port numbers to the subsystems used by Jobscheduler.

   Using an editor, add the following service names and their corresponding port numbers to the **services** file.

   - jobsch_win1
   - jobsch_win2
   - jobsch_win3
   - jobsch_win4
   - jobsch_win5
   - jobsch_win6
   - jobsch_win7
   - jobsch_win8
   - jobsch_win9

   For example, if you wish to start subsystem 5, add "jobsch_win5" and its corresponding port number to the **services** file. You can use any unused port number. You can use any unused port number in form of "port number/tcp".

3. Assign port numbers for network jobs.

   When a job is submitted as a network job from a subsystem, it is executed with subsystem 0 on the submitting Systemwalker Operation Manager server. If you have no problem in this job execution, you need not set port numbers.

   Port numbers for network jobs need to be assigned when requesting network jobs from one Systemwalker Operation Manager server performing multi-subsystem operations to another Systemwalker Operation Manager server performing multi-subsystem operations. You need edit the **services** file on all of linked servers for multiple-subsystem operations.

Using an editor such as "vi" or Notepad, add the following service names and their corresponding port numbers to the **services** file.

- mjsnet1
- mjsnet2
- mjsnet3
- mjsnet4
- mjsnet5
- mjsnet6
- mjsnet7
- mjsnet8
- mjsnet9

You can use any unused port number in form of "port number/tcp". The same service name and port number must always be used on all of linked servers.

EE

2.5.3 Deleting the Subsystem Environment [Windows]

Outline

The existing multiple-subsystem operating environment for Windows can be deleted.

Operation procedure

Issue the following command on the server where you are operating multi-subsystems. The system administrator (the user belonging to the Administrators group or the superuser) must issue the commands.

Terminate the following services before executing the command.

- Systemwalker MpMjesn
- Systemwalker MpJobschn

```
deletesubsystem.exe -sys n
```

Note 1:

This command is stored in the following directory.
Systemwalker installation directory \MpWalker.JM\bin

Note 2:

n: Subsystem number 1 to 9 to be deleted

When you issue the **deletesubsystem** command, the subsystem environment of the specified subsystem number is deleted. However, the database directory for Jobscheduler and the spool directory for Job Execution Control are NOT deleted.

For the **deletesubsystem** command details, refer to the *Systemwalker Operation Manager Reference Guide*.

EE

2.5.4 Deleting the Subsystem Environment [UNIX]

Outline

The existing multiple-subsystem operating environment for UNIX can be deleted.

Advance tasks when the Master Schedule Management function is enabled

Advance tasks when the Master Schedule Management function is enabled

If the Master Schedule Management function has been enabled and the subsystem to be deleted is being operated using either daily schedule management or daily schedule management (test mode), perform the following tasks according to the environment being used.

When the environment is built as a management server

In a **Master Schedule Management Environment Setup** dialog box that is connected to the management server, clear all of the schedule servers that have been registered with the subsystem to be deleted.

Refer to "Change to Normal Schedule" in the *Systemwalker Operation Manager User's Guide - Master Schedule Management* for information on removing the schedule server.

When the environment is built as a schedule server

In a **Master Schedule Management Environment Setup** dialog box that is connected to the management server, clear the applicable schedule server out of the schedule servers that have been registered with the subsystem to be deleted. When the schedule server is cleared, a dialog box will be displayed asking whether to restart the Jobscheduler daemon, but there is no need to restart it.

Refer to "Change to Normal Schedule" in the *Systemwalker Operation Manager User's Guide - Master Schedule Management* for information on clearing the schedule server.

Deletion procedure

Use the following steps to delete the subsystem environment.

1. Stop the subsystem to be deleted.

   Stop the subsystem from the **Systemwalker Operation Manager Environment Setup** window or manually.

   Refer to "How to shut down multiple subsystems manually" in the *Systemwalker Operation Manager User's Guide* for information on how to shut down manually.

   Refer to "Starting and Stopping Daemons in Cluster Systems" in the *Systemwalker Operation Manager Cluster Setup Guide for UNIX* for information on how to stop daemons in the cluster system.

2. Delete the following directories and files.

   In a cluster system, the shared disk is released if the daemon is stopped. Therefore, mount the shared disk first, then delete the following directories and files.

   a. Calendar control information files (See Note)

   ```
   Solaris version : /var/opt/FJSVjmcal/post/sysn/*.dat
   HP-UX version   : /opt/FHPjmcal/post/sysn/*.dat
   Linux version   : /var/opt/FJSVjmcal/post/sysn/*.dat
   AIX version     : /opt/FAIXjmcal/post/sysn/*.dat
   ```

   ```
   n: Subsystem number 1 to 9 to be deleted

   Note:

   If the calendar control information directory is deleted, no directory is created
   when the same subsystem is recreated.
   ```

   b. Jobscheduler database directory

   ```
   Solaris version : /var/opt/FJSVJOBSC/JOBDBn
   HP-UX version   : /opt/FHPJOBSCH/db/JOBDBn
   Linux version   : /var/opt/FJSVJOBSC/JOBDBn
   AIX version     : /usr/FAIXJOBSC/db/JOBDBn
   ```

   ```
   n: Subsystem number 1 to 9 to be deleted
   ```

   c. Job Execution Control spool directory

   ```
   Solaris version : /var/opt/FJSVMJS/var/spool/mjes/mjesn
   HP-UX version   : /opt/FHPMJS/var/spool/mjes/mjesn
   ```

```
Linux version   : /var/opt/FJSVMJS/var/spool/mjes/mjesn
AIX version     : /opt/FAIXMJS/var/spool/mjes/mjesn
```

```
n: Subsystem number 1 to 9 to be deleted
```

d. Job Execution Control operating information directory

```
Solaris version : /etc/opt/FJSVMJS/etc/mjes/mjesn
HP-UX version   : /opt/FHPMJS/etc/mjes/mjesn
Linux version   : /etc/opt/FJSVMJS/etc/mjes/mjesn
AIX version     : /opt/FAIXMJS/etc/mjes/mjesn
```

```
n: Subsystem number 1 to 9 to be deleted
```

e. Master Schedule Management database directory (Only when the Master Schedule Management function is enabled)

```
Solaris version : /var/opt/FJSVstem/stemDBn
HP-UX version   : /var/opt/FJSVstem/stemDBn
Linux version   : /var/opt/FJSVstem/stemDBn
AIX version     : /var/opt/FJSVstem/stemDBn
```

```
n: Subsystem number 1 to 9 to be deleted
```

3. Delete subsystem port numbers.

   Delete subsystem port numbers created in the /etc/services file at "2.5.2 Assigning Subsystem Port Numbers".

2.6 Definition of Power Control

This section explains how to define Power Control functions.

Outline

The server power turns on when a user logs on a client if the Power Control function command is stored as the startup program on the client. The startup program is executed automatically when the Windows system starts. You can register the startup program in the Windows system.

Note that this function can only be used if the server is running Windows x86.

Definition procedure

1. Right click on the desktop and select **New** >> **Shortcut**.
2. Using the **Create Shortcut** wizard, input the command line below into **Type the location of the item**, and then click **Next**.

   If PowerChute(R) plus or PowerChute(R) Business Edition is used

   <*Systemwalker installation directory*>\MpWalker.JM\bin\f3crhpcs.exe <*IP address*>

   ```
   The "IP address" must be the IP address of the PowerNetSNMP adapter which is
   connected to the server whose power is controlled.
   ```

3. Specify a shortcut name, and click **Finish**.

   Example shortcut name: Power Control client function

4. Right click the created shortcut, and display the properties window from **Properties**. Click **Advanced...** in the **Shortcut** tab

   After selecting **Run as administrator** in the opened window, click **OK**. After clicking **Apply** in the properties window, close by clicking **OK**

5. Register the shortcut icon that has been created by opening Explorer, and dragging & dropping them into the startup program registration folder (*1).

   *1: Below is an example from Windows Server 2008. Note that the folder differs depending on the OS:

   C:\Users\<*user name*>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

   Ensure that you show hidden files and folders in the settings.

Note

If a Windows server shares folders on the network

If a shared folder for servers has been assigned to a directory on the client and if such assignment is used automatically during user logon, you must take the following notes.

If you have set the server to turn on when a user logs on a client, the server may not turn on when a client is turned on. In such case, the directory assignment fails on the client. If you need to assign the shared folder for servers to the directory on the client, you must manually assign it after the server has started up.

2.7 Definition of Jobscheduler

This section explains how to define an operating environment for Jobscheduler functions.

2.7.1 Defining Startup Parameters

The following explains how to define startup parameters of Jobscheduler services and daemons.

If you have changed the startup parameter definition, you must restart Jobscheduler services and daemons to make your change valid.

Outline

The following seven (7) sheets are included in the **Define Jobscheduler Startup Parameters** window to define startup parameters of Jobscheduler services and daemons.

Windows used for startup parameter definition:

- Database sheet in the Define Jobscheduler Startup Parameters window
- Use function1 sheet in the Define Jobscheduler Startup Parameters window
- Advanced Settings for Verification window
- Use function2 sheet in the Define Jobscheduler Startup Parameters window
- Event output sheet in the Define Jobscheduler Startup Parameters window
- Advanced Settings for Event Output window
- Mail sheet in the Define Jobscheduler Startup Parameters window
- Output file sheet in the Define Jobscheduler Startup Parameters window
- Test mode sheet in the Define Jobscheduler Startup Parameters window

Definition procedure

1. Display the **Define Jobscheduler Startup Parameters** window.

   Click **Startup parameter** in the **Systemwalker Operation Manager Environment Setup** window, and the **Define Jobscheduler Startup Parameters** window will appear.

2. Select the desired sheet (**Database**, **Use Function1**, **Use Function2**, **Event output**, **Mail**, **Output file**, or **Test mode** sheet).

   To define the database information (for database directory or log file setup), select the **Database** sheet.

To enable the Job net startup API, Message waiting, Verification at error occurrence, and Status option functions, select the **Use Function1** sheet.

To set the Halt recreation of startup days, warn at job net registration count, and Limit the number of connected clients options, select the **Use Function2** sheet.

To set up information relating to event output (the output conditions for job net execution histories, links to Systemwalker Centric Manager and delay monitoring management for jobs and job nets), select the **Event output** sheet.

To set the mail waiting conditions, select the **Mail** sheet.

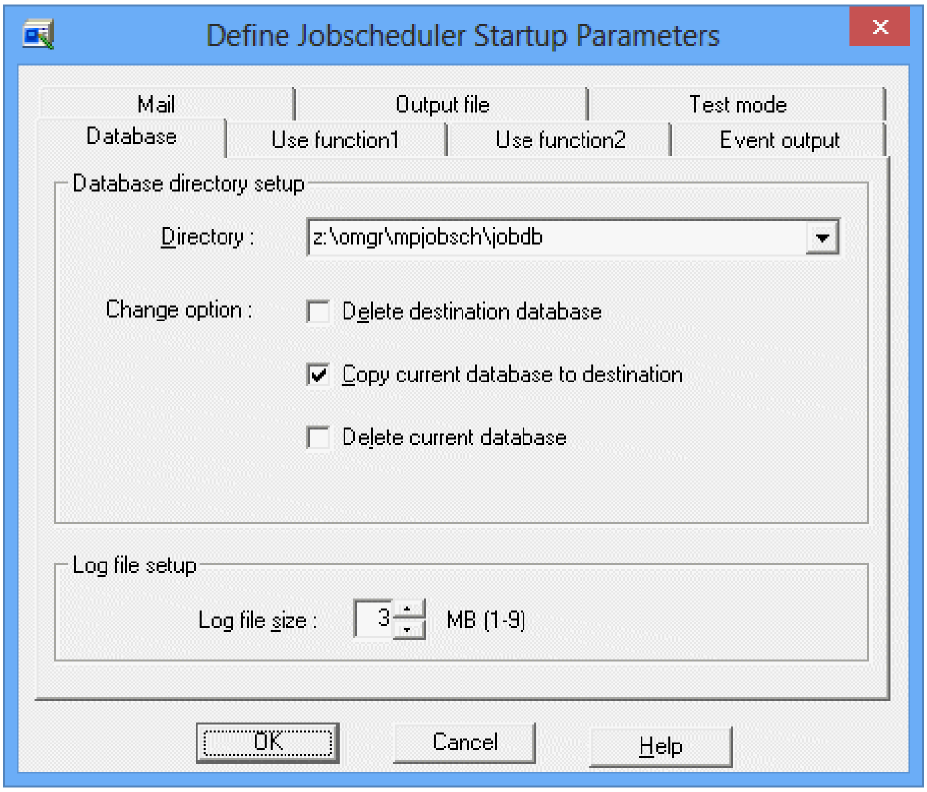
To set output file options of jobs, select the **Output file** sheet.

To use the Test Mode operation (in virtual time), select the **Test mode** sheet.

3. Register the startup parameter information.

   After you have set the startup parameters on each sheet, click **OK** to store them.

Database sheet in the Define Jobscheduler Startup Parameters window



Database directory setup

Directory : z:\omgr\mpjobsch\jobdb

Change option : □ Delete destination database

☑ Copy current database to destination

□ Delete current database

Log file setup

Log file size : 3 MB (1-9)

Directory:

[Windows]

Specify the directory to store the database that the Jobscheduler services use in the format of "drive-name directory-name" in no more than 254 bytes. The "drive-name" can be a fixed disk drive only. The directory cannot be specified during operation of a Jobscheduler service. This parameter is always required. The following initial values are set during system installation.

```
Systemwalker Operation Manager installation directory
\MpWalker.JM\mpjobsch\jobdb
```

The standard output (stdout) and standard error output (stderr) for each job registered with the Jobscheduler will be stored in a file in the directory specified here, with the file name "<*project name*>_<*job net name*>_cccccccccccccccc.log", where "cccccccccccccccc" is an arbitrary string.

EE

When connected to the server for multiple-subsystem operations, the initial values of database storage directory are stored in the following file.

```
Systemwalker Operation Manager installation directory\MpWalker.JM
\mpjobsch\jobdbn
```

Where, "*n*" of "jobdbn" is a subsystem number (1 to 9). If subsystem 0 is specified, the information is stored in the same directory as that is used when multi-subsystems are NOT started.

[UNIX]

You cannot specify a database directory. The database used by Jobscheduler daemons is always stored in the following location. You must create a symbolic link to change it.

Solaris	/var/opt/FJSVJOBSC
HP-UX version	/opt/FHPJOBSCH/db
AIX version	/usr/FAIXJOBSC/db
Linux	/var/opt/FJSVJOBSC

EE

When connected to the server for multiple-subsystem operations, the database is always stored in the following directory independent from destination subsystems.

Solaris	/var/opt/FJSVJOBSC/JOBDBn
HP-UX version	/opt/FHPJOBSCH/db/JOBDBn
AIX version	/usr/FAIXJOBSC/db/JOBDBn
Linux	/var/opt/FJSVJOBSC/JOBDBn

where, "*n*" of "JOBDB*n*" is a subsystem number (1 to 9). If subsystem 0 is specified, the information is stored in the same directory as that is used when multi-subsystems are NOT started.

The standard output (stdout) and standard error output (stderr) for each job registered with the Jobscheduler will be stored in a file in the fixed database directory shown above, with the file name "<*project name*>_<*job net name*>_nn.log", where nn is an arbitrary string.

Change option [Windows]:

This option allows you to change the directory which stores the database used by Jobscheduler services. This option cannot be specified when the Jobscheduler service is running. These options are explained below.

Delete destination database:

Deletes a database if it exists in the specified directory.

Copy current database to destination:

Copies the current database to the specified directory. If the database already exists in the specified directory, it is overwritten.

Delete current database:

Deletes the current database.

Log file size:

Specify the file size (from 1M to 99M bytes) to be used when the Jobscheduler log file is switched. The initial value is 3M bytes. If the size of Jobscheduler log file exceeds the specified value, three files (jobdb1.log, jobdb2.log, and jobdb3.log) are switched in order.

Note

Intensified log file access

The log file is accessed by the following Systemwalker Operation Manager operations:

- Display of the **Job History** window or the **Job Net History** window
- Startup of a job net or job

If startup of a job net or job is triggered by the display of the **Job Net History** window or the **Job History** window, access to the log file may become intensified, which may result in slower display performance or startup performance. Deterioration in startup performance may lead to the job net or job not starting at the scheduled time.

Therefore, refrain from displaying the **Job Net History** window or the **Job History** window while a job net or job is running.

Information

Setting the log file size

Estimate the total log file size by referring to the following formula. As a guide, if the log file size estimated exceeds 20MB (Note), set the estimated size after thoroughly examining the time required to display the **Job History** window and impacts on responses to other Operation Manager clients.

Note)

In addition to the operations listed in the "Concentrated access of the log file" section above, responses to other Operation Manager clients may also be affected by the log file size.

If the estimated log file size exceeds the guideline of 20 MB, carefully consider any possible impact when setting this value.

The correct value of the log file size varies depending on computer performance or network performance. The log file size shown here should be considered as just a reference value.

```
(Size of daily job net start log + Size of daily job start log + Size of daily job
termination log + Size of daily job net termination log) x Number of keepdays / 2
```

Note that immediately after the log file is switched, etc, only 1 file can be referenced by the Operation Manager client and jobschprint command. In cases where there is a requirement to constantly reference the file for the number of keepdays, make your estimate without including the '/ 2' part of the estimation formula cited above.

Each log size can be estimated by referring to the following.

When the number of job net starts varies every day, it is recommended to estimate the job net log size based on the largest number of job nets started a day. The lengths of each name or comment should be the maximum value among the actually registered values. If any value is unknown, use the possible maximum value provided inside ( ) below.

Job net start log	50 + S + P + J + N
Job start log	50 + S + P + J + N + j + n
Job termination log	75 + S + P + J + N + j + n
Job net termination log	75 + S + P + J + N

```
S: Local server name length
P: ProjectName length (50 bytes)
J: JobNetName length (50 bytes)
N: JobNetComment length (100 bytes)
j: JobName length (Job command length if JobName is not specified(300 bytes)) (64 bytes)
n: Comment length (64 bytes)
```

[Estimation examples]

Examples of size estimations will be shown assuming the following environment.

- Number of job nets started and terminated a day: 1000
- Number of jobs started and terminated a day: 4000

- Server name: 6 bytes
- ProjectName: Max. 12 bytes
- JobNetName: Max. 8 bytes
- JobNetComment: Max. 16 bytes
- JobName: Max. 10 bytes
- Comment: Max. 20 bytes
- Keepdays: 30 days

Job net start log

50 + 6(S) + 12(P) + 8(J) + 16(N) = 92

Job start log

50 + 6(S) + 12(P) + 8(J) + 16(N) + 10(j) + 20(n) = 122

Job termination log

75 + 6(S) + 12(P) + 8(J) + 16(N) + 10(j) + 20(n) = 147

Job net termination log

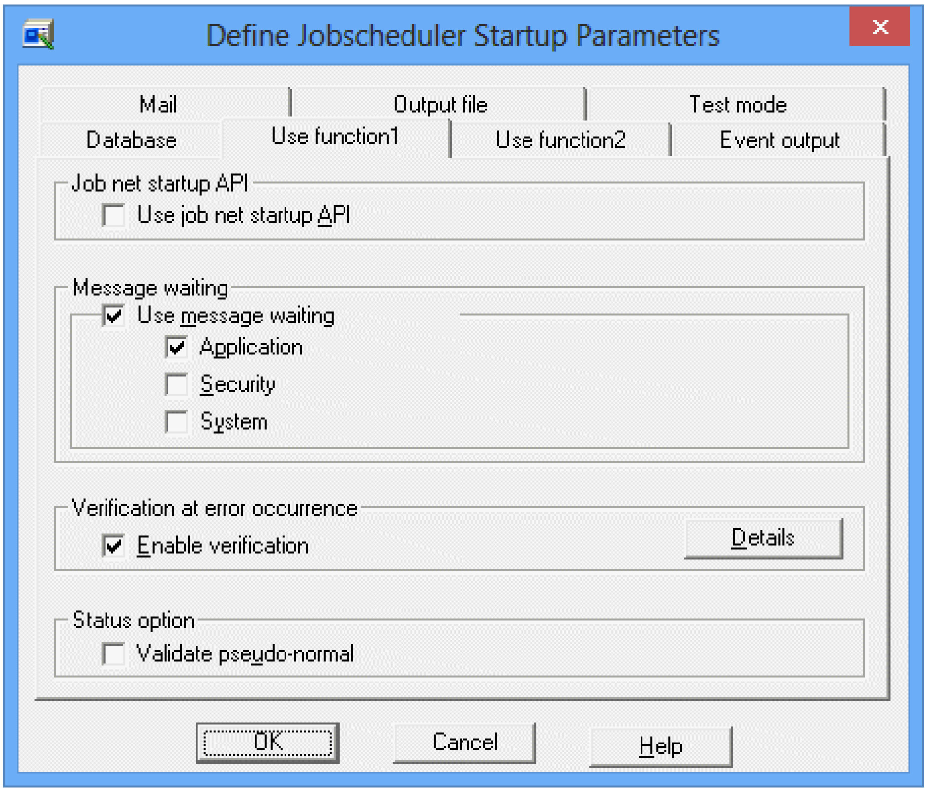
75 + 6(S) + 12(P) + 8(J) + 16(N) = 117

Log file size

(92 x 1,000 + 122 x 4,000 + 147 x 4,000 + 117 x 1,000) x 30 / 2 = 19,275,000 (Approx. 18.4 MB)

In this example, round up 18.4 and register 19 MB as the total log size.

Use function1 sheet in the Define Jobscheduler Startup Parameters window



Job net startup API

□ Use job net startup API

Message waiting

☑ Use message waiting

☑ Application

□ Security

□ System

Verification at error occurrence

☑ Enable verification

Status option

□ Validate pseudo-normal

Job net startup API [Windows]:

Select **Use job net startup API** to start job nets using a job net startup API.

This option is not selected by default. If omitted, you cannot start up a job net using the job net startup API. However, you can use the job net startup time modification API, the job net operation API and group operation API independent from this selection.

Message waiting [Windows]:

Select **Message waiting** to start job nets when a specific message (an event) is output to the event log. This option is enabled by default. If this option is unselected, no message is waited even if a message has been registered on the message table.

There are three types of event logs (applications, security and system event logs). When you specify the **Message waiting** option, you can select one or more of these logs to be monitored. If omitted, **Application** is only selected. To generate a message event using the message event generation command (jobschmsgevent), select **Application**. This option is not selected by default. The next operation starts regardless of the result of the previous execution.

Verification at error occurrence:

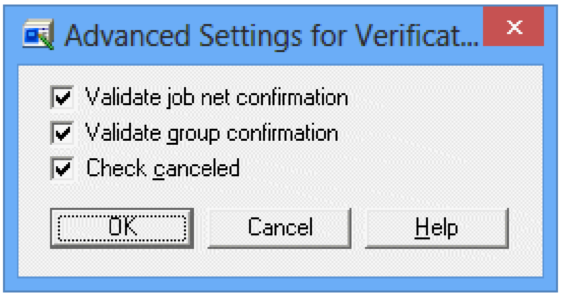
Specify this option to suppress the execution of the next job when a job net or group has terminated abnormally or been terminated forcibly. Details relating to this setting can be specified via the **Advanced Settings for Verification** window, which is displayed by clicking the **Advanced Settings** button.

Status Option:

Select this option to indicate the normal termination or Pseudo-normal termination of each job, job net and group status display. This option is NOT selected by default. If not selected, the "Pseudo-normal termination" is indicated as "normal termination."

Advanced Settings for Verification window

This window is displayed when **Validate confirmation operation** is specified in the **Use function** tab of the **Define Jobscheduler Startup Parameters** window and then the **Advanced Settings** button is clicked.

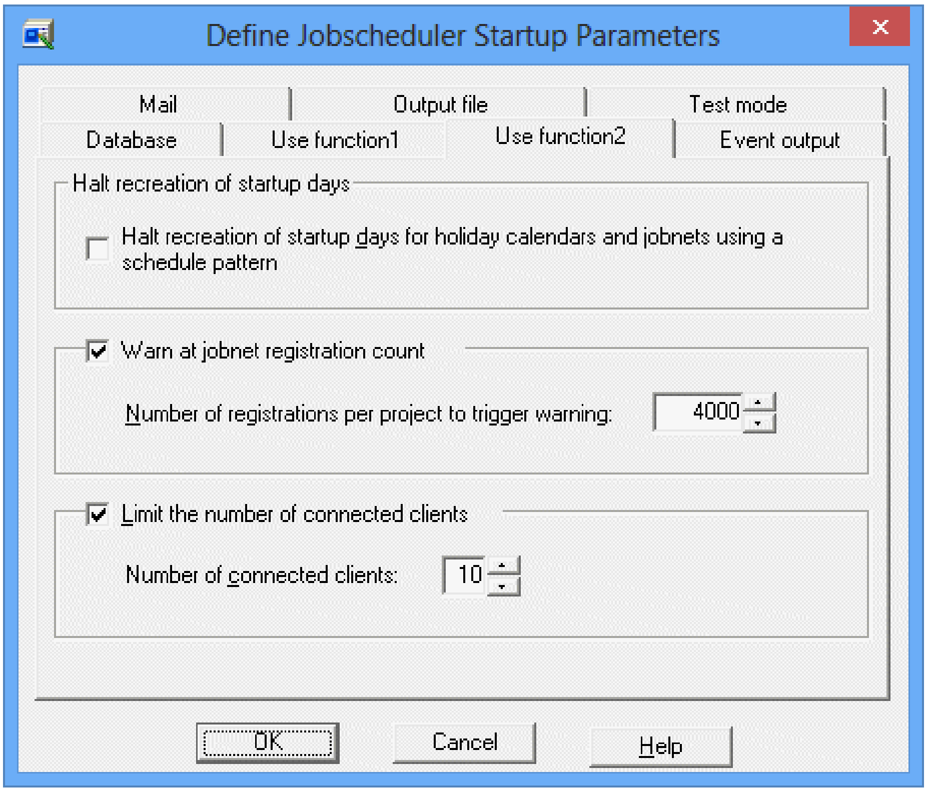

Advanced Settings for Verificat...
☑ Validate job net confirmation
☑ Validate group confirmation
☑ Check canceled
OK
Cancel
Help

Advanced Settings for Verification:

Use this option to suppress the next startup until you confirm after an abnormal or forcible termination of a job net or group. You can select **Check cancelled** only when you have specified at least one of other two options.

All of these options are selected by default if the connection server is Windows. If the connection server is UNIX, it's status is specified other than **Check cancelled.**

Use function2 sheet in the Define Jobscheduler Startup Parameters window



Define Jobscheduler Startup Parameters

Halt recreation of startup days

□ Halt recreation of startup days for holiday calendars and jobnets using a schedule pattern

☑ Warn at jobnet registration count

Number of registrations per project to trigger warning: 4000

☑ Limit the number of connected clients

Number of connected clients: 10

Halt recreation of startup days:

Select this option NOT to recreate a job net execution day if you have changed the holiday calendar or the schedule pattern. This option is NOT selected by default.

Warn at job net registration count:

Select this option to output an alarm message if the number of a job net to be registered for a single project exceeds the limit. In the **Number of registrations per project to trigger warning**, you can specify the limit number of job net. If the user specified job net count exceeds this limit, the following alarm is output.

```
The job net count exceeded the limit.
```

The registration limit can be an integer of 1 to 99999. No alarm is output by default. If the message output is specified in the Systemwalker Operation Manager SE version, the **Number of registrations per project to trigger warning** is set to 255 by default. In the Systemwalker Operation Manager EE version, it is set to 4000 by default.

Limit the number of connected clients:

Specifies the maximum number of clients that can be connected to the Jobscheduler server. The servers to be monitored by the Multi-server monitoring client and the Print Jobscheduler Info clients are also included. If the clients exceeding the limit attempt to connect to the Jobscheduler server, such connection fails and the following error message appears when the **Jobscheduler** is selected during job selection from the Systemwalker Operation Manager client.

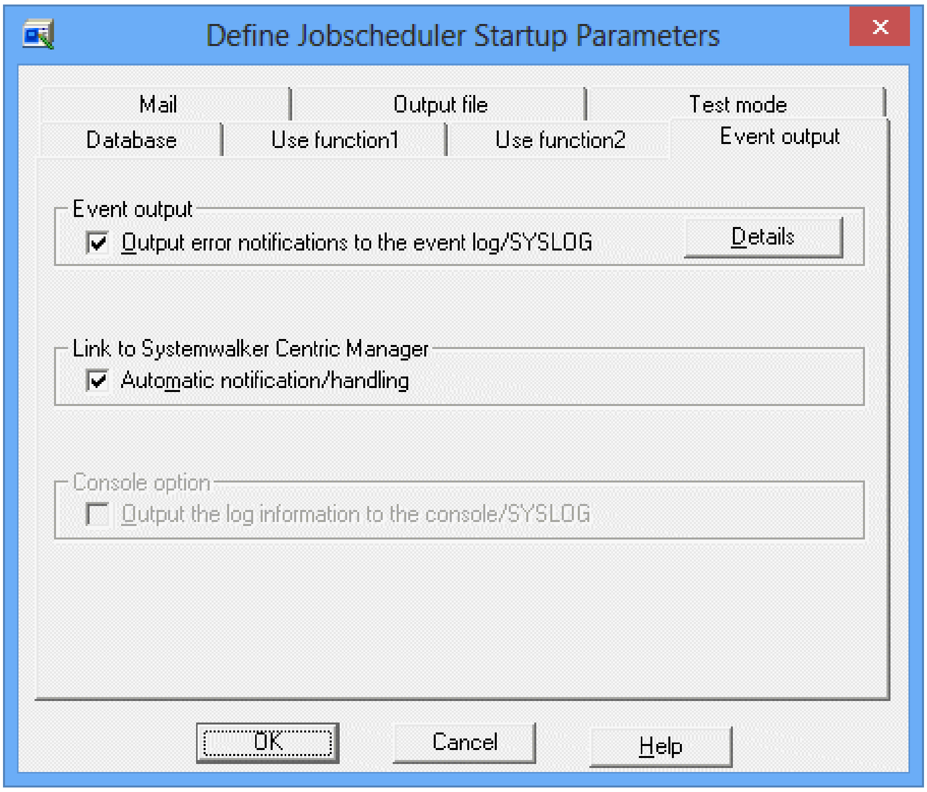
```
Too many clients attempt to connect to the Jobscheduler server.
```

One to 62 (Note) clients can be connected to the Jobscheduler server. The default is unlimited.

If the number of connected clients exceeds the limit during connection by multi-server monitoring client, the client displays the "Access denied" server status.

Note) The maximum value may vary depending on the operating system you use.

Event output sheet in the Define Jobscheduler Startup Parameters window


Define Jobscheduler Startup Parameters

Event output

☑ Output error notifications to the event log/SYSLOG

Link to Systemwalker Centric Manager

☑ Automatic notification/handling

Console option

□ Output the log information to the console/SYSLOG

Event output:

To output error notifications to the event log or syslog, select the **Output error notifications to syslog/event log** check box.

Details relating to output are specified via the **Advanced Settings for Event Output Details** window, which is displayed by clicking the **Advanced Settings** button.

Link to Systemwalker Centric Manager:

Select this option to link to Systemwalker Centric Manager.

If you check the **Automatic notification/handling** box, the abnormal events are displayed in the **Monitor** window of Systemwalker Centric Manager when job net of Systemwalker Operation Manager have terminated abnormally. Also, when a user restarts the abnormally terminated job net, those events are set to the **Resolved** in the **Monitor** window. This box is UNCHECKED and the "Automatic notification/handling" is NOT executed by default.

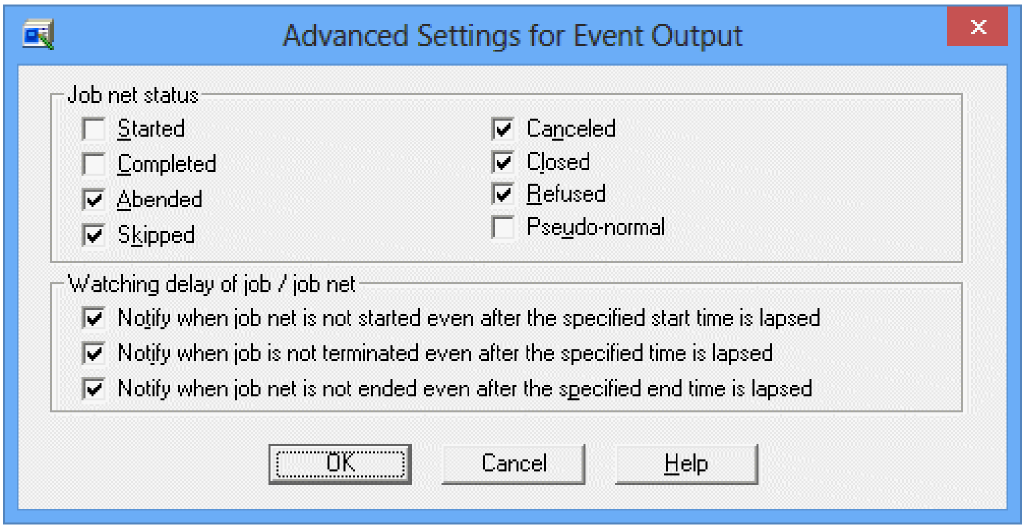
Console Option [UNIX]:

If checked, a message is also output to the console or SYSLOG when it is output to the log file. The message facility level is user.info.

This is unchecked by default. No message is output. Consider that output to SYSLOG increases if you specify this option.

Advanced Settings for Event Output window

This window is displayed when the **Output error notifications to syslog/event log** check box is selected in the **Event output** tab of the **Define Jobscheduler Startup Parameters** window and then the **Advanced Settings** button is clicked.



Advanced Settings for Event Output

Job net status

□ Started

□ Completed

☑ Abended

☑ Skipped

☑ Canceled

☑ Closed

☑ Refused

□ Pseudo-normal

Watching delay of job / job net

☑ Notify when job net is not started even after the specified start time is lapsed

☑ Notify when job is not terminated even after the specified time is lapsed

☑ Notify when job net is not ended even after the specified end time is lapsed

[Windows]

Job net status:

Specify the output condition (**Job Net Status**) to output the job net execution history to the event log. You can select one or more of eight job net states (Started, Completed, Abended, Canceled, Closed, Refused, Skipped and Pseudo-normal). For example, select **Abended** to output an event that signifies that a job net terminated abnormally to the event log. If you want to output an event indicating abnormal termination resulting from execution suspension to the event log, select **Closed** instead of **Abended**.

The following are selected by default:

- Abended:
- Skipped:
- Canceled:
- Closed:
- Refused:

The following are event ID and text details that can be output to the event log depending on the job net status. Using this event log, you can monitor batch jobs in Systemwalker Centric Manager.

Started:

9000/The job net has started. JobNetComment=a JobNetName=b ProjectNam=c

Completed:

9001/The job net has normal ended. JobNetComment=a JobNetName=b Code=c ProjectName=d

Abended:

9002/The job net has abended JobNetComment=a JobNetName=b Code=c ProjectName=d

Canceled:

9002/The job net has abended JobNetComment=a JobNetName=b Code=256 ProjectName=c

Closed:

9002/The job net has abnormal ended. JobNetComment=a JobNetName=b Code=239 ProjectName=c

Refused:

9003/The job net has refused. JobNetComment=a JobNetName=b ProjectName=c

Skipped:

9004/The job net has skipped. JobNetComment=a JobNetName=b ProjectName=c

Pseudo-normal:

9005/The job net has pseudo-normal ended. JobNetComment=a JobNetName=b Code=c ProjectName=d

The followings are the facility levels of the messages that are output to the SYSLOG according to the job net status.

Started:

Information

Completed:

Information

Abended:

Error

Canceled:

Error

Closed:

Error

Refused:

Warning

Skipped:

Warning

Pseudo-normal:

Information

[UNIX]

Job net status:

Specifies the output conditions (job net status) to be used when the job net history is output to the syslog. You can select one or more of eight job net states (Started, Completed, Abended, Canceled, Closed, Refused, Skipped and Pseudo-normal). For example, you can select **Abended** to output an abnormal termination of job nets to the syslog. If you want to output an event indicating abnormal termination resulting from execution suspension to the event log, select **Closed** instead of **Abended**.

The following are selected by default:

- Abended
- Skipped
- Canceled:
- Closed:
- Refused:

The ID and text output to syslog according to the status of a job net are shown below. Note that this syslog can be used by Systemwalker Centric Manager to monitor batch business.

Started:

328/The job net has started. JobNetComment=a JobNetName=b ProjectName=c

Completed:

329/The job net has normal ended. JobNetComment=a JobNetName=b Code=c ProjectName=d

Abended:

330/The job net has abnormal ended. JobNetComment=a JobNetName=b Code=c ProjectName=d

Canceled:

330/The job net has abnormal ended. JobNetComment=a JobNetName=b Code=256 ProjectName=c

Closed:

330/The job net has abnormal ended. JobNetComment=a JobNetName=b Code=239 ProjectName=c

Refused:

331/The job net has refused. JobNetComment=a JobNetName=b ProjectName=c

Skipped:

332/The job net has skipped. JobNetComment=a JobNetName=b ProjectName=c

Pseudo-normal:

333/The job net has pseudo-normal ended. JobNetComment=a JobNetName=b Code=c ProjectName=d

The followings are the facility levels of the messages that are output to the SYSLOG according to the job net status.

Started:

user.info

Completed:

user.info

Abended:

user.er

Canceled:

user.err

Closed:

user.err

Refused:

user.warning

Skipped:

user.warning

Pseudo-normal:

user.info

For details on the job net status, refer to "Job net status" in the *Systemwalker Operation Manager User's Guide*.

Watching delay of job/job net:

Use this option to monitor the scheduled job net startup time, the job's estimated processing time, and the scheduled job net end time. These options are explained below.

Notify when job net is not started even after the specified start time is lapsed:

Check this option to output a notification event or a message to the event log or syslog if a job is not executed even after the job net startup time has elapsed.

This option is selected by default.

Notify when job is not terminated even after the specified time is lapsed:

Select this option to output a notification event or message to the event log or syslog if a job fails to end after the specified time has elapsed.

This option is selected by default.

Notify when job net is not ended even after the specified end time is lapsed:

Check this option to output a notification event or message to the event log or syslog if a job net does not end even though the scheduled termination time has elapsed (the status of the job net is "Executing Jobs", "Warning" or "Start delayed").

This option is selected by default.

The following explains the event IDs, message IDs and message text that are output to the event log or syslog in these states.

All of the messages output to the event log become the "Warning" messages.

Facility levels of messages to syslog are as follows. [UNIX]

If a job net is not started even after the specified startup time has elapsed or a job net is not ended after the specified end time has elapsed:

user.warning

If a job does not end even after the job's estimated processing time has elapsed:

daemon.warning

Using these event logs or syslog, you can monitor batch jobs in Systemwalker Centric Manager.

If a job net is not executed even after the scheduled startup time has elapsed:

[Windows]

4305/XXXX YYYY did not start at scheduled time.

[UNIX]

310/XXXX YYYY did not start at scheduled time.

XXXX: Project name

YYYY: Job net name

If a job does not end even after the job's estimated processing time has elapsed:

[Windows]

9006/It doesn't end even if job name [jobname] lapses by end plan time [time] minutes.

[UNIX]

10114/It doesn't end even if job name (jobname) lapses by end plan time (time) seconds.(Project Name=project name, Job Net=jobnet name)

job name: Job name

time: The estimated processing time that is defined

project name: Project name

jobnet name: Job net name

If a job net does not end even though the scheduled end time has elapsed:

[Windows]

4306/XXXX YYYY did not finish before Estimated end time.

[UNIX]

311/XXXX YYYY did not finish before Estimated end time.

XXXX: Project name

YYYY: Job net name

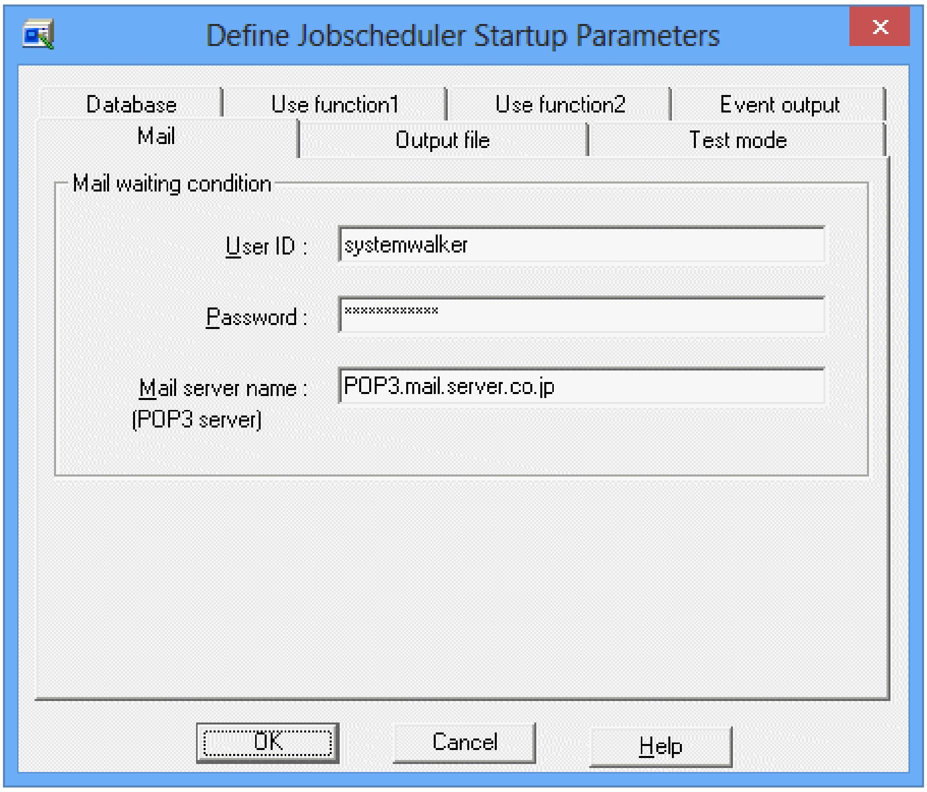
Note

Notification events or messages when a job net is not executed even after the scheduled startup time has elapsed

- No notification event or message is output for a job net in a group that has an invalid startup time.
- No notification event or message is output for a job net that is paused or disabled.
- **Validate job net confirmation** is specified in the **Advanced Settings for Verification** window and no notification event or message is output for a job net that terminated abnormally
- If job nets belonging to a group have valid startup time, notification events or messages are output at the startup time specified in the **Job Net Properties** window rather than the "Scheduled Day and Time" of job nets shown in the **Job Net Lists** window or **Job Lists** window.

Mail sheet in the Define Jobscheduler Startup Parameters window

This window is for setting up the mail waiting conditions when email is used.



User ID : systemwalker

Password : *************

Mail server name : (POP3 server) POP3.mail.server.co.jp

User ID:

For the mail waiting condition, specify the user ID of the user who will receive the mail, using no more than 20 bytes. Mail sent to the specified user will be queued.

EE

For systems operating multiple subsystems, the user ID must be unique in each subsystem.

Password:

Specify the password for the user ID that was specified in the User ID field.

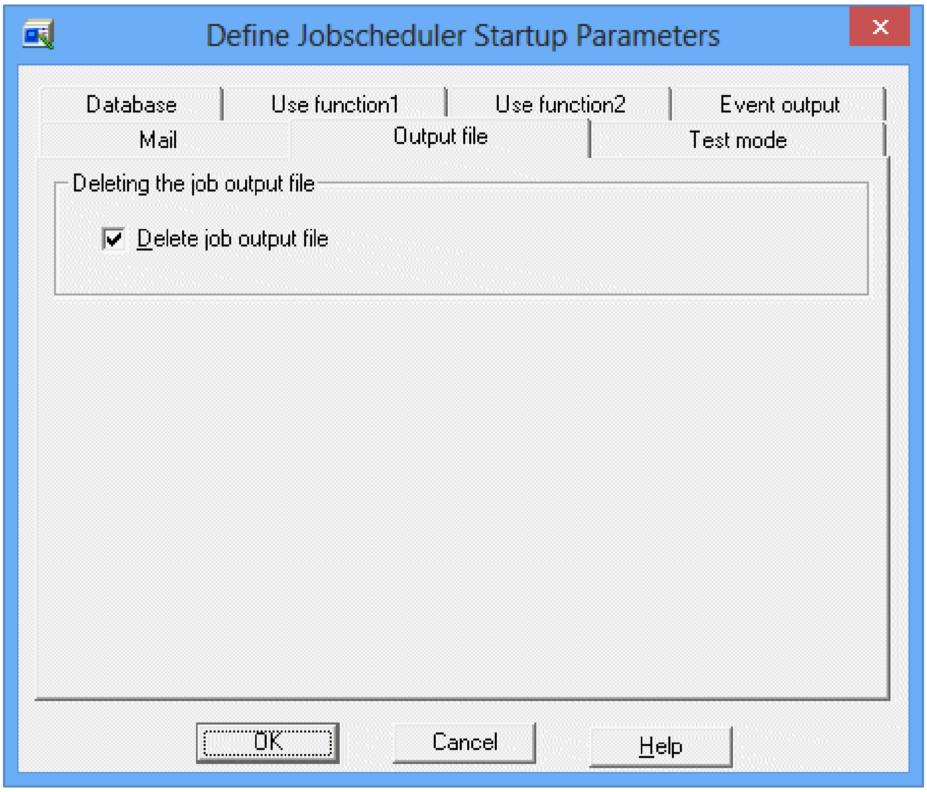
Mail server name:

Specifies a host name of the mail server (POP3 server) that will receive e-mails, using up to 128 characters.

Definition procedure

1. To start job nets triggered by email reception, specify the user ID, password, and name of the mail server as mail waiting conditions.
2. On the mail server, create a user with the user ID specified in Step 1, and specify a password for the user ID.

Output file sheet in the Define Jobscheduler Startup Parameters window



Deleting the job output file

☑ Delete job output file

[Windows]

Deleting the job output file:

Use this option to delete the job output file created during job execution.

This is checked by default, and the job output file is deleted.

[UNIX]

Deleting the job output file:

Use this option to delete the job output file which is created when a job stored in the job net having "Job Execution Control" attributes is executed.

This is checked by default, and the job output file is deleted.

The following lists the "job output files" which are created by the Job Execution Control functions

- jobname.o_job-number (Standard output files)
- jobname.e_job-number (Standard error output files)
- jobname.1_job-number (Job list files)

However, if the schedule server is a Windows server, **Delete job output file** has not been selected, and the names of the standard output file and the standard error output file for schedule jobs have not been specified, then the standard error output file (jobname.e_job-number) will not be created and both the standard output and the standard error output will be sent to the standard output file (jobname.o_job-number).

EE

The "job output files" can be output in the following format if a subsystem other than subsystem 0 is used.

- jobname.s_subsystem-number.o_job-number (Standard output files)
- jobname.s_subsystem-number.e_job-number (Standard error output files)
- jobname.s_subsystem-number.1_job-number (Job list files)

Note

- If you have UNCHECKED the **Deleting the job output file** checkbox, you must delete job output files periodically. If not deleted, the system performance may drop or the disk resources may be exhausted.
- Job list files are not deleted for jobs for which you specified **Standard output file** in the **Detail information** tab of the **Add/ Change - Job** window, even if you selected the **Deleting the job output file** check box. Periodically delete the job list files. Otherwise, performance may drop or disk resources may be depleted.

Job output files

[Windows]

If **Delete job output file** is unchecked, the output files are stored in the "work" directory locating under the database directory.

If **Delete job output file** is checked, the files stored in the "work" directory under the database directory are deleted when the job ends or when the Jobscheduler service starts.

If **Delete job output file** has not been selected, and if the names of the standard output file and the standard error output file for schedule jobs have not been specified, the standard error output file (jobname.e_job-number) will not be created and both the standard output and the standard error output will be sent to the standard output file (jobname.o_job-number).

[UNIX]

a. With a local job

   If **Delete job output file** is unchecked, the output files are stored in the directory you have specified in the Standard information of the job. If no directory is specified, the output files are stored in the home directory of the project owner registering the job (or the user if the user name is specified in **Effective user name** in the **Detail Information** sheet in the **Add/Change/Monitor - Job** window).

   If **Delete job output file** is checked, the output files are stored in the "work" directory locating under the database directory and they are deleted later.

b. With a network job

   - If **Before job execution, change to directory specified at job registration** is selected:

     The following directory of the schedule server becomes the output destination.

     - If **Delete job output file** is not selected:

       The output files are stored in the home directory of the project owner (or the user if the user name is specified in **Effective user name** in the **Detail Information** sheet in the **Add/Change/Monitor - Job** window).

     - If **Delete job output file** is selected:

       The output files are created in the work directory under the database directory but later deleted.

   - If **Before job execution, change to directory specified at job registration** is not selected:

     In the schedule server, the output files are stored in the directory specified in above "a. With a local job."

[Common]

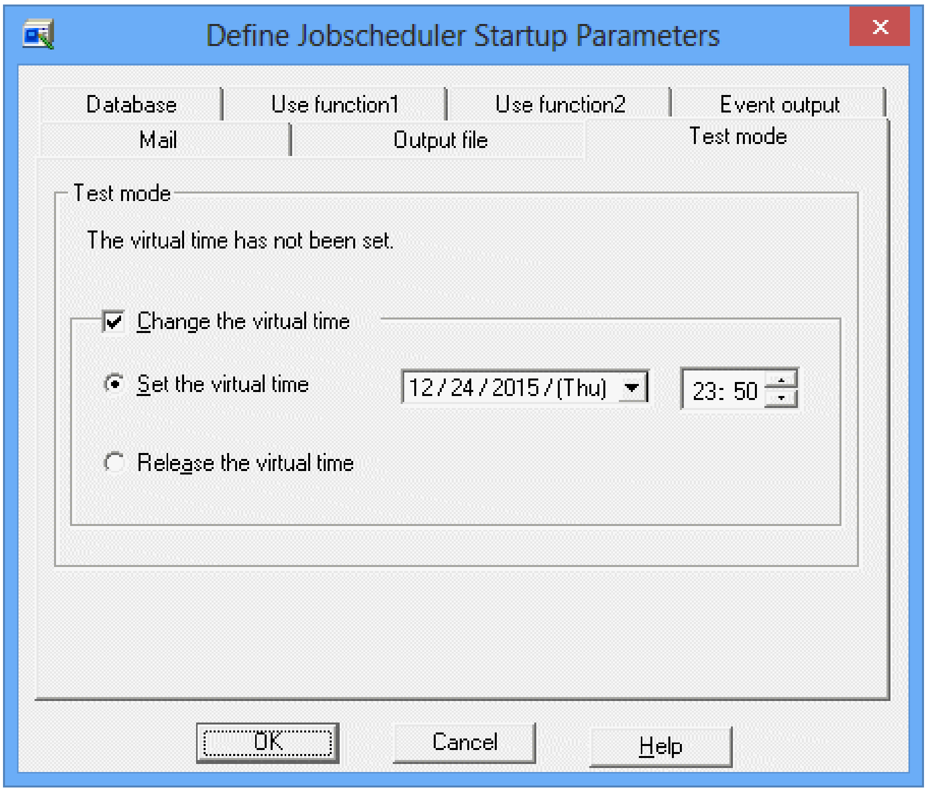
If you have specified the "-o" or "-e" option in the "command name" of jobs, the job files are output to a directory OTHER THAN the "work" directory under the database directory. In such case, the files are output to the specified directory and NOT deleted even if you have checked the **Delete job output file** box.

Also, for on-demand jobs, output files will not be deleted regardless of the settings for the **Delete job output file** checkbox.

The system administrator must delete those output files at regular intervals.

Test mode sheet in the Define Jobscheduler Startup Parameters window

You can set a virtual time on a subsystem to be operated in the Test mode. After you have set the virtual time, you must restart the Jobscheduler services or daemons.



Define Jobscheduler Startup Parameters

Test mode

The virtual time has not been set.

☑ Change the virtual time

● Set the virtual time 12/24/2015/(Thu) 23: 50

○ Release the virtual time

Test mode:

Indicates a time difference from the system if the virtual time has been set.

Change the virtual time:

When you set a virtual time, select the **Set the virtual time** option and set its date and time. It can be up to three (3) years from the present year (this year) to the year after next. (You can set a virtual time before December of 2014 when this year is 2012.)

You cannot set the past date.

To release the virtual time setup, select the **Release the virtual time** option.

Refer to "Operating in the Test Mode" in the *Systemwalker Operation Manager User's Guide* for details.

2.7.2 Defining a Message Table [Windows]

Job net can be started by event log outputs by the OS or other products. To make Jobscheduler recognize the event logs that start job nets, you must associate the "source name" and "event ID" of event logs to the message events which start job net. Use the **Message Table** for their association.

The following explains how to define the message table.

Outline

The message table can be defined from the **Define Message Table** window.

Definition procedure

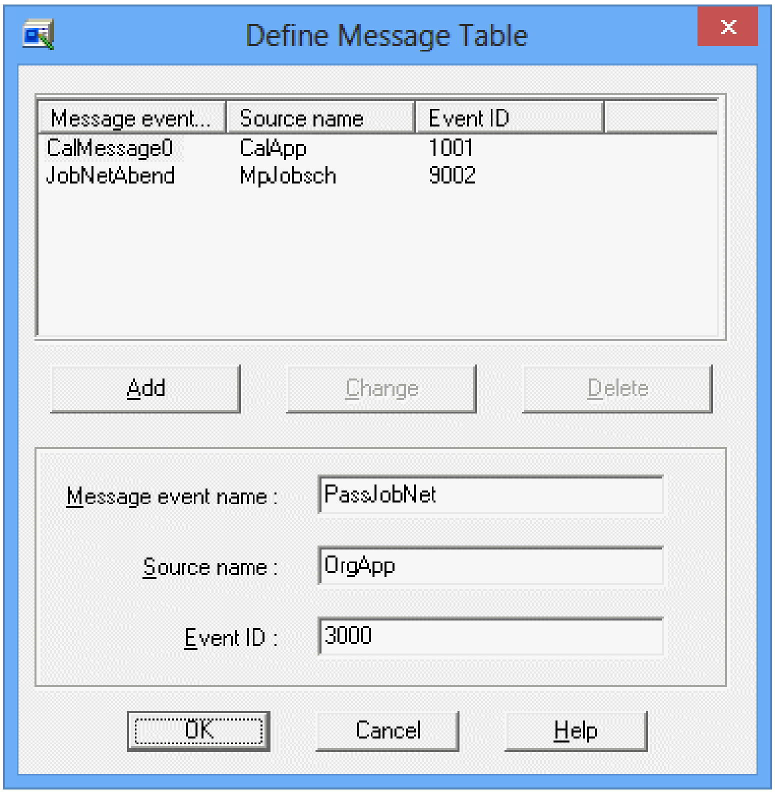
1. Open the **Define Message Table** window.

   Click **Message table** in the **Systemwalker Operation Manager Environment Setup** window, and the **Define Message Table** window will appear.

2. Register message table data.

   Set a message event name, source name, and an event ID, and click **Add** to add them to the list. Click **OK** to register your entries.

Define Message Table window



Message event...	Source name	Event ID
CalMessage0	CalApp	1001
JobNetAbend	MpJobsch	9002

Message event name : PassJobNet

Source name : OrgApp

Event ID : 3000

Add button:

Adds the message event name, source name and event ID in the list when the **Add** button is clicked. The same source name and event ID cannot be duplicated.

Change button:

When you select an already registered message, its data is shown in each field (message event name, source name and event ID). After you have changed the data, click **Change** to update it.

Delete button:

Deletes the selected information from the list.

Message event name:

Specifies a message event name to be set in Jobscheduler, using up to 12 characters. This name CANNOT contain a space, a comma (,) and a colon (:).

Source name:

Specifies a source name of the event to be associated with the message event, using up to 64 characters.

Event ID:

Specifies an event ID, using an integer of 0 to 65535.

2.7.3 Defining a Monitoring Permitted Host

The following explains the preparations required for monitoring the Jobscheduler service or daemon to run on multi-servers when you monitor them from the multi-server monitoring client.

To monitor multi-servers, you must define the name of servers permitting to be monitored on each of those servers.

The following explains how to define a monitoring permitted host.

Outline

A monitoring permitted host can be defined from the **Define Monitoring Permission Host** window.

Definition procedure

1. Open the **Define Monitoring Permission Host** window.

   Click the **Monitoring permission host** button in the **Systemwalker Operation Manager Environment Setup** window to display the **Define Monitoring Permission Host** window.

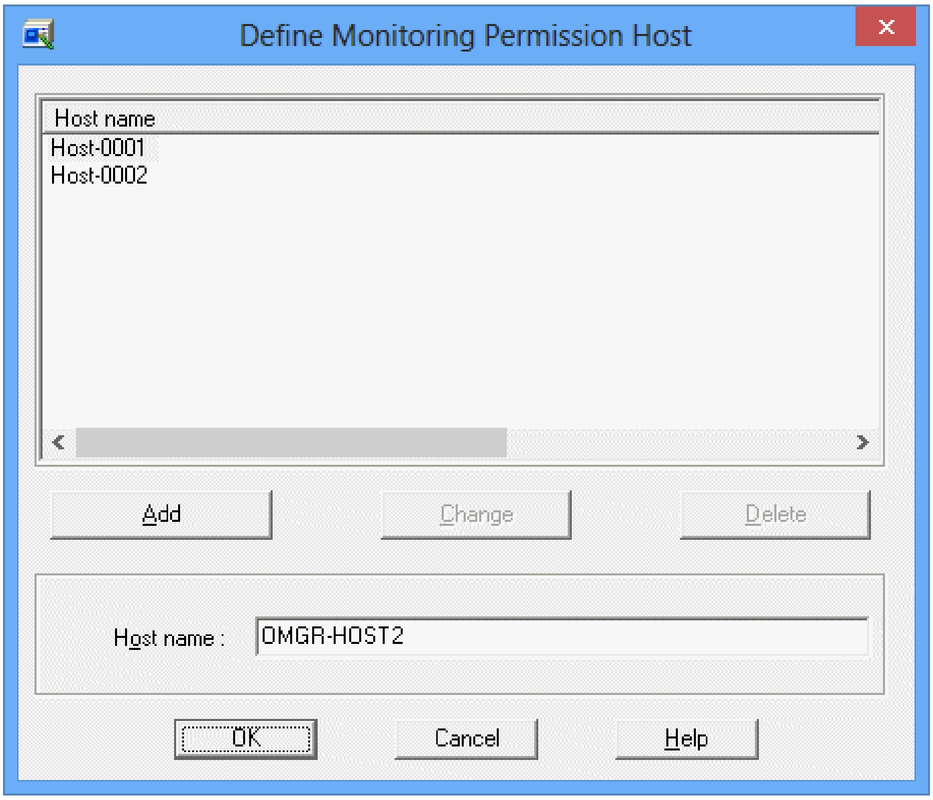
2. Register a monitoring permitted host.

   Enter a monitoring permitted host name and click **Add** to add it to the list. Click **OK** to register your entries.

Note

If the monitoring server is in the multiple NIC environment, write the host names and IP addresses that correspond to all NICs as monitoring permission hosts.

Define the Monitoring Permission Host window



Host-0001
Host-0002

Host name : OMGR-HOST2

Add button:

Enter a host name and click **Add** to add it to the list. The same host name cannot be duplicated.

Change button:

When you select an already registered host name, it is shown in the host name entry field. After you have changed the name, click **Change** to rename the host.

Delete button:

Press this button to delete the selected host from the list.

Host name:

Specify a host name of the monitoring server, using up to 128 characters to permit multi-server monitoring.

You cannot monitor multi-servers from a server NOT defined as the monitoring server (the access will be denied).

Note

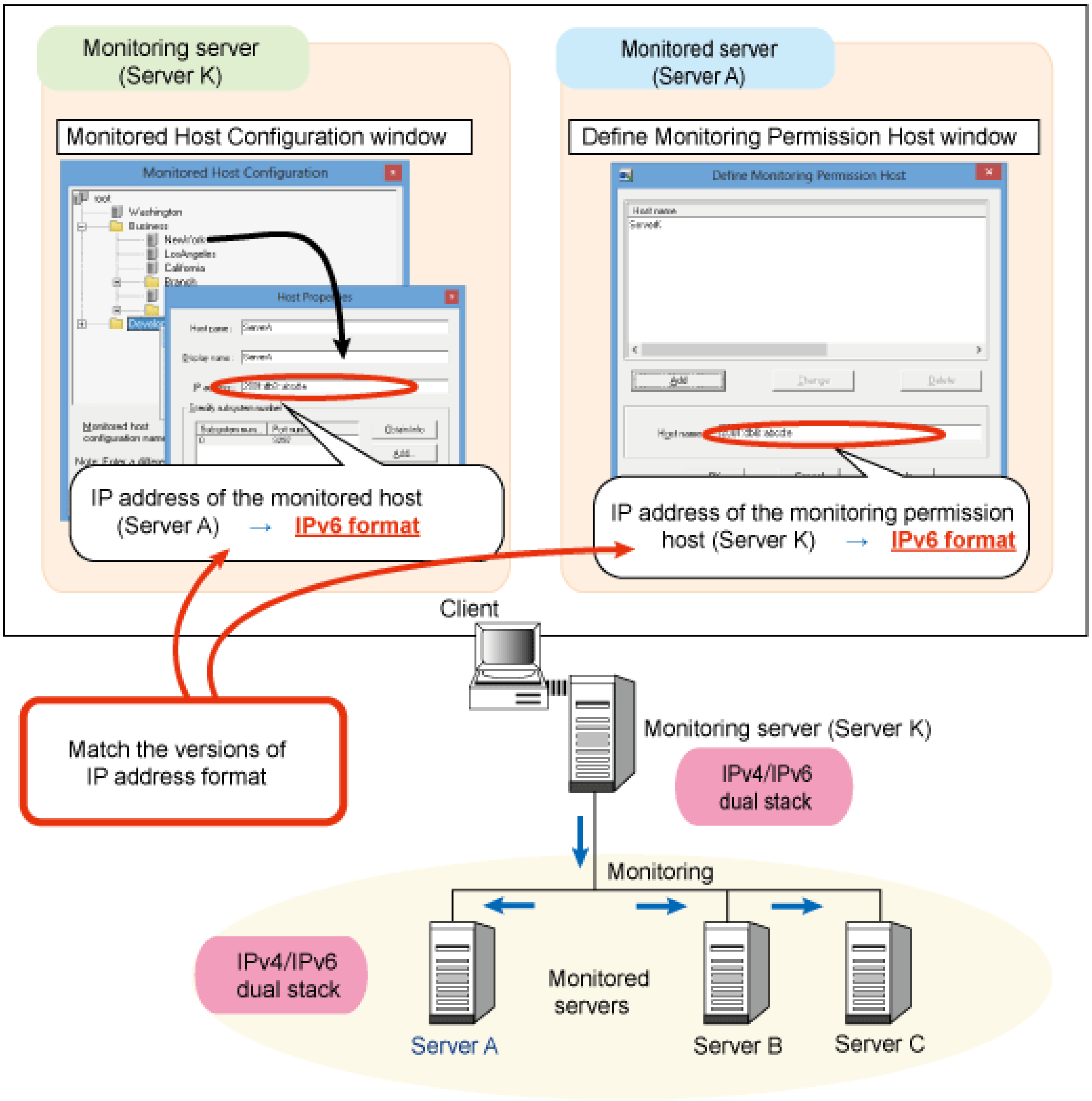
Notes for when mixing internet protocol versions (IPv4/IPv6)

Care must be taken in Systemwalker Operation Manager multi-server monitoring environments when internet protocol versions (IPv4/IPv6) are mixed.

- Specifying IP addresses for the **Host name**

  When registering IP addresses to the monitoring permission host's host name, in the **Define Monitoring Permission Host** window, you must register the IP addresses according to the internet protocol versions being used for communications between the monitoring server and the monitored server.

  For example, if you register the IP address of the monitored server in IPv6 format in the **Monitored Host Configuration** window as below, then the IP address in the **Define Monitoring Permission Host** window on the monitored server side must also be registered in the IPv6 format.



Similarly, in the **Monitored Host Configuration** window, if the IP address of the monitored server is registered in IPv4 format, then the IP address in the **Define Monitoring Permission Host** window on the monitored server side must also be registered in the IPv4 format. If IP addresses with different versions are registered, then the monitored server will be displayed as "Access denied" on the multi-server monitoring client.

- Specifying host names in **Host name**

When registering host names to the monitoring permission host in the **Define Monitoring Permission Host** window, you must ensure that name resolution to IP addresses for internet protocol versions being used for communications between the monitoring server and the monitored server can be performed on the monitored server.

For example, when registering the IP address of the monitored server in IPv6 format in the **Monitored Host Configuration** window, you must ensure that name resolution in the host name of the monitoring server can be performed on the monitored server in IPv6 format. In the same way, when registering the monitored host definitions in IPv4 format, you must ensure that name resolution can be performed in IPv4 format.

If name resolution cannot be correctly performed, then the monitored server will be displayed as 'Access denied' in the multi-server monitoring client.

2.8 Definition of Job Execution Control

This section explains how to define an environment for Job Execution Control.

Job Execution Control manages the job execution environment. Using Job Execution Control, the user can configure a secure and efficient job execution environment by adjusting the job execution order, the number of concurrently executed jobs and others.

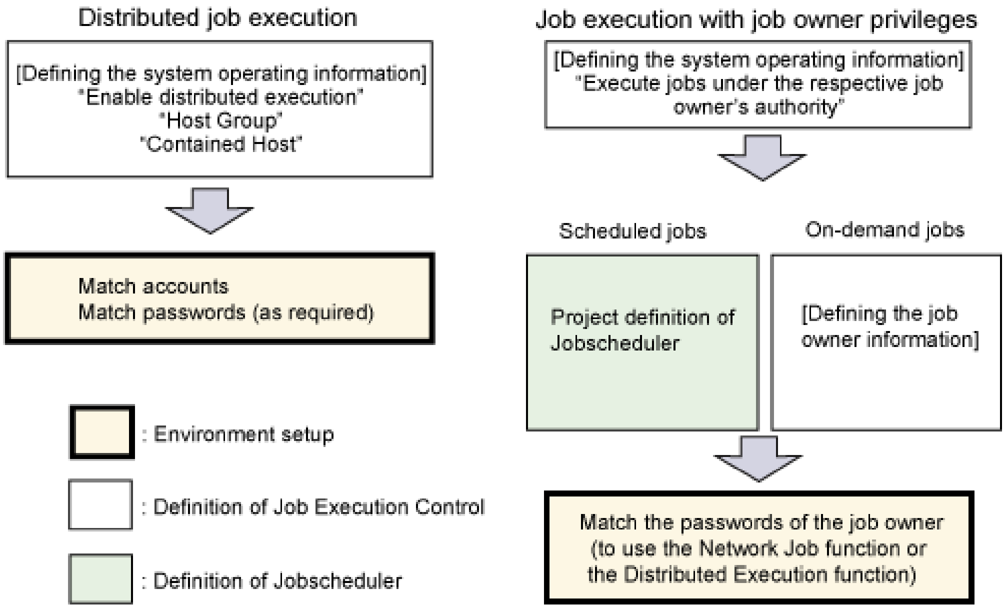
Job Execution Control allows you to define the following job execution environment data.

- Defining the System Operating Information
- Defining a Trust Host
- Defining the Job Owner Information [Windows]
- Defining the user control list for job execution [UNIX]

Once defined, you can use the following functions.

- Distributed job execution
- Job execution with job owner privileges [Windows]

The following outlines the definition flow to use these functions.


Distributed job execution
[Defining the system operating information]
"Enable distributed execution"
"Host Group"
"Contained Host"
Match accounts
Match passwords (as required)
: Environment setup
: Definition of Job Execution Control
: Definition of Jobscheduler
Job execution with job owner privileges
[Defining the system operating information]
"Execute jobs under the respective job owner's authority"
Scheduled jobs
On-demand jobs
Project definition of Jobscheduler
[Defining the job owner information]
Match the passwords of the job owner
(to use the Network Job function or
the Distributed Execution function)

2.8.1 Defining the System Operating Information

The following explains how to define the system operating information.

If you have changed the operating information definition, you must restart Job Execution Control services or daemons to make your change valid.

Outline

The basic job execution environment can be defined using the seven sheets (**Operation Control**, **Logs**, **Use Function**, **Previous Compatibility**, **Cluster Setup**, **Network**, and **Printing Formats**, or using the six sheets excluding **Printing Formats** with the UNIX version) of the **Define Operating Information** window.

Windows used for operating information definition:

- Operating control sheet in the Define Operating Information window
- Create/Edit Queue window
- Logging sheet in the Define Operating Information window
- Options sheet in the Define Operating Information window
- Backward compatibility sheet in the Define Operating Information window

- Cluster settings sheet in the Define Operating Information window
- Add/Edit Node window
- Network sheet in the Define Operating Information window
- Print format sheet in the Define Operating Information window [Windows]

Definition procedure

1. Open the **Define Operating Information** window.

   Click **Operating Information** in the **Systemwalker Operation Manager Environment Setup** window to display the **Define Operating Information** window.

2. Select the desired sheet (**Operation Control**, **Logs**, **Use Function**, **Previous Compatibility**, **Cluster Setup**, **Network**, or **Printing Formats**).

   To define the job and queue control, select the **Operation Control** sheet.

   To define the storage of job execution history and operation records, select the **Logs** sheet.

   To define the code conversion of files and termination code of job steps, select the **Options** sheet.

   To use the previous compatibility in the updated system version, select the **Previous Compatibility** sheet.

   To define the server setup in cluster system operation, select the **Cluster Settings** sheet.

   To define the retry operation in the case of a connection error, select the **Network** sheet.

   When connected to a server running in the Windows version and when you define the printing format of jobs using the Job Results Batch Output function in JCL, check the **Enable prt parameter** on the **Options** sheet and select the **Printing Formats** sheet.

3. Change the definitions.

   When Systemwalker Operation Manager is first installed, the standard definitions including **Job Control** and **Queues** of the **Operating control** sheet the job execution history (**Saved Directory** and **Retention**) of the **Logs** sheet are set. Change the definitions of each sheet according to the system operation.

4. Save your settings.

   Click **OK** to save your settings.

5. Apply your settings.

   When you restart the Job Execution Control services or daemons in the next time, the system starts in the Initialization mode and your settings apply.

Syntax rules

In the **Define Operating Information** window, the following syntax rules apply to the definitions.

Entering a path:

A space, a tab, and the following symbols are NOT allowed to enter.

, ; * ? " < > |

Symbol "\" is NOT recognized as an escape character.

Entering a numerical value:

An alphabet, special characters, a space, and a tab are NOT allowed to enter.

Entering any other text or a text of pull-down menu:

A space, a tab, and the following symbols are NOT allowed to enter.

\ / : ; , * ? " < > |

Note

However, symbols are allowed in the following windows.

When entering a queue name or a host group in the Create/Edit Queues window:

> Only alphanumeric characters, hyphens (-) and underscores (_) can be used. The first character must always be an alphabet. Queue names are NOT case sensitive.

When entering a configuration host name in the Create/Edit Queues window:

> A space, a tab, and the following symbols are NOT allowed to enter.
>
> \ / ; * ? " < > | ( )

If you edit the initialization file directly

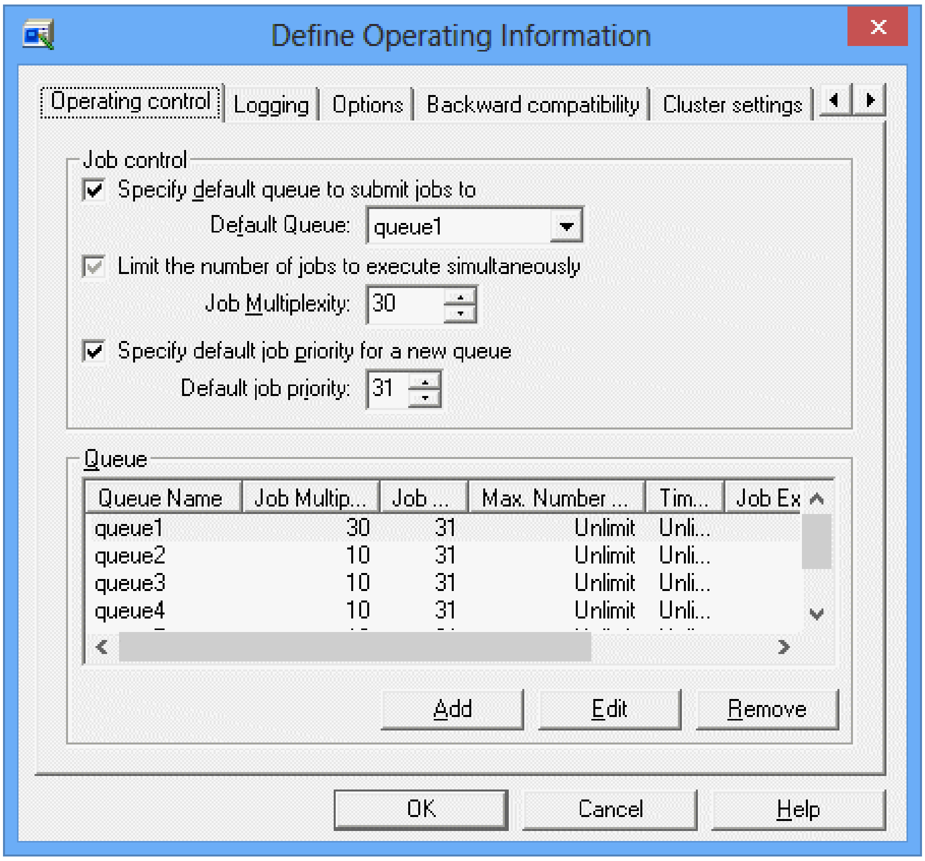
Any change in the **Define Operating Information** window applies to the initialization file of Job Execution Control. You can directly edit the initialization file using an editor such as "vi" or Notepad.

For the definition to allow direct editing of initialization file, see "B.1 Initialization File (Job Execution Control)".

To enable the definitions in the initialization file after editing it, it is required to start Job Execution Control in the initialization mode as described below.

- Execute the mjstop operation termination command by specifying the -c option to terminate the Job Execution Control operation, and then execute the mjstart operation start command to restart the operation. For the mjstart operation start command and mjstop operation terminate command, see the *Systemwalker Operation Manager Reference Guide*.

Operating control sheet in the Define Operating Information window



Job control

☑ Specify default queue to submit jobs to

Default Queue: queue1

☑ Limit the number of jobs to execute simultaneously

Job Multiplexity: 30

☑ Specify default job priority for a new queue

Default job priority: 31

Queue

Queue Name	Job Multip...	Job ...	Max. Number ...	Tim...	Job Ex
queue1	30	31	Unlimit	Unli...	
queue2	10	31	Unlimit	Unli...	
queue3	10	31	Unlimit	Unli...	
queue4	10	31	Unlimit	Unli...	

Specify default queue to submit jobs to:

Specifies a default queue to be used when a job is submitted or when a job is registered in the job net (having the Job Execution Control attributes). The queue name you have defined in the **Create Queue** window must be entered in the **Default Queue** field.

If the destination queue is omitted during job submission, the job is placed in the queue you have specified here. If you omit this option, you must specify the job submission queue during job entry.

Limit the number of jobs to execute simultaneously:

Limits the maximum number of jobs that can be executed concurrently on all servers where Systemwalker Operation Manager has been installed. You must specify this limit in the **Job Multiplexity**. It can be an integer of 1 to 999.

Note that the default value for Windows is 30 and the default value for UNIX is 256.

EE

If multi-subsystems are operating, this limit applies to the jobs concurrently executed on each subsystem. In such case, you cannot limit the number of concurrently executable jobs on the entire server.

Specify default job priority for a new queue:

This priority is used for the queue if the **Default job priority** is not checked in the **Create Queues** window. You can specify a value between 0 and 63, and the larger value has the higher priority.

If omitted, you must check the **Default job priority** in the **Create Queue** window for all queues.

Queue:

Lists queues.

To create a queue, click **Add**. To change the setup of an existing queue, select it from the list and click **Edit**. To delete a queue, select it from the list and click **Remove**.

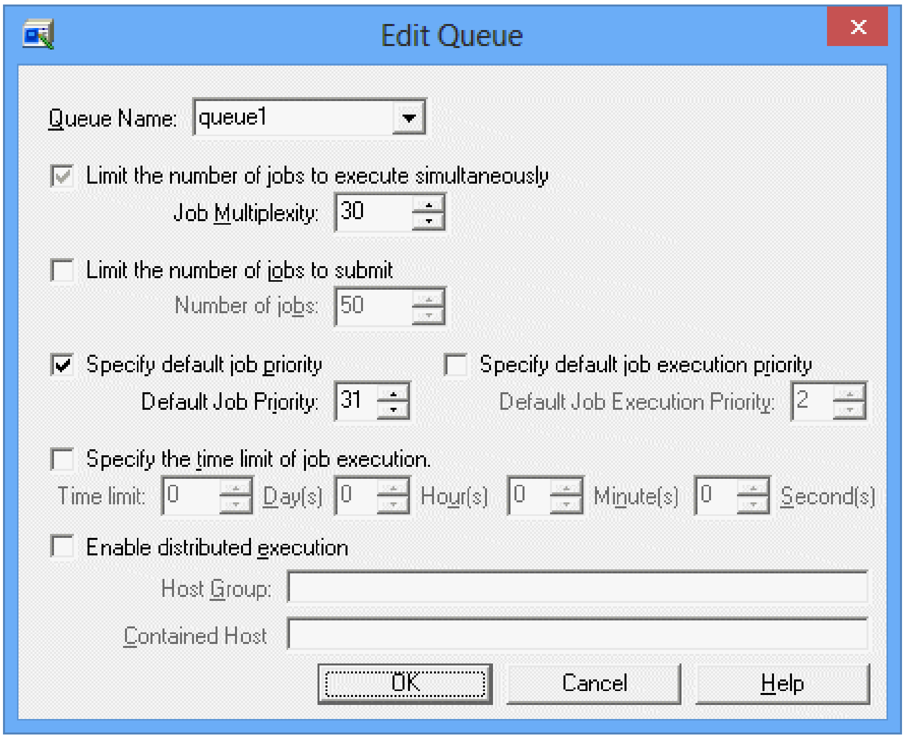
When you click **Add**, the **Create Queue** window appears. When you click **Edit**, the **Edit Queue** window appears. You can set a queue you wish to add to its list or change the setup of an existing queue in the **Create/Edit Queues** window.

Up to 64 queues can be created.

Note

At the **Job Multiplexity**, you can specify a value between 1 and 999. For Windows version, you are recommended to specify a value below 30 as a guide. If the job multiplicity is increased to a higher level, a performance problem may occur or the desktop heap (the area controlled by the Windows system) may be exhausted and the job may terminate abnormally. If you specify 31 or more, be sure to sufficiently verify the performance before operation.

Create/Edit Queue window



Edit Queue

Queue Name: queue1

☑ Limit the number of jobs to execute simultaneously

Job Multiplexity: 30

□ Limit the number of jobs to submit

Number of jobs: 50

☑ Specify default job priority

Default Job Priority: 31

□ Specify default job execution priority

Default Job Execution Priority: 2

□ Specify the time limit of job execution.

Time limit: 0 Day(s) 0 Hour(s) 0 Minute(s) 0 Second(s)

□ Enable distributed execution

Host Group:

Contained Host

The following explains the queue definition.

When you define a queue and press **OK**, it is added to or reflected on the definition of the queue list. However, if you enter a queue name already used in the **Queue Name** field or if you enter an incorrect value, its error is displayed.

Queue Name:

Specifies a queue name. Specify a queue name, using up to 15 bytes.

The queue name is always required.

Limit the number of jobs to execute simultaneously:

Limits the maximum number of jobs that can be executed concurrently in the queue (the job multiplicity in the queue). The **Job Multiplexity** can be an integer of 1 to 999.

Limit the number of jobs to submit:

Limits the number of jobs that can be submitted to this queue (total number of jobs in this queue). The **Number of jobs** can be an integer of 1 to 999.

You can avoid having jobs to be queued by specifying the same value as the Job multiplicity of the queue.

If it is omitted, the number of submittable jobs is NOT limited.

Specify default job priority:

Specifies the priority of jobs placed in the current queue. The **Default Job Priority** can be an integer of 0 to 63. If the priority is omitted during job submission, the operand specified here is used as the priority of the job.

You must specify this option if the **Default Job Priority** is omitted on the **Operation Control** sheet of **Define Operating Information** window.

Specify default job execution priority [Windows]:

Specifies a priority of program thread to be started by the job. The **Default Job Execution Priority** can be an integer of 0 to 4. The larger value has the higher priority of thread.

The following compares priority values 0 to 4.

Set value	Priority class	Thread priority
4	NORMAL	HIGHEST
3	NORMAL	ABOVE_NORMAL
2	NORMAL	NORMAL
1	NORMAL	BELOW_NORMAL
0	NORMAL	LOWEST

Value 2 is set by default.

Specify default job execution priority [UNIX]:

Specifies the CPU allocation priority to jobs. The **Default Job Execution Priority** can be an integer of -20 to 19. The smaller value has the higher CPU allocation priority.

It specifies an execution priority of the process that executes jobs. Values -20 to 19 correspond to the nice values in the UNIX system.

Value 0 is set by default.

A value of -20 to 19 specified here is converted into a value of 0 to 39 and indicated (as the "Default execution priority") in both the **Temporarily Change Queue Definitions** and **Display Detailed Queue Information** dialog boxes. The larger value indicates the higher CPU allocation priority.

Specify the time limit of job execution:

Limits an elapsed time of job execution in the current queue. The time can be an integer of 1 second to 999 days, 23 hours, 59 minutes and 59 seconds.

The job execution elapsed time is NOT set by default.

Enable distributed execution:

Job Execution Control allows distributing the load of each server by allocating the submitted jobs to other servers. It is called the Distributed Execution function. To apply this function to the current queue, specify the **Host Group** and **Contained Host**. The queue that is created when **Enable distributed execution** is selected is referred to as the Distributed Execution queue.

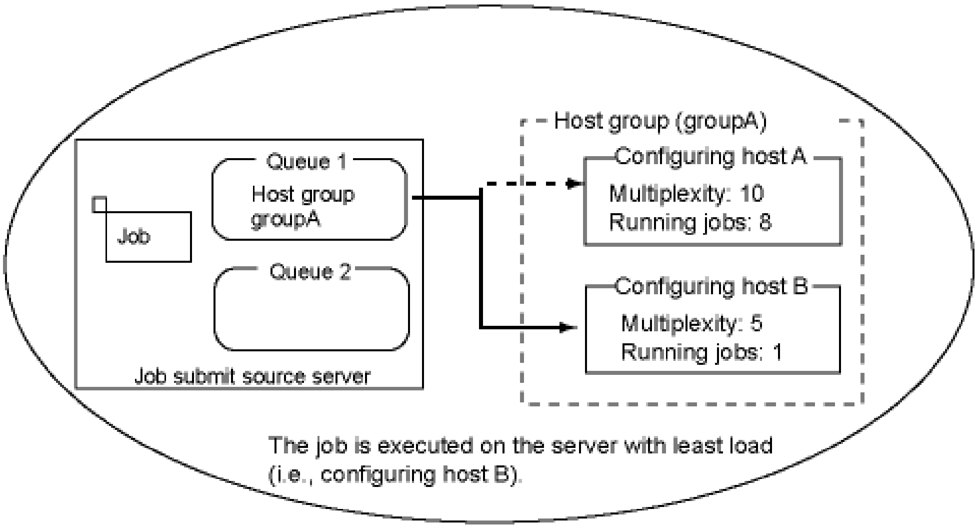
The Host group must be a name of host group (group of servers for load distribution), consisting of up to 64 bytes.

The Configuration host name must be a host name of the server which configures the host group and a multiplicity of jobs (the number of concurrently executable jobs on each server) in the "host-name (multiplicity)" format. You can specify up to 100 host names. Also, you can specify a PC name (including the local host) as the host name. The host name itself CANNOT contain a left parenthesis "(" and a right parenthesis ")". The job multiplicity (the number of jobs that can run concurrently on each server) should be specified as a number between 1 and 999. You can specify multiple sets of job multiplicity by separating them from each other by a comma (,) and by enclosing those sets by a pair of parentheses.

An example is:

```
(host1(4),host2(2))
```

When the Distributed Execution function is used, the "number of executing jobs divided by the multiplicity you have specified in **Configuration host name** is executed by the server having the least load.



During operation, you can change job multiplexity at the distributed server or add/delete a configuration host from the host group for distributed execution. For more details, refer to the *Systemwalker Operation Manager Reference Guide*.

Notes on Distributed Execution function

When using the Distributed Execution function, you must take the following notes.

- If the Distributed Execution function and the Previous Load Distribution function are mixed in the same environment, the system operation is unreliable.
- If you have checked the **Enable the Distributed Execution function** box and if you have distributed to the execution servers the policy of operation information that defines the **Host Group** and **Contained Host**, you must delete these definitions of the Distributed Execution function from the execution servers.
- If a server for distributed job execution has gone down, the problem server is deleted and the distributed jobs are executed by the remaining servers. When the down server is recovered, it may take up to 10 minutes of idling time to restart the distributed job execution.
- If a sever goes down when it is executing a distributed job, this job is terminated abnormally.
- The maximum job multiplicity that can be specified is 999, but the job multiplicity that can actually be achieved depends on environmental factors such as the hardware specifications and the network speed.
- A server down is determined when jobs are submitted to distributed execution servers. When determined, the submitted jobs are distributed to other servers.
- The jobs placed in the distributed execution queue CANNOT be moved to another queue.
- The jobs placed in a queue other than the distributed execution queue CANNOT be moved to the distributed execution queue.
- Jobs submitted using the Distributed Execution function cannot be submitted to a particular subsystem (on the execution server) (when the submitter makes the request for the job, it cannot specify the subsystem number).
- When adding a server that can run in Systemwalker Operation Manager V11.0L10 or later to use the Previous Compatible Load Distribution function, you must enable the Previous Compatible Load Distribution function.
- You cannot use an execution subsystem name in **Contained Host**.

Limited use of Distributed Execution function

You cannot use the Distributed Execution function if:

- Jobs are written in the Job Control Language (JCL).

- Network jobs are submitted, that is if:
    - You have checked the **Submit a Job as a Network Job** checkbox and the specified the **Requesting Host Name** on the **Standard information** sheet of the **Add/Change-Jobs** window,
    - You have checked the **Submit a Job in the Job Net as a Network Job** checkbox and specified the **Default Host Name** on the **Standard information** sheet of the **Job Net Properties** window,
    - You have specified a host name with the "-rh" option in the **qsub** command, or
    - You have specified a host name with the "-rh" option in the **submitinf** argument of Mp_SubmitJob API.
- Jobs are submitted to any given subsystem using the qsub command with the -rsys option specified.
- Jobs are submitted by another host.
    - If the job is a network job submitted from the request source host
    - If the job is submitted using the Distributed Execution function from the request source host
    - If the job is submitted from the request source host, specifying the host name of another server using Job Control Language (JCL), etc.
- Jobs are submitted by anything other than the job net having Job Execution Control attributes.
- The following jobs or commands are used.
    - Task Link command
    - SMS command [Windows]
    - Interstage Work Units
    - REST execution job [Windows][Linux]
    - SAP cloud service link job [Windows][Linux]

Requirements for the Distributed Execution function

When using the Distributed Execution function, you must satisfy the following requirements.

- The account to be inherited must match between this server and the distributed servers. For the account details, see "User privileges required for network jobs and Distributed Execution function" in "2.4.2.1 User Control in Systemwalker Operation Manager."

Previous Load Distribution function [Windows]

If the **Enable the previous Load Distribution Functions** box is checked on the **Previous Compatibility** sheet of **Define Operating Information** window, the Load Distribution functions provided by Systemwalker OperationMGR V10.0L21 or earlier are used. The queue created by specifying **Enable the Load Balancer function of the previous version** in the **Create/Edit Queue** window is referred to as the Backward Compatibility Load Balancing Queue.

You can define a host name for servers in the same domain as the current server in the "Host group" and "Configuration host name." You cannot define a host name of the server participating in another domain or a host name of the server NOT participating in the current domain.

The following message is output to the standard error of jobs. The job execution is NOT affected even if this message is output.

```
'\\job-submitting-computer-name\F3CU_RMT\_wk\job-number' is invalid as
the current directory path. UNC path is not supported. Windows directory will be
used.
```

For details on the previously compatible Load Distribution functions, see the respective manuals of Systemwalker OperationMGR V10.0L21 or earlier.

Notes on setup in the Create/Edit Queues window

The following gives the notes you notice during setup in the **Create/Edit Queues** window.

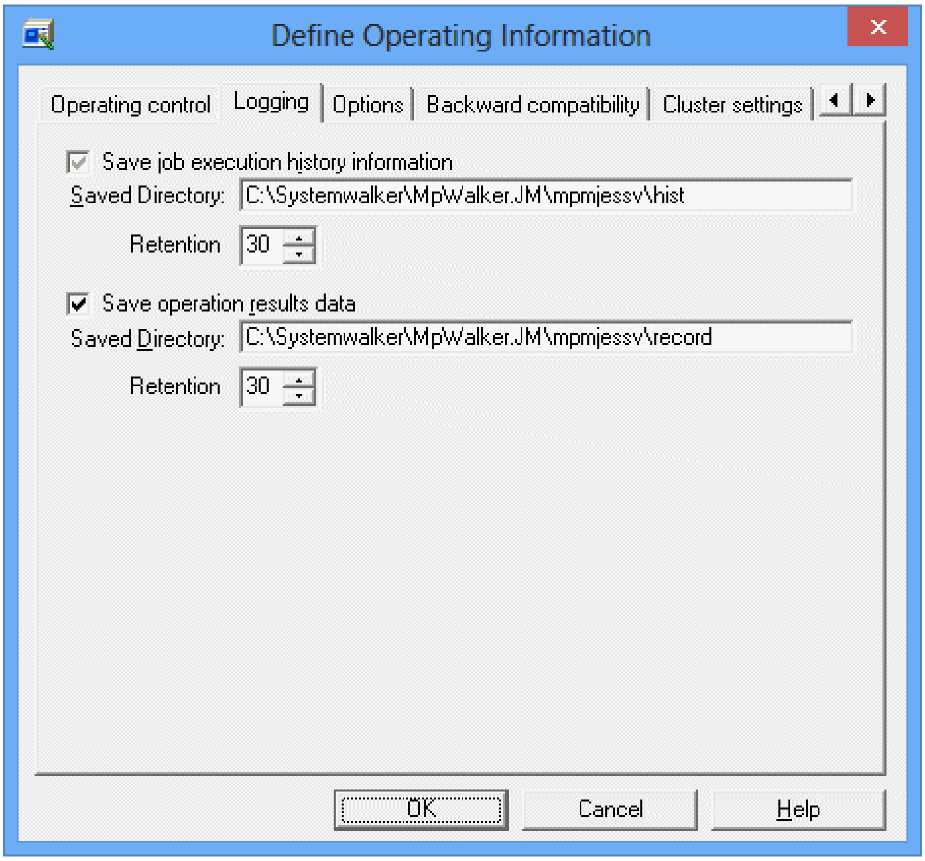
- You cannot omit the definition in the **Create Queues** window.
- To submit an online job (for startup and shutdown control of InterStage work units), define a queue dedicate to online jobs. During this time, do not set the job execution time limit.

  When Systemwalker Operation Manager is first installed, the "online1" queue which is dedicated to online jobs is defined. You can use this queue. It has the following preset parameters.

  - Queue name: online1
  - Number of concurrently executable jobs: 30[Windows]: 256[UNIX]
  - Default queue priority: 31

  However, if you have upgraded the system from version V5.0L10 or earlier (or V4.1 or earlier in UNIX system), the "online1" queue is NOT defined. You must add a queue dedicate to online jobs.

Logging sheet in the Define Operating Information window



☑ Save job execution history information

Saved Directory: C:\Systemwalker\MpWalker.JM\mpmjessv\hist

Retention 30

☑ Save operation results data

Saved Directory: C:\Systemwalker\MpWalker.JM\mpmjessv\record

Retention 30

Save job execution history information:

Saves the job execution history information (log file) of Systemwalker Operation Manager. If selected, the **Job execution history information** box is always checked. You can only change the **Saved Directory** and **Retention** on this sheet.

Saved Directory:

Specify a full path name where you create a log file. The path name can be up to 245 bytes long. If you have entered a non-existing path name, you are asked for your confirmation.

A log file is named as follows and it is created under this path.

```
date.log
```

date: The date (year, month and day) when a log file is created.
The year is indicated by 4 digits, the month is indicated by 2 digits, and the day is indicated by 2 digits.

When the system is first installed, the log file is stored under the following directory.

[Windows]

```
Systemwalker Operation Manager installation directory
\MpWalker.JM\mpmjessv\hist
```

EE

When connected to the server during multi-subsystem operation, you must specify the following path.

- Subsystem number 0: Destination path (the path where the log file is created)
- Subsystem numbers 1 to 9: Destination-path\n (where, "*n*" if a subsystem number).

[UNIX]

```
/var/spool/mjes/hist
```

EE

When connected to the server during multi-subsystem operation, you must specify the following path.

- Subsystem number 0: Destination path (the path where the log file is created)
- Subsystem numbers 1 to 9: Destination-path/*n* (where, "*n*" if a subsystem number).

Retention:

Specifies a number of days when the log file is kept. It can be from 1 day to 31 days. When a log file exceeds its storage period, it is deleted.

Save operation results data:

You must specify this option to collect the operating results data.

Saved Directory:

Specify a full path name where you create an operating results data file. The path name can be up to 245 bytes long. If you have entered a non-existing path name, you are asked for your confirmation.

The operation results data file is named as follows and it is created under this path.

```
date.csv
```

date: The date (year, month and day) when an operating results data file is created.
The year is indicated by 4 digits, the month is indicated by 2 digits, and the day is indicated by 2 digits.

EE

When connected to the server during multi-subsystem operation, you must specify the following path.

- Subsystem number 0: Destination path (the path where the log file is created)
- Subsystem numbers 1 to 9: destination-path\n (where, "n" if a subsystem number).

  It must be "destination-path/*n*" (where, "*n*" if a subsystem number) in the UNIX system.

Retention:

Specifies a number of days when the operating results data file is kept. It can be from 1 day to 31 days. When an operating results data file exceeds its storage period, it is deleted.

For details on the operation result information files, refer to the *Systemwalker Operation Manager Reference Guide*.

Estimation for log files and operation results data files

If you have specified the Storage location option for log files and operation results data files, they are created and stored in the specified location. Therefore, you must calculate the required disk capacity and assign it in advance. If jobs are forcibly terminated, the slightly larger disk capacity is required. You must assign an enough disk capacity.

Estimation Formula for Log Files

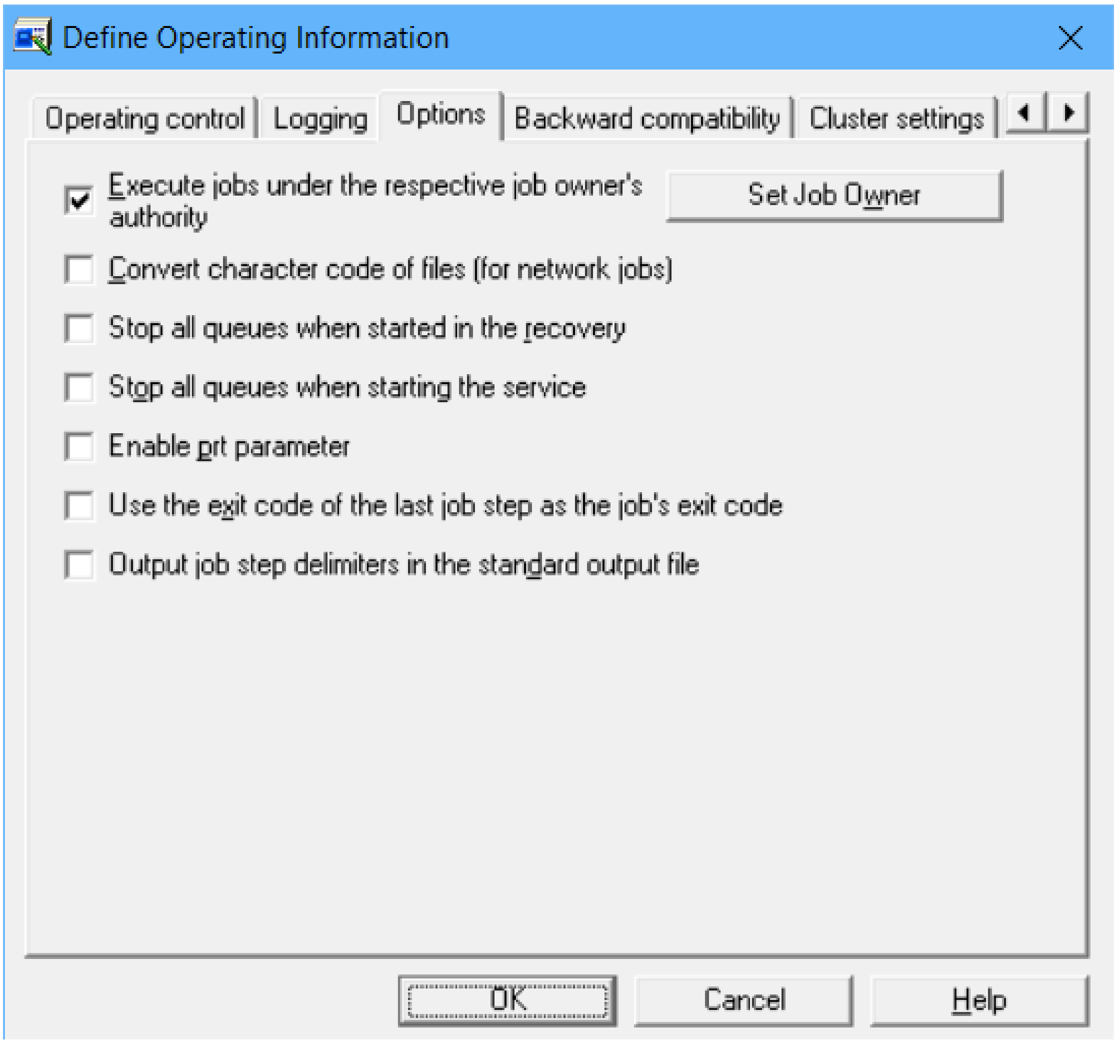
(No. of jobs per day) x (300 bytes) x (Storage period in days) + (No. of forcible termination times of jobs) x (80 bytes)

Estimation Formulas for Operation Results Data Files

(Service startup/shutdown record capacity + Job record capacity + Step record capacity) x Storage period in days

```
Service startup/shutdown record capacity (in bytes per day)
  (72 + h) x S
    h: Host name length
    S: Number of service/daemon startup/shutdown times in a day

Job record capacity (in bytes per day)
  (429 + (4 x h) + j + u + (2 x q) + c) xJ
    h: Host name length (Use its maximum value.)
    j: Job name length (Use its maximum value.)
    u: User name length (Use its maximum value.)
    q: Queue name length (Use its maximum value.)
    c: Command name length (Use its maximum value.)
    J: Number of job startup times in a day

Step record capacity (in bytes per day)
  (182 + (2 x h) + j + s)x S
    h: Host name length (Use its maximum value.)
    j: Job name length (Use its maximum value.)
    s: Step name length (Use its maximum value.)
    S: Maximum number of steps within the job startup count in a day

If the maximum values are unknown, use the following reference values.
    h: Host name length    64 bytes
    u: User name length    64 bytes
    j: Job name length    64 bytes
    q: Queue name length    15 bytes
    s: Step name length    16 bytes
```

Options sheet in the Define Operating Information window



☑ Execute jobs under the respective job owner's authority

□ Convert character code of files (for network jobs)

□ Stop all queues when started in the recovery

□ Stop all queues when starting the service

□ Enable prt parameter

□ Use the exit code of the last job step as the job's exit code

□ Output job step delimiters in the standard output file

Execute jobs under the respective job owner's authority [Windows]:

The jobs executed on Systemwalker Operation Manager of the Windows version are executed under the privilege of the Job Execution Control service log on account on the server. If you check this box, the user having the job execution privilege can execute each job.

If this function is used with network jobs, this checkbox must be selected on both the server from which the job is submitted and the server to which it is submitted.

Refer to "2.4.2.2 Job Execution Privileges" for information about job execution privileges assigned when this checkbox is selected.

In order to execute jobs under the authority of the respective job owners, you must carry out the following tasks in addition to specifying this parameter.

- Select **Administrative Tools** >> **Local Security Policy** in the **Control Panel**, to assign **Log on as a batch job** privileges to the respective accounts of the job owners.

  When using this function for network jobs, execute on both the server that submits the job and the server that receives the job. Also execute on both the server that actually submits jobs and the server used to execute jobs for domain users.

- Define the job owner information.

  When using this function for network jobs, execute on the server that submits the job.

  Enable the **Set Job Owner** button by selecting the **Execute jobs under the respective job owner's authority** check box. Click **Set Job Owner** to define the job owner information. Refer to "2.8.3 Defining the Job Owner Information [Windows]" for details.

Notes if the Execute job under the respective job owner's authority option is specified:

- You cannot execute a network job for which the job submitting server is running UNIX and the destination server is running Windows if you specified **Execute jobs under the respective job owner's authority** on the destination server.
- If you use the previous Load Distribution functions by selecting the **Execute job under the respective job owner's authority** option, you must assign the same job owner password on all servers. When network jobs are submitted or when the distributed execution queues are used for job submission to other servers, the authentication data used on the job submitting server is passed to the destination server. Therefore, if the password does not match between those servers, the jobs are terminated abnormally.

  The password matching between servers depends on the user account type as follows.

Account type of job execution user	Relationship between job submitting server and its destination server		
	Within the same domain	Within the trusted domain	Outside of the domain
Domain account	_	_	_
Local account	Same	Same	Same

```
_: Different passwords may be used.
Same: The same password must be used.
```

Convert character code of files (for network jobs):

The file code conversion is required for execution of network jobs or distributed execution jobs among the servers having different code systems. Specify the operation code conversion if required during execution of network jobs or distributed execution jobs.

If not specified, no code conversion takes place during execution of those jobs.

Note

If a non-text file is specified as the standard output file for execution of network jobs or distributed execution jobs, the code conversion may fail.

Stop all queues when started in the recovery:

If the system is shut down due to a system crash or power failure, Job Execution Control services will resume operations with the queue in progress when the system starts up next time (Recovery mode). However, before resuming operations, you may want to take the required corrective actions by checking the status of servers and jobs where Systemwalker Operation Manager has been installed. In such case, you must check this box.

If you have checked this box, the jobs are waited (stopped queue status). The jobs are executed only when the queue is started. After you have taken the corrective actions, you can restart the operation by activating the queue using the **qstart** command.

Stop all queues when starting the service:

Use this option if you do not start job execution until you have checked the system status during periodical hardware maintenance or others. If you have checked this box, the jobs are waited (stopped queue status) when the Job Execution Control services or daemons are restarted. After you have taken the corrective actions, you can restart the operation by activating the queue using the **qstart** command.

Enable prt parameter [Windows]:

Use this option to use the Batch Output function for JCL job results.

When you check this box, the **Printing Formats** sheet appears and you can set the printing parameters on it.

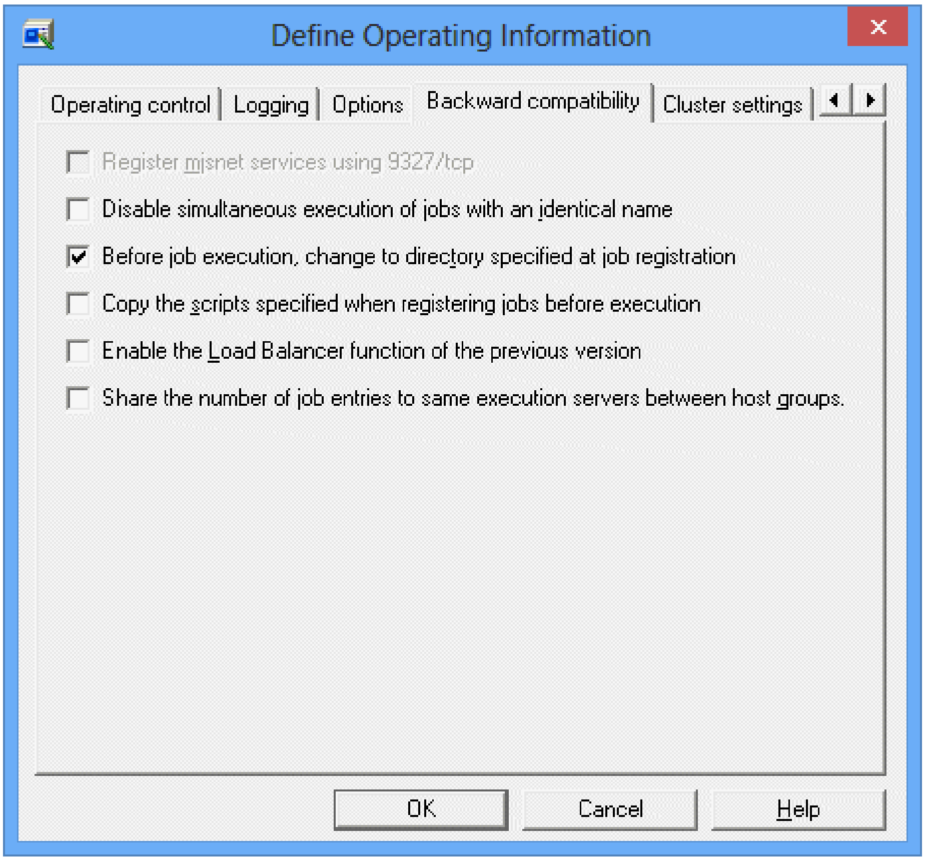
Use the exit code of the last job step as the job's exit code:

Check this box to use a termination code of the recently executed job step written in the Job Control Language (JCL) as the job termination code. If not checked, a termination code of the largest job step written in the JCL is used as the job termination code.

Output job step delimiters in the standard output file:

Use this option to output both the job step name and the job step termination code to the standard output file of job steps written in the JCL.

Backward compatibility sheet in the Define Operating Information window



□ Register mjsnet services using 9327/tcp

□ Disable simultaneous execution of jobs with an identical name

☑ Before job execution, change to directory specified at job registration

□ Copy the scripts specified when registering jobs before execution

□ Enable the Load Balancer function of the previous version

□ Share the number of job entries to same execution servers between host groups.

Register mjsnet services using 9327/tcp [Windows]:

Use this option to add the "mjsnet" services to the **services** file using 9327/tcp. We recommend you to specify this option here as the port numbers must be consistent between servers for network job execution. You can use this option if you are using the system in V5.0L30 only.

Disable simultaneous execution of jobs with an identical name:

Use this option NOT to execute jobs having the same name concurrently.

Before job execution, change to directory specified at job registration:

This is checked by default. Usually, you need not to change it. If checked, jobs having Job Execution Control attributes are executed in the directory you have specified during job registration. If unchecked, jobs are executed in the following directory.

[Windows]

Jobs are executed in the temporary work area of Job Execution Control.

[UNIX]

Jobs are executed in the home directory of the project owner who has registered the job net.

Copy the scripts specified when registering jobs before execution:

This is not checked by default. The job performance improves by clearing this option. Usually, you need not to change it.

Use this option to copy the script file or batch file you have specified during job registration to the spool and execute it.

If checked, the options of the batch file are resolved during job submission.

Note

If this check box is selected, the length allowed for a row of the script file or batch file that can be submitted as a job is up to 2,050 bytes.

Enable the Load Balancer function of the previous version [Windows]:

Use this option to enable the previous Load Distribution functions. If unchecked, the Distributed Execution function is enabled.

Note

When **Restrict so that only users included in the swadmin group can start demand jobs, start jobnet Job Execution Control attributes or use Jobscheduler command functions.** is checked in the **Define Operation Manager Shared Parameter** window for user restriction, the Previous Load Distribution CANNOT be used.

To use the Previous Load Distribution function, disable the user restriction definition.

Share the number of job entries to same execution servers between host groups.

For distributed execution jobs, select this checkbox to share the "number of jobs submitted to identical execution servers" between different host groups.

If this checkbox is selected and execution servers with the same name have been defined in different host group definitions, "the number of jobs submitted" will be shared between the host groups. If the host groups have different settings for the maximum number of jobs that can execute concurrently, jobs will be allocated within the maximum number of concurrent jobs that has been defined for each group.

By default, this option is not selected.

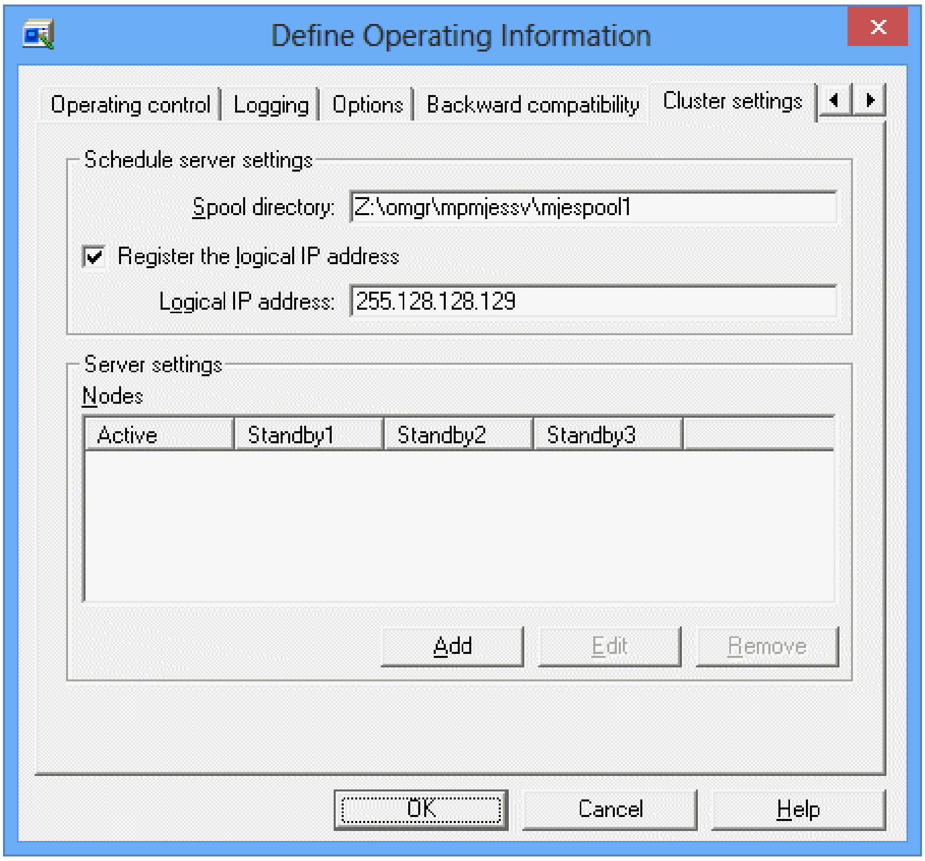
If the **Enable the Load Balancer function of the previous version** checkbox has been selected, this option will be grayed out and the function cannot be enabled.

Cluster settings sheet in the Define Operating Information window

The following explains how to configure the cluster system using the **Cluster Setup** sheet.

Setup of schedule server

The following explains your setup on the schedule server.



Schedule server settings

Spool directory: Z:\omgr\mpmjessv\mjespool1

☑ Register the logical IP address

Logical IP address: 255.128.128.129

Server settings

Nodes

Active	Standby1	Standby2	Standby3

Schedule server settings:

You must set the followings on ALL schedule servers which configure the cluster system.

Spool directory [Windows]:

Specifies a location to store the spool directory if the cluster system on the schedule server runs in the Windows version. The storage location must be the shared disk.

Register the logical IP address:

Use this option to control network job submission using its logical IP address. Use this option to specify a logical IP address, using up to 64 bytes. The same logical IP address must be used on both active and standby systems of all schedule servers which configure the cluster system.

If you have set the logical IP address, you need not set it up on the execution servers.

Server settings:

Use this option for setup on the destination server which executes the submitted network jobs. No setup is required on the schedule server.

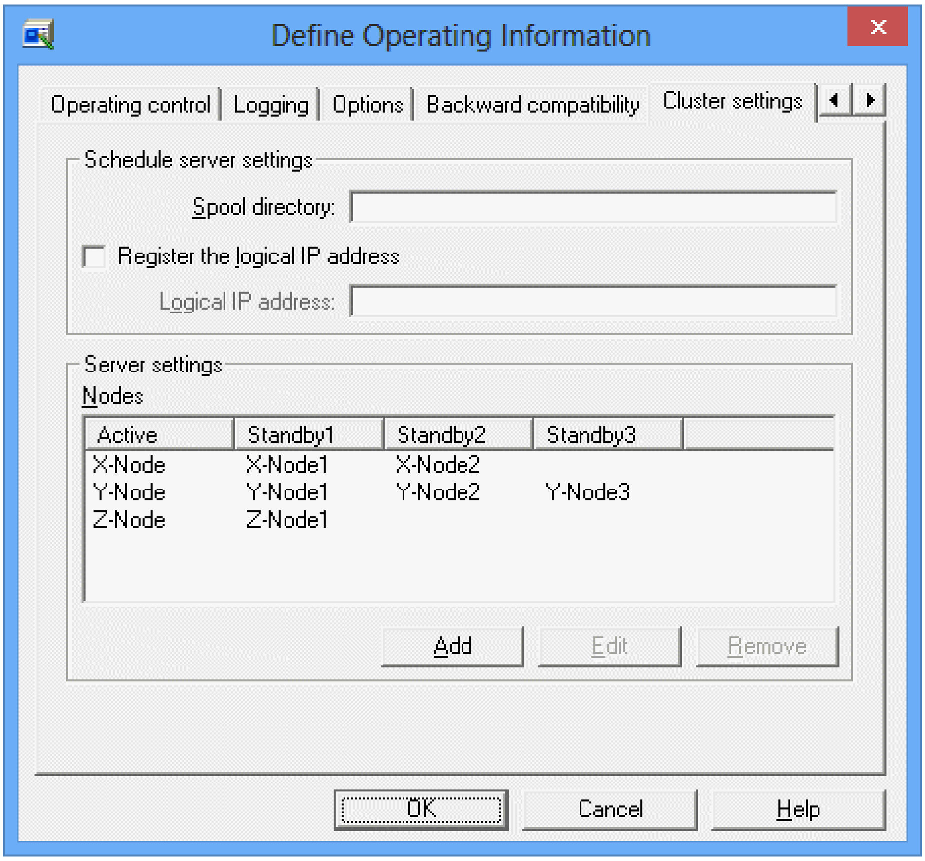
Information

The logical IP address is used as the destination address of the job termination notification.

When the logical IP address of the cluster is registered, the execution server can notify the schedule server of job termination even if the active and standby systems are switched due to failover of the schedule server in the middle of network job execution.

Setup of execution servers

The following explains your setup on the execution servers.



Spool directory:

□ Register the logical IP address

Logical IP address:

Nodes

Active	Standby1	Standby2	Standby3
X-Node	X-Node1	X-Node2	
Y-Node	Y-Node1	Y-Node2	Y-Node3
Z-Node	Z-Node1		

Schedule server settings:

Use this option for setup on the network job submitting server. No setup is required on the execution servers.

Server settings:

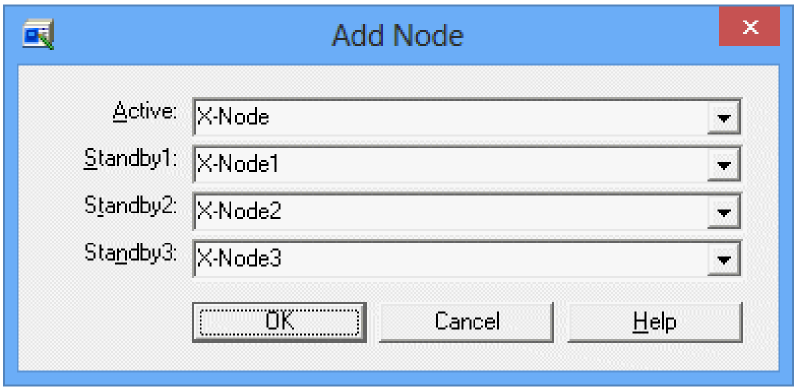
Use this option for setup on the destination server which executes the submitted network jobs. You must set this option to accept network jobs submitted by the schedule server which configures the cluster system. This setup is NOT required if you do not accept network jobs submitted by the schedule server which configures the cluster system. Also, this setup is NOT required if you have specified the logical IP address during schedule server setup.

Click **Add** to open the **Add Node** window, and you can configure the schedule server for network job submission.

When you have set, the schedule server which configures the cluster system is displayed on the Node tree.

When you select a row on the Node tree and click **Edit**, the **Editing the Node Name Definition** window appears and you can change the schedule server of the cluster system. Click **Remove** to delete the schedule server configuration from the selected Node tree.

Add/Edit Node window



Active: X-Node

Standby1: X-Node1

Standby2: X-Node2

Standby3: X-Node3

Active:

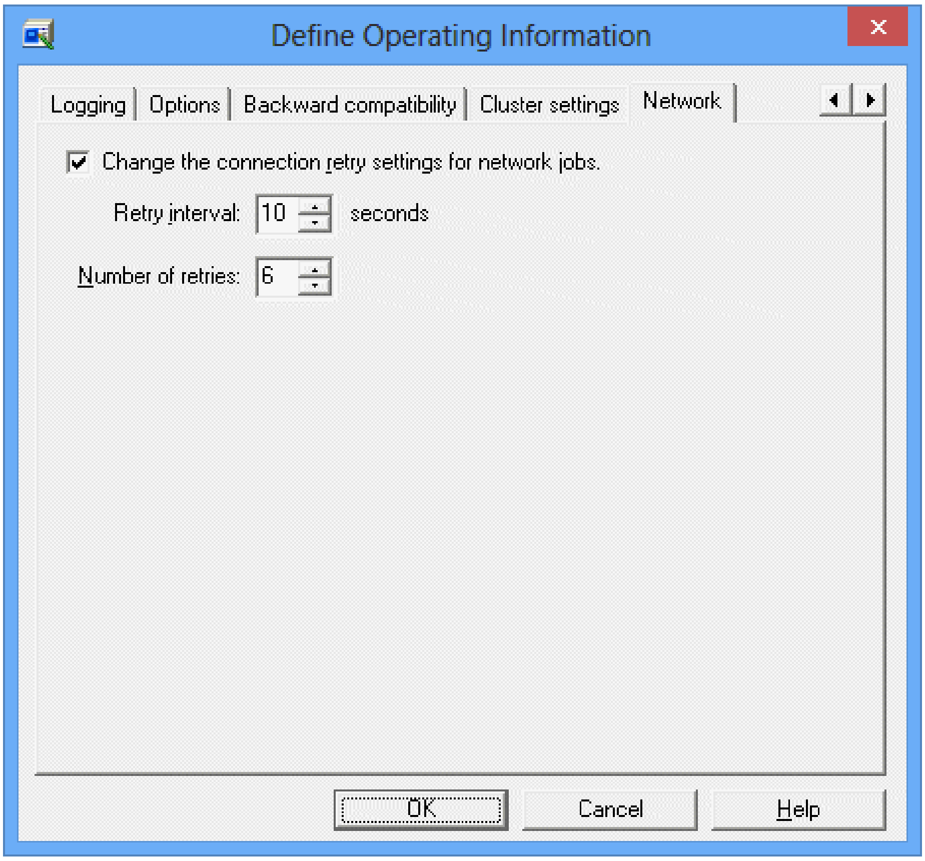
Specifies a node name of the active (or currently operating) schedule server which configures the cluster system.

Standby1/Standby2/Standby3:

Specifies a node name of the standby schedule server which configures the cluster system. You can specify standby2 and 3 if they exist.

If multiple standby systems exist, you must specify the active system first and specify the standby systems according to their failover priority. If the standby systems are NOT specified according to their priority, more time may be required for network job execution.

Network sheet in the Define Operating Information window



☑ Change the connection retry settings for network jobs.

Retry interval: 10 seconds

Number of retries: 6

Change the connection retry settings for network jobs:

When this checkbox is checked, **Retry interval** and **Number of retries** can be set for the retry operation.

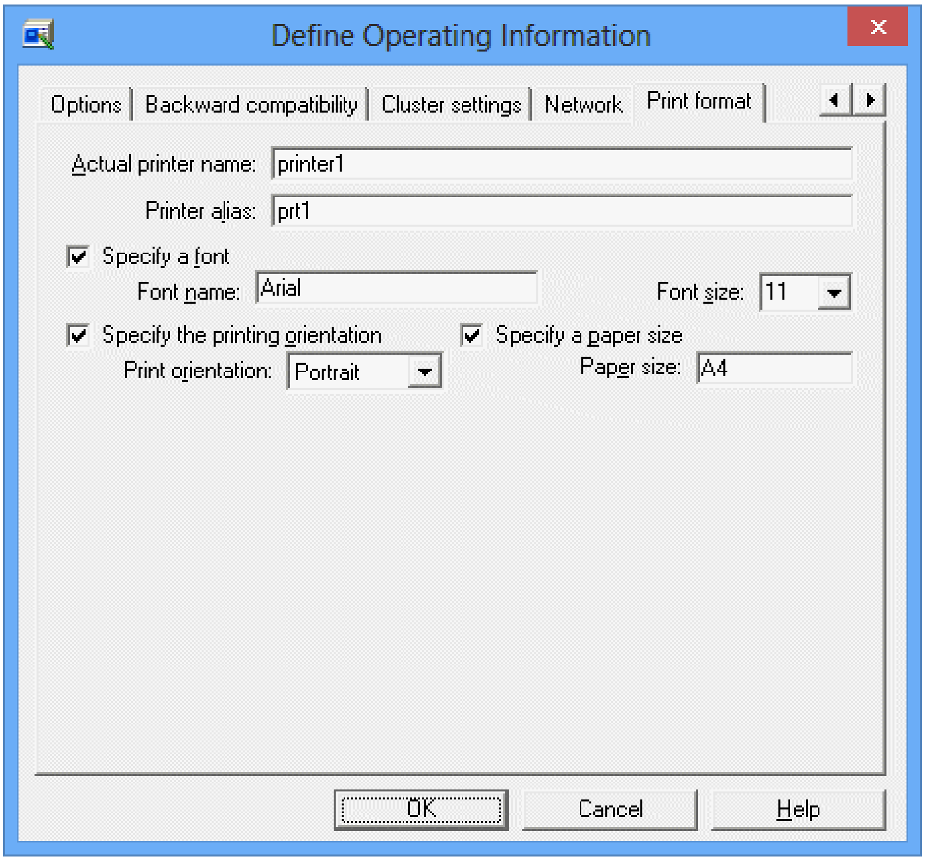
Retry interval:

Set the interval between retries in the range from 0 to 600 (seconds). The default is 10 (seconds).

Number of retries:

Set the number of retries in the range from 0 to 20 (times). The default is 6 (times).

Print format sheet in the Define Operating Information window [Windows]



Actual printer name: printer1

Printer alias: prt1

☑ Specify a font

Font name: Arial

Font size: 11

☑ Specify the printing orientation

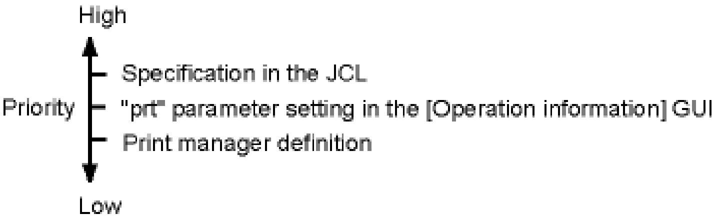
Print orientation: Portrait

☑ Specify a paper size

Paper size: A4

You can use the **Print format** sheet for the Batch Output function of JCL job execution results. This sheet is displayed if you have selected the **Enable prt parameter** option on the **Options** sheet.

If you use the Batch Output function of JCL job results, the attributes for print formats are used in the following priority.



Therefore, you can omit the print attribute setup of JCL jobs if you have defined the attributes here.

For the JCL details, refer to the *Systemwalker Operation Manager Reference Guide*.

Actual printer name:

Specifies the actual name of the printer to be controlled by Printer Manager, using up to 32 alphanumeric bytes. The printer alias CANNOT contain a space, an ampersand (&), and left and right parentheses.

Printer alias:

Specifies an alias of the printer. You can specify any printer name consisting of up to 32 alphanumeric bytes. The printer alias CANNOT contain a space, an ampersand (&), and left and right parentheses.

In addition to the actual printer name, you can specify the printer alias you have defined here in the "prt" operand of JCL file control statement.

Specify a font:

Specifies the default font name of the current printer. You can enter a font name in the **Font name** field, and select a font size in the **Font Size** field. If omitted, the definitions of the Print Manager are used.

Specify the printing orientation:

Specifies a printing direction or a print orientation of the printer. You can select the horizontal or vertical print orientation in the **Print orientation** field. The definition of Print Manager is always used for a continuous feed printer.

Specify a paper size:

Specifies the default paper size for the specified printer.

The definitions of Print Manager are always used for a continuous feed printer.

2.8.2 Defining a Trust Host

This section explains how to define a trust host.

If you have changed the operating information definition, you must restart Job Execution Control services or daemons to make your change valid.

Outline

Job Execution Control allows you to submit jobs to other servers connected via the network. In defining trust hosts, you will specify whether or not your own server should accept requests for job execution when requested by another server. This definition enables the server to block network jobs and distributed execution job from unwanted servers.

If the system is installed first, any job submitted by any server is accepted. If you want to limit the acceptance of network jobs from other servers, define the host names of servers from which requests are permitted using the **Define Trust Host** window. Network jobs and distributed execution job from servers that are not defined here will not be accepted.

Moreover, for servers from which acceptance is permitted, jobs can only be denied if the job submitter belongs to the Administrators group or is a superuser.

If a job execution is requested by another server using the previous load distribution function of the Windows server, the trust host definition is ignored.

Definition procedure

1. Display the **Define Trust Host** window.

   Click **Trust Host** in the **Systemwalker Operation Manager Environment Setup** window, and the **Define Trust Host** window will appear.

2. Specify the servers to accept network jobs and distributed execution jobs.

   Specify the servers which accept jobs from other hosts in the **Define Trust Host** window.

   To allow only the job submission from the registered hosts, click **Add** or **Edit**. When the **Add/Edit Trust Hosts** window appears, add or change the hosts in it.

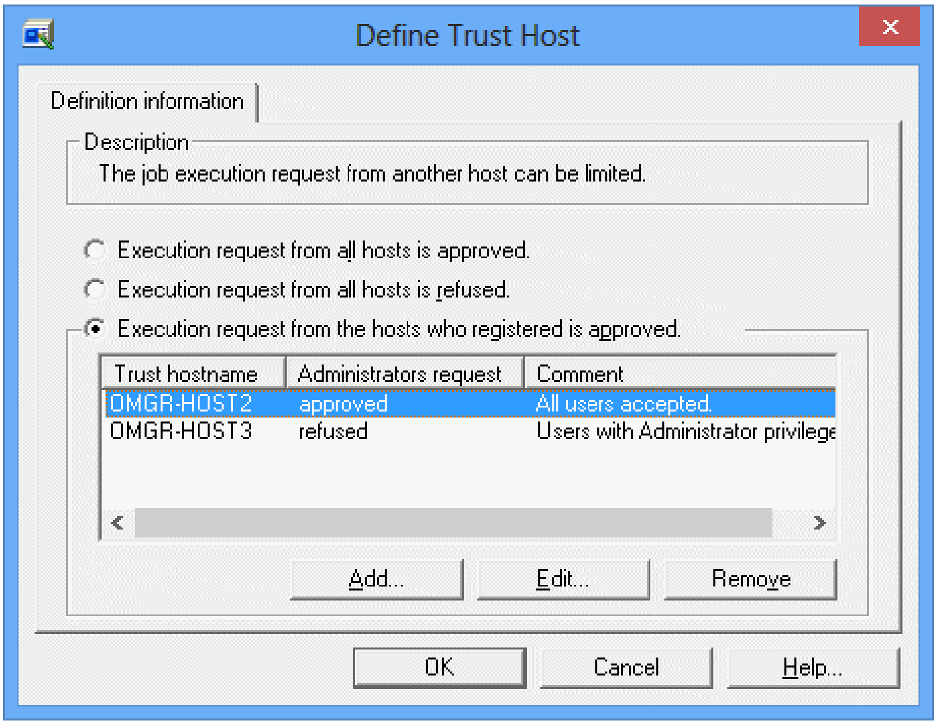
3. Save your settings.

   Click **OK** to save your settings.

4. Apply your settings.

   The definition you have changed is made valid when Job Execution Control services or daemons are started next time.

Define Trust Host window



Description
The job execution request from another host can be limited.

○ Execution request from all hosts is approved.
○ Execution request from all hosts is refused.
● Execution request from the hosts who registered is approved.

Trust hostname	Administrators request	Comment
OMGR-HOST2	approved	All users accepted.
OMGR-HOST3	refused	Users with Administrator privilege

Execution request from all hosts is approved:

Allows a job submission from any host.

Execution request from all hosts is refused:

Rejects a job submission from any host.

Execution request from the hosts who registered is approved:

Allows a job submission from registered hosts only. The registered hosts are listed.

Trust host name:

Sets the trust host name.

Administrators request:

approved: Permits acceptance of a job submitted by all users.

refused: Rejects acceptance of a job submitted by the user having the administrator privileges.

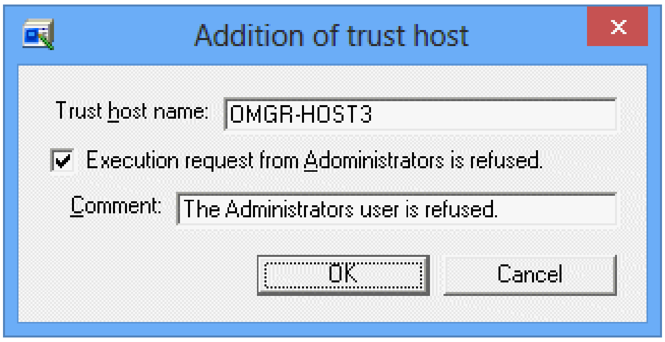
Comment:

Sets a comment.

When you click **Add** or **Edit**, the **Add/Edit Trust Host** window appears. You can add a host or change an existing host in this window.

You can delete a registered host by selecting it from the list and by clicking **Remove**.

Addition/Edit of trust host window



Addition of trust host

Trust host name: OMGR-HOST3

☑ Execution request from Administrators is refused.

Comment: The Administrators user is refused.

Trust host name:

Specifies a trust host name, using up to 64 bytes.

On the server that needs to be permitted to accept jobs, specify the host name displayed by the following command.

[Windows]: *hostname* command

[UNIX]: *uname -n* command

An IP address cannot be specified. Also, the trust host name CANNOT begin with symbol "#".

However, you can specify the same logical IP address as the schedule server's logical IP address for the trust host name if it has been specified in **Systemwalker Operation Manager Environment Setup** window >> **Define Operating Information** window >> **Cluster settings** sheet >> **Schedule server settings** field.

Execution request from Administrators is refused:

If checked, the system rejects network jobs submitted by the user having administrator privileges.

Comment:

Specifies a comment, using up to 128 bytes. The comment CANNOT begin with the "noroot" character string in both uppercase and lowercase letters.

If you directly edit the trusted host definition file

Any change in the **Define Trust Host** window is stored in the Trust Host Definition file. You can directly edit this file using an editor such as "vi" or Notepad.

For the trusted host definition file, see "B.2 Trusted Host Definition File".

2.8.3 Defining the Job Owner Information [Windows]

This section explains how to define the job owner information.

Outline

You must define the job owner information if you have selected the **Execute job under the respective job owner's authority** option on the **Options** sheet of the **Define Operating Information** window.

When using Systemwalker Operation Manager, a user having job owner privileges can execute jobs if his or her password has been set as the job owner information.

If **Execute jobs under the respective job owner's authority** has been specified, all jobs and job nets requested from users whose **Status** is "Undefined" in the **Define Job Owner's Information** window will terminate abnormally.

The user ID and password of the applicable user must be defined in this window, in the same way as when a specific user wants to execute a job (if the execution user has been specified by **Executive user name** on the **Detail information** sheet of **Add/Change - Job** window).

Definition procedure

The following explains the procedure for defining job owner information for scheduled jobs and on-demand jobs.

Definition procedure for scheduled job owners

If a project was defined using the standard procedure, the job owner information can be defined by specifying the owner and the owner password in the **New Project** window.

However, if **Execute jobs under the respective job owner's authority** is enabled in the **Options** sheet of the **Define Operating Information** window after the project is defined, use the following procedure to define the job owner information:

1. Display the **Define Job Owner Information** window.

   Display this window by using one of the following methods:

   - Open the **Define Operating Information** window and the **Options** sheet. Select **Execute jobs under the respective job owner's authority** to enable the **Set Job Owner** button, and then click it.

   - Click **Job owner** in the **Systemwalker Operation Manager Environment Setup** window.

   Ensure that the registered project owner is displayed in the **User ID** column.

2. Set a password in the **Define Password Information** dialog box.

   Select the target user in the **Define Job Owner's Information** window, and then select **Define** from the **User** menu. The displayed **Define Password Information** dialog box appears. Enter password information.

   If the entry is properly authenticated, the "Defined" for the target user will be displayed in the **Status** field of **Define Job Owner Information** window.

Note

- If there are multiple projects with the same owner in the **Define Job Owner's Information** window, and password information is defined to a project with "Undefined" password information, it will also be applied to all the other projects (that have "Undefined" password information). The status will be changed to "Defined" when the screen is refreshed.

  However, if the password information is changed for a project where the password information is already "Defined", only the definition for that project will be changed.

- To execute a job using the defined user ID, it is necessary to separately grant **Log on as a batch job** rights to each user ID. If using a network job, rights are required for both the job submitting server and server that receives the job. You can set the **Log on as a batch job** rights through **Control Panel** >> **Administrative Tools** >> **Local Security Policy**.

Definition procedure for on-demand job owners

1. Display the **Define Job Owner Information** window.

   Display this window using one of the following methods:

   - Open the **Define Operating Information** window and the **Options** sheet. Select **Execute jobs under the respective job owner's authority** to enable the **Set Job Owner** button, and then click it.

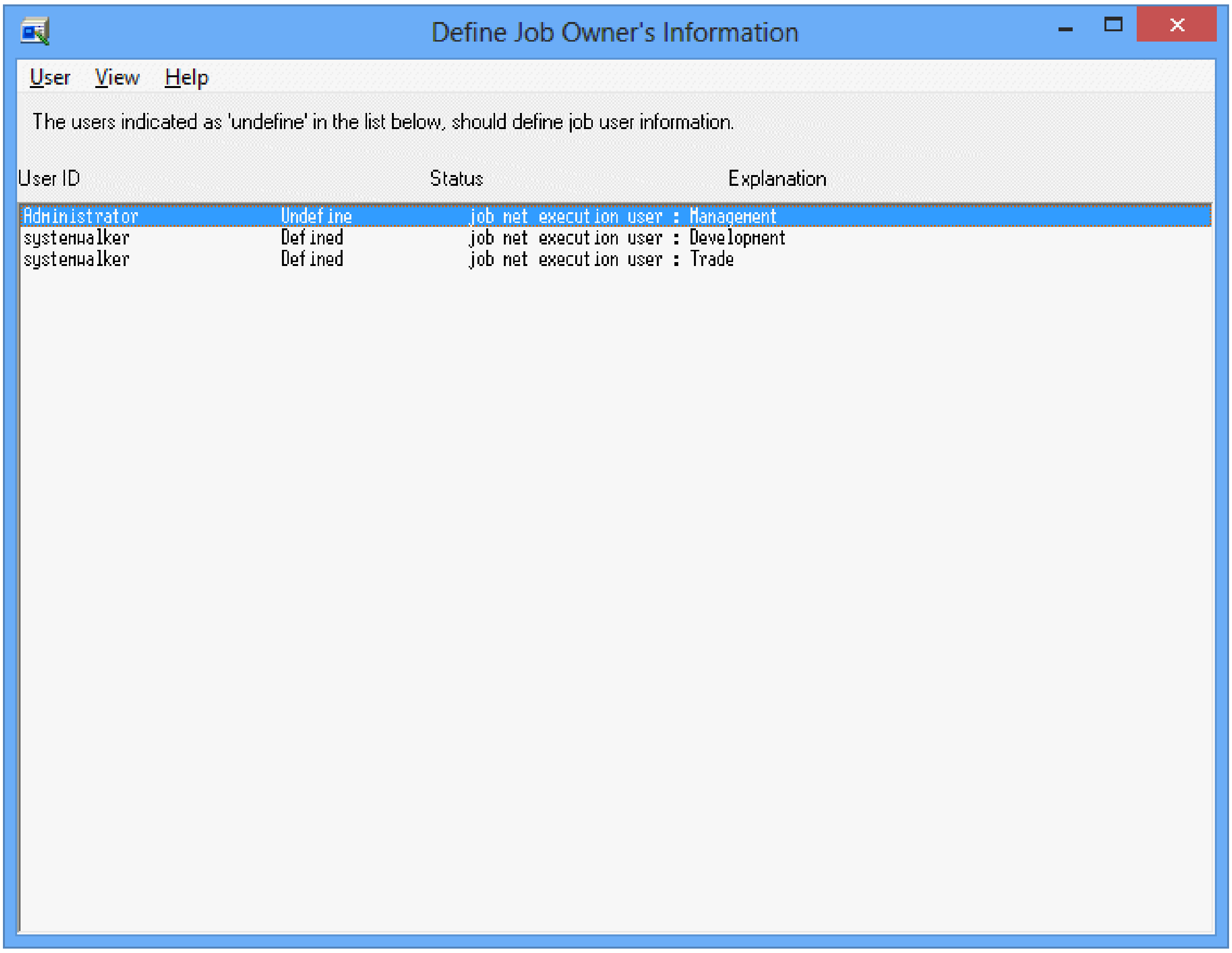
   - Click **Job owner** in the **Systemwalker Operation Manager Environment Setup** window.

2. Set up the job owner information in the **Define New User** dialog box.

   In the **Define Job Owner Information** window, select **New User** from the **User** menu. When the **Define New User** dialog box appears, enter the on-demand job owner information and click **OK**.

   If the entry is properly authenticated, the user information will be displayed in the **Define Job Owner Information** window.

Define the Job Owner's Information window



The users indicated as 'undefine' in the list below, should define job user information.

User ID	Status	Explanation
Administrator	Undefine	job net execution user : Management
systemwalker	Defined	job net execution user : Development
systemwalker	Defined	job net execution user : Trade

This window displays a list of the scheduled job owner names you have set in the project definition of Jobscheduler and on-demand job owner names you have registered in the **Define New User** dialog box. The following explains their meanings.

User ID:

This is the job owner name. User IDs that are displayed as "job net execution user" in the **Explanation** column are the owners of scheduled jobs. Other user IDs are the owners of on-demand jobs.

Status:

Indicates whether or not the password for the relevant user has been set.

Undefined:

No password has been registered.

Defined:

The password has been registered.

Explanation:

If the relevant user is a scheduled job owner, this column indicates which project owner this user is.

If the relevant user is an on-demand job owner, it displays one of the following depending on whether or not this user is a domain user.

If the user is a domain user:

The domain name is displayed.

If the user is not a domain user:

Nothing is displayed.

The sequence for displaying **User Names** in the **Define Job Owner Information** window can be selected from the following two types by selecting **Sort Users** from the **View** menu.

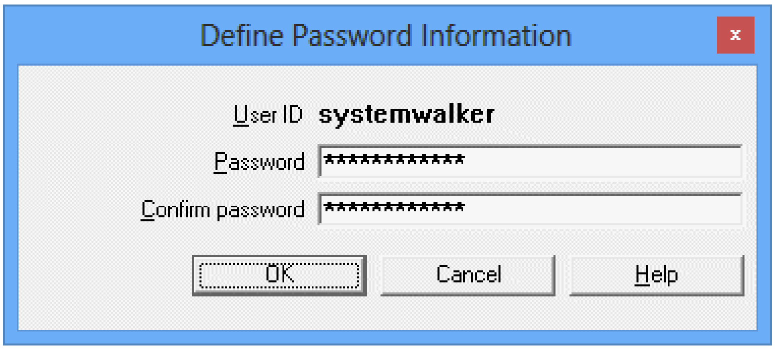
By User ID:

The user IDs are sorted and displayed in alphabetical order.

By Status:

The user names are sorted and displayed in the order from "Undefined" to "Defined" according to the display of the **Status** field.

Define Password Information dialog box



Define Password Information

User ID systemwalker

Password *************

Confirm password *************

Each column is described below.

User ID:

This field displays the target user ID.

Password:

Enter a password of the relevant user. This password should be same as the password that is used when logging onto the server. Entry characters are indicated by asterisks (*) indicating the number of characters you have entered.

Confirm password:

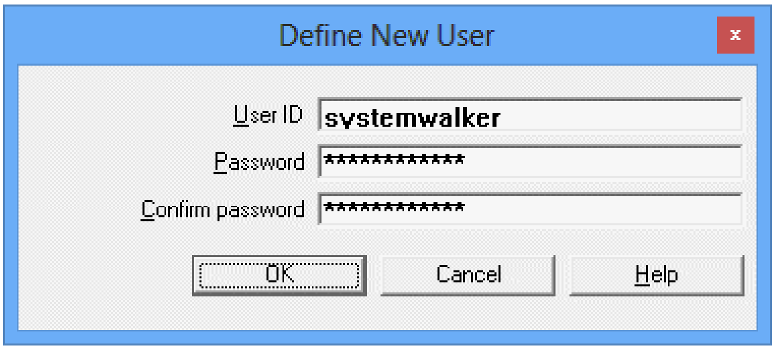
You must re-enter the password for confirmation. Entry characters are indicated by asterisks (*) indicating the number of characters you have entered.

OK button:

Press it to register the password.

The password is actually tested for authentication to confirm if the entered password is correct. If it is correct, the **Status** field of the relevant user is changed to the "Defined" in the **Define Job Owner's Information** window. If the specified password is incorrect, an error message is displayed, and the **Define Password Information** dialog box is displayed again.

Define New User dialog box



User ID:

Enter the user ID of the owner of the on-demand job. To specify a domain account, separate the NETBIOS domain name and the user ID with a backslash ("\").

Password:

Enter a password of the relevant user. Entry characters are indicated by asterisks (*) indicating the number of characters you have entered.

Confirm password:

You must re-enter the password for confirmation. Entry characters are indicated by asterisks (*) indicating the number of characters you have entered.

OK button:

Authentication will be performed on the user ID and password that have been entered. An error message will be displayed if the specified user ID and password are incorrect. If authentication is successful, the user will be registered and the status of the user will appear as "Defined" in the list in the **Define Job Owner's Information** window.

2.8.4 Defining the User Control List for Job Execution [UNIX]

To restrict job execution users, create a user control list for job execution using a text editor such as vi or Notepad.

Only users listed in the user control list for job execution can execute jobs. Job execution is restricted as shown in the following table when the user control list for job execution has been set up. User limit lists for job execution are not set up immediately after installation. User limit lists for job execution are created separately for each subsystem, and are only valid for the particular subsystem for which they have been created.

User control list for job execution exists?	User registered with the user control list for job execution?	Job execution
Exists	Registered	Can execute jobs (*1)
	Not registered	Cannot execute jobs (*2)
Does not exist	-	Can execute jobs

*1

Note that commands that require system administrator privileges cannot be executed as jobs unless the system administrator (root) is registered in the user control list for job execution.

*2

If a user that has been specified by the job privileges does not exist in the user control list for job execution, a submission error will occur when the job is submitted, and the job will not be executed.

Refer to "2.4.2.2 Job Execution Privileges" for details on job privileges.

Creation Procedure

Use the following procedure to create user limit lists for job execution.

Only the system administrators can create the user limit list for job execution.

EE

If multiple subsystem operations are being performed, create a separate user control list for job execution for each subsystem.

1. Create a user control list for job execution

   Use an editor such as vi or Notepad to enter the names of users that will be allowed to execute jobs in a user control list for job execution.

2. Save the user control list for job execution

   Use the following file name to save the user control list for job execution that has been created:

   ```
   mjexuser
   ```

3. Restart Job Execution Control

   Job Execution Control must be restarted to enable these settings. Restart the Job Execution Control daemon.

Refer to "User Limit Lists for Job Execution" for details on how to specify user limit lists for job execution, file storage locations, and other notes.

Once these settings have been enabled, the users that are allowed to execute jobs can be changed simply by changing the content of the user control list for job execution.

To disable a user control list for job execution, delete the user control list for job execution and then restart the Job Execution Control daemon.

Information

- Backing up and restoring user limit lists for job execution

  User limit lists for job execution can be backed up and restored using the mpbko command and the mprso command respectively.

  Refer to "Chapter 3 Backing Up or Restoring Operation Environment" for details on the backup and restoration procedures.

- Extracting and distributing policy information

  The user information in user limit lists for job execution can be extracted and distributed as policy information. Policy information can be extracted and distributed by selecting **Operation information** from the **Environment definition** tab of the **Extract Policy** window.

  Refer to "2.13.1 Extracting the Policy Data" and "2.13.2 Distributing the Policy Data" for details on the procedures for extracting and distributing policy information.

- Network jobs

  For network jobs, execution users can be restricted by creating a user control list for job execution on either the schedule server or the execution server.The relationship with older versions is as follows:

  - If a network job request is sent to V13.1.0 or earlier:

    Create a user control list for job execution on the schedule server.

  - If network jobs are received from V13.1.0 or earlier:

    Create a user control list for job execution on the execution server.

2.8.5 Defining an Execution Subsystem Name

Defining an execution subsystem name in advance is useful so that it can be used later as the execution server name for network jobs.

Define the host name and subsystem number that make up the execution subsystem name. The execution subsystem name that you specify for a network job will be replaced with the defined host name and subsystem number before the job is submitted.

Define an execution subsystem name in the following situations:

- To give a meaningful name to a combination of host name and subsystem number, thereby facilitating the specification of the subsystem that will execute the network job
- To avoid having to change **Default host name** (registered in a job net) and **Request host** (registered in a job) when the execution server name is changed due to a system migration

Definition procedure

Perform the following procedure to define the execution subsystem name in the job submitting server (schedule server). If the job submitting server is running multi-subsystem operation, create an execution subsystem name for each subsystem.

Only the system administrator can define an execution subsystem name.

1. Ensure that no active job has the execution subsystem name to be edited.

   If one exists, wait for it to complete or forcibly terminate it.

2. Edit the execution subsystem name definition file.

   Using an editor such as vi or Notepad, specify the execution subsystem name, host name, and subsystem number.

3. Restart Job Execution Control.

   Restart the Job Execution Control service/daemon so that the settings take effect.

Refer to the *Systemwalker Operation Manager Reference Guide* for information on how to define the execution subsystem name definition file, the storage location of the file, and notes.

Information

- Backup and restore

  Execution subsystem name definition files are subject to backup and restore.

  Refer to "Chapter 3 Backing Up or Restoring Operation Environment" for details.

- Policy data extraction and distribution

  Execution subsystem name definition files are subject to policy data extraction and distribution. You can extract and distribute policy data by clicking **Extract Policy** >> **Environment definition**, and selecting **Operation information**.

  Refer to "2.13.1 Extracting the Policy Data" and "2.13.2 Distributing the Policy Data" for details.

2.9 Definition of Event Monitoring [Windows]

This section explains the environment definitions that are needed to use the Event Monitoring function.

2.9.1 Defining an Event Monitoring Environment

This section explains how to define an event monitoring environment.

Outline

The definition to use the Log File Monitoring function is explained first. This function considers addition of a text to the monitored log file as an event occurrence. To use the Log File Monitoring, you must define the log files to be monitored in advance. When you select **Log File Monitoring** as a monitored event, you can monitor abnormal events by logging them in independent text log files, even for products that do not output an event log.

Use the **Monitored Log File Setup** dialog box to define the monitored log files. You can monitor up to 20 log files.

Note

If you are using Systemwalker Operation Manager V5.0 or later together with Systemwalker Centric Manager, you CANNOT use the **Monitored Log File Setup** dialog box. In such system, you must use the similar dialog box provided by the **Monitor** window of Systemwalker Centric Manager.

Definition procedure

1. Open the **Define Event Monitoring Conditions** window.

   To do this, click **Define Event Monitoring Conditions** on the **Options** menu of the **Systemwalker Operation Manager** window.

2. Open the **Monitored Log File Setup** dialog box.

   To do so, click **Monitored Log File Setup** on the **Environment Setup** menu of **Define Event Monitoring Conditions** window.

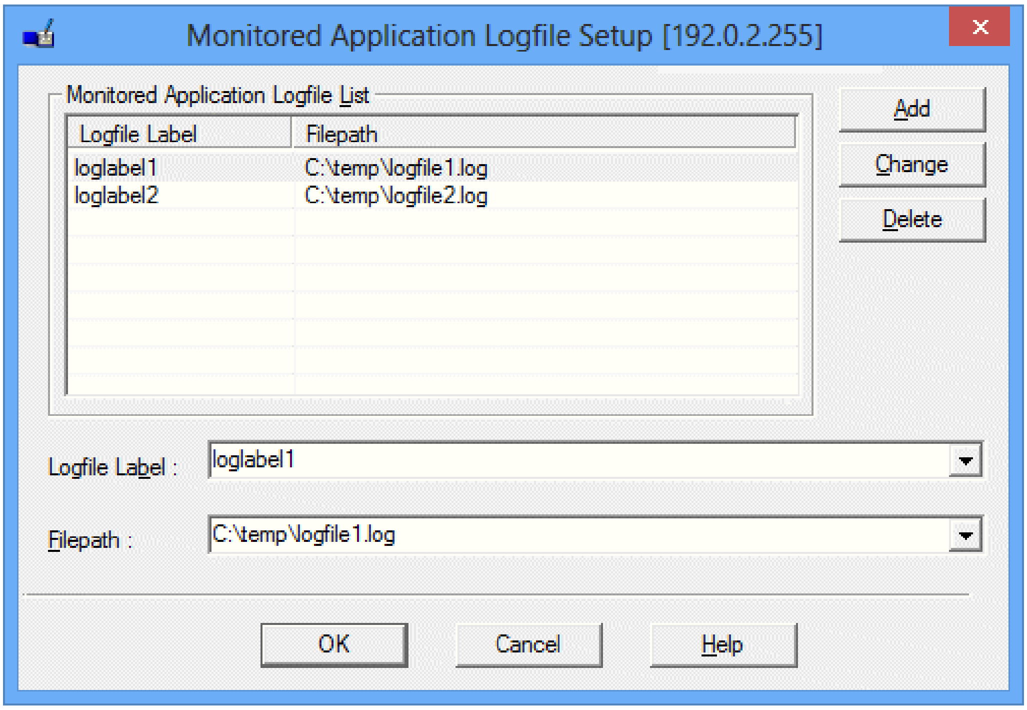
3. Define the monitored log files.

   Use the **Monitored Log File Setup** dialog box to define log files to be monitored.

4. Save your definitions.

   Click **OK** to save your settings.

Monitored Application Logfile Setup dialog box



Monitored Application Logfile Setup [192.0.2.255]

Monitored Application Logfile List

Logfile Label	Filepath
loglabel1	C:\temp\logfile1.log
loglabel2	C:\temp\logfile2.log

Logfile Label : loglabel1

Filepath : C:\temp\logfile1.log

Monitored Application Logfile List:

This list contains the monitored log files already registered.

When you select a log file from the **List of Registered Monitored Log Files**, the selected log data is shown in the **Logfile Label** and **Filepath** fields.

Logfile Label:

You can set a label of the file to be monitored, using up to 256 characters. It must be a unique name to identify the monitored file. The label CANNOT contain the following symbols.

( ) [ ] ^ $ * + \ ? . | "

Also, DO NOT use the following character strings as the message monitoring (filtering) may fail.

- INFO
- Information
- WARNING
- Warning
- ERROR
- Error
- HALT
- Stop
- Information
- Warning
- Error
- Stop

Filepath:

You can specify a name of log file to be monitored, using up to 259 characters. The log file name must be unique on the list.

Do not specify any file that is opened in an exclusive mode by other applications. If you specify such a file, applications or Systemwalker Operation Manager will fail to open the file and as a result they may not run normally. Check the application documentation to see if it opens log files in exclusive mode.

Add button:

Adds your definition to the selected item of the **List of Registered Monitored Log Files**.

Change button:

Applies your change to the selected item of the **List of Registered Monitored Log Files**.

Delete button:

Deletes an item you have selected from the **List of Registered Monitored Log Files**.

2.9.2 Defining an Action Execution Environment

This section explains how to define an action execution environment.

Outline

The Event Monitoring function allows you to automatically carry out actions such as "sending a Short Mail to the system administrator" and "starting an application to handle the event occurred" when an event such as an "output of message indicating the system failure" has occurred. You must set up the environment in advance in order to automatically initiate actions when an event occurs. The following are the actions for which the environments need to be set up and the dialog boxes to use for these environment settings.

- E-mail transmission

  Mail sheet of Action Environment Setup dialog box

- Short Mail notification

  Short Mail sheet in the Action Environment Setup dialog box

  COM Port sheet in the Action Environment Setup dialog box

Definition procedure

1. Open the **Define Event Monitoring Conditions** window.

   To do so, click **Define Event Monitoring Conditions** on the **Options** menu of the **Systemwalker Operation Manager** window.

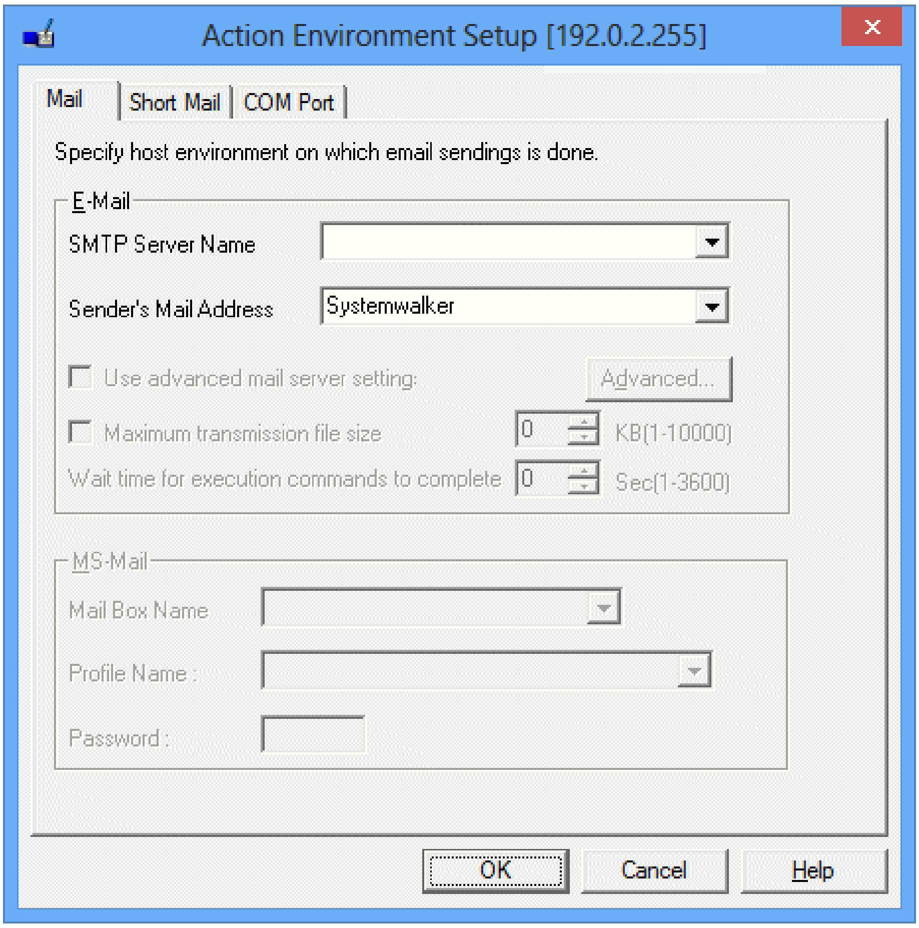
2. Open the **Action Environment Setup** dialog box.

   To do so, click **Action Environment Setup** on the **Environment Setup** menu of the **Define Event Monitoring Conditions** window. Or, click **Action** in the **Systemwalker Operation Manager Environment Setup** window.

3. Set up an environment.

   Define the environment by selecting each sheet of the **Action Environment Setup** dialog box that is displayed.

Mail sheet of Action Environment Setup dialog box



Specify host environment on which email sendings is done.

E-Mail

SMTP Server Name:

Sender's Mail Address: Systemwalker

□ Use advanced mail server setting

□ Maximum transmission file size: 0 KB(1-10000)

Wait time for execution commands to complete: 0 Sec(1-3600)

MS-Mail

Mail Box Name:

Profile Name :

Password :

E-Mail:

Define the following items for E-mail transmission.

SMTP Server Name:

Specifies an E-mail transmission server name, using up to 256 characters.

Sender's Mail Address:

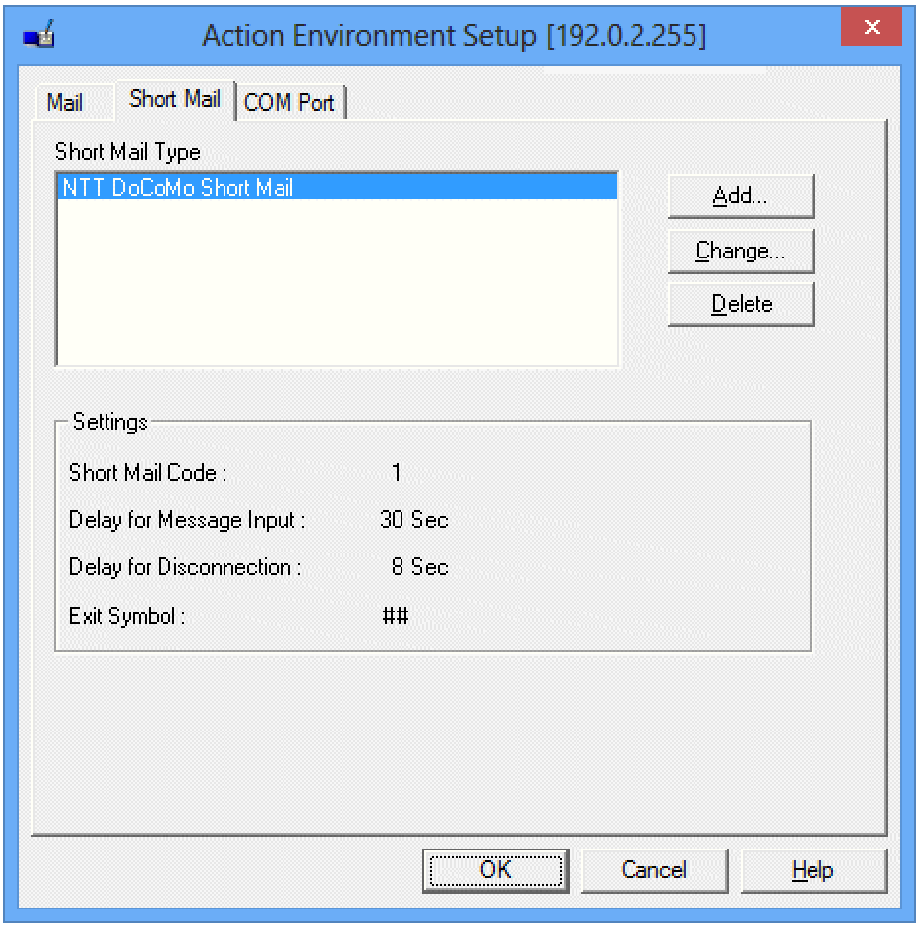
Specifies a default source name, using up to 256 characters.

Note

E-Mail transmission

- No dialup connection to the SMTP server is supported.
- Systemwalker Operation Manager does not support SMTP and POP authentication such as "POP before SMTP" and "SMTP-AUTH". For E-Mail transmission, use an SMTP server which does not require such the authentication.
- Emails cannot be sent if the address format specified in the **Sender's Mail Address** field of the **Mail** sheet of the **Action Environment Setup** dialog box does not match the address formats permitted by the SMTP server. The permitted address formats and character strings vary depending on the security setting of the SMTP server. For the permitted formats, consult the administrator of the SMTP server.
- When transmitting an E-mail outside the company while the current operation requires the outgoing transmission privilege, specify a mail address with this privilege in **Sender's Mail Address**.
- A string containing multi-byte characters cannot be specified as the transmission file name of E-mail transmission.

Short Mail sheet in the Action Environment Setup dialog box



Action Environment Setup [192.0.2.255]

Short Mail Type

NTT DoCoMo Short Mail

Settings

Short Mail Code : 1

Delay for Message Input : 30 Sec

Delay for Disconnection : 8 Sec

Exit Symbol : ##

Short Mail Type:

Registered Short Mail types are listed.

Add button:

Adds a Short Mail type. When you click **Add**, the **Add Short Mail Types** dialog box appears.

You can register up to 20 Short Mail types.

Change button:

Changes the transmission environment of the Short Mail you have selected in the **Short Mail Type** field. When you click **Change**, the **Change Short Mail Types** dialog box appears.

Delete button:

Deletes the Short Mail you have selected from the **Short Mail type** field from the list.

Settings:

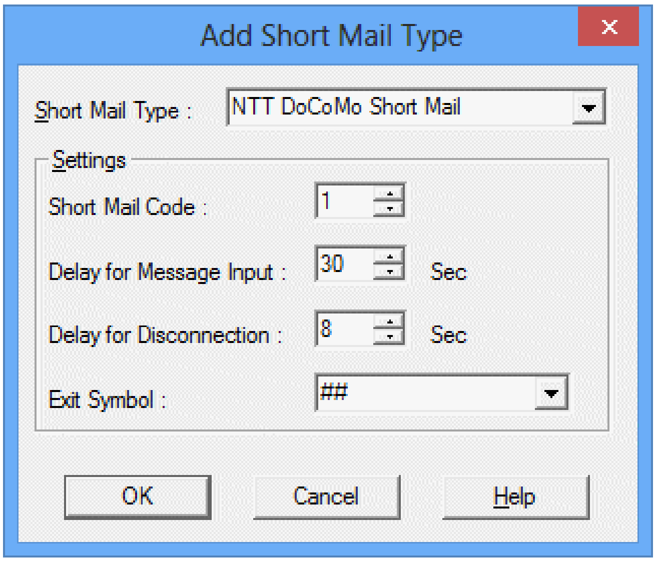
Details the transmission environment definitions you have set in the **Add Short Mail Type** or **Change Short Mail Types** dialog box.

Note

Modem setup for using a Short Mail

To use a Short Mail, you must prepare a modem on the server for executing Short Mail actions. To use the modem, define the COM port on the **COM Port** sheet of the **Action Environment Setup** dialog box.

Add Short Mail Type dialog box



Add Short Mail Type

Short Mail Type : NTT DoCoMo Short Mail

Settings

Short Mail Code : 1

Delay for Message Input : 30 Sec

Delay for Disconnection : 8 Sec

Exit Symbol : ##

Short Mail Type:

Specifies a name to identify the Short Mail service company to be accessed for actions.

To use a new Short Mail to execute its actions, you must prepare the code conversion DLL (an exit of message conversion for unsupported Short Mail) in advance. For its details, refer to the *Systemwalker Operation Manager Reference Guide*.

Settings:

Define the following.

Short Mail Code:

Specifies a Short Mail service company ID code, using an integer of 1 to 20. You cannot specify an already used code.

Delay for Message Input:

Message input becomes possible after a connection has been established with the Short Mail company of the other party and the audio instructions have finished playing. This setting specifies the time between when dialing completes and when message input becomes possible. Specify a value no more than 300 (seconds). The default setting is 30 seconds. Try calling once to measure the time interval until message entry is enabled. This time is reduced if no voice guidance is used.

If the time specified in the Time interval until message entry is incorrect, sent messages may have garbled characters or may not be sent at all.

Delay for Disconnection:

When you end your message by entering an end signal (symbols "##"), you hear the Short Mail service audio instruction confirming the end of your message entry.

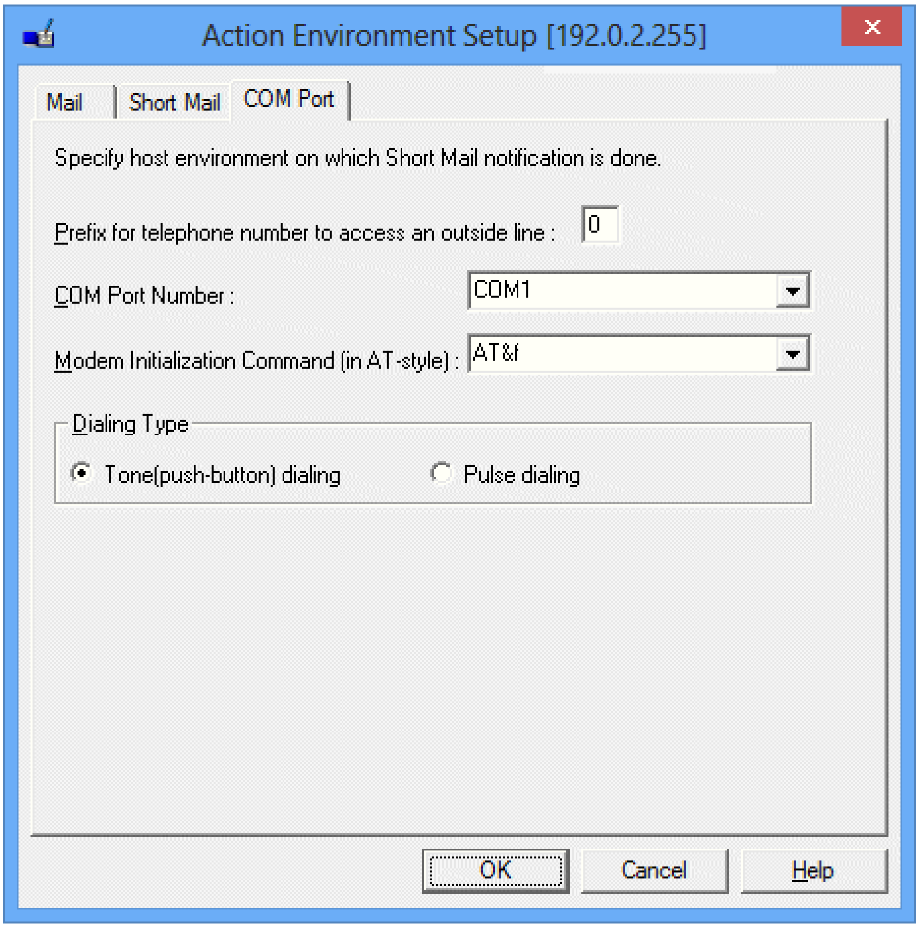
Enter a time interval within 300 seconds until the line is cut.

The default setting is 8 seconds.

Exit Symbol:

To end message entry from your Short Mail enter an end signal such as "##" after the ordinary numbers you have entered.

COM Port sheet in the Action Environment Setup dialog box



Action Environment Setup [192.0.2.255]

Specify host environment on which Short Mail notification is done.

Prefix for telephone number to access an outside line : 0

COM Port Number : COM1

Modem Initialization Command (in AT-style) : AT&f

Dialing Type

● Tone(push-button) dialing ○ Pulse dialing

Prefix for telephone number to access an outside line:

When your company has a telephone system with internal extensions, enter the number you must dial to get an outside line. Leave the field blank if you do not have to dial a number to get an outside line.

The default setting is 0.

COM Port Number:

Enter the port number to which the modem is connected. You can select COM1 through COM4, or enter another number. You can add only one number. The default is "COM1."

Power control devices also use COM ports. Be careful not to cause COM port conflicts when you are also controlling the power on a machine.

Modem Initialization Command (in AT-style):

Sets the modem initialization command. The default setting is "AT&f".

See your modem manual for details about the modem initialization command.

Dialing Type:

Specifies a telephone line type.

The default is **Tone(push-button) dialing**.

Tone(push-button) dialing:

Selects tone dialing.

Pulse dialing:

Selects pulse dialing.

Note

Modem setup for using a Short Mail

To use a Short Mail you need a modem. An external modem can normally be connected to either the COM1 or COM2 port. However, power control devices and SNMP adapters may also use COM ports. Therefore, you must set up the COM ports so that the COM port numbers and their interrupts (IRQs) will not conflict. Also, some power control hardware requires the use of COM1. When you use both power control and a modem, connect an RS-232C cable to COM1 for power control and connect the modem to COM2.

If the modem is connected to the telephone extensions

The modem may not detect a dial tone during dialing due to the limited specifications of telephone extension exchange system. If it has occurred, the following message is shown in the event log and the messaging to the Short Mail is failed. If this message is displayed, you must set the command (an example of "AT&fX3") in the **Modem Initialization AT Command** field to start dialing without waiting for the dial tone detection. See your modem manual for the detailed command setup.

Source name: MpAosfB

```
4109: No dial tone can be detected from the telephone line.
```

2.10 Definition of Task Link

This section explains how to define the operating environment for Task Link.

Note

Windows

When connections are achieved using a UNC format specification, file control using Windows directory sharing (Windows sharing) is performed. For this reason, when simultaneously connecting to the same server from the Task Link command or other applications (such as Explorer), the same user's credentials (user name and password) must be used. Note that a connection error will occur if different user's credentials are used.

2.10.1 Defining a Password Management Book

Task Link enables the extraction of user passwords required for operation from the password management book. Accordingly, you must define the user name and password in the password management book in advance.

A password management book manages sets of user names and passwords under the same login definition name as a file. Prepare a log for each server that uses the job linking function.

A login definition name is a name under which the password management book is managed, and a group name that has been registered in the system is used as a login definition name.

Define a password management book using the password management command on a server that executes the job linking command. For the definition details, refer to the *Systemwalker Operation Manager Reference Guide*.

Only the users listed below are allowed to manage the password management files.

- Users that belong to the "Administrators/root" group
- Users that belong to the groups identified by the login definition name

The extension ".ini" is added to a login definition name, and a password management file is stored in the following directory.

[Windows]

```
Systemwalker Operation Manager installation directory\MpWalker.JM
\mpnjsosv\manage
```

[UNIX]

Solaris	/opt/FJSVsnjss/manage
HP-UX version	/opt/FHPsnjss/manage
AIX version	/opt/FAIXsnjss/manage
Linux version	/opt/FJSVsnjss/manage

Note

For the user registered in the password management book for Task Link, the user's password that has been set in the password management book must also be updated when the password is due to expire and needs changing.

2.10.2 Definition for Task Link with Clients

To enable Task Link with a client, you must first register the Client Task Link in the startup program on the client.

Definition procedure

1. Displaying the storage folder for the Client Task Link execution file

   Start Explorer and open the following folder in advance.

   ```
   Systemwalker Operation Manager installation directory
   \MpWalker.JM\mpnjsocl\
   ```

2. Displaying the startup folder

   Start Explorer and open the folder below. (Configure the settings to display hidden files and folders.)

   ```
   C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
   \Startup
   ```

   <*user name*> is the name of the operating system login user.

3. Registering to the startup program

   Drag and drop "CNSCLENG.EXE" in the folder of 1 to the folder of 2. When dropping it, release the left button on the mouse while pressing the CTRL and Shift keys. (*Note)

   Note) At this time, release the left button on the mouse with the small arrow icon displayed. This icon indicates to create a shortcut icon.

4. Confirming that Client Task Link has been registered

   Confirm that a shortcut file "Shortcut to CNSCLENG.EXE" has been created in the folder of 2.

Startup and shutdown of Client Task Link

Client Task Link must be active on the client that you want to link. To do so, start up the Client Task Link in one of the following ways.

- Startup by registration in the startup program
- Manual startup by the user that has logged in to the client

  Select Start or Apps >> Systemwalker Operation Manager >> Task Link clients.

Client Task Link always resides as it is shown by its icon. Shut it down by using one of the following ways.

- Shutdown from the menu

  When you left-click this icon, the menu appears. Select Close from the menu.
- Logging out from the console
- System shutdown

2.10.3 Defining the Host Information

You can create a host information definition file and turn on the client power using the Task Link function. This file defines the clients to be turned on, and it can specify the information about multiple hosts.

You must create a host information definition file having the "hostinfo.ini" name and store it in the following directory.

[Windows]

```
Systemwalker Operation Manager installation directory\MpWalker.JM
\mpnjsosv\manage
```

[UNIX]

Solaris	/opt/FJSVsnjss/manage
HP-UX version	/opt/FHPsnjss/manage
AIX version	/opt/FAIXsnjss/manage
Linux version	/opt/FJSVsnjss/manage

You can directly edit this file using an editor such as "vi" or Notepad. The following gives the syntax rules.

Coding format

For IPv4 communications

```
[HostName]
MACAddress=mac_address
IPAddress=ip_address
SubnetMask=subnet_mask
```

For IPv6 communications

```
[HostName]
MACAddress=mac_address
IPAddress=ip_address
```

* For IPv6 format, there is no need to specify SubnetMask.

Parameters

[HostName]

Specifies a host name of the client to be turned on.

This host name must be the same as the "HostName" you specify in the client power-on command. A pair of brackets ([ ]) are required.

MACAddress=*mac_address*

Specifies a MAC address of the client to be turned on.

The "mac_address" must be hexadecimal value sets such as "00-00-0E-9D-2C-38." This parameter is always required.

IPAddress=*ip_address*

Specifies an IP address of the client to be turned on. Specify the IP address in IPv4 or IPv6 format for the "ip_address".

This parameter may be omitted.

The IP address is first searched as the "HostName". If it cannot be resolved, the IP address specified here is used.

SubnetMask=*subnet_mask*

Specifies a subnet mask of the client to be turned on.

For IPv4 environment communications only, the "subnet_mask" must be decimal value sets such as "255.255.255.0." This parameter is always required.

Omit for IPv6 communications environments.

Sample Definition

Examples for IPv4:

```
[foo]
MACAddress=00-00-0E-9D-2C-38
IPAddress=192.0.2.0
SubnetMask=255.255.255.0
```

Examples for IPv6 format:

```
[foo]
MACAddress=00-00-0E-9D-2C-38
IPAddress=2001:0db8:0000:0000:0123:4567:89ab:cdef
```

Usage notes

The host information definition file is also used for policy data distribution as part of Jobscheduler information.

If the information is distributed to a server where SystemWalker/OperationMGRV4.0L20 or earlier Windows or V5.0 or earlier [UNIX] has been installed, the host information distribution file remains in the working directory of the destination server.

2.11 Definition of SSH Communication

Use SSH communication when using the mjrmtjob command to execute jobs on a remote machine. This section explains the required definitions for SSH communication.

You need a remote machine license to use the mjrmtjob command.

2.11.1 Configuring SSH Communication

The mjrmtjob command uses SSH communication. Perform the following before using the mjrmtjob command as a job:

1. Prepare an account for performing remote connection (login).

   #### Tasks on the Systemwalker Operation Manager server (SSH client) that will execute the mjrmtjob command

   Prepare an account for the user who will execute the mjrmtjob command. (This user is hereinafter referred to as USERA.)

   #### Tasks on the remote machine (SSH server)

   Prepare an account for <*user name*> to be specified in the mjrmtjob command. (This user is hereinafter referred to as USERB.)

2. Configure firewall settings.

   #### Tasks on the remote machine (SSH server)

   Set the port that will use SSH through the firewall.

   Port used for SSH:

   Default (not specified by the mjrmtjob command -P option): 22/TCP

   Specified by the mjrmtjob command -P option: Specified Port

3. Start the SSH service.

   #### Tasks on the remote machine (SSH server)

   Start the SSH service. If SSH has not been installed, install it. Refer to "Related Software" in the *Systemwalker Operation Manager Technical Guide* for information on the required SSH version.

   Refer to the relevant SSH manuals for information on how to install and start the service.

4. Configure login without a password.

   You must configure these settings both on the Systemwalker Operation Manager server (SSH client) that will execute the mjrmtjob command and on the remote machine (SSH server).

   If there are multiple accounts, configure them all in the same way.

   The following steps use /home/USERA and /home/USERB as the home directories of the accounts that you prepared in step 1.

   #### 1) Configure the Systemwalker Operation Manager server (SSH client) that will execute the mjrmtjob command.

   a. Execute the following to generate a public key:

      ```
      $ ssh-keygen -t rsa
      Generating public/private rsa key pair.
      Enter file in which to save the key (/home/USERA/.ssh/id_rsa):
      Enter passphrase (empty for no passphrase):
      Enter same passphrase again:
      Your identification has been saved in /home/USERA/.ssh/id_rsa.
      :
      :
      ```

      The following two files will be created in /home/USERA/.ssh/:

      - id_rsa (private key)
      - id_rsa.pub (public key)

   b. Set permissions for the /home/USERA/.ssh/ directory and the id_rsa file (private key) located in it.

      ```
      $ chmod 700 /home/USERA/.ssh
      $ chmod 600 /home/USERA/.ssh/id_rsa
      ```

c. Copy the id_rsa.pub file (public key) that was generated in step a to the remote machine (SSH server). The example below copies the file to /tmp on the remote machine. You can delete the id_rsa.pub file (public key) after you have deleted it.

```
$ scp /home/USERA/.ssh/id_rsa.pub USERB@<remote machine>:/tmp
```

Sytemwalker Operetion Manager server is Windows

a. Create public key.

The user (who execute mjrmtjob command) who create public key is as "USERA", execute as below if it is created under the d:\temp.

```
$ mjkeygen create -k d:\temp
```

The following file is created under the d:\temp.

```
USERA.mjeskey.pub(Public Key)
```

Note

The user who create public key (who execute mjrmtjob command)

In the job execution control, if the Execute jobs under the respective job owner's authority has not been specified, the user who execute mjrmtjob command is startup account of the "Systemwalker MpMjesuser" service.

If you need to change startup account, refer to the "D.1.1 Changing the Startup Account".

b. Transfer the USERA.mjeskey.pub (public key) created in a. to a remote machine (SSH server side), by ftp and so on.

You can delete USERA.mjeskey.pub (the public key) after the transfer.

In the following description, you transferred to/tmp on the remote machine.

2) Configure the remote machine (SSH server).

In Windows, perform the tasks below on the Cygwin Terminal started (installed) in step 3. The actual home directory exists under the cygwin installation folder.

a. If the .ssh directory does not exist in the /home/USERB home directory of the account, create it and set permissions.

```
$ mkdir /home/USERB/.ssh
$ chmod 700 /home/USERB/.ssh
```

b. Add id_rsa.pub (public key) that you copied in step c of "1) Configuring the Systemwalker Operation Manager server (SSH client) that will execute the mjrmtjob command" to the /home/USERB/.ssh/authorized_keys file. Set permissions when you first create the authorized_keys file. Then delete the /tmp/id_rsa.pub file.

```
$ cat /tmp/id_rsa.pub >> /home/USERB/.ssh/authorized_keys
$ chmod 600 /home/USERB/.ssh/authorized_keys
$ rm /tmp/id_rsa.pub
```

3) Check the connection from the Systemwalker Operation Manager server (SSH client) that will execute the mjrmtjob command to the remote machine (SSH server).

Systemwalker Operation Manager server is Solaris/Linux

Check if you can connect (log in) from the Systemwalker Operation Manager server (SSH client) that will execute the mjrmtjob command to the remote machine (SSH server) without entering a password.

On the Systemwalker Operation Manager server (SSH client) that will execute the mjrmtjob command, execute the following as the user who will execute the mjrmtjob command:

```
$ ssh USERB@<remote machine>
```

Configuration is complete if you are not prompted for your password after you execute the above command.

If you are prompted for your password, there is an invalid setting. Review the settings.

Systemwalker Operation Manager server is Windows

Confirm that the mjrmtjob command can be executed. Note that if step 5 is required, confirm it after configuring the settings in step 5.

5. Set the environment variables.

   On the remote machine, set the environment variables that are required for executing commands or shell scripts. Refer to the relevant SSH manuals for details.

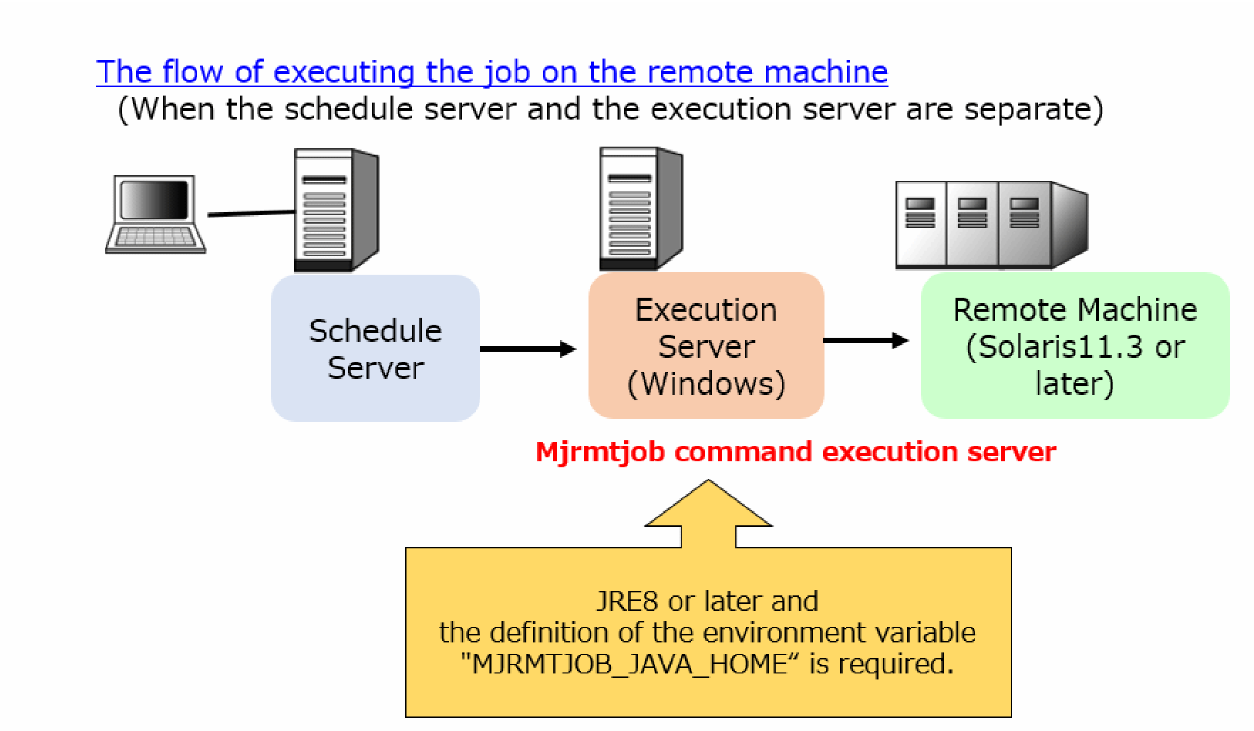
   If the operating system of the server that executes the mjrmtjob command is Windows and the operating system of the remote machine is Solaris 11.3 or later

   For the above combination, JRE8 or later is required for the Systemwalker Operation Manager server (Windows) that executes the mjrmtjob command. Install JRE8 or later and set the installation path to the environment variable "MJRMTJOB_JAVA_HOME".

   Configure the following settings for the Systemwalker Operation Manager server (Windows) that executes the mjrmtjob command in **System Properties** >> **Environment Variables** >> **System variables**.

   Variable: MJRMTJOB_JAVA_HOME

   Value: Installation path for JRE


The flow of executing the job on the remote machine
(When the schedule server and the execution server are separate)
Schedule Server
Execution Server (Windows)
Remote Machine (Solaris11.3 or later)
Mjrmtjob command execution server
JRE8 or later and
the definition of the environment variable
"MJRMTJOB_JAVA_HOME" is required.

2.11.2 Canceling the SSH Communication Configuration

The mjrmtjob command uses SSH communication. If you installed and configured SSH to use the mjrmtjob command with jobs but SSH communication is not required for any command other than mjrmtjob, use the following procedure to cancel the configuration:

1. Stop the SSH service.

2. Clear the port settings that are used for SSH communication through the firewall.

   Port used for SSH:

   Default (not specified by the mjrmtjob command -P option): 22/TCP

   Specified by the mjrmtjob command -P option: Specified Port

   ```
   Delete the private key that you created on the Systemwalker Operation Manager server
   (SSH client side) running the mjrmtjob command and the public key that you created on
   the remote machine (SSH server side). If the SSH client is Solaris/Linux, delete the
   id_rsa (public key). If the SSH client is Windows, delete the key pair with the
   mjkeygen command as follows.$ mjkeygen delete
   ```

   On the remote machine, remove the id _ rsa.pub (public key) or user name.mjeskey.pub (public key) information that you added to the authorized_keys file during setting.

3. If you added accounts for SSH communication, delete obsolete accounts.

4. Uninstall OpenSSH.

   If you installed OpenSSH and do not need it, uninstall it. If SSH has been installed as a standard operating system feature on Linux, you do not need to uninstall it.

2.12 Definitions for Monitoring the Execution Status of Job Nets by Linking to Systemwalker Centric Manager

This section explains the definitions for monitoring the execution status of job nets by linking to Systemwalker Centric Manager.

Note

To monitor the job net execution status, Systemwalker Centric Manager should be configured to be capable of monitoring the following messages. The monitored event type is "Batch Job".

[Windows]

- Systemwalker CentricMGR V10.0L20 or earlier

```
AP:jobschExit: ERROR: JOBNET has abnormal ended.
JobNetComment=xxx JobNetName=xxx Code=xxx
ProjectName=xxx SubSystemNumber=xxx
```

- Systemwalker CentricMGR V11.0L10 or later

```
AP:jobschExit: ERROR: JOBNET terminated abnormally.
JobNetComment=xxx JobNetName=xxx Code=xxx
ProjectName=xxx SubSystemNumber=xxx
```

[UNIX]

- Systemwalker Centric Manager 11.0 or earlier

```
UX:jobschExit: ERROR: JOBNET has abnormal ended.
JobNetComment=xxx JobNetName=xxx Code=xxx ProjectName=xxx
SubSystemNumber=xxx
```

- Systemwalker Centric Manager 12.0 or later

```
UX:jobschExit: ERROR: JOBNET terminated abnormally.
JobNetComment=xxx JobNetName=xxx Code=xxx ProjectName=xxx
SubSystemNumber=xxx
```

For details on the setting for event monitoring, see the *Systemwalker Centric Manager User's Guide* - *Monitoring Functions*.

2.12.1 When You Monitor an Abended Job Net and Take Automatic Resolved Status in Response to the Restart or Confirmation of Job Net

When you restart or confirm the Abended status job net, its operation is reported to Systemwalker Centric Manager and the execution status is changed to "Resolved" automatically.

Definition procedure

1. Install any of the following Systemwalker Centric Manager's server functions on the computer where the Systemwalker Operation Manager server has been installed.
   - Operation Management Server
   - Asset Management Server
   - Section Management Server (SMS)
   - Job Server
2. Check the **Automatic notification/handling** box on the **Event output** sheet of the **Define Jobscheduler Startup Parameters** window. If checked, an abended job net and its restart or confirmation are automatically reported to the **Monitor** window of Systemwalker Centric Manager.
3. Restart the Jobscheduler services or daemons.

For operation in the cluster configuration

If you are using Systemwalker Operation Manager together with Systemwalker Centric Manager both of which are operated in the cluster configuration, register them in the resource or group of the same cluster system.

The resource and group of each cluster are as follows.

- Sun Cluster: Resource group
- MSCS: Cluster group
- Microsoft(R) Fail Over Clustering: Cluster service
- PRIMECLUSTER: Cluster application

2.12.2 Directly Displaying the Monitoring Window for the Abended Job Net

It is possible to display the monitoring window for the job net that terminated abnormally directly from the event list of the Systemwalker Centric Manager monitoring window.

This function is available if all versions of Systemwalker Operation Manager Server and Clients, and Systemwalker Centric Manager Operation Management Server and Operation Management Clients of Systemwalker Centric Manager are V12.0L10/12.1 or later.

This section explains the definitions for displaying the Monitoring Window monitoring and the the monitoring procedure from the Systemwalker Centric Manager.

The definition procedure is different according to the version of linked Systemwalker Centric Manager.

Systemwalker Centric Manager V13.4.0 or later

If the version of all the Systemwalker Centric Manager Operation Management Server and Operation Management Client is V13.4.0 or later, the definition procedure is different according to presence/absence of the installation of the client functions of the Systemwalker Operation Manager.

The client of the Systemwalker Operation Manager is installed

If the client of the Systemwalker Operation Manager is installed in the machine that the Systemwalker Centric Manager Console is running, define the following according to the displaying the Monitoring Window.

The definition procedure for displaying windows client

1. Select the **Design Settings** of the **View** menu in the **Monitor** of the Systemwalker Console for the Systemwalker Centric Manager.

2. Select the **Monitored Event Type** Window tab in the displayed the **Design Settings** dialog box.

3. Select the "**BatchJob**" in the monitored event type of the **Monitored List** of the **Monitored Event Type Window** sheet and click the **Modify** button.

4. Modify values of the **Command Line** in the displayed **Customize dialog box** as below.

   Command Line:

   ```
   mpjobgui.exe /T %EVENTTEXT /H %HOST /I %IP /P %PAC
   ```

   Note: The destination of mpjobgui.exe:
   <Systemwalker Operation Manager installation directory>\MPWLKER.JM\bin

The definition procedure for displaying Web console

1. Edit the following file.

   ```
   Systemwalker Centric Manager installation directory\mpwalker.dm\mpbcmgui
   \etc\mpjobweb.ini
   ```

   The "mpjobweb.ini" is specified as the following format.

   ```
   [mpjobweb]
   CLIENT=WEB
   ```

   [mpjobweb]

   If the Web console is displayed, specify this section.

   CLIENT=WEB

   Specify it in all uppercase. If other than this format (including blank) is specified, it is ignored.

   If there are sections of the same name, add only "CLIENT=WEB" line under the existing section of the same name.

2. Define the following specified in the "The client of the Systemwalker Operation Manager is not installed"

The client of the Systemwalker Operation Manager is not installed

In the environment that the Systemwalker Operation Manager is not installed, use the Web console for monitoring. To display the Web console, define in the httpd.conf file and the mpjobweb.ini file.

The definition procedure for httpd.conf

1. Log in as system administrator (user belonging to the Administrator group or superuser) to the monitoring target server.

2. Execute the poperationmgr command to stop Systemwalker Operation Manager.

3. Add the following to httpd.conf.

   [Solaris/Linux]
   /opt/FJSVftlo/mpahs/conf

```
LoadModule rewrite_module "/opt/FJSVftlo/mpahs/modules/mod_rewrite.so"
<Location ~ /Systemwalker-omgr/>
RewriteEngine on
SetEnvIf Request_URI .*home\.op HOMEOP
SetEnvIf HTTPS "on" P_TYPE=https://
SetEnvIf P_TYPE "^$" P_TYPE=http://
RewriteRule .* - [E=INFO_REFERER:%{ENV:P_TYPE}%{HTTP_HOST}/]
RequestHeader set referer "%{INFO_REFERER}e" env=HOMEOP
</Location>
```

[Windows]
<Systemwalker Operation Manager installation directory>\mpwalker.jm\mpahs\conf

```
LoadModule rewrite_module "<Systemwalker Operation Manager installation directory>/mpwalker.jm/mpahs/modules/mod_rewrite.so"
<Location ~ /Systemwalker-omgr/>
RewriteEngine on
SetEnvIf Request_URI .*home\.op HOMEOP
SetEnvIf HTTPS "on" P_TYPE=https://
SetEnvIf P_TYPE "^$" P_TYPE=http://
RewriteRule .* - [E=INFO_REFERER:%{ENV:P_TYPE}%{HTTP_HOST}/]
RequestHeader set referer "%{INFO_REFERER}e" env=HOMEOP
</Location>
```

4. Execute the soperationmgr command to start Systemwalker Operation Manager.

The definition procedure for mpjobweb.ini

If Systemwalker Centric Manager Operation Management Server and the Systemwalker Operation Manager server have been installed on the same machine, this definition is unnecessary.

1. Edit the following file.

```
<Systemwalker Operation Manager installation directory>\mpbcmgui\etc\mpjobweb.ini
```

   Edit the "mpjobweb.ini" file using the following format:

```
[mpjobweb]
WEB_IP_ADDR=%IP%
```

   [mpjobweb]

      Do not edit this item.

   WEB_IP_ADDR=%IP%

      Specify the IP address of the Systemwalker Operation Manager Web server in the %IP%.

      If there are sections of the same name, add only "WEB_IP_ADDR=%IP%" line under the existing section of the same name.

2. Enter the host name and IP address of the Web server for Systemwalker Operation Manager in the "hosts" file for the hosts where the Operation Management Client has been installed.

When the port number of Operetion Manager common service(JMSRV) is changed

If the port number for the JMSRV Operation Manager common service has been changed on the Systemwalker Operation Manager Web server or the Systemwalker Operation Manager server, settings for the JMSRV Operation Manager common service must be added to the "services" file for the Systemwalker Centric Manager environment, using the same value as was specified for Systemwalker Operation Manager. Refer to "2.2.2 Changing Port Numbers" for information on how to specify these settings.

Systemwalker Centric Manager V13.3.0/V13.3.1 or earlier

If the version of any of the Systemwalker Operation Manager server, Systemwalker Centric Manager Operation Management Server and Operation Management Client is V13.3.0/V13.3.1 or earlier, the **Monitor Job Net** window will be displayed on the Windows client. For information on the settings for Systemwalker Operation Manager servers running V13.3.0/V13.3.1 or earlier, refer to the Systemwalker Operation Manager manuals for the version being used. If the version of Systemwalker Centric Manager is V13.3.0/V13.3.1 or earlier, use the following definition procedure:

1. Install any of the following Systemwalker Centric Manager's server functions on the computer where the Systemwalker Operation Manager server has been installed.

    - Operation Management Server

    - Section Management Server

    - Job Server

2. Check the **Automatic notification/handling** box on the **Event output** sheet of the **Define Jobscheduler Startup Parameters** window.

3. Restart the Jobscheduler services or daemons.

For operation in the cluster configuration

When you are operating the Systemwalker Operation Manager server in the cluster configuration, create a cluster_ip.csv definition file and define the logical IP address, subsystem number and physical IP address in it, in addition to the definition procedure given above. For details on the cluster_ip.csv definition file, refer to the *Systemwalker Operation Manager Reference Guide*.

Procedure for monitoring from Systemwalker Centric Manager

Use the following procedure to display the Systemwalker Operation Manager monitoring window from the Systemwalker Centric Manager monitoring window:

1. From the **Event List** of the Systemwalker Centric Manager's **Monitor** window, select the event of the abended job net.

2. Select **Jobscheduler** from either the **Tools** menu or the right-click pop-up menu.

When displaying the Systemwalker Operation Manager monitoring window directly from the event list in the Systemwalker Centric Manager monitoring window, the window can be displayed using general user authority by the system administrator or via user authentication.

In an environment where a Windows client is connected, in the following cases, the host name of the server at the point when the job net terminated abnormally will be displayed for the **Connected host name** in the **Monitor Job Net** window:

- The host name is changed after a problem occurs in the job net.

- The host name of the connection destination server is changed due to switching clusters.

Note

If the windows cannot be linked, the following cases are possible. Check the settings.

- When there is an error with the command line settings for a linked product for which the monitored event type has been defined as "BatchJob" in the **Monitored Event Type Window** sheet of the **Design Settings** dialog box (which is displayed by selecting **Design Settings** from the **View** menu).

  Use the following procedure to return the current settings to the original settings. You must perform the procedure for every login user of the **Monitor** window of the Systemwalker for which you added modifications to the definition.

1. In the **Systemwalker Console - Monitor**, select **Design Settings** from the **View** menu.

   The **Design Settings** dialog box appears.

2. Click **Default Values** in the **Monitored Event Type Window** sheet to return the settings of **Monitored Event Type List** to the original settings.

3. In the **Design Settings** dialog box, click **OK**.

However, note that this procedure will initialize the settings for all types, temporarily save any settings that you do not want initialized.

In this case, initialize the settings as follows, making sure to save the necessary settings:

1. Select a type that has already been set and is to be saved from **Monitored Event Type List**.

2. Open the **Customize** dialog box by clicking **Modify**. Then, save the values set in **Command Name** and **Command Line**.

- When an attempt is made to view one of the following hosts from Systemwalker Centric Manager in an environment where **Web Console** is connected

  - A host that has not been set in the **Monitored Host Configuration** window on the Windows client

  - A host that has not been set in the **Setting** view >> **Monitored Hosts** in **Web Console**.

  To view these hosts, set them in both the **Monitored Host Configuration** window on the Windows client and the **Settings** view >> **Monitored Hosts** in **Web Console**.

2.12.3 When You Monitor the Job Net Execution by Checking the Execution History to be Output to the Event Log or SYSLOG

You can monitor any job net execution except for an abended job net and its restart by checking the execution history to be output to the event log or SYSLOG.

This monitoring method does not enable automatic resolving when an abended job net is restarted.

Note

- If monitoring is performed using this method while **Automatic notification/handing** has been enabled in the **Event output** sheet of the **Define Jobscheduler Startup Parameters** window, duplicate notifications will be made if an abended, canceled, or closed status occurs. To suppress duplicate notifications, perform monitoring based on the method described in "2.12.1 When You Monitor an Abended Job Net and Take Automatic Resolved Status in Response to the Restart or Confirmation of Job Net".

- If a same message is output from SYSLOG continuously, the second and subsequent messages will be changed to ones starting with "last messages repeated"; this may cause incorrect monitoring.

Definition procedure

1. Install any of the following Systemwalker Centric Manager's server functions on the computer where the Systemwalker Operation Manager server has been installed.

   - Operation Management Server

   - Asset Management Server

   - Section Management Server (SMS)

   - Job Server

2. Use the **Details** button in the **Event output** field of the **Event output** sheet of the **Define Jobscheduler Startup Parameters** window to select the execution status of the job net to be monitored. The history of the selected job execution will be output to the event log.

3. Restart the Jobscheduler services.

4. The server installed by Step 1 specifies by Systemwalker Centric Manager, to monitor the operations from the Operation Management Server of Systemwalker Centric Manager.

   [Windows]

   Normally, only warning or error level event log messages are monitored by Systemwalker Centric Manager. If you monitor event log messages other than warning or error level messages, including the job net startup (information level), you must change the definitions to monitor those event log messages. If changed, the execution history is displayed in the **Monitor** window when it is output to the event log.

   [UNIX]

   Normally, only the SYSLOG messages higher than the ERROR or WARNING level messages are monitored by Systemwalker Centric Manager. If you monitor the SYSLOG messages other than WARNING or ERROR level messages, including the job net startup (INFO level), you must change the definitions to monitor those SYSLOG messages. If changed, the execution history is displayed in the **Monitor** window when it is output to the SYSLOG.

   For the definition details, refer to the *Systemwalker Centric Manager Installation Guide*.

If the mail transmission action of event monitoring is used to send information about completed job nets, refer to the *Systemwalker Centric Manager User's Guide - Monitoring Functions* and "jobschgetoutput Command" in the *Systemwalker Operation Manager Reference Guide*.

2.12.4 Definitions for Using the Web Console from the Web Linkage Top Page

This section explains the definitions for using the Systemwalker Operation Manager Web console from the Web linkage top page.

Definition procedure

If necessary, perform the following setup procedure:

1. Update the connection information used during linkage

   If Systemwalker Centric Manager is installed after Systemwalker Operation Manager V13.8.0 or later has already been installed, execute the following command in the Systemwalker installation directory:

   Windows:

   ```
   COPY MPWALKER.JM\mpjmweb\f3csbjob.htm MPWALKER\inet\wwwroot
   \mpjm\f3csbjob.htm /Y
   ```

   UNIX:

   ```
   ln -s -f /opt/FJSVjmweb/f3csbjob.htm /opt/systemwalker/inet/wwwroot/mpjm/f3csbjob.htm
   ```

2. Change the connection information used during linkage

   If the following changes have been made with Systemwalker Operation Manager, modify the "f3csbjob.htm" linkage connection information file:

   - When 2.4.7 Definitions for Encrypted Communications (HTTPS Communications) for the Web Console/ Web API have been made

   - If the port number used by the Web server has been changed from the default value (9900)

   File to modify:

   Windows:

   MPWALKER\inet\wwwroot\mpjm\f3csbjob.htm

   UNIX:

   /opt/systemwalker/inet/wwwroot/mpjm/f3csbjob.htm

Location to modify:

```
top.location.replace('http://' + location.hostname + ':9900/Systemwalker-omgr/login.op');
```

How to make the modification:

Edit the file using a text editor such as vi or Notepad.

To use HTTPS communications

Replace the "http" above with "https". If HTTPS communications are not used, change "https" back to "http".

To change the port number:

Replace "9900" above with the new port number.

2.13 Definitions when Constructing the Existing Environment on Another Server

Systemwalker Operation Manager allows you to extract the following information from an operating server and to distribute it to another server. Only the system administrator belonging to the Administrators group or the superuser can extract and distribute such information. When the Extended User Management function is valid in the UNIX system, only the Operation Manager user having the administrative authority can perform it.

- The environment definition information of Systemwalker Operation Manager
- The registration information of Systemwalker Operation Manager

The information above is collectively referred to as "policy data."

By extracting and distributing policy data, the same operating environment as that of an already operating server can be configured on another server.

The policy data can be extracted and distributed for each function provided by Systemwalker Operation Manager. However, you cannot select part of each function (such as a particular calendar and a particular exit) for extraction and distribution.

You cannot distribute the policy data extracted from a Windows server to a UNIX server. Also, you cannot distribute the policy data extracted from a UNIX server to a Windows server.

This section explains the followings:

- Extracting the Policy Data
- Distributing the Policy Data
- Extracting/distributing policy data when using the Extended User Management function [UNIX]

If you need to extract and distribute the policy data (including copying files) between the current version and an earlier version, refer to the *Systemwalker Operation Manager Technical Guide*.

EE

Refer to Systemwalker Operation Manager User's Guide - Master Schedule Management for details on the method that is used to extract and distribute policy information for the Master Schedule Management function.

2.13.1 Extracting the Policy Data

This section explains how to extract the policy data.

Definition procedure

1. Open the **Extract Policy** window.

   To do so, click **Extract Policy** in the **Systemwalker Operation Manager Environment Setup** window.

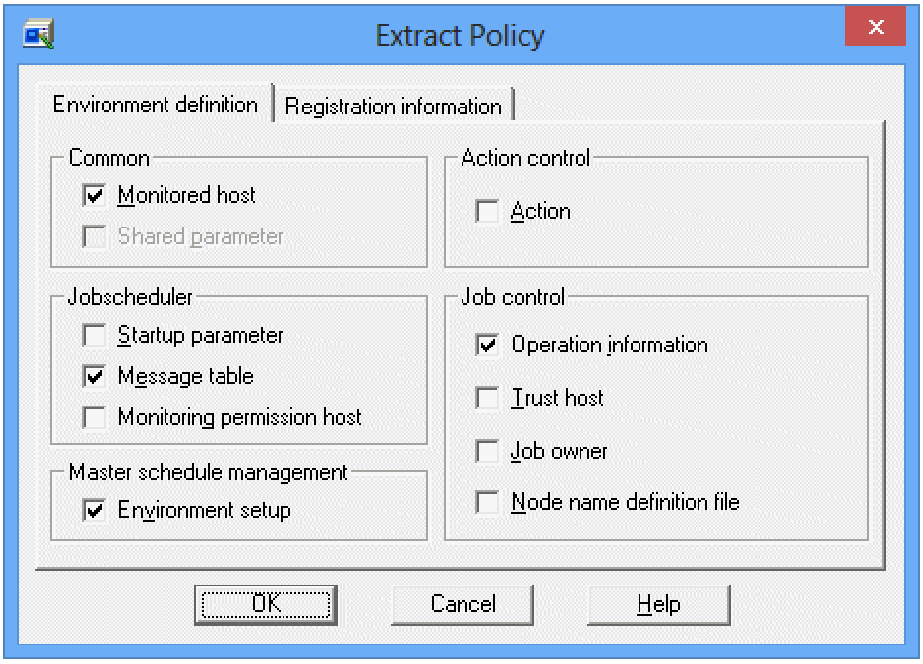
2. Set up the policy data.

   When the **Extract Policy** window appears, select the desired sheet from it.

3. Save the policy data.

   Click **OK** to save the policy data.

Environment definition sheet in the Extract Policy window



Common

☑ Monitored host

□ Shared parameter

Action control

□ Action

Jobscheduler

□ Startup parameter

☑ Message table

□ Monitoring permission host

Job control

☑ Operation information

□ Trust host

□ Job owner

□ Node name definition file

Master schedule management

☑ Environment setup

Monitored host:

Use this option to extract the monitoring host information which has been set in the environment definition (the Monitored Host).

Shared parameter [UNIX]:

Use this option to extract the security information which has been set in the environment definition (the Operation Manager's shared parameter definition).

Action [Windows]:

Use this option to extract the information about the action execution environment which has been set in the environment definition (action).

Startup parameter:

Use this option to extract the startup parameter information which has been set in the environment definition (startup parameters).

Message table [Windows]:

Use this option to extract the message table information which has been set in the environment definition (message table).

Monitoring permission host:

Use this option to extract the information that permits the multi-server monitoring function to be monitored and that has been set in the environment definitions (monitoring permission host).

Operation information:

Use this option to extract the operating information that has been set in the environment definitions (operation information).

Trust host:

Use this option to extract the trust host information that has been set in the environment definitions (trust host).

Job owner [Windows]:

Use this option to extract the job owner information that has been set in the environment definitions (job owner).

Node name definition file:

Use this option to extract the node name information used for the cluster system that has been set in the environment definitions (operation information).

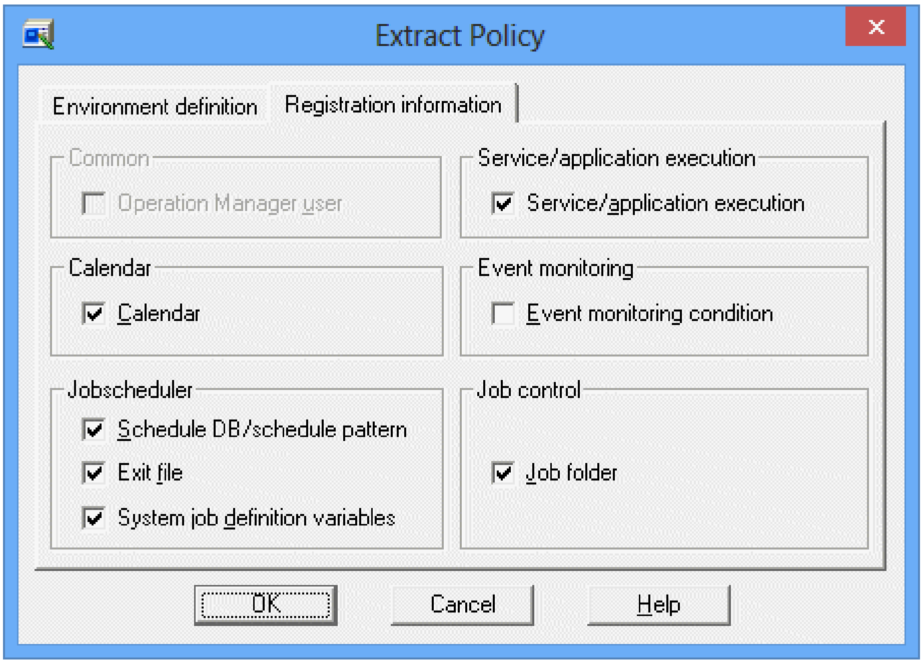
EE

Environment setup:

Select this checkbox to extract information about environment settings relating to the Master Schedule Management function that have been specified using the Master Schedule Management environment setup client.

Refer to the *Systemwalker Operation Manager User's Guide - Master Schedule Management* for details.

Registration information sheet in the Extract Policy window



Common
☐ Operation Manager user

Service/application execution
☑ Service/application execution

Calendar
☑ Calendar

Event monitoring
☐ Event monitoring condition

Jobscheduler
☑ Schedule DB/schedule pattern
☑ Exit file
☑ System job definition variables

Job control
☑ Job folder

Operation Manager user [UNIX]:

Select this sheet to extract Operation Manager user information registered by the Extended User Management function. The Operation Manager user information is distributed regardless of whether the Extended User Management function is enabled or disabled in the extraction source and distribution destination. The enable or disable status of the Operation Manager user in the distribution source is not changed

Do not select this item if the policy extraction source and distribution destination perform cluster operations. Refer to "Extracting Operation Manager user information in a cluster environment [UNIX]" for details on extracting Operation Manager user information in a cluster environment.

Calendar:

Use this option to extract the calendar information and the power control information which have been registered by the Calendar function.

Service/application execution:

Use this option to extract the services and applications startup information which has been registered by the Service/application execution function.

Schedule DB/schedule pattern:

Select this checkbox in the following situations

- When extracting schedule information and schedule pattern information that has been registered with the Jobscheduler function
- When extracting information about access rights that have been set up for projects
- When extracting password management book information for Task Link
- When extracting authentication information registered by the jobschsetauthinfo command
- EE When extracting master information for the Master Schedule Management function
- When extracting the subsystem day change time

Exit file:

Use this option to extract the exit program file to be called by the Jobscheduler function.

System job definition variables:

Select this option to extract job definition variables registered using the Jobscheduler function.

Event monitoring condition [Windows]:

Use this option to extract the monitored event and execution action information which has been registered using the **Event Monitoring Conditions Definition** window.

Job folder:

Use this option to extract the job folder information (including the job file information) which has been registered by the Job function.

Point

Distribution of Calendar and Schedule DB/schedule pattern policies

- The reflection start date set in the **Save Calendar** window is not distributed in the policies.
- If you select **Calendar** to distribute the policy when the **Halt recreation of startup days** option is not selected in the **Use Function2** sheet of the **Define Jobscheduler Startup Parameters** window, the startup days of the calendar-based job nets are recreated and information of the startup days of job nets individually set in the **Startup days** window is cleared regardless of whether **Schedule DB/schedule pattern** extraction is selected.
- To make the startup day information for the server where policies are distributed match the server where the policies are extracted, either extract only **Schedule DB/schedule pattern** policy information without **Calendar** policy information, or select the **Halt recreation of startup days** option in the **Use Function2** sheet of the **Define Jobscheduler Startup Parameters** window for distributing the policy. If there is no calendar information that can be referred to on the server where the policy is distributed, the following message may be output to the event log or SYSLOG when the Jobscheduler starts or when the year changes.

  "Calendar information not found."

Extracting Operation Manager user information in a cluster environment [UNIX]

If the policy extraction source and distribution destination perform cluster operations, do not select **Operation Manager user** when extracting a policy.

Use the following procedure to extract Operation Manager user information as a policy:

1. After the policy extraction (without **Operation Manager user** specified) in the **Extract Policy** window has completed, log in as superuser (root) to the policy extraction source environment.
2. Execute the following command at the policy extraction source.

   ```
   /opt/FJSVfwseo/bin/mpuserspol -u -d <any directory>
   ```

3. Copy userdata.sh (generated in step 2 in the directory specified in the -d option) to the policy distribution destination environment.

Refer to "Distributing Operation Manager user information to a cluster environment [UNIX]" for information on tasks required at the distribution destination.

Notes on extraction of policies for schedule DB/schedule pattern information [UNIX]

If you have registered the same project names consisting of different uppercase and lowercase letters, you cannot extract their schedule information correctly. In such case, follow the procedure given below.

The policy data you have extracted and distributed in the following procedure will be used only when the daemon is started in the next time.

1. Issue the following command from the server where you extract the policy.

   The access privileges setup script will appear.

   ```
   /usr/bin/mkbat -j -f acldata.bat
   ```

   EE

   To extract the policy from the server during multi-subsystem operation, issue the following command.

   ```
   /usr/bin/mkbat -j -x -c -r mpjobsch/schedulen -f acldata.bat
   ```

   ```
   where, "n" is a number of the subsystem used for policy extraction.
   ```

2. Directly copy the following **acldata.bat** file (the access privileges setup script) under the following directory of the policy destination server using the "ftp" or others.

Solaris	/var/opt/FJSVJMCMN/policy
DS version	/var/opt/uxpJMCMN/policy
HP-UX version	/opt/FHPJMCMN/db/policy
AIX version	/usr/FAIXJMCMN/db/policy
Linux	/var/opt/FJSVJMCMN/policy

   EE

   When you copy the above file (**acldata.bat**) on the server used for multiple-subsystem operations, the policy is reflected on the Jobscheduler of subsystem 0.

   To reflect the policy on any of subsystems 1 to 9, rename the file to **acldatan.bat**, where, "*n*" is a subsystem number of the corresponding destination Jobscheduler.

3. Copy the following files locating under the database directory of Jobscheduler directly to the policy destination server using the "ftp" or others.

   - project-name.jsp
   - project-name.dbz
   - project-name.grz
   - db_calendar_ex.default

   [Destination directory]

Solaris	/var/opt/FJSVJMCMN/policy/ jobdb
DS version	/var/opt/uxpJMCMN/policy/ jobdb
HP-UX version	/opt/FHPJMCMN/db/policy/ jobdb
AIX version	/usr/FAIXJMCMN/db/policy/ jobdb

Linux	/var/opt/FJSVJMCMN/policy/ jobdb

EE

When you copy the policy data to the above files using the servers available for multiple-subsystem operations, the policy is reflected on the Jobscheduler of subsystem 0.

To reflect the policy on the Jobscheduler for any of subsystems 1 to 9, rename the destination directory to **jobdbn**, where, "*n*" is a subsystem number of the corresponding destination Jobscheduler.

EE

4. If the Master Schedule Management function is being used, master settings for the master project that has been distributed must be specified again on the policy distribution destination server after the policy has been applied. Refer to "stemSetPrjMaster Project Master Setting Command" in the *Systemwalker Operation Manager Reference Guide* for details.

2.13.2 Distributing the Policy Data

The following explains how to distribute the policy data.

Definition procedure

1. Open the **Systemwalker Operation Manager Distribution [Login]** window.

   To do this, click **Distribute Policy** in the **Systemwalker Operation Manager Environment Setup** window.

2. Specify the policy destination.

   To do this, specify the policy destination in the **Systemwalker Operation Manager Distribution [Login]** window. You can enter a host name or a folder name to specify the policy destination. When you specify a host name, enter the host name, the user ID, and the password. When you specify a folder name, click **Select Folder** and enter the destination folder from the **Select Distribution Destination Folder** window.

3. Open the **Apply Policy** window.

   When the policy data is properly authenticated, the **Apply Policy** window is displayed. (Note)

EE

Note:

> When multi-subsystems are running on the server, the **Specify Destination Subsystem** window appears after the Log in the **Systemwalker Operation Manager Distribution [Login]** window. Select the destination subsystem number and click **OK**, and the **Apply Policy** window will appear.

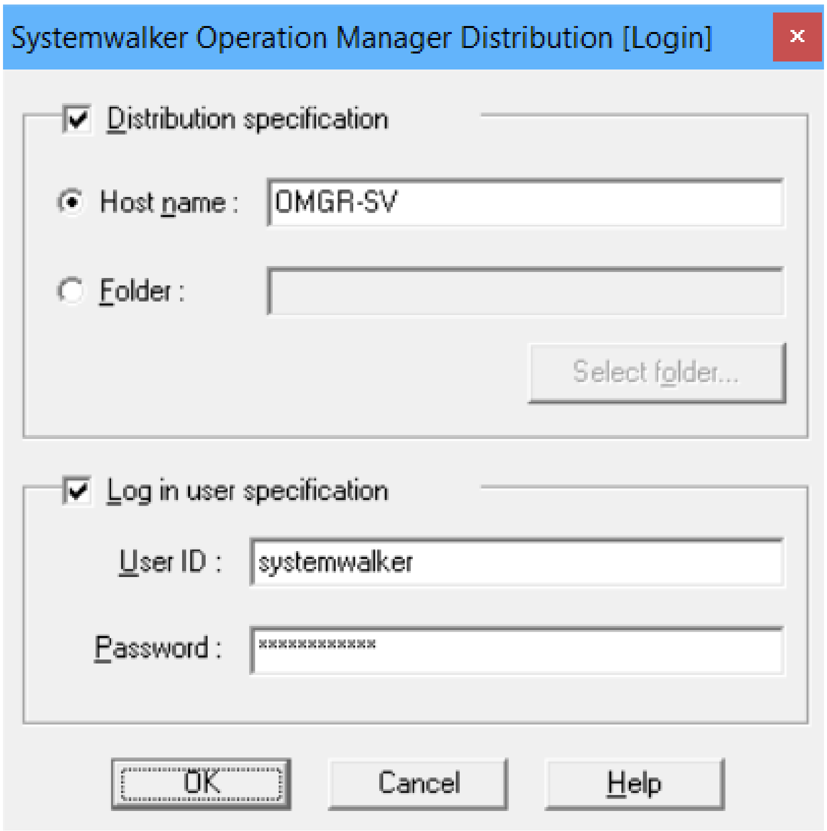
4. Apply the policy data.

   Click **OK** to apply your policy data.

Note

When specifying a distribution destination on the **Systemwalker Operation Manager Distribution [Login]** window, use the system administrator user ID (if the destination server is running the Windows version this will be a user that belongs to the Administrators group, whereas if the destination server is running the UNIX version this will be a superuser). However, if the Extended User Management function (UNIX) has been enabled, use the Operation Manager user ID with administrator privileges. The **Apply Policy** window cannot be used if a user ID is specified that does not have administrator privileges.

Systemwalker Operation Manager Distribution [Login] window


Systemwalker Operation Manager Distribution [Login]
☑ Distribution specification
● Host name :
○ Folder :
Select folder...
☑ Log in user specification
OK
Cancel
Help

Host name: OMGR-SV

User ID : systemwalker

Password : ************

Host name:

Specifies a host name (DNS host name or IP address) to which the policy data is distributed. The user name can be up to 128 characters.

If omitted, the policy information will be distributed to the server (a server running Systemwalker Operation Manager environment setup client). Cannot be omitted in the environment where only the client has been installed.

Folder:

Use this option to display the selected folder in the **Select Distribution Destination Folder** window by clicking **Select folder**.

Select folder:

Use this option to display the **Select Distribution Destination Folder** window. The folders of the monitored host information, which has been stored on the server connected from the **Systemwalker Operation Manager Environment Setup** window, are listed. You can select the policy destination folder from the list.

User ID:

Specify a login user ID.

If a user ID is omitted, the desktop login user ID will be used for the connection. Cannot be omitted in the environment where only the client has been installed.

[Windows]

For domain users, separate the domain name and the user ID with a backslash ("\"). Specify a user ID up to 36 bytes.

If a password has been set up for the specified user ID, it must also be specified. User IDs whose password is invalid cannot be specified.

[UNIX]

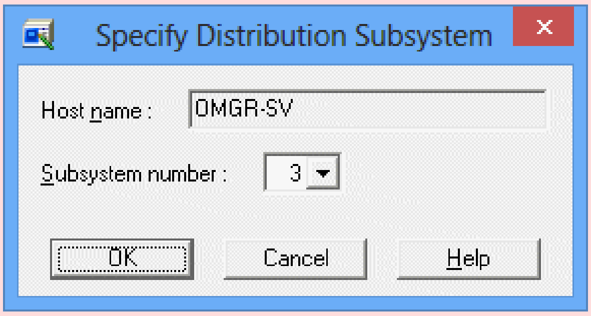
Specify a user ID up to 20 bytes. User IDs whose password is invalid cannot be specified.

Password:

Specify a login user password up to 50 bytes long.

EE

Specify Destination Subsystem window



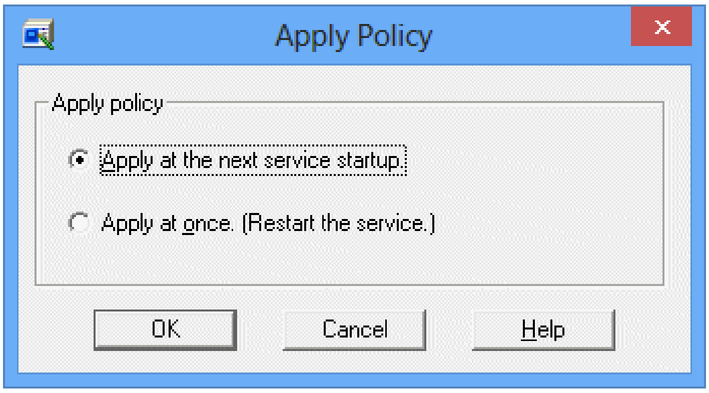
Host name : OMGR-SV

Subsystem number : 3

Subsystem number:

Use this option to select a subsystem number of the corresponding subsystem to be connected.

Apply Policy window



● Apply at the next service startup.

○ Apply at once. (Restart the service.)

Apply at the next time service startup:

Use this option to distribute the policy data only. The policy data is applied when the services or daemons are started in the next time.

The monitored host configuration information and the job folder information are applied at the same time when distributed even if you have selected the Apply at the next time service/daemon startup option. In such case, however, the services or daemons are NOT restarted.

[UNIX]

When you distribute the startup parameters, you must restart the following daemons at the same time if the enable or disable setup of Continuous Execution mode does not match between the policy data extracting server and the policy data destination server. If any of those servers is restarted, part of policy data may not match and the servers may not operate normally.

- Jobscheduler daemon
- Job Execution Control daemon

Apply at once. (Restart the service.):

Use this option to distribute and apply the policy data at once. If used, the services or daemons at the destination are restarted and the system operations are interrupted temporarily. If the services or daemons are not active, the services or daemons are not started.

EE

If the system is used for multiple-subsystem operations, the subsystem which correspond to the subsystem number you have selected from the Specify Destination Subsystem window is started.

Distributing policies to servers that cannot be connected via the network

When distributing the extracted policy data to servers that cannot be connected via the network, you can distribute the policy by copying its file. For the detailed procedure, see "2.13.2.1 Distributing Policy Data by Copying Files".

Notes on policy distribution

Distributing the startup parameters [Windows]

When you distribute the startup parameters of Jobscheduler, you must complete certain operations in addition to the ordinary policy distribution and extraction if:

a. The database storage directory does not match between the policy data extracting server and the policy data destination server, or

b. The Continuous Execution mode setup for network jobs does not match between the policy data extracting server and the policy data destination server.

The following details the operations you must complete.

a. If the database directory does not match between the servers

If the database directory does not match between the policy data extracting server and the policy data destination server, complete the following procedure on the destination server BEFORE applying the policy.

1. Shut down the Jobscheduler services from the **Systemwalker Operation Manager Environment Setup** window.
2. Open the **Define Jobscheduler Startup Parameters** window, and enter the same directory name as that used to store the database on the policy extracting server in the **Directory** field of the **Database** sheet.
3. Check the **Copy current database to destination** checkbox on the **Database** sheet of **Define Jobscheduler Startup Parameters** window.

b. If the Continuous Execution mode setup differs between the servers

If the Continuous Execution mode setup does not match between the policy data extracting server and the policy data destination server, complete the following procedure on the destination server AFTER you have applied the policy.

- If the setup on the policy extracting server is valid but the setup on the destination server is invalid:

  Issue the **jmmode** command with the "continue" operand to enable the Continuous Execution mode.

- If the setup on the policy extracting server is invalid but the setup on the destination server is valid:

  Issue the **jmmode** command with the "cancel" operand to disable the Continuous Execution mode.

Distributing the monitored host

- If you distribute the policy when no policy distribution destination host is included in the monitored host configuration information at the policy extraction source, you must register the policy distribution destination host name in the Define Monitored Host after distributing the policy.

Distributing the shared parameter [UNIX]

When you distribute the extracted shared parameter data, you must restart the Systemwalker Operation Manager server on the destination server at the same time.

Distributing policies for the operation information

- Use the **Logging** sheet of the **Define Operating Information** window to check the location where job execution history and operation results of the server from where data will be extracted are stored and verify that the specified location exists on the destination server. If it does not, an error will occur when you restart Systemwalker Operation Manager after distribution, so create a directory on the destination server that is identical to the storage location on the source server.
- If information is distributed from a source server running V13.2.0 or earlier to a newly installed destination server running V13.3.0 or later, the default storage locations for the job execution history are different between these servers.

This will result in an error when Systemwalker Operation Manager is restarted. To prevent this problem, take one of the following measures [Windows]:

- Before distributing operation information, create a directory on the destination server that is the same as the storage location for job execution history on the source server.
- After distributing operation information, use the **Logging** sheet of the **Define Operating Information** window to set the default storage location on the destination server.

  In a new installation of V13.3.0 or later, the default storage location is as follows:

  ```
  C:\systemwalker\MpWalker.JM\mpmjessv\hist
  ```

- When policy information extracted from a cluster environment is distributed to a non-cluster environment, **Spool directory** may not be specified in the **Cluster settings** sheet of the **Define Operating Information** window on the distribution destination server. In this case, an error occurs when you restart Systemwalker Operation Manager after distribution. Therefore, set the following for **Spool directory** on the distribution destination [Windows]:

  - If the distribution destination is not operating multiple subsystems, or for Subsystem0:

    <*Systemwalker Operation Manager installation directory*>\MpWalker.JM\mpmjessv\mjespool

  - If the distribution destination is Subsystem1 to 9:

    <*Systemwalker Operation Manager installation directory*>\MpWalker.JM\mpmjessv\mjes<*n*>\mjespool

    (<*n*> is the subsystem number.)

- If policy information is distributed to a cluster environment, the **Logical IP address** field in the **Cluster settings** sheet of the **Define Operating Information** window may be set to the IP address of the machine from which the policy information was extracted. After distributing the policy information, check the **Logical IP address** field, and change it if necessary.

Distributing Operation Manager user information to a cluster environment [UNIX]

To distribute Operation Manager user information when the policy extraction source and distribution destination perform cluster operations, perform the following tasks after the policy has been applied in the **Apply Policy** window:

1. Log in as superuser (root) to the distribution destination environment.
2. Execute userdata.sh (copied from the extraction source when "Extracting Operation Manager user information in a cluster environment [UNIX]").

Distributing policies for Schedule DB/ schedule pattern information

When distributing policies for the Schedule DB/schedule pattern information of Jobscheduler, you must notice the following notes.

- If the policy data extracting server and the policy destination server have different user account and domain information, you must change the security information of the project.

  Follow the procedure below.

  1. Change the security information of the access privileges setup script before applying the policy data. Correct both the **mpsetacl** command and **mpchown** command operands stored in the **acldata.bat** file which locates under the policy data storage directory, and change the project owner information and the access privileges information.

     The policy data you have extracted (but not distributed yet) is located under the following directory on the PC where you have opened the **Systemwalker Operation Manager Environment Setup** window.

     ```
     Systemwalker Operation Manager installation directory
     \MpWalker.JM\mpjmcl\work\policy
     ```

     When distributed, the policy data is stored under the following directory on the policy destination server.

     [Windows]

```
Systemwalker Operation Manager installation directory
\MpWalker\mpaosfsv\policy
```

[UNIX]

Solaris	/var/opt/FJSVJMCMN/policy
DS version	/var/opt/uxpJMCMN/policy
HP-UX version	/opt/FHPJMCMN/db/policy
AIX version	/usr/FAIXJMCMN/db/policy
Linux version	/var/opt/FJSVJMCMN/policy

For details on the **mpsetacl** and **mpchown** commands, refer to the *Systemwalker Operation Manager Reference Guide*.

2. Change the security information of Jobscheduler after you have applied the policy data (that is, after restart of servers or daemons). Start the Systemwalker Operation Manager client, connect to the policy destination server as the user belonging to the Administrators group or as the superuser, and change the project owner information and the access privileges information. To change the project owner information and the access privileges information, use the **Change Owner** window and the **Set Permissions** window.

- The jobs, job nets and groups are Waiting on the destination server immediately after you have distributed or applied the policy data (except for the Paused or Disabled status). The job execution results including the start time, end time and completion codes are initialized and displayed. Also, the message event occurrence is cleared.

- The user ID that has been specified as the project owner on the server from which the policy information was extracted, and the user ID for which access privileges to the project have been set up must have been registered on the server to which the policy information is distributed. Refer to "mplstacluser Command" in the *Systemwalker Operation Manager Reference Guide* for information on how to check the user IDs for which access privileges to the project have been set up.

Distributing policies for job folders

When distributing policies regarding job folders, notice the following notes.

- If you have set a directory containing the system information in a job folder and if you distribute policies to another system, the information of that system is overwritten by the distributed policies. To avoid this problem, release (or delete) the directory containing the system information before distributing policies.

- When you distribute policies for job folders, the files are transferred directly from the policy extracting server to the policy destination server. Therefore, you must set the following environments.

  - Define a host name of policy destination server and its IP address in the "hosts" file on the policy extracting server. This can resolve the host name during policy distribution.

Distributing the job owner information [Windows]

The **Log on as a batch job** privilege, which is assigned to the user ID of the job owner on the extraction source server, is not distributed, as this privilege is managed by the operating system. Assign the **Log on as a batch job** privilege to the user ID of the job owner on the distribution destination server.

For details, see "Execute the job with the owner right [Windows]" on the "**Options** sheet in the **Define Operating Information** window" of the "2.8.1 Defining the System Operating Information".

Distributing the Monitored Event Table function [Windows]

If Systemwalker Centric Manager has been installed, use Systemwalker Centric Manager to set up and distribute a policy for the Monitored Event Table.

For the distribution of policies related to the Monitored Event Table function when Systemwalker Centric Manager is installed, see "Setting up Other Function Policies" in the *Systemwalker Centric Manager User's Guide - Monitoring Functions*.

Distributing to environments with different user management methods

If the environments where policies are extracted and distributed use different methods to manage user IDs, the access rights information for the projects that are distributed will be as follows:

	Distribution destination		
	Method for managing user IDs	OS-based user management or Systemwalker authentication repository (*)	Extended User Management function [UNIX]
Source	OS-based user management or Systemwalker authentication repository (*)	- The system administrator will have the update right. - The project owner will have the update right for his/her own project. - The access rights information for OS users that have been set up for the project will be distributed.	- Operation Manager users with administrator privileges will have update rights.
	Extended User Management function [UNIX]	- The system administrator will have the update right. - The project owner will have the update right for his/her own project.	-

*:

If the source uses "OS-based user management", the destination will use a "Systemwalker authentication repository", and if the source uses a "Systemwalker authentication repository", the destination will use "OS-based user management".

In additions, if the V17.0 or later, you cannot select to manage with the Systemwalker authentication repository.

2.13.2.1 Distributing Policy Data by Copying Files

If you cannot connect to the policy destination servers, you can distribute the policy data by copying its files to those servers.

The following explains how to distribute policy data by copying files.

Definition procedure

1. Extract the policy information by following the procedure of "2.13.1 Extracting the Policy Data."

   When completed, the extracted policy data is stored under the following directory on the PC where you have opened the **Systemwalker Operation Manager Environment Setup** window.

   - The directory which stores the extracted policy data:

   ```
   Systemwalker Operation Manager installation directory
   \MpWalker.JM\mpjmcl\work\policy
   ```

2. Save all files locating under "The directory which stores the extracted policy data" explained above on a storage medium. You must store those files in the same directory structure.

3. If you can connect to the destination server and if Systemwalker Operation Manager's client functions have been installed on that server, store the files having the same directory structure (you have saved in Step 2 in the following directory.

   Prior to storing the files, delete all files and directories under the destination directory.

   - The destination directory to store the distributed policy data:

```
Systemwalker Operation Manager installation directory
\MpWalker.JM\mpjmcl\work\policy
```

4. Open the **Systemwalker Operation Manager Environment Setup** window, and click **Distribute Policy** to distribute policy data to the destination server.

Notes on policy distribution by copying files

When you distribute policy data by copying files, notice the following notes.

- No job folder information is applied by this method.

  You must copy each job file separately and create a new job folder.

For more information and notes, see "Notes on policy distribution" and the *Systemwalker Operation Manager Technical Guide*.

2.13.3 Extracting/Distributing Policy Data when Using the Extended User Management Function [UNIX]

You can distribute Operation Manager user information set using the Extended User Management function and the access privileges to projects to a different Systemwalker Operation Manager server using the Policy Data Extraction/Distribution functions.

This section describes how to extract or distribute the policy data using the Extended User Management function.

Note

- If the enable or disable setup of the Extended User Management function differs between the policy data extraction source and destination, the Operation Manager user is distributed to the destination but function enable or disable setup is not changed at the destination.

- You cannot distribute policy data of "Schedule DB/schedule pattern" extracted in version V11.0 or earlier to an environment where the Extended User Management function is enabled. If you need to distribute it, first disable the Extended User Management function by issuing the mpsetusermode command. For the mpsetusermode command details, refer to the *Systemwalker Operation Manager Reference Guide*.

Definition procedure

1. Before extracting or distributing the policy data, check the following.

   The system administrator of the extraction source or an OS user associated with the Operation Manager user must be registered in the distribution destination as well. If not, you fail policy data distribution. Before distributing the policy, check that they are registered in the distribution destination server. If not, register them. The OS user privileges in both of the extraction source and distribution destination must be the same.

2. In the extraction source server, check the policy distribution method of Operation Manager user information. Change it if necessary.

   Use the **mpupolmode** command to display the policy distribution methods.

   Use the **mpsetupolmode** command to change the policy distribution methods. By default, "keep" is set in which mode Operation Manager user information registered in the distribution destination server is not deleted. To delete the user information before distributing the policy, specify "clear" and execute the command.

   For the command details, refer to the *Systemwalker Operation Manager Reference Guide*.

3. Extract policy data.

   To extract/distribute Operation Manager user information registered using the Extended User Management function, select **Extract Policy** window >> **Registration Information** sheet, and then **Operation Manager user**.

To extract/distribute Operation Manager user information registered using the Extended User Management function or the access privileges information set for projects, select **Extract Policy** window >> **Registration Information** sheet, **Operation Manager user** and then **Schedule DB/schedule pattern**.

For more information on how to extract the policy data, see "2.13.1 Extracting the Policy Data".

4. Distribute the policy data.

   Operation Manager user information is distributed regardless of whether the Extended User Management function is enabled or disabled in the policy data extraction source and distribution destination servers.

   If you set the policy distribution method to "keep" in Step 2 and the Operation Manager user information already exists in the distribution destination, it is merged. If user information with the same name exists, it is overwritten by the extraction source information.

   If you set the policy distribution method to "clear" in Step 2, the existing Operation Manager user information in distribution destination server is deleted, then the Operation Manager user information in extraction source server is distributed.

   For more information on how to distribute the policy data, see "2.13.2 Distributing the Policy Data ".

5. Change the enabled or disabled status of the Extended User Management function if necessary

   Even if the policy data is distributed, the enabled or disabled status of the Extended User Management function is not changed. Change the enabled or disabled status of this function on the destination server if necessary.

Notes on access privileges information distribution

- Even if you extract and distribute schedule DB/schedule pattern alone when the Extended User Management function is not enabled in the distribution destination server, the access privileges information of the Operation Manager user set for projects using the Extended User Management function is not distributed. When distributing Operation Manager user's access privileges information by selecting only **Schedule DB/schedule pattern**, enable the Extended User Management function in the distribution destination server before distributing it.

- Regardless of whether the Extended User Management function is enabled or disabled, the access privileges information of a user who does not exist in the distribution destination server, is not set in the destination server even if you distribute it. In this case, the following message appears in SYSLOG.

  ```
  Access control information was restored incompletely. For details, see %1
  ```

  ```
  %1 : File name holding description of the error cause
  ```

  When you see this message, create a user in the distribution destination server, and distribute the policy again.

- If you distribute the access privileges information for a project which exists in the policy data extraction source server, but not in the policy data distribution destination server, by selecting **Schedule DB/schedule pattern**, the distribution destination server will have the following access privileges.;

  - When the Extended User Management function is enabled on the extraction source server and disabled on the distribution destination server (if OS-based user management is being used)

    The system administrator will have the update right.

    The project owner will have the update right for his/her own project.

  - If the Extended User Management function is disabled on the source (if OS-based user management is being used) and enabled on the destination

    The Operation Manager user with the administrator privileges will have the update right.

2.14 Definition for Maintenance

This section explains the system setup to be required for the maintenance of Systemwalker Operation Manager itself.

2.14.1 Defining the Process Monitoring Function

The following provides an outline, the definition information, and the customizing procedure of Systemwalker Operation Manager's Process Monitoring function.

2.14.1.1 Systemwalker's Process Monitoring Function

Systemwalker Operation Manager's Process Monitoring function can monitor process operations of Systemwalker itself. The Process Monitoring function regularly monitors whether the processes that start Systemwalker services or daemons are operating. If it detects a process violation (a process that should have started does not exist), it notifies the administrator by outputting an application log reporting the error (or a system log in the case of UNIX). If the processes exist, the Process Monitoring function does not report an error.

Information

If Systemwalker Centric Manager coexists:

If Systemwalker Operation Manager and Systemwalker Centric Manager coexist in the same environment, a report from the Process Monitoring function is automatically passed to the host server by Systemwalker Centric Manager's system monitoring agent function.

Using the Process Monitoring function

As the Process Monitoring function automatically starts at the system start time, the user needs not recognize it. When the function is active, the process of Systemwalker itself is monitored at fixed intervals.

If a process error is detected, the user must check the operation status of Systemwalker Operation Manager on the detected machine and isolate the error cause.

List of processes to be monitored

The following lists the processes which can be monitored by the Process Monitoring function. The corresponding service and function names are also listed.

[Windows]

Abbreviated function category	Function category: Description	Function name	Service name	Service display name	Name of process monitored
BASE	Authentication	Security	Fujitsu MpWalker ACL Manager	Systemwalker ACL Manager	f3crssvr.exe
OMGR	Operation Manager	Calendar	Fujitsu MpWalker MpJmCal	Systemwalker MpJmCal	f3crhcs1.exe f3crhcs2.exe
		Power control (power control, service/ application execution)	MpAosfP	Systemwalker MpAosfP	f3crhsv2.exe
		Automatic operation support (event monitoring, action management)	MpAosfB	Systemwalker MpAosfB	f3crhesv.exe f3crhdsv.exe f3crhxsw.exe f3crhesv_64.exe (Note 1) f3crhdsv_64.exe (Note 1) f3crhxsw_64.exe

Abbreviated function category	Function category: Description	Function name	Service name	Service display name	Name of process monitored
					(Note 1) f3crhesv_x64.exe (Note 2) f3crhdsv_x64.exe (Note 2) f3crhxsw_x64.exe (Note 2)
		Systemwalker Operation Manager infrastructure	Fujitsu MpWalker MpJmSrv	Systemwalker MpJmSrv	mpjmsrv.exe jmnetsv.exe java.exe
		Systemwalker Operation Manager infrastructure Task Link	SystemwalkerMpAHSO	Systemwalker MpAHSO	httpd.exe
			MpNjsosv	Systemwalker MpNjsosv	CNSSVENG.exe
		Job Execution Control	Fujitsu MpWalker MpMjes	Systemwalker MpMjes	mjssvc.exe mjsoba.exe
		Jobscheduler	Fujitsu MpWalker MpJobsch	Systemwalker MpJobsch	tskmnsrv.exe

Note 1:

This is the process name for the Windows for Itanium version.

Note 2:

This is the process name for the Windows x64 version.

[UNIX]

Abbreviated function category	Function category	Function name	Function	Startup command	Name of process monitored
BASE	Authentication	Security	FJSVfwseo	rc.mpfwsec	MpFwsec
OMGR	Operation Manager	Calendar	FJSVjmcal	S99JMCAL	f3crhcs2
		Systemwalker Operation Manager infrastructure	FJSVJMCMN (Note 2)	start_jmcmn	mpjmsrv jmnetsv java httpd
		Job Execution Control	FJSVMJS (Note 2)	S99MJS	mjsdaemon (Note 1) mjsnetsv (Note 1)
		Jobscheduler	FJSVJOBSC (Note 2)	start_jobs	tskmnsrv (Note 1)

Note 1:

A process exists for each subsystem when multi-subsystems are operated.

Note 2:

This is the package name for the Solaris or Linux version. For the HP-UX and AIX versions, the package names are as follows:

[HP-UX version]

Systemwalker Operation infrastructure: FHPJMCMN
Job Execution Control: FHPMJS
Jobscheduler: FHPJOBSCH
Calendar: FHPjmcal

[AIX version]

Systemwalker Operation infrastructure: FAIXJMCMN
Job Execution Control: FAIXMJS
Jobscheduler: FAIXJOBSC
Calendar: FAIXjmcal

Terminating the Process Monitoring function

The Process Monitoring function is stopped automatically when Systemwalker Operation Manager is stopped by the **poperationmgr** command or when the system is shut down.

To terminate the Process Monitoring function when Systemwalker Operation Manager is operating, specify the following from the Systemwalker Operation Manager server.

[Windows]

Select **Control Panel** >> **Administrative Tools** >> **Services** and shut down the following service.

```
Systemwalker MpPmonO
```

[UNIX]

Execute the following command to stop the daemon of the Process Monitoring function.

```
/opt/FJSVftlo/pmon/bin/stpmppmon
```

Suppressing the automatic startup of Process Monitoring function

The Process Monitoring function starts automatically when Systemwalker Operation Manager is started up. To suppress the automatic startup of the Process Monitoring function, specify as follows. Your setup is effective in the next startup.

[Windows]

Select **Control Panel** >> **Administrative Tools** >> **Services** and set the following service to "**Manual**" startup.

```
Systemwalker MpPmonO
```

[UNIX]

Definition procedure

1. On the Systemwalker Operation Manager server, open the definition file of the following daemon startup/shutdown command using an editor.

   ```
   /etc/opt/FJSVftlo/daemon/custom/rc3.ini
   ```

2. Edit the definition file as follows.

   Enter character "#" at the beginning of the line where the daemon startup command of the Process Monitoring function is written. This line will be treated as a comment.

   From

   ```
   ...DAEMONnn="/opt/FJSVftlo/pmon/bin/strmppmon"
   ```

To

```
...
#DAEMONnn="/opt/FJSVftlo/pmon/bin/strmppmon"
```

2.14.1.2 Changing the Processes to be Monitored

You can select a process to be monitored by the Process Monitoring function. The following explains the definition file contents and the method to change them.

Changing the process to be monitored

Use the following procedure to change the process to be monitored.

1. Change the definition file.

   Change the definition file of the process to be monitored. The definition file contents and the method to change the contents are explained later.

2. Restart the Process Monitoring function.

   Monitoring of the selected process is enabled only after you have restarted the Process Monitoring function. Restart the function in the following way.

   [Windows]

   - Select **Control Panel** >> **Administrative Tools** >> **Services** and restart the following service.

   ```
   Systemwalker MpPmonO
   ```

   [UNIX]

   1. Stop the Process Monitoring function.

      To do so, issue the following command.

      ```
      /opt/FJSVftlo/pmon/bin/stpmppmon.sh
      ```

   2. Start the Process Monitoring function.

      To do so, issue the following command.

      ```
      /opt/FJSVftlo/pmon/bin/strmppmon.sh
      ```

Definition file

The definition file of the process to be monitored is stored in the following location.

[Windows]

```
Systemwalker Operation Manager installation directory\mpwalker.jm\mpcmtool
\pmon\etc\mppmon.usr
```

[UNIX]

```
/etc/opt/FJSVftlo/pmon/mppmon.usr
```

Contents of the definition file

The definition file has the following contents. Change the set values by referring to the "Set values of the definition file" given below.

```
[Windows] [BASE]

Fujitsu MpWalker ACL Manager=1
```

```
[OMGR]
Fujitsu MpWalker MpJmCal=1
MpNjsosv=1
MpAosfP=1
MpAosfB=1
MpAosfX=1
Fujitsu MpWalker MpJobsch=1
Fujitsu MpWalker MpJmSrv=1
Fujitsu MpWalker MpMjes=1
SystemwalkerMpAHSO=1
```

[UNIX]

```
[BASE]
rc.mpfwsec=1
[OMGR]
S99JMCAL=1
start_jmcmn=1
start_jobs=1
S99MJS=1
```

Set values of the definition file

The following explains the values being set in the definition.

```
[Function category]
Function=Monitoring
```

Function category:

Abbreviated function category

Function:

Abbreviated function name

Monitoring:

0 or 1

0: No process is monitored.

1: The process is monitored and its error is reported if occurred.

For details including the function categories, functions, and processes belonging to functions, see "List of processes to be monitored".

How to change the definition file?

You can change only the values of a process to be monitored. Do not change the function category and the function.

Example:

To release the Calendar function from being monitored in the Windows version, change the definition file as follows.

From

```
[OMGR]
```

```
Fujitsu MpWalker MpJmCal=1
```

To

```
[OMGR]
Fujitsu MpWalker MpJmCal=0
```

Note

Monitoring is not performed for the following functions even if you specify the setting to perform monitoring (monitoring action: "1").

- Functions that have not been installed
- Functions for which the **Startup Type** in the **Services** dialog box has been set to **Manual** or **Disabled** [Windows]
- Functions for which the automatic daemon startup settings have been cleared in the following daemon batch startup customization file [UNIX]:

  /etc/opt/FJSVftlo/daemon/custom/rc3.ini

2.14.1.3 Changing the Definition Information of Process Monitoring Function

The Process Monitoring function is executed according to the definition file contents. You can change the definition file contents when necessary. The following explains the file contents and the method to change them.

Changing the definition information

Use the following procedure to change the definition information of the Process Monitoring function.

1. Change the definition file.

   Change the definition file of the Process Monitoring function. The definition file contents and the method to change the contents are explained later.

2. Restart the Process Monitoring function.

   You need to restart the Process Monitoring function to make the changed definition information effective. Restart the function in the following way.

   [Windows]

   - Select **Control Panel** >> **Administrative Tools** >> **Services** and restart the following service.

   ```
   Systemwalker MpPmonO
   ```

   [UNIX]

   1. Stop the Process Monitoring function.

      To do so, issue the following command.

      ```
      /opt/FJSVftlo/pmon/bin/stpmppmon.sh
      ```

   2. Start the Process Monitoring function.

      To do so, issue the following command.

      ```
      /opt/FJSVftlo/pmon/bin/strmppmon.sh
      ```

Definition file

The definition file of the Process Monitoring function is stored in the following location.

[Windows]

```
Systemwalker Operation Manager installation directory\mpwalker.jm\mpcmtool
\pmon\etc\mppmon.ini
```

[UNIX]

```
/etc/opt/FJSVftlo/pmon/mppmon.ini
```

Contents of the definition file

The definition file has the following contents. Change the set values by referring to the "List of definition items" given below.

```
# Process Monitoring Definition File
#    Systemwalker Operation Manager

[Common]
StartWait=60      # Interval to Start Monitoring
                  # 60-3600 secs is available

CheckWait=60      # Interval of Each Monitoring
                  # (If, Monitor Result is Normal)
                  # 60-3600 secs is available

RetryWait=60      # Interval of Retry Monitoring
                  # (If, Monitor Result is Abnormal)
                  # 60-3600 secs is available

RetryCount=3      # Time to Retry
                  # 3-255 times is available

[Notification]
Destination=
                  # Destination Nodes to Notify
                  # You can direct until 4 nodes, as
                  # "Destination=node1,node2,node3,node4"
                  # If you don't direct any node, we use
                  # System Monitor default notification node
                  # (If System Monitor is running).

MyIPaddr=
                  # IP address of this host.
                  # If you don't direct, we try to find
                  # the one of this host, and use the one
                  # which we find at first.

MpTrap=OFF        # If you want to use Systemwalker Trap,
                  # edit as "MpTrap=ON",
                  # otherwise edit as "MpTrap=OFF"

MpConsole=OFF     # If you want to notify to Systemwalker Console,
                  # edit as "MpConsole=ON",
                  # otherwise edit as "MpConsole=OFF"

MpEvlog=ON        # If you want to output Eventlog,
                  # edit as "MpEvlog=ON",
                  # otherwise edit as "MpEvlog=OFF"

UserOriginal=OFF  # If you want to use your original command,
                  # edit as "UserOriginal=ON",
                  # otherwise edit as "UserOriginal=OFF"

### End of Definition File ###
```

List of definition items

The following lists the definition file items of the Process Monitoring function.

[Common] section

Set value	Description	Initial value	Valid entry
StartWait	Specifies a waiting time (in seconds) until the process monitoring is activated during startup.	60	60 - 3600
CheckWait	Specifies a time interval (in seconds) until the process status check.	60	60 - 3600
RetryWait	Specifies a time interval (in seconds) until the recheck of process error after its first detection.	60	60 - 3600
RetryCount	Specifies a number of times to recheck the process error after its first detection and notification.	3	3 - 255

[Notification] section

Set value	Description	Initial value	Valid entry
Destination (Note 1)	Specifies a node to which a process status error is reported. Up to four (4) nodes can be specified. If omitted, the destination of Systemwalker Centric Manager's system monitoring is used. The destination setup is valid if the Trap Notification function or the Customize Notification command is used. Setup example: Destination=node1,node2,node3	None	Up to 4 nodes separated by a comma from each other
MyIPaddr (Note 1)	Specifies an IP address of the source (local node) which detects and reports a process status error. Use the IP address to identify the fixed source IP if the node has multiple IP addresses. The default is the IP address of the first detected local node.	None	xxx.xxx.xxx.xxx format
MpTrap (Note 1)	Allows the Trap Report function to report an error. It is valid if Systemwalker Centric Manager V10L20/10.1 or later is running at the destination. ON: Enable/OFF: Disable	OFF	ON or OFF
MpConsole (Note 2)	Displays an error report in the dialog of the screen where the Systemwalker Centric	OFF	ON or OFF

Set value	Description	Initial value	Valid entry
	Manager's Systemwalker console is active. ON: Enable/OFF: Disable		
MpEvlog	Outputs an error information to the application log or system log of the detecting source during error detection. ON: Enable/OFF: Disable	ON	ON or OFF
UserOriginal	Executes the Customize Notification command during error detection. ON: Enable/OFF: Disable	OFF	ON or OFF

Note 1:

Trap Report function is valid only when Systemwalker Operation Manager coexists with Systemwalker Centric Manager.

Note 2:

It is valid only when the Systemwalker Centric Manager operation management server coexists.

Executing a specific processing during error detection

If a process error is detected by the Process Monitoring function, the user-defined specific process can be executed.

This process must be written in the Customize Notification command (a batch file or shell script) and the UserOriginal parameter must be turned "ON" in the Notification section of "mppmon.ini" file (the process monitoring definition file) in advance so that the specific processing is executed during an error.

Customize Notification command

[Windows]

```
Systemwalker Operation Manager installation directory\mpwalker.jm\mpcmtool
\pmon\bin\mppmonsnd.bat
```

[UNIX]

```
/opt/FJSVftlo/pmon/bin/mppmonsnd.sh
```

Contents of the command

No commands are executed by default. Write processing in the command, if necessary.

[Windows]

- mppmonsnd.bat

```
@echo off
REM
#############################################################
REM # [Usage]
REM # mppmonsnd.bat %1 %2 %3 %4 %5 %6 %7 %8
REM #
REM # Parameters
REM # %1: Product Information(CMGR 1, OMGR 2)
REM # %2: Error Process Name
REM # %3: IP Address (My Host)
REM # %4: The Number of Destination Hosts
REM # %5: Destination Host1 (if directed at mppmon.ini)
REM # %6: Destination Host2 (if directed at mppmon.ini)
REM # %7: Destination Host3 (if directed at mppmon.ini)
REM # %8: Destination Host4 (if directed at mppmon.ini)
REM
#############################################################

REM # Specify User Original Commands.
REM #
REM # If you want to execute this mppmonsnd.bat, you should edit
REM # mppmon.ini file. you should edit like "UserOriginal=ON" of
REM # [Notification] section. So, in case that some processes of
REM # Systemwalker are in trouble, this mppmonsnd.bat will be
REM # executed.
REM # mppmon.ini is at [INSTALLDIR]\MpWalker.JM\mpcmtool\pmon\
REM #


REM ### End of mppmonsnd.bat ###################################
```

[UNIX]

- mppmonsnd.sh

```
#!/bin/sh
###############################################################
#
# [Usage]
# mppmonsnd.sh $1 $2 $3 $4 $5 $6 $7 $8
#
# Parameters
# $1: Product Information(CMGR 1, OMGR 2)
# $2: Error Process Name
# $3: IP Address (My Host)
# $4: The Number of Destination Hosts
# $5: Destination Host1 (if directed at mppmon.ini)
# $6: Destination Host2 (if directed at mppmon.ini)
# $7: Destination Host3 (if directed at mppmon.ini)
# $8: Destination Host4 (if directed at mppmon.ini)
###############################################################
#

# Specify User Original Commands.
#
# If you want to execute this mppmonsnd.bat, you should edit
# mppmon.ini file. you should edit like "UserOriginal=ON" of
# [Notification] section. So, in case that some processes of
# Systemwalker are in trouble, this mppmonsnd.bat will be
# executed.
# mppmon.ini is at /opt/FJSVftlc[o]/pmon/
#


########### End of mppmonsnd.sh ################################
```

2.14.2 Defining the Collect Maintenance Information Tool

The Collect Maintenance Information tool can collect the information required to take actions against the problem if it has occurred during operation of Systemwalker Operation Manager.

2.14.2.1 Collecting the Maintenance Information During Problem Occurrence

The process of each command provided by the Collect Maintenance Information tool is NOT canceled because those commands do not display nay message box and they do not display any inquiry during their processing.

If a problem has occurred, you can set certain commands of the Collect Maintenance Information tool by linking with the command generation function of Event Monitoring or Process Monitoring. Once set, the inspection data can be collected automatically during problem.

Examples

- Set a command as an action in the function which automatically executes the action when an event (a message) has occurred. If you have set certain commands of the Collect Maintenance Information tool in this command, they are executed automatically when an event has occurred and you can collect the inspection data.

  For the action definition details, refer to the *Systemwalker Operation Manager User's Guide*.

- Using the Systemwalker's Process Monitoring function, you can set certain commands of the Collect Maintenance Information tool to execute during process error detection. Once set, the inspection data is collected immediately when a problem is detected.

  1. Edit the process monitoring definition file (**mppmon.ini**) as follows.

     The Customize Notification command is executed during problem detection.

     ```
     [Notification]
     UserOriginal=ON
     ```

  2. Edit the Customize Notification command ("**mppmonsnd.bat**" (Windows) or "**mppmonsnd.sh**" (UNIX)) of the Process Monitoring function as follows.

     Set the Collect Maintenance Information tool command (**swcolinf**).

     [Windows]

     ```
     swcolinf [/i function-name] /o storage-directory [/c comment]
     ```

     [UNIX]

     ```
     swcolinf [-i function-name] -o storage-directory [-c comment]
     ```

     For the swcolinf command details, refer to the *Systemwalker Operation Manager Reference Guide*.

  For details including the process monitoring definition file and customize notification commands, see "2.14.1.3 Changing the Definition Information of Process Monitoring Function".

2.14.2.2 Setup of Generation Management

When you collect the maintenance information by executing the Collect Maintenance Information tool, you can control the generation of such information for each folder. Three generations of information collection is initially set. You can change the generation count by using its command as follows.

Definition procedure

Execute the command from the command line as follows.

The system administrator (the user belonging to the Administrators group or the superuser) must issue the commands.

[Windows]

```
Systemwalker Operation Manager installation directory \mpwalker.jm
\mpcmtool\swcolinf\swcolinf.exe /w number-of-generations
```

[UNIX]

```
/opt/FJSVftlo/swcolinf/swcolinf -w number-of-generations
```

number-of-generations:

Specifies the number of generations of information to be controlled, using an integer of 1 to 10.

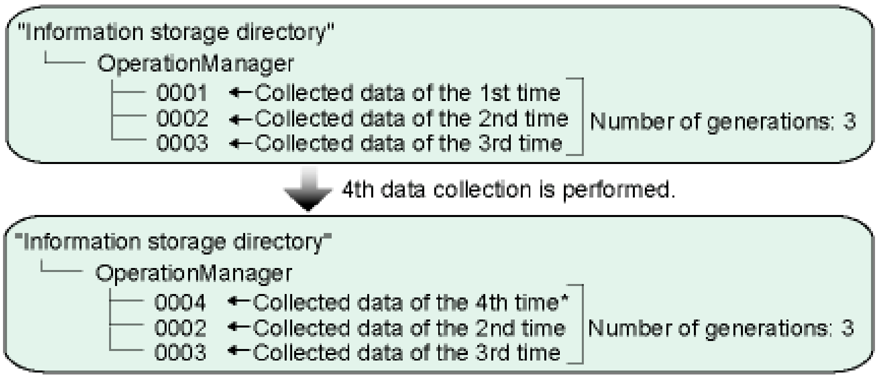
If you do not control the generation of information, set it to 1.

For more information on how to use the command, refer to the *Systemwalker Operation Manager Reference Guide*.

Information

An example directory configuration for generation management

The following gives an example configuration of the information storage directory if you have set "3" generations for information management and if you collect the information using the Collect Maintenance Information tool.



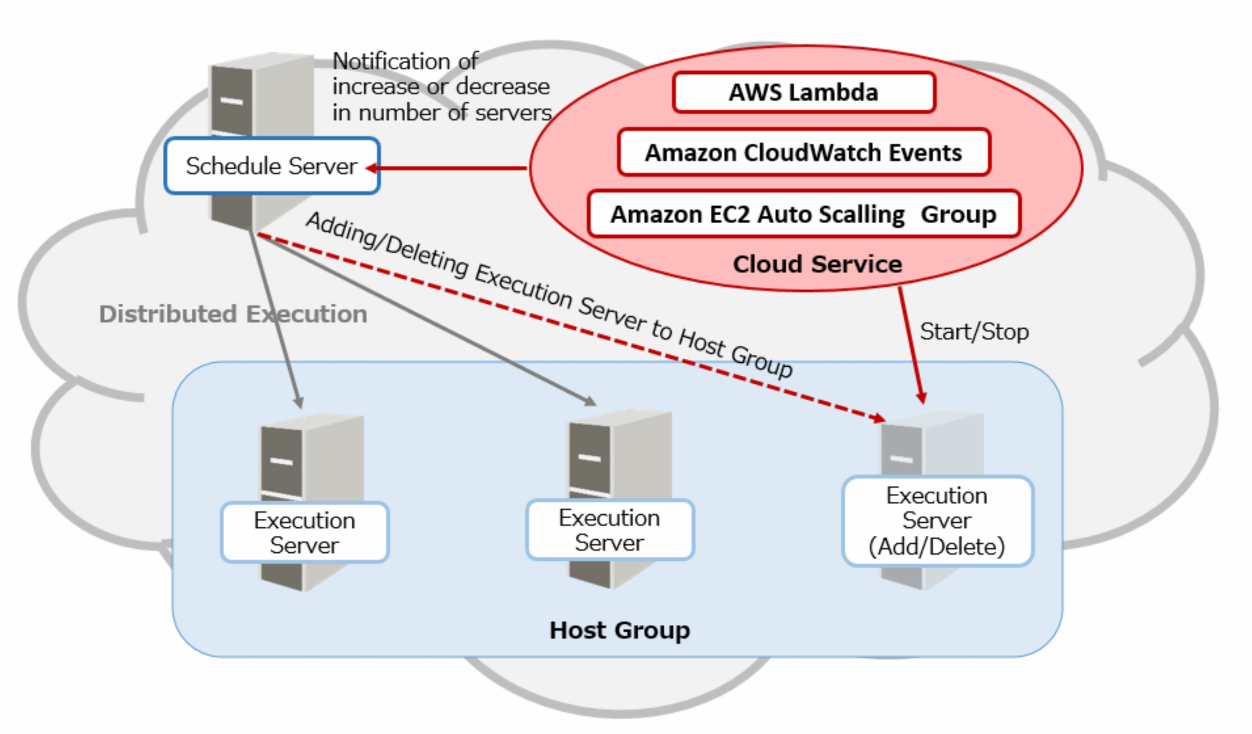
```
"Information storage directory"
  └── OperationManager
        ├── 0001  ←Collected data of the 1st time ┐
        ├── 0002  ←Collected data of the 2nd time │Number of generations: 3
        └── 0003  ←Collected data of the 3rd time ┘

              4th data collection is performed.

"Information storage directory"
  └── OperationManager
        ├── 0004  ←Collected data of the 4th time* ┐
        ├── 0002  ←Collected data of the 2nd time  │Number of generations: 3
        └── 0003  ←Collected data of the 3rd time  ┘
```

2.15 Definitions when linking with Cloud Service to perform distributed execution by using Auto Scaling [Windows] [Linux]

This section explains define how to automatically increase or decrease the number of execution servers in a host group according to workload and resource usagehe when linking with Cloud Service.

2.15.1 Using Amazon Web Service

The configuration for distributed execution using Auto Scaling linking with Amazon Web Service is shown below.


Notification of increase or decrease in number of servers
Schedule Server
AWS Lambda
Amazon CloudWatch Events
Amazon EC2 Auto Scalling Group
Cloud Service
Adding/Deleting Execution Server to Host Group
Distributed Execution
Start/Stop
Execution Server
Execution Server
Execution Server (Add/Delete)
Host Group

Definition procedure

The procedure to build the above configuration are as follows.

In additions, for the detail of the cloud service, refer to the documentation provided from Amazon Web Service.

1. In the Amazon Elastic Compute Cloud (hereinafter referred to as Amazon EC2), set the following to the machine installed the Systemwalker Operation Manager for the execution server.

   - Settings required for distributed execution

     When registering execution users for distributed execution and using distributed execution, define the necessary job execution controls.

     For the detail, refer to the "2.8 Definition of Job Execution Control".

   - Creating multiple subsystem environment (Only using multiple subsystem)

     When using multiple subsystem, create subsystem environment before the following procedure. For setting up multiple subsystem operations, refer to the "2.5 Definition of Multi-Subsystem Operations".

2. In the Amazon EC2, create the Amazon machine image (hereinafter referred to as AMI) for the execution server from the machine of the execution server that set procedure 1.

3. Create "Launch configurations" in the Auto Scaling of the Amazon EC2.

   - For AMI, select the AMI that created in the procedure 2.

   - Set security groups to allow communication between the schedule server and the execution server. For the port number used for two-way communication between the schedule server and the execution server, refer to the "C. 1 Listing of Port Numbers".

4. Create "Auto Scaling Group" in the Auto Scaling of the Amazon EC2.

   - For the launch configurations , select the "Launch configurations" that created in the procedure 3.

   - Set the schedule server and the execution servers of the Auto Scaling group to have private connections.

   - At least one instance must always be running in the Auto Scaling group. Therefore, in the scaling policy, set the minimum size of the instance to be started to 1 or greater.

- Add the End Instance lifecycle hook to the Auto Scaling group so that the instance is not deleted as soon as it is scaled in. Set the pause time for scale-in in the heartbeat timeout for the life cycle hook. If the job running on the execution server does not finish within the set time, it will abend.

5. In the schedule server, create a queue to use the distributed execution. In the configure of the host group to be assigned to the distributed execution queue, register the instance of the Auto Scaling group that you started in step 4 as the configuration host. For an example design of the distributed execution, refer to the "I Want to Automatically Distribute Jobs for Execution on Servers with Low Load" in the *Systemwalker Operation Manager How-To Guide.*

6. In AWS Lambda, create a function that asks the Systmwalker Operation Manager to add/remove a configuration host. The function must be created in the same AWS account and region as the Auto Scaling group. Create a function that execute the following.

   - Determines whether to scale out or scale in from event data sent to AWS Lambda during autoscaling, and extracts instance ID.

     - Determine the scale action type from the "detail-type" value of the event data

       EC2 Instance Launch Successful: scale out

       EC2 Instance-terminate Lifecycle Action: scale in

     - Extracts the instance ID from the value of "EC2InstanceId" in the event data

   - Extracts the host name requested to be added/removed as a distributed execution destination from the target instance ID, and requests to add/remove a configuration host

     - Scale out: Request to Systemwalker Operation Manager to add a configuration host

     - Scale in: Request to Systemwalker Operation Manager to delete a configuration host

   Use the Web API to request the addition or removal of a configuration host. For the how to use Web API, refer to the "Web API [Windows] [Linux]" in the *Systemwalker Operation Manager Reference Guide.*

   Point

   You can specify the multiplicity when you request to add a configuration host. If omitted, multiplicity 10 is set. Set the multiplicity as needed.

7. In the Amazon CloudWatch Events, set the Lambda function to be executed in response to an auto Scaling event. Create the following rules in the Amazon CloudWatch Events. Rules should be created in the same AWS account and region as the Auto Scaling group.

   - Event source

     Service name: Auto Scaling

     Event type: Instance Launch and Terminate

     Specific instance event: select the following

     - EC2 Instance Launch Successful

     - EC2 Instance-terminate Lifecycle Action

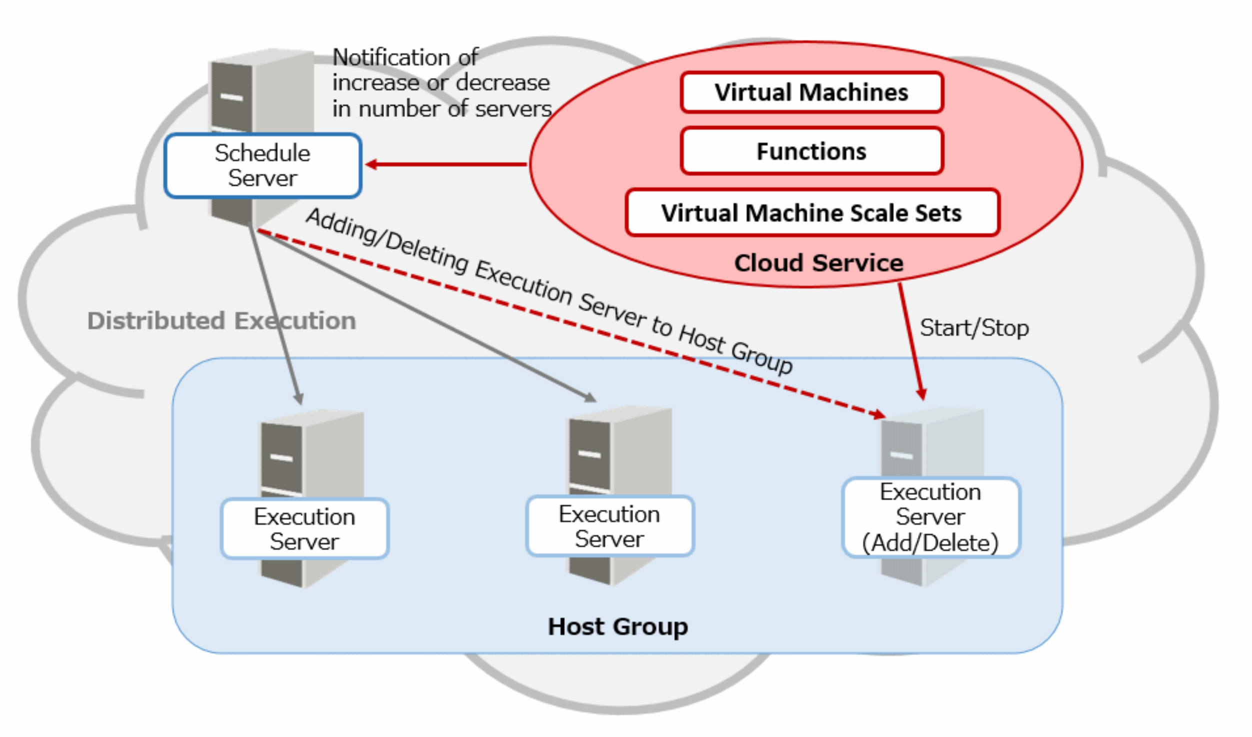
   - Target: Lambda function created in procedure 6

Information

If a running job does not finish within the heartbeat timeout period set in procedure 4 and ends abnormally, review the Auto Scaling group settings and execute the job again.

2.15.2 Using Microsoft Azure

The configuration for distributed execution using Auto Scaling linking with Microsoft Azure is shown below.



Definition procedure

The procedure to build the above configuration are as follows.

In additions, for the detail of the cloud service, refer to the documentation provided frome Microsoft Azure.

1. In the Virtual Machines, set the following to the machine installed the Systemwalker Operation Manager for the execution server.

   - Settings required for distributed execution

     When registering execution users for distributed execution and using distributed execution, define the necessary job execution controls.

     For the detail, refer to the "2.8 Definition of Job Execution Control".

   - Creating multiple subsystem environment (Only using multiple subsystem)

     When using multiple subsystem, create subsystem environment before the following procedure. For setting up multiple subsystem operations, refer to the "2.5 Definition of Multi-Subsystem Operations".

2. In the Virtual Machines, create the image for the execution server from the machine of the execution server that set procedure 1.

3. Create the Virtual Machine Scale Sets

   - For the image, select the image that created in the procedure 2.

   - Set to the same private network as the schedule server.

   - Set the network security groups to allow port communication between the schedule server and execution server using host names. For the port number used for two-way communication between the schedule server and the execution server, refer to the "C.1 Listing of Port Numbers".

   - The initial number of instances must be greater than or equal to 1.

   - Set rules for automatic scaling. The minimum value for a VM must be greater than or equal to 1.

   - Set the "Termination delay (minutes)" in the "Instance termination notification", If a job executed in the Systemwalker Operation Manager does not finish within the specified time, the job will abend.

4. In the schedule server, create a queue to use the distributed execution. In the configure of the host group to be assigned to the distributed execution queue, register the instance of the instance that you started in step 3.

   Set the host group to be assigned to the Distributed Execution QueueRegister the host with the instance that was started in step 3. For an example design of the distributed execution, refer to the "I Want to Automatically Distribute Jobs for Execution on Servers with Low Load" in the *Systemwalker Operation Manager How-To Guide*.

5. In Functions, create a function that executes based on an HTTP request. The function must be created in the same subscription and region as the private network.
   Create the function to execute the following.

   - Analyzes the request for a Webhook notification and determine if notification occurs at scale-in or scale-out timing.

     - Determine the scale action type frome the "operation" of the Request Body value.

   - Processing if a notification occurs during scale-out

     a. Request the schedule server to obtain a list of configuration hosts, and obtain the configuration host list under the host group set in procedure 4 from the response information.

        To request to obtain a list of configuration hosts, use Web API.

     b. Check the provisioning status of the instance in the Virtual Machine Scale Sets. Monitor all instances until the provisioning state is successful.

     c. Obtain the host name list of the virtual machine in the Virtual Machine Scale Sets

     d. Compare the list of host names for the configuration host obtained in step a. with the list of host names obtained in step c, and identify the added host name.

        With using the added host name, request the scheduling server to add the host group you registered in the procedure 4 to the configuration host.

        Use the Web API to request additional configuration hosts.

        Point

        You can specify the multiplicity when you request to add a configuration host. If this option is omitted, multiplicity 10 is set.

        Set the multiplicity as needed.

   - Notification when scaling in

     a. To the schedule server, request a Web API to get a list of configured hosts.

        Use the Web API to request a list of configuration host information.

     b. Check the provisioning state of the instance in Virtual Machines Scale Sets and get the hostname of the virtual machine whose state is Deleting.

     c. Using the host name obtained in step b, request the schedule server to delete the configured hosts of the host group registered in step 4.

        Use the Web API to requests to delete configuration hosts.

   For the how to use Web API, refer to the "Web API [Windows] [Linux]" in the *Systemwalker Operation Manager Reference Guide*.

6. In the Virtual Machine Scale Sets, configure automatic scaling Webhook notification settings. Set the notification recipient to the URL of the function you created in the procedure 5.

Information

If the running job does not finish and will abend within the specified time, "Termination delay (minutes)" in the "Instance termination notification" specified in the procedure 3, review the instance termination notification settings and execute the job again.

Chapter 3 Backing Up or Restoring Operation Environment

Systemwalker Operation Manager provides useful tools and commands to back up and restore user registration information and operation management information for use in the case of its destruction or erroneous deletion of the operation environment.

This chapter provides information on backup and restore procedures.

3.1 Backup

You can save the user registration information, management information (registries) and log information which have been created on the server when Systemwalker Operation Manager is being operated, onto the hard disk using the backup tools (or commands for the UNIX version).

We recommend to back up the information if:

- The definition or setup is changed.
- The operation data is saved.

3.1.1 Notes during Backup

Take the following notes during backup.

- Make a backup in an environment where Systemwalker Operation Manager is operating normally.
- When you start a backup, the Systemwalker Operation Manager services or daemons are stopped automatically. The stopped services or daemons are started up automatically when the backup has completed.
- We recommend to make a backup in the time period when job, job net and group are not executed.
- If a backup is performed while a job, job net or group is being executed and the backup fails (an error message is output), perform the backup again.
- If you make a backup when a job, job net or group is being executed and if you restore its information, its job, job net or group is abnormally terminated with completion code 239.
- If Systemwalker Operation Manager is linked to Systemwalker Centric Manager and Systemwalker Centric Manager is being operated as a cluster system, use the windows indicated below (depending on the cluster system being used) to place the group for Systemwalker Centric Manager offline before backing up:
  - Microsoft(R) Failover Clustering
    - Failover Cluster Manager
- Ensure that the following conditions are the same for both the backup source and the restoration destination:
  - The user names, passwords and user group names that have been registered with the operating system

3.1.2 Backing up the Windows Server Environment

The following explains how to back up the Windows server environment.

Operation procedure

The system administrator (the user belonging to the Administrator group) must back up the Windows server environment on the machine where the Systemwalker Operation Manager server functions have been installed. The following shows the backup procedure.

a. Check the space size of the data save area.

   Make sure that the drive has an enough capacity to save the data.

b. Start the backup.

Use the wizard to back up the Windows server environment as follows.

1. Start the Operation Environment Maintenance wizard.

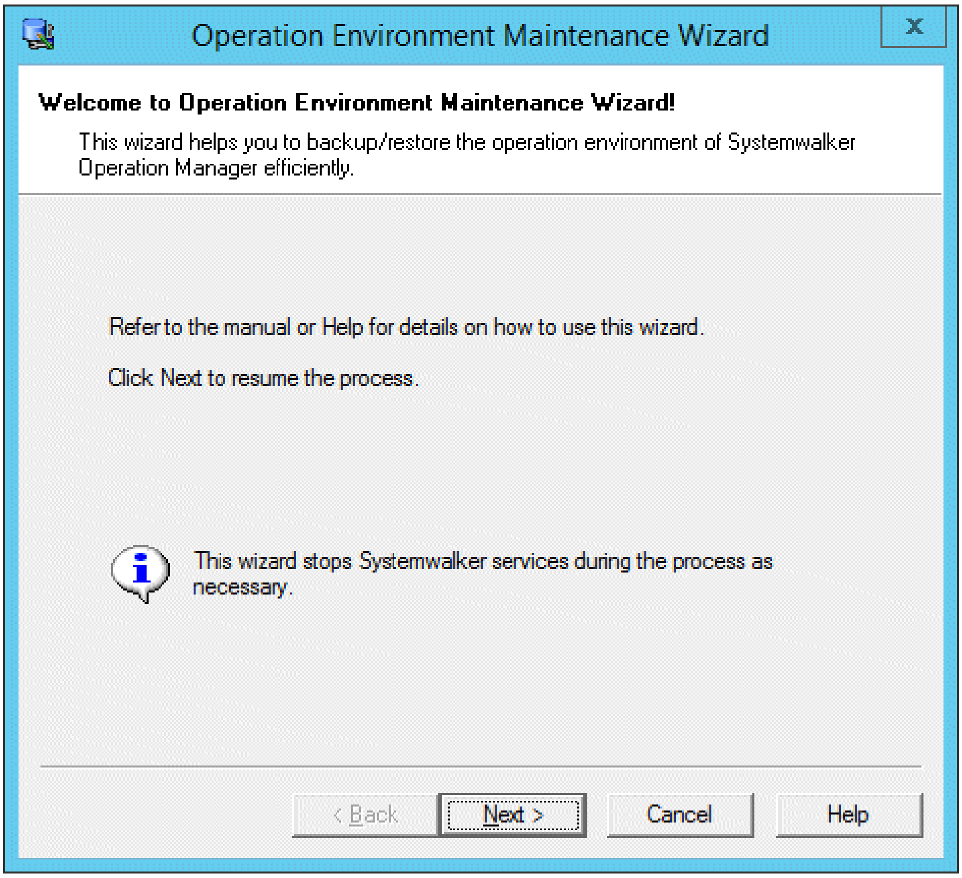
   For environments other than Server Core, select **Start** or **Apps** >> **Systemwalker Operation Manager** >> **Operation Environment Maintenance**.

   For Server Core environments, execute the following command from the command prompt:

   ```
   <Systemwalker Operation Manager installation directory>\mpwalker.jm
   \mpcmtool\common\mpenvset.exe
   ```

   Refer to "mpenvset Operation Environment Maintenance Wizard Startup Command" in the *Systemwalker Operation Manager Reference Guide* for details on the command.

   When the following window appears, confirm the contents and click **Next**.



Operation Environment Maintenance Wizard

Welcome to Operation Environment Maintenance Wizard!

This wizard helps you to backup/restore the operation environment of Systemwalker Operation Manager efficiently.

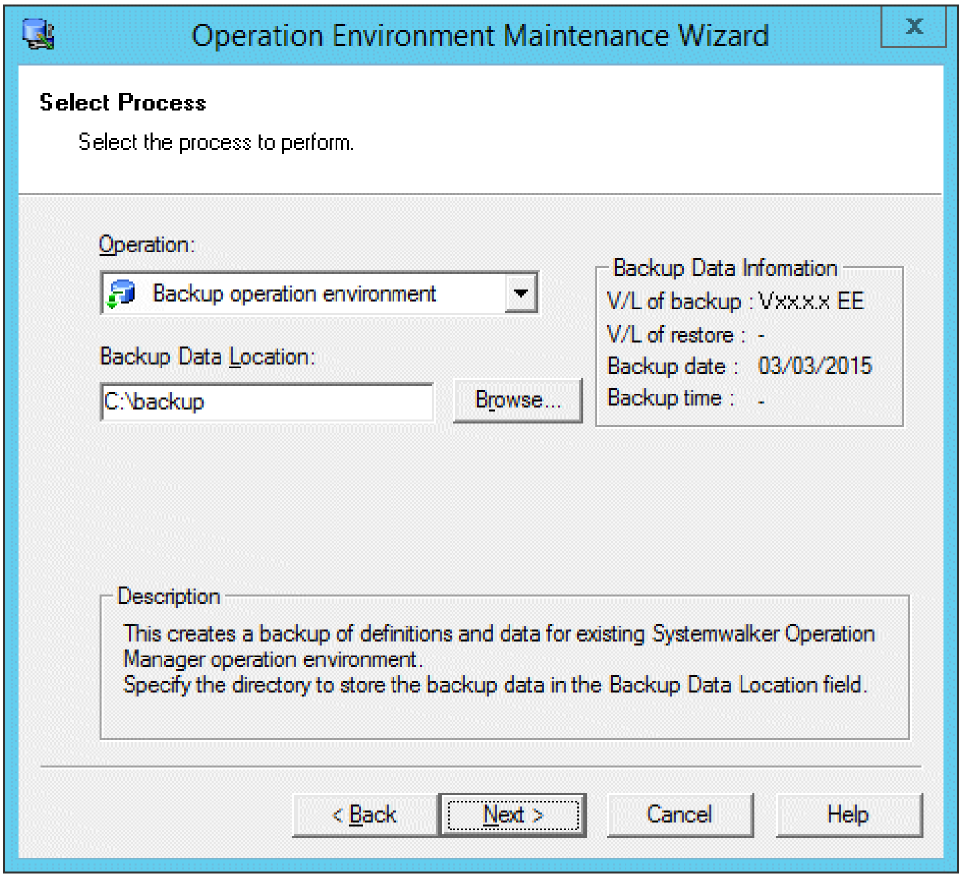
Refer to the manual or Help for details on how to use this wizard.

Click Next to resume the process.

This wizard stops Systemwalker services during the process as necessary.

2. Specify the process type and the save data storage location as follows.

   When the following window appears, select **Backup operation environment**, specify a location to save data, and click **Next**.



Operation Environment Maintenance Wizard

Select Process

Select the process to perform.

Operation: Backup operation environment

Backup Data Location: C:\backup

Backup Data Infomation

V/L of backup : Vx.x.x.x EE

V/L of restore : -

Backup date : 03/03/2015

Backup time : -

Description

This creates a backup of definitions and data for existing Systemwalker Operation Manager operation environment.
Specify the directory to store the backup data in the Backup Data Location field.

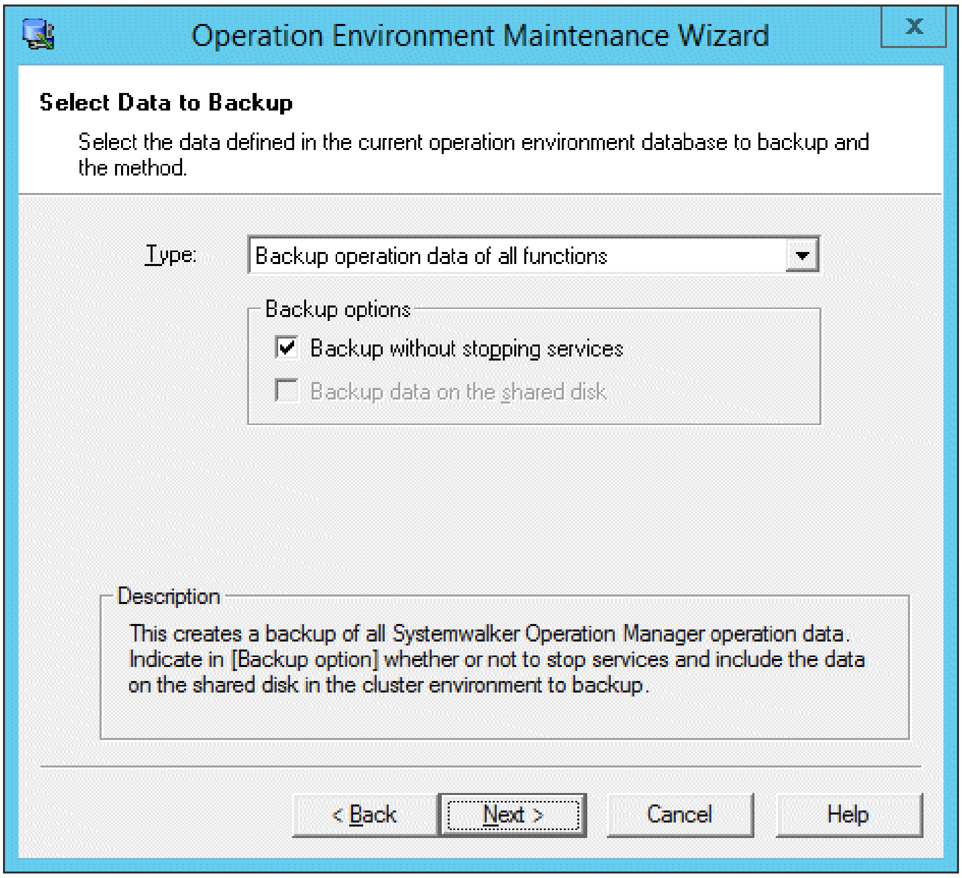
Backup Data Location:

Specify the data save area.

The name of data save area must be up to 32 alphanumeric characters long. No spaces are allowed in this name.

3. Specify how to save the operation data.

   When the following window appears, select the data save options if necessary. Click **Next**.



Select Data to Backup

Select the data defined in the current operation environment database to backup and the method.

Type: Backup operation data of all functions

Backup options

☑ Backup without stopping services

□ Backup data on the shared disk

Description

This creates a backup of all Systemwalker Operation Manager operation data. Indicate in [Backup option] whether or not to stop services and include the data on the shared disk in the cluster environment to backup.

Backup option:

Define the followings.

Backup without stopping services:

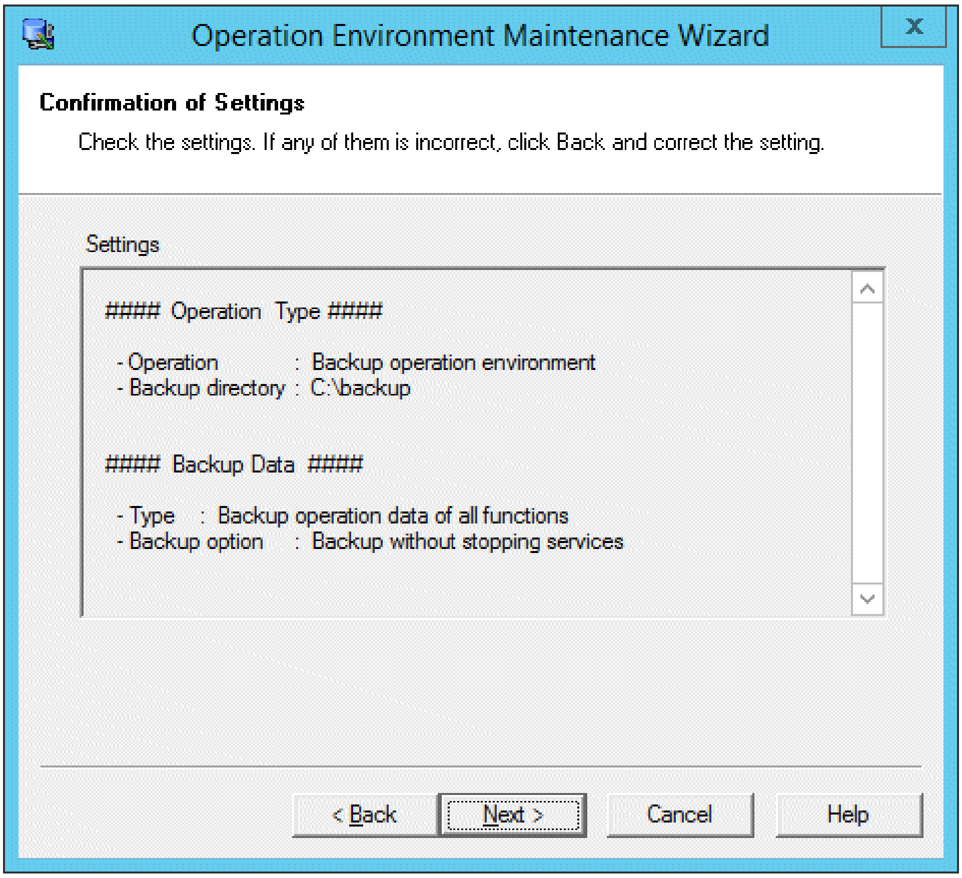
Select this option to make a backup without stopping the services.

Backup data on the shared disk:

This can be selected if the backup is made on an active node of the cluster system. If selected, both the information of the active node and the information of the shared disk are backed up.

4. Confirm your settings.

When the following window appears, confirm your settings. If **OK**, click **Next**.



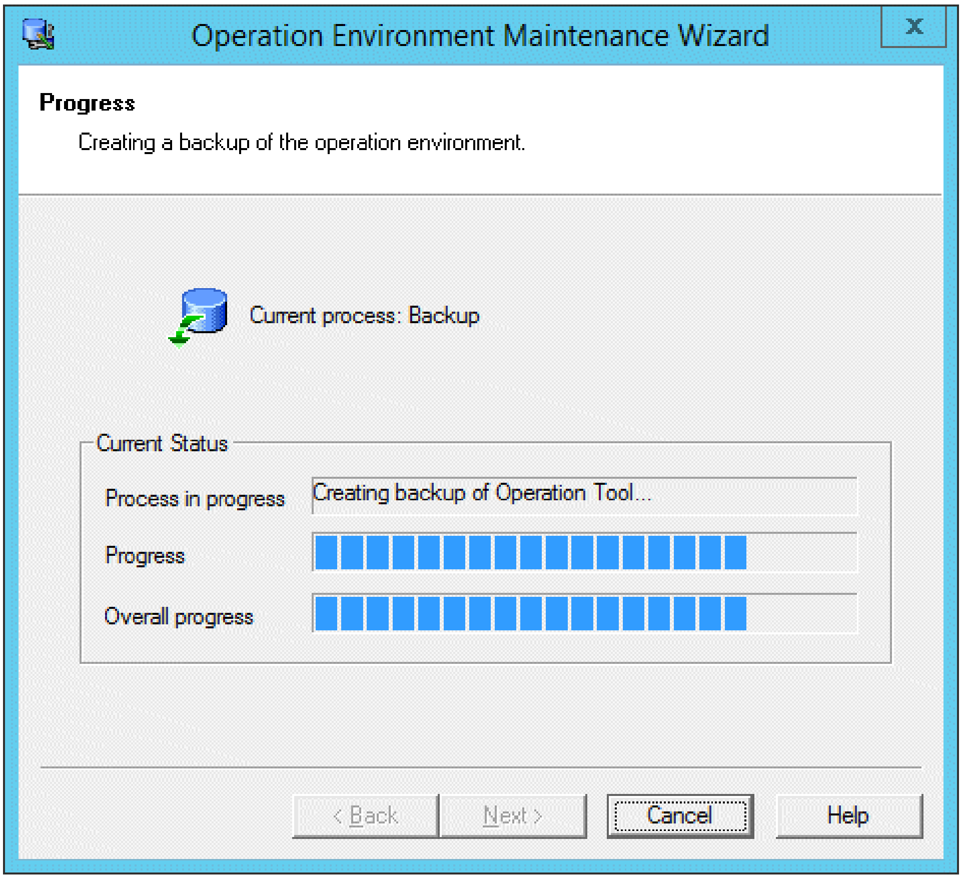
Confirmation of Settings

Check the settings. If any of them is incorrect, click Back and correct the setting.

Settings

```
#### Operation  Type ####

 - Operation          :  Backup operation environment
 - Backup directory  :  C:\backup


#### Backup Data  ####

 - Type    :  Backup operation data of all functions
 - Backup option     :  Backup without stopping services
```

The backup process starts and the following window appears.



Operation Environment Maintenance Wizard

Progress

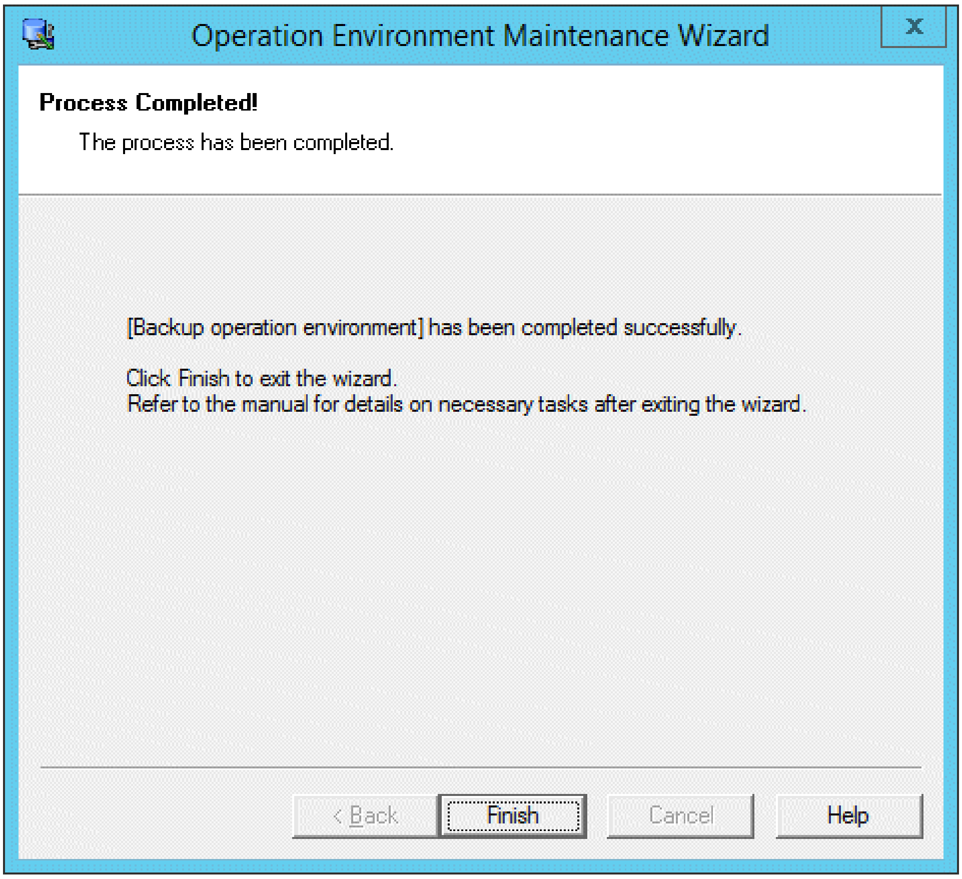
Creating a backup of the operation environment.

Current process: Backup

Current Status

Process in progress: Creating backup of Operation Tool...

When the process completes, the following window appears.



Operation Environment Maintenance Wizard

Process Completed!

The process has been completed.

[Backup operation environment] has been completed successfully.

Click Finish to exit the wizard.
Refer to the manual for details on necessary tasks after exiting the wizard.

The backup process has completed.

3.1.3 acking up the UNIX Server Environment

The following explains how to back up the UNIX server environment.

Operation procedure

The system administrator (the superuser) must back up the UNIX server environment on the machine where the Systemwalker Operation Manager server functions have been installed. The following shows the backup procedure.

1. Check the space size of the data save area.

   Make sure that the drive has an enough capacity to save the data. Use the following calculation as a reference.

   ```
   Total capacity locating under "/etc/opt/FJSV*"
   + Total capacity locating under "/var/opt/FJSV*"
   ```

   where, FJSV* is the package name of a product component.
   This name varies depending on the OS you use. Read it as follows for calculation.

   Solaris, Linux version: FJSV*
   HP-UX version: FHP*
   AIX version: FAIX*

2. Issue the backup command.

   Execute the following command to back up the information.

   ```
   /opt/systemwalker/bin/mpbko -b destination-directory-name
   ```

For the "mpbko" command usage, refer to the *Systemwalker Operation Manager Reference Guide*.

For the information types to be backed up by the mpbko command, see "Appendix A Storage Location of Definition Information Files."

The following gives an example to make a backup in the /var/tmp/OMGRBack directory.

```
/opt/systemwalker/bin/mpbko -b /var/tmp/OMGRBack
```

If the destination directory is not empty, a confirmation message appears.

If you respond with Yes, the existing files are deleted and the backup is made. If you respond with No, the backup process is cancelled.

Note

- Specify this command in the full path name.
- Specify the -SN option to make a backup without stopping the Systemwalker Operation Manager daemons.
- If the backup has failed, take the following actions and rerun the mpbko command.
    - Check that the destination directory has an enough space area.

Information

Registering Jobs

- You can schedule the mpbko command as a job. To do so, always specify the -SN option in the command and ensure that the daemons are not stopped during backup.
- The job nets are held in the status when they are backed up (Active status). If you start the Jobscheduler daemon of the job net which you have backed up after its restoration, it is abended with completion code 239 (Closed).

3.2 Restore

You can save the user registration information and the management information which have been saved by the backup tool (or commands in the UNIX version) using the restore tools (or commands in the UNIX version).

3.2.1 Notes during Restoring

Take the following notes during restoring.

- Make a restore in an environment where Systemwalker Operation Manager is operating normally.
- If you have backed up the data using backup commands or tools in an earlier version/level, you cannot restore it using the restore commands or tools in the current version/level.
- The backup data in a different product (OS type/supported architecture type) cannot be restored.
- The backup data in a different installation drive or directory cannot be restored.
- The Systemwalker Operation Manager services or daemons are stopped automatically during restoring. Automatic start up of the Systemwalker Operation Manager services or daemons when restore is complete differs according to the restore method, as noted below:
    - If you restore using the Operation Environment Maintenance Wizard, the services or daemons are started up automatically when restore is complete.
    - If you restore using the mprso command, the services or daemons are not started up automatically when restore is complete.

- Even if the mprso command is executed, the following data newly added after the backup will not be deleted.
    - Project
    - Holiday calendar
- To make the settings of Job Execution Control valid after restoring, you must restart the system in the Initialization mode. For startup in the Initialization mode, refer to the *Systemwalker Operation Manager Reference Guide*.
- If the Extended User Management function is used in the UNIX version, the data is restored differently according to the enable or disable setup of Extended User Management function.
    - If the Extended User Management function was enabled during the backup, this function is made enable regardless of whether it was enabled or not. Both the Operation Manager user information and the access rights information to the Operation Manager user projects will be restored.
    - If the Extended User Management function was disabled during backup, the Extended User Management function remains disabled regardless of whether it is enabled or disabled during restoring, and the privilege information on the OS user's project access is restored.
- Ensure that the following conditions are the same for both the backup source and the restoration destination:
    - The user names, passwords and user group names that have been registered with the operating system
- The user ID specified as the project owner in the backup source server or the user ID that has been given access privileges to the project must be registered on the restoration destination server. Refer to "mplstacluser Command" in the *Systemwalker Operation Manager Reference Guide* for details on how to check user IDs for which access privileges to the project have been set.
- If Systemwalker Operation Manager is linked to Systemwalker Centric Manager and Systemwalker Centric Manager is being operated as a cluster system, use the windows indicated below (depending on the cluster system being used) to make the group for Systemwalker Centric Manager offline before restoring:
    - Microsoft(R) Failover Clustering
        - Failover Cluster Manager

EE GEE

- If the restore destination environment is not the same as the backup environment, make them the same.

    To restore, the following environments must be the same as the backup environment:

    - Building multiple subsystem environments (subsystem configuration)
    - Building a cluster environment
    - Building the Master Schedule Management function

    If the environments above have been built, it is necessary to ensure that the restore destination is in the same environment as the restore source.

3.2.2 Restoring the Windows Server Environment

The following explains how to restore the Windows server environment.

Operation procedure

The system administrator (the user belonging to the Administrator group) must restore the Windows server environment on the machine where the Systemwalker Operation Manager server functions have been installed. Follow the procedure below.

a. Check the space area size of the drive to restore data.

   The drive must have an enough capacity to store data when restored.

b. Restore the server environment data.

   Use the wizard to restore the data as follows.

1. Start the Operation Environment Maintenance wizard.

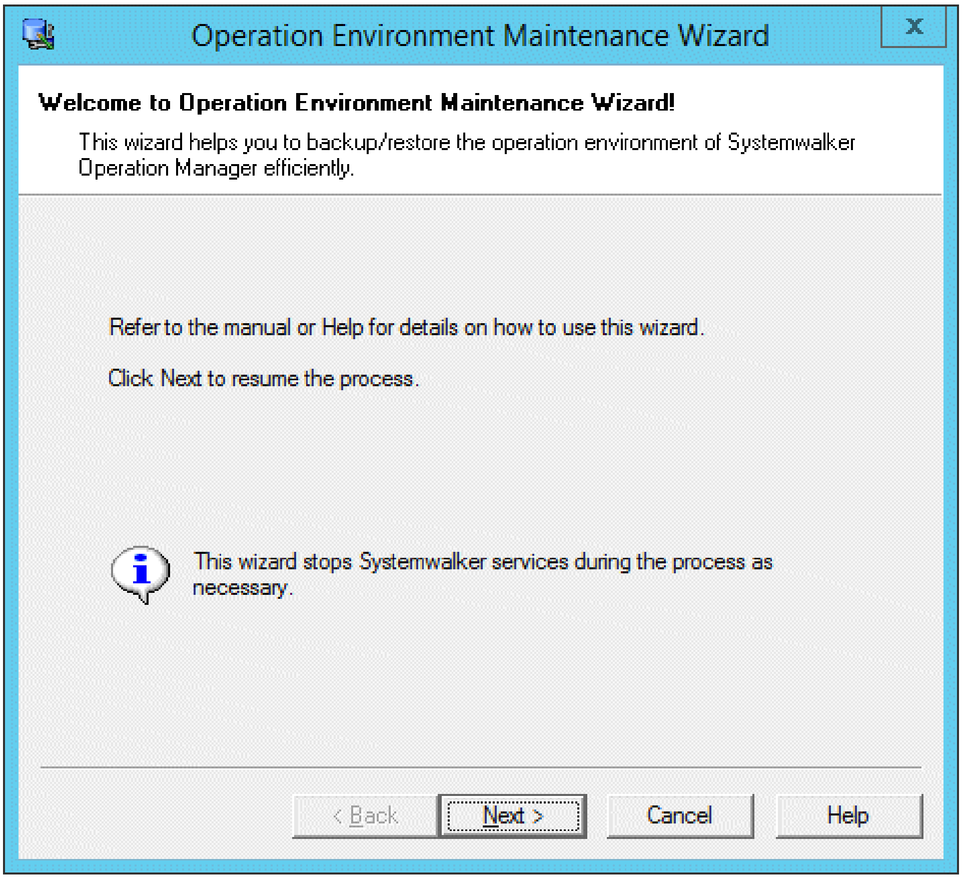
   For environments other than Server Core, select **Start** or **Apps** >> **Systemwalker Operation Manager** >> **Operation Environment Maintenance**.

   For Server Core environments, execute the following command from the command prompt:

   ```
   <Systemwalker Operation Manager installation directory>\mpwalker.jm
   \mpcmtool\common\mpenvset.exe
   ```

   Refer to "mpenvset Operation Environment Maintenance Wizard Startup Command" in the *Systemwalker Operation Manager Reference Guide* for details on the command.

   When the following window appears, confirm the contents and click **Next**.



Operation Environment Maintenance Wizard

Welcome to Operation Environment Maintenance Wizard!

This wizard helps you to backup/restore the operation environment of Systemwalker Operation Manager efficiently.

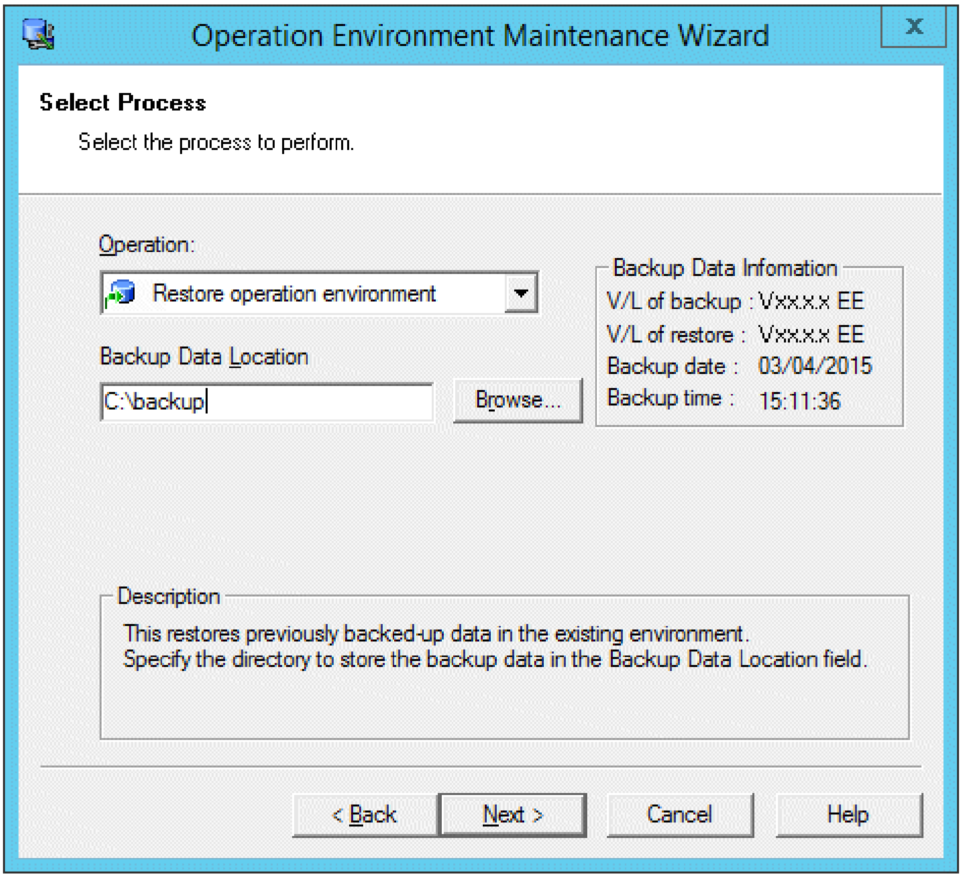
Refer to the manual or Help for details on how to use this wizard.

Click Next to resume the process.

This wizard stops Systemwalker services during the process as necessary.

2. Specify the process type and the restored data storage location as follows.

   When the following window appears, select **Restore Operation Environment**, specify a location to store data, and click **Next**.



Operation Environment Maintenance Wizard

Select Process

Select the process to perform.

Operation: Restore operation environment

Backup Data Location: C:\backup

Backup Data Infomation
V/L of backup : Vxx.x.x EE
V/L of restore : Vxx.x.x EE
Backup date : 03/04/2015
Backup time : 15:11:36

Description
This restores previously backed-up data in the existing environment.
Specify the directory to store the backup data in the Backup Data Location field.

   Backup Data Location:

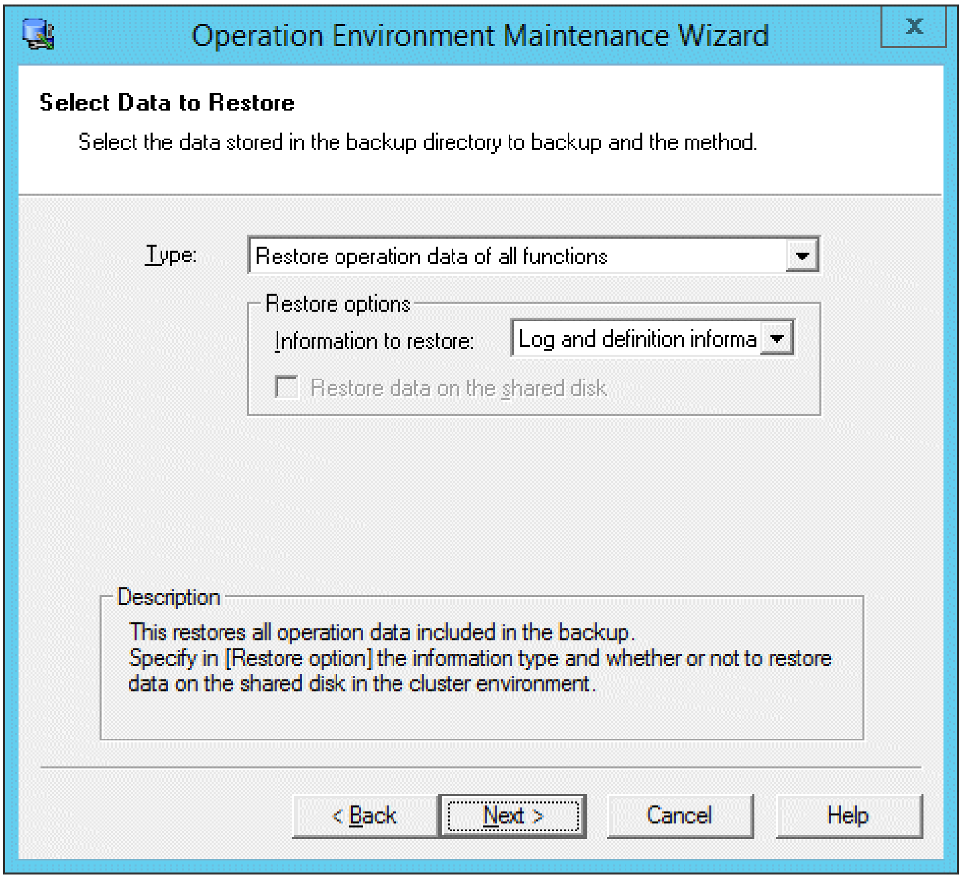
   Specify the backup data location.

   The name of data save area must be up to 32 alphanumeric characters long. No spaces are allowed in this name.

3. Specify how to restore saved data.

   When the following window appears, select how to restore the data and select the information to be restored by the restore options.

Then, click **Next**.



Operation Environment Maintenance Wizard

Select Data to Restore

Select the data stored in the backup directory to backup and the method.

Type: Restore operation data of all functions

Restore options

Information to restore: Log and definition informa

□ Restore data on the shared disk

Description

This restores all operation data included in the backup.
Specify in [Restore option] the information type and whether or not to restore data on the shared disk in the cluster environment.

Restore option:

Define the followings.

Information to restore:

Select either **Log and definition information**, **Log information only** or **Definition information only** for the information to be restored.

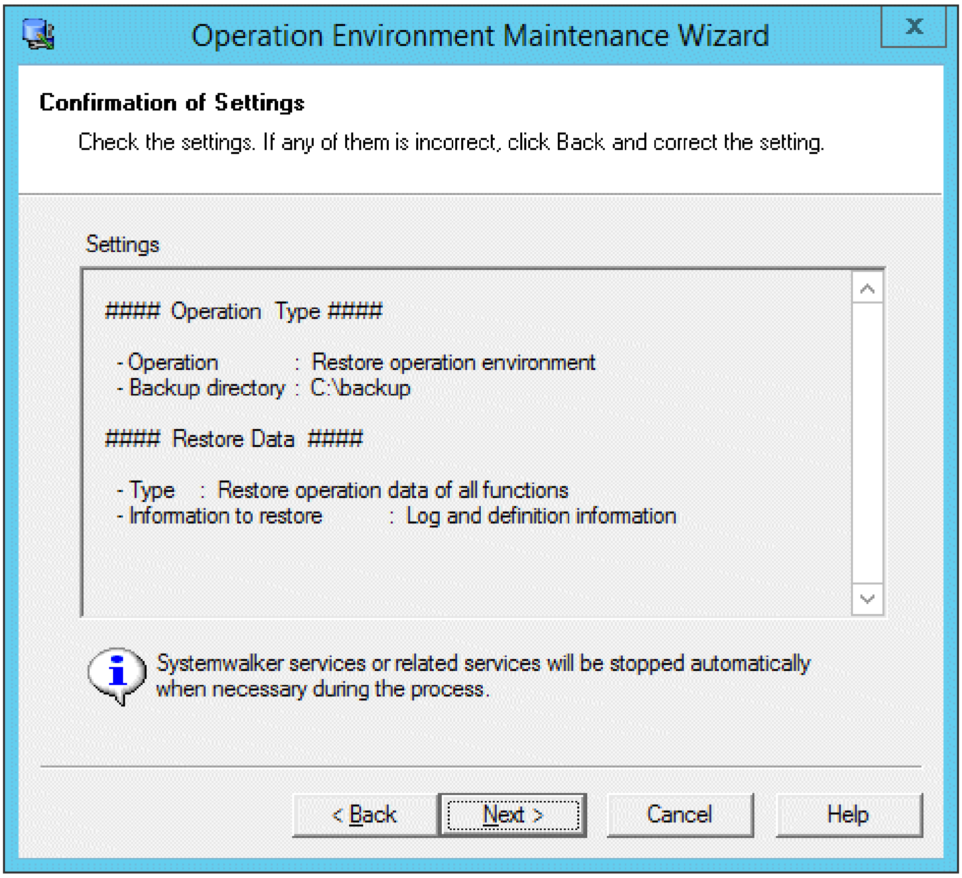
Restore data on the shared disk:

If specified, the information is restored on both the active node and the shared disk.

You can select this option if you have selected the **Backup data on the shared disk** option during backup, if you have collected the data on the shared disk, and if you have specified the data storage location on an active node of the cluster system.

4. Confirm your settings.

   When the following window appears, confirm your settings. If OK, click **Next**.



Operation Environment Maintenance Wizard

Confirmation of Settings

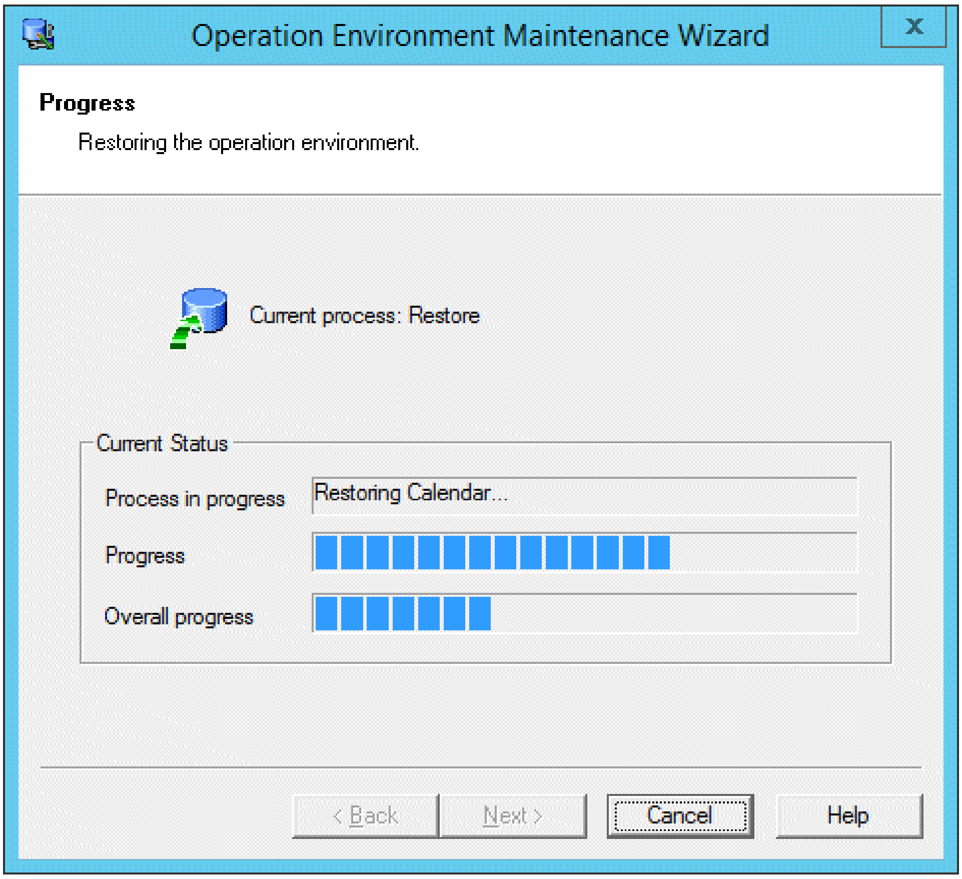
Check the settings. If any of them is incorrect, click Back and correct the setting.

Settings

```
#### Operation  Type ####

 - Operation           :  Restore operation environment
 - Backup directory  :  C:\backup

#### Restore Data  ####

 - Type    :  Restore operation data of all functions
 - Information to restore           :  Log and definition information
```

Systemwalker services or related services will be stopped automatically when necessary during the process.

The backup process starts and the following window appears.



Operation Environment Maintenance Wizard

Progress

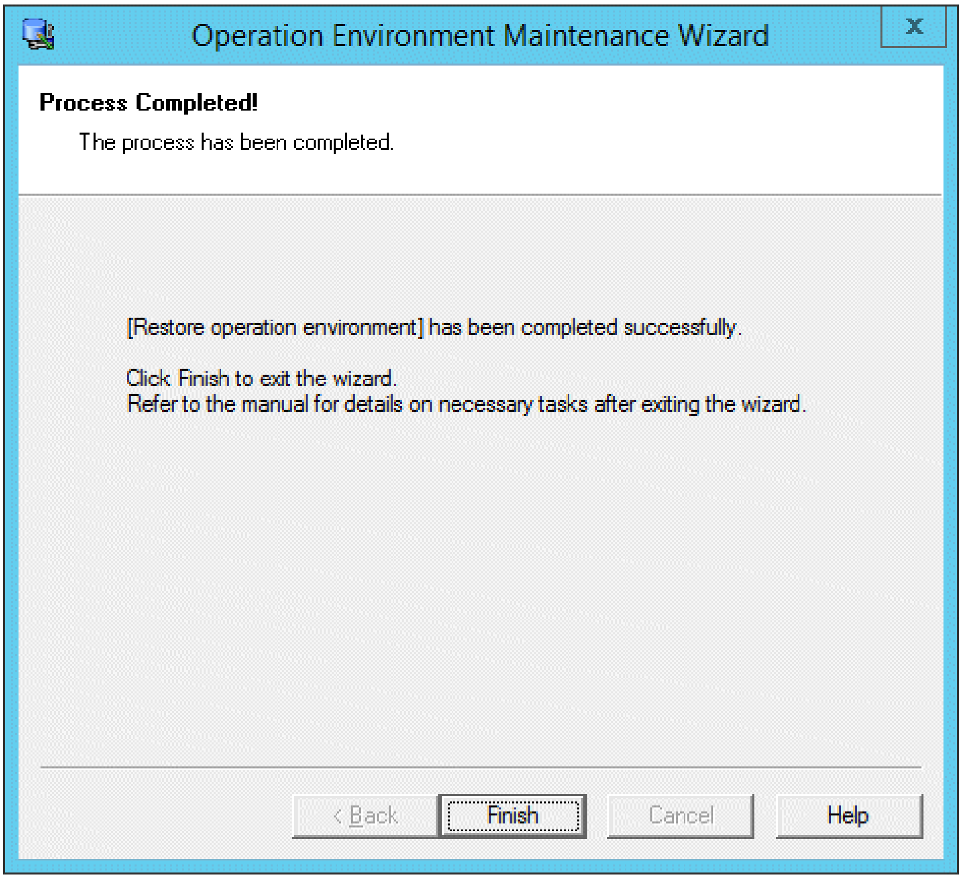
Restoring the operation environment.

Current process: Restore

Current Status

Process in progress: Restoring Calendar...

When the process completes, the following window appears.



Operation Environment Maintenance Wizard

Process Completed!

The process has been completed.

[Restore operation environment] has been completed successfully.

Click Finish to exit the wizard.
Refer to the manual for details on necessary tasks after exiting the wizard.

The restore process has completed.

3.2.3 Restoring the UNIX Server Environment

The following explains how to restore the UNIX server environment.

Operation procedure

The system administrator (the superuser) must restore the UNIX server environment on the computer where the Systemwalker Operation Manager server functions have been installed. Follow the procedure below.

1. Restore the server environment data.

   Execute the following command to restore the backed up data.

   ```
   /opt/systemwalker/bin/mprso -b backup-data-storage-directory-name
   ```

   For the "mprso" command usage, refer to the *Systemwalker Operation Manager Reference Guide*.

   The following gives an example to restore the backed up data in the /var/tmp/OMGRBack directory.

   ```
   /opt/systemwalker/bin/mprso -b /var/tmp/OMGRBack
   ```

2. Start up the Systemwalker Operation Manager daemons.

   Issue the **soperationmgr** command to start up each Systemwalker Operation Manager daemon.

Note

- Specify this command in the full path name.

3.3 Cautions If Systemwalker Centric Manager Coexists

Take the following notes when you back up or restore the server environment data if Systemwalker Operation Manager and Systemwalker Centric Manager coexist.

[Windows version]

- The Systemwalker Centric manager's services stop at the same time in the following cases.
    - When escape option **Backup without stopping services** is not specified before executing backup.
    - When restore is executed.
- If you have changed the settings of Event Monitoring functions or Action Management functions, back up the environment information of both Systemwalker Operation Manager and Systemwalker Centric Manager even when you have changed only the settings of either Systemwalker Operation Manager or Systemwalker Centric Manager.

Information

If Systemwalker Operation Manager and Systemwalker Centric Manager coexist in the same environment, you can schedule the backup command of Systemwalker Centric Manager by using the Jobscheduler. For information on the backup command of Systemwalker Centric Manager, refer to the *Systemwalker Centric Manager Reference Guide*.

Appendix A Storage Location of Definition Information Files

This appendix shows where Systemwalker Operation Manager environment definition information and operation management information definition files are stored.

You can back up these definition information files using the backup tools (the Operation Environment Maintenance wizard in the Windows system, or the **mpbko** command in the UNIX system).

For the backup procedure, see "Chapter 3 Backing Up or Restoring Operation Environment."

A.1 Common Function Information

The information common to each function (or the common function information) is stored in the following location.

[Windows version]

```
<Systemwalker Operation Manager installation directory>
 |_ MpWalker.JM
    |_ mpjmsrv
      |_ etc
         |- monitor_hosts_ex <- Definition information for monitored hosts (DEFAULT)
         |- *.mhz            <- Definition information for monitored hosts
         |_ OMGRev.txt       <- Common parameter information
```

[UNIX version]

```
<Directory specific for each OS> (Notes)
 |_ etc
    |- monitor_hosts_ex   <- Definition information for monitored hosts (DEFAULT)
    |- *.mhz             <- Definition information for monitored hosts
    |_ OMGRev.txt        <- Common parameter information
```

Notes:

The "Directory specific for each OS" in this section are as follows

Solaris	/var/opt/FJSVJMCMN
HP-UX version	/opt/FHPJMCMN/db
AIX version	/usr/FAIXJMCMN/db
Linux	/var/opt/FJSVJMCMN

A.2 Calendar and Power Control Information

The information about the Calendar function and the Power Control function (or the Calendar and Power Control information) is stored in the following location.

[Windows version]

```
<Systemwalker Operation Manager installation directory>
|- MpWalker
| |_ mpaosfsv
|    |_ ini
|        |_ *       <- Definition files for starting services and applications
|_ MpWalker.JM
   |_ mpjmcal
      |- caldb
      | |_ *        <- Definition files for calendars and power control
      |_ etc
         |_ *        <- Definition files for calendars (for clusters)
```

[UNIX version]

```
<Directory specific for each OS> (Notes)
  |- caldb
  | |- *         <- Definition files for calendars and power control
  | |_ old_back
  |    |_ *      <- Definition files for calendars
  |- srvapp
  | |_ *         <- Definition files for starting applications
  |_ etc
     |_ *         <- Definition files for calendars (for clusters)
```

Notes:

The "Directory specific for each OS" in this section are as follows

Solaris	/var/opt/FJSVjmcal
HP-UX version	/opt/FHPjmcal
AIX version	/opt/FAIXjmcal
Linux	/var/opt/FJSVjmcal

A.3 Jobscheduler Information

Information on the Jobscheduler functions to be backed up by the backup tool (the **mpbko** command in the UNIX system) is classified into the following three categories.

- Jobscheduler information
- Access Control information set for the project and Operation Manager user information
- Exit file

Each category is described below.

Jobscheduler information

The Jobscheduler information is stored in the following location.

[Windows version]

```
<Systemwalker Operation Manager installation directory>
  |_ MpWalker.JM
     |_ mpjobsch
        |- jobdb   (Note 1)
        | |- *.jsp                 <- Project information
        | |- *.dbz                 <- Job net information
        | |- *.grz                 <- Group information
        | |- sysfile.sys                <- System information
        | |- db_calendar_ex.default     <- Schedule pattern information
        | |- msm.db
        | | |_ access_hosts            <- Monitoring permission host information
        | |- jobschprop
        | | | *.prm              <- Job parameter information
        | | |_*.tpr              <- Job parameter information
        | |- jobschtvr
        | | | *.tvr             <-Job net variable information
        | | |_*.tvh             <-Job net variable information
        | |- *.log                  <- Log information
        | |_ sroot.var              <- Job definition variable information
        |_ etc
            |_ jobschev.txt (Note 2)    <- Startup parameter information
```

[UNIX version]

```
<Directory specific for each OS> (Note 3) (Database directory)
 |_ (JOBDBn)  (Note 4)
     |- *.jsp                         <- Project information
     |- *.dbz                         <- Job net information
     |- *.grz                         <- Group information
     |- sysfile.sys                   <- System information
     |- db_calendar_ex.default        <- Schedule pattern information
     |- msm.db
     |   |_ access_hosts             <- Monitoring permission host information
     |- jobschprop
     |   | *.prm              <- Job parameter information
     |   |_*.tpr              <- Job parameter information
     |- jobschtvr
     |   | *.tvr             <-Job net variable information
     |   |_*.tvh             <-Job net variable information
     |- etc
     |  |_ jobschev.txt              <- Startup parameter information
     |- sroot.var                     <- Job definition variable information
     |_ *.log                         <- Log information
```

Note 1

This becomes "jobdb*n*" when a multi-subsystem environment exists. "*n*" indicates a subsystem number.

Note 2

This becomes "jobschev*n*.txt" when a multi-subsystem environment exists. "*n*" indicates a subsystem number.

Note 3

The "Directory specific for each OS" in the UNIX version are as follows

Solaris	/var/opt/FJSVJOBSC
HP-UX version	/opt/FHPJOBSCH/db
AIX version	/usr/FAIXJOBSC/db
Linux	/var/opt/FJSVJOBSC

Note 4

This is stored under the "JOBDB*n*" when a multi-subsystem environment exists. The "*n*" in "JOBDB*n*" indicates a subsystem number. When a multi-subsystem environment does not exist, it is stored under a "Directory specific for each OS".

Access Control information set for the project and Operation Manager user information

The Access Control information and Operation Manager user information are stored in the following location.

[Windows version]

```
<Systemwalker Operation Manager installation directory>
  |_ MpWalker
     |_ mpaclmgr
        |_ config
           |_ JM
              |_ *      <- Access control information files
```

[UNIX version]

```
var
 |_ opt
    |_ FJSVfwseo   (Notes)
       |_ config
          |_ JM
```

```
             |_ *     <- Access control information files
                           Operation Manager user information
```

Notes:

"FJSVfwseo" should be read as "FJSVfwsec" if:

- The same version of Systemwalker Centric Manager is installed after Systemwalker Operation Manager has been installed, or
- A newer version of Systemwalker Centric Manager is installed when Systemwalker Operation Manager is installed (in any sequence of their installation).

Exit file

The exit file is stored in the following location.

[Windows version]

```
<Systemwalker Operation Manager installation directory>
  |_ MpWalker.JM
     |_ bin
        |- *exit.bat      <- Exit files
        |- *exit.exe      <- Exit files
        |- *exitex.bat    <- Exit files
        |_ *exitex.exe    <- Exit files
```

Notes:

If the file name identified by an asterisk (*) is one of the followings, it can be backed up by the backup tool.

- "normal"
- "jobsch"
- "job"
- "jobdb"
- "time"
- "jobschend"
- "jobschnoend"
- "startlate"
- "endlate"

[UNIX version]

```
<Directory specific for each OS> (Notes)
    |_ bin
       |- *.exit          <- Exit files
       |_ *.exit.normal   <- Exit files
```

Notes:

The "Directory specific for each OS" in this section are as follows.

Solaris	/opt/FJSVJOBSC
HP-UX version	/opt/FHPJOBSCH
AIX version	/usr/FAIXJOBSC
Linux	/opt/FJSVJOBSC

A.4 Job Execution Control Information

The Job Execution Control information is stored in the following location.

[Windows version]

Files

```
<Systemwalker Operation Manager installation directory>
  |_ MpWalker.JM
     |_ mpmjessv
        |- mjespool
        | |_ *              <- Spools
        |- mjsinfo
        | |- jfinfo         <- Job folder definition file
        | |_ jnuinfo        <- Job owner information file
        |_ user (User environment definition information directory)
           |- initfile.txt   <- Initialization file
           |- nodemap        <- Node name definition file
           |- mjhosts        <- Trusted host definition file
           |_ mjsubsysname.txt <- Execution subsystem name definition file
```

Registry

```
\\HKEY_LOCAL_MACHINE
 |_ \SOFTWARE
    |_ \Fujitsu
       |_ \MpWalker
          |_ \CurrentVersion
             |_ \MpMjes      <- Everything under the MpMjes key
```

[UNIX version]

```
etc
|_ mjes (Operation information directory)
   |- initfile    <- Initialization file
   |- mjhosts     <- Trusted host definition file
   |- nodemap     <- Node name definition file
   |_ mjsubsysname.txt <- Execution subsystem name definition file

var
|_ spool
   |_ mjes (Spool directory)
      |- mjespool     <- Spool
      |_ mjsinfo
         |_ jfinfo    <- Job folder definition file
```

Note 1

The spool directory is NOT backed up if the **Backup without stopping services** option is selected in the Windows system or if the **-SN** option of **mpbko** command is specified in the UNIX system during backup.

EE

Note 2

When connected to the server during Multi-subsystem operation, the definition files are stored in the following locations.

[Windows version]

Systemwalker Operation Manager installation directory
\MpWalker.JM\mpmjessv\mjes*n*

[UNIX version]

Initialization file and trusted host definition file:

Under /etc/mjes/mjes*n*

Spools and job folder definition file:

Under /var/spool/mjes/mjes*n*

The "*n*" in "mjes*n*" indicates a subsystem number.

A.5 Event Monitoring and Action Management Information [Windows version]

The information about Event Monitoring and Action Management functions is installed in the following locations.

```
<Systemwalker Operation Manager installation directory>
  |_ MpWalker
     |_ mpaosfsv
        |_ base
           |- etc
           | |_ *   <- Information relating to events and actions
           |_ temp
              |_ *   <- Information relating to events and actions
```

A.6 Task Linking Information

The Task Linking information is stored in the following location.

[Windows version]

```
<Systemwalker Operation Manager installation directory>
  |_ MpWalker.JM
     |_ mpnjsosv
        |_ manage
           |- hostinfo.ini   <- Host information definition file
           |_ *.ini          <- Password management book files
```

[UNIX version]

```
<Directory specific for each OS> (Notes)
  |_ manage
     |- hostinfo.ini   <- Host information definition file
     |_ *.ini          <- Password management book files
```

Notes:

The "Directory specific for each OS" in this section are as follows.

Solaris	/opt/FJSVsnjss
HP-UX version	/opt/FHPsnjss
AIX version	/opt/FAIXsnjss
Linux	/opt/FJSVsnjss

EE

A.7 Information Relating to Master Schedule Management Function

This section describes the storage directories for information relating to the Master Schedule Management function.

The following information is backed up by the mpbko command and restored by the mprso command when the Master Schedule Management function is enabled.

If the Operation Management Server is used

[Windows version]

```
<Systemwalker Operation Manager installation directory>
  |_ mpwalker.jm
     |_ mpstemsv
        |- stemDBn             (Note 1) (Database directory)
        | |- etc
        | | |_ stemmanager.ini            <- Schedule environment settings file
        | |
        | |- stemmanager.db              <- Schedule status database
        | |- *.lst                       <- Carry-over status files
        | |- change_master.log           <- Operation change log file
        | |- project
        | | |- *.org                      <- Project control statements (registered)
        | | |_ *.err                    <- Project control statements (error information)
        | |- rcv
        | | |- *.log                     <- Schedule application databases
        | | |- *.exc                     <- Project control statements
        | | |- *.lst                     <- Distribution file lists
        | | |- *.dbz,*.grz               <- Schedule files
        | | |- work
        | | | |- yyyymmdd.dat  (Note 2)  <- Schedule submission list files
        | | | |_ yyyymmdd.loc  (Note 2)  <- Carry-over monitoring files
        | | |_ jobschpropmmdd     (Note 2)
        | |    |_ *.prm                  <- Job parameter information
        | |- snd                         <- Distribution-related information
        | |- log
        | | |_ *.log                     <- Trace information
        | |- Start_Check.log             <- Carry-over log file
        | |_ move
        |    |_ *.dbz,*.grz,*.jsp,*.prm  <- Backup schedule files
        |- stem.ini                  <- Environment configuration definition file
        |_ log
           |_ *.log                      <- Trace information

<Systemwalker Operation Manager installation directory>
  |_ mpwalker.jm
     |_ mpjobsch
        |_ jobdb       (Note 3)
           |_ jobschbackup2                 <- Operation change backup information
```

Note 1

"*n*" indicates a subsystem number (an integer of 0 to 9).

Note 2

yyyymmdd (year-month-day) and mmdd (month-day) contains the figures of date.

Note 3

This becomes "jobdb*n*" when a multi-subsystem environment exists.

The "*n*" indicates a subsystem number (1 to 9).

[UNIX version]

```
/var/opt/FJSVstem
  |- stemDBn           (Note 1) (Database directory)
  | |- etc
  | | |- stemmanager.ini       <- Schedule environment settings file
  | | |_ schedule_hosts        <- Schedule server list file
  | |- stemmanager.db          <- Schedule status database
  | |- *.lst                   <- Carry-over status files
  | |- change_master.log       <- Operation change log file
  | |- project
  | | |- *.org             <- Project control statements (registered)
  | | |_ *.err             <- Project control statements (error information)
  | |- rcv
  | | |- *.log             <- Schedule application databases
  | | |- *.exc             <- Project control statements
  | | |- *.tar             <- .tar files for distribution
  | | |- *.lst             <- Distribution file lists
  | | |- *.dbz,*.grz       <- Schedule files
  | | |_ work
  | |    |- yyyymmdd.dat (Note 2)   <- Schedule submission list files
  | |    |_ yyyymmdd.loc (Note 2)   <- Carry-over monitoring files
  | |- snd                  <- Distribution-related information
  | |- log
  | | |_ *.log              <- Trace information
  | |- Start_Check.log      <- Carry-over log file
  | |_ move
  |    |_ *.dbz,*.grz,*.jsp,*.prm     <- Backup schedule files
  |- stem.ini                         <- Environment configuration definition file
  |_ log
     |_ *.log               <- Trace information

<Directory specific for each OS> (Note 3)
  |_ (JOBDBn)               (Note 4)
     |_ jobschbackup2        <- Operation change backup information
```

Note 1

"*n*" indicates a subsystem number (an integer of 0 to 9).

Note 2

yyyymmdd (year-month-day) and mmdd (month-day) contains the figures of date.

Note 3

With the UNIX version, "Directory specific for each OS" refers to the following directories.

Solaris version	/var/opt/FJSVJOBSC
HP-UX version	/opt/FHPJOBSCH/db
AIX version	/usr/FAIXJOBSC/db
Linux version	/var/opt/FJSVJOBSC

Note 4

This is stored under the "JOBDB*n*" when a multi-subsystem environment exists. The "*n*" in "JOBDB*n*" indicates a subsystem number (1 to 9). When a multi-subsystem environment does not exist, it is stored under a "Directory specific for each OS".

If the Schedule Server is used [UNIX version]

```
/var/opt/FJSVstem
  |- stemDBn       (Note 1) (Database directory)
  | |- etc
  | | |_ stemmanager.ini            <- Schedule environment settings file
  | |- *.lst                        <- Carry-over status files
  | |- rcv
  | | |- *.log                      <- Schedule application databases
  | | |- *.exc                      <- Project control statements
  | | |- *.tar                      <-.tar files for distribution
  | | |- *.lst                      <- Distribution file lists
  | | |- *.dbz,*.grz                <- Schedule files
  | | |_ work
  | |    |- yyyymmdd.dat (Note 2)    <- Schedule submission list files
  | |    |_ yyyymmdd.loc (Note 2)    <- Carry-over monitoring files
  | |- log
  | | |_ *.log                       <- Trace information
  | |- Start_Check.log               <- Carry-over log file
  | |_ move
  |    |_ *.dbz,*.grz,*.jsp,*.prm    <- Backup schedule files
  |- stem.ini                         <- Environment configuration definition file
  |_ log
     |_ *.log                        <- Trace information
```

Note 1

"*n*" indicates a subsystem number (an integer of 0 to 9).

Note 2

yyyymmdd (year-month-day) and mmdd (month-day) contains the figures of date.

Appendix B Definition of Operating Information in a File

This appendix explains how to edit operating information definitions directly in a text file.

B.1 Initialization File (Job Execution Control)

The initialization file of Job Execution Control has been stored in the following location as a text file.

You can directly edit this file using an editor such as "vi" or Notepad.

However, NEVER change the file path and the file name.

File name:

[Windows version] initfile.txt

[UNIX version] initfile

Storage path:

[Windows version]

Systemwalker Operation Manager installation directory\MpWalker.Jm\mpmjessv\user

EE

The followings apply if Multi-subsystem operations are supported.

Subsystem number 0:

Same as when NO subsystem operations are supported.

Subsystem numbers 1 to 9:

Directory where Systemwalker Operation Manager has been installed \MpWalker.Jm\mpmjessv\mjesn\user, where "*n*" is a subsystem number.

[UNIX version]

/etc/mjes

EE

The followings apply if Multi-subsystem operations are supported.

Subsystem number 0:

Same as when NO subsystem operations are supported.

Subsystem numbers 1 to 9:

/etc/mjes/mjes*n*, where "*n*" is a subsystem number.

Coding format

The following shows the standard coding format of the initialization file. For the detailed parameter and operand information, see "B.1.1 List of Initialization File Definitions".

[Windows version]

```
system [dfltqueue=queue name,]
        maxexec=job multiplexity in the system[,
        dfltprty=default job priority]
queue name=queue name,
        maxexec=job multiplexity in the queue[,
        dfltprty=default job priority][,
        limittime=Job running time limit][,
        maxjob=max submit jobs][,
        dfltdprty=default job execution priority][,
        host=host group name]
hostgrp name=host group name,
        host=(host name (max execution)[, ...])
prt printer name=alias
        fontname=font name, fontsize=fontsize][,
        orient={port|land}][,
        form=paper size]
log path=path name[,
        keepdays=retention]
record path=path name[,
        keepdays=retention]
execasuser
convert
qinactive
namechk
scriptnocopy
clusterip ipaddress
jclexitcode
jclstdout
distexec
qstop
networkretry interval = retry interval,retry = number of retries
```

[UNIX version]

```
system [dfltqueue=queue name,]
        maxexec=job multiplexity in the system[,
        dfltprty=default job priority]
queue name=queue name,
        maxexec=job multiplexity in the queue[,
        dfltprty=default job priority][,
        limittime=Job running time limit][,
        maxjob=max submit jobs][,
        dfltdprty=default job execution priority][,
        host=host group name]
hostgrp name=host group name,
        host=(host name (max execution)[, ...])
log path=path name[,
        keepdays=retention]
record path=path name[,
        keepdays=retention]
convert
qinactive
namechk
scriptnocopy
clusterip ipaddress
jclexitcode
jclstdout
qstop
networkretry interval = retry interval,retry = number of retries
```

Syntax rules

The following syntax rules apply to the initialization file description.

- Only a space or spaces can be entered before a parameter.
- Only a single parameter is allowed on a single line.
- If a parameter definition continues onto the next line or lines, the subsequent line must end with a comma (,) as the delimiter.

- One or more spaces are required between a parameter and its operand.
- No blank space is allowed before and after an equal sign (=).
- Multiple operands must be separated by a comma (,) from each other. No space is allowed before the comma delimiter.
- Any combination of uppercase and lowercase letters and digits can be used in an operand. However, the following special symbols cannot be used.

  ? " / \ < > * | : ,

  Note:

  - You can use symbols "\", "/" and ":" to specify a file path.
  - You can use ":" to specify host names for IP addresses in the IPv6 format.
- The queue name is not case sensitive.
- The **system** and **queue** parameter definition is always required.
- The **system** parameter must precede the **queue** parameter setup.
- A comment can be written on a comment line only. The comment line starts if it has an asterisk (*) in column 1.
- The tab character is not allowed to be used.

B.1.1 List of Initialization File Definitions

You can also specify the parameters and operands of initialization file definition from the **Define Operating Information** or **Create Queue** window. The following explains the list of initialization file setup options relating to the actual on-screen options.

For the detailed parameter and operand information, see "2.8.1 Defining the System Operating Information".

Options listed on the Operation control sheet of Define Operating Information window

Window definition options	Parameter and operands of initialization file
"Specify default queue to which the job is submitted." (Default queue name)	"dfltqueue" operand of "system" parameter
"Limit the number of concurrently executable jobs." (Job multiplicity)	"maxexec" operand of "system" parameter
"Specify the default priority ranking." (Default priority)	"dfltprty" operand of "system" parameter

Options to be set from the Create Queue window

Window definition options	Parameter and operands of initialization file
Queue name	"name" operand of "queue" parameter
"Limit the number of concurrently executable jobs." (Job multiplicity)	"maxexec" operand of "queue" parameter
"Limit the number of concurrently executable jobs." (Job count)	"maxjob" operand of "queue" parameter
"Specify the default priority ranking." (Default priority)	"dfltprty" operand of "queue" parameter
"Specify job execution priority." (Job execution priority)	"dfltdprty" operand of "queue" parameter
"Limit job execution elapsed time." (Limit of job execution time)	"limittime" operand of "queue" parameter

Window definition options	Parameter and operands of initialization file
"Use the distributed execution function." (Host group name)	"name" operand of "hostgrp" parameter
"Use the distributed execution function." (Configuration host name)	"host" operand of "hostgrp" parameter (See Notes.)

Note:

When you edit the initialization file directly, use the "host" operand of "queue" parameter to specify the host or host group name for distributed execution of actual jobs in this queue. You must use the "hostgrp" parameter to define the host group name and its configuration host only.

Options listed on the Logging sheet of Define Operating Information window

Window definition options	Parameter and operands of initialization file
"Save job execution history information." (Storage location)	"path" operand of "log" parameter (Note 1)
"Save job execution history information." (Storage period in days)	"keepdays" operand of "log" parameter (Note 2)
"Save the operating results data." (Storage location)	"path" operand of "record" parameter (Note 1)
"Save the operating results data." (Storage period)	"keepdays" operand of "record" parameter (Note 2)

Note 1:

If you specify a path name that exceeds the limit or if you specify a non-existing path name during direct editing of the initialization file, the following error occurs.

If Windows server is used: An error message is output to the event log, and the service fails to start up.
If UNIX server is used: An error message is output to SYSLOG, and the daemon fails to start up.

Note 2:

If omitted during direct editing of the initialization file, 7 days are set by default.

Options listed on the Options sheet of Define Operating Information window

Window definition options	Parameter and operands of initialization file
"Execute jobs under the respective job owner's authority" [Windows version]	"execasuser" parameter [Windows version]
"Convert file codes."	"convert" parameter
"Halt all queues during startup in startup of services."	"qstop" parameter
"Enable "prt" parameter." [Windows version]	The corresponding parameter and operands do not exist.
"Use the job termination code of the recently executed job step."	"jclexitcode" parameter
"Delimiter Output of Job Steps as Standard Output"	"jclstdout" parameter
"Halt all queues during startup in Recovery mode."	"qinactive" parameter

Options listed on the Backward compatibility sheet of Define Operating Information window

Window definition options	Parameter and operands of initialization file
"Register "mjsnet" services using 9327/tcp." [Windows version]	The corresponding parameter and operands do not exist.
"Do not execute jobs having the same name concurrently."	"namechk" parameter
"Move to the directory specified during job registration and execute the job."	"nochdir" parameter (Note 1)
"Copy the script file specified during job registration to the spool and execute it."	"scriptnocopy" parameter (Note 1)
"Enable the Load Balancer function of the previous version." [Windows version]	"distexec" parameter (in Windows system) (Note 1)
"Share the number of job entries to same execution servers between host groups"	"shareruncount" parameter (Note 2)

Note 1:

If the parameter is omitted, the function shown as the window definition option is used by default.
Note 2:

The distexec parameter must also be specified at the same time.

Options listed on the Cluster settings sheet of Define Operating Information window

Window definition options	Parameter and operands of initialization file
Spool directory [Windows version]	"path" operand of "spool" parameter [Windows version]
Logical IP address	"clusterip ipaddress" parameter
Node tree	No parameter and operands exist for the initialization file. You must set them in the window.

Options listed on the Network sheet of Define Operating Information window

Window definition options	Parameter and operands of initialization file
Change the retry operation in case of connection error with a network job (Retry interval)	"interval" operand of the "networkretry" parameter
Change the retry operation in case of connection error with a network job (Number of retries)	"retry" operand of the "networkretry" parameter

Options listed on the Print format sheet of Define Operating Information window [Windows version]

Window definition options	Parameter and operands of initialization file
Printer name or alias	"prt" parameter operand
"Specify a font name." (Font name)	"fontname" operand of "prt" parameter
"Specify a font size." (Font size)	"fontsize" operand of "prt" parameter
"Specify a print orientation."	"orient" operand of "prt" parameter
"Specify a paper size."	"form" operand of "prt" parameter

B.2 Trusted Host Definition File

The Trusted Host Definition file has been stored in the following location as a text file.

You can directly edit this file using an editor such as "vi" or Notepad.

File name:

mjhosts

Storage path:

The Trusted Host Definition file must be stored in the following location of the server.

[Windows version]

Systemwalker Operation Manager installation directory\MpWalker.Jm\mpmjessv\user

EE

The followings apply if Multi-subsystem operations are supported.

Subsystem number 0:

Same as when NO subsystem operations are supported.

Subsystem numbers 1 to 9:

Directory where Systemwalker Operation Manager has been installed \MpWalker.Jm\mpmjessv\mjesn\user, where "*n*" is a subsystem number.

[UNIX version]

/etc/mjes

EE

The followings apply if Multi-subsystem operations are supported.

Subsystem number 0:

Same as when NO subsystem operations are supported.

Subsystem numbers 1 to 9:

/etc/mjes/mjes*n*, where "*n*" is a subsystem number.

However, NEVER change the file path and the file name. In particular, if a new mjhosts file "mjhosts.txt" is created with Notepad, it is renamed to mjhosts.txt and its definition is made invalid.

Coding format

The syntax of the trusted host definition file is:

```
host-name [noroot]
```

host-name:

Specifies the host name of job submission server which accepts network jobs. A 64-byte or less host name can be specified.

noroot:

Allows to accept jobs when a network job request is sent from the specified server and when the jobs are submitted by ordinary users. Jobs submitted by the system administrator (the user belonging to the Administrators group or the superuser) are not accepted.

Syntax rules

The following syntax rules apply for the trusted host definition file.

- A server must be defined on a line.

- Only a space or spaces are allowed before the host name.
- The host name and noroot parameter must be separated from each other by one or more spaces.
- Up to 256 host names can be defined.
- If identical host names are defined, the definition written first is made valid.
- If a host name exceeds 64 bytes long, this line is made invalid.

Comments

- The noroot parameter can be followed by a comment if they are separated from each other by one or more spaces.
- A comment can be up to 128 bytes long.
- A blank line is treated as a comment line.
- If a host name is followed by a character string other than the noroot parameter, such character string is treated as a comment.

Example

The following is a coding example.

```
server1 This server is ......
server2 noroot This server is ......
```

Appendix C Listing of Port Numbers

This appendix lists the initial values assigned to ports used by each Systemwalker Operation Manager function.

C.1 Listing of Port Numbers

Various Systemwalker Operation Manager functions use the following default port numbers.

If the following default port numbers are already being used for other products, you must release those port numbers and reassign unused port numbers to those products. For details, see "2.2.2 Changing Port Numbers".

[For external communication]

The firewall must be assigned a port number if it exists between the source and destination (between the server and a client).

Function name	Service name	Port number	**Automatic addition to the services file (Note 4)**		Data transmission direction		Remarks
			Windows	**UNIX**	Source	Destination	
Common services of Operation Manager	JMSRV	9367/tcp	Y	N	Client	Server	For client connection authentication
					Server	Client	
	jmnet	9352/tcp	N	N	Client	Server	For client data communications
					Job requesting server	Job execution server	For canceling network jobs
					Job execution server	Job requesting server	For notifying network job termination
					Message event source	Message event destination	For notifying message events to other servers
Calendar Starting Services and Applications	JMCAL	9368/tcp	Y	N	Client Server (Note 2)	Server	For calendar data notification
Jobscheduler	jobsch_win	9297/tcp	Y	N	Client	Server	For registration, monitoring and operation of job nets
					Server	Client	

Function name	Service name	Port number	Automatic addition to the services file (Note 4)		Data transmission direction		Remarks
			Windows	**UNIX**	Source	Destination	
					Monitoring Host	Monitored Host	For monitoring of multi-servers
					Monitored Host	Monitoring Host	
Job Execution Control	mjsnet	9327/tcp	N	N	Job requesting server	Job execution server	For requesting and monitoring network jobs
Security	mpaclmgr	4013/tcp	Y	Y	Client	Server	For privilege checkout
Event Monitoring (Note 1)	JMEVT1	9371/tcp	Y	N	Client	Server	For condition definition of Event Monitoring
Action Management (Note 1)	JMACT1	9369/tcp	Y	N	Client	Server	For (synchronous) action management
	JMACT2	9370/tcp	Y	N	Client	Server	For (asynchronous) action management
	JMACT3	6961/tcp	Y	N	Server	Client	For action execution
Task Linking (Note 3)	mpnjsocl	2685/tcp	N	N	Server	Client	For client's Task Linking commands
	mpnjsc	1952/tcp 1952/udp	N	N	Server	Client	For remote power control
Remote Power Control	JMPWR	9373/tcp	Y	N	Systemwalker Centric Manager	Server	For communication from the power control function of Systemwalker Centric Manager Able to use only when the Systemwalker Centric Manager is installed.

Function name	Service name	Port number	Automatic addition to the services file (Note 4)		Data transmission direction		Remarks
			Windows	UNIX	Source	Destination	
Web console/Web API	mpahso	9900/tcp	N	N	Web console/Web API	Server	For FJApache HTTP service

Note 1:

The port number is NOT used if connected to a UNIX server.

Note 2:

If the System Power Control function is used.

Note 3:

The port number is NOT used if the function is not used.

Note 4:

This column shows whether the port number is added automatically to the services file at the time of installation.
Y: Added automatically.
N: Not added automatically.

[For internal communication]

Function name	Service name	Port number	Automatic addition to the services file (Note 2)		Data transmission direction		Remarks
			Windows	UNIX	Source	Destination	
Task Link	mpnjsomb	2681 /tcp	N	N	Client	Same as source client	For internal control of Task Link
	mpnjsosv (Note 1)	2684 /tcp	N	N	Server	Same as source server	For server's Task Link commands
	mpnjsomg (Note 1)	2686 /tcp	N	N	Server	Same as source server	For internal control of Task Link.
Web console/ Web API	mpojeed1httpo	9901 /tcp	N	N	Server	Same as source server	For internal control of Web console/Web API.
	mpojeed1httpso	9902 /tcp	N	N			
	mpojeed1admino	9903 /tcp	N	N			
	mpojeed1jmso	9904 /tcp	N	N			
	mpojeed1iiopo	9905 /tcp	N	N			
	mpojeed1iiopsmo	9906 /tcp	N	N			

Function name	Service name	Port number	Automatic addition to the services file (Note 2)		Data transmission direction		Remarks
			Windows	UNIX	Source	Destination	
	mpojeed1iiopso	9907 /tcp	N	N			
	mpojeed1jmxo	9908 /tcp	N	N			

Note 1:

The port number is NOT used if connected to a UNIX server.

Note 2:

This column shows whether the port number is added automatically to the services file at the time of installation.
Y: Added automatically.
N: Not added automatically.

Remote machine (port numbers that should accept external server access)

Use the port numbers listed below for SSH communication when using the mjrmtjob command to execute jobs on a remote machine. You need a remote machine license to use the mjrmtjob command.

Function name	Service name	Port number	Automatic addition to the services file (Note 1)		Data transmission direction		Remarks
			Windows	UNIX	Source	Destination	
mjrmtjob command	-	22/tcp (Note 2)	N	N	Server that executes the mjrmtjob command	Remote machine	For executing remote commands or scripts

Note 1:

This column shows whether the port number is added automatically to the services file at the time of installation.
Y: Added automatically.
N: Not added automatically.

Note 2:

Default value. If you specify "-P" option of mjrmtjob command, this value is "-P" option's value.

Appendix D Changing the System Installation Environment

This Appendix explains how to change the system environment where you install Systemwalker Operation Manager.

D.1 Changing the Startup Account [Windows version]

This section explains how to change the startup account specified in Systemwalker Operation Manager.

D.1.1 Changing the Startup Account

The following explains how to change the startup account of Systemwalker Operation Manager. If you are using the startup account as the Systemwalker Operation Manager user, you must change the user information of Systemwalker Operation Manager, too.

The "Systemwalker Operation Manager user" is:

- A owner of a Jobscheduler project
- A job owner
- A user registered in the password management book for Task Link.

Procedure

1. Shut down Systemwalker Operation Manager's services.
2. Rename the startup account name.
3. Change the startup account of Systemwalker Operation Manager's services.
4. Restart Systemwalker Operation Manager's services.
5. Reset the shutdown job nets.
6. Change the user information of Systemwalker Operation Manager. (If the information change is required)
    1. Change the security information of job projects.
    2. Change the job owner information
    3. Change the definition information of password management book for Task Link

These steps are detailed below.

1) Shut down Systemwalker Operation Manager's services.

Shut down all services of Systemwalker Operation Manager.

For details of service shutdown, see the section "Shutting Down the Systemwalker Operation Manager Servers [Windows version]" of the *Systemwalker Operation Manager User's Guide*. You cannot shut down all services of Systemwalker Operation Manager from the **Service Control** of the **Systemwalker Operation Manager Environment Setup** window.

2) Rename the startup account name.

Rename the user of the startup account using the OS's user renaming function.

To use a new or existing user as the startup account rather than changing the user name (while still keeping the old user), the new account must meet all of the following conditions.

a. The user must belong to the Administrators group on the local computer.

b. The following privileges must have been assigned to the user:

   The **Log on as a service** privilege

The **Act as part of the operating system** privilege

The **Adjust memory quotas for a process** privilege

The **Replace a process level token** privilege

c. The password for the user must not expire.

d. The user name and password must not include spaces.

e. A local system account must not be selected.

If these conditions are not met, the following issues will occur:

- The Systemwalker Operation Manager service will fail to start.

  This is caused by conditions b and c above.

- A user authentication error will occur when the client starts and an attempt is made to connect by specifying the user name and password.

  This is caused by conditions a and b above.

To use the server function of this software on a computer that belongs to a Windows Server 2008 or later domain, specify the following kind of user as the startup account for the "Systemwalker ACL Manager" service.

- A domain user who satisfies all the conditions above and belongs to the Domain Admins group

3) Change the startup account of Systemwalker Operation Manager's services.

Select **Control Panel** >> **Administrative Tools** >> **Services** of Windows Server 2008, and check and change the following items for each of the Systemwalker Operation Manager's services.

Confirmation:

Make sure that the startup account has been set in the service logon account.

If the startup account is already set:

Enter the changed account name in the **Account** field, and enter the changed password in the **Password** and **Password Confirmation** fields.

If the startup account is notset:

No action is required.

4) Restart Systemwalker Operation Manager's services.

Restart Systemwalker Operation Manager's services you have shut down in Step 1.

For details of service startup, see the section "Starting Up the Systemwalker Operation Manager Servers [Windows version]" of the *Systemwalker Operation Manager User's Guide*.

5) Reset the shutdown job nets.

You must set the shutdown job nets again if the "Shutdown job nets" have been defined in the Jobscheduler. For the details of shutdown job nets, see the section "Shutting Down the System at Optional Time [Windows version]" of the *Systemwalker Operation Manager User's Guide*.

To execute them as shutdown job nets, each account must satisfy the following requirements

- The job nets have been registered in the project having the same name as the startup account of "Systemwalker MpJobsch" services.

- The job net name is either "JSHEND" or "JSHFORCE."

Therefore, if you have changed the service startup account, you must create a project having the same name as the new startup account on the Jobscheduler and you must copy the shutdown job net ("JSHEND" or "JSHFORCE") in a location under the new project. (Also, you must delete the old project information after this copy.)

Reset the system if necessary.

6) Change the user information of Systemwalker Operation Manager.

You must change the specified information if the startup account has been defined as the job owner or if it has been defined in the password management book for Task Link.

The following explains how to change the user information of Systemwalker Operation Manager in the following steps.

- Change the security information of job projects.
- Change the job owner information
- Change the definition information of password management book for Task Link

These steps are detailed below.

Change the security information of job projects.

You must change the project owner if the startup account of a Jobscheduler project has been set as the owner. Also, you must change the access privilege information of the project if the access privileges of the startup account has been set for the project.

Changing the project owner:

For the procedure to change the project owner, see the section "Changing Projects" of the *Systemwalker Operation Manager User's Guide*.

Changing the access privileges of a project:

Refer to "Setting up Access Permissions for Projects" in the *Systemwalker Operation Manager User's Guide* for details on how to change the access privileges for projects.

Change the job owner information

You must change the information of job owner if you have specified the **Execute jobs under the respective job owner's authority** option in the Job Execution Control definition and if there is a job whose startup account has been defined as the owner.

Procedure

1. Check whether or not the **Execute jobs under the respective job owner's authority** has been enabled in the Job Execution Control definition.

   If enabled, go to Step 2.

   For the checkout method, see "2.8.1 Defining the System Operating Information".

   If this option is disabled, you need not change the job owner information.

2. Check whether or not the startup account is registered after you have changed the definition of job owner information.

   If the startup account has been registered after the change, you must set the password information again. If not registered, you must register the startup account.

   For details to check the definition of job owner information and to set the password, see "2.8.3 Defining the Job Owner Information [Windows]".

If the Previous Load Distribution function is used:

If you are using the Previous Load Distribution function, you must rename the startup account of the distributed server.

The Job Execution Control startup account of the server and the job execution service startup account of the load distribution server must be the same. You must change the startup account name of the distributed load server.

For details of Distributed Execution function and Previous Load Distribution function, see "2.8.1 Defining the System Operating Information".

Change the definition information of password management book for Task Link

You must add the startup account after its change if the Task Link function is used and if the startup account has been defined in the password management book for Task link.

For the definition of password management book, see "2.10.1 Defining a Password Management Book".

D.2 Changing the IP Addresses and Host Names

The following explains the procedures to change the IP addresses and host names in the system environment where Systemwalker Operation Manager has been installed.

D.2.1 Changing the IP Address and Host Name of Systemwalker Operation Manager Server

The following explains how to change the IP address and host name of the Systemwalker Operation Manager server. Also, it explains the items you must change.

Procedure

Use the following procedure to change the IP address and host name of the Systemwalker Operation Manager server.

1. Before changing the IP address and host name of the Systemwalker Operation Manager server, check the points of server and clients you must change by referring to "Items You Must Change".

   You may need to shut down or restart the Operation Manager server other than the one whose IP address and host name you change. Check the items carefully.

2. Shut down Systemwalker Operation Manager both on the server whose IP address or host name you will change and on the server where you must shut down Systemwalker Operation Manager due to change of its items.

3. Change the IP address and/or host name of the Systemwalker Operation Manager server.

4. Change the items on the Systemwalker Operation Manager server or client.

5. Restart both the server where you have shut down Systemwalker Operation Manager and the Systemwalker Operation Manager server whose IP address and/or host name has been changed.

Items You Must Change

When changing the IP address and/or host name of the Systemwalker Operation Manager server, you must check or change the following items.

- Defining a Monitored Host
- Defining the Power Control (if the batch power control is used or if the server is turned on by the client)
- Defining a Monitoring Permitted Host (if multi-servers are monitored)
- Defining the requesting host name and the default host name (if network jobs are used)
- Defining an execution subsystem name (if an execution subsystem name is used for network jobs)
- Defining a Trust Host (if the trusted host has been defined)
- Defining a node name in the operation information (if the cluster system configuration has been defined)
- Defining the configuration host name (if the Distributed Execution function or the Previous Load Distribution function is used)
- Defining the Process Monitoring function (if the process monitoring has been defined)
- Setting the message event destination (if a message is generated by the command)
- Defining a calendar (For the cluster system configuration).
- Defining the logical IP address of operation information (For the cluster system configuration).
- Defining a demand job (When using the network job).
- EE Defining Master Schedule Management [UNIX] (if the Master Schedule Management function is used)

Defining a Monitored Host

If you have changed the IP address or host name of the Systemwalker Operation Manager server, you must change the definition of the Monitored Host on all servers which monitor or operate the Systemwalker Operation Manager server you have changed.

Click **Monitored host** in the **Systemwalker Operation Manager Environment Setup** window, and the **Select Monitored Host Configuration** window will appear. Select a monitored host configuration from the list of "Monitored host configuration name" and click **Edit**. The **Monitored Host configuration** window appears. Check **Host Properties** and change the IP address and host name.

For details, see "2.4.1 Defining the Monitored Host in Systemwalker Operation Manager".

Defining the Power Control

You must change the Power Control definition if:

- If the batch power control is used
- If the server power is controlled by the client

If the batch power control is used

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you use it for batch power control, you must check the following host names and IP addresses of both the controlling host and the controlled hosts. Also, you must change their host names and IP addresses as follows.

- If you have selected the **Use this computer as a power control host** option from the **Power Control Setting** window, check **Target Host Name** and **IP Address of UPS** displayed in the **Power Control Target Hosts** window. Then, set the host name and/or IP address you have changed.
- If you have selected **Control the power as batch control** option from the **Power Control Setting** window, check **Power Control Host Name** and set the host name you have changed.

For details, see "Setting the Power Control" of the *Systemwalker Operation Manager User's Guide*.

If the server power is controlled by the client

If a server is turned on when a user logs on a client and if the IP address or host name of this server has been changed, you may need to change the power control software parameters on the client.

For details, see "2.6 Definition of Power Control".

Defining a Monitoring Permitted Host

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you use it to monitor multi-servers, you must check the definition of the monitoring permission host on the monitoring server. Also, you must set the host name you have changed.

To do so, click the **Monitoring permission host** button in the **Systemwalker Operation Manager Environment Setup** window. When the **Define Monitoring Permission Host** window appears, check **Monitoring permission host** and set the host name you have changed.

For details, see "2.7.3 Defining a Monitoring Permitted Host".

Defining the requesting host name and the default host name

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you use it to submit a network job, you must check the following definitions of job nets and jobs on this server. Also, you must set the IP address/host name you have changed.

- Check **Request host** on the **Standard information** sheet displayed in the **Add/Change/Monitor - Job** window.
- Check **Default host name** on the **Standard information** sheet displayed in the **Job Net Properties** window.

Note that it is not necessary to restart the server to make your changes valid. However, you must set them only when no job is executed.

For details, see the sections "Registering Job Nets" and "Setting Job Net Data" of the *Systemwalker Operation Manager User's Guide*.

Defining an execution subsystem name

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you use it to submit a network job and is also defined in the execution subsystem name definition file, you must set the new IP address or host name in the execution subsystem name definition file in the Operation Manager server that submits the network jobs.

Restart the Job Execution Control service/daemon so that the settings take effect.

Refer to "Defining an Execution Subsystem Name" in the *Systemwalker Operation Manager Installation Guide* for details.

Defining a Trust Host

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you have defined it as the trusted host on another server, you must set the trusted host you have changed.

To do so, click the **Trust host** button in the **Systemwalker Operation Manager Environment Setup** window. When the **Define Trust Host** window appears, check the trust host definition and set the host name you have changed.

To make your changes valid, you must restart Systemwalker Operation Manager.

For details, see "2.8.2 Defining a Trust Host".

Defining a node name in the operation information

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you use it in a cluster system configuration, you must set the node name you have changed on the job execution server.

To do so, click the **Operation information** button in the **Systemwalker Operation Manager Environment Setup** window. When the **Define Operating Information** window appears, click the **Edit** button of the Server settings option on the **Cluster settings** sheet. Then, set the node name you have changed in the **Edit Node** window.

To make your changes valid, you must restart Systemwalker Operation Manager.

For details, see "2.8.1 Defining the System Operating Information".

Defining the configuration host name

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you have specified it as the configuration host for the Distributed Execution function or Previous Load Distribution function of queues, you must change the configuration host.

To do so, click the **Operation information** button in the **Systemwalker Operation Manager Environment Setup** window. When the **Define Operating Information** window appears, select the **Operating control** sheet. Select the **queue** and when the **Edit Queue** window appears, check the configuration host name. Then, set the host name you have changed.

To make your changes valid, you must restart Systemwalker Operation Manager.

For details, see "2.8.1 Defining the System Operating Information".

Defining the Process Monitoring function

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you specify "MyIPaddr" (IP address of the local node) in the **mppmon.ini** definition file for the Process Monitor function of this server, you must change the IP address.

For details, see "2.14.1.3 Changing the Definition Information of Process Monitoring Function".

Setting the message event destination

If you have changed the IP address or host name of the Systemwalker Operation Manager server and if you specify a job to generate a message event to this server using the **jobschmsgevent** command option, you must review the job definition on the Systemwalker Operation Manager server (schedule server) where you have defined the **jobschmsgevent** command as a job.

Note that it is not necessary to restart the server to make your changes valid. However, you must set them only when no job is executed.

For the **jobschmsgevent** command details, see the *Systemwalker Operation Manager Reference Guide*.

Defining a calendar

When the Operation Manager Server whose IP address and host name have been changed is in the cluster system configuration, it is required to set the each node name changed at the operation node and standby node onto the calendar destination host definition file.

[Procedures]

1. Open the Calendar Destination Host Definition File "calcphost.def" by the editor such as notepad.

   The Calendar Destination Host Definition File is stored in the following directory.

   [Windows version]

   Systemwalker Operation Manager installation directory\MPWALKER.JM\mpjmcal\etc\calcphost.def

   [Solaris version and Linux version]

   /var/opt/FJSVjmcal/etc/calcphost.def

   [HP-UX version]

   /opt/FHPjmcal/etc/calcphost.def

   [AIX version]

   /opt/FAIXjmcal/etc/calcphost.def

2. Modify the IP address and host name in the Calendar Destination Host Definition File.

3. To activate the information in the Calendar Destination Host Definition File, restart the calendar service.

For details on Calendar Destination Host Definition File "calcphost.def," see the *Systemwalker Operation Manager Reference Guide*.

Defining the logical IP address of operation information

When the Operation Manager Server whose IP address or host name has been changed is in the cluster system configuration, and it is defined in the following, set the changed IP address.

- **Define Operating Information-Cluster settings-Schedule server settings-Logical IP address**

It is required to set the changed IP address for each of the operation node and standby node [Windows]. For details, see "Setting IP address for job execution control" in the *Systemwalker Operation Manager Cluster Setup Guide for Microsoft Cluster Server for Windows*.

Defining a demand job

When the Operation Manager Server whose IP address or host name has been changed is the destination of network job submission, confirm the following definitions of demand job and set the changed host name on the Operation Manager Server which is the source of network job.

Set this host name when the corresponding job is not running. To activate this setting, no restarting is required.

- **Edit Job Information/Submit-Additional Information-Execution Server Name**
- A host name specified for -rh option of qsub command.
- A host name specified for connect control statement in JCL.
- Theo host name specified for -rh option in the second argument of job input API (MP_SubmitJob)

For details, see the following manuals. "qsub Job Submit Command" in the *Systemwalker Operation Manager Reference Guide* and "Registering Demand Job in Job Folders" in the *Systemwalker Operation Manager User's Guide*

EE

Defining Master Schedule Management [UNIX]

If the host name or IP address is changed for an Operation Manager server where a Master Schedule Management environment has already been created, then the definitions will need to be changed.

- If you have changed the IP address of the management server:

  Execute the **stemConfig** command on the management server and on all schedule servers, and change the definition.

- If you have changed the IP address of a schedule server:

  Execute the **stemConfig** command on the management server and change the definition.

  Alternatively, edit the schedule server using a **Master Schedule Management Environment Setup** dialog box connected to the management server.

- If you have changed the host name of the management server:

  Edit all of the schedule servers using a **Master Schedule Management Environment Setup** dialog box connected to the management server. Do not change the IP address of each schedule server, but click **OK** to register the schedule servers again.

- If you have changed the host name of a schedule server:

  In a **Master Schedule Management Environment Setup** dialog box connected to the management server, clear the host name of the schedule server, and add the new host name to the schedule server.

Remark:

If the host name of the schedule server has been changed, the Master Schedule Management function will treat the schedule server as a different host.

Refer to the *Systemwalker Operation Manager Reference Guide* for details on the stemConfig command, and refer to the *Systemwalker Operation Manager User's Guide - Master Schedule Management* for details on the **Master Schedule Management Environment Setup** dialog box.

D.2.2 Changing the IP Address and Host Name of Systemwalker Operation Manager Clients

The following explains how to change the IP address and host name of the Systemwalker Operation Manager client. Also, it explains the items you must change.

Procedure

Use the following procedure to change the IP address and/or host name in the system environment where Systemwalker Operation Manager has been installed.

1. If you have changed the IP address and/or host name of a Systemwalker Operation Manager client, check the items you must change on the server and clients by referring to "Items You Must Change" given below.
2. Shut down the Systemwalker Operation Manager client. Also, shut down Systemwalker Operation Manager on the server where you need to shut down Systemwalker Operation Manager.
3. Change the IP address and/or host name of the Systemwalker Operation Manager client.
4. Change the items on the Systemwalker Operation Manager server or client.
5. Restart the server where you have shut down Systemwalker Operation Manager. Also, restart the Systemwalker Operation Manager client.

Items You Must Change

When changing the IP address and/or host name of the Systemwalker Operation Manager client, you must change the following item.

- Definition of Task Link

Definition of Task Link

If you have installed the Task Link function, you must change the following items.

- Defining the Host Information

- Parameters of Client Task Linkage command

Defining the Host Information

If you turn the client power on using the Task Link function, you must change the IP address and/or host name of the changed Systemwalker Operation Manager client on the server to be used for client power control.

Specify the IP address and/or host name of the changed Systemwalker Operation Manager client in the "**hostinfo.ini**" host information definition file.

For details, see "2.10.3 Defining the Host Information".

Parameters of Client Task Linkage command

If you have stored the Client Task Linkage command as a job, you must change the parameter of this command to the IP address and/or host name of the Systemwalker Operation Manager client to be changed.

To do so, check the job definition on the Systemwalker Operation Manager server (the schedule server) where you have defined the Client Task Linkage command as a job, and set the IP address and/or host name you have changed.

Note that it is not necessary to restart the server to make your changes valid. However, you must set them only when no job is executed.

For details of Client Task Link command, refer to the *Systemwalker Operation Manager Reference Guide*.

D.2.3 Changing the IP Address and Host Name of the Server Linked to Systemwalker Operation Manager

If you have changed the IP address and/or host name of a server linked to Systemwalker Operation Manager, you may need to change its definition on Systemwalker Operation Manager.

If you have changed the IP address and/or host name of the linked server, you must change the following items on Systemwalker Operation Manager.

- Defining the Automatic Operation Support [Windows version]]

Defining the Automatic Operation Support [Windows version]

If an SNMP trap is issued as an action to an event and if you have changed the IP address and/or host name of the trap destination server, you must change the definition.

To do so, select the event from the **Monitored Event Table** window. When the **Action** menu appears, select **Define Actions**. Then, select **Action Definition** and change the **Host name** of **Trap Destination** on the **SNMP Trap** sheet.

For details, see the section "Registering Actions" of the *Systemwalker Operation Manager User's Guide*.

If you are using this function and Systemwalker Centric Manager with together and if an SNMP manager exists on Systemwalker Centric Manager's Operation Management Server, you must change the definition by referring to the *Systemwalker Centric Manager Installation Guide*.

D.3 Changing User IDs and Passwords

This section explains how to add, change or delete user IDs or passwords.

Using the operating system's user management function

Add, change or delete user IDs and passwords by following the instructions in the manuals of the operating system being used.

If a user ID has been added or changed, the required access rights must be set up.

Refer to "Setting up Access Permissions for Projects" in the *Systemwalker Operation Manager User's Guide* for details on how to set access rights.

Using the Systemwalker Extended User Management function

To add, change or delete Operation Manager users for the Systemwalker Extended User Management function, use the mpadduser command or the mpdeluser command.

To change the OS users associated with Operation Manager users, use the mpmoduser command.

To set, change or delete passwords for Operation Manager users, use the mpsetpasswd command.

Refer to the *Systemwalker Operation Manager Reference Guide* for details on the command.

If an Operation Manager user has been added or changed, the required access rights must be set up.

Refer to "Setting up Access Permissions for Projects" in the *Systemwalker Operation Manager User's Guide* for details on how to set access rights.

D.3.1 When the Password of an OS User ID is Changed

If the password is changed for an OS user ID, then the password information for the Systemwalker Operation Manager user must also be changed as required.

This information must be changed for the following Systemwalker Operation Manager users:

- Job owners [Windows]
- Users registered in the Task Link password management book

The procedure to change the password for each user type is described below.

Changing the password for a job owner [Windows]

If **Execute jobs under the respective job owner's authority** is specified in the Job Execution Control definition and a job exists for which the relevant user ID has been defined as the owner, the password information for the job owner must be changed.

Procedure

1. Click **Operation information** in the **Systemwalker Operation Manager Environment Setup** window to display the **Define Operating Information** window. Ensure that **Execute jobs under the respective job owner's authority** is enabled in the **Options** sheet.

   If **Execute jobs under the respective job owner's authority** is enabled, proceed to the next step.

   If not enabled, there is no need to change the job owner password.

2. Check if a user ID has been registered that corresponds to the job owner information definition. If so, update the password information for the user ID by specifying the new password.

   Select the **Options** sheet in the **Define Operating Information** window, and click **Set Job Owner** to display the **Define Job Owner's Information** window. Select the user ID for which you want to change the password information, and then select **Define** from the **User** menu. The **Define Password Information** dialog box will be displayed. Enter the changed password.

3. If using network jobs or the Distributed Execution function, check if **Execute jobs under the respective job owner's authority** is enabled on the execution server, as in Step 1. If **Execute jobs under the respective job owner's authority** is also enabled on the execution server side, perform the following:

   - The job will be executed under the authority of the user submitting the job, so the password corresponding to the user ID of the user submitting the job must match at the submission source and on the execution server. Therefore, the password corresponding to the user ID on the execution server must also be changed.

   Refer to "2.8.1 Defining the System Operating Information" for information on network jobs and the Distributed Execution function.

Changing the definition information for a user registered in the Task Link password management book

If using the Task Link function and a user ID has been defined in the Task Link password management book, change the password definition.

Refer to "2.10.1 Defining a Password Management Book" for information on how to change the password information in the password management book.

D.4 Changing User Management Methods

This section explains the procedure for changing the user management method.

D.4.1 Switching from OS User to Operation Manager User

If you enable the Extended User Management function after creating a project by the name of OS user, only Operation Manager users having the Administrator's privileges can update all projects. The project owner information is inherited. Set the access privileges, if necessary.

Use the following steps if you create a project as the OS user and then, inherit the project access information as the Operation Manager user having the same name.

1. Back up the access privileges and owner information of the project.

   You must execute the following command using the system administrator privileges on the Operation Manager server.

   ```
   mkbat -f file name -j
   ```

2. Create an Operation Manager user having the same name as the OS user.
3. Enable the Extended User Management function by issuing the **mpsetusermode** command.

   ```
   mpsetusermode -s on
   ```

4. Execute the file output in Step 1 as a shell script.

   Give the execution right to the file created under the name in Step 1, and execute it using the system administrator privileges on the Operation Manager server.

For the mkbat command and mpsetusermode command details, refer to the *Systemwalker Operation Manager Reference Guide*.

D.4.2 Switching from Operation Manager User to OS User

If you disable the Extended User Management function after creating a project under the name of an Operation Manager user, the system administrator (superuser) has the update right to all projects and the project owner has the update right to his/her own project. Set the access privileges, if necessary.

Use the following steps if you register an Operation Manager user and create a project, and then switch to the OS user while inheriting the access privilege information of the project.

1. Back up the access privileges and owner information of the project.

   You must execute the following commands using the system administrator privileges on the Operation Manager server.

   ```
   mkbat -f file name -j
   ```

2. Create an OS user having the same name as the Operation Manager user.
3. Disable the Extended User Management function by issuing the **mpsetusermode** command.

   ```
   mpsetusermode -s off
   ```

4. Execute the file output in Step 1 as a shell script.

   Give the execution right to the file created under the name in Step 1, and execute it using the system administrator privileges on the Operation Manager server.

For the mkbat command and mpsetusermode command details, refer to the *Systemwalker Operation Manager Reference Guide*.

D.5 Promoting/Demoting a Sever Machine to or from a Domain Controller

This section explains how to promote a server machine used in the installation environment to a domain controller, and also how to demote a server machine from a domain controller.

1) Perform backup

Perform a backup before promoting a machine to a domain controller or demoting a machine from a domain controller. Refer to "3.1 Backup" for an explanation of the backup procedure.

2) Register users

Confirm and record the users belonging to the local groups listed below. (This information recorded here will be used to return the server machine to the pre-promotion/demotion state if this operation is required after the machine has been promoted to or demoted from a domain controller.) The local group to confirm and the verification method are as follows:

- [Local group]

  swadmin

- [Verification method]

  The following menus can be used to confirm the local group:

  - For promotion

    Open **Control Panel** and select **Administrative Tools** >> **Computer Management** >> **System Tools** >> **Local Users and Groups** >> **Groups**

  - For demotion

    Open **Control Panel** and select **Administrative Tools** >> **Active Directory Users and Computers** >> **Domain name** >> **Users**

3) Perform promotion/demotion

Promote or demote the server machine to or from a domain controller. Refer to the relevant operating system manual for the promotion or demotion procedure.

4) Check/Set local group information

Check that the following local group is registered with the system. If it is not, create it. The local group to check and the checking and registration methods are explained below.

- [Local group]

  swadmin

- [Verification method]

  The following menus can be used to confirm the local group:

  - For promotion

    Open **Control Panel** and select **Administrative Tools** >> **Active Directory Users and Computers** >> **Domain name** >> **Users**

  - For demotion

    Open **Control Panel** and select **Administrative Tools** >> **Computer Management** >> **System Tools** >> **Local Users and Groups** >> **Groups**

- [Registration method]

  Open a command prompt window.

  Run the following command to create the local group:

```
> net localgroup swadmin /ADD
```

5) Delete unknown account information

Display the properties of the following directory in Explorer and delete any unknown accounts in the **Group or user names** in the **Security** tab.

- [Directory]

```
Systemwalker installation directory\MpWalker.JM
```

6) Set the required access permissions

Set the access permissions as below.

1. Log in as a user belonging to the Administrators group.
2. Open a command prompt window.
3. Run the following command to set access permissions:

```
Systemwalker installation directory\MpWalker\bin\mpsetseco.exe /o
```

7) Set users belonging to the local group

Set the users belonging to the following local group to the same state as in the confirmation results recorded in step 2) above. (Add or delete users as required.)

- [Local group]

  swadmin

8) Reset the job ownership definition

If the **Execute jobs under the respective job owner's authority** check box in the **Options** sheet of the **Define Operating Information** window is selected, reset the job ownership definition by defining the following items again:

- Use the **Define Job Owner's Information** window to specify the password for the user ID that will submit jobs.
- Assign the **Log on as a batch job** privilege to the user ID that will submit jobs.

Appendix E Usage Restrictions Based on Access Rights

This appendix lists the items that can be used by different access rights.

E.1 Availability of Operation Management Client (Jobscheduler Function) Menu Items Based on Access Rights

This section lists the Operation Management Client (Jobscheduler function) window menu items that can be used by different access rights.

- File menu of the Systemwalker Operation Manager window
- Tools menu of the Systemwalker Operation Manager window
- Pop-up menus accessed from the Systemwalker Operation Manager window
- File menu of the Job Net Management window
- Tools menu of the Job Net Management window
- Pop-up menus accessed from the Job Net Management window
- File menu of the Group Management window
- Tools menu of the Group Management window
- Pop-up menus accessed from the Group Management window
- File menu of the Monitor Job Net window
- Pop-up menus accessed from the Monitor Job Net window
- File menu of the Monitor Group window
- Pop-up menus accessed from the Monitor Group window

File menu of the Systemwalker Operation Manager window

Menu item name		Reference right	Operation right	Change right	Update right
Open		Y	Y	Y	Y
Close		-	-	-	-
Batch Processing	Pause All	N	Y	N	Y
	Continue All	N	Y	N	Y
	Disable All	N	Y	N	Y
	Enable All	N	Y	N	Y
Schedule Operation	Cancel	N	Y	N	Y
	Start	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y

Menu item name			Reference right	Operation right	Change right	Update right
	Confirm		N	Y	N	Y
	Reinstate		N	Y	N	Y
	Revoke		N	Y	N	Y
	Start with variable parameters		N	Y	N	Y
Job Operation			-	-	-	-
Queue Operation			-	-	-	-
Job Net Remarks			Y (Note 1)	Y	Y	Y
New	Calendar		-	-	-	-
	Project		N (Note 2)	N (Note 2)	N (Note 2)	N (Note 2)
	Group		N	N	Y	Y
	Job Net	Job Execution Control	N	N	Y	Y
		PowerAIM	N	N	Y	Y
		Interstage	N	N	Y	Y
		Normal	N	N	Y	Y
	Job Folder		-	-	-	-
	Job File		-	-	-	-
Modify			N	N	Y	Y
Delete			N	N	Y	Y
Startup days			Y (Note 1)	Y (Note 1)	Y	Y
Status			-	-	-	-
Copy			Y (Note 3)	Y (Note 3)	Y (Note 3)	Y (Note 3)
Paste			Y (Note 3)	Y (Note 3)	Y (Note 3)	Y (Note 3)
Reuse			Y (Note 3)	Y (Note 3)	Y (Note 3)	Y (Note 3)
Save			-	-	-	-
Job Definition Variables			Y	Y	Y	Y
Properties			Y (Note 1)	Y (Note 1)	Y	Y
Import			N	N	Y	Y
Export			N	N	Y	Y
Exit			Y	Y	Y	Y

Y: Can be accessed

N: Cannot be accessed

-: Disabled when the Jobscheduler function is selected

Note 1:

The setting cannot be changed.

Note 2:

Can only be used by a system administrator or an Operation Manager user with Administrator privileges.

Note 3:

Job nets cannot be pasted to projects with reference and operation rights and job nets to be reused cannot be copied from such projects.

Tools menu of the Systemwalker Operation Manager window

Menu item name	Reference right	Operation right	Change right	Update right
Job Net History	Y	Y	Y	Y
Job History	Y	Y	Y	Y
Message event list	Y	Y	Y	Y
Job Net Temporary Change	Y (Note 1)	Y (Note 1)	Y	Y
Return to Normal Schedule	Y (Note 1)	Y (Note 1)	Y	Y
Stop Time Temporary Change	N	Y	N	Y
Application Plan	Y (Note 1)	Y (Note 1)	Y	Y
Schedule Pattern	Y (Note 2)	Y (Note 2)	Y (Note 2)	Y (Note 2)
Master Linked Job Net List	Y	Y	Y	Y
Job Net Management	Y	Y	Y	Y
Group Management	Y	Y	Y	Y
Confirmation Settings	Y	Y	Y	Y

```
Y: Can be accessed
```

```
N: Cannot be accessed
```

Note 1:

The setting cannot be changed.

Note 2:

The setting cannot be changed. This menu item can only be used by a system administrator or an Operation Manager user with Administrator privileges.

Pop-up menus accessed from the Systemwalker Operation Manager window

Menu item name		Reference right	Operation right	Change right	Update right
Open		Y	Y	Y	Y
Batch Processing	Pause All	N	Y	N	Y
	Continue All	N	Y	N	Y
	Disable All	N	Y	N	Y
	Enable All	N	Y	N	Y
Operation	Cancel	N	Y	N	Y
	Start	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y

Menu item name			Reference right	Operation right	Change right	Update right
	Continue		N	Y	N	Y
	Disable		N	Y	N	Y
	Enable		N	Y	N	Y
	Confirm		N	Y	N	Y
	Reinstate		N	Y	N	Y
	Revoke		N	Y	N	Y
	Start with variable parameters		N	Y	N	Y
Job Net Remarks			Y (Note 1)	Y	Y	Y
New	Project		N (Note 2)	N (Note 2)	N (Note 2)	N (Note 2)
	Group		N	N	Y	Y
	Job Net	Job Execution Control	N	N	Y	Y
		PowerAIM	N	N	Y	Y
		Interstage	N	N	Y	Y
		Normal	N	N	Y	Y
Modify			N	N	Y	Y
Delete			N	N	Y	Y
Copy			Y (Note 3)	Y (Note 3)	Y (Note 3)	Y (Note 3)
Paste			Y (Note 3)	Y (Note 3)	Y (Note 3)	Y (Note 3)
Reuse			Y (Note 3)	Y (Note 3)	Y (Note 3)	Y (Note 3)
Startup days			Y (Note 1)	Y (Note 1)	Y	Y
Import			N	N	Y	Y
Export			N	N	Y	Y
Sort Schedule	by Entry		Y	Y	Y	Y
	by Name		Y	Y	Y	Y
	by Start Time		Y	Y	Y	Y
	by Status		Y	Y	Y	Y
All			Y	Y	Y	Y
Filtering			Y	Y	Y	Y

Y: Can be accessed

N: Cannot be accessed

Note 1:

The setting cannot be changed.

Note 2:

Can only be used by a system administrator or an Operation Manager user with Administrator privileges.

Note 3:

Job nets cannot be pasted to projects with reference and operation rights and job nets to be reused cannot be copied from such projects.

File menu of the Job Net Management window

Menu item name		Reference right	Operation right	Change right	Update right
Operation	Cancel	N	Y	N	Y
	Start	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y
	Confirm	N	Y	N	Y
	Reinstate	N	Y	N	Y
	Revoke	N	Y	N	Y
	Start with variable parameters	N	Y	N	Y
Job Net Remarks		Y (Note 1)	Y	Y	Y
New	Job Execution Control	Y (Note 2)	Y (Note 2)	Y (Note 2)	Y (Note 2)
	PowerAIM	Y (Note 2)	Y (Note 2)	Y (Note 2)	Y (Note 2)
	Interstage	Y (Note 2)	Y (Note 2)	Y (Note 2)	Y (Note 2)
	Normal	Y (Note 2)	Y (Note 2)	Y (Note 2)	Y (Note 2)
Modify		N	N	Y	Y
Delete		N	N	Y	Y
Reuse		Y (Note 3)	Y (Note 3)	Y (Note 3)	Y (Note 3)
Startup days		Y (Note 1)	Y (Note 1)	Y	Y
Properties		Y (Note 1)	Y (Note 1)	Y	Y
Exit		Y	Y	Y	Y

`Y: Can be accessed`

`N: Cannot be accessed`

Note 1:

The setting cannot be changed.

Note 2:

New cannot be used on projects with reference and operation rights.

Note 3:

Job nets to be reused cannot be copied to projects with reference and operation rights.

Tools menu of the Job Net Management window

Menu item name	Reference right	Operation right	Change right	Update right
Job Net Monitoring	Y	Y	Y	Y
Job History	Y	Y	Y	Y
Message event list	Y	Y	Y	Y
Job Net Temporary change	Y (Note 1)	Y (Note 1)	Y	Y
Return to Normal Schedule	Y (Note 1)	Y (Note 1)	Y	Y

```
Y: Can be accessed
```

```
N: Cannot be accessed
```

Note 1:

The setting cannot be changed.

Pop-up menus accessed from the Job Net Management window

Menu item name		Reference right	Operation right	Change right	Update right
Operation	Cancel	N	Y	N	Y
	Start	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y
	Confirm	N	Y	N	Y
	Reinstate	N	Y	N	Y
	Revoke	N	Y	N	Y
	Start with variable parameters	N	Y	N	Y
Job Net Remarks		Y (Note 1)	Y	Y	Y
Job Net Monitoring		Y	Y	Y	Y
Job History		Y	Y	Y	Y
Message event list		Y	Y	Y	Y
Modify		N	N	Y	Y
Delete		N	N	Y	Y
Reuse		Y (Note 2)	Y (Note 2)	Y (Note 2)	Y (Note 2)
Startup days		Y (Note 1)	Y (Note 1)	Y	Y
Properties		Y (Note 1)	Y (Note 1)	Y	Y
Job Net Temporary change		Y (Note 1)	Y (Note 1)	Y	Y
Return to Normal Schedule		Y (Note 1)	Y (Note 1)	Y	Y

```
Y: Can be accessed
```

```
N: Cannot be accessed
```

Note 1:

The setting cannot be changed.

Note 2:

Job nets to be reused cannot be copied to projects with reference and operation rights.

File menu of the Group Management window

Menu item name		Reference right	Operation right	Change right	Update right
Operation	Cancel	N	Y	N	Y
	Start	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y
	Confirm	N	Y	N	Y
New		Y (Note 2)	Y (Note 2)	Y (Note 2)	Y (Note 2)
Modify		N	N	Y	Y
Delete		N	N	Y	Y
Properties		Y (Note 1)	Y (Note 1)	Y	Y
Exit		Y	Y	Y	Y

`Y: Can be accessed`

`N: Cannot be accessed`

Note 1:

The setting cannot be changed.

Note 2:

New cannot be used on projects with reference and operation rights.

Tools menu of the Group Management window

Menu item name	Reference right	Operation right	Change right	Update right
Group Monitoring	Y	Y	Y	Y

`Y: Can be accessed`

`N: Cannot be accessed`

Pop-up menus accessed from the Group Management window

Menu item name		Reference right	Operation right	Change right	Update right
Operation	Cancel	N	Y	N	Y
	Start	N	Y	N	Y

Menu item name		Reference right	Operation right	Change right	Update right
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y
	Confirm	N	Y	N	Y
Group Monitoring		Y	Y	Y	Y
Modify		N	N	Y	Y
Delete		N	N	Y	Y
Properties		Y (Note 1)	Y (Note 1)	Y	Y

`Y: Can be accessed`

`N: Cannot be accessed`

Note 1:

The setting cannot be changed.

File menu of the Monitor Job Net window

Menu item name		Reference right	Operation right	Change right	Update right
Save		-	-	-	-
Save As		-	-	-	-
Operation	Cancel	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y
Recovery	Start from Specified Job	N	Y	N	Y
	Restart from Specified Job	N	Y	N	Y
	Start from Next Job	N	Y	N	Y
	Specified Job Only	N	Y	N	Y
Restart Flow		N	Y	N	Y
Properties		Y (Note 1)	Y	Y (Note 1)	Y
Output Information		Y	Y	Y	Y
job flow		Y	Y	Y	Y
Recovery Change		N	N	Y	Y
Exit		Y	Y	Y	Y

`Y: Can be accessed`

`N: Cannot be accessed`

```
-: Disabled
```

Note 1:

The setting cannot be changed.

Pop-up menus accessed from the Monitor Job Net window

Menu item name		Reference right	Operation right	Change right	Update right
Operation	Cancel	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y
Recovery	Start from Specified Job	N	Y	N	Y
	Restart from Specified Job	N	Y	N	Y
	Start from Next Job	N	Y	N	Y
	Specified Job Only	N	Y	N	Y
Job Flow		Y	Y	Y	Y
Properties		Y (Note 1)	Y	Y (Note 1)	Y
Output Information		Y	Y	Y	Y
Select Previous		Y	Y	Y	Y
Select Next		Y	Y	Y	Y
Select Previous & Next		Y	Y	Y	Y
Select All Precedent		Y	Y	Y	Y
Select All Subsequent		Y	Y	Y	Y
Restart Flow		N	Y	N	Y

```
Y: Can be accessed

N: Cannot be accessed
```

Note 1:

The setting cannot be changed.

File menu of the Monitor Group window

Menu item name		Reference right	Operation right	Change right	Update right
Save		-	-	-	-
Save As		-	-	-	-
Operation	Cancel	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y

Menu item name		Reference right	Operation right	Change right	Update right
Save		-	-	-	-
Save As		-	-	-	-
	Enable	N	Y	N	Y
Restart Flow		N	Y	N	Y
Properties		Y	Y	Y	Y
Job Flow		Y	Y	Y	Y
Exit		Y	Y	Y	Y

Y: Can be accessed

N: Cannot be accessed

-: Disabled

Pop-up menus accessed from the Monitor Group window

Menu item name		Reference right	Operation right	Change right	Update right
Operation	Cancel	N	Y	N	Y
	Restart	N	Y	N	Y
	Pause	N	Y	N	Y
	Continue	N	Y	N	Y
	Disable	N	Y	N	Y
	Enable	N	Y	N	Y
Job Flow		Y	Y	Y	Y
Properties		Y	Y	Y	Y
Select Previous		Y	Y	Y	Y
Select Next		Y	Y	Y	Y
Select Previous & Next		Y	Y	Y	Y
Select All Precedent		Y	Y	Y	Y
Select All Subsequent		Y	Y	Y	Y
Restart Flow		N	Y	N	Y

Y: Can be accessed

N: Cannot be accessed

E.2 Availability of Jobscheduler Commands and APIs Based on Access Rights

The following table lists the Jobscheduler commands and APIs that can be used by different access rights.

Item	Reference right	Operation right	Change right	Update right
jobschsetgrp	N	N	Y	Y

Item	Reference right	Operation right	Change right	Update right
jobschsetnet -nent	N	N	Y	Y
jobschsetnet -nche	N	N	Y	Y
jobschsetnet -ncheall	N	N	Y	Y
jobschsetnet -ndel	N	N	Y	Y
jobschsetnet -ncpy (Copy source)	Y	Y	Y	Y
jobschsetnet -ncpy (Copy destination)	N	N	Y	Y
jobschsetnet -sent	N	N	Y	Y
jobschsetnet -sdel	N	N	Y	Y
jobschmove	N	N	Y	Y
jobschnetmemo -ent	N	Y	Y	Y
jobschnetmemo -del	N	Y	Y	Y
jobschnetmemo -out	Y	Y	Y	Y
jobschnetmemo -find	Y	Y	Y	Y
jobschctlgrp	N	Y	N	Y
jobschcontrol	N	Y	N	Y
jobschctljob	N	Y	N	Y
jobschoperate	N	Y	N	Y
jobschmsgclear	N	Y	N	Y
jobschcancelnet	N	Y	N	Y
jobschprint -j(-J)	Y	Y	Y	Y
jobschprint -n(-N)	Y	Y	Y	Y
jobschprint -a(-A)	Y	Y	Y	Y
jobschprint -e(-E)	Y	Y	Y	Y
jobschprint -i(-I)	Y	Y	Y	Y
jobschprint -l(-L)	Y	Y	Y	Y
jobschprint -m(-M)	Y	Y	Y	Y
jobschprint -p(-P)	Y	Y	Y	Y
jobschprint -q(-Q)	Y	Y	Y	Y
jobschprint -R	Y	Y	Y	Y
jobschprint -r	Y	Y	Y	Y
jobschprint -s(-S)	Y	Y	Y	Y
jobschprint -w(-W)	Y	Y	Y	Y
jobschprint -x(-X)	Y	Y	Y	Y
jobschprint -y(-Y)	Y	Y	Y	Y
jobschprint -o(-O)	Y	Y	Y	Y
jobschprintcsv -n	Y	Y	Y	Y
jobschprintcsv -l	Y	Y	Y	Y
Mp_JobschControl	N	Y	N	Y
Mp_JobschControlEx	N	Y	N	Y

Item	Reference right	Operation right	Change right	Update right
Mp_JobschControlParam	N	Y	N	Y
Mp_JobschControlParamEx	N	Y	N	Y
Mp_JobschCtlGrp	N	Y	N	Y
Mp_JobschCtlGrpEx	N	Y	N	Y
JSNetStart	N	Y	N	Y
JSNetStartEx	N	Y	N	Y
Mp_JobschCtlStartTime	Y (Note 1)	Y (Note 1)	Y	Y
Mp_JobschCtlStartTimeEx	Y (Note 1)	Y (Note 1)	Y	Y

Y: Can be accessed

N: Cannot be accessed

Note 1:

The startup time cannot be changed.