Systemwalker

Systemwalker
Runbook Automation

Installation Guide

Windows/Linux

Preface

Purpose of This Document

This document describes how to install Systemwalker Runbook Automation V15.1.0

Intended Readers

This document is intended for people who will use Systemwalker Runbook Automation to perform administration tasks.

This document assumes that readers already have the following knowledge:

- Windows(R)

- Linux

- Solaris

- Internet

- Relational databases

- Web servers

- LDAP

- Java

Abbreviations and Generic Terms Used

- The term "Windows(R) 7" refers to the following products:

  - Windows(R) 7 Home Premium(x86)

  - Windows(R) 7 Professional(x86)

  - Windows(R) 7 Ultimate(x86)

  - Windows(R) 7 Home Premium(x64)

  - Windows(R) 7 Professional(x64)

  - Windows(R) 7 Ultimate(x64)

- The term "Windows Server 2008" refers to the following products:

  - Microsoft(R) Windows Server(R) 2008 R2 Standard(x64)

  - Microsoft(R) Windows Server(R) 2008 R2 Enterprise(x64)

  - Microsoft(R) Windows Server(R) 2008 R2 Datacenter(x64)

  - Microsoft(R) Windows Server(R) 2008 Standard(x86)

  - Microsoft(R) Windows Server(R) 2008 Enterprise(x86)

  - Microsoft(R) Windows Server(R) 2008 Standard(x64)

  - Microsoft(R) Windows Server(R) 2008 Enterprise(x64)

  - Microsoft(R) Windows Server(R) 2008 Datacenter(x64)

  - Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(x86)

  - Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(x86)

  - Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(x64)

- The term "Windows Vista(R)" refers to the following products:

  - Windows Vista(R) Home Basic(x86)

  - Windows Vista(R) Home Premium(x86)

  - Windows Vista(R) Business(x86)

  - Windows Vista(R) Ultimate(x86)

  - Windows Vista(R) Enterprise(x86)

  - Windows Vista(R) Business(x64)

  - Windows Vista(R) Ultimate(x64)

- The term "Windows Server 2003" refers to the following products:

  - Microsoft(R) Windows Server(R) 2003, Standard Edition

  - Microsoft(R) Windows Server(R) 2003, Enterprise Edition

  - Microsoft(R) Windows Server(R) 2003, Standard x64 Edition

  - Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition

  - Microsoft(R) Windows Server(R) 2003 R2, Standard Edition

  - Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition

  - Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition

  - Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition

- The term "Windows(R) XP" refers to the following products:

  - Microsoft(R) Windows(R) XP Professional x64 Edition

  - Microsoft(R) Windows(R) XP Professional

  - Microsoft(R) Windows(R) XP Home Edition

- The Oracle Solaris Operating System may be referred to as Solaris, Solaris Operating System or Solaris OS.

- Microsoft (R) Cluster Server and Microsoft (R) Cluster Service are referred to as MSCS.

- The versions of Systemwalker Runbook Automation that run on Windows systems are referred to as the Windows version.

- The versions of Systemwalker Runbook Automation that run on Linux systems are referred to as the Linux version.

Export Restriction

If this document is to be exported or provided overseas, it is necessary to check Foreign Exchange and Foreign Trade Law, and take the necessary procedure according to these laws.

Trademarks

ITIL(R) is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the US Patent and Trademark Office.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, Windows Server, and Microsoft Cluster Service are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

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

Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Systemwalker, Interstage, CollaborationRing, and Symfoware are registered trademarks of Fujitsu Limited.

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

VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are trademarks or registered trademarks of VMware, Inc. in the United States and other jurisdictions.

Other company names and product names are trademarks or registered trademarks of respective companies.

The company names, system names, product names and other proprietary names that appear in this document are not always accompanied by trademark symbols (TM or (R)).

This guide uses screenshots in accordance with Microsoft Corporation's guidelines.

July 2012

Contents

Chapter 1 Before Installation

This chapter explains the steps required before Systemwalker Runbook Automation can be installed.

1.1 Installation Procedure for Systemwalker Runbook Automation

This section explains how to install Systemwalker Runbook Automation.
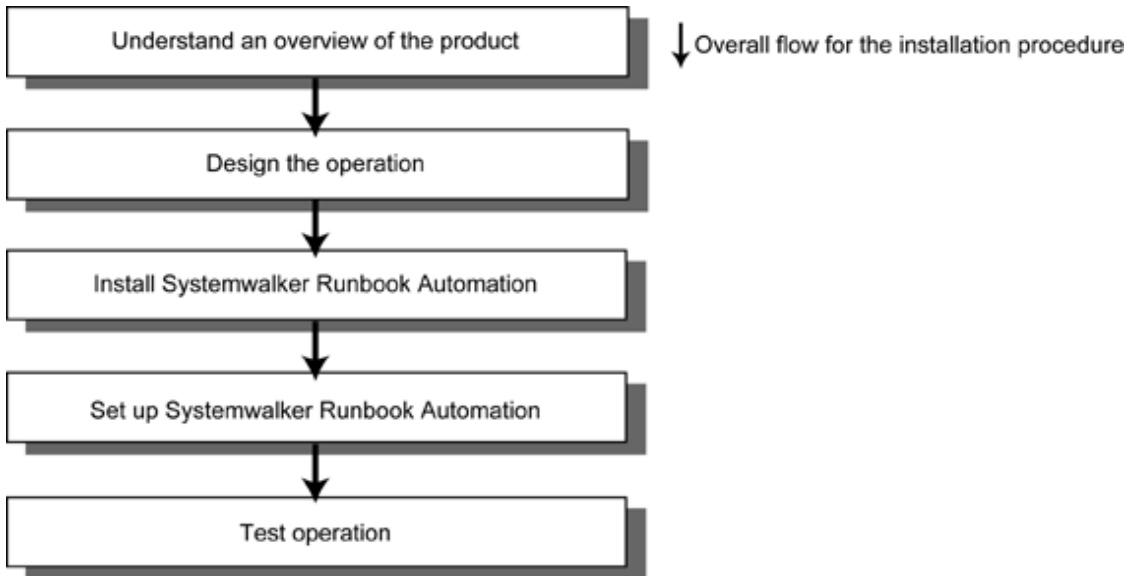
Gain an overview of the product

In order to use Systemwalker Runbook Automation, it is necessary to understand its functions.

Before starting the design work, refer to "Overview" in the *Systemwalker Runbook Automation Technical Guide* for information on the basic terminology and how to use the product.

Design the operation

Design how the operation will work with Systemwalker Runbook Automation.

Refer to "1.2 Design the Operation" for details.

Install Systemwalker Runbook Automation

Install Systemwalker Runbook Automation.

Refer to "Chapter 2 Installation" for details.

Set up Systemwalker Runbook Automation

Set up Systemwalker Runbook Automation using the commands and setup tools provided with the product.

Refer to "Chapter 3 Setup" for details.

Test the operation

Check whether you can log in to the Web console.

Refer to "Chapter 5 Operation Testing" for details.

1.2 Design the Operation

Design the following items to match the operation.

Determine the system configuration

Consider what kind of system configuration to use, by taking into account the environment where Systemwalker Runbook Automation will be installed. Refer to "System Configuration" in the *Systemwalker Runbook Automation Technical Guide* for information on system configurations.

Perform the following installation tasks for each server and computer in the system configuration.

Management Server

Install and set up the Manager for Management Server.

Development Computer

Install Systemwalker Runbook Automation Studio and a Web browser.

Linked Server/Relay Server

Install and set up the Agent for Linked Server/Relay Server.

Business Server

To use file transfer infrastructure as the method of communication between the Management Server and Business Server in the following functions, install "Agent for Business Server".

- Operation component (when the Business Server is specified as the operation target server)

- Collection of configuration information

If the Agent is not installed, communication will be executed using SSH (it must be installed and setup prior to use).

Web Console

Install a Web browser.

If it is in a cluster configuration or it uses VM environment, refer to the "Required Software" in the *Systemwalker Runbook Automation Technical Guide* and consider to which cluster software or VM software is used.

If the installation tasks for the cluster configuration, refer to the *Systemwalker Runbook Automation Cluster Setup Guide.* If the installation tasks for using VM environment, refer to the VM software manual.

Design the port numbers

The list of port numbers used in Systemwalker Runbook Automation is mentioned in "9.1 Port Numbers".

Consider the environment that Systemwalker Runbook Automation will be installed in when designing which port numbers will be used.

Estimate disk space requirements

Refer to "Disk Capacity" in the *Systemwalker Runbook Automation Technical Guide* for information on how to estimate the required disk capacity and reserve file systems of a sufficient size.

Consider which communication method to use

Determine which communication method to use based on the methods supported by the operation components to be used.

File transfer infrastructure

It is a communication method that can be used to install Systemwalker Runbook Automation agent. You do not need to setup it.

SSH

SSH is an abbreviation for Secure Shell. Almost all operation components support SSH. If the Systemwalker Runbook Automation Agent has not been installed on the operation target server or file transfer infrastructure has stopped, then communication will be executed using SSH. If the operation target server is running Windows, then it will be necessary to install and set up SSH.

Windows PowerShell [Windows]

This is the Windows system communication method, and is supported through the operation component "Execute arbitrary command". It can be used by specifying Windows PowerShell as the method of communication with the operation target server. Windows PowerShell 2.0 must be installed and set up in the Management Server and operation target server.

Telnet

Telnet is supported through the operation components "Execute arbitrary command" and "Execute multiple commands". It can be used by specifying Telnet as the method of communication with the operation target server. Telnet must be installed and set up in the operation target server.

RSH and REXEC

These are short for Remote Shell and Remote Process Execution, respectively. Both are supported through the operation component "Execute arbitrary command". They can be used by specifying RSH and REXEC as the methods of communication with the operation target server. RSH and REXEC must be installed and set up in the operation target server.

FTP

This is short for File Transfer Protocol, and is supported through the operation component **Transfer files** It can be used by specifying FTP as the method of communication with the operation target server. FTP must be installed and set up in the operation target server.

Consider what configuration information to collect

In Systemwalker Runbook Automation, the management target ICT device (Business Server or network device) is used by collecting IT resource information. The type of IT resource information to be collected depends on the operation component used.

Additionally, it will be necessary to configure the environment settings in the management target ICT device according to the IT resource information type that will be collected.

The IT resource information types are listed below:

- Node information (IP address, host name, LAN information, name of operating system)

- Logical server information (operating system details, logical CPU, logical memory, logical disk, registry)

- Installed software information (product name, package information, version)

- Hardware information (product name, type name, serial number, physical CPU, physical memory, physical disk)

The relationships between the types and settings for the IT resource information to be collected are shown below.

[1] Collecting only node information (without OS name and Lan information)

[2] Collecting only node information (with OS name and Lan information)

[3] Collecting IT resource information (without Hardware information)

[4] Collecting IT resource information (with Hardware information)

	Information to be collected						SNMP Agent settings	Installation of Systemwalker Runbook Automation agent or setting of SSH (*2)	Installation of linked products (*3)
	Node information			Logical server information	Information about installed software	Hardware information			
	IP address	Host name	OS name LAN information						
[1]	Y	Y (*1)	N	N	N	N	Not required	Not required	Not required
[2]	Y	Y (*1)	Y	N	N	N	Required	Not required	Not required

	Information to be collected						SNMP Agent settings	Installation of Systemwalker Runbook Automation agent or setting of SSH (*2)	Installation of linked products (*3)
	Node information			Logical server information	Information about installed software	Hardware information			
	IP address	Host name	OS name LAN information						
[3]	Y	Y	Y	Y	Y	N	Required	Required	Not required
[4]	Y	Y	Y	Y	Y	Y	Required	Required	Required

Y: Collected, N: Not collected

*1: The host name must be registered in the hosts file or DNS of the server that will execute the collection of the configuration information.

*2: To use SSH, the authentication information (user ID and password) for connecting via SSH must be registered on the Management Server.

*3: The hardware information is collected by the linked server management products installed on the Business Server. For this reason, it will be necessary to install these linked products on the Business Server.

Consider the authentication method to use

Design an authentication method that is required to operate Systemwalker Runbook Automation.

Systemwalker Runbook Automation provides the following authentication methods:

- Authentication via Single Sign-On

- Authentication via LDAP

Authentication via Single Sign-On

This method uses a user that has been registered with a repository in a Single Sign-On environment as the login user for Systemwalker Runbook Automation, and has the following advantages:

- The same user information can be shared by all products that support the Single Sign-On environment. User information can be managed centrally in the repository in the Single Sign-On environment.

- The information that was used to log in to the Systemwalker Runbook Automation Management Server can be used to seamlessly start software products that use Single Sign-On, without a new login window being displayed.

Systemwalker Runbook Automation can use the following Single Sign-On functions:

- Interstage Single Sign-On

Use the Interstage Directory Service to create the repository for the Interstage Single Sign-On environment. If the Interstage Directory Service has already been installed, the existing Interstage Directory Service can be used.

- ServerView Operations Manager Single Sign-On

If there is a ServerView Operations Manager Single Sign-On environment that has already been created, the same authentication infrastructure can be used with Systemwalker Runbook Automation as well. For the repository for the ServerView Operations Manager Single Sign-On environment, use the OpenDS or Active Directory provided by ServerView Operations Manager.

Authentication via LDAP

You can create an environment for authenticating via LDAP.

Note that an LDAP directory already created for user authentication can be used. By making the user the same as the user that operates Systemwalker Runbook Automation, user information can be managed centrally, making user maintenance easier.

Systemwalker Runbook Automation can use the following types of LDAP directory:

- Active Directory

- Interstage Directory Service

- OpenLDAP

Active Directory, the Interstage Directory Service and OpenLDAP can be used to create the LDAP authentication repository. If Active Directory, the Interstage Directory Service, or OpenLDAP has already been installed, these can be used for the LDAP authentication repository.

Add the required users

In order to install Systemwalker Runbook Automation, the following users must be added to the LDAP directory beforehand.

- The users required for installation

    - Refer to "3.1.6 Registering Users, Groups and Organizational Units" for information on adding the users required for installation.

- The users that will use Systemwalker Runbook Automation during operations

    - Refer to "Registering user in Directory Service" and "Registering Local Group and Adding User" in the *Systemwalker Runbook Automation Operation Guide* for information on how to register users with Systemwalker Runbook Automation.

    - Refer to "3.1.6 Registering Users, Groups and Organizational Units" for information on how to register users to use authentication via the Interstage Single Sign-On function.

1.3 Uninstall (middleware)

Uninstall (middleware) is a tool used by Fujitsu middleware products. It performs information management for middleware products, and also, starts the uninstaller for removing these products from the installed systems.

Systemwalker Runbook Automation supports Uninstall (middleware). It is installed, by default, when Systemwalker Runbook Automation is installed.

Uninstall (middleware) controls the installation and uninstallation of Fujitsu middleware products. Note that the installation will not be performed if Uninstall (middleware) is already installed.

The Uninstall (middleware) installation directory is saved at:

[Windows]

%SystemDrive%\FujitsuF4CR

[Linux] [Solaris]

/var/opt/FJSVcir

Chapter 2 Installation

This chapter describes how to install Systemwalker Runbook Automation.

2.1 Pre-installation Tasks

This section describes the steps that need to be followed before installation.

2.1.1 Tuning System Parameters [Linux] [Solaris]

Before the product is installed, the system parameters must be tuned. Refer to the following table for the system parameters that require tuning and their values. Set the parameters as below, depending on the "Type".

If the Type is "Maximum":

There is no need to change the value if the value that has already been set (either the initial value or the previous setting) is equal to or greater than the value in the table. If the current value is smaller than the value in the table, change the parameter to the value in the table.

If the Type is "Addition":

Add the value in the table to the value that has already been set (either the initial value or the previous setting). Check the upper limit for the system before adding the value, and if the sum of the two values is greater than the upper limit for the system, set the parameter to the upper limit for the system.

Refer to the Linux and Solaris manuals for details.

Settings procedure (Linux)

Tuning values for system parameters (Management Servers)

- Shared memory

Parameter	Description	Value	Type
shmmax	Maximum segment size for shared memory	2684354560	Maximum
shmall	Total amount of shared memory available	655360	Maximum
shmmni	Maximum number of shared memory segments	75	Addition

- Semaphores

For the semaphore settings, specify each parameter value using the following format:

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

Parameter	Description	Value	Type
para1	Maximum number of semaphores per semaphore identifier	512	Maximum
para2	Number of semaphores for the entire system	7998	Addition
para3	Maximum number of operators per semaphore call	50	Maximum
para4	Number of semaphore identifiers for the entire system	1364	Addition

- Message queues

Parameter	Description	Value	Type
msgmax	Maximum size of messages	16384	Maximum
msgmnb	Maximum number of messages that can be held in a single message queue	114432	Maximum
msgmni	Maximum number of message queue IDs	1053	Addition

Tuning values for system parameters (Linked Servers, Relay Servers and Business Servers)

- Semaphores

  For the semaphore settings, specify each parameter value using the following format:

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

Parameter	Description	Value	Type
para1	Maximum number of semaphores per semaphore identifier	1	Maximum
para2	Number of semaphores for the entire system	2	Addition
para3	Maximum number of operators per semaphore call	1	Maximum
para4	Number of semaphore identifiers for the entire system	2	Addition

- Message queues

Parameter	Description	Value	Type
msgmnb	Maximum number of messages that can be held in a single message queue	106496	Maximum
msgmni	Maximum number of message queue IDs	512	Addition

Tuning procedure

1. Check the current settings for the system parameters in the tables above:

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

   Example:

   ```
   #/sbin/sysctl -a
   .
   (Omitted)
   .
   kernel.sem = 250 32000 32 128
   kernel.msgmnb = 16384
   kernel.msgmni = 16
   kernel.msgmax = 8192
   kernel.shmmni = 4096
   kernel.shmall = 2097152
   kernel.shmmax = 33554432
   .
   (Omitted)
   .
   ```

2. Refer to "Tuning values for system parameters" above, and compare the current settings to the values above. Calculate an appropriate value for each parameter, taking into account the parameter type ("Maximum" or "Addition").

3. Edit /etc/sysctl.conf.

   Tune the system parameters as displayed in the example below:

   Example:

   ```
   kernel.shmmax=2684354560
   kernel.shmall=655360
   kernel.shmmni=4171

   kernel.sem=512 39998 50 1492

   kernel.msgmax=16384
   kernel.msgmnb=114432
   kernel.msgmni=1069
   ```

4. Check whether the changes have been applied:

   ```
   #/bin/cat /etc/sysctl.conf
   ```

5. Enable the settings above, by using either of the methods below:

   Method 1: Reboot the system:

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

   Method 2: Execute "/sbin/sysctl -p":

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

   Note: There is no need to reboot the system if this command is used.

6. Check whether the parameters have been updated:

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

Confirmation command execution example

```
# /sbin/sysctl -a
   .
  (Omitted)
   .
kernel.sem=512 39998 50 1492
kernel.msgmnb=114432
kernel.msgmni=1069
kernel.msgmax=16384
kernel.shmmni=4171
kernel.shmall=655360
kernel.shmmax=2684354560
   .
  (Omitted)
   .
```

🔰 **Note**

. . . .

This operation must be performed with system administrator (superuser) privileges.

. . . .

Settings procedure (Solaris)

Systemwalker Runbook Automation runs under the following projects.

- system project

  The project for running the daemons, for example, that exists in the operating system initial setup state

- user.root project

  The project for processes that run with root privileges in the operating system initial setup state

System parameter tuning values (Business Server)

- Semaphores

Parameter	Description	Value	Type	Privilege
project.max-sem-ids	Number of semaphore identifiers	512	Addition	Privilege level

- Message queues

Parameter	Description	Value	Type	Privilege
process.max-msg-qbytes	Maximum number of bytes in a queue	106496	Maximum	Privilege level
project.max-msg-ids	Number of wait message identifiers	512	Addition	Privilege level
process.max-msg-messages	Maximum number of messages in the message queue	10650	Addition	Privilege level

- File descriptors

Parameter	Description	Value	Type	Privilege
process.max-file-descriptor	Maximum number of file descriptors	2816	Maximum	Privilege level

📒 **Note**

. . . .

"privileged" is specified as the privilege level in /etc/project.

. . . .

Tuning tasks procedure

Edit the /etc/project file in order to edit the system parameters.

1. Check the values specified in the example below for the parameters listed in the table above.

   Example:

   ```
   # projects -l
   system
   projid : 0
   comment: ""
   users : (none)
   groups : (none)
   attribs:
   ```

user.root

projid : 1

comment: ""

users : root

groups : root

attribs:

noproject

projid : 2

comment: ""

users : (none)

groups : (none)

attribs:

default

projid : 3

comment: ""

users : (none)

groups : (none)

attribs: <--Confirm a project which it has no entry in "attribs"

newtask -p default

prctl $$
process: 1000: sh

NAME PRIVILEGE VALUE FLAG ACTION RECIPIENT

...
(omitted)
...
process.max-msg-messages

privileged 8.19K - deny -

system 4.29G max deny -

process.max-msg-qbytes

privileged 64.0KB - deny -

system 16.0EB max deny -
process.max-file-descriptor

basic 256 - deny 1000

privileged 65.5K - deny -

system 2.15G max deny -
project.max-msg-ids

privileged 128 - deny -

system 16.8M max deny -

project.max-sem-ids

privileged 128 - deny -

system 16.8M max deny -
...

```
(omitted)
...
```

2. Compare the parameter values listed above against the ones listed in section "Tuning values for system parameters" above, then calculate an appropriate value, considering the Maximum and Addition types for each parameter.

3. Edit /etc/project.

   To tune the system parameters, edit the tuning records in the /etc/project file as shown in the following example.

   Example:

   ```
   system:0::::project.max-sem-ids=(privileged,640,deny)
   ;process.max-msg-qbytes=(privileged,106496,deny)
   ;project.max-msg-ids=(privileged,640,deny)
   ;process.max-msg-messages=(privileged,19032,deny)
   user.root:1:::: project.max-sem-ids=(privileged,640,deny)
   ;process.max-msg-qbytes=(privileged,106496,deny)
   ;project.max-msg-ids=(privileged,640,deny)
   ;process.max-msg-messages=(privileged,19032,deny)
   ```

   P Point

   ···

   - Define the settings values on a separate line for each project.

   - Set parameters for the system and for the superuser.

   ···

4. Reboot the system to reflect the change.

5. Check that the system parameters that were set are effective through the output of the following command:

   ```
   # projects -l
   ```

Example of the confirmation command execution

```
# projects -l
system
        projid : 0
        comment: ""
        users  : (none)
        groups : (none)
        attribs: project.max-sem-ids=(privileged,640,deny)
                 process.max-msg-qbytes=(privileged,106496,deny)
                 project.max-msg-ids=(privileged,640,deny)
                 process.max-msg-messages=(privileged,19032,deny)
user.root
        projid : 1
        comment: ""
        users  : root
        groups : root
        attribs: project.max-sem-ids=(privileged,640,deny)
                 process.max-msg-qbytes=(privileged,106496,deny)
                 project.max-msg-ids=(privileged,640,deny)
                 process.max-msg-messages=(privileged,19032,deny)
noproject
        projid : 2
        comment: ""
        users  : (none)
```

```
        groups : (none)
        attribs:
default
        projid : 3
        comment: ""
        users  : (none)
        groups : (none)
        attribs:
```

2.1.2 Setting up the Firewall

To install Systemwalker Runbook Automation in an environment where a firewall function is being used, the firewall must be set up so as to allow communications to the necessary ports.

Refer to the operating system manual for information on how to set up the firewall.

Refer to "9.1 Port Numbers" for details on the port numbers used by Systemwalker Runbook Automation.

It must be set up so as to allow "The port number which needs to accept from external server".

📎 Note
....

Note for using on Windows Server 2008

Because the firewall function is effective with default settings, the using port number and protocol must be set up so as to allow exception firewall.

....

2.1.3 Checking the Settings in the hosts File or the DNS Server

It must be possible to resolve the IP address correctly from the local host name. Check the hosts file or the DNS server settings before installing the product, and ensure that host names can be resolved correctly.

2.1.4 Installing required software

Install required software depend on system construct and using Operation Component.

Management Server

Linux

Install the following software which attached operating system.

Install them referring to operating system manuals.

- redhat-lsb packages

- Elfutils package

Red Hat Enterprise Linux 5.2 or earlier

elfutils-libelf-0.125-3.el5.i386.rpm (*1)

Red Hat Enterprise Linux 5.3 or later

elfutils-libelf-0.137-3.el5.i386.rpm

Red Hat Enterprise Linux 6.0 or later

elfutils-libelf-0.148-1.el6.i686.rpm

*1: Install 32-bit version of elfutils package even if Linux operating system is 64-bit version.

For Red Hat Enterprise Linux 6.0 or later, also install the software listed below, which is distributed with the operating system (refer to the operating system manual before installing).

Red Hat Enterprise Linux 6.0 or later (for x86)

- alsa-lib package (32-bit version)

- cloog-ppl package (32-bit version)

- compat-readline5 package (32-bit version)

- compat-libtermcap package (32-bit version)

- cpp package (32-bit version)

- file package (32-bit version)

- gcc package (32-bit version)

- gcc-c++ package (32-bit version)

- gdb package (32-bit version)

- glibc-devel package (32-bit version)

- glibc-headers package (32-bit version)

- kernel-headers package (32-bit version)

- libICE package (32-bit version)

- libSM package (32-bit version)

- libX11 package (32-bit version)

- libX11-common package

- libXau package (32-bit version)

- libXext package (32-bit version)

- libXi package (32-bit version)

- libXp package (32-bit version)

- libXt package (32-bit version)

- libXtst package (32-bit version)

- libgomp package (32-bit version)

- libstdc++-devel package (32-bit version)

- libtool-ltdl package (32-bit version)

- libxcb package (32-bit version)

- make package (32-bit version)

- mpfr package (32-bit version)

- nss-softokn-freebl package (32-bit version)

- perl package (32-bit version)

- perl-Module-Pluggable package (32-bit version)

- perl-Pod-Escapes package (32-bit version)

- perl-Pod-Simple package (32-bit version)

- perl-libs package (32-bit version)

- perl-version package (32-bit version)

- ppl package (32-bit version)

- strace package (32-bit version)

- tcsh package (32-bit version)

- unixODBC package (32-bit version)

Red Hat Enterprise Linux 6.0 or later (for Intel64)

- alsa-lib package (32-bit version)

- audit-libs package (32-bit version)

- cloog-ppl package (64-bit version)

- compat-readline5 package (32-bit version)

- compat-libtermcap package (32-bit version)

- cpp package (64-bit version)

- cracklib package (32-bit version)

- db4 package (32-bit version)

- expat package (32-bit version)

- file package (64-bit version)

- gcc package (64-bit version)

- gcc-c++ package (64-bit version)

- glibc package (32-bit version)

- glibc-devel package (32-bit version)

- glibc-headers package (64-bit version)

- kernel-headers package (64-bit version)

- libICE package (32-bit version)

- libSM package (32-bit version)

- libX11 package (32-bit version)

- libX11-common package

- libXau package (32-bit version)

- libXext package (32-bit version)

- libXi package (32-bit version)

- libXp package (32-bit version)

- libXt package (32-bit version)

- libXtst package (32-bit version)

- libattr package (32-bit version)

- libcap package (32-bit version)

- libgcc package (32-bit version)

- libgomp package (64-bit version)

- libselinux package (32-bit version)

- libstdc++ package (32-bit version)

- libstdc++-devel package (64-bit version)

- libtool-ltdl package (32-bit version)

- libuuid package (32-bit version)

- libxcb package (32-bit version)

- make package (64-bit version)

- mpfr package (64-bit version)

- ncurses-libs package (32-bit version)

- nss-softokn-freebl package (32-bit version)

- pam package (32-bit version)

- perl package (64-bit version)

- perl-Module-Pluggable package (64-bit version)

- perl-Pod-Escapes package (64-bit version)

- perl-Pod-Simple package (64-bit version)

- perl-libs package (64-bit version)

- perl-version package (64-bit version)

- ppl package (64-bit version)

- readline package (32-bit version)

- tcsh package (64-bit version)

- unixODBC package (32-bit version)

- zlib package (32-bit version)

Using operation components developed using Perl

Install the following software.

- strawberry perl 5.12.0

Specify any directory as install directory.

After installing, it must be set up information of install path to operation component execution setup file. Also if you use library for Perl which Systemwalker Runbook Automation is provided, it is necessary to install the following module.

- XML::Simple 2.18

- XML::Parser 2.40

Note

In library which Systemwalker Runbook Automation is provided, only "Input information library" can use in Operation component developed by Perl script. Install Perl library and Perl module to Management Server as necessary.

For the detail about library which Systemwalker Runbook Automation provide, refer to "*Systemwalker Runbook Automation Reference Guide*"

Building an environment using LDAP authentication

Install one of the following directory services.

- OpenLDAP

- Active Directory

- Interstage Directory Service

However, Interstage Directory Service is installed with installing Systemwalker Runbook Automation.

You do not need to install Interstage Directory Service again.

Linked Server/Relay Server/Business Server

Linux

Install the software shown below, which is provided with the operating system (refer to the operating system manual before installing it).

- redhat-lsb packages

On Red Hat Enterprise Linux 6 (for Intel64) environments, install the 32-bit version of the following software provided with the operating system. Refer to the operating system manual for the installation procedure. [Linux]

- expat package

- glibc package

- libattr package

- libcap package

- libgcc package

- libstdc++ package

- nss-softokn-freebl package

- zlib package

Solaris

If collecting IT resource information, install the following software:

- Enhanced Support Facility

Using the operation component to direct the operation to each server

- The software below is required to perform SSH communications between the Management Server and the Linked Server, Relay Server and Business Server.

[Windows]

- SSH V2.0 or later

Install OpenSSH (cygwin OpenSSH V1.7 or later) in environments in which SSH has not been installed yet.

[Linux] [Solaris]

- SSH V2.0 or later

In Red Hat Enterprise Linux 5.0 or later and Solaris 10 or later, SSH is already installed as a standard feature. Install OpenSSH in environments in which SSH has not been installed yet.

- The software below is required to perform Windows PowerShell communications between the Management Server and the Linked Server, Relay Server and Business Server.

[Windows]

- Windows PowerShell 2.0

Install in environments in which it has not been installed yet. Refer to "Article ID: 968929" of "Microsoft Support" for information on Windows PowerShell 2.0.

- The software below is required to perform Telnet communications between the Management Server and the Linked Server, Relay Server and Business Server.

  [Windows]

  - Telnet Server Service

    Install the Telnet Server Service in environments in which it has not been installed yet.

  [Linux]

  - telnet-server

    Install telnet-server in environments in which it has not been installed yet.

  [Solaris]

  - telnet service

    The telnet service is already installed as a standard operating system feature.

- The software types shown below are required to perform RSH/REXEC communications between the Management Server and the Linked Server, Relay Server, and Business Server.

  [Windows]

  - Subsystem for UNIX-based Application(SUA)

    Install Subsystem for UNIX-based Application(SUA) in environments in which it has not been installed yet.

  [Linux]

  - rsh-server

    Install rsh-server in environments in which it has not been installed yet.

  [Solaris]

  - rexec service

    The rexec service is already installed as a standard operating system feature.

- The software below is required to perform FTP communications between the Management Server and the Linked Server, Relay Server and Business Server.

  [Windows]

  - Internet Information Service (IIS) and FTP Service

  [Linux] [Solaris]

  - vsftpd

- The software below is required to perform SNMP communications between the Management Server and the Linked Server, Relay Server and Business Server.

  [Windows]

  - SNMP Agent

  [Linux]

  - Net-snmp (or ucd-snmp)

  [Solaris]

  Solaris 10

  - SUNWsmmgr

  - SUNWsmagt

  - SUNWsmcmd

  Solaris 11

- system/management/snmp/net-snmp/addons

- system/management/snmp/net-snmp

- system/management/snmp/net-snmp/documentation (required by the SNMP Agent document)

Development Computer

- Confirm to be installed one of the following Web browsers.

  - Microsoft(R) Internet Explorer 7

  - Microsoft(R) Internet Explorer 8

  - Microsoft(R) Internet Explorer 9

Web console

- Confirm to be installed one of the following Web browsers.

  - Microsoft(R) Internet Explorer 7

  - Microsoft(R) Internet Explorer 8

  - Microsoft(R) Internet Explorer 9

2.2 Installing on Management Servers

This section describes how to install Systemwalker Runbook Automation on Management Servers.

Note
- Ensure that no conflicting products have been installed on the Management Server.

- Refer to "Appendix A Installing Operation Management Products on the Systemwalker Runbook Automation Management Server" before installing any other operation management products on the Management Server.

2.2.1 Notes before Installing

This section describes points to note before installing the Manager or Agent on the Management Server.

The following functions are installed on the Management Server:

- The following functions that the Systemwalker Runbook Automation Management Server requires to operate:

  - Interstage Application Server

  - Interstage Business Process Manager

  - Systemwalker Operation Manager

  - PostgreSQL

  - Fujitsu XMLprocessor

  - CMDB Manager

  - SMEE, Securecrypto runtime library

  - File transfer function

- The following function that the Systemwalker Runbook Automation Business Server requires to operate:

  - File transfer infrastructure

Meanwhile, when uninstalled Systemwalker Runbook Automation Management Server, a part of function, it is shared with other product, so it is not uninstalled.

For the detail of uninstall, refer "Uninstall Management Server"

[Windows]

- Ensure that the operating system is not a Japanese environment.

- If a Terminal Server has been installed, then change it to Install Mode:

  CHANGE USER /INSTALL

- If Internet Information Service (IIS) has been installed, then the port number for IIS may conflict with the port number for the Web server for Interstage Application Server. In this case, either change the port number for IIS beforehand, or specify a port number during the installation of Systemwalker Runbook Automation that does not cause conflict.

- During Systemwalker Runbook Automation been installing, "swrbadbuser " and "swrbajobuser " are registered as OS user. Confirm that "swrbadbuser" and "swrbajobuser" have not been registered in OS. If they have already exist, delete them.

[Linux]

- Look up the LANG item in /etc/sysconfig/i18n, and check that the value of the character encoding for the system is not "ja_JP.UTF-8", "ja_JP.SJIS" or "ja_JP.WINDOWS-31J". These characters have not been supported.

- During Systemwalker Runbook Automation been installing, "swrbadbuser" and "swrbajobuser" are registered as OS user. Confirm that "swrbadbuser" and "swrbajobuser" have not been registered in OS. If they have already exist, delete them.

- Check the /etc/hosts settings to confirm whether "localhost" has been set in IPv4 format (127.0.0.1). If it has been set in IPv6 format, change the setting to IPv4 format (127.0.0.1).

- Please confirm /etc/hosts and make sure "127.0.0.1" is not set to localhostname.

2.2.2 Installing on Windows Systems

This section describes how to install Systemwalker Runbook Automation on the Windows Management Server.

There are two types of installation: Standard Installation and Custom Installation. To set up all parameters using the default values, perform a Standard Installation. To set up parameters using values other than the default values, perform a Custom Installation.

Note

- To install Systemwalker Runbook Automation on a cluster environment, there are other points for which care is required.

  Refer to "Installing Systemwalker Runbook Automation" in the *Systemwalker Runbook Automation Cluster Setup Guide*.

- If the installation fails, restart the system and then log in again as the same user that performed the installation. Then, uninstall the product according to the uninstallation procedure.

  After uninstalling the product, eliminate the cause of the failure by referring to the meaning and action method for the message that was output, and then install Systemwalker Runbook Automation again.

  Refer to the *Systemwalker Runbook Automation Message Guide* for details on the message.

  Refer to "Chapter 7 Uninstallation" for information on how to uninstall Systemwalker Runbook Automation.

  If the problem cannot be addressed based on the message that was output, collect the following log file from the directory indicated by the %SystemDrive% environment variable, and then contact Fujitsu technical support:

  - swrba_inst.log

2.2.2.1 Standard Installation

This section explains the Standard Installation procedure.

To set all of the installation parameters to the default values, perform a Standard Installation.

The Standard Installation procedure is explained below.

A Standard Installation installs Systemwalker Runbook Automation using the following default values:

Setting item	Meaning	Default value
Installation folder	The installation folder for the Management Server	C:\Fujitsu\Systemwalker\SWRBAM
CMDB Manager database directory	Database storage folder for the CMDB Manager	C:\Fujitsu\Systemwalker\SWRBAM \CMDB
Interstage Management Console port	The port number for accessing the Interstage Management Console	12000
Port number of Web server (Interstage HTTP Server)	The port number for accessing the Web console	80
Port number of CORBA service	Port numbers used internally	8002
Port number of HTTP Listener	Port numbers used internally	28080
Port number of HTTP Listener for Operation Management	The port number for accessing the Interstage Java EE Management Console	12001
Port number of IIOP	Port numbers used internally	23600
Port number of IIOP_SSL	Port numbers used internally	23601
Port number of IIOP_MUTUALAUTH	Port numbers used internally	23602
Port number of JMX_ADMIN	Port numbers used internally	8686
Subsystem Number	The subsystem number for Systemwalker Operation Manager that is used by Systemwalker Runbook Automation	9
Job Scheduler Port number	Port numbers used internally	9690
Job Execution Control Port number	Port numbers used internally	9691

Note

Refer to "2.2.2.2 Custom Installation" for information on the settings and information used to check for port number duplication.

1. Log in using an account that belongs to the Administrators group.

2. Start the installer.

   The installer will start automatically when the following DVD-ROM is inserted in the DVD-ROM drive. If the installer does not start automatically, start it manually by executing "swsetup.exe".

   - Systemwalker Runbook Automation Media Pack (V15.1.0) Disc No. 1/2

Note
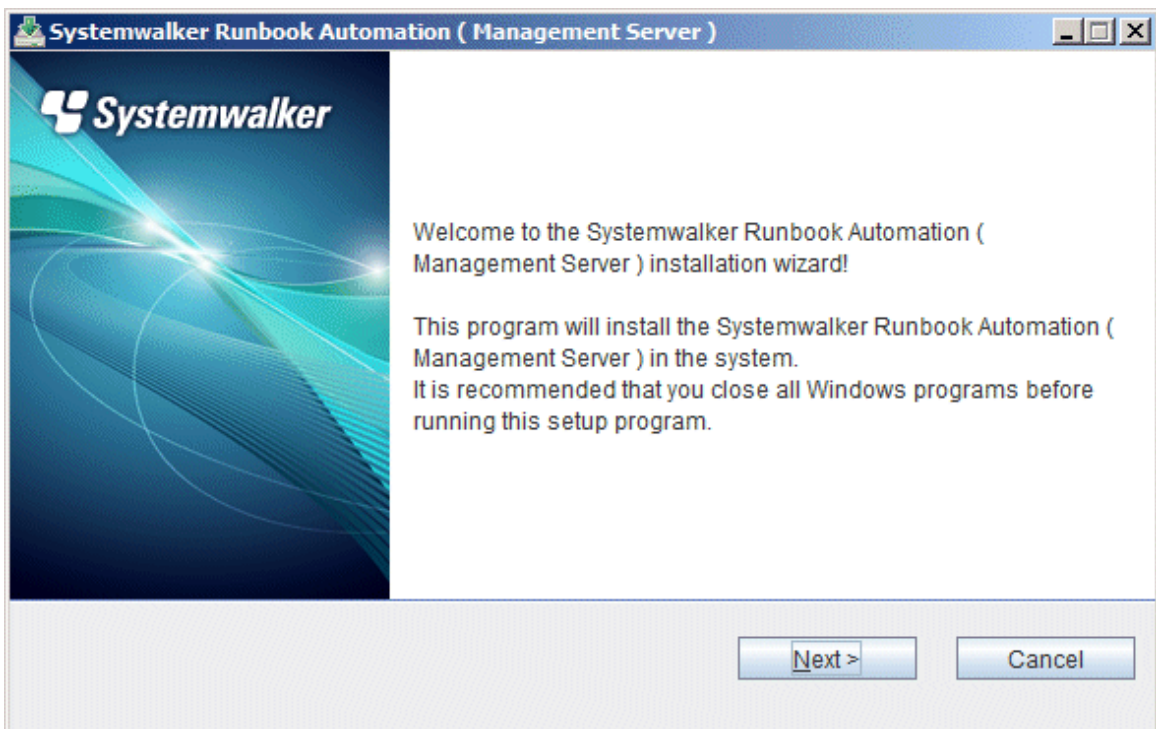
If the operating system being used is Windows Server 2008, execute the installer as an Administrator.

In the window that is displayed, select **Install on Management Server**.

3. The welcome dialog box will be displayed.

Check the content of the dialog box and click the **Next** button.

4. The **Select Installation Type** dialog box will be displayed.

   Select **Standard Installation** and click the **Next** button.
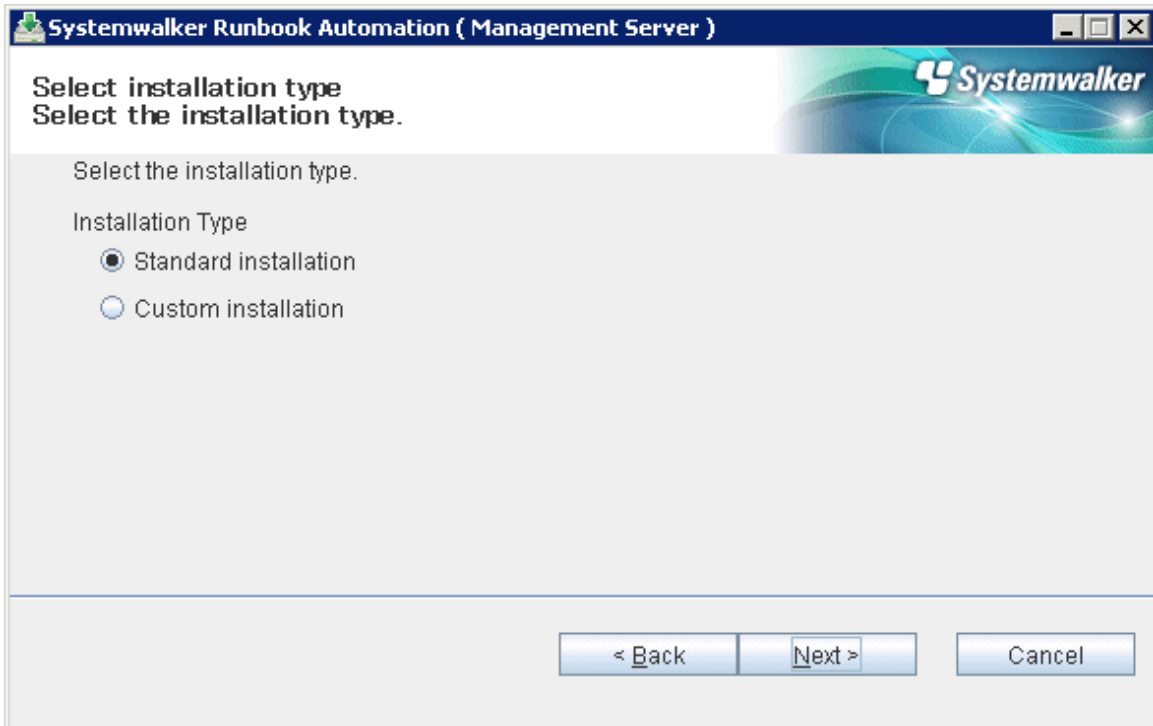
5. Check the installation settings.

   In the **Check on Installation** window, check the content that has been entered, and then click the **Confirm** button if there are no mistakes. Installation will start.

   To change the settings, click the **Back** button and then select **Custom Installation** in the **Select Installation Type** dialog box.
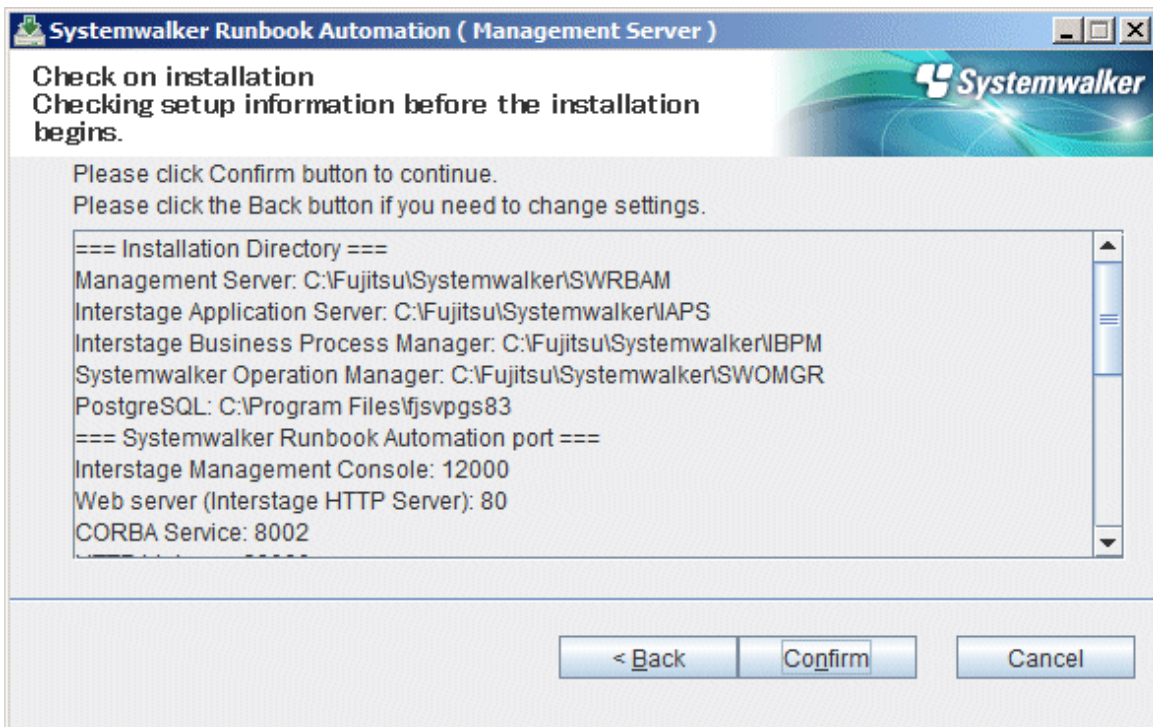
6. After the installation is completed, the window shown below will be displayed.

   Click the **Finish** button.
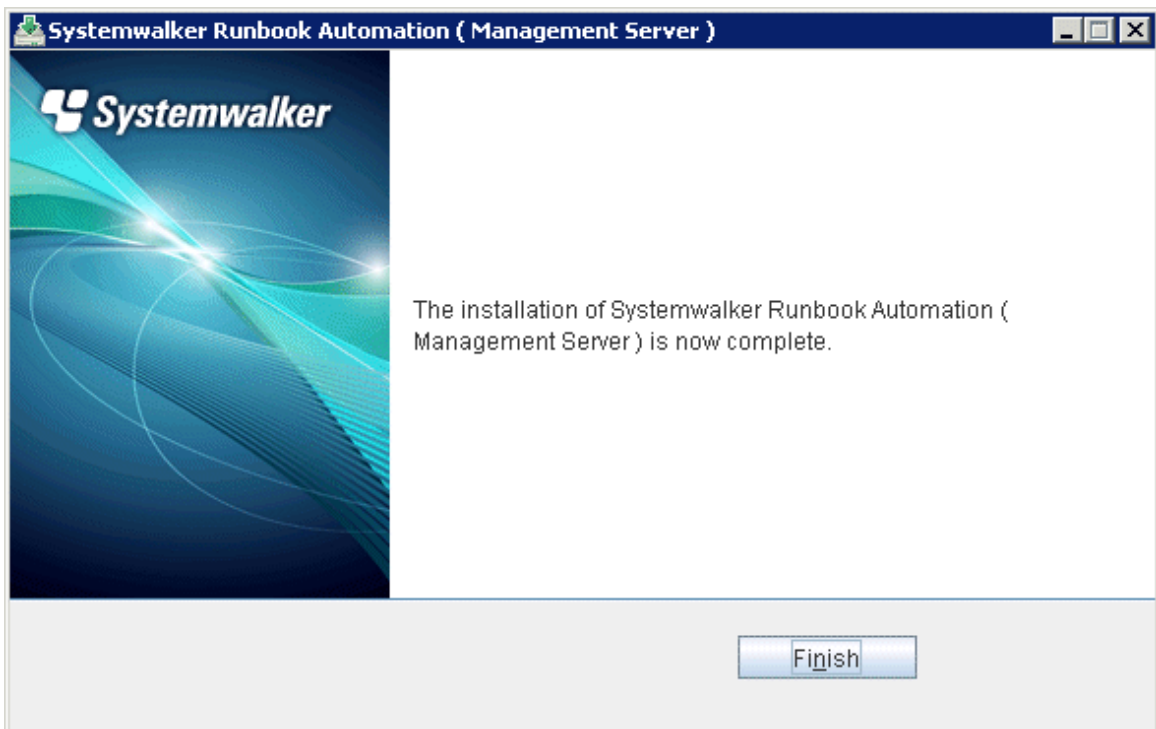
7. Restart the system.
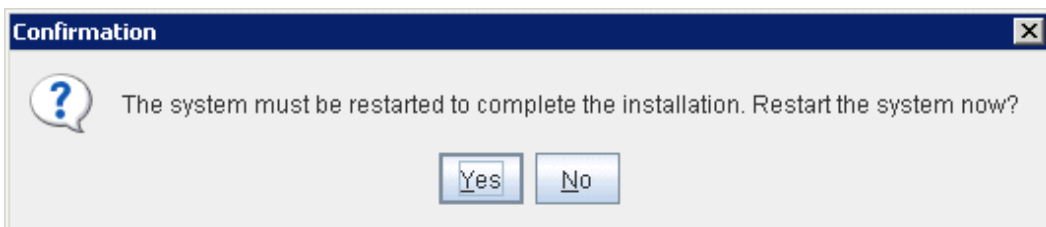
   Click the **Yes** button.

2.2.2.2 Custom Installation

This section explains the Custom Installation procedure.

1. Log in using an account that belongs to the Administrators group.

2. Start the installer.

   The installer will start automatically when the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 1/2" DVD-ROM is inserted in the drive.

   If the installer does not start automatically, then start it manually by executing "swsetup.exe".

   Note
   ....
   If the operating system being used is Windows Server 2008, execute the installer as an administrator.
   ....

In the window that is displayed, select **Install on Management Server**.
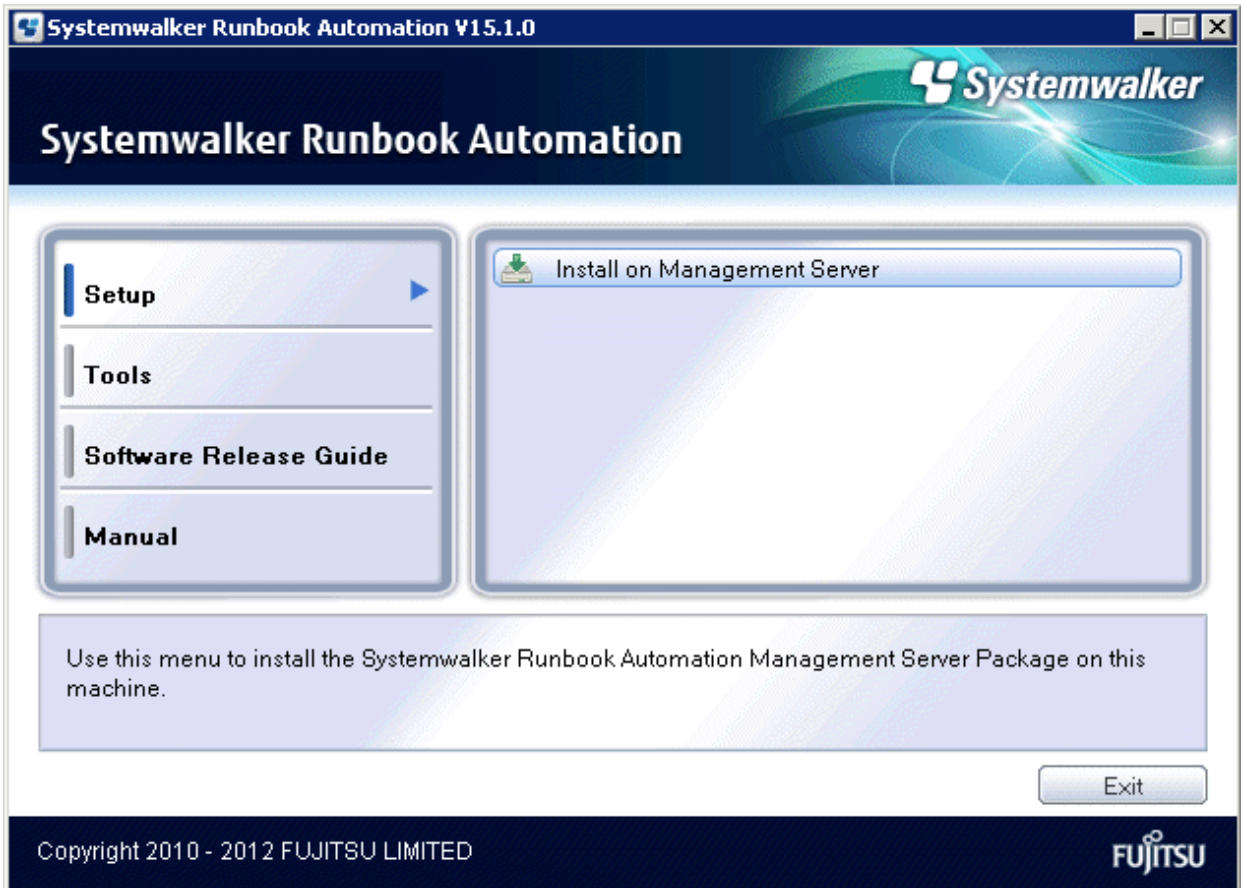
3. The welcome dialog box will be displayed.

Check the content of the dialog box and click the **Next** button.
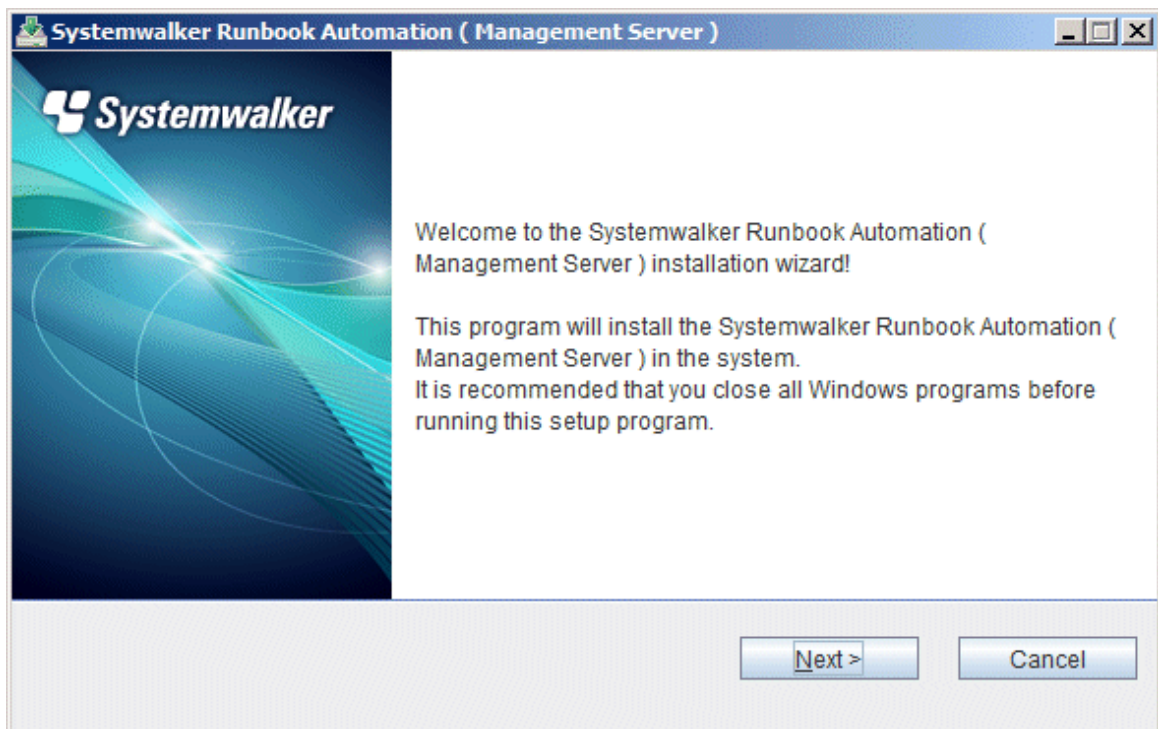
4. The **Select Installation Type** dialog box will be displayed.

   Select **Custom Installation** and click the **Next** button.
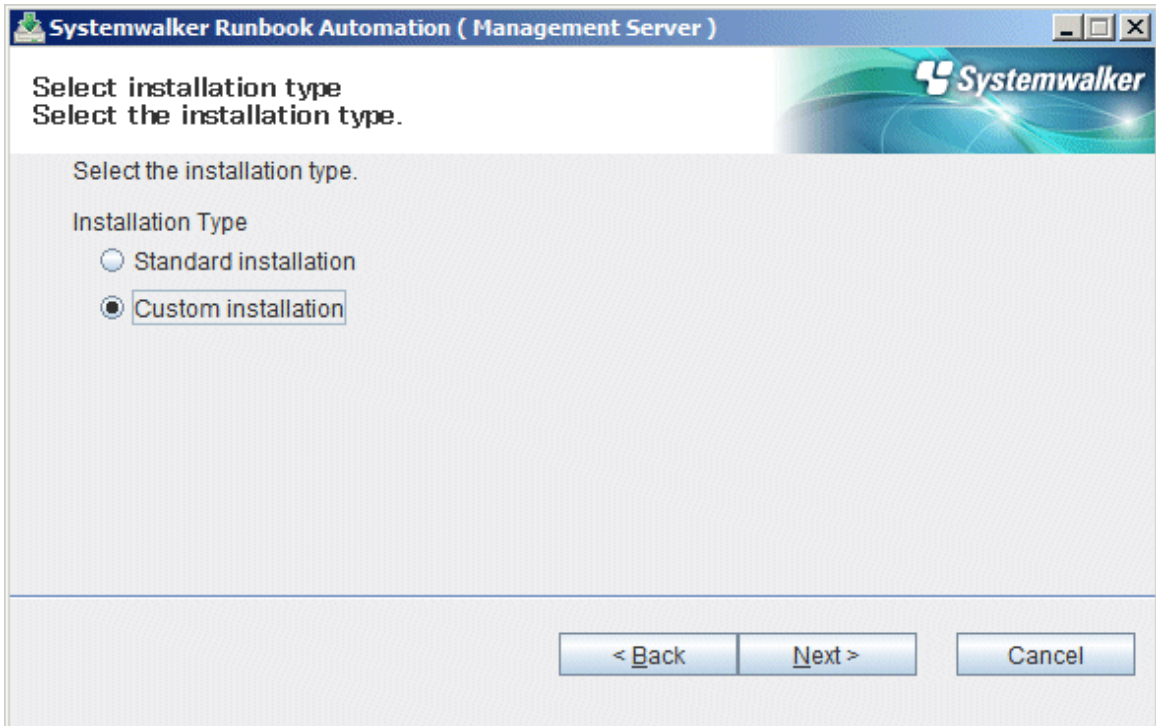
5. Select the installation directory for Systemwalker Runbook Automation.

   Specify the directory, and then click the **Next** button.
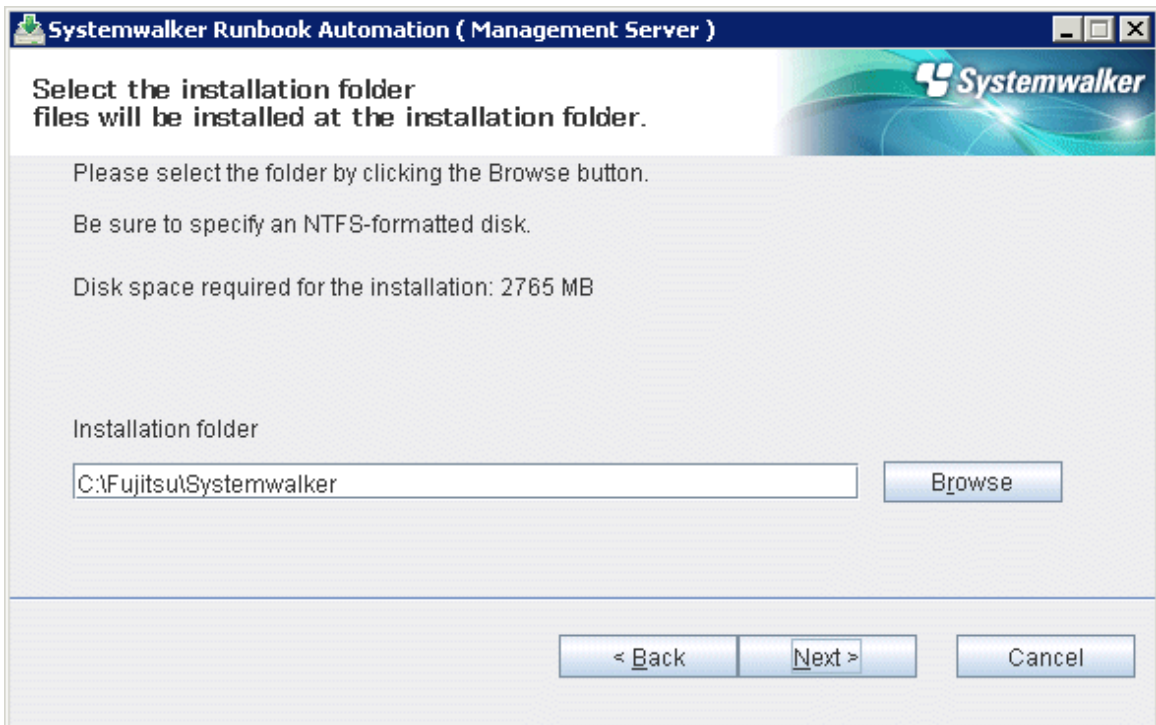
Note

- The installation directory can contain up to 25 characters.

- Specify an NTFS format disk for the installation directory.

- Do not specify path or relative path name beginning with "\\".

- The directory name can contain only alphanumeric characters, hyphens (-), underscores (_), and spaces.

- A standard directory under "C:\Program Files" or "C:\Program Files (x86)" can also be specified.

- Do not include whitespace characters in the installation directory if using the library below to create an operation component, otherwise the operation results from using the library are not guaranteed.

    - File transfer

    - Configuration Management Database

    - Host name change

    - Network settings

    - Install software

- The required products will be installed using the following directory configuration. Meanwhile if the directory which you specify already exists and the directory has any file or directory, it may have failed to install:

    - <Installation directory>/SWRBAM: Systemwalker Runbook Automation Management Server

    - <Installation directory>/IBPM: Interstage BPM

    - <Installation directory>/IAPS: Interstage Application Server

    - <Installation directory>/SWOMGR: Systemwalker Operation Manager

- Do not change the following directory as static directory

    - Installation directory for PostgreSQL

    - %ProgramFiles%\ fjsvpgs83

6. Specify the port numbers used by Systemwalker Runbook Automation.

    In the **Port Number Settings** (1/2) window, specify the port number to be used by Systemwalker Runbook Automation, and then click the **Next** button.

In the **Port Number Settings (2/2)** window, specify the port number to be used by Systemwalker Runbook Automation, and then click the **Next** button.

🖙 **Note**

. . . .

- Do not specify port numbers currently used. To check which port numbers are currently used:

  ```
  > netstat -a -n
  ```

- Even port numbers not displayed by the command above might be in use by another application. Refer to "9.1 Port Numbers" for information on how to check that the port number is not being used.

- There is no confirmation for port number on the environment which installed Systemwalker Service Catalog Manager. Use same port number which you specified when you installed Systemwalker Service Catalog Manager

. . . .

7. Specify the directory where the CMDB Manager database is stored.

   Set **Select the Database Storage Folder** window, then click the **Next** button.

It is recommended to store the CMDB Manager database in a dedicated disk, because performance will drop if the database conflicts with other applications for disk I/O.
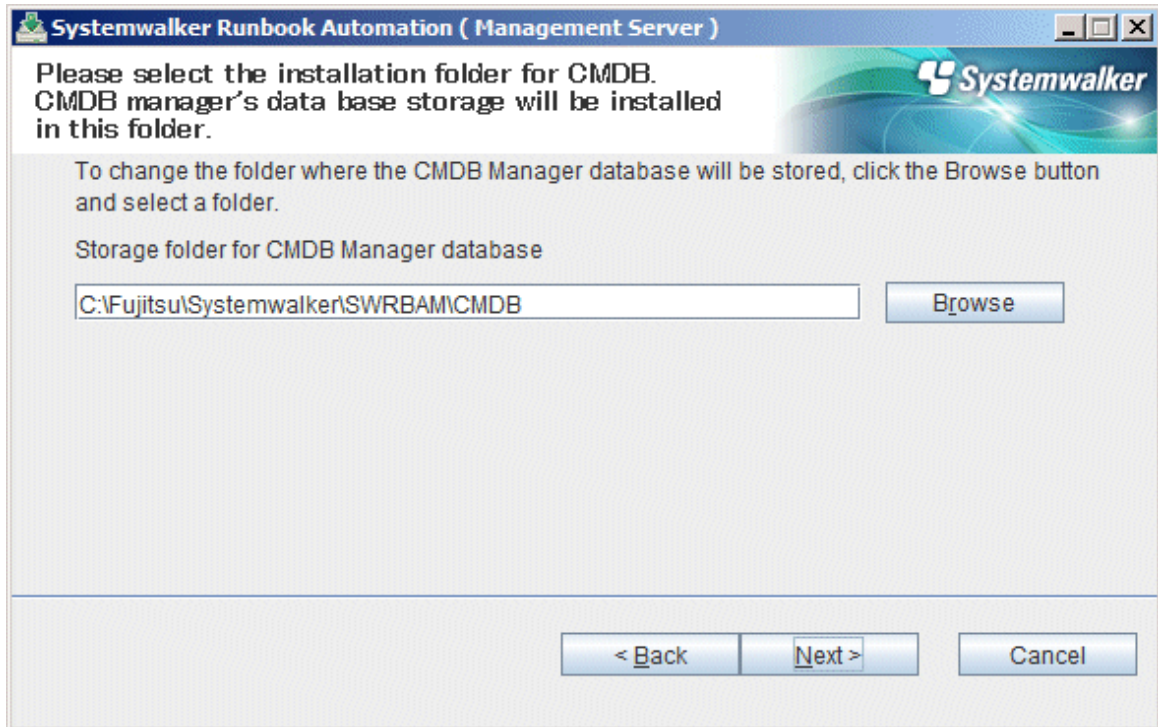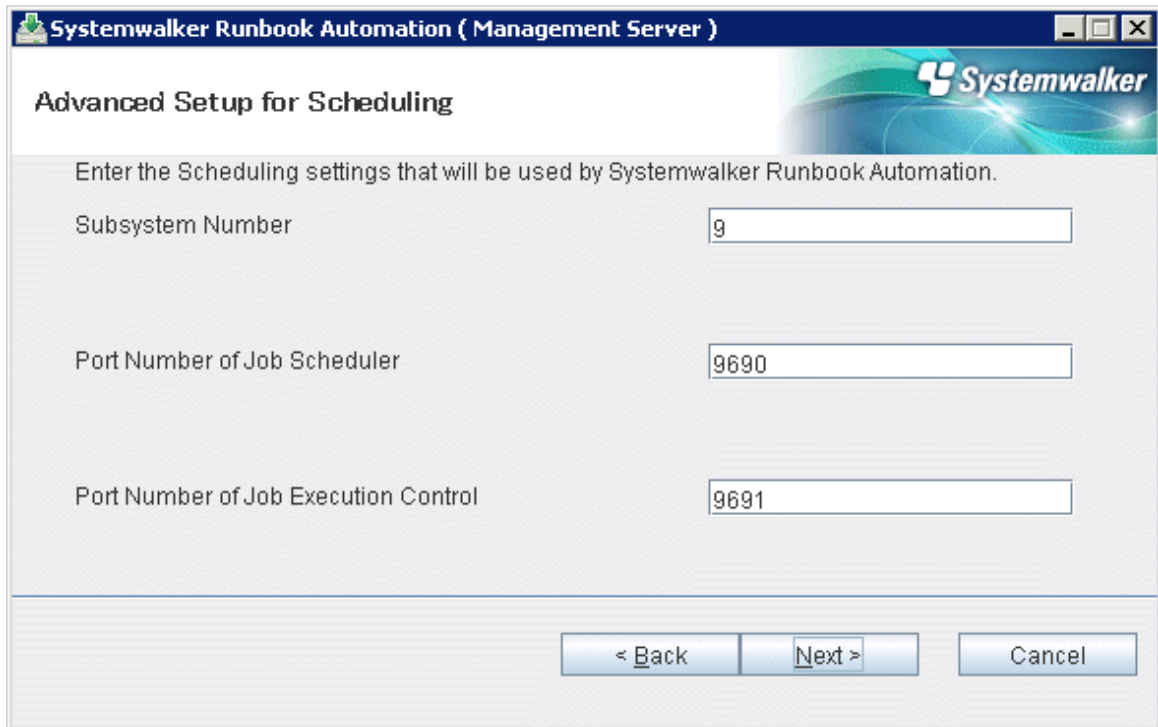
Note

- The installation directory can contain up to 64 characters.

- Specify an NTFS format disk for the installation directory.

- Specify new directory definitely.

- Do not specify path or relative path name beginning with "\\".

- The directory name can contain only alphanumeric characters, hyphens (-), underscores (_), and spaces.

- A standard directory under "C:\Program Files" or "C:\Program Files (x86)" can also be specified.

8. Specify the subsystem number and port number used by the schedule function.

If the default port number used by the schedule function is already used by another application, specify a different port number.

If you do not have Systemwalker Operation Manager coexist on the Management Server, or if the default port number is not used by another application, leave the default settings unchanged, and click the **Next** button.

Note

- The port number that is currently being used can be checked using the following command. Do not specify the port number that is displayed by this command.

```
> netstat -a -n
```

- Although the specified port number is not currently in use, it may already have been assigned to other software. Refer to "9.1 Port Numbers" to check that the port number has not already been used.

9. Check the installation settings.

Ensure that the settings are correct, and then click the **Next** button.
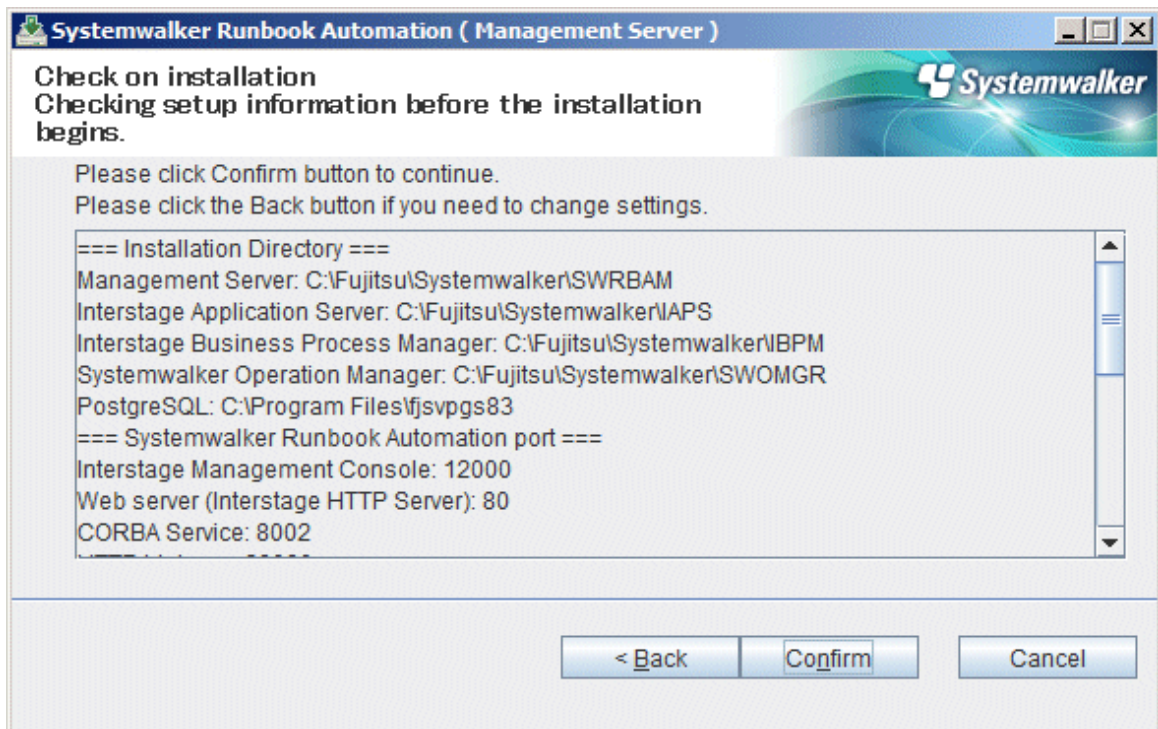
10. Installation will complete.

In the completion window, click the **Finish** button.
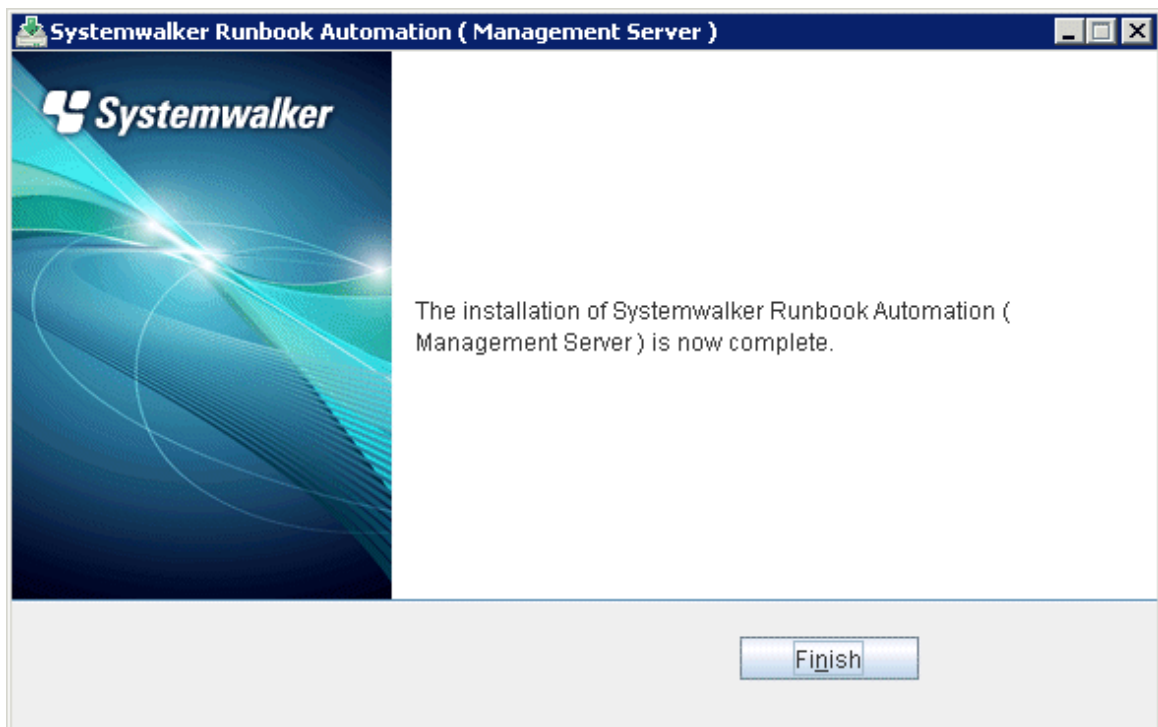
11. Restart Systemwalker Runbook Automation, then click the **Yes** button.
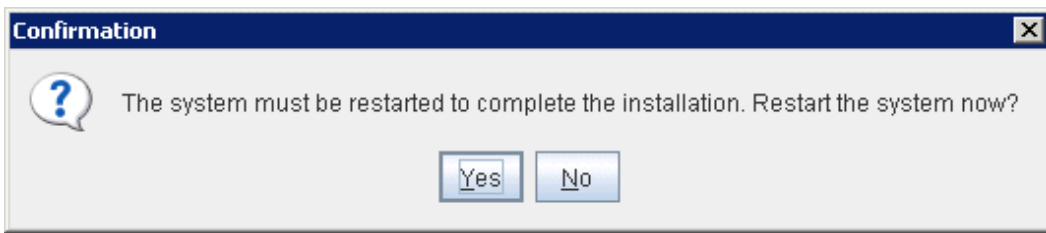
2.2.3 Installing on Linux Systems

This section describes how to install when the Management Server is running on Linux.

There are two types of installation: Standard Installation and Custom Installation. To set up all parameters using the default values, perform a Standard Installation. To set up parameters using values other than the default values, perform a Custom Installation.

📋 Note

- If the installation fails, restart the system and then log in again as the same user that performed the installation. Then, uninstall the product according to the uninstallation procedure.

  After uninstalling the product, eliminate the cause of the failure by referring to the meaning and action method for the message that was output, and then install Systemwalker Runbook Automation again.

  Refer to the *Systemwalker Runbook Automation Message Guide* for details on messages.

  Refer to "Chapter 7 Uninstallation" for details on how to uninstall Systemwalker Runbook Automation.

  If the problem cannot be resolved based on the messages that are output, collect the following log files and contact Fujitsu technical support.

    - /var/tmp/swrba_inst.log

    - /var/tmp/bndl_inst.log

    - /opt/FJSVibpm/Interstage-BPM-log.txt

    - /opt/FJSVcmdbm/var/log/cmdbInstLog

    - /var/opt/FJSVcmdbm/var/log/cmdbInstLog

2.2.3.1 Standard Installation

This section explains the Standard Installation procedure.

A Standard Installation installs Systemwalker Runbook Automation using the following default values:

Setting item	Meaning	Default value
CMDB Manager database directory settings	Database storage directory for the CMDB Manager	/var/opt
Interstage Management Console port	The port number for accessing the Interstage Management Console	12000
Port number of Web server (Interstage HTTP Server)	The port number for accessing the Web console	80
Port number of CORBA service	Port numbers used internally	8002
Port number of HTTP Listener	Port numbers used internally	28080

Setting item	Meaning	Default value
Port number of HTTP Listener for peration Management	The port number for accessing the Interstage Java EE Management Console	12001
Port number of IIOP	Port numbers used internally	23600
Port number of IIOP_SSL	Port numbers used internally	23601
Port number of IIOP_MUTUALAUTH	Port numbers used internally	23602
Port number of JMX_ADMIN	Port numbers used internally	8686
Subsystem Number	The subsystem number for Systemwalker Operation Manager that is used by Systemwalker Runbook Automation	9
Job Scheduler Port number	Port numbers used internally	9690
Job Execution Control Port number	Port numbers used internally	9691

Note

Refer to "2.2.3.2 Custom Installation" for information on the settings and information used to check for port number duplication.

1. Log in as a superuser on the system.

2. Insert the DVD-ROM in the DVD-ROM drive.

   Insert the DVD-ROM labeled "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 1/2" in the DVD-ROM drive.

3. Mount the DVD-ROM.

   Use the following command to mount the DVD-ROM.

   If the DVD-ROM is automatically mounted by the "autofs" automatic mount daemon, "noexec" will be set for the mount option, and so the installer will fail to start.

   ```
   # mount -t iso9660 -r /dev/mnt <mount point for the DVD-ROM>
   ```

4. Start the installer.

   Executing the special installation command for this software (swsetup) installs multiple packages as a batch. The method for starting the installer is as follows:

   ```
   # <mount point for the DVD-ROM>/swsetup
   ```

5. A welcome window will be displayed. Press the **Enter** key.

   ```
   ================================================================================
                      Systemwalker Runbook Automation Setup
                                    V15.1.0
           All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================


   Welcome to the Systemwalker Setup.
   The setup will install Systemwalker Runbook Automation.

   Press ENTER.
   ```

6. A window for selecting the installation destination server will be displayed. Select "Management server". Enter "1".

```
================================================================================
                    Systemwalker Runbook Automation Setup
                                  V15.1.0
         All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
================================================================================


<< Select the installation folder >>


1. Management server


================================================================================
Select one of the items above.
[q,number]
=>1
```

7. The installer for the Management Server will start. To start the installation process, press "y".

```
Preparing installation.
Please wait for a while.
Systemwalker Runbook Automation ( Management Server )
Start the installation?
[y,n]
=> y
```

8. Select the installation type. To perform a Standard Installation, enter "1".

```
===<Select installation type> ===
Input Installation Type
1:Standard installation
2:Custom installation
[ENTER:1]
=> 1
```

9. Check the installation settings.

In the **Confirm continuation of installation processing** window, check the content that has been entered, and then enter "y" if there are no mistakes. Installation will start.

If the installation information is changed, enter the port number for the items that are changed.

```
=== Select Installation Type ===
1.Installation Type: Standard installation

=== Installation Directory  ===
Program deployment destination: /opt
Setup files deployment destination: /etc/opt
Work files deployment destination: /var/opt
=== Storage folder for CMDB Manager database  ===
CMDB Manager database directory: /var/opt
=== Systemwalker Runbook Automation port  ===
Port number of Interstage Management Console: 12000
Port number of Web server (Interstage HTTP Server): 80
Port number of CORBA Service: 8002
Port number of HTTP Listener: 28080
Port number of HTTP Listener for Operation Management: 12001
Port number of IIOP: 23600
Port number of IIOP_SSL: 23601
Port number of IIOP_MUTUALAUTH: 23602
Port number of JMX_ADMIN: 8686
=== Systemwalker Runbook Automation Advanced Setup for Scheduling  ===
Subsystem Number: 9
Port number of Job Scheduler: 9690
```

```
Port number of Job Execution Control: 9691

Is it OK to install by this settings? To change an item input the item number.
[y,q,number]
=> y
```

![Note icon] **Note**

. . . .

Port numbers are not displayed in an environment where Systemwalker Service Catalog Manager has been installed.

. . . .

10. The installation will start.

    Once the preparations for the installation are complete, the following window will be displayed, and the installation will start.

    ```
    Installing...
    ```

11. The installation process will be terminated.

    After the installation is completed, the window below will be displayed. Enter "y" to restart the system.

    ```
    Systemwalker Runbook Automation ( Management Server ) install completed.
    The system must be restarted to complete the installation. Restart the system now?
    [y,n]}
    ```

2.2.3.2 Custom Installation

This section explains the Custom Installation procedure.

1. Log in as a superuser on the system.

2. Insert the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 1/2 Disc" DVD-ROM in the drive.

3. Mount DVD-Rom by following command

   If you start by automatic mount daemon(autofs), installer will be failed because of having "noexec" option.

   ```
   # mount -t iso9660 -r /dev/mnt DVD-ROM mount point
   ```

4. Start the installer:

   ```
   # <DVD-ROM mount point>/swsetup
   ```

   This command installs multiple packages as a batch.

5. After the welcome text, press **Enter** key.

   ```
   ================================================================================
                       Systemwalker Runbook Automation Setup
                                       V15.1.0
            All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================

   Welcome to the Systemwalker Setup.
   The setup will install Systemwalker Runbook Automation.

   Press ENTER.
   ```

6. At the prompt for the installation directory, enter "1".

   ```
   ================================================================================
                       Systemwalker Runbook Automation Setup
                                       V15.1.0
            All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================
   ```

```
<<Select the Installation Folder>>

1. Management server


==============================================================================
Select one of the items above.
[q,number]
=>1
```

7. At the prompt for installation confirmation, enter "y".

```
Preparing to install

Please wait.
Systemwalker Runbook Automation (Management server)
Start installation
[y,n]
=> y
```

8. Select the installation type. To perform a Custom Installation, enter "2".

```
=== <Select Installation Type> ===
1. Standard Installation
The installation will use the default value.
2. Custom Installation
The installation will use the parameter that was set.

Select one of the items above.
[q,number]
=> 2
```

9. Specify the installation directory for the CMDB database.

```
===<CMDB Manager database directory>===
Enter the CMDB Manager database directory.
[ENTER:/var/opt]
=>
```

10. Set the following port numbers used by Systemwalker Runbook Automation:

  - Port number for the Interstage Management Console

  - Port number for the Web server (Interstage HTTP Server)

  - Port number for the CORBA Service

  - Port number for the HTTP listener

  - Port number for IIOP

  - Port number for IIOP_SSL

  - Port number for IIOP_MUTUALAUTH

  - Port number for JMX_ADMIN

Enter the port numbers, or press **Enter** key at each prompt to use the existing value.

```
=== Systemwalker Runbook Automation port  ===
Input Port number of Interstage Management Console
[ENTER:12000]
=>


=== Systemwalker Runbook Automation port  ===
Input Port number of Web server (Interstage HTTP Server)
[ENTER:80]
=>
```

```
=== Systemwalker Runbook Automation port  ===
Input Port number of CORBA service
[ENTER:8002]
=>


=== Systemwalker Runbook Automation port  ===
Input Port number of HTTP Listener
[ENTER:28080]
=>


=== Systemwalker Runbook Automation port  ===
Input Port number of HTTP Listener for Operation Management
[ENTER:12001]
=>


=== Systemwalker Runbook Automation port  ===
Input Port number of IIOP
[ENTER:23600]
=>


=== Systemwalker Runbook Automation port  ===
Input Port number of IIOP_SSL
[ENTER:23601]
=>


=== Systemwalker Runbook Automation port  ===
Input Port number of IIOP_MUTUALAUTH
[ENTER:23602]
=>


=== Systemwalker Runbook Automation port  ===
Input Port number of JMX_ADMIN
[ENTER:8686]
=>
```

Note

- Do not specify port numbers currently used. To check which port numbers are currently used:

```
# netstat -a -n
```

- Even port numbers not displayed by the command above might be in use by another application. Refer to "9.1 Port Numbers" for information on how to check that the port number is not being used.

- There is no confirmation for port number on the environment which installed Systemwalker Service Catalog Manager. Use same port number which you specified when you installed Systemwalker Service Catalog Manager

11. Set the subsystem number and port number that will be used by Scheduling.

    - If the default port number used by the schedule function is already used by another application, specify a different port number.

If you do not have Systemwalker Operation Manager coexist on the Management Server, or if the default port number is not used by another application, leave the default settings unchanged, and press the **Enter** key.

```
=== <Systemwalker Runbook Automation Schedule Advanced Setup> ===
Enter a subsystem number.
[ENTER:9]
=>
=== <Systemwalker Runbook Automation Schedule Advanced Setup> ===
Enter the JobScheduler port number.
[ENTER:9690]
=>
```

```
=== <Systemwalker Runbook Automation Schedule Advanced Setup> ===
Enter the Job Execution Control port number.
[ENTER:9691]
=>
```

Note

. . . .

- The port number that is currently being used can be checked using the following command. Do not specify the port number that is displayed by this command.

```
# netstat -a -n
```

- Although the specified port number is not currently in use, it may already have been assigned to other software. Refer to "9.1 Port Numbers" to check that the port number has not already been used.

. . . .

12. Check the installation settings.

    Ensure that the settings are correct, and then enter "y". If a setting must be corrected, then enter its number.

```
'=== Select Installation Type ===
1.Installation Type: Custom installation
=== Installation Directory  ===
Program deployment destination(This cannot be changed): /opt
Setup files deployment destination(This cannot be changed): /etc/opt
Work files deployment destination(This cannot be changed): /var/opt
=== Storage folder for CMDB Manager database  ===
2.Installation folder of the CMDB manager's data base: /var/opt
=== Systemwalker Runbook Automation port  ===
3.Port number of Interstage Management Console: 12000
4.Port number of Web server (Interstage HTTP Server): 80
5.Port number of CORBA service: 8002
6.Port number of HTTP Listener: 28080
7.Port number of HTTP Listener for Operation Management: 12001
8.Port number of IIOP: 23600
9.Port number of IIOP_SSL: 23601
10.Port number of IIOP_MUTUALAUTH: 23602
11.Port number of JMX_ADMIN: 8686
=== Systemwalker Runbook Automation Advanced Setup for Scheduling  ===
12.Subsystem Number: 9
13.Port number of Job Scheduler: 9690
14.Port number of Job Execution Control: 9691

Is it OK to install by this settings? To change an item input the item number.
[y,q,number]
=> y

Installation will start
```

Note

. . . .

If the environment which Systemwalker Service Catalog Manager has been installed, the port number is not displayed.

. . . .

13. The message below will be displayed.

```
Installation in progress
```

14. Installation will complete.

    At the prompt for system restart enter "y".

```
The installation of Systemwalker Runbook Automation (Management Server) is now complete.
Restart now?
[y,n]
=>
```

2.2.4 Post-installation Notes

This section describes points that require attention after the installation is complete.

[Windows]

- If a Terminal Server has been installed, then change it to Execute Mode:

CHANGE USER /EXECUTE

- Apply the following software update to the product in which Systemwalker Runbook Automation is bundled.
  Refer to "Applying Updates to Systemwalker Runbook Automation" for details about how to apply the update.

Product name	Version level	Update number
Systemwalker Operation Manager Enterprise Edition	V13.4.0B	T004598WP-04

- The user below will be added:

User name	swrbadbuser

"swrbadbuser" is used as the account for accessing the Process Management Database.

Do not delete this account with Systemwalker Runbook Automation installed.

User name	swrbajobuser

swrbajobuser is used as the operating system account for starting Systemwalker Runbook Automation Job Execution Control services.
Do not delete this account with Systemwalker Runbook Automation installed.

[Linux]

- Apply the following software update to the product in which Systemwalker Runbook Automation is bundled.
  Refer to "Applying Updates to Systemwalker Runbook Automation" for details about how to apply the update.

- Red Hat Enterprise Linux 5

Product name	Version level	Update number
Systemwalker Operation Manager Enterprise Edition	V13.4.1A	- T005956LP-01 - T004600LP-05

- Red Hat Enterprise Linux 6

Product name	Version level	Update number
Systemwalker Operation Manager Enterprise Edition	V13.4.1A	- T005958LP-01 - T006139LP-02

- Character encoding

Do not change the system character encoding for the system after installation.

- The user below will be added:

User name	swrbadbuser

"swrbadbuser" is used as the account for accessing the Process Management Database.

Do not delete this account with Systemwalker Runbook Automation installed.

2.3 Installing on Development Computers

This section describes how to install Systemwalker Runbook Automation on Development Computers.

Note

. . . .

- When installing Systemwalker Runbook Automation Studio on a Development Computer:

    - Ensure that the operating system is an English environment.

    - Ensure that you are logged in as a user that belongs to the Administrators group on the computer where the installation is to be performed.

. . . .

2.3.1 Installing Systemwalker Runbook Automation Studio

This section describes how to install Systemwalker Runbook Automation Studio on development computers.

1. Log in using an account that belongs to the Administrators group.

2. Start the installer.

   The installer will start automatically when the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 2/2 Disc" DVD-ROM is inserted in the drive.

   If the installer does not start automatically, then start it manually by executing "swsetup.exe".

The security warning window may be displayed depending on OS, it is OK. After confireming, you can keep to installe it.

3. Select **Install on Development Computer.**

4. Click the **Next** button.

5. Specify the installation directory.
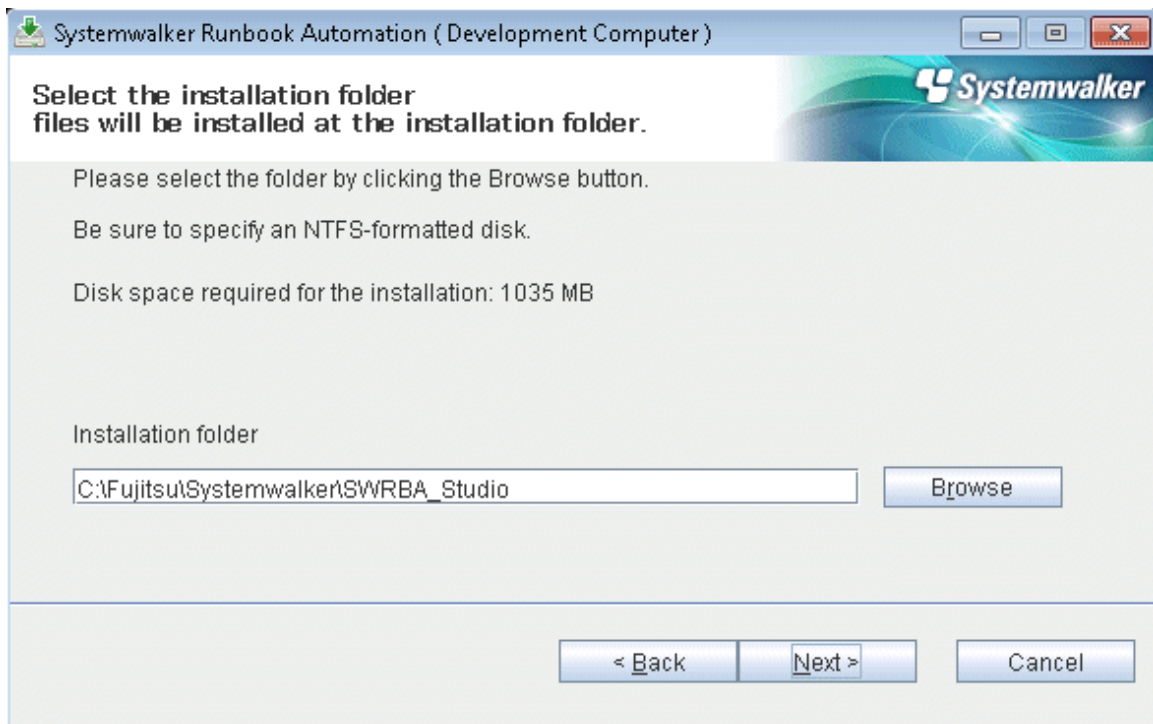
Specify the directory, and then click the **Next** button.

- The installation directory can contain up to 58 characters.

- Specify an NTFS format disk for the installation directory.

- Be sure to specify a new directory.

- Relative paths and paths starting with "\\" cannot be specified.

- The directory name can contain only alphanumeric characters, hyphens (-), underscores (_), and spaces.

- A standard directory under "C:\Program Files" or "C:\Program Files (x86)" can also be specified.

6. Check the installation settings.

   Ensure that the settings are correct, and then click the **Confirm** button.
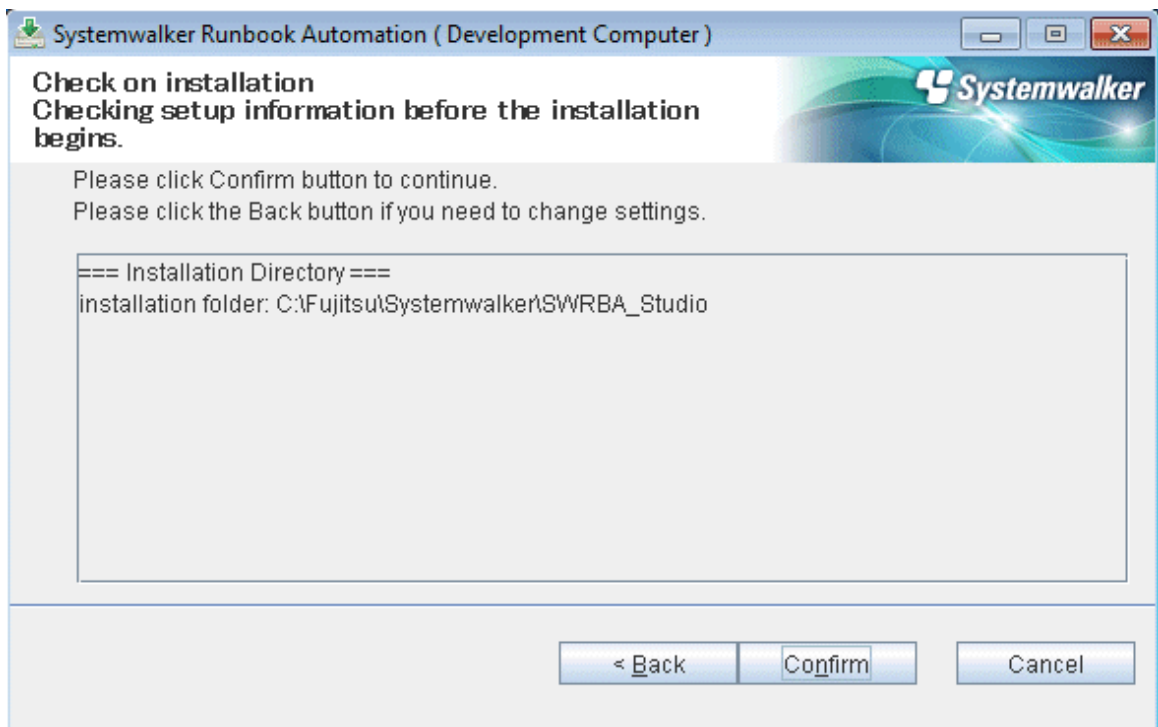
   Installation will start.

7. Installation will complete.

   In the completion window, click the **Finish** button.

2.4 Installing on Linked Servers and Relay Servers

This section describes how to install Systemwalker Runbook Automation on Linked Servers and Relay Servers.

P Point
. . . .

- The Agents installed on Linked Servers and Relay Servers periodically collect information and send it to the CMDB Manager on the Management Server.

- If the Systemwalker Centric Manager Operation Management Server is in a cluster configuration, install an Agent on both the active system and the standby system.

- If the Systemwalker Centric Manager Operation Management Server is in a redundant configuration, install an Agent on either of the two Operation Management Servers.

- If Systemwalker Centric Manager systems have been layered using a Master Monitoring Server, install an Agent on the Operation Management Servers under the Master Monitoring Server.

. . . .

G Note
. . . .

Ensure that the version of the product for which information is to be collected is as follows:

- Systemwalker Centric Manager V13.0.0 or later

. . . .

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the installer as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

Preparations before starting the installation

Before executing the installer, refer to the *Systemwalker Runbook Automation Technical Guide* to understand the installation conditions and collect the necessary information.

2.4.1 Pre-installation Notes

This section describes points to note before installing the Agent.

Inatllation for required functions

- Install the following function which Systemwalker Runbook Automation Linked Servers and Relay Servers can run.

  - CMDB Agent

  - SMEE, Securecrypto runtime library

  - Systemwalker communicate basic function

  - File transfer function

  Meanwhile, when uninstalled Systemwalker Runbook Automation Linked Servers and Relay Servers a part of function, it is shared with other product, so it is not uninstalled.

  For the detail of uninstall, refer "7.2.3 Uninstalling the Linked Server/Relay Server".

2.4.2 Installing on Windows Systems

This section describes how to install Systemwalker Runbook Automation on Windows systems.

2.4.2.1 Installing Systemwalker Runbook Automation

This section describes how to install the Agent for Systemwalker Runbook Automation on Linked Servers and Relay Servers.

1. Start the installer.

   The installer will start automatically when the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 2/2" DVD-ROM is inserted in the drive.

If the installer does not start automatically, then start it manually by executing "swsetup.exe".

2. Select **Install on Linkage Server/Relay Server**.

   Refer to "2.4.1 Pre-installation Notes" and the CPU architecture of the server where the product will be installed before deciding whether to select the 32-bit version or the 64-bit version.

Click the **Next** button.
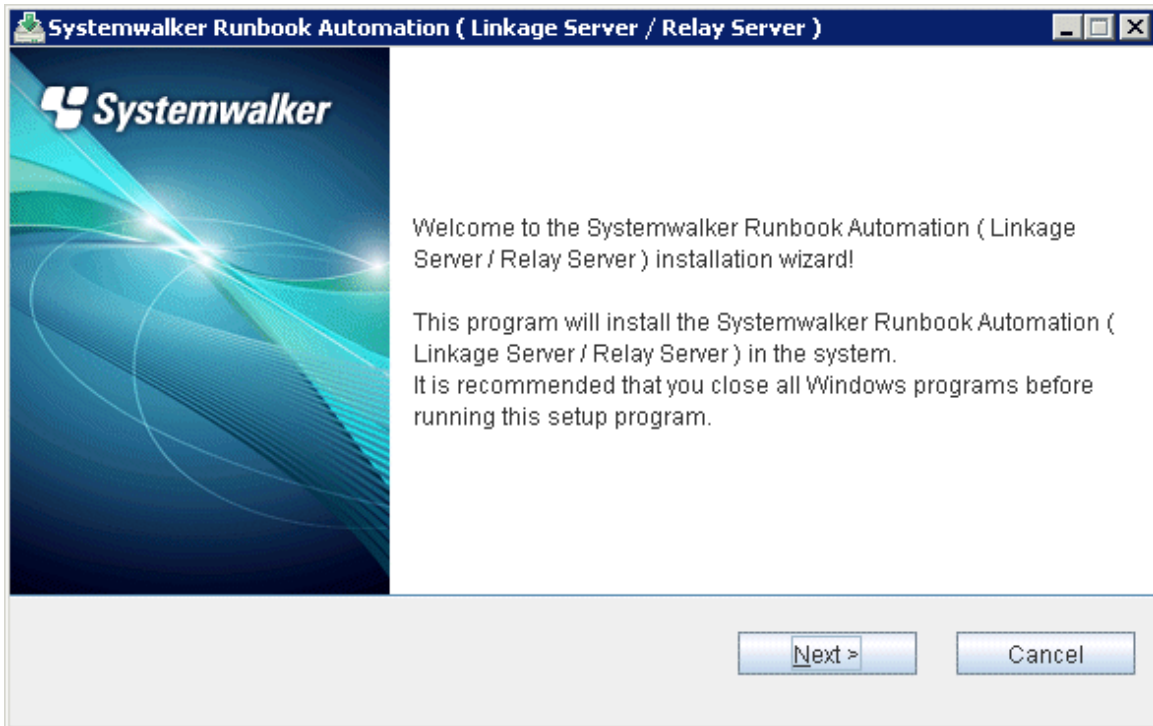
3. Specify the installation directory.
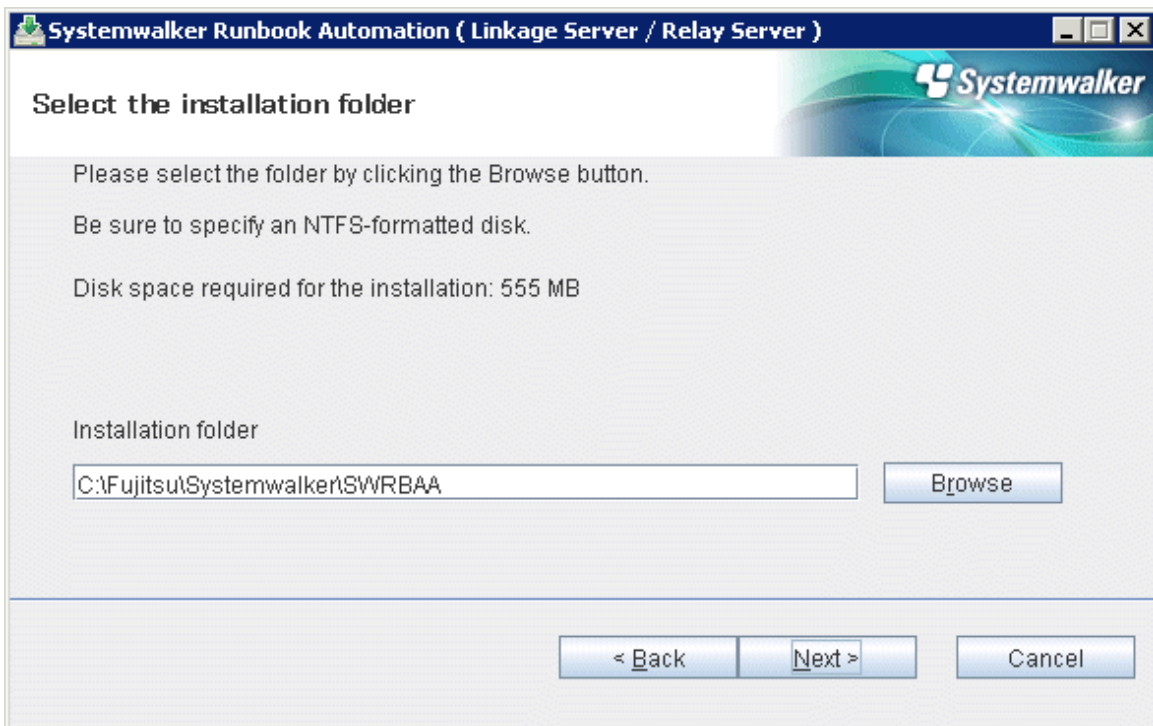
   Specify the directory, and then click the **Next** button.

![Note icon] **Note**

. . . .

 - The installation directory can contain up to 58 characters.

 - Specify an NTFS format disk for the installation directory.

- Be sure to specify a new directory.

- Relative paths and paths starting with "\\" cannot be specified.

- The directory name can contain only alphanumeric characters, hyphens (-), underscores (_), and spaces.

- A standard directory under "C:\Program Files" or "C:\Program Files (x86)" can also be specified.

4. Specify the host name and port number for the Management Server.

   You can use the default port number, and then click the **Next** button.

5. Check the installation settings.

   Ensure that the settings are correct, and then click the **Next** button.

6. Installation will start.

7. Installation will complete.

   In the completion window, click the **Finish** button.
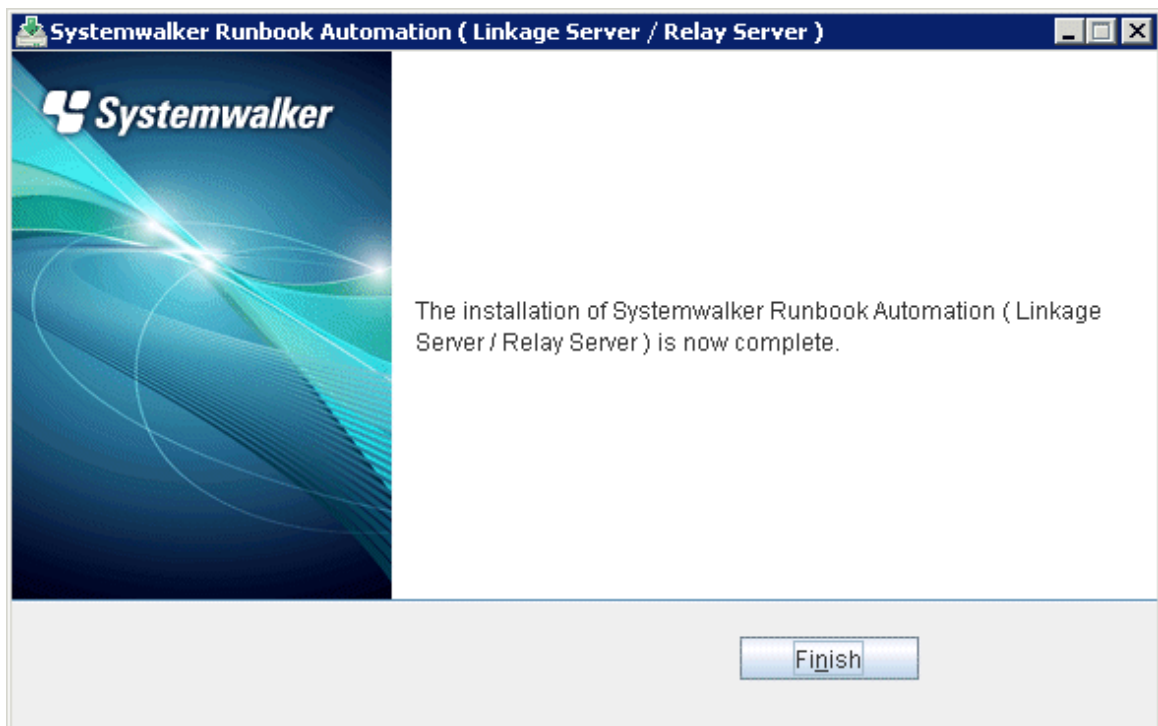
2.4.3 **Installing on Linux Systems**

This section describes how to install Systemwalker Runbook Automation on Linux systems.

2.4.3.1 Installing Systemwalker Runbook Automation

This section describes how to install the Agent for Systemwalker Runbook Automation on Linked Servers and Relay Servers.

1. Log in as a superuser on the system.

2. Insert the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 2/2" DVD-ROM in the drive.

   If the volume management daemon is not running, then mount the DVD-ROM:

   ```
   # mount -t iso9660 -r /dev/mnt <DVD-ROM mount point>
   ```

3. Mount DVD-Rom by following command

   If you start by automatic mount daemon(autofs), installer will be failed because of having "noexec" option.

   ```
   # mount -t iso9660 -r /dev/mnt DVD-ROM mount point
   ```

4. Start the installer.

   ```
   # <DVD-ROM mount point>/swsetup
   ```

   This command installs multiple packages as a batch.

5. After the welcome text, press **Enter** key.

   ```
   ================================================================================
                      Systemwalker Runbook Automation Setup
                                    V15.1.0
           All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================


   Welcome to the Systemwalker Setup.
   The setup will install Systemwalker Runbook Automation.

   Press ENTER.
   ```

6. At the prompt for the server installation directory, enter " Linked Server/Relay Server ".

   Refer to "2.4.1 Pre-installation Notes" and the architecture of the server where the product will be installed before deciding whether to select the 32-bit version or the 64-bit version.

   ```
   ================================================================================
                      Systemwalker Runbook Automation Setup
                                    V15.1.0
           All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================


   <<Select the Installation Folder>>

   1. Linked Server/Relay Server (32-bit)
   2. Linked Server/Relay Server (64-bit)
   3. Business Server (32-bit)
   4. Business Server (64-bit)


   ================================================================================
   Select one of the items above.
   [q,number]
   =>1
   ```

7. At the prompt for Linked Servers/Relay Servers installation confirmation, enter "y".

```
Preparing to install
Please wait.
Systemwalker Runbook Automation (Linked Server/Relay Server)
Start installation?
[y,n]
=>
```

8. Specify the host name or ip address for the Management Server.

```
===<Management Server information>===
Enter the host name or ip address for the Management Server.

=>swrba
```

9. Specify the port number for the Management Server.

   You can use the default value.

```
===<Management Server information>===
Enter the port number for the Management Server (Web Server).
[ENTER:80]
=>
```

10. Check the installation settings.

    Ensure that the settings are correct, and then enter "y". If a setting must be corrected, then enter its number.

```
===<Installation Directory>===
Program deployment target (This cannot be changed): /opt
Setup files deployment target (This cannot be changed): /etc/opt
Work files deployment target (This cannot be changed): /var/opt
===<Management Server information>===
1. Management Server Host Name or IP address: swba
2. Management Server (Web Server) Port number: 80

Install with these settings? To change a setting, enter the number of the setting item.
[y,q,number]
=> y
```

11. Installation will start.

    The message below will be displayed.

```
Installation in progress
```

12. Installation will complete.

    The message below will be displayed.

```
The installation of Systemwalker Runbook Automation (Linked Server/Relay Server) is now complete.
```

2.5 Installing on Business Servers

This section describes how to install Systemwalker Runbook Automation on Business Servers.

There is no need to install Systemwalker Runbook Automation to execute operation components using SSH

Note that there is no need to perform this installation when using the Management Server as a Business Server as well, because the Business Server function has already been installed on the Management Server.

Privileges required for execution

[Windows]

Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the installer as an administrator.

[Linux] [Solaris]

System administrator (superuser) privileges are required.

Preparations before starting the installation

Before executing the installer, refer to the *Systemwalker Runbook Automation Technical Guide* to understand the installation conditions and collect the necessary information.

2.5.1 Pre-installation Notes

This section describes points to note before installing the Agent.

- Install the following function which Systemwalker Runbook Automation Business Servers can run.

    - File transfer function

For the detail of uninstall, refer "7.2.4 Uninstalling the Business Server".

If the Systemwalker Software Configuration Manager Agent is installed:

Since the Systemwalker Runbook Automation Agent is included within the Systemwalker Software Configuration Manager Agent, there is no need to install an agent again.

2.5.2 Installing on Windows Systems

This section describes how to install Systemwalker Runbook Automation on Windows systems.

2.5.2.1 Installing Systemwalker Runbook Automation

This section describes how to install Systemwalker Runbook Automation on Business Servers.

1. Start the installer.

   The installer will start automatically when the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 2/2" DVD-ROM is inserted in the drive.

If the installer does not start automatically, then start it manually by executing "swsetup.exe".
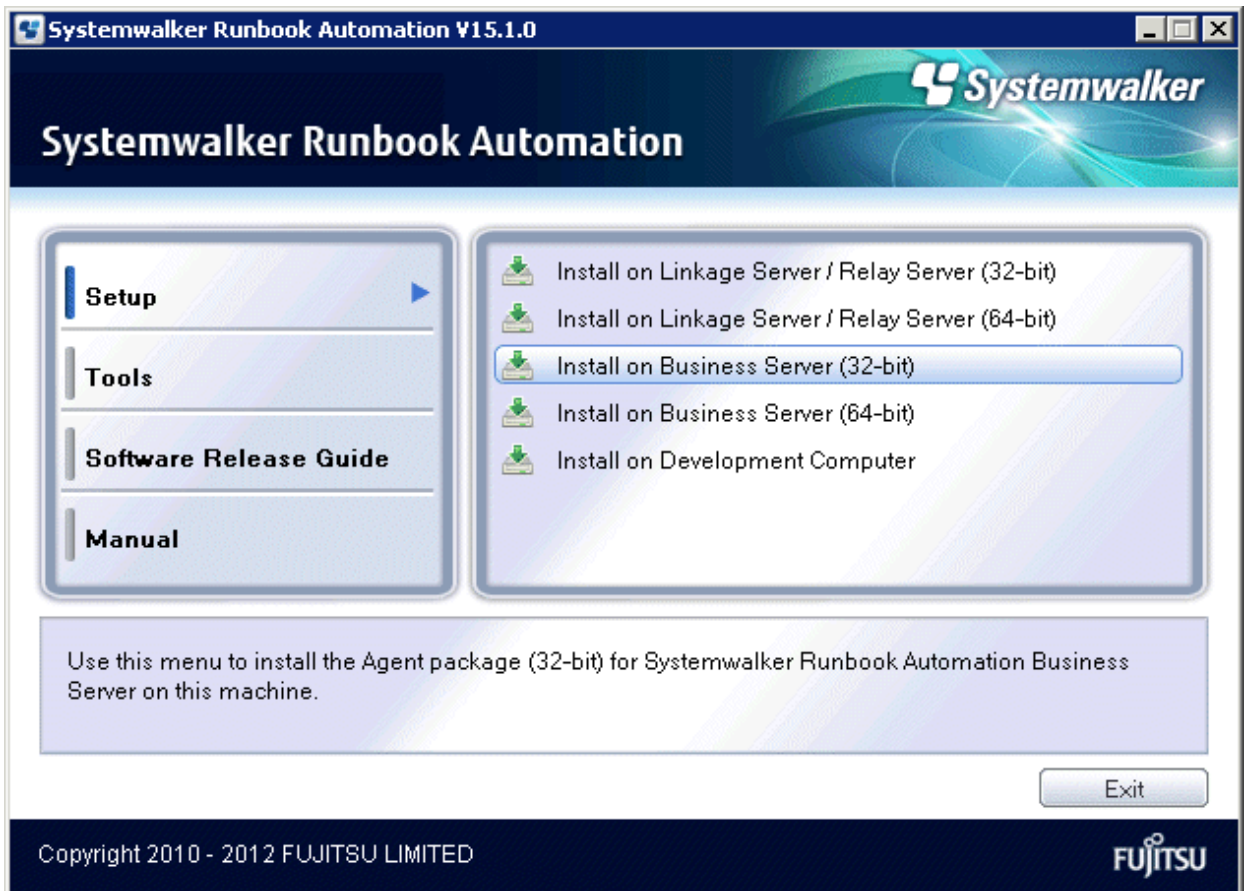
2. Select **Install on Business Server**.

3. Select the 32-bit or the 64-bit version, depending on the CPU architecture of installation destination server.

   Click the **Next** button.
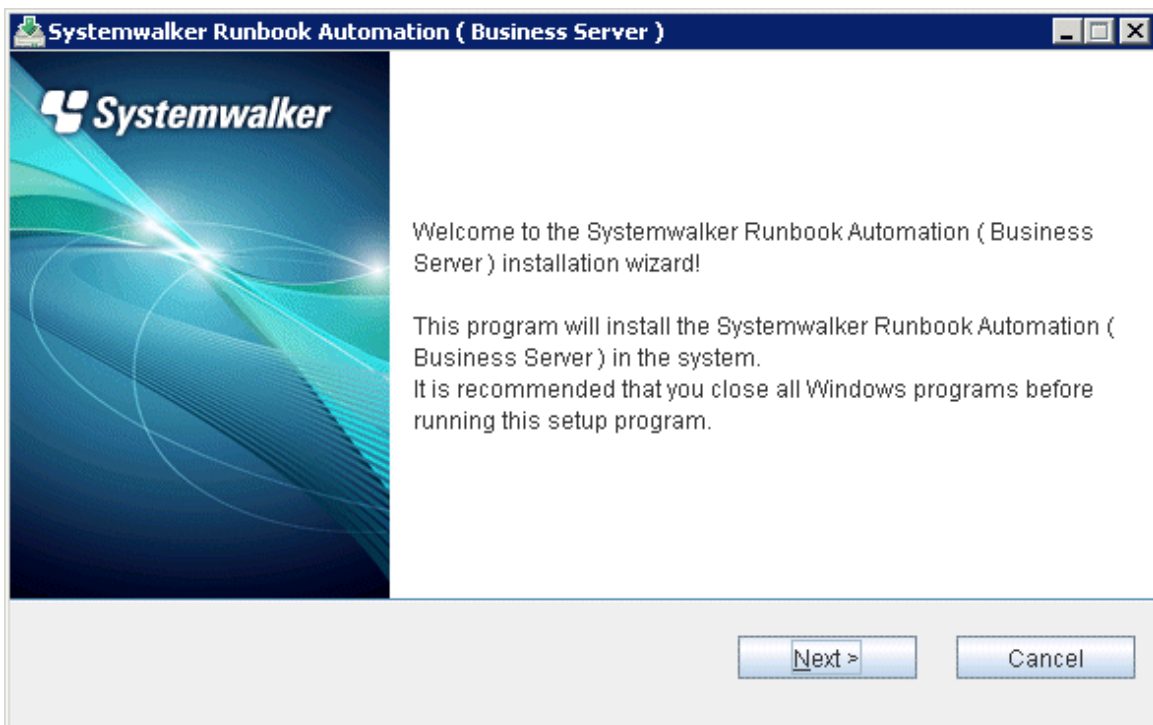
4. Specify the installation directory.
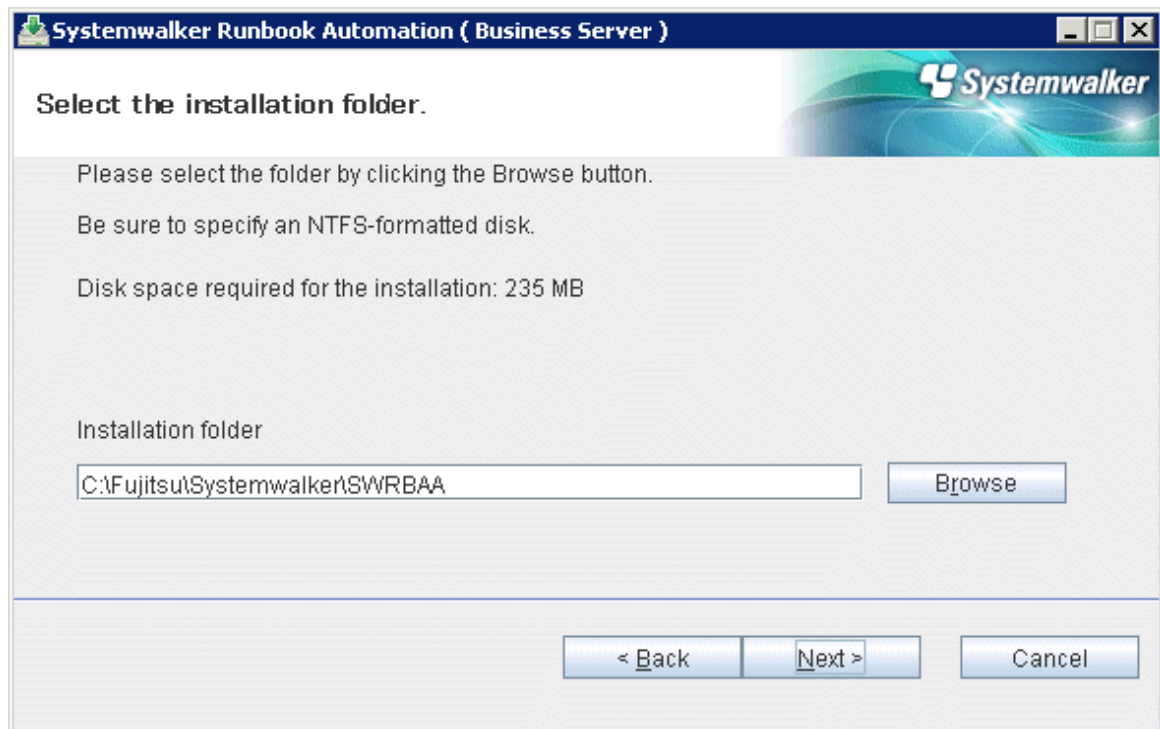
   Specify the directory, and then click the **Next** button.

📑 Note

- The installation directory can contain up to 58 characters.

- Specify an NTFS format disk for the installation directory.

- Be sure to specify a new directory.

- Relative paths and paths starting with "\\" cannot be specified.

- The directory name can contain only alphanumeric characters, hyphens (-), underscores (_), and spaces.

- A standard directory under "C:\Program Files" or "C:\Program Files (x86)" can also be specified.

5. Check the installation settings.

   Ensure that the settings are correct, and then click the **Next** button.
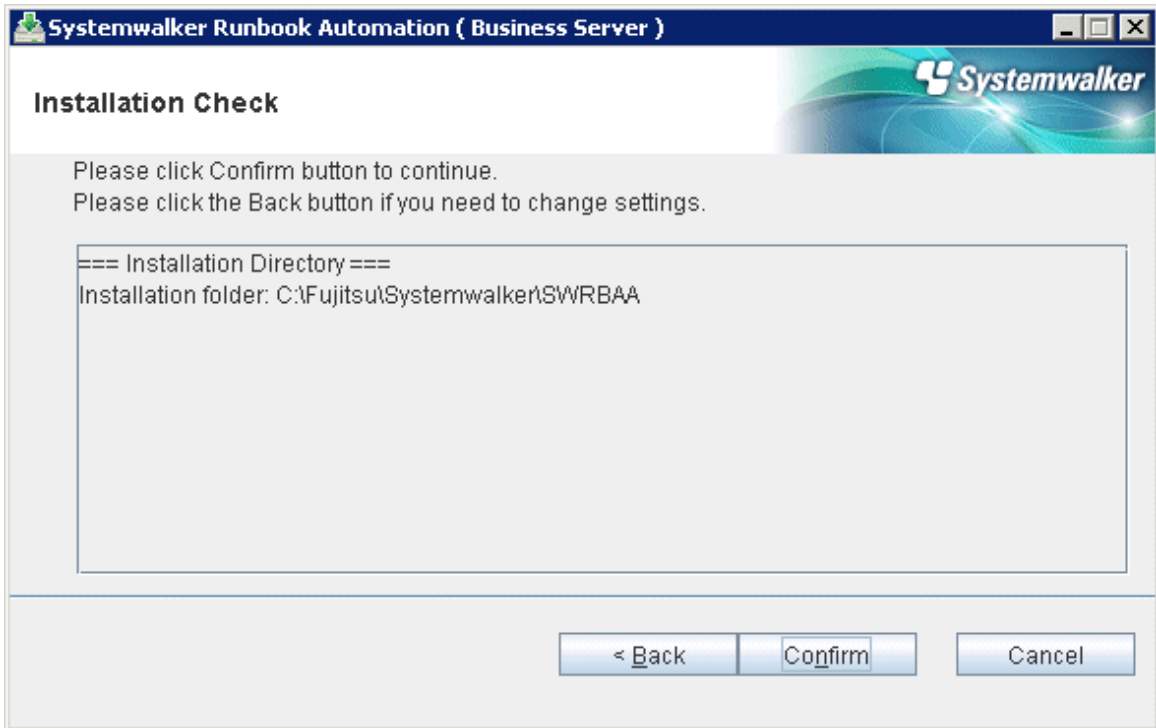
   Installation will start.

6. Installation will complete.

   In the completion window, click the **Finish** button.
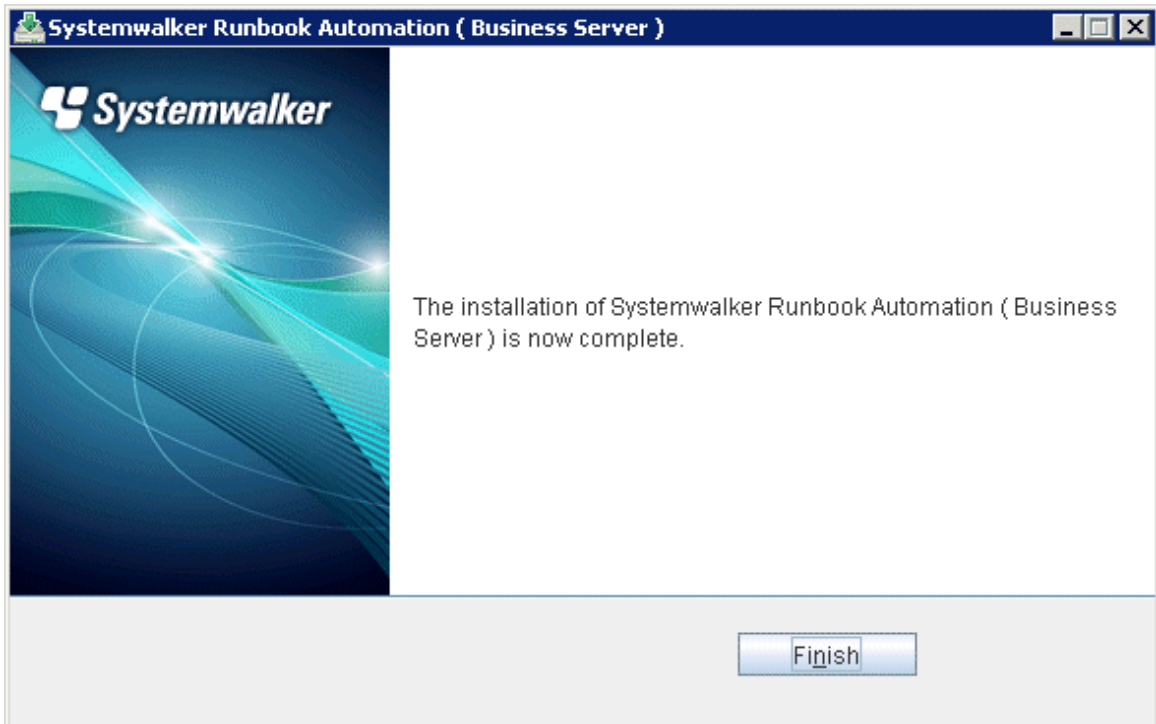
2.5.3 Installing on Linux/Solaris Systems

This section describes how to install Systemwalker Runbook Automation on Linux/Solaris systems.

2.5.3.1 Installing Systemwalker Runbook Automation

This section describes how to install Systemwalker Runbook Automation on Business Servers.

1. Log in as a superuser on the system.

2. Insert the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 2/2" DVD-ROM in the drive.

3. Mount DVD-Rom by following command

   If you start by automatic mount daemon(autofs), installer will be failed because of having "noexec" option.

   [Linux]

   ```
   # mount -t iso9660 -r /dev/mnt DVD-ROM mount point
   ```

   [Solaris]

   ```
   # mount -F udfs  -r DVD-ROM device DVD-ROM mount point
   ```

4. Start the installer:

   This command installs multiple packages as a batch.

   [Linux]

   ```
   # <DVD-ROM mount point>/swsetup
   ```

   [Solaris]

   ```
   # /bin/sh DVD-ROM mount point/swsetup
   ```

5. After the welcome text, press **Enter** key.

   ```
   ================================================================================
                     Systemwalker Runbook Automation Setup
                                   V15.1.0
            All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================

   Welcome to the Systemwalker Setup.
   The setup will install Systemwalker Runbook Automation.

   Press ENTER.
   ```

6. At the prompt for the server installation directory server, enter "Business Server".

   [Linux]

   Select the 32-bit or the 64-bit version, depending on the CPU architecture of installation destination server.

   ```
   ================================================================================
                     Systemwalker Runbook Automation Setup
                                   V15.1.0
            All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================

   <<Select the Installation Folder>>

   1. Linked Server/Relay Server (32-bit)
   2. Linked Server/Relay Server (64-bit)
   3. Business Server (32-bit)
   4. Business Server (64-bit)
   ```

```
================================================================================
Select one of the items above.
[q,number]
=>4
```

[Solaris]

```
================================================================================
                  Systemwalker Runbook Automation Setup
                               V15.1.0
        All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
================================================================================


<<Selection of installation destination>>

1. Business Server


================================================================================
Select 1 from the above.
[q,number]
=>1
```

7. At the prompt for Business Server installation confirmation, press "y".

```
Preparing to install
Please wait.
Systemwalker Runbook Automation (Business Server)
Start installation?
[y,n]
=> y
```

8. For Solaris, select install destination.

```
=== <<Installation directory>> ===
Input the deployment destination of the program.
[ENTER:/opt]
=>

=== <<Installation directory>> ===
Input deployment destination of the setup file.
[ENTER:/etc/opt]
=>

=== <<Installation directory>> ===
Input work files deployment destination.
[ENTER:/var/opt]
=>
```

9. Check the installation settings.

Ensure that the settings are correct, and then enter "y". If a setting must be corrected, then enter its number.

[Linux]

```
===<Installation Directory>===
Program deployment target (This cannot be changed): /opt
Setup files deployment target (This cannot be changed): /etc/opt
Work files deployment target (This cannot be changed): /var/opt


Install with these settings?
[y,q]
=> y
```

[Solaris]

```
=== <Installation directory> ===
1. Deployment destination of the program: /opt
2. deployment destination of the setup file: /etc/opt
3. Deployment destination of the work files: /var/opt

Install with these settings? To specify a different value, enter the item number.
[y,q,number]
=> y
```

10. Installation will start.

The message below will be displayed.

```
Installation in progress
```

11. Installation will complete.

The message below will be displayed.

```
The installation of Systemwalker Runbook Automation (Business Server) is now complete.
```

2.6 Installing a Web Console

This section describes how to install a Web console.

2.6.1 Setting up the Web Browser

To use Systemwalker Runbook Automation, it is necessary to set up the Web browser to operate it.

Refer to "Web Browser Settings" in the *Syetemwalker Runbook Automation Operation Guide* for how to set.

Chapter 3 Setup

This chapter describes how to set up Systemwalker Runbook Automation.

3.1 Setting up the Management Server

After Systemwalker Runbook Automation is installed, the Management Server must be set up.

This section describes how to set up the Management Server.

Refer to the *Systemwalker Runbook Automation Cluster Setup Guide* for information on creating a Systemwalker Runbook Automation cluster environment.
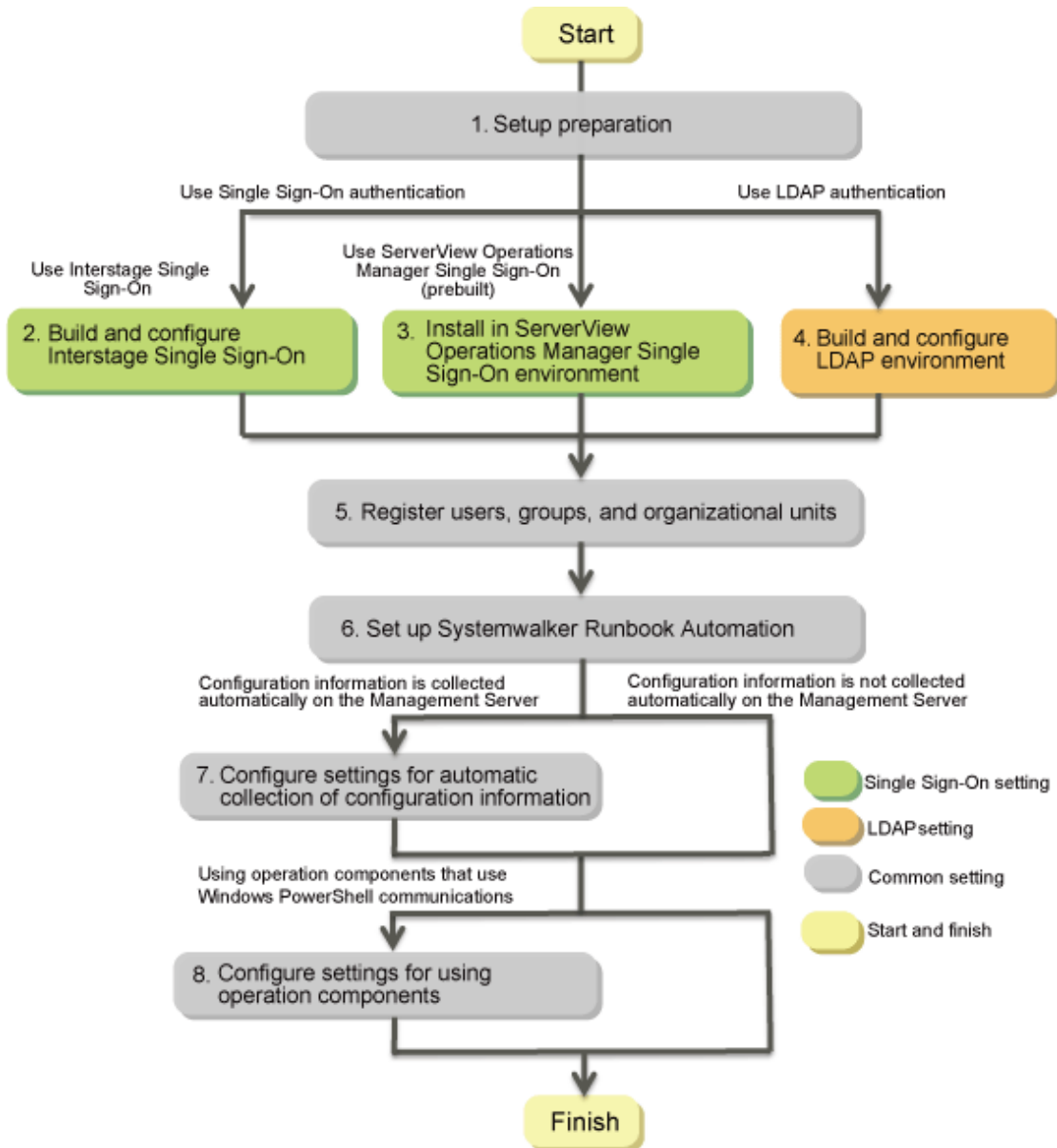
1. Setup Preparation

   Refer to "3.1.2 Setup Preparation".

2. Interstage Single Sign-On Build and Settings

   Refer to "3.1.3 Interstage Single Sign-On Build and Settings".

3. Install in a ServerView Operations Manager Single Sign-On Environment

   Refer to "3.1.4 Installing in a ServerView Operations Manager Single Sign-On Environment".

4. LDAP Environment Build and Settings

   Refer to "3.1.5 LDAP Environment Build and Settings".

5. Register Users, Groups and Organizational Units

   Refer to "3.1.6 Registering Users, Groups and Organizational Units".

6. Set up Systemwalker Runbook Automation

   [Windows]

   Refer to "3.1.7 Setting up Systemwalker Runbook Automation [Windows]".

   [Linux]

   Refer to "3.1.8 Setting up Systemwalker Runbook Automation [Linux]".

7. Settings for Automatically Collecting Configuration Information

   Refer to "3.1.9 Settings for Automatically Collecting Configuration Information".

8. Settings for Using the Operation Component

   Refer to the "3.1.10 Settings for Using the Operation Component".

Note
....
Refer to "3.1.1 Pre-setup Notes" for information on steps required before setup.
....

3.1.1 Pre-setup Notes

This section describes points that require attention when performing the setup.

The environment where the setup is performed

Check the following items for the environment where the setup is performed.

- Check whether Systemwalker Runbook Automation has been installed, and whether the system was restarted after the installation.

- Ensure that you are logged in as a user with administrator privileges.

- To cancel the setup, the login ID used for the setup will be required.

- Use either the isstat command or the Interstage Management Console to check whether Interstage is running. Refer to the *Interstage Application Server Reference Manual (Command Edition)* for details on the command. Refer to Interstage Management Console Help for details on the Interstage Management Console.

3.1.2 Setup Preparation

Design the Systemwalker Runbook Automation operation.

1. Refer to "*Systemwalker Runbook Automation Technical Guide*", estimate database for Systemwalker Runbook Automation operation, and prepare enough size of file system.

   [Linux]

   Prepared file system is not mounted on operating system, mount file system on operating system. For details on how to mount, refer to the operating system manuals.

2. Decide directory for registering process management database. Decide the directory so as to become directory on file system as prepared in 1. above.

3. Add access authority to directory.

   Without creating directory for registering process management database(when specified directory does not exist, Setup command will create it with adding appropriate access authority), from root directory to registering real database directory for process management, if one of them are already created, add the following access authority to directory.

   [Linux]

   Add authority so that the "swrbadbuser" operating system user can read from and write to the file system (or directory).

   [Windows]

   Add changeable authority to User group which belong to operating system user "swrbadbuser".

   Also do not add changeable authority to only operating system user "swrbadbuser". Add changeable authority to User group. If you add changeable authority to only operating system user "swrbadbuser", setup will be aborted with error.

Point

- The "swrbadbuser" operating system user is created when this product is installed.

3.1.3 Interstage Single Sign-On Build and Settings

This chapter explains how to build and set up Interstage Single Sign-on.

The flow for the setup of Interstage Single Sign-on and the setting of information in the existing Interstage Single Sign-on is shown below:
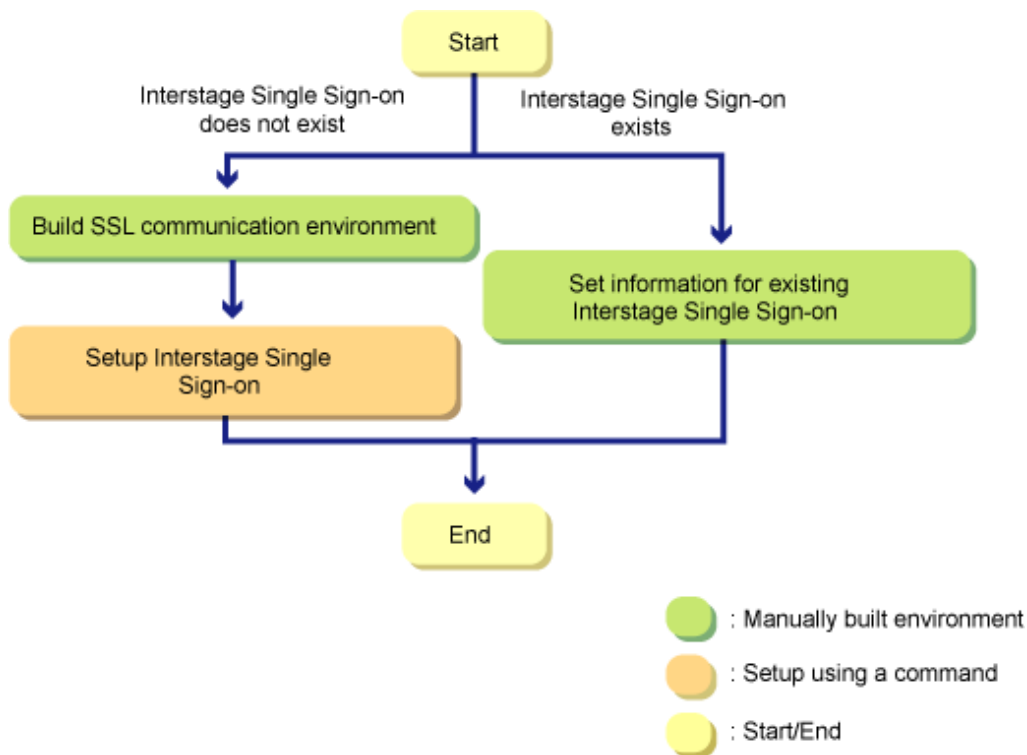
Note

- Execute the procedures explained in this chapter using administrator privileges.

- Execute the procedures explained in this chapter after the following products are installed:

  - Systemwalker Runbook Automation

  - Systemwalker Configuration Manager

- Systemwalker Service Catalog Manager

- The LDAP using Interstage Single Sign-on is only Interstage directory service. You do not use Active Directory/OpenLDAP.

- Log into the Interstage Management Console explained on this chapter in the following procedure.

  Input the following URL to the browser and display the Log in windows. Specify system administrator for operating system as user login.

```
http://[The hostname for Management server]:[Interstage Management Console port number]/IsAdmin
```

or

```
https://[ The hostname for Management server]:[Interstage Management Console port number]/IsAdmin
```

3.1.3.1 Building the SSL Communication Environment

This section explains how to build the SSL communication environment.

Note

There is no need to perform this task if the SSL communication environment build is already completed.

Procedure to build the SSL communication environment

Build the SSL communication environment as preparation before the Interstage Single Sign-on setup.
Build the SSL communication environment using the following procedure:

1. Setting the Interstage Certificate Environment Access Permissions

2. Creating the Interstage Certificate Environment and the Application to Obtain the Certificate that is used for SSL Communication

3. Registering Certificates used in SSL Communication

4. Settings for SSL Communication

Information

Refer to "Chapter 9 Setting and Use of the Interstage Certificate Environment" in the *Interstage Application Server Security System Guide* for information on how to build the SSL environment.

3.1.3.1.1 Setting the Interstage Certificate Environment Access Permissions [Linux]

Create an owner group that has permissions to access the Interstage certificate environment.
An example of creating the owner group using the command is shown below:

Note

Only the Operating system which is built Interstage Single Sign-On is Linux, Execute this work. If your environment is Windows. This work is not needed.

1. Create the Interstage certificate environment owner group.

   In the following example, the owner group is created as "iscertg".

```
# groupadd iscertg
```

Note

The owner group that was created at the time of the Interstage certificate environment build must be specified in the -g option of the Certificate Signing Request (CSR) creation command (scsmakeenv). Refer to "3.1.3.1.2 Creating the Interstage Certificate Environment and the Application to Obtain the Certificate that is used for SSL Communication" for information on the CSR creation command.

2. Register the executing user in the "iscertg" group.

   In the following example, the executing user is created as "nobody".

   ```
   # usermod -G iscertg nobody
   ```

Note

The executing user that is registered in the Interstage certificate environment owner group must have been set in the User directive of the Interstage HTTP Server environment configuration file (httpd.conf). The user "nobody" has been set if you installed Interstage Application Server bundled with Systemwalker Service Catalog Manager.

3.1.3.1.2 Creating the Interstage Certificate Environment and the Application to Obtain the Certificate that is used for SSL Communication

The CSR creation command (from now on, this is referred to as the "scsmakeenv command") is used to create the CSR that will create the Interstage certificate environment and apply for the certificate that is used for SSL communication.
The creation procedure and execution example are shown below:

Creation procedure

1. Set the JDK or JRE installation path in the JAVA_HOME environment variable. This procedure is only required for Linux. Setting of the environment variable JAVA_HOME is unnecessary for Windows.

2. Execute the scsmakeenv command.

   [Windows]

   ```
   scsmakeenv -n <private key nickname> -f <output destination file name for the CSR>
   ```

   [Linux]

   ```
   scsmakeenv -n <private key nickname> -f <output destination file name for the CSR> -g <Group that
   has permissions to access the Interstage certificate environment>
   ```

   Change the CSR output destination file name if necessary.

Note

The private key nickname specified in the scsmakeenv command will be required when the site certificate obtained from the CA is registered.

Information

Refer to "Chapter 16 SSL Environment Setting Commands" in the *Interstage Application Server Reference Manual (Command Edition)* for information on the scsmakeenv command.

3. Enter a password to access the Interstage certificate environment.

   The password will be required to access the Interstage certificate environment.

4. Enter an identifier.

   When the "What is your first and last name?" (**a**lphanumeric name) enquiry is made, specify the FQDN of the server used to apply for the certificate as the Web server host name.

5. As with step 4, enter the following items:

   - Name of organizational unit

   - Name of organization

   - Name of City or Locality

   - Name of State or Province

   - Two-letter country code

6. Check the values that were entered.

   To create the CSR using the values that were entered, enter **yes**. To change the values that were entered, enter **no**.

7. Send the CSR to the CA to request that a certificate be issued.

   If the scsmakeenv command has terminated normally, the CSR will be output to the certificate output destination file name that was specified in the -f option of the scsmakeenv command. Send that file to the CA and request that a certificate be issued. Follow the request method used by the CA.

Execution example [Windows]

The command execution examples shown below use the following values:

```
- Site certificate nickname: SERVERCERT
- Applicant output destination file name: C:\temp\ssocert.txt
- First and last name: ssoserver.example.com
- Name of organizational unit: FUJITSU TOKYO
- Name of organization: FUJITSU
- Name of City or Locality: Shinjuku
- Name of State or Province: Tokyo
- Two-letter country code for this unit:jp
```

In the example, the applicant output file name is "C:\temp\ssocert.txt". Change the applicant output file name if necessary.

At the password prompt, enter the password that will be used to access the Interstage certificate environment. (it will not be displayed).

```
C:\>scsmakeenv -n SERVERCERT -f C:\temp\ssocert.txt
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]: ssoserver.example.com
What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
  [Unknown]: FUJITSU
What is the name of your City or Locality?
  [Unknown]: Shinjuku
What is the name of your State or Province?
  [Unknown]: Tokyo
What is the two-letter country code for this unit?
  [Un]: jp

Is <CN=ssoserver.example.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
  [no]: yes
<SCS: INFO: scs0101: CSR was issued <C:\temp\ssocert.txt>
C:\>
```

Execution example [Linux]

The command execution examples shown below use the following values:

```
- Site certificate nickname: SERVERCERT
- Applicant output destination file name: /tmp/ssocert.txt
- Group that has permissions to access the Interstage certificate environmentiscertg
- First and last name: ssoserver.example.com
- Name of organizational unit: FUJITSU TOKYO
- Name of organization: FUJITSU
- Name of City or Locality: Shinjuku
- Name of State or Province: Tokyo
- Two-letter country code for this unit:jp
```

In the execution example, a new Interstage certificate environment is created for which "iscertg" access permissions are set, and the CSR is also created. If an Interstage certificate environment has already been created, then set access permissions to it if necessary.

The Bourne shell has been used in the execution example.

```
# JAVA_HOME=/opt/FJSVawjbk/jdk5;export JAVA_HOME
# scsmakeenv -n SERVERCERT -f /tmp/ssocert.txt -g iscertg
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]: ssoserver.example.com
What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
  [Unknown]: FUJITSU
What is the name of your City or Locality?
  [Unknown]: Shinjuku
What is the name of your State or Province?
  [Unknown]: Tokyo
What is the two-letter country code for this unit?
  [Un]: jp

Is <CN=ssoserver.example.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
  [no]: yes
UX:SCS: INFO: scs0101: CSR was issued </tmp/ssocert.txt>
UX:SCS: INFO: scs0180: The owners group of Interstage certificate environment was set.
#
```

📒 **Note**
. . . .
You will be prompted to input password for Interstage certificate environment if Interstage certificate environment is already configured. In this case, input the password that was set when you configured Interstage certificate environment.
. . . .

📖 **Information**
. . . .
Test site certificates can be used in the test environment. Note that these test site certificates are only for test environments, and so should not be used for actual operations.
Refer to Appendix B Creating Test Site Certificates for information on creating test site certificates.
. . . .

3.1.3.1.3 Registering Certificates used in SSL Communication

Obtain the site certificate that was issued by the CA, and the CA certificate of the issuer of that certificate, and register them using the certificate/CRL registration command (from now on, this is referred to as the "scsenter command").

Creation procedure

1. Set the JDK or JRE installation path in the JAVA_HOME environment variable.

   This is necessary procedure for Linux. For Windows, it is not necessary.

2. Register the CA certificate using the scsenter command.

   ```
   scsenter -n <CA certificate nickname> -f <CA certificate>
   ```

3. Enter a password to access the Interstage certificate environment.

   Enter the password that was specified in the scsmakeenv command to access the Interstage certificate environment.

4. Register the site certificate using the scsenter command.

   ```
   scsenter -n <Site certificate nickname> -f <Site certificate> -o
   ```

   To register the site certificate that was obtained from the CA, specify the nickname that was specified in the private key in the scsmakeenv command. Note that the -o option must be specified to register the site certificate.

5. Enter a password to access the Interstage certificate environment.

   Enter the password that was specified in the scsmakeenv command to access the Interstage certificate environment.

Execution example [Windows]

The command execution examples shown below use the following values:

```
- CA certificate: C:\temp\ca-cert.cer
- CA certificate nickname: CACERT
- Site certificate: C:\temp\server-cert.cer
- Site certificate nickname: SERVERCERT
```

In the examples, the CA and site certificates obtained are "C:\temp\ca-cert.cer" and "C:\temp\server-cert.cer". Change the file path name of each certificate if necessary.

At the password prompt, enter the password that will be used to access the Interstage certificate environment (it will not be displayed).

```
C:\>scsenter -n CACERT -f C:\temp\ca-cert.cer
Password:
Certificate was added to keystore
SCS: INFO: scs0104: Certificate was imported.
C:\>scsenter -n SERVERCERT -f C:\temp\server-cert.cer -o
Password:
Certificate reply was installed in keystore
SCS: INFO: scs0104: Certificate was imported.
C:\>
```

Execution example [Linux]

The command execution examples shown below use the following values:

```
- CA certificate: /tmp/ca-cert.cer
- CA certificate nickname: CACERT
- Site certificate: /tmp/server-cert.cer
- Site certificate nickname: SERVERCERT
```

Change the file names of the CA and site certificates that were obtained if necessary.
The Bourne shell has been used in the execution example.

```
# JAVA_HOME=/opt/FJSVawjbk/jdk5;export JAVA_HOME
# scsenter -n CACERT -f /tmp/ca-cert.cer
Password:
Certificate was added to keystore
UX:SCS: INFO: scs0104: Certificate was imported.
# scsenter -n SERVERCERT -f /tmp/server-cert.cer -o
Password:
Certificate reply was installed in keystore
UX:SCS: INFO: scs0104: Certificate was imported.
#
```

3.1.3.1.4 Settings for SSL Communication

Using the Interstage Management Console, create the SSL definition.

1. Start the Interstage Management Console.

   Follow the procedure below to start the Interstage Management Console:

   1. Start the Web browser.

   2. Specify the Interstage Management Console URL.

      The URL format is shown below:
      (When SSL encrypted communication is not used)

      http://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

      (When SSL encrypted communication is used)

      https://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

   3. Log into the Interstage Management Console.

2. Create the SSL definition.

   Select the **System** >> **Security** >> **SSL** >> **Create a new SSL Configuration** tabs to show **General Settings**, then select the registered site certificate nickname, then create the SSL definition.
   Specify the following items, then push **Create** button.

Settings item	Settings value

Configuration name	Set the name that will identify the SSL definition.
	Specify the Configuration name set here at the time of the Interstage Single Sign-on setup.
	You can use 32 or less alphanumeric characters and following symbols.
	
	  - Hyphen "-"
	
	  - Rounded bracket "()"
	
	  - Square brackets "[]"
	
	  - Underline "_"

Settings item	Settings value
Site Certificate Nickname	Set the nickname that was specified when the site certificate was registered in the Interstage certificate environment, in "3.1.3.1.3 Registering Certificates used in SSL Communication". The site certificate that was selected can be checked in the **System** >> **Security** >> **Certificates** >> **Site Certificates** window of the Interstage Management Console.
Protocol Version	Select "SSL 3.0" and "TLS 1.0".
Verify Client Certificate?	Select "**No**".
Encryption Method	Refer to the Interstage Management Console Help, and change this if necessary.
CA Certificate Nickname	Refer to the Interstage Management Console Help, and change this if necessary.

3.1.3.2 Setup of Interstage Single Sign-On

This section explains how to set up Interstage Single Sign-On.

Note

There is no need to perform this task if the Interstage Single Sign-On setup is already complete.

3.1.3.2.1 Creating the Management Server Web Server

Using the Interstage Management Console, create the Management Server Web server (Interstage HTTP Server).

Note

There is no need to perform this task if the Management Server Web server has already been built. Normally, this is created automatically at the time of product installation.

Using the Interstage Management Console, create the Management Server Web server (Interstage HTTP Server).

1. Start the Interstage Management Console.

    Follow the procedure below to start the Interstage Management Console:

    1. Start the Web browser.

    2. Specify the Interstage Management Console URL.

        The URL format is shown below:
        (When SSL encrypted communication is not used)

        http://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

        (When SSL encrypted communication is used)

        https://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

    3. Log into the Interstage Management Console.

2. Create the Management Server Web server (Interstage HTTP Server).

    Select the **System** >> **Services** >> **Web Server** >> **Create a new Web Server** tabs, and configure the Interstage HTTP Server environment settings.

    Specify the following items:

Settings item	Settings value
Web Server Name	Set "FJapache".
Port Number	Set "80".

Select the Web server name that was created, open the environment settings tab, click **Detailed Settings** >> **Show**, change the environment settings as shown below, then click the Update button.

Settings item	Settings value
Enable SSL Encryption	Select "**No**".

3.1.3.2.2 Executing the Interstage Single Sign-On Setup Command

Set up Interstage Single Sign-On using the Interstage Single Sign-On Setup command ("ssoclsetup command").
By executing the ssoclsetup command, the servers shown below that are required for Interstage Single Sign-On are built:

- Repository server (update type)

- Authentication server

- Business server

Following information is set by ssoclsetup command.

Settings item	Settings value
Public directory	ou=interstage, o=fujitsu, dc=com
Administrator DN	cn=manager, ou=interstage, o=fujitsu, dc=com
Authentication Web server name	SSOauth
Authentication server port number	10443 10550 10555
Idle monitoring time	30 min.
Re-authentication interval	480 min.
Lock User	Consecutive failures: 6
Release lock	Auto release time: 30 min.
Business server name	FJapache
Business server port number	80

🕝 Note
....

The following information is required to execute the ssoclsetup command:

(Mandatory)

- Server FQDN

- SSL definition

For the SSL definition, specify the SSL definition created in "3.1.3.1.4 Settings for SSL Communication".Refer to the *Building environment command* in the *Systemwalker Runbook Automation Reference Guide* for information on the ssoclsetup command
....

Creation procedure

1. Perform the following tasks beforehand if this product has been installed in "C:\Program Files (x86)" on a machine running 64-bit Windows:

   1. Create the following two folders. The folder name can contain up to 192 characters, and can contain alphanumeric characters, whitespace characters, and the following symbols ($ & ' + - . = @ _ ` ~ [ ] { } : /).

      - The SSO repository database storage folder (Example:C:\SSORepository\Database)

      - The the SSO repository access log storage folder (Example:C:\SSORepository\var)

   2. Edit the following SSO repository operating environment definition file:

      ```
      [Systemwalker Runbook Automation Management Server installation directory]\sso\F3FMctsec\sso
      \conf\irep\irep.conf
      ```

      Specify the directory created in the previous step as indicated below:

      - SSO repository database storage directory

        [Before]

        ```
        #ena_directory:
        ```

        [After (Example)]

        Example in which C:\SSORepository\Database was created as the SSO repository database storage directory:

        ```
        ena_directory: C:\SSORepository\Database
        ```

      - SSO repository access log storage directory

        [Before]

        ```
        #accesslog_dir:
        ```

        [After (Example)]

        Example in which C:\SSORepository\var was created as the SSO repository access log storage directory:

        ```
        accesslog_dir: C:\SSORepository\var
        ```

2. Execute the ssoclsetup command:

   [Windows]

   ```
   [Systemwalker Runbook Automation management server installation directory]\sso\bin\ssoclsetup
   FQDN SSLConfName [-rn RepositoryName] [-lp LDAPPort]
   ```

   [Linux]

   ```
   /opt/FJSVctsec/sso/bin/ssoclsetup FQDN SSLConfName [-rn RepositoryName] [-lp LDAPPort]
   ```

3. Enter the SSO repository administrator DN password. Note that $, \, ", and spaces must not be used.

For the detail of ssoclsetup command, refer to "ssoclsetup (Interstage Single Sign-on Setup Command)"

in the *Syetemwalker Runbook Automation Reference Guide.*

By executing the ssoclsetup command, the servers shown below that are required for Single Sign-On are built.

- Repository server (update type)

- Authentication server

- Business server

Execution example [Windows]

The command execution examples shown below use the following values:

```
- Server FQDN: ssoserver.example.com
- SSL definition: AuthSSL
- Repository name:rep001
- Repository port number:389
```

Change the FQDN and SSL definition if necessary.

In Systemwalker Runbook Automation, the command is stored in the following folder:

[*Systemwalker Runbook Automation management server installation directory*]\sso\bin

```
ssoclsetup ssoserver.example.com AuthSSL
Please input SSO Repository administrator DN password
Password:
Retype:
IREP: INFO: irep10815: Password file was created.
file=C:\INTERS~3\F3FMsso\ssoatcsv\conf\tmp_passwdfile
checking the repository configuration... (1/4)
initializing the repository... (2/4)
creating the public directory. (3/4)
updating the repository management list... (4/4)
IREP: INFO: irep70001: Repository environment configured. [rep001]
IHS: INFO: ihs01000: The command terminated normally.
IHS: INFO: ihs01000: The command terminated normally.
IHS: INFO: ihs01000: The command terminated normally.
IREP: INFO: irep70000: Repository environment setup updated. [rep001]
IHS: INFO: ihs01000: The command terminated normally.
```

Execution example [Linux]

The command execution examples shown below use the following values:

```
- Server FQDN: ssoserver.example.com
- SSL definition name: AuthSSL
- Repository name:rep001
- Repository port number:389
```

Change the FQDN and SSL definition name if necessary.
The Bourne shell has been used in the execution example.

```
# /opt/FJSVctsec/sso/bin/ssoclsetup ssoserver.example.com AuthSSL
Please input SSO Repository administrator DN password
Password:
Retype:
UX:IREP: INFO: irep10815: Password file was created. file=/etc/opt/FJSVssosv/conf/tmp_passwdfile
checking the repository configuration... (1/4)
initializing the repository... (2/4)
creating the public directory. (3/4)
updating the repository management list... (4/4)
UX:IREP: INFO: irep70001: Repository environment configured. [rep001]
UX:IREP: INFO: irep10000: Repository started. [rep001]
UX:IHS: INFO: ihs01000: The command terminated normally.
UX:IHS: INFO: ihs01000: The command terminated normally.
UX:IHS: INFO: ihs01000: The command terminated normally.
UX:IREP: INFO: irep70000: Repository environment setup updated. [rep001]
UX:IREP: INFO: irep10000: Repository started. [rep001]
UX:IHS: INFO: ihs01000: The command terminated normally.
```

3.1.3.3 Setting Information in the Existing Interstage Single Sign-On

This section explains the setting of information in the existing Interstage Single Sign-On.

3.1.3.3.1 Adding Roles

This section explains the setting of additional roles in the existing Interstage Single Sign-On.

Creation procedure

1. Check public directory that was set as SSO repository of existing Interstage Single Sign-On.

   Open **System** >> **Services** >> **Repository,** and click repository name that was set as SSO repository to check the public directory.

2. Check LDIF file defining roles.

   Confirm that the LDIF file defining roles is stored in the following place.

   [Windows]

   ```
   [Systemwalker Runbook Automation management server installation directory]\sso\ldif
   \cloud_role.ldif
   ```

   [Linux]

   ```
   /opt/FJSVswrba/sso/ldif/cloud_role.ldif
   ```

3. Copy the LDIF file defining roles to another folder, and open the copied file.

   Confirm that the following string is set in the file.

   [Windows]

   $PUBLIC_DIR$

   [Linux]

   %PUBLIC_DIR%

   ![Note icon] **Note**
   . . . .
   Open the copied file because the LDIF file described in step 2 is the master file.
   . . . .

4. Change string which confiremed in step3 to value of public directory which confiremed in step1.

5. Specify the file changed in 4 in the ldapmodify command, and add the role to the existing Interstage Single Sign-On.

   Refer to the *Interstage Application Server/Interstage Web Server Reference Manual (Command Edition)* for information on the ldapmodify command.

6. Using the Interstage Management Console click **System** >> **Security** >> **Single Sign-on** >> **Authentication Infrastructure** >> **Repository Server** >> **Update Role Information** tab, **Update** button.

Settings example

The LDIF file settings example shown below uses the following environment:

```
- Public directory: ou=interstage,o=fujitsu,dc=com
```

```
#Systemwalker Software Configuration Manager V14g Role
dn: cn=CFMGSystemAdmin,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
objectClass: ssoRole
objectClass: top
cn: CFMGSystemAdmin

dn: cn=CFMGSystemUser,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
objectClass: ssoRole
```

```
objectClass: top
cn: CFMGSystemUser

#Systemwalker Service Catalog Manager V14g Role
dn: cn=CTMGProviderAdmin,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
objectClass: ssoRole
objectClass: top
cn: CTMGProviderAdmin

dn: cn=sop_contractor,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
objectClass: ssoRole
objectClass: top
cn: sop_contractor

dn: cn=sop_resource_manager,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
objectClass: ssoRole
objectClass: top
cn: sop_resource_manager

dn: cn=sop_delegated_manager,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
objectClass: ssoRole
objectClass: top
cn: sop_delegated_manager

dn: cn=sop_restricted_user,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
objectClass: ssoRole
objectClass: top
cn: sop_restricted_user
```

Execute ldapmodify command.

Execute the ldapmodify command specifying the LDIF file modified in step 5 to add roles to Interstage Single Sign-On.

[Windows]

The command execution examples shown below use the following settings values:

```
- SSO repository FQDN: existing_ssoserver.example.com
- SSO repository port number: 389
- SSO repository administrator DN: cn=manager,ou=interstage,o=fujitsu,dc=com
- SSO repository administrator DN password: admin
```

```
[Interstage Application Server installation directory]\bin\ldapmodify -H ldap://
existing_ssoserver.example.com: 389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w admin -a -f
copy destination folder\cloud_role.ldif
```

[Linux]

The command execution examples shown below use the following values:

```
- SSO repository FQDN: existing_ssoserver.example.com
- SSO repository port number: 389
- SSO repository administrator DN: cn=manager,ou=interstage,o=fujitsu,dc=com
- SSO repository administrator DN password: admin
```

```
# /opt/FJSVirepc/bin/ldapmodify -H ldap://existing_ssoserver.example.com:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -w admin -a -f copy destination
```

After the command has been executed, using the Interstage Management Console click **System** >> **Security** >> **Single Sign-on** >> **Authentication Infrastructure** >> **Repository Server** >> **Update Role** I**nformation** tab, **Update** button.

3.1.3.3.2 storehouse Server Environment Settings

To use the existing Interstage Single Sign-On, the repository server environment settings must be configured.
With the Interstage Management Console, register the repository server using the following procedure:

1. Perform the environment settings for repository server.

   Click **System** >> **Security** >> **Single Sign-on** >> **Authentication infrastructure** >> **Repository server**, then select the Settings tab.

2. Click **Repository server detailed settings** >> **Show**, then set "o" in Information notified to the Business System >> **Extended user information**, then click **Update** button.

3. Restart the authentication server.

   Click **System** >> **Services** >> **Web Server** >> [**SSOauth**], then select the Web Server Status tab

   - When the status of the Web server (SSOauth) is running: Click Stop Button, then click Start button.

   - When the status of the Web server (SSOauth) is stopped: Click [start] button.

3.1.3.3.3 Registering the Management Server

To use the existing Interstage Single Sign-On, the Management Server must be registered in the existing Interstage Single Sign-On.
With the Interstage Management Console, register the Management Server using the following procedure:

1. Registering Management Server Site Definitions

2. Registering Protected paths

3. Creating the Business system setup file

4. Adding Interstage Single Sign-On Business Servers

5. Suppressing Contents Cache

📄 Note
. . . .
The ssoclsetup command cannot be used to register the Management Server.
. . . .

Registering Management Server Site Definitions

With the Interstage Management Console, set the Management Server public URL using the following procedure:

1. Start the Interstage Management Console.

   Refer to 3.1.3.2.1 Creating the Management Server Web Server *for the Management Server* for information on the Interstage Management Console start procedure.

2. Set the Management Server public URL.

   Open the **System** >> **Security** >> **Single Sign-on** >> **Authentication infrastructure** >> **Repository server** >> **Protected resource** >> **New** tab.
   In **Site Definition** >> **FQDN, Port Number,** enter the Management Server FQDN and port number (80) then click the **Create** button.

Registering Protected Paths

With the Interstage Management Console, register the protected path using the following procedure:

1. Start the Interstage Management Console.

   Refer to 3.1.3.2.1 Creating the Management Server Web Server for information on the Interstage Management Console start procedure.

2. Register the protected path.

Select the **System** >> **Security** >> **Single Sign-on** >> **Authentication infrastructure** >> **Repository server** >> **Protection Resource** >> **Management Server FQDN:80** >> **Protection Path** >> **Create a New Path configuration** tab.
Set the role/roleset for the path definition and path as shown below, then create the new protected path.

Path Configuration Settings		Role/Roleset
Path	**Notify extended user information**	(Select the following items)
/console/Default/	-	-
/managerview/	Select "o"	CFMGSystemAdmin CFMGSystemUser
/myportal/	Select "o"	sop_contractor sop_resource_manager sop_restricted_user
/op_portal/	-	CTMGProviderAdmin
/ibpmm/dashboard/	-	CTMGProviderAdmin
/CTMGApproverSelection/	-	sop_contractor sop_resource_manager sop_restricted_user
/CMDBConsole/	-	-

Creating the Business System Setup File

With the Interstage Management Console, create the business system build file using the following procedure:

1. Start the Interstage Management Console.

   Refer to 3.1.3.2.1 Creating the Management Server Web Server for information on the Interstage Management Console start procedure.

2. Create the business system build file.

   Click **System** >> **Security** >> **Single Sign-on** >> **Authentication Infrastructure** >> **Business system setup file** tab.
   Set **Business System Information** as shown below, enter a password (6 or more characters), then click **Download**.

Settings item	Settings value
Public URL	http://Management Server FQDN:80
Linkage with Interstage Portalworks?	**No**

3. Save the downloaded file.

Registering the Management Server

With the Interstage Management Console, add the Interstage Single Sign-On business server to the Management Server using the following procedure:

1. Start the Interstage Management Console.

   Refer to 3.1.3.2.1 Creating the Management Server Web Server for information on the Interstage Management Console start procedure.

2. Set the business system build file and password.

   Click **System** >> **Security** >> **Single Sign-on** >> **Business System** >> **Addition of Business server** tab.

Set the business system build file and password that were downloaded in "Creating the Business System Setup File" in **Business System Setup File** and **Password of file,** then click **Next**.

3. Add the Interstage Single Sign-On business server to the Management Server.

   Set the following simple settings values, then click the **Add** button.

Settings item	Settings value
Business system Name	Business001
Web Server used	Fjapache
Host for Web server used	Main host: 80
When updating Access Control Information?	**Execute when Business server is started**
Use Single Sign-On JavaAPI?	**Yes**

4. Change the environment settings.

   Click **System** >> **Security** >> **Single Sign-on** >> **Business system** >> **Business system Name**. **Business system Name** is the business system name that was specified in step 3.

   Open the environment settings tab, click **Detailed Settings** >> **Show**, change the environment settings as shown below.

Settings item	Settings value
Enable Client IP Address Check?	**No**
Notify User Information?	**Yes**
Notify Sign-off URL?	**Yes**

5. Check the values that were set.

   Once the above settings are complete, click the Update button.

Suppressing Contents Cache

Activate the Web browser cache settings using the following procedure:

1. Start the Interstage Management Console.

   Refer to 3.1.3.2.1 Creating the Management Server Web Server for information on the Interstage Management Console start procedure.

2. Stop the Web server.

   With the Interstage Management Console, select **System** >> **Services** >> **Web Server** >> **FJapache** to display **FJapache:Status**, then click the **Stop** button.

3. Update the business server environment definition file.

   Using an editor, update the business server environment definition file.
   The business server environment definition file storage location and file name are as follows:

   [Windows]

   ```
   <Interstage Application Server installation folder>\F3FMsso\ssoatzag\conf\ssoatzag.conf
   ```

   [Linux]

   ```
   /etc/opt/FJSVssoaz/conf/ssoatzag.conf
   ```

   Edit the above file as follows:
   Add "http-cache-cntl=NO" to the line that follows "business-system-name = <business system name that was specified in 3.1.3.3.3 Registering the Management Server>".

   In the execution example below, "Business001" has been used for the business system name.

```
ServerPort=80
    (snip)
business-system-name=Business001
http-cache-cntl=NO
```

4. Start the Web server.

    Select **System** >> **Services** >> **Web Server** >> **FJapache** to display **FJapache:Status**, then click the **Start** button.

3.1.4 Installing in a ServerView Operations Manager Single Sign-On Environment

If there is a ServerView Operations Manager Single Sign-On environment that has already been created, the same authentication infrastructure can be used with Systemwalker Runbook Automation as well.

Refer to the ServerView Operations Manager manuals for information on creating a single sign-on environment for ServerView Operations Manager.

Note

- ServerView Operations Manager must be installed on the Management Server for Systemwalker Runbook Automation.

- Note that $, \, ", and spaces must not be used in the LDAP repository administrator password used in ServerView Operations Manager Single Sign-On.

3.1.5 LDAP Environment Build and Settings

When user authentication is performed using only the LDAP repository, and without using Interstage Single Sign-On authentication infrastructure, the LDAP environment is built using this procedure.

3.1.5.1 Creating an Environment for the Interstage Directory Service

To use the Interstage Directory Service with LDAP authentication, create an environment for the Interstage Directory Service by following the steps below.

Note

- If an environment for the Interstage Directory Service has already been created, change the settings in the Detailed Settings item to match the Systemwalker Runbook Automation operation.

- Refer to the *Interstage Application Server Directory Service Operator's Guide* for details.

1. Open the login window for the Interstage Management Console by entering the following URL in a Web browser.

    http://<*Host name of the Interstage Directory Service*>:[*port number for the Interstage Management Console*]/
    IsAdmin

2. Specify the following login ID and password in the login window, and then click the Login button.

    [Windows]

User ID	Password
Administrator	Password for the administrator

    [Linux]

User ID	Password
root	Password for the root account

3. Open the repository window by selecting **System** >> **Service** >> **Repository** from the tree view (the pane on the left-hand side of the window).

4. Select the Create tab.

5. Specify the following items in the General Settings section.

Item name	Description	Input value
Repository Name	Repository name. Item can be specified only when creating a repository.	Optional
Administrator DN	Administrator of the created repository, using DN (distinguished name) format. Item can be specified only when creating a repository.	LDAP administrator name
Administrator DN password	Administrator password. Note that $, \, ", and spaces must not be used.	Password for the LDAP administrator
Administrator DN password (re-enter)	Administrator password (confirmation).	Password for the LDAP administrator
Public Directory	Directory where the repository will be published, using DN (distinguished name) format. Item can be specified only when creating a repository.	The name of the domain that has been created (in "dc=..." format) Example: ou=interstage,o=fujitsu,dc=dom
Repository Database	If an RDB is used, more than 10,000 items of entry information can be managed. Item can be specified only when creating a repository.	Standard DB is recommended.
Database Storage Directory	Directory where the database is stored. The specified directory must already exist. Item can be specified only when creating a repository. 📒 **Note** . . . . There is no need to change the storage directory if it located in a directory under "C:\Program Files (x86)" on a machine running 64-bit Windows.	[Windows] Default value: <*Interstage installation directory*> \Enabler\EnablerDStores\IREP [Linux] Default value: /var/opt/FJSVena/DStores/FJSVirep (*1)
Cache Size	Size of the cache to be used for search processing.	1000

*1: If the specified directory is different from the default, then privilege settings will need to be specified.
Refer to "Repository Operation and Maintenance" in the *Interstage Application Server Directory Service Operator's Guide* for details.

6. Display Detailed Settings and enter the following settings.

Search settings	
Item name	**Input value**
Maximum number of entries that can be searched for	Specify a value greater than the number of users that will be registered with Systemwalker Runbook Automation. Default value: 500
Search Timeout	Specify the timeout (in seconds) for authentication processing. Default value: 3600

Access log definition	
Item name	**Input value**
Directory	Specify the existing access log storage directory. **Note** . . . . There is no need to change the storage directory if it is located in a directory under "C:\Program Files (x86)" on a machine running 64-bit Windows. . . . .

Point

. . . .

This procedure lists only mandatory items. Refer to "Repository Operation and Maintenance" in the *Interstage Application Server Directory Service Operator's Guide* for information on how to customize other setting items.

. . . .

7. Click the Create button - a message informing that creation is complete will be displayed.

8. Select the name of the repository that has been created, then click the Start button - a message informing that the repository has started will be displayed.

9. Log out.

3.1.5.2 Creating an Environment for Active Directory or OpenLDAP

To use Active Directory or OpenLDAP, refer to each manual. Note that $, \, ", and spaces must not be used in the OpenLDAP repository administrator password.

3.1.6 Registering Users, Groups and Organizational Units

To create an environment for Systemwalker Runbook Automation , register the required user information on a directory service. This section explains the registration method for each authentication protocol. Register user information in accordance with the authentication protocol being used.

- Authentication using Interstage Single Sign-On

- Authentication Using ServerView Operations Manager Single Sign-On

- Authentication via LDAP

Note

. . . .

- Users, groups and organizational units only need to be registered with the LDAP directory for the initial setup after installation. This is not required when the setup is canceled and then performed again

- There is no need to create organizational units if the LDAP directory is to be operated using organizational units that have already been created.

- The users and groups created in this chapter are the ones required for Systemwalker Runbook Automation to run. Be sure to create these users and groups.

  Refer to the *Systemwalker Runbook Automation Operation Guide* for details on how to create and register users that will actually perform operations.

- Creating LDIF file with copying example from this manual is discouraged. Because it is occurred to drop linefeed or to add linefeed doubly, by your using Web browser or viewer program. Recommend using sample according to procedure on this manual.

  By necessity, to copy example from this manual, create LDIF file with well-confirming that linefeed is added according to displayed manuals.

3.1.6.1 Authentication using Interstage Single Sign-On

To use authentication using the Interstage Single Sign-On function, register user information with the Interstage Directory Service.

3.1.6.1.1 Registering user information on Interstage Directory Service

This section describes procedure that register user on Interstage Directory Service

This section describes how to register user with using LDIF file.

- How to Register User Information Using Sample LDIF File

- How to Create and Register LDIF File

Note

For details of LDIF file, Refer to the *Interstage Application Server Directory service Operation Guide*

Information

Registering User information can also be done with using Entry management tool of GUI. For details, Refer to the *Interstage Application Server Directory service Operation Guide*

How to Register User Information Using Sample LDIF File

This section describes method that registering User information using sample LDIF file specified user information to build Systemwalker Runbook Automation environment.

Register location for sample LDIF file

Register LDIF sample on as below.

[Windows]

```
Systemwalker Runbook Automation Install directory for Management Server\etc\sample\ldif
```

[Linux]

```
/etc/opt/FJSVswrbam/sample/ldif/
```

LDIF File	Explanation
swrba_sso_sample.ldif	This is ldif file to create Users, Groups and Organizational Units and to add user to Group If you use Interstage Single Sign-On authentication foundation, use this sample.
swrba_no_sso_sample.ldif	This is ldif file to create Users, Groups and Organizational Units and to add user to Group

LDIF File	Explanation
	If you do not use Interstage Single Sign-On authentication foundation, use this sample.

Sample definitional content and how to edit

This sample assumes the following LDAP composition

Edit file according to LDAP environment and make sure to change password for process control and user for schedule startup

Public directory	ou=interstage,o=fujitsu,dc=com
Organizational Units for registering user	ou=User
Organizational Units for registering group	ou=Group
User for process control	swrbaadmin
User password for process control	systemwalker#1
User for schedule startup	swrbasch
Password of user for schedule startup	systemwalker#2

For detail explanation of contents specified LDIF file, Refer to the How to Create and Register LDIF File

How to register sample

Register definition information of LDIF file on LDAP with using ldapmodify command

[Windows]

```
ldapmodify -H ldap://<Interstage Directory Service host name>:<port number> -D "<administrator DN>" -w <password> -a -f <edit LDIF file>
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://<Interstage Directory Service host name>:<port number> -D "<administrator DN>" -w <password> -a -f <edited LDIF file>
```

Example

Interstage Directory Service host name: hostname

Port number: 389

Administrator DN: cn=manager, ou=interstage, o=fujitsu, dc=com

Manager DN password: password

Name of the LDIF file that was edited: rbauser.ldif

[Windows]

```
ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f rbauser.ldif
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f rbauser.ldif
```

For the detail ldapmodify command, Refer to the Interstage directory service operation command in the Interstage Application Server/ Interstage Web Server Reference (Command)

How to Create and Register LDIF File

This section describes method that creating LDIF file for registering the following User information.

Although this section describes that creating three LDIF file, it is possible to register on LDAP with all files in one file.

- LDIF file for creating Organizational Units (OU)

- LDIF file for registering users

- LDIF file for registering groups and adding users

LDIF file for creating Organizational Units (OU)

Describes definition for registering Organizational Units (OU) indicated the following table on LDAP

Name of creating Organizational Units (OU)	Whether an arbitrary name can be specified
Group	Yes
User	Yes

🅿 Point

· ·

It is possible to be hierarchized Organizational Units (OU).

· ·

Create LDIF file for registering Organizational Units (OU) as directed setting example

Setting Example1:In case of using User as a Group managed User

User Group is created automatically when repository is created.

To use User Group as a group managed user, Prepare LDIF file which registered only group as below.

```
dn: ou=Group,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: Group
```

Setting Example2:In case of using except User Group as a Group managed User:

To use except name "User" Group as a group managed user, Prepare LDIF file which registered two groups, which one group managed a group and the other group managed user as below.

```
dn: ou=Group,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: Group

dn: ou=<ou name except User>,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: <ou name except User>
```

Note that the %...% parts of the file should be replaced with the elements in the list below.

Replace Target List

Replace target symbol	Setting value after replacing
%DOMAIN%	Public directory (Example) ou=interstage,o=fujitsu,dc=com

Replace target symbol	Setting value after replacing
	Note: To setup after building LDAP, It is necessary to specify this setting value on LDAP key name when setup.

P Point

....

For the detail of object class and attribute which specified on setting example, Refer to the *Object Class List* and *Attribute List* in the *Interstage Application Server Directory Service Operation Guide*.

....

LDIF file for registering users

Describes definition for registering user indicated the following table on LDAP

User name	Password	Explain
swrbaadmin :Note1	systemwalker#1 :Note2	User which needed by Systemwalker Runbook Automation control process. (mandatory)
swrbasch (Note 1)	systemwalker#2 (Note 2)	User required by Systemwalker Runbook Automation to start the Automated Operation Process according to a schedule (mandatory)

Note 1
Although it is suggested user name, it is possible to specify any name.

Note 2
Systemwalker#1 and Systemwalker#2 is default. This can be changed to any password, except one containing $, \, ", and spaces.

Create LDIF file to register user according to the setting example.

Setting example 1: n case of using Interstage Single Sign-On

```
dn: uid=swrbaadmin ,ou=%USER%,%DOMAIN%
changetype: add
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
objectClass: ssoUser
cn: swrbaadmin
sn: swrbaadmin
givenName: swrbaadmin
userPassword: systemwalker#1
uid: swrbaadmin

dn: uid=swrbasch,ou=%USER%,%DOMAIN%
changetype: add
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
objectClass: ssoUser
cn: swrbasch
sn: swrbasch
givenName: swrbasch
```

```
userPassword: systemwalker#2
uid: swrbasch
```

Setting example 2: In case of not using Interstage Single Sign-On

```
dn: uid=swrbaadmin ,ou=%USER%,%DOMAIN%
changetype: add
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: swrbaadmin
sn: swrbaadmin
givenName: swrbaadmin
userPassword: systemwalker#1
uid: swrbaadmin

dn: uid=swrbasch,ou=%USER%,%DOMAIN%
changetype: add
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: swrbasch
sn: swrbasch
givenName: swrbasch
userPassword: systemwalker#2
uid: swrbasch
```

Note that the %...% parts of the file should be replaced with the elements in the list below.

Replace Target List

Replace target symbol	Setting value after replacing
%DOMAIN%	Public directory
	(Example) ou=interstage,o=fujitsu,dc=com
	Note: To setup after building LDAP, It is necessary to specify this setting value on LDAP key name when setup.
%USER%	Organizational Units (OU) User (if it is changed name in Creating an organizational unit (OU), specify changed name of Organizational Units (OU).
	(Example) User
	Note: To setup after building LDAP, It is necessary to specify "ou=<%USER% setting value>" in Organizational Units which stored user account.

📌 Point

For the detail of object class and attribute which specified on setting example, Refer to the *Object Class List* and *Attribute List* in the *Interstage Application Server Directory Service Operation Guide*.

LDIF file for registering groups and adding users

Describes definition for registering group indicated the following table

Group name	Member belonged
AdminRole	- swrbaadmin

Group name	Member belonged
	- swrbasch
IflowUsers	- swrbaadmin
	- swrbasch
IflowGroups	- AdminRole
	- swrba_Exe
	- Role
swrba_Exe	- swrbaadmin
Role	- swrbaadmin

🖢 **Note**

. . . .

Not attach user except of *swrbaadmin* in swrba_Exe group.

If you attach except of swrbaadmin user, it may occur error on Automated Operation Process

. . . .

Create LDIF file to register group and add user according to the setting example.

Setting example

```
dn: cn=AdminRole,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: AdminRole
member: uid=swrbaadmin ,ou=%USER%,%DOMAIN%
member: uid=swrbasch,ou=%USER%,%DOMAIN%

dn: cn=IflowUsers,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: IflowUsers
member: uid=swrbaadmin ,ou=%USER%,%DOMAIN%
member: uid=swrbasch,ou=%USER%,%DOMAIN%

dn: cn=IflowGroups,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: IflowGroups
member: cn=AdminRole,ou=%GROUP%,%DOMAIN%
member: cn=swrba_Exe,ou=%GROUP%,%DOMAIN%
member: cn=Role,ou=%GROUP%,%DOMAIN%

dn: cn=swrba_Exe,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: swrba_Exe
member: uid=swrbaadmin,ou=%USER%,%DOMAIN%

dn: cn=Role,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
```

```
cn: Role
member: uid=swrbaadmin,ou=%USER%,%DOMAIN%
```

Note that the %...% parts of the file should be replaced with the elements in the list below.

Replace Target List

Replace target symbol	Setting value after replacing
%DOMAIN%	Public directory (Example) ou=interstage,o=fujitsu,dc=com Note: To setup after building LDAP, It is necessary to specify this setting value on LDAP key name when setup.
%USER%	Organizational Units (OU) User (if it is changed name in Creating an organizational unit (OU), specify changed name of Organizational Units (OU). (Example) User Note: To setup after building LDAP, It is necessary to specify "ou=<%USER% setting value>" in Organizational Units which stored user account.
%GROUP%	Organizational Units (OU) Group (if it is changed name in Creating an organizational unit (OU), specify changed name of Organizational Units (OU). (Example) Group Note: To setup after building LDAP, It is necessary to specify "ou=<%Group% setting value>" in Organizational Units which stored user account.

🅿 Point

For the detail of object class and attribute which specified on setting example, Refer to the *Object Class List* and *Attribute List* in the *Interstage Application Server Directory Service Operation Guide.*

Registering procedure

Register Organizational Unit, Group, and user on Interstage Directory Service.
Show the registering entry data example with using ldapmodify command and LDIF file as below.

[Windows]

```
ldapmodify -H ldap://<Interstage Directory Service host name>:<port number> -D "<administrator DN>" -w <password> -a -f <edited LDIF file >
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://<Interstage Directory Service host name>:<port number> -D "<administrator DN>" -w <password> -a -f <edited LDIF file>
```

📝 Example

Interstage Directory Service host name: hostname

Port number: 389

Manager DN: cn=manager, ou=interstage, o=fujitsu, dc=com

Manager DN password: password

Edited LDIF file: rbauser.ldif

[Windows]

```
ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f rbauser.ldif
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w
password -a -f rbauser.ldif
```

・・・

For the detail ldapmodify command, Refer to the *Interstage directory service operation command* in the *Interstage Application Server/ Interstage Web Server Reference (Command)*

3.1.6.2 Authentication Using ServerView Operations Manager Single Sign-On

To use ServerView Operations Manager Single Sign-On authentication, register user information with OpenDS , or Active Directory.

3.1.6.2.1 Registering User Information with OpenDS

This section explains the procedure for registering users with OpenDS.

This section explains how to register user information using LDIF files, which is one of the methods for registering users.

- How to register user information using a sample LDIF file

- How to register user information by creating a new LDIF file

How to register user information using a sample LDIF file

This section explains how to register the user information required to create a Systemwalker Runbook Automation environment by using a sample LDIF file that defines the user information.

Location of the sample LDIF files

The sample LDIF file is stored in the following location:

[Windows]

```
<Installation directory for the Systemwalker Runbook Automation Management Server>\etc\sample\ldif
```

[Linux]

```
/etc/opt/FJSVswrbam/sample/ldif/
```

LDIF file	Description
swrba_svsso_sample.ldif	This is an LDIF file for creating users, groups and organizational units, and for adding users to groups. To use the authentication infrastructure for ServerView Operations Manager Single Sign-On, use this sample file.

The definitions in the sample file and how to edit them

This sample file assumes the following LDAP configuration.

Edit the file according to the LDAP environment being used. Also, be sure to change the password for the process control user and the password for the schedule startup user.

Public directory	dc=fujitsu,dc=com
Organizational unit that contains users	ou=users
Organizational unit that contains groups	ou=Group
Process control user	swrbaadmin
Process control user password	systemwalker#1

Schedule startup user	swrbasch
Schedule startup user password	systemwalker#2

Refer to "How to Create and Register LDIF File" for details on the content of LDIF files.

How to register the sample file

Use the ldapmodify command to register the definition information contained in the LDIF file with the LDAP directory:

[Windows]

> *<OpenDS installation directory>*\bat\ldapmodify.bat -p *<port number>* -Z -D *<administrator DN>* -w *<password for the administrator DN>* -f *<name of the edited LDIF file>*

[Linux]

> *<OpenDS installation directory>*/bin/ldapmodify -p *<port number>* -Z -D *<administrator DN>* -w *<password for the administrator DN>* -f *<name of the edited LDIF file>*

Example

Port number: 1474

Administrator DN: cn=Directory Manager,cn=Root DNs,cn=config

Password for the administrator DN: admin

Name of the edited LDIF file: rbauser.ldif

[Windows]

> ldapmodify.bat -p 1474 -Z -D "cn=Directory Manager,cn=Root DNs,cn=config" -w admin -f rbauser.ldif

[Linux]

> ldapmodify -p 1474 -Z -D "cn=Directory Manager,cn=Root DNs,cn=config" -w admin -f rbauser.ldif

How to register user information by creating a new LDIF file

This section explains how to create the following LDIF files that register the user information with LDAP.

Here we will create three LDIF files, but it is also possible to register the same information with LDAP by grouping all of the information into a single LDIF file.

- LDIF file for creating organizational units (OUs)

- LDIF file for registering users

- LDIF file for registering groups and adding users to groups

LDIF file for creating organizational units (OUs)

This section explains the definitions for registering the following organizational units (OUs) with LDAP.

Name of the organizational unit to be created	Whether an arbitrary name can be specified
Group	Yes
User	Yes

> ### ℗ Point
> ....
> Organization units (OUs) can be layered.
> ....

Create LDIF files to register organizational units in accordance with the settings examples.

Example 1: Using "users" as the group for managing users

> The "users" group is created automatically when the repository is created.
>
> To use this "users" group as the group for managing users, prepare an LDIF file that registers only the "Group" organizational unit, as below:

```
dn: ou=Group,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: Group
```

Example 2: Using a group other than "users" as the group for managing users

> To use a group with a name other than "users" as the group for managing users, prepare an LDIF file that registers two organizational units (one for managing groups and the other for managing users), as below:

```
dn: ou=Group,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: Group

dn: ou=<organizational unit name other than "users">,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: <organizational unit name other than "users">
```

> Note that the %...% parts of the file should be replaced with the elements in the list below:

List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	Public directory Example: dc=fujitsu,dc=com Note: To execute the setup after creating an LDAP directory, this setting must be specified for the LDAP key name when the setup is executed.

LDIF file for registering users

> This section explains the definitions for registering the following users with LDAP:

User name	Password	Description
swrbaadmin (*1)	systemwalker#1 (*2)	The user that Systemwalker Runbook Automation requires in order to control processes. (Required)
swrbasch (*1)	systemwalker#2 (*2)	The user that Systemwalker Runbook Automation requires in order to start Automated Operation Processes in accordance with the schedule. (Required)

*1:

This is the recommended user name, but any name can be specified.

*2:

Systemwalker#1 and Systemwalker#2 are the default values. This can be changed to any password, except one containing $, \, ", and spaces.

Create an LDIF file to register users in accordance with the settings example.

Settings example

```
dn: cn=swrbaadmin ,ou=%USER%,%DOMAIN%
changetype: add
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: swrbaadmin
sn: swrbaadmin
givenName: swrbaadmin
userPassword: systemwalker#1
uid: swrbaadmin


dn: cn=swrbasch,ou=%USER%,%DOMAIN%
changetype: add
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: swrbasch
sn: swrbasch
givenName: swrbasch
userPassword: systemwalker#2
uid: swrbasch
```

Note that the %...% parts of the file should be replaced with the elements in the list below:

List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	Public directory Example: dc=fujitsu,dc=com Note: To execute the setup after creating an LDAP directory, this setting must be specified for the LDAP key name when the setup is executed.
%USER%	The "users" organizational unit (OU) (If the name of the OU created in "Creating an organizational unit (OU)" has been changed, specify the new name.) Example: users Note: To execute the setup after creating an LDAP server, ou=<*%USER% setting*> must be specified in the organization unit settings for storing LDAP user accounts when the setup is executed.

LDIF file for registering groups and adding users to groups

This section explains the definitions for registering the following groups:

Group name	Members
AdminRole	- swrbaadmin

Group name	Members
	- swrbasch
IflowUsers	- swrbaadmin
	- swrbasch
IflowGroups	- AdminRole
	- swrba_Exe
	- Role
swrba_Exe	- swrbaadmin
Role	- swrbaadmin

📖 Note

. . . .

Do not assign any users other than the "swrbaadmin" user to the "swrba_Exe" group.

If users other than "swrbaadmin" are assigned to this group, problems may occur with the behavior of Automated Operation Processes.

. . . .

Create an LDIF file for registering groups and adding users in accordance with the settings example.

Settings example

```
dn: cn=AdminRole,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: AdminRole
member: cn=swrbaadmin ,ou=%USER%,%DOMAIN%
member: cn=swrbasch,ou=%USER%,%DOMAIN%

dn: cn=IflowUsers,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: IflowUsers
member: cn=swrbaadmin ,ou=%USER%,%DOMAIN%
member: cn=swrbasch,ou=%USER%,%DOMAIN%

dn: cn=IflowGroups,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: IflowGroups
member: cn=AdminRole,ou=%GROUP%,%DOMAIN%
member: cn=swrba_Exe,ou=%GROUP%,%DOMAIN%
member: cn=Role,ou=%GROUP%,%DOMAIN%

dn: cn=swrba_Exe,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
cn: swrba_Exe
member: cn=swrbaadmin,ou=%USER%,%DOMAIN%

dn: cn=Role,ou=%GROUP%,%DOMAIN%
changetype: add
objectClass: groupOfNames
objectClass: top
```

```
cn: Role
member: cn=swrbaadmin,ou=%USER%,%DOMAIN%
```

Note that the %...% parts of the file should be replaced with the elements in the list below:

List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	Public directory Example: dc=fujitsu,dc=com Note: To execute the setup after creating an LDAP server, this setting must be specified for the LDAP key name when the setup is executed.
%USER%	The "users" organizational unit (OU) (If the name of the OU created in "Creating an organizational unit (OU)" has been changed, specify the new name.) Example: users Note: To execute the setup after creating an LDAP directory, ou=<*%USER% setting*> must be specified in the organization unit settings for storing LDAP user accounts when the setup is executed.
%GROUP%	The "Group" organizational unit (OU) (If the name of the OU created in "Creating an organizational unit (OU)" has been changed, specify the new name.) Example: Group Note: To execute the setup after creating an LDAP directory, ou=<*%GROUP% setting*> must be specified in the LDAP organizational unit settings when the setup is executed.

Registration procedure

Register the organizational units, groups and users with OpenDS.

The following example shows how to register entry data using the ldapmodify command and an LDIF file:

[Windows]

<OpenDS installation directory>\bat\ldapmodify.bat -p <port number> -Z -D <administrator DN> -w <password for the administrator DN> -f <name of the edited LDIF file>

[Linux]

<OpenDS installation directory>/bin/ldapmodify -p <port number> -Z -D <administrator DN> -w <password for the administrator DN> -f <name of the edited LDIF file>

Example

Port number: 1474

Administrator DN: cn=Directory Manager,cn=Root DNs,cn=config

Password for the administrator DN: admin

Name of the edited LDIF file: rbauser.ldif

[Windows]

ldapmodify.bat -p 1474 -Z -D "cn=Directory Manager,cn=Root DNs,cn=config" -w admin -f rbauser.ldif

[Linux]

ldapmodify -p 1474 -Z -D "cn=Directory Manager,cn=Root DNs,cn=config" -w admin -f rbauser.ldif

3.1.6.2.2 Registering User information with Active Directory

This section describes how to register users with Active Directory.

To register users with Active Directory, follow the steps below:

- Creating an organizational unit (OU)

- Creating users

- Creating groups and adding users

Creating an organizational unit (OU)

Create the organizational units (OUs) shown in the following table on Active Directory.

Name of the organizational unit to be created	Whether an arbitrary name can be specified
Group	Yes
User	Yes

P Point

....

Organizational units (OUs) can be layered.

....

Follow the steps below to register the organizational unit.

1. Select **Control Panel**, **Administrative Tools**, and then **Active Directory Users and Computers** from the **Start** menu.

2. Right-click the domain name managed by the Active Directory domain controller, and select **New** and then **Organizational Unit**.

3. In the **New Object** - **Organizational Unit** window, enter the name of the organizational unit (OU) shown in the table above, and then click the **OK** button.

4. Create all organizational units by repeating steps 2 and 3.

Creating users

Register the users shown in the following table on Active Directory.

Last name	First name	Initials	User logon name	Password	Whether to select check boxes in the password input window (*1)	Description
swrbaadmin (*2)	Bla nk	Bla nk	swrbaadmin (*2)	systemwalker#1 (*3)	D: **User must change password at next logon** O: **User cannot change password** S: **Password never expires** D: **Account is disabled**	User for process control (required)
swrbasch (*2)	Bla nk	Bla nk	swrbasch (*2)	systemwalker#2 (*3)	D: User must change password at next logon O: User cannot change password S: Password never expires D: Account is disabled	User for schedule startup (mandatory)

***1:** Select this check box O: Selecting this check box is optional D: Clear this check box

***2:** This is the recommended value, but any value can be specified

*3: Systemwalker#1 and Systemwalker#2 are the default values, but any value can be specified

Follow the steps below to register users:

1. Select **Control Panel, Administrative Tools**, and then **Active Directory Users and Computers** from the **Start** menu.

2. Right-click the "User" organizational unit (OU), and select **New** and then **User**. If the name of the OU created in "Creating an organizational unit (OU)" has been changed, then specify the new name.

3. In t he **New Object** - **User** window, enter the "Last name", "First name", "Initials" and "User logon name" fields as shown in the table above, and then click the **Next** button.

4. In the password window, select the check boxes as shown in the table above, and then click the **Next** button.

5. In the confirmation window, click the **OK** button.

Creating groups and adding users

Register the groups shown in the following table on Active Directory, and add users to these groups.

Group name	Group scope	Group type	Members
AdminRole	Global	Security	- swrbaadmin - swrbasch
IflowUsers	Global	Distribution	- swrbaadmin - swrbasch
IflowGroups	Global	Distribution	- AdminRole - swrba_Exe - Role
swrba_Exe	Global	Security	swrbaadmin
Role	Global	Security	swrbaadmin

Note

. . . .

- Not attach user except of *swrbaadmin* in swrba_Exe group.

  If you attach except of swrbaadmin user, it may occur error on Automated Operation Process

- Set swrbaadmin user as a member of Administrators group.

. . . .

Follow the steps below to register groups and add users:

1. Select **Control Panel, Administrative Tools**, and then **Active Directory Users and Computers** from the **Start** menu.

2. Right-click the "Group" organizational unit (OU), and select **New** and then **Group**. If the name of the OU created in "Creating an organizational unit (OU)" has been changed, then specify the new name.

3. In the **New Object** - **Group** window, enter the **Group name**, **Group scope**, and **Group type** items as shown in the table above, and then click the **OK** button.

4. Right-click one of the groups that have been created and then select **Properties**.

5. Select the **Member Of** tab and click the **Add** button.

6. In the **Select Users**, **Contacts**, **Computers or Groups** window, set the **Enter the object names to select** field to the users in the "Members" column of the table above, and then click the **OK** button.
   Separate users with semicolons (;).

7. In the group properties window, ensure that the group members have been added correctly, and then click the **OK** button.

8. Register all groups by repeating steps 2 to 7.

Note

....

It may take up to 90 minutes for the registration results to be reflected in the repository. To reflect the registration results immediately, restart Systemwalker Runbook Automation.

....

3.1.6.3 Authentication via LDAP

To use authentication via LDAP, register user information in accordance with the directory service being used.

- Registering User information with the Interstage Directory Service

- Registering User information with Active Directory

- Registering User information with OpenLDAP

3.1.6.3.1 Registering User Information with the Interstage Directory Service

Refer to "3.1.6.1.1 Registering user information on Interstage Directory Service" for information on registering information with the Interstage Directory Service.

3.1.6.3.2 Registering User information with Active Directory

Refer to "Registering User Information with Active Directory".

3.1.6.3.3 Registering User information with OpenLDAP

This section describes how to register users with OpenLDAP.

To register users with OpenLDAP, follow the steps below:

- Building public directory and creating manager DN

- Creating an organizational unit (OU)

- Creating users

- Creating groups and adding users

Building public directory and creating manager DN

Follow the steps below to create a public directory of OpenLDAP and register an administrator DN.

Note

....

This procedure is not required if a public directory has already been created and an administrator has been registered.

....

1. Create an LDIF file.

   If public directory contains organizational unit (OU), it is necessary to create organizational unit (OU).

   After it, Create LDAP administrator

   The file has the syntax below:

   ```
   dn: <public directory >

   objectClass: organizationalUnit

   ou: <Organization name>


   dn: cn=<LDAP administrator name>,<public directory name >

   objectClass: organizationalRole
   ```

```
cn: <LDAP administrator name>
```

An example is displayed below:

```
dn: ou=interstage,o=fujitsu,dc=com
objectClass: organizationalUnit
ou: interstage

dn: cn=manager,ou=interstage,o=fujitsu,dc=com
objectClass: organizationalRole
cn: manager
```

2. Register the domain and administrator with OpenLDAP:
   Execute the following command to register the domain and administrator with OpenLDAP.

```
ldapadd -x -W -D "cn=< LDAP administrator>,<Public directory>" -f <LDIF file created>
```

Note: The user will be prompted for the LDAP administrator password.

Creating an organizational unit (OU)

Create the organizational units (OUs) shown in the following table on OpenLDAP.

Name of the organizational unit to be created	Whether an arbitrary name can be specified
Group	Yes
User	Yes

🅿 Point

・・・

Organizational units (OUs) can be layered.

・・・

Follow the steps below to register an organizational unit:

1. Create an LDIF file.

   The file has the syntax below:

```
dn: ou=Group,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: Group

dn: ou=User,%DOMAIN%
changetype: add
objectClass: organizationalUnit
ou: User
```

   Note that the %...% parts of the file should be replaced with the elements in the list below.

   List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	<Public directory> (Example) ou=interstage,o=fujitsu,dc=com

Replacement symbol	Setting after replacement
	Note: To execute the setup after creating an LDAP directory, this setting must be specified for the LDAP key name when the setup is executed.

2. Register the organizational unit (OU) on OpenLDAP:

   Execute the following command to register the organizational unit (OU) on OpenLDAP:

   > ldapadd -x -W -D "cn=<*Name of the LDAP administrator*>,<*Public directory*>" -f <*Name of the LDIF file created*>

   Note: The user will be prompted for the LDAP administrator password.

Creating users

Register the users shown in the following table on OpenLDAP.

User name	Password	Description
swrbaadmin (*1)	systemwalker#1 (*2)	The user required for Systemwalker Runbook Automation to control processes (Required)
swrbasch (*1)	systemwalker#2 (*2)	User required by Systemwalker Runbook Automation to start automated operation process according to a schedule (mandatory)

*1: This is the recommended value, but any value can be specified

*2: Systemwalker#1 and Systemwalker#2 are the default values, but this can be changed to any password, except one containing $, \, ", and spaces

Follow the steps below to register users.

1. Create an LDIF file.

   In the following specification example, the default user IDs and passwords listed in the table above are specified as the user IDs and passwords.

   > dn: uid=swrbaadmin,ou=%USER%,%DOMAIN%
   > changetype: add
   > objectClass: inetOrgPerson
   > objectClass: organizationalPerson
   > objectClass: person
   > objectClass: top
   > cn: swrbaadmin
   > sn: swrbaadmin
   > givenName: swrbaadmin
   > userPassword: systemwalker#1
   > uid: swrbaadmin
   >
   > dn: uid=swrbasch,ou=%USER%,%DOMAIN%
   > changetype: add
   > objectClass: inetOrgPerson
   > objectClass: organizationalPerson
   > objectClass: person
   > objectClass: top
   > cn: swrbasch
   > sn: swrbasch
   > givenName: swrbasch

```
userPassword: systemwalker#2
uid: swrbasch
```

Note that the %...% parts of the file should be replaced with the elements in the list below.

List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	*<Public directory>* (Example) ou=interstage,o=fujitsu,dc=com Note: To execute the setup after creating an LDAP directory, this setting must be specified for the LDAP key name when the setup is executed.
%USER%	The "User" organizational unit (OU) (If the name of the OU created in "Creating an organizational unit (OU)" has been changed, specify the new name.) (Example) User Note: To execute the setup after creating an LDAP directory, ou=*<%USER% setting>* must be specified in the organizational unit settings for storing LDAP user accounts when the setup is executed.

2. Register the users on OpenLDAP:
   Execute the following command to register the user on OpenLDAP.

   ```
   ldapadd -x -W -D "cn=< LDAP administrator>,<Public directory>" -f <LDIF file created>
   ```

   Note: The user will be prompted for the LDAP administrator password.

Creating groups and adding users

Register the groups shown in the following table on OpenLDAP, and add users to these groups.

Group name	Members
AdminRole	- swrbaadmin - swrbasch
IflowUsers	- swrbaadmin - swrbasch
IflowGroups	- AdminRole - swrba_Exe - Role - IFlowPublishers
swrba_Exe	- swrbaadmin
Role	- swrbaadmin
IFlowPublishers	- swrbaadmin

Note

. . . .

Not attach user except of *swrbaadmin* in swrba_Exe group.

If you attach except of swrbaadmin user, it may occur error on Automated Operation Process

. . . .

Follow the steps below to register groups and add users.

1. Create an LDIF file.

   In the following specification example, the default user IDs and passwords listed in the table above are specified as the user IDs and passwords.

   Specification example

   ```
   dn: cn=AdminRole,ou=%GROUP%,%DOMAIN%
   changetype: add
   objectClass: groupOfNames
   objectClass: top
   cn: AdminRole
   member: uid=swrbaadmin,ou=%USER%,%DOMAIN%
   member: uid=swrbasch,ou=%USER%,%DOMAIN%

   dn: cn=IflowUsers,ou=%GROUP%,%DOMAIN%
   changetype: add
   objectClass: groupOfNames
   objectClass: top
   cn: IflowUsers
   member: uid=swrbaadmin,ou=%USER%,%DOMAIN%
   member: uid=swrbasch,ou=%USER%,%DOMAIN%

   dn: cn=IflowGroups,ou=%GROUP%,%DOMAIN%
   changetype: add
   objectClass: groupOfNames
   objectClass: top
   cn: IflowGroups
   member: cn=AdminRole,ou=%GROUP%,%DOMAIN%
   member: cn=swrba_Exe,ou=%GROUP%,%DOMAIN%
   member: cn=Role,ou=%GROUP%,%DOMAIN%
   member: cn=IFlowPublishers,ou=%GROUP%,%DOMAIN%

   dn: cn=swrba_Exe,ou=%GROUP%,%DOMAIN%
   changetype: add
   objectClass: groupOfNames
   objectClass: top
   cn: swrba_Exe
   member: uid=swrbaadmin ,ou=%USER%,%DOMAIN%

   dn: cn=Role,ou=%GROUP%,%DOMAIN%
   changetype: add
   objectClass: groupOfNames
   objectClass: top
   cn: Role
   member: uid=swrbaadmin ,ou=%USER%,%DOMAIN%

   dn: cn= IFlowPublishers,ou=%GROUP%,%DOMAIN%
   changetype: add
   objectClass: groupOfNames
   objectClass: top
   cn: IFlowPublishers
   member: uid=swrbaadmin ,ou=%USER%,%DOMAIN%
   ```

   Note that the %...% parts of the file should be replaced with the elements in the list below.

   List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	*<Public directory>* (Example) ou=interstage,o=fujitsu,dc=com Note: To execute the setup after creating an LDAP directory, this setting must be specified for the LDAP key name when the setup is executed.
%USER%	The "User" organizational unit (OU) (If the name of the OU created in "Creating an organizational unit (OU)" has been changed, specify the new name.) (Example) User Note: To execute the setup after creating an LDAP directory, ou=*<%USER% setting>* must be specified in the organizational unit settings for storing LDAP user accounts when the setup is executed.
%GROUP%	The "Group" organizational unit (OU) (If the name of the OU created in "Creating an organizational unit (OU)" has been changed, specify the new name.) (Example) Group Note: To execute the setup after creating an LDAP directory, ou=*<%GROUP% setting>* must be specified in the LDAP organization unit settings when the setup is executed.

2. Register the groups and users on OpenLDAP:
   Execute the following command to register the organizational unit (OU), groups and users on OpenLDAP.

   ```
   ldapadd -x -W -D "cn=<LDAP administrator>,<Public directory>" -f <LDIF file created>
   ```

   Note: The user will be prompted for the LDAP administrator password.

3.1.7 Setting up Systemwalker Runbook Automation [Windows]

Set up Systemwalker Runbook Automation.

1. Log in to the Management Server as a user with administrator privileges.

2. Start the setup:

   ```
   <Installation directory for the Systemwalker Runbook Automation Management Server>\bin
   \swrba_setup -s
   ```

Note

If the operating system being used is Windows Server 2008, execute the command above as an administrator.

3. The Systemwalker Runbook Automation Setup Tool will start.

   Check the settings displayed, and then click the **Next** button.
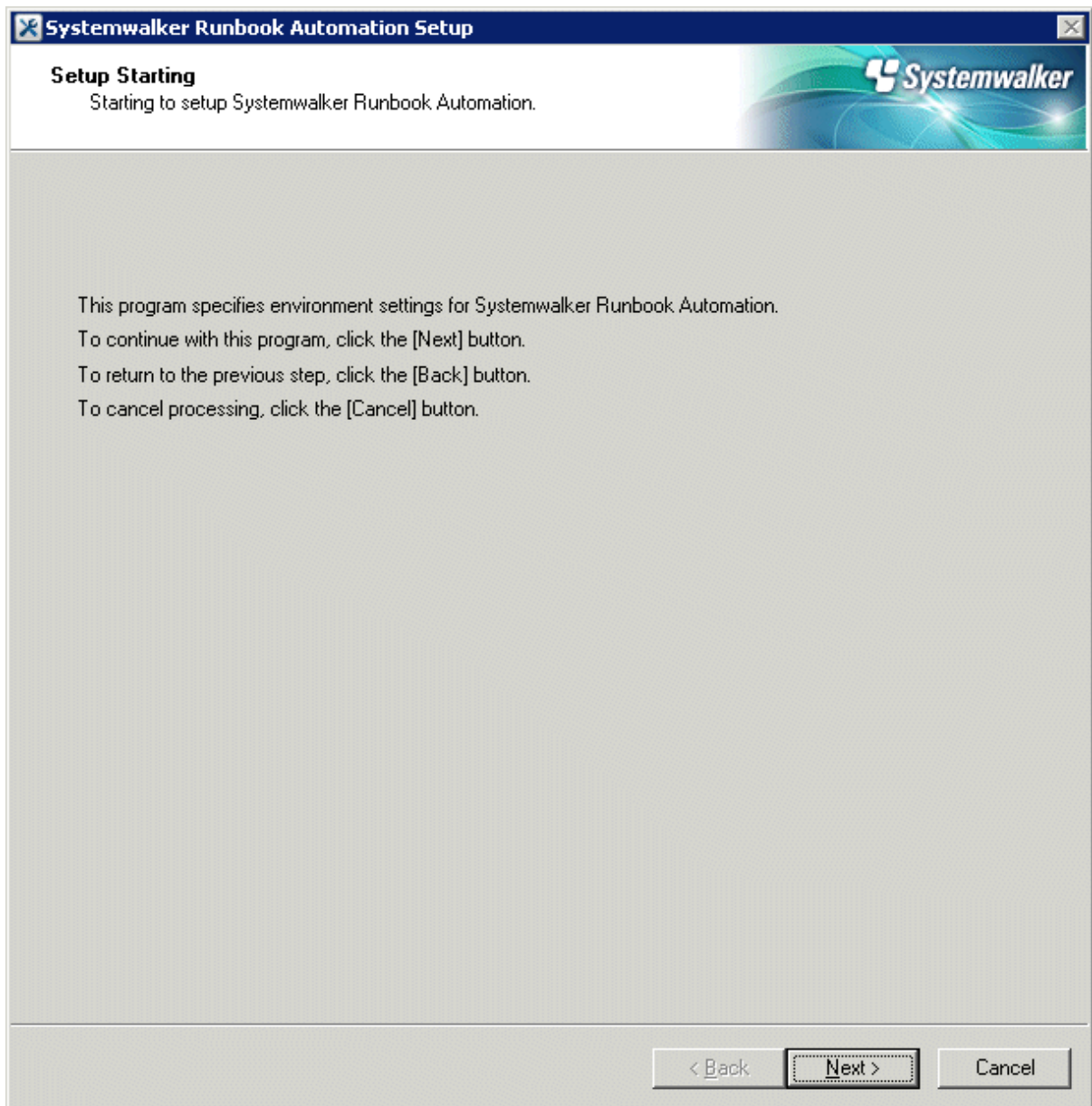
4. Specify the server type settings.

   Enter each setting, and then click the **Next** button.

Item name		Input value
Select the build server type:		Select the operating type of the Management Server from the following options: - **Standalone Server (Normal operations)** - **Standalone Server (Cluster operations - primary node)** - **Standalone Server (Cluster operations - secondary node)**
High-Reliability Environment Settings	**Inherit File Storage Directory**	Specify this parameter if "**Cluster operations**" has been specified in **Select the build server type**. Specify the directory that will store the files for inheriting information about the Management Server when a failover

Item name	Input value
	occurs. Specify the absolute path to a directory on the shared disk that can be accessed by both the primary node and the secondary node. The value can contain up to 100 characters, but cannot contain spaces.
Primary Node Host Name	Specify this parameter for the server type that is to be built, when a cluster operation has been specified. Specify the host name for the primary node physical IP address.
Secondary Node Host Name	Specify this parameter for the build server type, when a cluster operation has been specified. Specify the host name for the secondary node physical IP address.

5. Set up the Process Management Database.

   Enter each setting, and then click the **Next** button.

Item name	Input value
Port number for Process Management Database	Specify the port number for accessing the Process Management Database.
Process Management Database Storage Directory	Specify the directory for storing the database. The value can be up to 100 characters long. Not specify path beginning with \\ string or absolute path. In this specified directory, It is necessary to add readable and writable authority to User Group
Account for Process Management Database	Register a new account, which will be required for Systemwalker Runbook Automation to access the Process Management Database. The value can contain up to 18 initial alphanumeric characters. Note that the value specified for this item is required to directly manipulate the Process Management Database.
Account Password for Process Management Database	Specify the password for the account for accessing the Process Management Database. The value can contain up to 18 alphanumeric characters and symbols (*). Note that the value specified for this item is required to directly manipulate the Process Management Database. (*) The following symbols can be used: !#%=~:,_
Re-enter Password	Re-enter the password for the account for accessing the Process Management Database.

6. Set up the environment for the authentication server.

   Enter each setting, and then click the **Next** button.

Item name	Input value

The authentication server type to be used	Select the type of the authentication server to be used from the following options:
	
	  - Authentication server for Interstage Single Sign-On
	
	  - ServerView Operations Manager Single Sign-On Authentication Server
	
	  - LDAP server

LDAP Used	Select the LDAP to be used, depending on the authentication server type. Interstage Single Sign-On Authentication Server - Interstage Directory Service

Item name	Input value
	ServerView Operations Manager Single Sign-On Authentication Server - OpenDS - Active Directory LDAP server - Interstage Directory Service - Active Directory - OpenLDAP
Interstage Single Sign-on Environment Settings **Business System Name**	If "Authentication server for Interstage Single Sign-On" has been selected as the authentication server type, specify the name of the Business System. If an Interstage Single Sign-On environment has been created in accordance with the procedure in "Interstage Single Sign-On Build and Settings", specify "Business001". Default value: Business001

7. Set up the environment for user authentication.

Enter each setting, and then click the **Next** button.

Item name	Input value
Host Name or IP address	Specify the host name or IP address for the LDAP server. The value can contain up to 64 characters.
Port Number	Specify the port number for the LDAP server. The value must be between 1 and 65535. Default: 389
Key Name	Set up the public directory using the following format: default: ou=interstage,o=fujitsu,dc=com The value can contain up to 255 characters.

Item name	Input value
	🛈 **Note**
	Separate public directory levels with commas(,).
	Example: If the public directory is ou=interstage,o=fujitsu,dc=com itcm.com, specify ou=interstage,o=fujitsu,dc=com
Organizational Unit	Specify the name of the organizational unit using the following format: ou=<*Name of the organizational unit*> The value can contain up to 255 characters.
	Default: ou=Group
Account Storage Unit	Specify the name of the account storage unit using the following format: ou=<*Name of the account storage unit*> The value can contain up to 255 characters.
	Default: ou=User
Administrator DN	- Specify the distinguished name (DN) for the administrator of the LDAP repository using the following format:
	- cn=<*Administrator DN*>
	- This item can be entered if OpenLDAP or the Interstage Directory Service has been specified for the LDAP directory.
	Default: cn=manager
	Note: If only the name is specified, the public directory will be added automatically.
Password for Administrator DN	Specify the password for the LDAP repository administrator. Note that $, \, ", and spaces cannot be used.

🛈 **Note**

To click the **Next** button, Confirm authentication to LDAP Server.

Failed to confirm authentication to LDAP Server, Review the setting value with displayed error messages.

8. Specify user information.

   Enter each setting, and then click the **Next** button.

Item name	Input value
User for Process Control	Specify the user required for Systemwalker Runbook Automation to control processes.
	The recommend value is "swrbaadmin", but any value can be specified. This user must have been registered in the LDAP directory.
Password for the User for Process Control	Specify the password for the user for process control. Note that $, \, ", and spaces cannot be used.
User for Schedule Startup	Specify the user required by Systemwalker Runbook Automation to start automated operation process according to a schedule. swrbasch is the recommended value, however anything can be specified for this. This user must be registered in the LDAP.

Item name	Input value
Password of User for Schedule Startup	Specify the password of the user for schedule startup. Note that $, \, ", and spaces cannot be used.

Note

. . . .

To click the **Next** button, Confirm authentication to LDAP Server.

Failed to confirm authentication to LDAP Server, Review the setting value with displayed error messages.

And confirm as below.

- Because there may be error on setting LDAP Server, get back to previous window, and confirm if the information is set normally or not.

- Confirm if user information registered on LDAP server and group information are correct or not.

. . . .

9. Set up an environment for the SMTP server.

To send email notifications when tasks are allocated as part of Automated Operation Process operations, information for the SMTP server must be registered on the Management Server. Enter each setting, and then click the **Next** button.

Item name	Input value
Host Name or IP Address	Specify the host name or IP address for the SMTP server for sending emails. - Up to 255 characters can be specified, including alphanumeric characters, periods (".") and hyphens ("-"). - Default value: localhost
Port Number	Specify the port number for the SMTP server for sending emails. Default value: 25
SMTP server user name	Specify the name of the user that is used to authenticate with the SMTP server when emails are sent.

Item name	Input value
	Do not specify a value if authentication with the SMTP server is not performed when emails are sent.
SMTP server user password	Specify the password of the user that is used to authenticate with the SMTP server when emails are sent.
	Do not specify a value if authentication with the SMTP server is not performed when emails are sent.
Mail sender	Specify the sender (the "from" address) that will be assigned to the emails that are sent, using email address format.
	Note that this address will be used as the address for receiving error emails when the notification emails that are sent bounce because the recipient cannot be found. Specify the email address of someone who can respond to problems promptly.
Web console URL host name	Specify the host name of the Management Server, which will be embedded into the URL for the Web console. The host name specified here (in the following format) will be used in the URL that appears in the message text when email notifications are sent:
	- http://<*host name of the Management Server*>:<*port number for the Management Server (Web server)*>/console/
	Be sure to specify a URL that can be accessed by mail recipients. In particular, in environments that use single sign-on, be sure to specify the host name in FQDN format.

Information

. . . .

- The email sender and the host name for the Web console URL cannot be omitted. If the design of the SMTP server is not complete, enter provisional values for the mail sender and the host name for the Web console URL and then continue on. In this case, change the provisional values to the correct values when email notifications are used, by referring to "Changing the Mail Server Information Registered on the Management Server".

- Refer to "Setting Up Mail Notification" in the *Systemwalker Runbook Automation Operation Guide* for information on email notification.

. . . .

10. Configure the port number to be used by Systemwalker Runbook Automation.

Enter relevant values, and click **Next**.

Item name	Input value
Port Number for Message broker	Specify the port number required by Systemwalker Runbook Automation to use the Java EE feature.
Port Number for Server Function	Specify the port number required to run the Systemwalker Runbook Automation server feature.

11. The settings will be displayed.

Check the displayed values are correct, and then click the **Next** button. The setup will commence.
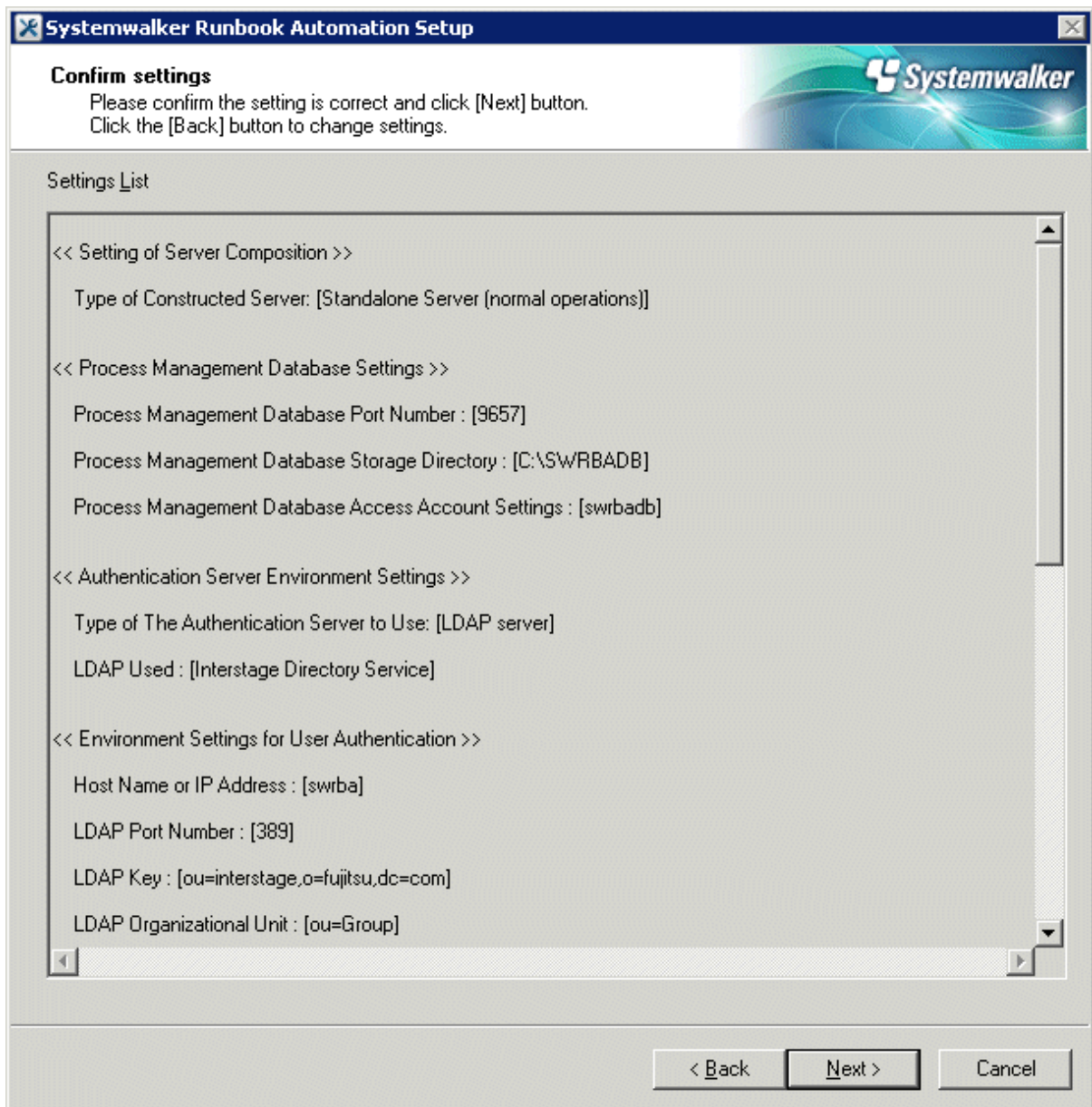
12. A window will be displayed indicating the setup progress.
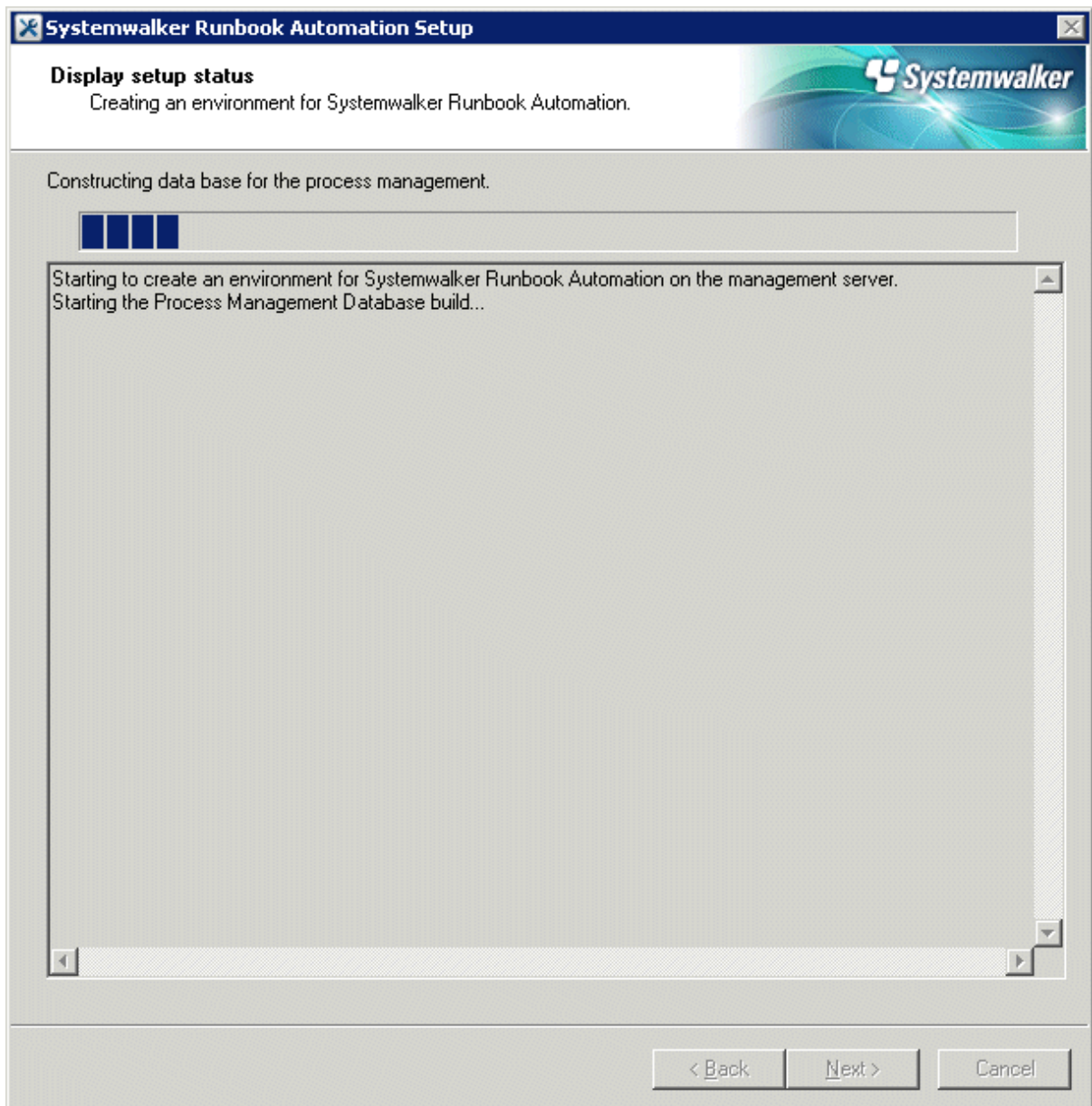
13. If the setup completes normally, the settings will be displayed. Check the settings that are displayed, and then click the **Finish** button.
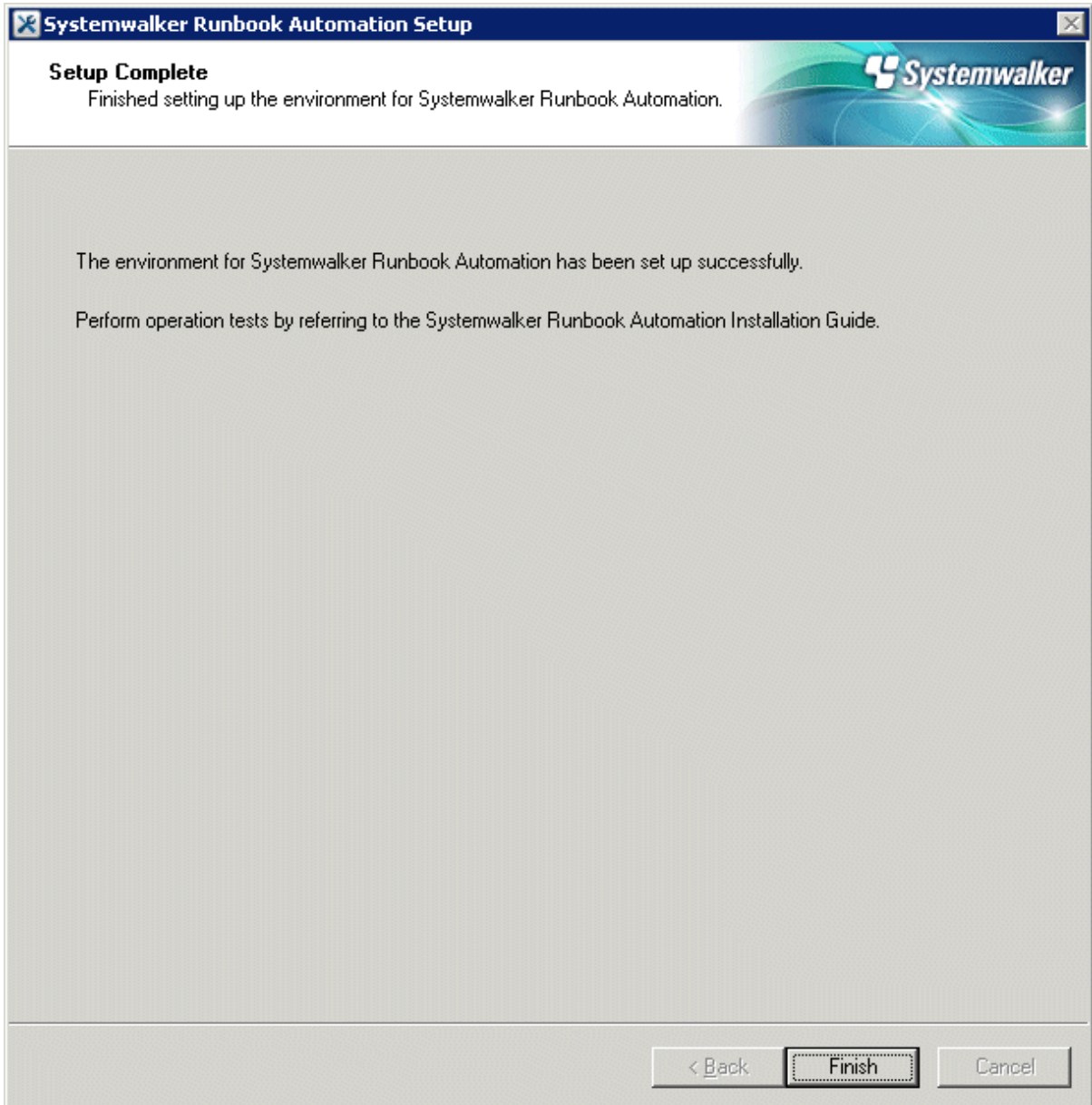
Note

If the setup fails for any reason, be sure to cancel the setup.

3.1.8 Setting up Systemwalker Runbook Automation [Linux]

Set up Systemwalker Runbook Automation.

Information

Input [!!] after ENTER==> to stop, except entering password and confirming setting up information. Setting up command is abort

---

1. Log in to the Management Server as a superuser.

2. Start Systemwalker Runbook Automation setup:

```
# /opt/FJSVswrbam/bin/swrba_setup -s
```

3. A message will be displayed indicating that the setup is about to start.

```
================================================================================
        Systemwalker Runbook Automation Setup Tool
                               V15.1.0
                               Copyright FUJITSU LIMITED 2010-2011
================================================================================
Starting to set up Systemwalker Runbook Automation.
Please input [!!] after ENTER==> to stop the setup
```

4. Specify the full path of the Process Management Database directory.

After "ENTER==>" will be displayed, input specified directory within 100-byte absolute path.

Specify directory name with one byte alphameric characters. Not specify it with relative path.

If only enter key is input, set default value "/var/opt/FJSVswrbam/SWRBADB".

```
 [Settings for the Process Management Database directory]
Specify the Process Management Database directory.
              * The Valid value can contain up to 100 characters.
The default will be used if no value is specified.
( default : /var/opt/FJSVswrbam/SWRBADB )
ENTER==>
```

5. Enter the port number that the Process Management Database will use.

```
[Settings for the communication port for Process Management Database]
Enter the port number used by the Process Management Database.
The default will be used if no value is specified.
( default : 9657 )
ENTER==>
```

6. Enter the account name and password for accessing the Process Management Database.

```
[Enter the account for accessing the Process Management Database]
Register a new account, which will be required for Systemwalker Runbook Automation to access the
Process Management Database.
The value can contain up to 18 alphanumeric characters.
The default will be used if no value is specified.
( default : swrbadb )
ENTER==>
[Enter the account password]
The value can contain up to 18 alphanumeric characters, spaces and symbols (!#%=~:).
Registers the account using the specified password.
ENTER==>
Re-enter the password.
ENTER==>
```

7. Select which type of authentication server the Management Server will use.

```
[Authentication server type settings]
Select the type of the authentication server to be used.
1. Interstage Single Sign-On Authentication Server
2. LDAP server
3. ServerView Operations Manager Single Sign-On Authentication Server
The default will be used if no value is specified.
( default : 1 )
ENTER==>
```

8. Enter the business system name that has been specified for the Interstage Single Sign-On Agent.

   If an Interstage Single Sign-On Authentication Server has been selected as the authentication server, a window for specifying the business system name that has been specified for the Interstage Single Sign-On Agent will be displayed.

   If Interstage Single Sign-On is built in 3.1.3 Interstage Single Sign-On Build and Settings Specify Business001.

```
 [Enter business system name]
Enter the business system name that has been specified for the Interstage Single Sign-On Agent.
The default will be used if no value is specified.
( default : Business001 )
ENTER==>
```

9. Specify the type of LDAP directory to be used.

   If an Interstage Single Sign-On Authentication Server or ServerView Operations Manager Single Sign-On Authentication Server has been selected as the authentication server, the type of LDAP directory to be used by the Single Sign-On Authentication Server must be specified for the authentication server.

   In case of selecting Interstage Single Sign-On as Authentication Server,

```
[Settings for the LDAP directory to use]
Select the LDAP to be used.
1. Interstage Directory Service
If Enter is pressed, the default value will be used.
( default : 1 )
ENTER==>
```

   In case of selecting ServerView Operations Manager Single Sign-On as Authentication Server,

```
[Settings for the LDAP used]
Select the LDAP that is used:
1. OpenDS
2. Active Directory
If Enter is pressed, the default value will be used.
( default : 1 )
ENTER==>
```

   In case of selecting LDAP Server as Authentication Server,

```
[Settings for the LDAP directory to use]
Select the LDAP to be used.
1. Interstage Directory Service
2. Active Directory
3. OpenLDAP
If Enter is pressed, the default value will be used.
( default : 1 )
ENTER==>
```

10. Specify the host name or IP address for the LDAP directory.

```
 [Settings for the host name]
Enter the LDAP server host name or ip address.
ENTER==>
```

11. Specify the port number for the LDAP directory.

```
[Settings for the port]
Enter the LDAP port number.
The default will be used if no value is specified.
( default : 389 )
ENTER==>
```

12. Specify the key name for the LDAP directory.

```
 [Settings for the key]
Enter a public directory.
If Enter is pressed, the default value will be used.
( default : ou=interstage,o=fujitsu,dc=com )
ENTER==>
```

13. Specify the organizational unit name for the LDAP directory.

```
 [Settings for the organizational unit]
Enter the organizational unit name.
(format : ou=<Name of the organizational unit>)
Example: If the organizational unit name is Group, [ou=Group]
The default will be used if no value is specified.
( default : ou=Group )
ENTER==>
```

14. Specify the account storage unit name for the LDAP directory.

```
 [Settings for the account storage unit]
Enter the account storage unit name.
(format: ou=account storage unit name)
Example: If the account storage unit name is User, [ou=User]
The default will be used if no value is specified.
( default : ou=User )
ENTER==>
```

15. Specify the administrator DN for the LDAP directory.

   This item is displayed if the Interstage Directory Service or OpenLDAP has been specified as the LDAP directory.

```
[Enter administrator DN]
Enter the administrator DN.
Example: cn=manager,ou=interstage,o=fujitsu,dc=com
The default will be used if no value is specified.
( default : cn=manager,ou=interstage,o=fujitsu,dc=com )
ENTER==>
```

16. Enter the password for the LDAP administrator DN.

   This item is displayed if the Interstage Directory Service or OpenLDAP has been specified as the LDAP directory. Note that $, \, ", and spaces cannot be used.

```
[Enter password for administrator DN]
Enter the password for the administrator DN.
ENTER==>
```

17. The system will then check with the LDAP server whether the administrator DN exists.

```
Checking LDAP server authentication...
```

   If LDAP server authentication has been confirmed normally, the following message will be displayed.

```
LDAP server authentication has completed.
```

   If LDAP server authentication has not been confirmed, the following message will be displayed.

```
LDAP server authentication could not be checked.
```

   Re-enter the user name and password for the administrator DN.

   If authentication has failed because the LDAP information is incorrect, enter "*" to change the information on the LDAP server.

```
 [Enter administrator DN ]
Enter the administrator DN.
```

```
format)cn=manager,ou=interstage,o=fujitsu,dc=com
If Enter is pressed, the default value will be used.
Or enter "*" to change the information on the LDAP server.
( default : cn=manager,ou=interstage,o=fujitsu,dc=com )
ENTER==>
[Enter password for administrator DN ]
Enter the password for the administrator DN.
ENTER==>
```

If administrator DN and password are not incorrect, Review them with the following viewpoint.

- Confirm if the connection information is correct.

- Confirm if the LDAP server has been started.

- Review user and group definition information registered on LDAP are correct.

- Confirm if the network to LDAP is down,

18. Enter the account name for the user for process control that has been registered with the LDAP directory.

```
 [Enter the user for process control]
Enter the account name for the user for process control.
The default will be used if no value is specified.
( default : swrbaadmin )
ENTER==>
```

19. Enter the password for the user for process control. Note that $, \, ", and spaces cannot be used.

```
[Enter password for the user for process control]
Enter the password for the user for process control.
ENTER==>
```

20. The system will then check with the LDAP server whether the user for process control exists.

```
Checking LDAP server authentication...
```

If LDAP server authentication has been confirmed normally, the following message will be displayed.

```
LDAP server authentication has completed.
```

If LDAP server authentication has not been confirmed, the following message will be displayed.

```
LDAP server authentication could not be checked.
```

Re-enter the user name and password for the user for process control.

If authentication has failed because the LDAP information is incorrect, enter "*" to change the information on the LDAP server.

```
[Enter the user for process control]
Enter the user for process control.
If Enter is pressed, the default value will be used.
Or enter "*" to change the information on the LDAP server.
 ( default : swrbaadmin )
ENTER==>
[Enter password for the user for process control]
Enter the password for the user for process control.
ENTER==>
```

If the user and password for process control are not incorrect, Review them with the following viewpoint.

- Confirm if the connection information is correct.

- Confirm if the LDAP server has been started.

- Review user and group definition information registered on LDAP are correct.

- Confirm if the network to LDAP is down,

21. Enter the account name for the user for schedule start that has been registered with the LDAP directory.

```
 [Enter the user for schedule start]
Enter the account name for the schedule start.
The default will be used if no value is specified.
( default : swrbasch )
ENTER==>
```

22. Enter the password for the user for schedule . Note that $, \, ", and spaces cannot be used.

```
[Enter password for the user for process control]
Enter the password for the user for process control.
ENTER==>
```

23. The system will then check with the LDAP server whether the user for process control exists.

```
Checking LDAP server authentication...
```

If LDAP server authentication has been confirmed normally, the following message will be displayed.

```
LDAP server authentication has completed.
```

If LDAP server authentication has not been confirmed, the following message will be displayed.

```
LDAP server authentication could not be checked.
```

Re-enter the user name and password for the user for process control.

If authentication has failed because the LDAP information is incorrect, enter "*" to change the information on the LDAP server.

```
[Enter the user for process control]
Enter the user for process control.
If Enter is pressed, the default value will be used.
Or enter "*" to change the information on the LDAP server.
 ( default : swrbaadmin )
ENTER==>
[Enter password for the user for process control]
Enter the password for the user for process control.
ENTER==>
```

If the user and password for process control are not incorrect, Review them with the following viewpoint.

- Confirm if the connection information is correct.

- Confirm if the LDAP server has been started.

- Review user and group definition information registered on LDAP are correct.

- Confirm if the network to LDAP is down,

24. Set either the host name or IP address of the SMTP server.

Specify the host name or IP address for the SMTP server for sending emails.

Up to 255 characters can be specified, including alphanumeric characters, periods (".") and hyphens ("-").

```
[SMTP server host name settings]
Enter the SMTP server host name or IP address.
If Enter is pressed, the default value will be used.
( default : localhost )
ENTER==>
```

 Note
....

- The email sender and the host name for the Web console URL cannot be omitted. If the design of the SMTP server is not complete, enter provisional values for the mail sender and the host name for the Web console URL. If provisional values have

been entered, change the provisional values to the correct values when email notifications are used, by referring to "8.4.1 Changing the Mail Server Information Registered on the Management Server".

- Refer to "Setting Up Mail Notification" in the *Systemwalker Runbook Automation Operation Guide* for information on email notification.

- -

25. Specify the port number for the SMTP server.

    Specify the port number for the SMTP server for sending emails.

```
[SMTP server port settings]
Enter the SMTP server port number.
If Enter is pressed, the default value will be used.
( default : 25 )
ENTER==>
```

26. Enter the user name for the SMTP server.

    Specify the name of the user that is used to authenticate with the SMTP server when emails are sent.

    Do not specify a value if authentication with the SMTP server is not performed when emails are sent.

```
[Enter SMTP server user name]
Enter the SMTP server user name.
If only the Enter key is pressed, the value will not be set.
ENTER==>
```

27. Enter the password of the user for the SMTP server. Note that $, \, ", and spaces cannot be used.

    This input item is displayed when the SMTP server user name has been specified.

    Specify the password of the user that is used to authenticate with the SMTP server when emails are sent.

```
[Enter SMTP server user password]
Enter the SMTP server user password.
If only the Enter key is pressed, the value will not be set.
ENTER==>
```

28. Enter the sender for emails.

    Specify the sender (the "from" address) that will be assigned to the emails that are sent, using email address format. Note that this address will be used as the address for receiving error emails when the notification emails that are sent bounce because the recipient cannot be found. Specify the email address of someone who can respond to problems promptly.

```
[Enter mail sender]
Enter the mail sender.
ENTER==>
```

29. Specify the host name of the Management Server, which will be embedded into the URL for the Web console. The host name specified here will be used (in the following format) in the URL that appears in the message text when email notifications are sent.

    - http://*<host name of the Management Server>*:*<port number for the Management Server (Web server)>*/console/

    Be sure to specify a URL that can be accessed by mail recipients. In particular, in environments that use single sign-on, be sure to specify the host name in FQDN format.

```
[Enter Web console URL host name]
Enter the Web console URL host name.
ENTER==>
```

30. Type the message broker port number.

    Specify the port number required by Systemwalker Runbook Automation to use the Java EE feature.

```
[ Message Broker Port Settings ]
Enter the message broker port number.
If only the <Enter> key is pressed, the setting will be made using the default value.
```

```
( default : 7676 )
ENTER==>
```

31. Type the port number used by the server feature.

Specify the port number required to run the Systemwalker Runbook Automation server feature.

```
[ Port number used for the server feature ]
Enter the port number used by the server feature.
If only the <Enter> key is pressed, the setting will be made using the default value.
( default : 23700 )
ENTER==>
```

32. Check the setup information.

Check the information entered in the settings window, and then enter "y" to start the setup processing.
If "n" is entered, the setup processing will be terminated and the display will return to the prompt.
If "r" is entered, the setup processing will be executed again from step 3.

```
[Confirm setup information]
Check the specified values.
================================================================
Systemwalker Runbook Automation operation model
Process Management Database directory      : /var/opt/FJSVswrbam/SWRBADB
Port number for Process Management Database : 9657
Account for Process Management Database     : swrbadb
Authentication server configuration         : LDAP server
Business system name                        : Business001
LDAP Used                                          : Interstage Directory Service
Business system name                               : Business001
LDAP Host Name                                     : swrba
LDAP Port                                          : 389
LDAP public directory                       : ou=interstage,o=fujitsu,dc=com
LDAP organizational unit name                   : ou=Group
LDAP account storage unit name                  : ou=User
LDAP administrator DN                       : cn=manager,ou=interstage,o=fujitsu,dc=com
Account for the user for process control    : swrbaadmin
Account for the user for schedule startup        : swrbasch
SMTP server host name                            : swrba.mail.server
Port number of SMTP                              : 25
SMTP server user name                           : swrbamailuser
Mail sender                                 : swrbamailuser@swrba.mail.server
Web console URL host name                   : ssoserver.example.com
Port number of the message broker               : 7676
Port number of Server function                  : 23700
 ================================================================
OK? [y: Start/n: Cancel/r: Repair]
ENTER==>
```

33. The setup will start.

Messages about the setup processing will be displayed, with a message indicating the completion of the setup being displayed at the end.

```
Starting to create an environment for Systemwalker Runbook Automation on the management server.
Starting the Process Management Database build... (This may take a few minutes.)
Creating the Process Management Database has completed.
Starting to set up the environment for Systemwalker Runbook Automation.
Setting up the environment for Systemwalker Runbook Automation has completed.
Setting up the environment for CMDB. (This may take a few minutes.)
CMDB environment setup has completed.
Creating an environment for Systemwalker Runbook Automation on the management server has
completed.
```

Note

⋯⋯⋯

If an error occurs during the Systemwalker Runbook Automation setup process, check the following items.

- If the setup processing terminates abnormally, execute the processing for canceling the setup, and then execute the setup processing again.

- If the setup processing terminates abnormally and then the processing for canceling the setup also produces an error, restart the system. If the error still persists, contact Fujitsu technical support.

⋯⋯⋯

3.1.9 Settings for Automatically Collecting Configuration Information

To collect configuration information automatically, specify the following settings on the Management Server.

To collect IT resource information, specify settings on the Business Server in advance.

Refer to *Settings up Business Server* for details.

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the collection processing as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

3.1.9.1 Setup procedure (when collecting IT resource information)

[Windows]

1. If Systemwalker Runbook Automation is running, then stop it:

   > *<Installation directory for the Systemwalker Runbook Automation Management Server>*\bin
   > \swrba_stop

2. Modify the IT resource information collection configuration file.

   To perform node discovery from a subnet other than the subnet where Management Servers are located, modify the file (for details, refer to "3.1.9.4 How to modify the IT resource information collection configuration file").

3. Set up the environment:

   > "%SWCMDB_INSTALL_PATH%\ FJSVcmdbm\bin\cmdbsetupenv.bat" -k AGT_INV

4. Modify the Definition File for Collection of Configuration Information

   In agent with setting up, it collects information at the following time everyday as a default.

   `4.30am`

   Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

   Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

   > `AGT_INV 30 4 * * *`

5. Start Systemwalker Runbook Automation:

   > *<Installation directory for the Systemwalker Runbook Automation Management Server>*\bin
   > \swrba_start

6. Automatically collect IT resource information:

```
"%SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\cmdbrefresh.exe" -q type=AGT_INV
```

As a result of this command, the nodes connected to the network will be detected automatically, and the information collected will be registered with the CMDB Manager.

7. Register authentication information on Business Server.

From Business Server which not installed agent package for Business Server, to collect logical server, hardware information, installed software information, as IT resource information, To be need to register authentication information for SSH communication on CMDB

Refer to the 3.1.9.6 Registering authentication information (when collecting IT resource information) .

📘 Point
. . . .

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the event log to check when the collection processing completes.

- FCMDB: INFO: [10004] Update check processing has started. '<Agent service type>'

- FCMDB: INFO: [10005] Update check processing has completed. '<Agent service type>'

. . . .

[Linux]

1. If Systemwalker Runbook Automation is running, then stop it by issuing the command below:

```
/opt/FJSVswrbam/bin/swrba_stop
```

2. Modify the IT resource information collection configuration file.

To perform node discovery from a subnet other than the subnet where Management Servers are located, modify the file (for details, refer to "3.1.9.4 How to modify the IT resource information collection configuration file").

3. Set up the environment:

```
/opt/FJSVcmdbm/bin/cmdbsetupenv.sh -k AGT_INV
```

4. Modify the Definition File for Collection of Configuration Information

In agent with setting up, it collects information at the following time everyday as a default.

```
4.30am
```

Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

```
AGT_INV 30 4 * * *
```

5. Start Systemwalker Runbook Automation

```
/opt/FJSVswrbam/bin/swrba_start
```

6. Automatically collect IT resource information:

```
/opt/FJSVcmdbm/bin/cmdbrefresh.sh -q type=AGT_INV
```

As a result of this command, the nodes connected to the network will be detected automatically, and the information collected will be registered with the CMDB Manager.

7. Register authentication information on Business Server.

   From Business Server which not installed agent package for Business Server, to collect logical server, hardware information, installed software information, as IT resource information, To be need to register authentication information for SSH communication on CMDB

   Refer to the *Registering authentication information(when collecting IT resource information)* .

    Point
   ....
   Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the syslog to check when the collection processing completes.

   - FCMDB: INFO: [10004] Update check processing has started. 'Agent service name'

   - FCMDB: INFO: [10005] Update check processing has completed. 'Agent service name'
   ....

3.1.9.2 Setup procedure (when collecting only node information)

[Windows]

1. If Systemwalker Runbook Automation is running, then stop it:

   > *<Installation directory for the Systemwalker Runbook Automation Management Server>*\bin
   > \swrba_stop

2. Modify the agent linkage configuration file.

   To perform node discovery from a subnet other than the subnet where Management Servers are located, modify the file (for details, refer to "3.1.9.5 How to modify the agent linkage configuration file").

3. Set up the environment:

   > "%SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\cmdbsetupenv.bat" -k AGT_ADSC

4. Modify the Definition File for Collection of Configuration Information

   In agent with setting up, it collects information at the following time everyday as a default.

   `4.30am`

   Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

   Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

   ```
   AGT_ADSC 45 4 * * *
   ```

5. Start Systemwalker Runbook Automation:

   > *<Installation directory for the Systemwalker Runbook Automation Management Server>*\bin
   > \swrba_start

6. :Update the observed records managed by the CMDB

   > "*<Installation directory for the Systemwalker Runbook Automation Management Server>*\CMDB
   > \FJSVcmdbm\bin\cmdbrefresh.exe" -q type=AGT_ADSC

   As a result of this command, the information collected will be registered with the CMDB Manager.

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the event log to check when the collection processing completes.

- FCMDB: INFO: [10004] Update check processing has started. '<Agent service type>'

- FCMDB: INFO: [10005] Update check processing has completed. '<Agent service type>'

・・

[Linux]

1. If Systemwalker Runbook Automation is running, then stop it:

   ```
   /opt/FJSVswrbam/bin/swrba_stop
   ```

2. Modify the agent linkage configuration file.

   To perform node discovery from a subnet other than the subnet where Management Servers are located, modify the file (for details, refer to "3.1.9.5 How to modify the agent linkage configuration file").

3. Set up the environment:

   ```
   /opt/FJSVcmdbm/bin/cmdbsetupenv.sh -k AGT_ADSC
   ```

4. Modify the Definition File for Collection of Configuration Information

   In agent with setting up, it collects information at the following time everyday as a default.

   ```
   4.30am
   ```

   Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

   Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

   ```
   AGT_ADSC 45 4 * * *
   ```

5. Start Systemwalker Runbook Automation

   ```
   /opt/FJSVswrbam/bin/swrba_start
   ```

6. Update the observed records managed by the CMDB:

   ```
   /opt/FJSVcmdbm/bin/cmdbrefresh.sh -q type=AGT_ADSC
   ```

   As a result of this command, the information collected will be registered with the CMDB Manager.

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the messages in the syslog to check when the collection processing completes.

・・

3.1.9.3 Setup procedure(When using the "Register logical node" operation component)

Perform this setup procedure when using the "Register logical node" operation component. Also, be sure to perform this setup procedure when using the "Deploying systems and registering them in CMDB" or "Changing systems and registering them in CMDB" template, which are operation templates for virtual environments that use the "Register logical node" operation component.

For information on the "Register logical node" operation component, refer to the *Systemwalker Runbook Automation Reference Guide*. For information on the "Deploying systems and registering them in CMDB" or "Changing systems and registering them in CMDB" template, refer to the *Systemwalker Runbook Automation Template Operator's Guide*.

[Windows]

1. When the Systemwalker Runbook Automation has been started, execute the following command and stop it

```
[Systemwalker Runbook Automation Install directory of Management Server \bin\swrba_stop
```

2. Execute the following setting environment command

```
"%SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\cmdbsetupenv.bat" -k AGT_INVIP
```

3. Execute the following command, start Systemwalker Runbook Automation

```
[Systemwalker Runbook Automation Install directory of Management Server]\bin\swrba_start
```

4. Register certification information of Business server

If you correct logical server information, hardware information, and installed software information such as a IT resource information from business server where it has not been installed agent package for Business server, you will need to register certification information to connect by SSH in CMDB.

Refer to the "3.1.9.6 Registering authentication information (when collecting IT resource information)" and register it.

[Linux]

1. When the Systemwalker Runbook Automation has been started, execute the following command and stop it

```
/opt/FJSVswrbam/bin/swrba_stop
```

2. Execute the following setting environment command.

```
/opt/FJSVcmdbm/bin/cmdbsetupenv.sh -k AGT_INVIP
```

3. Execute the following command, start Systemwalker Runbook Automation

```
/opt/FJSVswrbam/bin/swrba_start
```

4. Register certification information of Business server

If you correct logical server information, hardware information, and installed software information such as a IT resource information from business server where it has not been installed agent package for Business server, you will need to register certification information to connect by SSH in CMDB.

Refer to the "3.1.9.6 Registering authentication information (when collecting IT resource information)" and register it.

3.1.9.4 How to modify the IT resource information collection configuration file

This section describes how to specify the subnets for which IT resource information is to be collected.

1. IT resource information collection configuration file

Windows	- For Management Servers - *<CMDB Manager directory>*\CMDB\FJSVcmdba\etc\mdr_inv.properties - For Relay Servers - *<Agent installation directory>*\CMDB\FJSVcmdba\etc\mdr_inv.properties
Linux	/opt/FJSVcmdba/etc/mdr_inv.properties

2. Edit "mdr_inv. properties" with using editor.

Entry	Description
<Group name>.mdbad.inventory.network.address	- Subnet address. Separate subnets with commas (,).

Entry	Description
	This item can be omitted if node discovery is performed from only the subnet where Management Servers or Relay Servers are located.
	Nodes on the specified subnets will be detected.
<Group name>.mdbad.inventory.network.subnetmask	Subnet mask.
<Group name>.mdbad.inventory.snmp.community	SNMP community name (public).
<Group name>.mdbad.inventory.node.discovery.ignore	Whether to disable node discovery.
	If "true" is specified, then node discovery will not be performed when information is collected periodically by the agent's schedule function, and IT resource information will only be collected for nodes already detected.
	If IT resource information is collected using the cmdbrefresh command, then node discovery will be performed even if this parameter is set to "true".

To collect IT resource information by dividing multiple subnets into groups, specify the group name at the start of each parameter.

For large-scale systems, IT resource information can be collected sequentially by dividing subnets into multiple groups. To divide subnets into multiple groups, specify the four parameters for each group after changing the group name in each case.

By specifying the group name for <parameter> (for when the agent type is "AGT_INV") when using the configuration information collection schedule configuration file to specify the operation schedule for the agent that collects configuration information, information can be collected at the specified date and time for each group.

The following is an example of the IT resource information collection configuration file (mdr_inv.properties).

```
# default
mdbad.inventory.network.address=
mdbad.inventory.network.subnetmask=255.255.255.0
mdbad.inventory.snmp.community=public
mdbad.inventory.node.discovery.ignore=true
# group1
group1.mdbad.inventory.network.address= 192.0.2.0
group1.mdbad.inventory.network.subnetmask=255.255.255.0
group1.mdbad.inventory.snmp.community=public
group1.mdbad.inventory.node.discovery.ignore=true
# group2
group2.mdbad.inventory.network.address= 198.51.100.0
group2.mdbad.inventory.network.subnetmask=255.255.255.0
group2.mdbad.inventory.snmp.community=ABC
group2.mdbad.inventory.node.discovery.ignore=true
# group3
group3.mdbad.inventory.network.address= 203.0.113.0
group3.mdbad.inventory.network.subnetmask=255.255.255.0
group3.mdbad.inventory.snmp.community=DEF
group3.mdbad.inventory.node.discovery.ignore=true
```

3.1.9.5 How to modify the agent linkage configuration file

Follow the steps below to specify the subnets where node discovery will be performed.

1. Copy the template for the agent linkage configuration file as indicated below:

Source:

[Windows]

- For Management Servers

<div style="border:1px solid black; padding:4px;">

<CMDB Manager directory>\FJSVcmdba\etc\mdrdb.user.template

</div>

- For Relay Servers

<div style="border:1px solid black; padding:4px;">

<Agent installation directory>\CMDB\FJSVcmdba\etc\mdrdb.user.template

</div>

[Linux]

<div style="border:1px solid black; padding:4px;">

/opt/FJSVcmdba/etc/mdrdb.user.template

</div>

Target:

[Windows]

- For Management Servers

<div style="border:1px solid black; padding:4px;">

<CMDB Manager directory>\FJSVcmdba\etc\mdrdb.user

</div>

- For Relay Servers

<div style="border:1px solid black; padding:4px;">

<Agent installation directory>\CMDB\FJSVcmdba\etc\mdrdb.user

</div>

[Linux]

<div style="border:1px solid black; padding:4px;">

/opt/FJSVcmdba/etc/mdrdb.user

</div>

2. Edit the new file (mdrdb.user) as described in the table below:

Entry	Description
mdbad.autodiscovery.network.address	Subnet addresses where nodes on the network will be automatically detected. Separate subnets with commas (,). This item can be omitted if node discovery is performed from only the subnet where Management Servers or Relay Servers are located. Only nodes on the specified subnets will be detected. For this reason, if node discovery is to be performed from the subnet where Management Servers or Relay Servers are located as well as other subnets, be sure to specify addresses for all of the subnets where node discovery will be performed, including the addresses of the subnets where the Management Servers or Relay Servers are located.
mdbad.autodiscovery.network.subnetmask	Subnet mask.
mdbad.autodiscovery.snmp.community	SNMP community name.

The following is an example of the agent linkage configuration file (mdrdb.user).

```
# Subnet address where node is retrieved

mdbad.autodiscovery.network.address= 192.0.2.0,198.51.100.0

# Subnet mask for node retrieval

mdbad.autodiscovery.network.subnetmask=255.255.255.0

# Community name of SNMP

mdbad.autodiscovery.snmp.community=public
```

3.1.9.6 Registering authentication information (when collecting IT resource information)

By executing the cmdbrefresh command after the setup, the list of nodes will be registered with the CMDB. To collect IT resource information, the authentication information (user ID and password) for SSH connections and the machine model information must be registered.

Note that it will not be possible to collect IT resource information unless both the authentication information and the machine model information have been registered and are correct.

Note that nodes that were not running when node discovery was performed for the first time will not be detected, but these nodes can be added to the CMDB by executing the cmdbrefresh command again after these nodes have started.

To register authentication information, follow the steps below:

1. Create a (CSV format) configuration file.

   The file must contain the authentication information, the machine model information and other mandatory information (refer to the *Systemwalker Runbook Automation Reference Guide* for details).

2. Register authentication information with the CMDB:

   [Windows]

   <*Installation directory for the Systemwalker Runbook Automation Management Server*>\bin\swrba_uaimport -f <*file*>.csv

   [Linux]

   /opt/FJSVswrbam/bin/swrbauaimport -f <*file*>.csv

🅿 Point
. . . .

Triggers for collecting IT resource information

The collection of IT resource information is triggered by periodic node discoveries on the Management Server (and Relay Servers). The dates and times when periodic node discovery will run can be specified using the configuration information collection schedule configuration file.

Information can also be collected at any time by executing the cmdbrefresh command.
. . . .

3.1.10 Settings for Using the Operation Component

To perform operations for the operation target server from the Management Server, configure the communication settings according to the system configuration or the operation component that is used.

Using Windows PowerShell

To use the operation component "Execute arbitrary command" or "Collect fingerprint", which uses Windows PowerShell communication, configure the following setting on the Management Server:

- Windows PowerShell communication setting

  Refer to "3.4.3 Windows PowerShell Communication Setting" for information on the settings method.

3.2 Setting up Linked Servers

This section describes how to set up the Agents installed on Linked Servers.

P Point

. . . .

- A list of the Agents that have been set up and are recognized by the CMDB Manager can be displayed using the mdradmin command (with the "-l" option) for the CMDB Manager. Refer to "mdradmin (Agent Management Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the mdradmin command.

- If the Systemwalker Centric Manager Operation Management Server has been constructed in a cluster environment, a different method is used to set up the Agent installed on the Systemwalker Centric Manager Operation Management Server. Refer to the *Systemwalker Runbook Automation Cluster Setup Guide* for information on the setup procedure.

. . . .

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the setup as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

3.2.1 Setting procedure (Collecting Systemwalker Centric Manager Inventory Information)

Changing the execution privileges for the service [Windows]

If the linked Systemwalker Centric Manager server is running V13.2.0 or earlier, change the service execution privileges for the Agent to either the Systemwalker Centric Manager account or an account for a user with administrator privileges. For V13.3.0 or later, there is no need to make a change.

1. Stop the Agent:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
   ```

2. Open the Windows **Services** dialog box.

3. Open the **Properties** window for the "Systemwalker Jservlet (SWNET)" service.

4. Select **This account** in the **Log On** tab of the **Properties** window, and set it to either the Systemwalker administrator account, or an account with administrator privileges.

Executing the setup command

[Windows]

1. Stop the Agent:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
   ```

2. Set up the environment by issuing the commands below:

   ```
   <Agent installation directory>\CMDB\FJSVcmdba\bin\cmdbsetupenv.bat -k AGT_CENTINV
   <Agent installation directory>\CMDB\FJSVcmdba\bin\cmdbsetupenv.bat -k AGT_CENTREP
   ```

3. Modify the Definition File for Collection of Configuration Information

   In agent with setting up, it collects information at the following time everyday as a default.

   - AGT_CENTREP(Agent for collecting Systemwalker Centric Manager node information)

         2.00 AM

   - AGT_CENTINV(Agent for collecting Systemwalker Centric Manager Inventory Information)

         3.00 AM

   Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

   Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

   ```
   AGT_CENTREP 0 2 * * *
   AGT_CENTINV 0 3 * * *
   ```

4. Start the Agent:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
   ```

5. Collect information from Systemwalker Centric Manager:

   ```
   <Agent installation directory>\CMDB\FJSVcmdba\bin\cmdbrefresh.exe -q
   ```

   As a result of this command, the information collected will be registered with the CMDB Manager, which will recognize the existence of the Agent.

 Point

. . . .

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the event log to check when the collection processing completes.

- FCMDB: INFO: [10004] Update check processing has started. '<Agent service type>'

- FCMDB: INFO: [10005] Update check processing has completed. '<Agent service type>'

. . . .

[Linux]

1. Stop the Agent:

   ```
   /opt/FJSVswnc/bin/swncctrl stop
   ```

2. Set up the environment:

   ```
   /opt/FJSVcmdba/bin/cmdbsetupenv.sh -k AGT_CENTINV
   /opt/FJSVcmdba/bin/cmdbsetupenv.sh -k AGT_CENTREP
   ```

3. Start the Agent:

   ```
   /opt/FJSVswnc/bin/swncctrl start
   ```

4. Modify the Definition File for Collection of Configuration Information

In agent with setting up, it collects information at the following time everyday as a default.

- AGT_CENTREP(Agent for collecting Systemwalker Centric Manager node information)

    2.00 AM

- AGT_CENTINV(Agent for collecting Systemwalker Centric Manager Inventory Information)

    3.00 AM

Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

```
AGT_CENTREP 0 2 * * *
AGT_CENTINV 0 3 * * *
```

:

5. Collect information from Systemwalker Centric Manager

```
/opt/FJSVcmdba/bin/cmdbrefresh.sh -q
```

As a result of this command, the information collected will be registered with the CMDB Manager, which will recognize the existence of the Agent.

Point

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the messages in the syslog to check when the collection processing completes.

3.2.2 Setting procedure (Using Operation Component)

Specify the following settings, in accordance with the system configuration and the operation components to be used.

Using SSH

Follow the steps below on the Business Server to use operation components that use SSH communications:

1. Set up the firewall.

    Refer to "2.1.2 Setting up the Firewall" for details.

2. Set up SSH communications.

    Refer to "3.4.2 Setting up SSH Communications" for details.

Using the file transfer infrastructure

Follow the steps below on the Business Server to use operation components that use the file transfer infrastructure:

1. Set up the firewall.

    Refer to "2.1.2 Setting up the Firewall" for details.

2. Restart the file transfer infrastructure service.

    [Windows]

    Open **Control Panel**-**Management tool**-**Service**, restart the Systemwalker File Transfer Library Control service.

    [Linux]

    Execute the following commmnd.

```
# service FJSVlnkbs stop
# service FJSVlnkbs start
```

Using Windows PowerShell

To use the operation component "Execute arbitrary command" or "Collect fingerprint", which uses Windows PowerShell communication, configure the following setting on the Linked Server:

- Windows PowerShell communication setting

Refer to "3.4.3 Windows PowerShell Communication Setting" for information on the settings method.

Using Telnet

To use the operation components "Execute arbitrary command" and "Execute multiple commands", which use Telnet communication, configure the following setting on the Linked Server:

- Telnet communication setting

Refer to "3.4.4 Telnet Communication Setting" for information on the settings method.

Using RSH and REXEC

To use the operation component "Execute arbitrary command", which uses RSH and REXEC communication, configure the following setting on the Linked Server:

1. Firewall setting

Refer to "2.1.2 Setting up the Firewall" for information on the settings method.

2. RSH and REXEC communication setting

Refer to "3.4.5 RSH and REXEC Communication Setting" for information on the settings method.

Using FTP

To use the operation component "Transfer files", which uses FTP communication, configure the following setting on the Linked Server:

- Firewall setting

Refer to "2.1.2 Setting up the Firewall" for information on the settings method.

3.3 Setting up Relay Servers

This section describes how to set up the Agents that automatically collect Business Server configuration information from Relay Servers.

P Point

- A list of the Agents that have been set up and are recognized by the CMDB Manager can be displayed using the mdradmin command (with the "-l" option) for the CMDB Manager. Refer to "mdradmin (Agent Management Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the mdradmin command.

- The procedure for setting up Agents in systems where Relay Servers are operating in a cluster environment is exactly the same as for non-cluster environments. Install Agents on both the active node and the standby node in the cluster by using the same procedure as for non-cluster environments.

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the setup as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

3.3.1 Setup procedure (when collecting IT resource information)

[Windows]

1. Stop the Agent:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
   ```

2. Modify the IT resource information collection configuration file.

   To perform node discovery from a subnet other than the subnet where Relay Servers are located, modify the file (refer to "3.1.9.4 How to modify the IT resource information collection configuration file" for details).

3. Set up the environment:

   ```
   <Agent installation directory>\CMDB\FJSVcmdba\bin\cmdbsetupenv.bat -k AGT_INV
   ```

4. Modify the Definition File for Collection of Configuration Information

   In agent with setting up, it collects information at the following time everyday as a default.

   ```
   4.30am
   ```

   Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

   Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

   ```
   AGT_ADSC 45 4 * * *
   ```

5. Start the Agent:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
   ```

6. Collect IT resource information automatically:

   ```
   <Agent installation directory>\CMDB\FJSVcmdba\bin\cmdbrefresh.exe -q type= AGT_INV
   ```

   As a result of this operation, the nodes connected to the network will be detected automatically, and the information collected will be registered with the CMDB Manager.

7. Register authentication information on Business Server.

   From Business Server which not installed agent package for Business Server, to collect logical server, hardware information, installed software information, as IT resource information, To be need to register authentication information for SSH communication on CMDB

   Refer to the 3.1.9.6 Registering authentication information (when collecting IT resource information)

   ## Point

   ....

   Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the event log to check when the collection processing completes.

   - FCMDB: INFO: [10004] Update check processing has started. '<Agent service type>'

   - FCMDB: INFO: [10005] Update check processing has completed. '<Agent service type>'

   ....

[Linux]

1. Stop the Agent:

   ```
   /opt/FJSVswnc/bin/swncctrl stop
   ```

2. Modify the IT resource information collection configuration file.

   To perform node discovery from a subnet other than the subnet where Relay Servers are located, modify the file (refer to "3.1.9.4 How to modify the IT resource information collection configuration file" for details).

3. Set up the environment:

   ```
   /opt/FJSVcmdba/bin/cmdbsetupenv.sh -k AGT_INV
   ```

4. Modify the Definition File for Collection of Configuration Information

   In agent with setting up, it collects information at the following time everyday as a default.

   ```
   4.30am
   ```

   Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

   Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

   ```
   AGT_ADSC 45 4 * * *
   ```

5. Start the Agent

   ```
   /opt/FJSVswnc/bin/swncctrl start
   ```

6. Collect IT resource information automatically:

   ```
   /opt/FJSVcmdba/bin/cmdbrefresh.sh -q type= AGT_INV
   ```

   As a result of this operation, the nodes connected to the network will be detected automatically, and the information collected will be registered with the CMDB Manager.

7. Register authentication information on Business Server.

   From Business Server which not installed agent package for Business Server, to collect logical server, hardware information, installed software information, as IT resource information, To be need to register authentication information for SSH communication on CMDB

   Refer to the *Registering authentication information(when collecting IT resource information)*

📦 Point

. . . .

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the syslog to check when the collection processing completes.

   - FCMDB: INFO: [10004] Update check processing has started. 'Agent service name'

   - FCMDB: INFO: [10005] Update check processing has completed. 'Agent service name'

. . . .

3.3.2 Setup procedure (when collecting only node information)

[Windows]

1. Stop the Agent:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
   ```

2. Modify the agent linkage configuration file.

   To perform node discovery from a subnet other than the subnet where Relay Servers are located, modify the file (refer to "3.1.9.5 How to modify the agent linkage configuration file" for details).

3. Set up the environment:

```
<Agent installation directory>\CMDB\FJSVcmdba\bin\cmdbsetupenv.bat -k AGT_ADSC
```

4. Modify the Definition File for Collection of Configuration Information

In agent with setting up, it collects information at the following time everyday as a default.

```
4.45am
```

Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

```
AGT_ADSC 45 4 * * *
```

5. Start the Agent

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
```

6. Update the observed records managed by the CMDB:

```
<Agent installation directory>\CMDB\FJSVcmdba\bin\cmdbrefresh.exe -q type=AGT_ADSC
```

As a result of this operation, the information collected will be registered with the CMDB Manager, which will recognize the existence of the Agent.

Point

• •

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the event log to check when the collection processing completes.

- FCMDB: INFO: [10004] Update check processing has started. '<Agent service type>'

- FCMDB: INFO: [10005] Update check processing has completed. '<Agent service type>'

• •

[Linux]

1. Stop the Agent:

```
/opt/FJSVswnc/bin/swncctrl stop
```

2. Modify the agent linkage configuration file.

To perform node discovery from a subnet other than the subnet where Relay Servers are located, modify the file (refer to "3.1.9.5 How to modify the agent linkage configuration file" for details).

3. Set up the environment:

```
/opt/FJSVcmdba/bin/cmdbsetupenv.sh -k AGT_ADSC
```

4. Modify the Definition File for Collection of Configuration Information

In agent with setting up, it collects information at the following time everyday as a default.

```
4.45am
```

Refer to the *Definition File for Collection of Configuration Information* in the *Systemwalker Runbook Automation Reference Guide* and change to collecting schedule to any date.

Note that if you do not need to execute automated collect routinely, Add "#" to the first letter of following line with comment out.

```
AGT_ADSC 45 4 * * *
```

5. Start the Agent:

```
/opt/FJSVswnc/bin/swncctrl start
```

6. Update the observed records managed by the CMDB:

```
/opt/FJSVcmdba/bin/cmdbrefresh.sh -q type= AGT_ADSC
```

As a result of this operation, the information collected will be registered with the CMDB Manager, which will recognize the existence of the Agent.

Point

....

Refer to "cmdbrefresh (Observed Record Collection Request Command)" in the *Systemwalker Runbook Automation Reference Guide* for details on the cmdbrefresh command. Check the following messages in the syslog to check when the collection processing completes.

- FCMDB: INFO: [10004] Update check processing has started. 'Agent service name'

- FCMDB: INFO: [10005] Update check processing has completed. 'Agent service name'

....

3.3.3 Setting procedure (Using Operation Component)

Specify the following settings, in accordance with the system configuration and the operation components to be used.

Using SSH

Follow the steps below on the Business Server to use operation components that use SSH communications:

1. Set up the firewall.

   Refer to "2.1.2 Setting up the Firewall" for details.

2. Set up SSH communications.

   Refer to "3.4.2 Setting up SSH Communications" for details.

Using the file transfer infrastructure

Follow the steps below on the Business Server to use operation components that use the file transfer infrastructure:

1. Set up the firewall.

   Refer to "2.1.2 Setting up the Firewall" for details.

2. Restart the file transfer infrastructure service.

   [Windows]

   Open **Control** Panel-**Management tool**-**Service**, restart the Systemwalker File Transfer Library Control service.

   [Linux]

   Execute the following commmnd.

```
# service FJSVlnkbs stop
# service FJSVlnkbs start
```

Using Windows PowerShell

To use the operation component "Execute arbitrary command" or "Collect fingerprint", which uses Windows PowerShell communication, configure the following setting on the Relay Server:

- Windows PowerShell communication setting

  Refer to "3.4.3 Windows PowerShell Communication Setting" for information on the settings method.

Using Telnet

To use the operation components "Execute arbitrary command" and "Execute multiple commands", which use Telnet communication, configure the following setting on the Relay Server:

- Telnet communication setting

    Refer to "3.4.4 Telnet Communication Setting" for information on the settings method.

Using RSH and REXEC

To use the operation component "Execute arbitrary command", which uses RSH and REXEC communication, configure the following setting on the Relay Server:

1. Firewall setting

    Refer to "2.1.2 Setting up the Firewall" for information on the settings method.

2. RSH and REXEC communication setting

    Refer to "3.4.5 RSH and REXEC Communication Setting" for information on the settings method.

Using FTP

To use the operation component Transfer files, which uses FTP communication, configure the following setting on the Relay Server:

- Firewall setting

    Refer to "2.1.2 Setting up the Firewall" for information on the settings method.

3.4 Setting up Business Servers

This section describes how to set up Business Servers.

Setting communications

The following diagram shows an overview of the setup procedure.
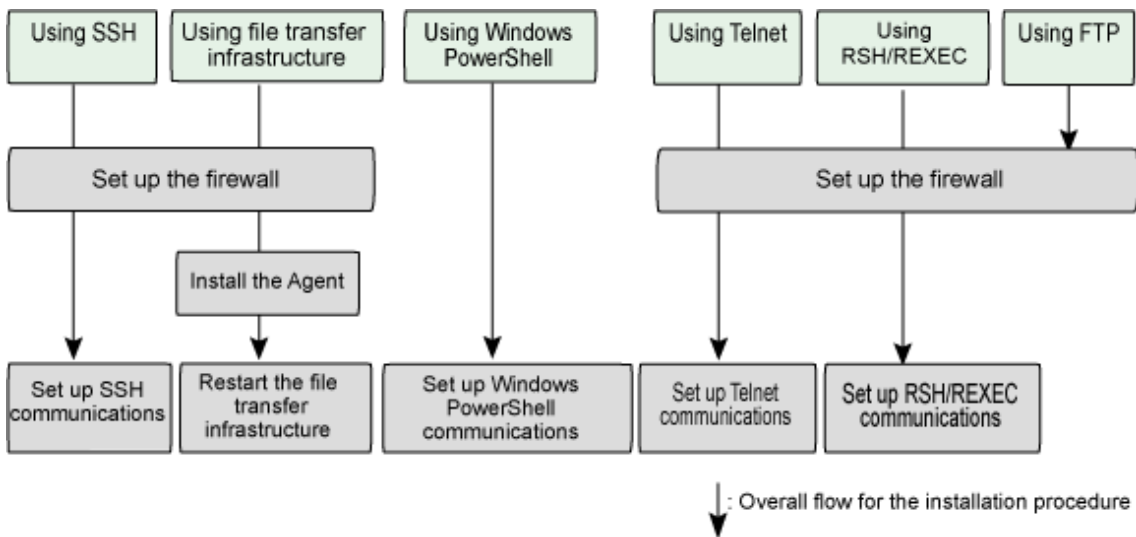
Specify the following settings, in accordance with the system configuration and the operation components to be used.

Using SSH

Follow the steps below on the Business Server to use operation components that use SSH communications:

1. Set up the firewall.

    Refer to "2.1.2 Setting up the Firewall" for details.

2. Set up SSH communications.

    Refer to "3.4.2 Setting up SSH Communications" for details.

Using the file transfer infrastructure

Follow the steps below on the Business Server to use operation components that use the file transfer infrastructure:

1. Set up the firewall.

   Refer to "2.1.2 Setting up the Firewall" for details.

2. Install the Agent.

   Refer to "2.5 Installing on Business Servers" for details.

3. Restart the file transfer infrastructure service.

   [Windows]

   Restart Systemwalker File Transfer Library Control with [**Service**] dialog box on [**Start**]-[Management Tool]

   [Linux]

   Execute the following command:

   ```
   # service FJSVlnkbs stop
   # service FJSVlnkbs start
   ```

   [Solaris]

   Execute the following command:

   ```
   # /etc/init.d/FJSVlnkbs stop
   # /etc/init.d/FJSVlnkbs start
   ```

Using Windows PowerShell

To use the operation component "Execute arbitrary command" or "Collect fingerprint", which uses Windows PowerShell communication, configure the following setting on the Business Server:

- Windows PowerShell communication setting

  Refer to "3.4.3 Windows PowerShell Communication Setting" for information on the settings method.

Using Telnet

To use the operation components "Execute arbitrary command" and "Execute multiple commands", which use Telnet communication, configure the following setting on the Business Server:

1. Firewall setting

   Refer to "2.1.2 Setting up the Firewall" for information on the settings method.

2. Telnet communication setting

   Refer to "3.4.4 Telnet Communication Setting" for information on the settings method.

Using RSH and REXEC

To use the operation component "Execute arbitrary command", which uses RSH and REXEC communication, configure the following setting on the Business Server:

1. Firewall setting

   Refer to "2.1.2 Setting up the Firewall" for information on the settings method.

2. RSH and REXEC communication setting

   Refer to "3.4.5 RSH and REXEC Communication Setting" for information on the settings method.

Using FTP

To use the operation component "Transfer file ", which uses FTP communication, configure the following setting on the Business Server:

- Firewall setting

  Refer to "2.1.2 Setting up the Firewall" for information on the settings method.

Setting to collect system configuration automatically

To collect system configuration automatically, it is different how to set according to the which information be collected or which communication method be used.

The following diagram shows an overview of procedure
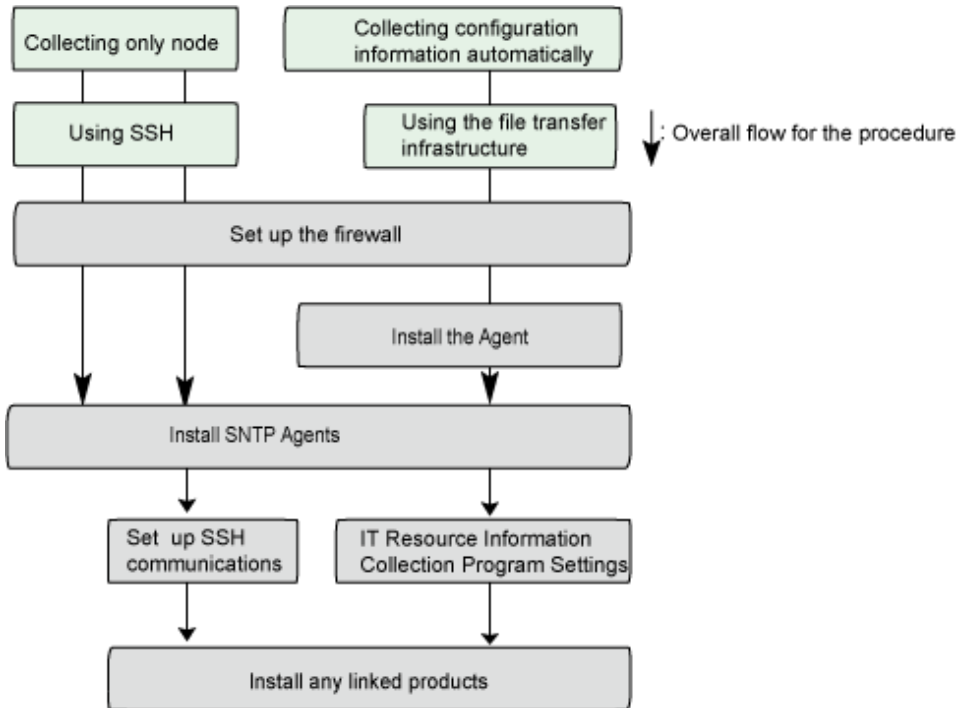
Collecting configuration information automatically (when using SSH)

Follow the steps below on the Business Server to collect IT resource information:

1. Set up the firewall.

   Refer to "2.1.2 Setting up the Firewall" for details.

2. Set up SNMP Agents.

   Refer to "3.4.1 Installing SNMP Agents" for details

3. Set up SSH communications.

   Refer to "3.4.2 Setting up SSH Communications" for details.

4. Install any linked products (optional).

   To collect more detailed information about IT resources, install linked products that run as server management tools.

   Refer to the manuals for the linked product for details on how to install the linked product.

   Refer to "Linked Software" in the *Systemwalker Runbook Automation Technical Guide* for information on products that can link to Systemwalker Runbook Automation.

Collecting configuration information automatically (when using file transfer infrastructure)

Follow the steps below on the Business Server to collect IT resource information:

1. Set up the firewall.

   Refer to "2.1.2 Setting up the Firewall" for details.

2. Set up Agents.

   Refer to "2.5 Installing on Business Servers" for details

3. Set up SNMP Agents.

   Refer to "3.4.1 Installing SNMP Agents" for details

4. Set up IT Resource Information Collection Program Settings.

   Refer to "3.4.6 IT Resource Information Collection Program Settings" for details.

5. Install any linked products (optional).

   To collect more detailed information about IT resources, install linked products that run as server management tools.

   Refer to the manuals for the linked product for details on how to install the linked product.

   Refer to "Linked Software" in the *Systemwalker Runbook Automation Technical Guide* for information on products that can link to Systemwalker Runbook Automation

Collecting only node

Follow the steps below on the Business Server to collect IT resource information:

1. Set up the firewall.

   Refer to "2.1.2 Setting up the Firewall" for details.

2. Set up SNMP Agents.

   Refer to "3.4.1 Installing SNMP Agents" for details

3.4.1 Installing SNMP Agents

An SNMP Agent must be installed beforehand.

P Point

. . . .

The difference between an SNMP Agent being installed or not on the target server is as follows:

- If an SNMP Agent is installed:

  When nodes are detected, MIB information can be collected, in addition to the IP address and host name.

  The vendor name and operating system type will be added to configuration information, allowing inventory information to be collected.

- If an SNMP Agent is not installed:

  Only the IP address and host name will be added to the CMDB.

  Inventory information will not be collected.

. . . .

This section describes how to install SNMP Agents.

For information on how to install and set up SNMP Agents for operating systems and network devices not listed in the descriptions (examples) below, refer to the manual for the operating system or network device in question.

Follow the steps below to install SNMP Agents.

```
Installing SNMP Agents
```

```
Setting up the SNMP service
```

Installing SNMP Agents

This section describes how to install SNMP Agents (examples).

[Windows]

- [Windows(R) 2003]

- [Windows(R) 2008]

For Windows Server 2003

To install an SNMP Agent on a computer where Windows(R) 2000 is already running, follow the steps below:

1. Double-click the Add or Remove Programs icon in the Control Panel.

2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components to display the Windows Component Wizard.

3. Select the Management and Monitoring Tools component from the Components list in the Windows Component Wizard, and then click the Details button.

4. Select Simple Network Management Protocol in the Management and Monitoring Tools dialog box, and then click the OK button.

5. Click the Next button in the Add or Remove Programs dialog box and then install according to the window directive.

For Windows Server 2008

1. Click Start >> Control Panel >> Programs and Features.

2. Select Turn Windows features on or off. From the Server Manager window, select Features >> Add Features to display Add Features Wizard.

3. From the Add Features Wizard list, select SNMP Services from the SNMP Services tree and click the Next button.

4. In Confirm Installation Selections, click the Install button, and then, insert the Windows operating system CD-ROM to start the installation.

[Linux]

Note

For systems where an update release has been applied, the update release must be reapplied after the SNMP service is installed.

To install an SNMP Agent, install the following rpm package.

- net-snmp (or ucd-snmp)

Information

Relevant commands

- When installing the rpm package, use the "-i" option with the rpm command.

- To remove the rpm package, use the "-e" option with the rpm command.

- To check whether the rpm package has been installed, use the "-q" option with the rpm command.

[Configuration file]

```
/etc/snmp/snmpd.conf
```

The following is an example of how to edit the SNMP Agent configuration file.

Refer to the man command for details.

[Before]

```
# sec.name source community
com2sec notConfigUser default public

# groupName securityModel securityName
group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser

# Make at least snmpwalk -v 1 localhost -c public system fast again.

# name incl/excl subtree mask(optional)
view systemview included .1.3.6.1.2.1.1
view systemview included .1.3.6.1.2.1.25.1.1

# group context sec.model sec.level prefix read write notif
access notConfigGroup "" any noauth exact systemview none none
```

[After]

```
# sec.name source community
#com2sec notConfigUser default public
com2sec systemwalker default public

# groupName securityModel securityName
#group notConfigGroup v1 notConfigUser
#group notConfigGroup v2c notConfigUser
group RWGroup v1 systemwalker
group RWGroup v2c systemwalker
group RWGroup usm systemwalker

# Make at least snmpwalk -v 1 localhost -c public system fast again.
# name incl/excl subtree mask(optional)
#view systemview included .1.3.6.1.2.1.1
#view systemview included .1.3.6.1.2.1.25.1.1
view all included .1 80

# group context sec.model sec.level prefix read write notif
#access notConfigGroup "" any noauth exact systemview none none
access RWGroup "" any noauth exact all none none
```

Restart the SNMP Agent after editing the configuration file.

```
# /etc/init.d/snmpd stop

# /etc/init.d/snmpd start
```

[Solaris]

Install the following packages when installing the SNMP agent:

Solaris10

- SUNWsmmgr

- SUNWsmagt

- SUNWsmcmd

P Point

- Please note the following about the commands used:

    - The pkgadd command is used to install packages.

    - The pkgrm command is used to remove packages.

- The pkginfo command is used to display information about installed packages.

- It is possible for the SNMP service to run using the post-installation settings. If necessary, refer to the SNMP service settings and the operating system manual first, before reconfiguring the settings.

Solaris11

- system/management/snmp/net-snmp

P Point

- Please note the following about the commands used:

    - The pkg install command is used to install packages.

    - The pkg uninstall command is used to remove packages.

    - The pkg search command is used to display information about installed packages.

- It is possible for the SNMP service to run using the post-installation settings. If necessary, refer to the SNMP service settings and the operating system manual first, before reconfiguring the settings.

Setting up the SNMP service

In order to automatically collect server configuration information, specify the community names matching the values set in the SNMP service in the IT resource information collection definition file.

Specify "public" as the SNMP community name - if another value is specified, the information that can be collected as part of IT resource information collection will be reduced.

[Windows]

Strat SNMP **Service Property** dialogue box from **Service** window where installed agent compiter, and set the term after **Security** tab.

Community name setting

Set a community name that the SNMP Agent accepts.

The following characters cannot be used for community names: spaces and the symbols below:

- !*"+=#>

- The following character pairs: "\^" and "\-"

Setting of host that allows access

To automatically collect inventory information for the server, specify the same community name specified for the SNMP service.

[Linux]

Community name setting

To set the community name, edit the following file:

[Configuration file]

/etc/snmp/snmpd.conf

Refer to the man command for details.

[Settings item]

Com2sec systemwalker default public

Setting of host that allows access

The explanation that follows assumes that the IP address of the host that allows SNMP packets to be received is "*.*.*.*".

Use this as the setting that allows SNMP packets from the Management Server or Linked Server/Relay Server.

In the default setting, SNMP packets are allowed.

[Configuration file]

```
/etc/snmp/snmpd.conf
```

Refer to the man command for details.

[Before]

```
Com2sec systemwalker default public
```

[After]

```
Com2sec systemwalker *.*.*.* public
```

After editing the configuration file, restart the SNMP agent.

```
# /etc/init.d/snmpd stop
# /etc/init.d/snmpd start
```

[Solaris]

Community name setting

To set the community name, edit the files shown below.

Normally, "public" is already set as the community name, therefore there is no need to edit the file.

Solaris10

[Configuration file]

```
/etc/sma/snmp/snmpd.conf
```

Refer to the man command for details.

[Settings item]

```
rocommunity public
```

Solaris11

[Configuration file]

```
/etc/net-snmp/snmp/snmpd.conf
```

Refer to the man command for details.

[Settings item]

```
rocommunity public
```

Setting of host that allows access

The explanation that follows assumes that the IP address of the host that allows SNMP packets to be received is "*.*.*.*".

Use this as the setting that allows SNMP packets from the Management Server or Linked Server/Relay Server.

In the default setting, SNMP packets are allowed.

Solaris10

[Configuration file]

```
/etc/sma/snmp/snmpd.conf
```

Refer to the man command for details.

[Before]

```
rocommunity public
```

[After]

```
rocommunity public *.*.*.*
```

After editing the configuration file, restart the SNMP agent.

```
# svcadm restart svc:/application/management/sma:default
```

Solaris11

[Configuration file]

```
/etc/net-snmp/snmp/snmpd.conf
```

Refer to the man command for details.

[Before]

```
rocommunity public
```

[After]

```
rocommunity public *.*.*.*
```

After editing the configuration file, restart the SNMP agent.

```
# svcadm -v restart net-snmp
```

3.4.2 Setting up SSH Communications

To use operation components that use SSH communications, follow the steps below:

1. Prepare an account for remote connections (login).

   Prepare an account with administrator privileges (the "root" account or an account that belongs to the "Administrators" group).

2. Open a hole in the firewall for the port used for SSH.

   Port used by SSH: 22/TCP

3. Start the SSH service.

   Install the following SSH function if it is has not been installed.

   [Windows]

   Install OpenSSH (Cygwin OpenSSH V1.7 or later).

   [Linux] [Solaris]

   If SSH has not been installed as one of the standard functions of the operating system, install OpenSSH.

   Refer to the SSH manual for information on how to install OpenSSH and start the service.

3.4.3 Windows PowerShell Communication Setting

To use the operation component "Execute arbitrary command" or "Collect fingerprint", which uses Windows PowerShell communication, execute the operation shown below.

- In order to give directions to each server using PowerShell in the operation component, the following Management Server/Business Server settings are required.

    - Management Server settings

        1. Start Windows PowerShell 2.0 as the administrator.
           Start->> **All Programs** >> **Accessory** >> **Windows PowerShell** >> **Windows PowerShell** >> **Execute the setup as an administrator** .

        2. Enter the following command, then press [y] to update TrustedHosts of the WinRM client.

        ```
        Set-Item WSMan:\localhost\Client\TrustedHosts -value <name or IP address of
        the Business Server machine>
        ```

        3. Enter the following command, then press [y] to set the PowerShell script execution policy as "RemoteSigned".

        ```
        Set-ExecutionPolicy remotesigned
        ```

    - Note 1: If the Management Server operating system is 64-bit, start Windows PowerShell 2.0 (x86) as the administrator before configuring the settings.

    - Business Server settings

        1. Start Windows PowerShell 2.0 as the administrator.
           Start >> All Programs >> **Accessory** >> Windows PowerShell >> Windows PowerShell >> **Execute the setup as an administrator.**

        2. Enter the following command, then press [y] to allow the WinRM service.

        ```
        Enable-PSRemoting
        ```

    - Note 1: After [y] is pressed, the content may be checked again. In this case, press [y] again.

    - Note 2: If the Business Server operating system is 64-bit, start Windows PowerShell 2.0 (x86) as the administrator before configuring the settings.

Refer to "TechNet Library" - "Running Remote Commands" in the Micorsoft TechNet website for information on how to set the server.

3.4.4 Telnet Communication Setting

To use the operation components "Execute arbitrary command" and "Execute multiple commands", which use Telnet communication, execute the operation shown below.

- Check whether Telnet requests a user name and password with the following login prompts. If not, commands cannot be executed using Telnet.

    - xxxlogin:

    - Password:

xxx: Any string

3.4.5 RSH and REXEC Communication Setting

To use the operation component "Execute arbitrary command", which uses RSH and REXEC communication, execute the operation shown below.

- Create environments on Linked Servers and Business Servers so that connections can be established using the following user on the Management Server.

If the Management Server is running Windows: "Administrator" user

If the Management Server is running Linux/Solaris: "root" user

3.4.6 IT Resource Information Collection Program Settings

To collect IT resource information using the file transfer infrastructure, follow the procedure shown below.

1. Install Systemwalker Runbook Automation on the management server, then download the files shown below from the server.

   When the management server is Windows

   When the target business server is Windows

   ```
   [Systemwalker Runbook Automation installation directory]\SWRBAM\CMDB\FJSVcmdba\inventory
   \FJSVcmdbi.ex_
   ```

   When the target business server is Linux

   ```
   [Systemwalker Runbook Automation installation directory]\SWRBAM\CMDB\FJSVcmdba\inventory
   \FJSVcmdbi-14.1.0-0.i386.rpm
   ```

   When the target Business Server is Solaris:

   ```
   [Systemwalker Runbook Automation installation directory]\SWRBAM\CMDB\FJSVcmdba\inventory
   \FJSVcmdbi-15.1.0.pkgtrans
   ```

   When the management server is Linux

   When the target business server is Windows

   ```
   /opt/FJSVcmdba/inventory/FJSVcmdbi.ex_
   ```

   When the target business server is Linux

   ```
   /opt/FJSVcmdba/inventory/FJSVcmdbi-14.1.0-0.i386.rpm
   ```

   When the target Business Server is Solaris:

   ```
   /opt/FJSVcmdba/inventory/FJSVcmdbi-15.1.0-0.pkgtrans
   ```

2. Install the IT resource information collection program on the business server.

   a. The files in 1 in can be stored in any directory.

   b. Execute the commands shown below using the administrative privileges (Administrator/root) account..

      When the target business server is Windows

      ```
      > move FJSVcmdbi.ex_ FJSVcmdbi.exe
      > cd C:\
      > [File storage directory]\FJSVcmdbi.exe
      > C:\FJSVcmdbi\bin\fcmdb_inv_lnksetup.bat
      ```

      When the target business server is Linux

      ```
      > rpm -i FJSVcmdbi-14.1.0-0.i386.rpm
      > service FJSVcmdbi_rcvctl start
      ```

      When the target Business Server is Solaris:

      ```
      > pkgadd -d FJSVcmdbi-15.1.0-0.pkgtrans FJSVcmdbi
      > /etc/init.d/FJSVcmdbi_rcvctl start
      ```

Chapter 4 Starting and Stopping

This chapter describes how to start and stop Systemwalker Runbook Automation and the agents.

- Start Systemwalker Runbook Automation

- Stop Systemwalker Runbook Automation

- Start Agents

- Stop Agents

📖 Note
. . . .

For information on starting and stopping Systemwalker Runbook Automation to apply an update, refer to "Applying Updates to Systemwalker Runbook Automation" in the *Systemwalker Runbook Automation Administration Guide*.
. . . .

4.1 Starting and Stopping the Management Server

4.1.1 Starting Systemwalker Runbook Automation

This section describes how to start Systemwalker Runbook Automation.

[Windows]

1. Log in to the Management Server as a user with Administrator privileges.

2. Start Systemwalker Runbook Automation, by using either of the methods below:

   Method 1: Via the command line:

   > *<Installation directory for the Systemwalker Runbook Automation Management Server>*\bin\swrba_start

   Method 2: Via the Start menu:

   Select **Programs**, **Systemwalker Runbook Automation** and then **Starting Management Server** from the **Start** menu.

📖 Note
. . . .

If the operating system being used is Windows Server 2008, execute the command above as an administrator.
. . . .

3. The message below will be displayed:

   If the command line was used:

   > Systemwalker Runbook Automation is starting up.
   > The Process Management Database has started.
   > The server function has started.
   > The console function has started.
   > CMDB Manager has started.
   > The Scheduling has started.
   > Systemwalker Runbook Automation startup has completed successfully.

   If the **Start** menu was used:

   > Press any key to continue.

[Linux]

1. Log in to the Management Server as a superuser.

2. Start Systemwalker Runbook Automation:

   ```
   # /opt/FJSVswrbam/bin/swrba_start
   ```

   This will start the daemon for each Systemwalker Runbook Automation function .

3. The message below will be displayed:

   ```
   Systemwalker Runbook Automation is starting up
   The Process Management Database has started.
   The server function has started.
   The console function has started.
   CMDB Manager has started.
   The Scheduling has started.
   Systemwalker Runbook Automation startup has completed successfully
   ```

4.1.2 Stopping Systemwalker Runbook Automation

This section describes how to stop Systemwalker Runbook Automation.

[Windows]

1. Log in to the Management Server as a user with Administrator privileges.

2. Stop Systemwalker Runbook Automation by using either of the methods below:

   Method 1: Via the command line:

   ```
   <Installation directory for the Systemwalker Runbook Automation Management Server>
   \bin\swrba_stop
   ```

   Method 2: Via the Start menu:

   Select **Programs**, **Systemwalker Runbook Automation** and then **Stopping Management Server** from the **Start** menu.

 Note
....
If the operating system being used is Windows Server 2008, execute the command above as an administrator.
....

3. The message below will be displayed:

   If the command line was used:

   ```
   Systemwalker Runbook Automation is stopping.
   The Scheduling has stopped.
   CMDB Manager has stopped.
   The console function has stopped.
   The server function has stopped.
   ```

```
The Process Management Database has stopped.
Systemwalker Runbook Automation stop has completed successfully.
```

If the **Start** menu was used:

```
Press any key to continue.
```

See

Refer to the *Systemwalker Runbook Automation Reference Guide* for details on swrba_stop.

[Linux]

1. Log in to the Management Server as a superuser.

2. Stop Systemwalker Runbook Automation:

```
# /opt/FJSVswrbam/bin/swrba_stop
```

3. The message below will be displayed:

```
Systemwalker Runbook Automation is stopping.
The Scheduling has stopped.
CMDB Manager has stopped.
The console function has stopped.
The server function has stopped.
The Process Management Database has stopped.
Systemwalker Runbook Automation stop has completed successfully.
```

See

Refer to the *Systemwalker Runbook Automation Reference Guide* for details on swrba_stop.

4.2 Starting and Stopping Linked Servers/Relay Servers

4.2.1 Starting Agents

This section describes how to start Agents.

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the startup process as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

Startup method

[Windows]

Issue the command below:

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
```

[Linux]

Issue the command below:

```
/opt/FJSVswnc/bin/swncctrl start
```

Execution results

The message below will be displayed if the command succeeds:

```
swncctrl start : SUCCESS
```

The message below will be displayed if the command fails:

```
swncctrl start : FAILURE <return code>
```

If the command fails, then check whether setup has been performed correctly (refer to "Chapter 3 Setup" for information). Refer to the *Systemwalker Runbook Automation Reference Guide* for information on return codes.

4.2.2 Stopping Agents

This section describes how to stop Agents.

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the stop process as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

Stop method

[Windows]

Issue the command below:

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
```

[Linux]

Issue the command below:

```
/opt/FJSVswnc/bin/swncctrl stop
```

Execution results

The message below will be displayed if the command succeeds:

```
swncctrl stop : SUCCESS
```

The message below will be displayed if the command fails:

```
swncctrl stop : FAILURE <return code>
```

Refer to the S*ystemwalker Runbook Automation Reference Guide* for information on return codes.

Chapter 5 Operation Testing

This chapter describes how to test the environment after setup.

5.1 Post-setup Checks

After the setup completes, check whether you can log in to the Web console.

📌 **Note**
. . . .
Ensure that it is possible to communicate via the network using the port numbers listed in "9.1 Port Numbers".
. . . .

5.1.1 Starting Systemwalker Runbook Automation

Refer to "4.1.1 Starting Systemwalker Runbook Automation" for details.

5.1.2 Operation Testing

This section describes how to log in to the Web console for Systemwalker Runbook Automation.

📌 **Note**
. . . .
If an error occurs, check for problems in installation and the setup procedures. Also check log information (refer to "8.1 Logs" for details).
. . . .

Operation

1. Start a Web browser.

2. Specify the URL for Systemwalker Runbook Automation using the following format.

   Specify the port number for the HTTP server set during installation.

   > http://<*Management Server host name*>:<*port number*>/console/Default/

   The login window will be displayed.

3. Log in as the user for process control.

📌 **Note**
. . . .
The user for process control is an internal user that is required for Systemwalker Runbook Automation to run.

This user should only be used for testing purposes.

Refer to the *Systemwalker Runbook Automation Operation Guide* for details on how to add Systemwalker Runbook Automation administrator users and general users.
. . . .

Chapter 6 Setup Cancellation

This chapter describes how to cancel the setup for Systemwalker Runbook Automation Management Servers.

- Points to note before canceling the setup

- Cancel the setup for Management Servers

- Cancel the setup for Linked Servers and Relay Servers

- Cancel the setup for Business Servers

6.1 Points to Note before Canceling the Setup

Note the following points before canceling setups.

Backing up user resources

When setup is canceled, all files and settings information including user assets will be deleted. For this reason, back up existing assets before canceling the setup if this information will be needed later. Refer to "8.3 Backup and Restoration" for information on backups.

Deleting directories

If a directory was specified during setup, it will still exist after the setup is canceled, and must be manually deleted after canceling the setup:

- Process Management Database directory

6.2 Cancelling the Setup for Management Servers

This section describes how to cancel the setup for Management Servers.
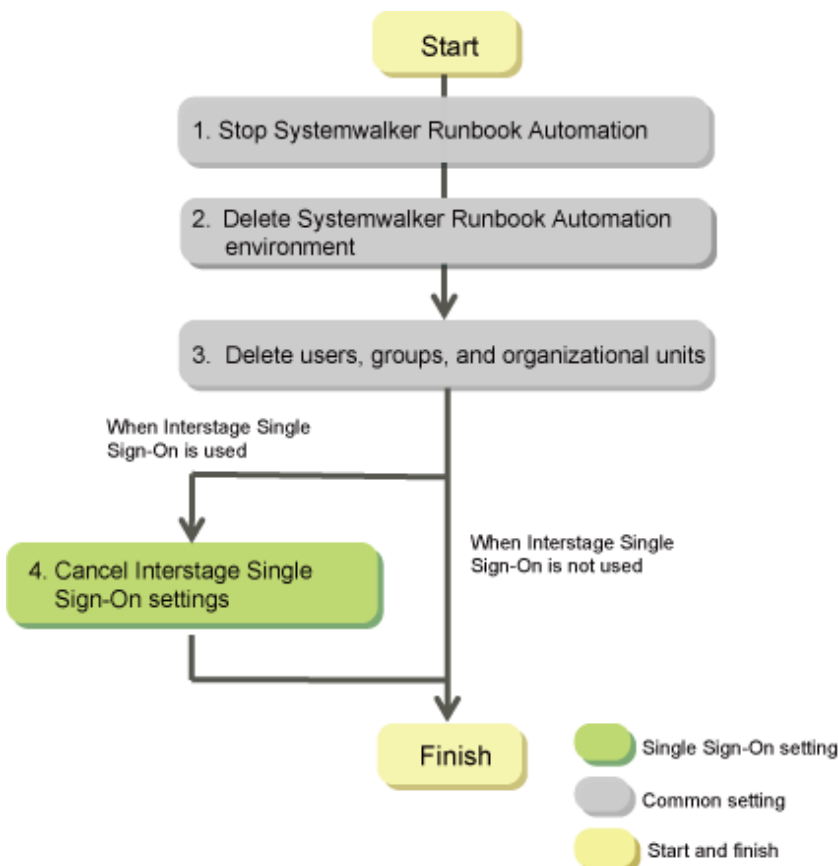
1. Stop Systemwalker Runbook Automation

   Refer to "6.2.1 Stopping Systemwalker Runbook Automation".

2. Delete the Environment for Systemwalker Runbook Automation

   [Windows]

   Refer to "6.2.2 Deleting the Environment for Systemwalker Runbook Automation [Windows]".

   [Linux]

   Refer to "6.2.3 Deleting the Environment for Systemwalker Runbook Automation [Linux]".

3. Delete Users, Groups and Organizational Units

   Refer to "6.2.4 Deleting the Users, Groups and Organizational Units".

4. Cancel the Setup for Interstage Single Sign-On

   Refer to "6.2.5 Cancelling Setup of Interstage Single Sign-On".

Note

- If the setup fails, then restart the system and cancel the setup.

- When canceling the setup for Systemwalker Runbook Automation:

    - Execute the "isstat" command and ensure that Interstage is running.

6.2.1 Stopping Systemwalker Runbook Automation

Follow the steps below to stop Systemwalker Runbook Automation:

1. Log in to the Management Server as a user with administrator privileges.

2. Stop Systemwalker Runbook Automation:

   [Windows]

   <Installation directory for the Systemwalker Runbook Automation Management Server>
   \bin\swrba_stop

   [Linux]

   # /opt/FJSVswrbam/bin/swrba_stop

Note

If the operating system being used is Windows Server 2008, execute the command above as an administrator.

See

Refer to "4.1.2 Stopping Systemwalker Runbook Automation" for details on how to stop Systemwalker Runbook Automation.

6.2.2 Deleting the Environment for Systemwalker Runbook Automation [Windows]

Follow the steps below to delete the Systemwalker Runbook Automation environment:

 Note

. . . .

To cancel the setup, log in as the same user that executed the setup.

. . . .

1. Log in to the Management Server as a user with administrator privileges.

2. Execute the following command to start the Systemwalker Runbook Automation Setup Cancellation Tool:

   > *<Installation directory for the Systemwalker Runbook Automation Management Server>*\bin
   > \swrba_setup -u

3. Click the **Next** button.

   It is recommended to backup resources such as ticket histories, because they will be deleted.
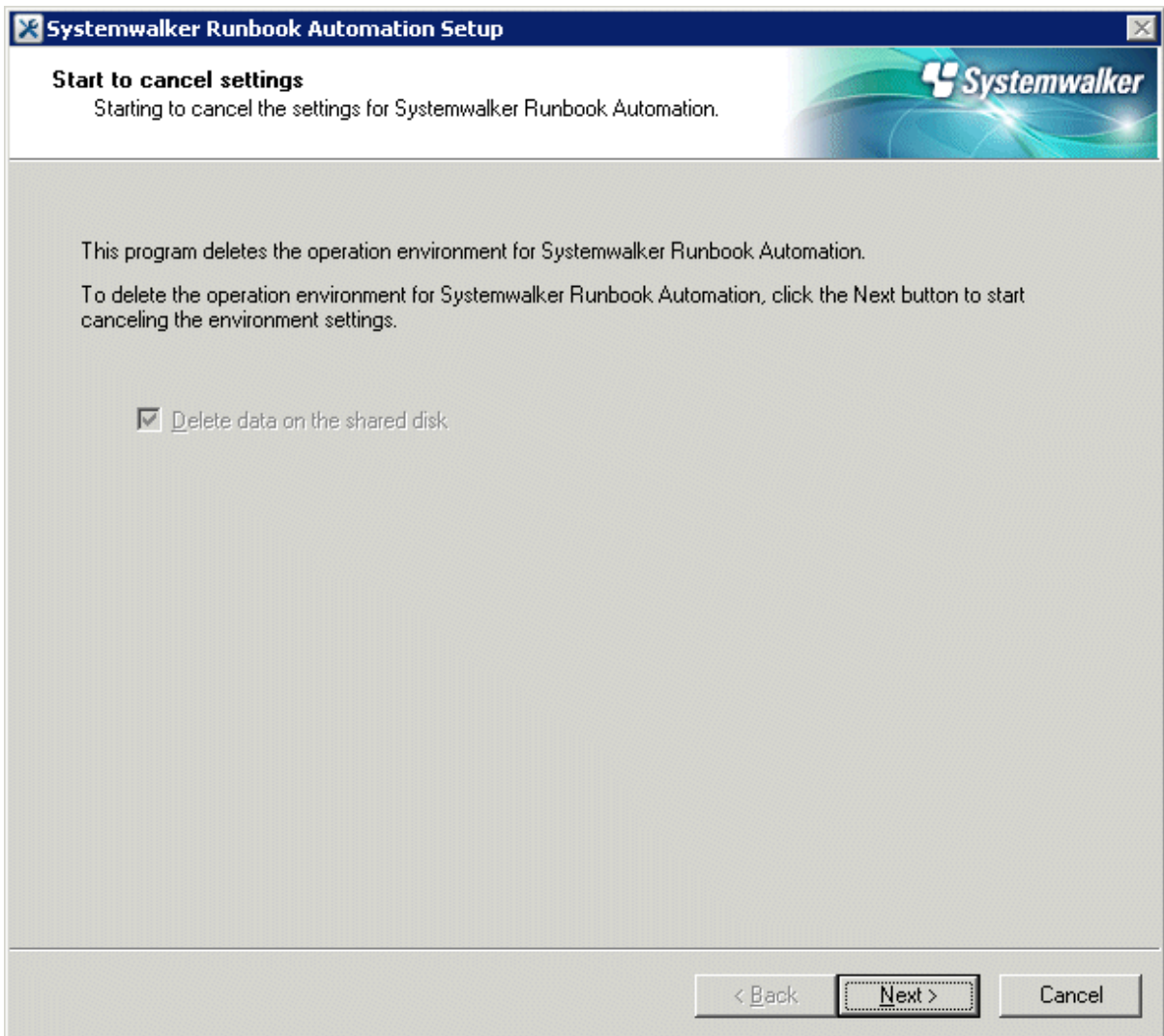
4. Click the **Yes** button.
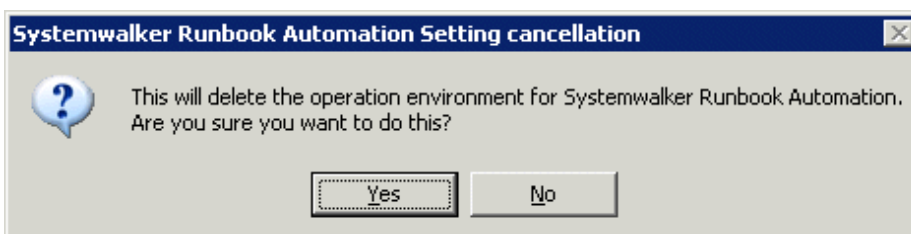
5. Setup cancellation will start.
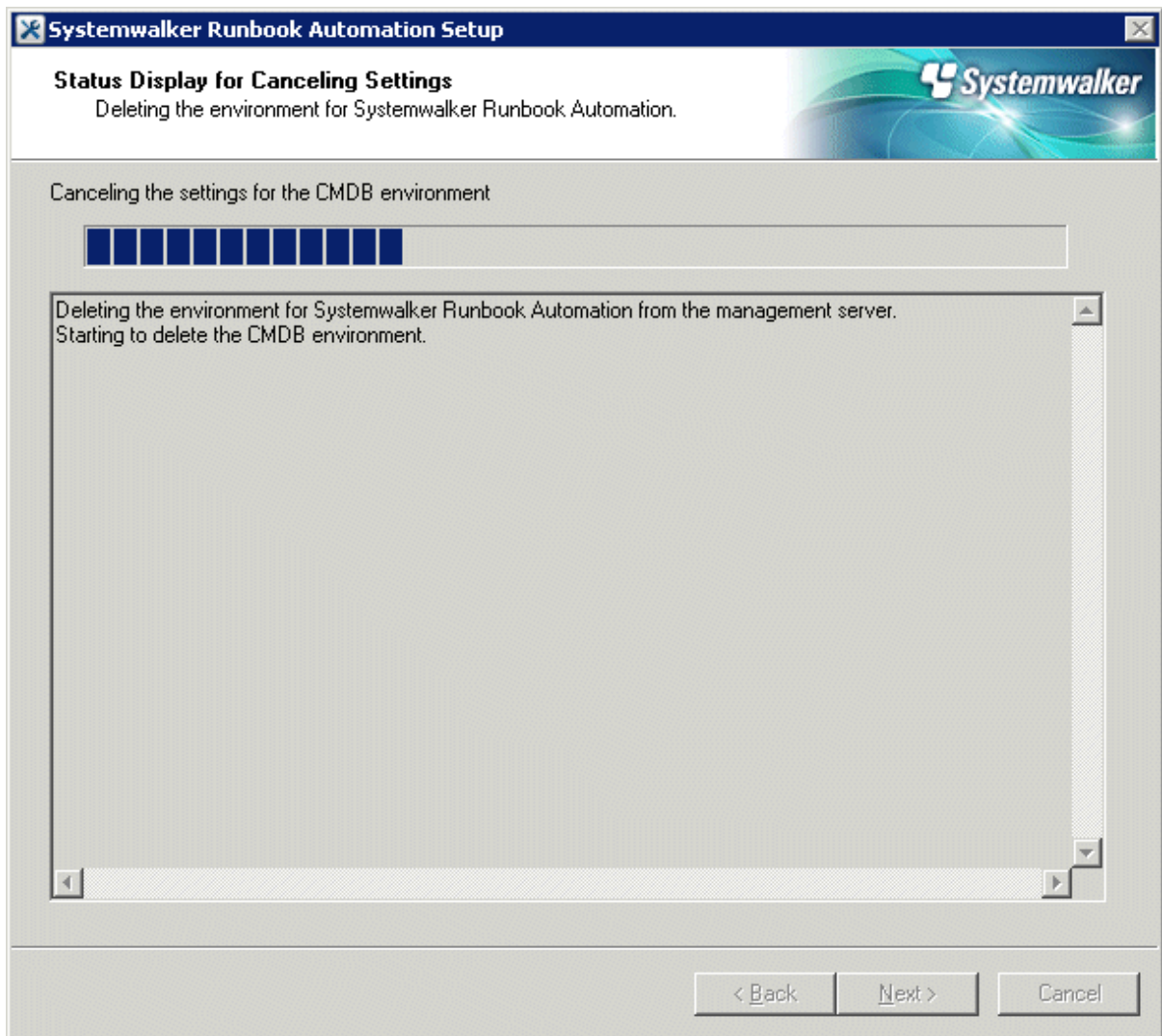
6. Setup cancelation will complete.

   Click the **Finish** button.
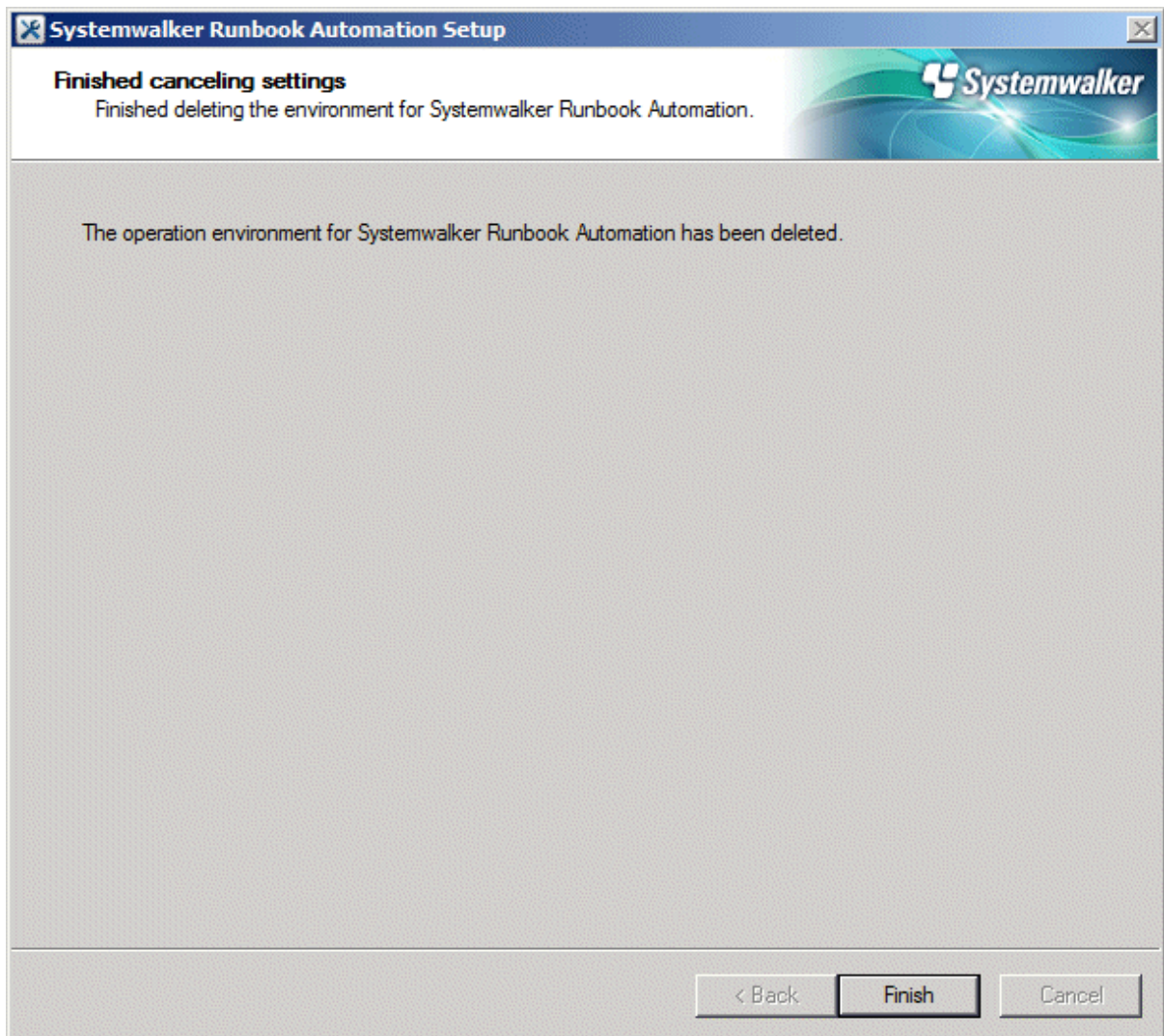
Note

If an error occurs during the cancellation of the setup

Take the appropriate action based on the message displayed, and then cancel the setup again.

If it still fails, then follow the steps below to uninstall each product:

1. Cancel the setup for the CMDB.

   [Windows]

   Depending on the error status, an error may occur at this step because the setup cancellation has already completed, but it can be ignored.

   ```
   "%SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\cmdbunsetupenv.bat" -k ALL
   ```

   ```
   "%SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\cmdbunsetupenv.bat" -k MGR
   ```

2. Uninstall Systemwalker Runbook Automation.

   Refer to "7.2.1.1 Uninstalling Systemwalker Runbook Automation" for details.

6.2.3 Deleting the Environment for Systemwalker Runbook Automation [Linux]

Follow the steps below to delete the Systemwalker Runbook Automation environment:

1. Execute the following command to start Systemwalker Runbook Automation setup:

```
# /opt/FJSVswrbam/bin/swrba_setup -u
```

2. At the prompt for setup cancellation confirmation, enter "y":

```
================================================================================
        Systemwalker Runbook Automation Setup Tool
                                V15.1.0
                                Copyright FUJITSU LIMITED 2010-2012
================================================================================
Starting to cancel setup for Systemwalker Runbook Automation.

Do you want to start the unsetup? [y:yes/n:no]
```

```
ENTER==>y
```

3. Setup cancellation will start.

   The message below will be displayed:

```
Deleting the environment for Systemwalker Runbook Automation from the management server.
```

```
Starting to delete the CMDB environment.
Deletion of the CMDB environment is now complete.
Canceling the environment settings for Systemwalker Runbook Automation.
The environment settings for Systemwalker Runbook Automation have been canceled.
Deletion of the Process Management Database is about to start.
Deletion of the Process Management Database is now complete.
The environment for Systemwalker Runbook Automation has been deleted from the management server.
```

4. Setup cancellation will complete.

   At the prompt, press **Enter** key.

   If an error occurs, take the appropriate action based on the message displayed, and then cancel the setup again.

   If it still fails, then follow the steps below to uninstall each product.

   1. Cancel the setup for the CMDB.

      Depending on the error status, an error may occur at this step because the setup cancellation has already completed, but it can be ignored.

      /opt/FJSVcmdbm/bin/cmdbunsetupenv.sh -k ALL

      /opt/FJSVcmdbm/bin/cmdbunsetupenv.sh -k MGR

   2. Uninstall Systemwalker Runbook Automation.

      Refer to "7.2.1.1 Uninstalling Systemwalker Runbook Automation" for details.

6.2.4 Deleting the Users, Groups and Organizational Units

The resources in the LDAP directory listed in the table below will be no longer required after setup cancellation, and can therefore be deleted.

The table lists the default values - if other values were specified during setup, then delete the corresponding users.

Type	Name
User	swrbaadmin

Type	Name
User	swrbasch
Group	AdminRole
Group	IflowUsers
Group	IflowGroups
Group	Role
Group	swrba_Exe
Organizational unit (*1)	Group
Organizational unit (*1)	USER

***1:** Ensure that there are no users or groups on the organizational unit before deleting it

6.2.5 Cancelling Setup of Interstage Single Sign-On

This chapter explains how to cancel Interstage Single Sign-On.

A flow of procedures required to cancel Interstage Single Sign-On and cancel the settings is shown below:
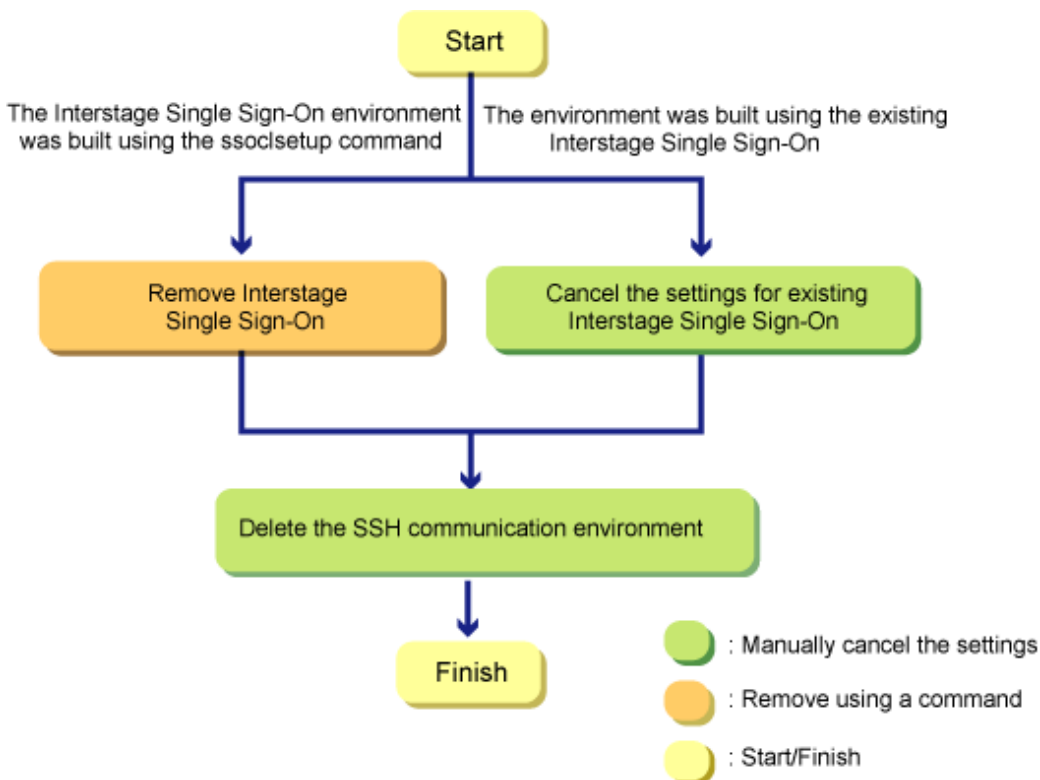
Note

The procedures explained in this chapter must be executed with administrator privileges.

6.2.5.1 Cancel setup Interstage Single Sign-On

This chapter explains how to cancel setup Interstage Single Sign-On.

> **Note**
>
> ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯
> Cancel setup Interstage Single Sign-On after setup removal is completed for Systemwalker Runbook Automation.
> ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

Execute the cancel setup command of Interstage Single Sign-On (hereafter referred to as the ssoclunsetup command) to cancel setup Interstage Single Sign-On.

The following Interstage Single Sign-On resources are deleted when the ssoclunsetup command is executed:

- The following Interstage Single Sign-On servers:

    - Repository server (update type)

    - Authentication server

    - Business server (*1)

- SSO repository referenced by the repository server (update type)

- Web server that built the repository server (update type) and the authentication server (*2)

*1: The ssoclunsetup command deletes all business servers for Interstage Single Sign-On built on the machine where it is executed. Note, however, that the Web server itself will not be deleted.

*2: Only the Web server (Web server name: SSOauth) that built the repository server (update type) and the authentication server will be deleted. Other Web servers will not be deleted.

> **Note**
>
> ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯
> Refer to *ssoclunsetup* (*Interstage Single Sign-On cancelling setup command*) in the *Systemwalker Runbook Automation Reference Guide* for information on the ssoclunsetup command.
> ⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯⋯

Procedure for deletion

1. Execute the ssoclunsetup command:

   [Windows]

   ```
   ssoclunsetup
   ```

   The ssoclunsetup command is located in the following folder:

   ```
   < Systemwalker Runbook Automation management server installation directory] \sso\bin
   ```

   [Linux]

   ```
   /opt/FJSVctsec/sso/bin/ssoclunsetup
   ```

2. Confirm the deletion.

   A message confirming the deletion of Interstage Single Sign-On will be displayed after executing the ssoclunsetup command. To delete, enter "yes". If a string other than "yes" is entered, "Command canceled" will be displayed and Interstage Single Sign-On will not be deleted.

3. A message containing the resource status will be displayed.

   The status of resources to be deleted will be displayed in a message after executing the ssoclunsetup command. A description of the resources is shown below:

Resource name	Description
Repository Server	Repository server (update type)
Authentication Server	Authentication server
Business Server	Business server

Resource name	Description
Web Server (Web server name)	Web server that built the repository server (update type) and the authentication server The default setting for Web server name is "SSOauth"
SSO Repository (repository name)	SSO repository referenced by the repository server (update type)

The status of resources is displayed in the following messages:

Message	Resource status
Exist	Exist
Not exist	Do not exist

Note

- After the ssoclunsetup command is completed, the Web server (Interstage HTTP Server) where the business servers were added will not be started.

- If the ssoclunsetup command is executed when there are no resources to be deleted, the command still completes successfully.

Execution example

[Windows]

```
ssoclunsetup
Repository Server         : Exist
Authentication Server     : Exist
Business Server           : Exist
Web Server (SSOauth)      : Exist
SSO Repository (rep001)   : Exist
Are you sure to delete the Single Sign-on system? (yes/no) yes
IHS: INFO: ihs01000: The command terminated normally.
IREP: INFO: irep70002: Repository environment deleted. [rep001]
```

[Linux]

```
#/opt/FJSVswrba/sso/bin/ssoclunsetup
Repository Server         : Exist
Authentication Server     : Exist
Business Server           : Exist
Web Server (SSOauth)      : Exist
SSO Repository (rep001)   : Exist
Are you sure to delete the Single Sign-on system? (yes/no) yes
UX : IHS: INFO : ihs01000: The command terminated normally
UX : IREP: INFO : irep70002: Repository environment deleted. [rep001]
```

6.2.5.2 Cancel Settings for Existing Interstage Single Sign-On

This section explains how to cancel the settings for existing Interstage Single Sign-On

6.2.5.2.1 Disable Contents Cache Inhibition

. Deactivate the Web browser contents cache settings using the following procedure:

1. Start the Interstage Management Console.

    1. Start the Web browser.

2. Specify the Interstage Management Console URL.

When SSL encrypted communication is not used: http://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

When SSL encrypted communication is used: https://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

3. Login to the Interstage Management Console.

2. Stop the Web server.

On the Interstage Management Console, select **System** >> **Services** >> **Web Server** >> **FJapache** to display **FJapache: Status**, then click the **Stop** button.

3. Update the environment definition file of the business server.

The environment definition file of the business server must be updated using the Editor.
The location and the file name of the environment definition file of the business server are shown below:

[Windows]

```
<Interstage Application Server installation folder>\F3FMsso\ssoatzag\conf\ssoatzag.conf
```

[Linux]

```
/etc/opt/FJSVssoaz/conf/ssoatzag.conf
```

Delete the line "http-cache-cntl=NO" in the above file.

4. Start the Web server.

Select **System** >> **Services** >> **Web Server** >> **FJapache** to display **FJapache: Status**, then click the **Start** button.

6.2.5.2.2 Delete Business System

On the Interstage Management Console, follow the procedure below to delete the business system of Interstage Single Sign-On.

1. Start the Interstage Management Console.

   Refer to 6.2.5.2.1 Disable Contents Cache Inhibition for information on how to start the Interstage Management Console.

2. Stop the Web server.

   Select **System** >> **Services** >> **Web Server**, and select the check box showing **FJapache** as the Web server name, then click the **Start** button.

3. Display the business system.

   Select **System** >> **Security** >> **Single Sign-on** >> **Business system**, and open **List**.

4. Delete the business system.

   From the business system where **FJapache** is specified as the Web server name, select the check box showing the business system name to be deleted, and click the **Delete** button.

5. Start the Web server.

   Select **System** >> **Services** >> **Web Server** >> **FJapache** to display **FJapache: Status**, then click the **Start** button.

6.2.5.2.3 Delete Site Definitions

On the Interstage Management Console, follow the procedure below to delete the site definitions:

1. Start the Interstage Management Console.

   Refer to 6.2.5.2.1 Disable Contents Cache Inhibition for information on how to start the Interstage Management Console.

2. Delete the site definitions.

Select **System** >> **Security** >> **Single Sign-on** >> **Authentication infrastructure** >> **Repository server** >> **Protection resource**, and open [**Protection resource: List**]. Select the site definitions registered when Interstage Single Sign-On was built, and click the **Delete** button.

6.2.5.3 Deleting the SSH Communication Environment

This section explains the deletion of the SSL communication environment.

📕 **Note**
. . . .
This task is not necessary if SSL communication is also used in cases other than Interstage Single Sign-On.
. . . .

6.2.5.3.1 Clearing the Settings for SSL Communication

Using the Interstage Management Console, delete the SSL definition.

1. Start the Interstage Management Console.

    1. Start the Web browser.

    2. Specify the Interstage Management Console URL.

        When SSL encrypted communication is not used: http://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

        When SSL encrypted communication is used: https://[*host name of the Management Server*]:[*port number for the Interstage Management Console*]/IsAdmin/

    3. Login to the Interstage Management Console.

2. Delete the SSL definition.

    Select **System** >> **Security** >> **SSL** to display the list of SSL definitions. Select the desired SSL definition, then click the **Delete** button.

6.2.5.3.2 Deleting Certificates used in SSL Communication

Delete the site certificate used in SSL communication, and the private key or CA certificate for that site certificate, from the Interstage certificate environment.

📕 **Note**
. . . .
- When the site certificate is deleted, the private key for that site certificate will also be deleted. Once a private key has been deleted, it cannot be registered again as a site certificate. Also, when a CA certificate is deleted, CA certificates and site certificates issued by that CA cannot be used. For this reason, take care when deleting certificates.

- It will not cause any problems if expired certificates that cannot be used any more are not deleted.
. . . .

Deletion procedure

The command execution examples shown below use the following settings values:

```
 Site certificate nickname:SERVERCERT
```

[Windows]

```
C:\> scsdelete -n SERVERCERT
Password:
SCS: INFO: scs0103: The certificate was deleted.
```

[Linux]

```
# scsdelete -n SERVERCERT
Password:
SCS: INFO: scs0103: The certificate was deleted.
```

6.2.6 Points to Note after Canceling the Setup

This section describes points that require attention after the cancelling the setup.

If an error occurred

If an error occurs during the setup cancellation, take the following action.

1. Uninstall Systemwalker Runbook Automation.

   Refer to "7.2.1.1 Uninstalling Systemwalker Runbook Automation".

2. To recreate an environment for Systemwalker Runbook Automation, it is necessary to install it.

   1. Install Systemwalker Runbook Automation.

      Refer to "Chapter 2 Installation" for details.

   2. Set up the Management Server.

      Refer to "3.1 Setting up the Management Server" for details.

6.3 Canceling the Setup for Linked Servers and Relay Servers

This section describes how to cancel the setup for Agents.

Refer to the *Systemwalker Runbook Automation Cluster Setup Guide* for information on canceling the setup for Systemwalker Runbook Automation cluster environments.

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the setup cancellation process as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

Executing the setup cancellation command

[Windows]

1. If the Agent service is running, then stop it:

   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop

2. Cancel the setup:

   <agent installation directory>\CMDB\FJSVcmdba\bin\cmdbunsetupenv.bat -k <agent type>

   For *<agent type>*, specify the type of Agent for which the setup is to be canceled (it must be a type of an Agent that has been set up):

   - AGT_CENTINV: Agent for collecting inventory information for Systemwalker Centric Manager

   - AGT_CENTREP: Agent for collecting node information for Systemwalker Centric Manager

   - AGT_INV: Agent for automatically collecting inventory information for servers connected to the network

   - AGT_ADSC: Agent for automatically collecting node

- ALL: All Agents that have been set up.

3. If there is another Agent on the target server that has been set up, then start the Agent:

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
```

[Linux]

1. Stop the Agent:

```
/opt/FJSVswnc/bin/swncctrl stop
```

2. Cancel the setup:

```
/opt/FJSVcmdba/bin/cmdbunsetupenv.sh -k <agent type>
```

For <*agent type*>, specify the type of Agent for which the setup is to be canceled (it must be a type of an Agent that has been set up):

- AGT_CENTINV: Agent for collecting inventory information for Systemwalker Centric Manager

- AGT_CENTREP: Agent for collecting node information for Systemwalker Centric Manager

- AGT_INV: Agent for automatically collecting inventory information for servers connected to the network

- AGT_ADSC: Agent for automatically collecting node

- ALLL: All Agents that have been set up.

3. If there is another Agent on the target server that has been set up, then start the Agent:

```
/opt/FJSVswnc/bin/swncctrl start
```

Changing the execution privileges for the service [Windows]

If the setup for the Agent for Systemwalker Centric Manager has been canceled, restore the execution privileges for the Agent service to the original account. However, if the execution privileges for the Agent service were not changed when the Agent for Systemwalker Centric Manager was set up (that is, if the version of Systemwalker Centric Manager to link to is V13.3.0 or later), no change is necessary.

1. If the Agent service is running, then stop it:

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
```

2. Open the Windows **Services** dialog box.

3. Open the **Properties** window for the "Systemwalker Jservlet (SWNET)" service.

4. Select **This account** in the **Log On** tab of the **Properties** window, and set it to "LocalSystem".

5. If the Agent service has been stopped, then start:

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
```

6.4 Cancel the Setup of the Business Server

Cancel the setup according to the setup performed for the business server during installation.

6.4.1 Clearing the SSH Communication Settings

If SSH was installed and the settings added in order to use Systemwalker Runbook Automation, and SSH communication is only required for Systemwalker Runbook Automation, then clear the settings using the following procedure:

1. Stop the SSH service.

2. Clear the port settings used in SSH communication for the firewall.

```
Port used in SSH: 22/TCP
```

3. If an account was added for SSH communication, delete unnecessary accounts.

4. Uninstall OpenSSH.

If OpenSSH has been installed but it is no longer necessary, uninstall it. If you are using Linux and SSH was installed as a standard function of the operating system, then there is no need to uninstall it.

6.4.2 Uninstalling SNMP Agent

If SNMP Agent has been installed and SNMP Agent is only required for Systemwalker Runbook Automation, then uninstall it using the following procedure:

1. Stop the SNMP service.

2. Clear the port settings used in SNMP Agent for the firewall.

```
Port used in SNMP Agent: 161/tcp
```

3. Uninstall SNMP Agent.

4. Refer to "3.4.1 Installing SNMP Agents" for information on the installation and setup content. Additionally, refer to each operating system manual for information on how to uninstall SNMP Agent, for example.

6.4.3 Uninstalling the IT Resource Information Collection Program

To uninstall the IT resource information collection program, follow the procedure shown below.

1. If the file transfer infrastructure is being used, then stop its service.

If an operation component that will use the file transfer infrastructure is being used, stop the file transfer infrastructure service.

[Windows]

```
C:\FJSVcmdbi\bin\fcmdb_inv_lnkunsetup.bat
```

[Linux]

```
service FJSVcmdbi_rcvctl stop
```

[Solaris]

```
/etc/init.d/FJSVcmdbi_rcvctl stop
```

2. Uninstall the IT resource information collection program.

[Windows]

Delete the following folder:

```
C:\FJSVcmdbi
```

[Linux]

Execute the following command:

```
rpm -e FJSVcmdbi
```

[Solaris]

Execute the following command:

```
pkgrm FJSVcmdbi
```

Chapter 7 Uninstallation

This chapter describes how to uninstall Systemwalker Runbook Automation.

- Pre-uninstallation notes

- Uninstallation procedure

- Post-uninstallation notes

7.1 Pre-uninstallation Notes

Note the following points when uninstalling Systemwalker Runbook Automation.

Before uninstalling the Management Server

Deleting the environment

- Before uninstalling Systemwalker Runbook Automation, the environment setup for Systemwalker Runbook Automation must be canceled. Refer to "Chapter 6 Setup Cancellation" for details.

- If the Systemwalker Centric Manager Operation Management Server has been installed, stop all Systemwalker Centric Manager functions (refer to the Systemwalker Centric Manager manuals for details on how to stop them).

Before uninstalling the Development Computer

Deleting the environment

Before uninstalling the Systemwalker Runbook Automation Development Computer, Systemwalker Runbook Automation must be stopped (refer to the *Systemwalker Runbook Automation BPM Studio User's Guide* for details).

7.2 Uninstallation Procedure

This section describes how to uninstall Systemwalker Runbook Automation.

7.2.1 Uninstalling the Management Server

This section describes how to uninstall the Systemwalker Runbook Automation Management Server.

7.2.1.1 Uninstalling Systemwalker Runbook Automation

This section explains how to uninstall Systemwalker Runbook Automation.

Uninstalling the Windows version of Systemwalker Runbook Automation

Uninstalling the Linux version of Systemwalker Runbook Automation

Note

- It is not possible to uninstall only Systemwalker Runbook Automation if any of the software below is installed in an environment where a Systemwalker Runbook Automation Management Server is installed - first, uninstalling the software below, then uninstall Systemwalker Runbook Automation:

  - ServerView Resource Orchestrator

  - Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager

  Refer to "ServerView Resource Orchestrator Installation Guide" for information on how to uninstall ServerView Resource Orchestrator.

Refer to *Cloud Infrastructure Management Software Users Guide* for information on how to uninstall the Cloud Infrastructure Management Software. Refer to "Uninstall" in the *Systemwalker Software Configuration Manager Operation Guide* for information on how to uninstall Systemwalker Software Configuration Manager.

Uninstalling the Windows version of Systemwalker Runbook Automation

📌 Note

- If an error occurs during uninstallation, refer to the *Systemwalker Runbook Automation Message Guide* for information on meanings and action methods for the messages that are output, and eliminate the cause of the error. Then, retry the uninstallation process.

  If the problem cannot be addressed based on the message that is output, collect the following log file from the directory indicated by the %SystemDrive% environment variable and contact Fujitsu technical support.

  - swrba_uninst.log

1. Log in using an account that belongs to the Administrators group.

2. Stop the Agent:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
   ```

3. Start the uninstaller.

   Select [Fujitsu]-[Uninstall] and Management (middleware) on [Start] menu - [Program] or [All programs]
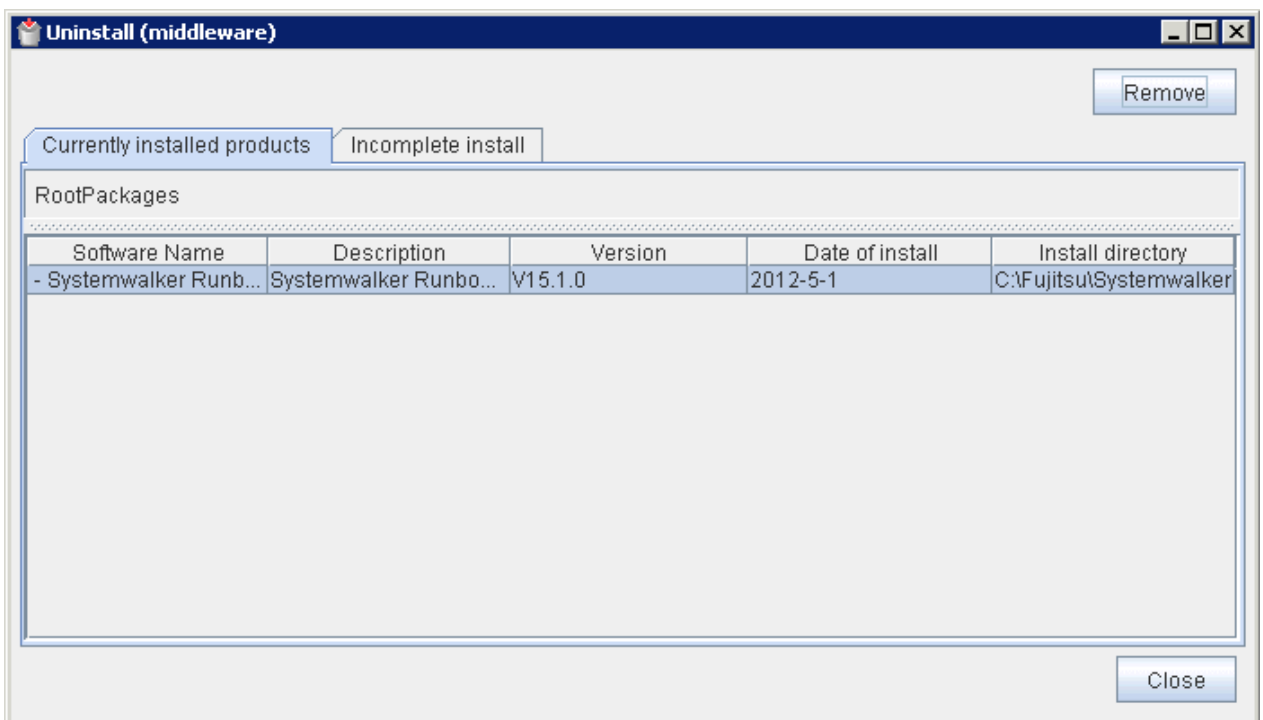
📌 Note

If failed to install Systemwalker Runbook Automation and to uninstall it, Systemwalker Runbook Automation may be displayed on [Install tab].

4. Select Systemwalker Runbook Automation (Management Server)], and click the [[delete] button.

   If it is OK to delete, click the [uninstall] button.
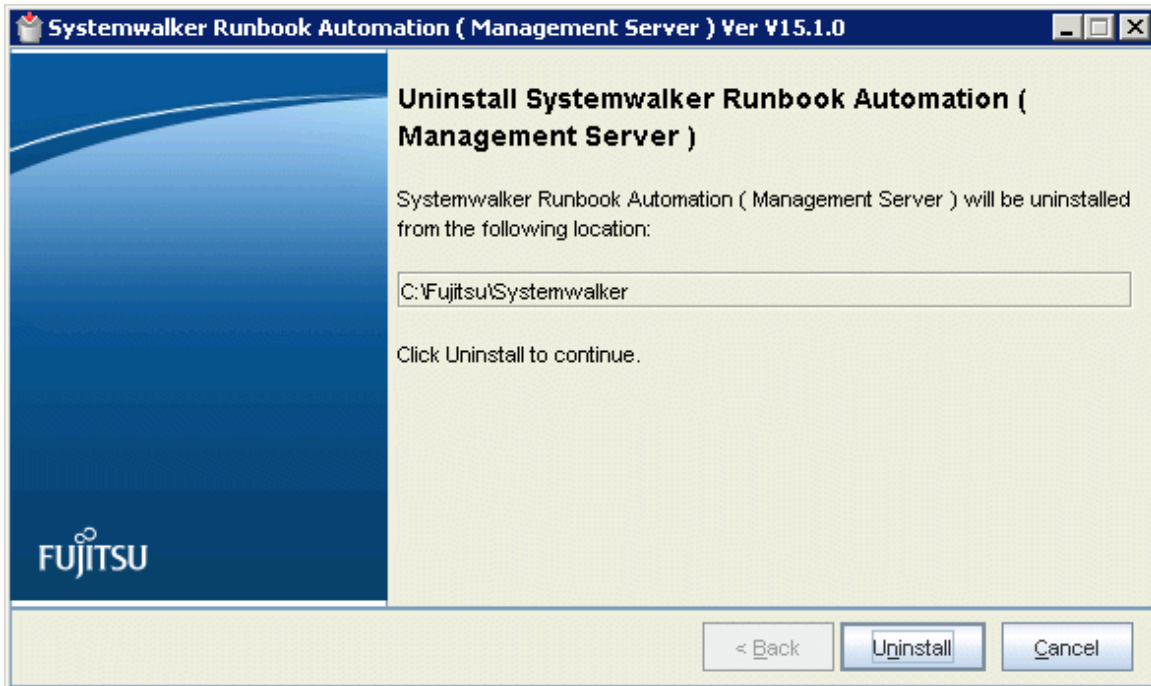
5. If uninstall is completed, click the [finish] button and uninstaller be done.

6. Restart it. Click [Yes].
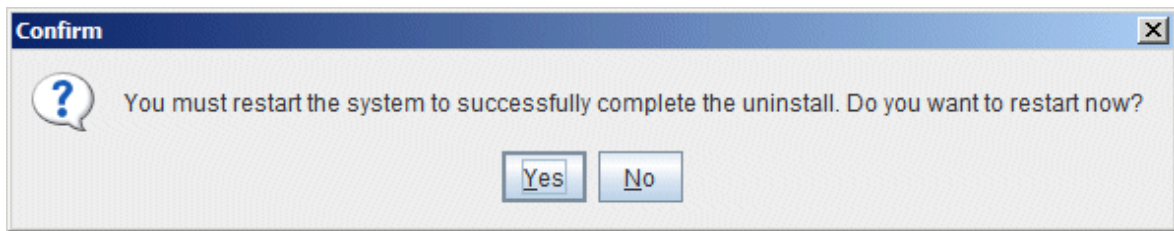
Uninstalling the Linux version of Systemwalker Runbook Automation

📝 **Note**

. . . .

If an error occurs during uninstallation, refer to the *Systemwalker Runbook Automation Message Guide* for information on meanings and action methods for the messages that are output, and eliminate the cause of the error. Then, retry the uninstallation process.

If the problem cannot be resolved based on the messages that are output, collect the following log files and contact Fujitsu technical support.

 - /var/tmp/swrba_inst.log

 - /var/tmp/swrba_uninst.log

 - /var/tmp/bndl_uninst.log

 - /var/tmp/bndl_inst.log

 - /var/tmp/symfoware_sv.log

 - /opt/FJSVcmdbm/var/log/cmdbInstLog

 - /tmp/cmdbInstLog

 - /opt/FJSVibpm/Interstage-BPM-log.txt

. . . .

1. Log in as a superuser on the system.

2. Stop the Agent:

```
# /opt/FJSVswnc/bin/swncctrl stop
```

3. If the CORBA Service is running, then stop it:

```
# isstop -f
```

4. If the service for using the Interstage Management Console is running, then stop it:

```
# ismngconsolestop
```

5. If the Interstage HTTP Server Service is running, stop it. Execute the following command:

```
# /opt/FJSVihs/bin/ihsstop -all
```

6. If the Interstage Java EE DAS Service is running, stop it. Execute the following command:

```
# /opt/FJSVisjee/bin/ijdasstop
```

7. If the Interstage Java EE Node Agent Service is running, stop it. Execute the following command:

```
# /opt/FJSVisjee/bin/ijnastop
```

8. If the Interstage Directory Service is being used, then stop all repositories.

   Use ireplist to check which repositories are running, and then, use irepstop to stop them.

```
# ireplist
No Repository Status
-- ---------- --------
 1 rep001    Active
# irepstop -R rep001
```

9. Start the uninstaller:

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

10. The Selection window of software uninstallation will be displayed.

    Select Systemwalker Runbook Automation (Management Server). If Select "q" to close the uninstaller "1

```
Loading Uninstaller...


Currently installed products.
1. Systemwalker Runbook Automation (Management Server) V15.1.0

Type [number] to select the software you want to uninstall.
[number,q]
=>1
```

11. Check the installation settings.

    Ensure that the settings are correct, and enter "y". If a setting must be corrected, then enter "b" to go back to the previous window.

```
 Systemwalker Runbook Automation (Management Server)
    Description: Systemwalker Runbook Automation (Management Server)
    Version: V15.1.0
    Manufacture: Fujitsu Limited
    Install directory: /opt
    Date of Installation: 2012-6-8



Starting the uninstall of the software. Are you sure you want to continue?
[y,b,q]
```

12. Uninstallation will start.

```
Uninstalling...

The following products have been uninstalled successfully.:
    Systemwalker Runbook Automation (Management Server)
```

13. Uninstallation will complete.

    The message below will be displayed.

```
Exiting Uninstaller.
```

7.2.1.2 Uninstalling the Fujitsu XML Processor [Windows]

This section describes how to uninstall the Fujitsu XML Processor.

Note

· ·

Ensure that no other products are using the Fujitsu XML Processor before uninstalling it.

The old version of the Fujitsu XML Processor may be displayed in the **Add or Remove Programs** dialog box (for Windows Server 2008, this is the **Programs and Features** dialog box). If this application is not required, uninstall it as well.

· ·

1. Log in using an account that belongs to the Administrators group.

2. Start the uninstaller.

   Click **Start** >> **Control Panel** >> **Program and Features**.

   Select **Fujitsu XML Processor V5.2.4**, and click the **Uninstall** button.

   Note

   If the operating system is Windows Server 2008, from the **Start** menu click **Control Panel >> Uninstall or change a program**, select "Fujitsu XML Processor V5.2.4", then click the **Uninstall** button.

3. Click the **OK** button:
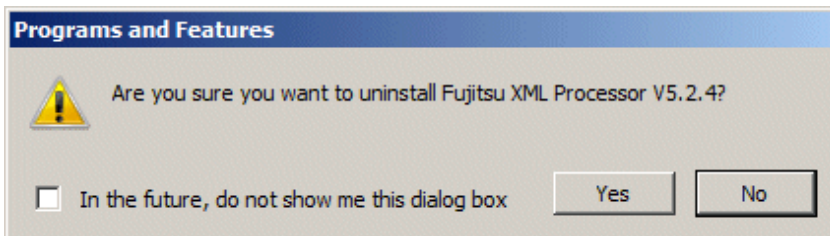
4. Uninstallation will start.

   The program removal window will be displayed, and the program will be deleted, together with its information in the registry.

7.2.1.3 Uninstalling SMEE [Linux]

This section describes how to uninstall SMEE.

Note

Ensure that no other products are using SMEE before uninstalling it.

1. Log in as a superuser on the system.

2. Remove the FJSVsmee package:

   ```
   # rpm -e FJSVsmee
   ```

7.2.1.4 Uninstalling Securecrypto Library RunTime [Linux]

This section describes how to uninstall Securecrypto Library RunTime.

Note

Ensure that no other products are using Securecrypto Library RunTime before uninstalling it.

1. Log in as a superuser on the system.

2. Remove the FJSVsclr package:

```
# rpm -e FJSVsclr
```

7.2.2 Uninstalling the Development Computer

This section describes how to uninstall the Systemwalker Runbook Automation Development Computer.

Note

Ensure that you are logged in using an account that belongs to the Administrators group on the computer where the uninstallation is to be performed.

7.2.2.1 Uninstalling Systemwalker Runbook Automation Studio

Follow the steps below to uninstall Systemwalker Runbook Automation Studio:

Note

If an error occurs during uninstallation, refer to the *Systemwalker Runbook Automation Message Guide* for information on meanings and action methods for the messages that are output, and eliminate the cause of the error. Then, retry the uninstallation process.

If the problem cannot be addressed based on the message that is output, collect the following log file from the directory indicated by the %SystemDrive% environment variable, and contact Fujitsu technical support.

- swrbastudio_uninst.log

1. Log in using an account that belongs to the Administrators group.

2. Start the uninstaller.

   Select either **Programs** or **All Programs** from the **Start** menu, and then, select **Fujitsu** >> **Uninstall (middleware).**
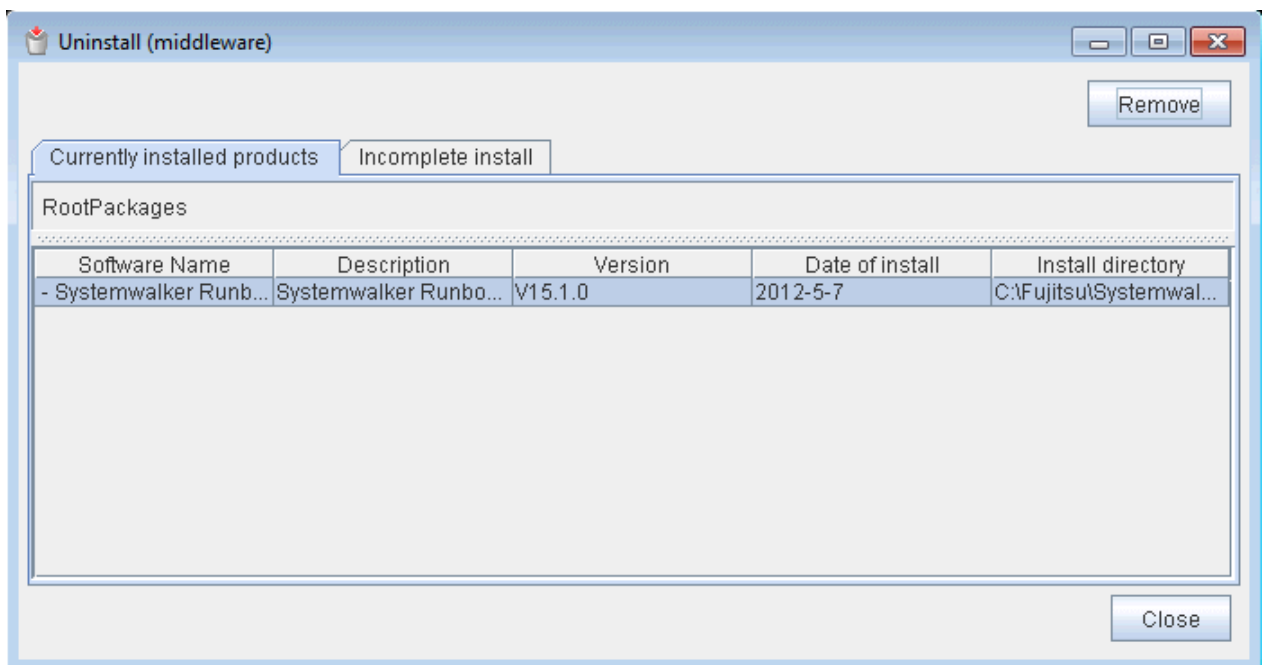
Note

Due to installation failure or for some other reason, Systemwalker Runbook Automation may be displayed in the **Incomplete install** tab. If Systemwalker Runbook Automation is not displayed in the **Currently installed products** tab, click the **Incomplete**

install tab and check if Systemwalker Runbook Automation is displayed there. The uninstallation procedure is the same even if Systemwalker Runbook Automation is displayed in the **Incomplete install** tab.

3. Select **Systemwalker Runbook Automation (Development Computer)**, and click the **Remove** button.

   If it is OK to remove the software, click the **Uninstall** button.
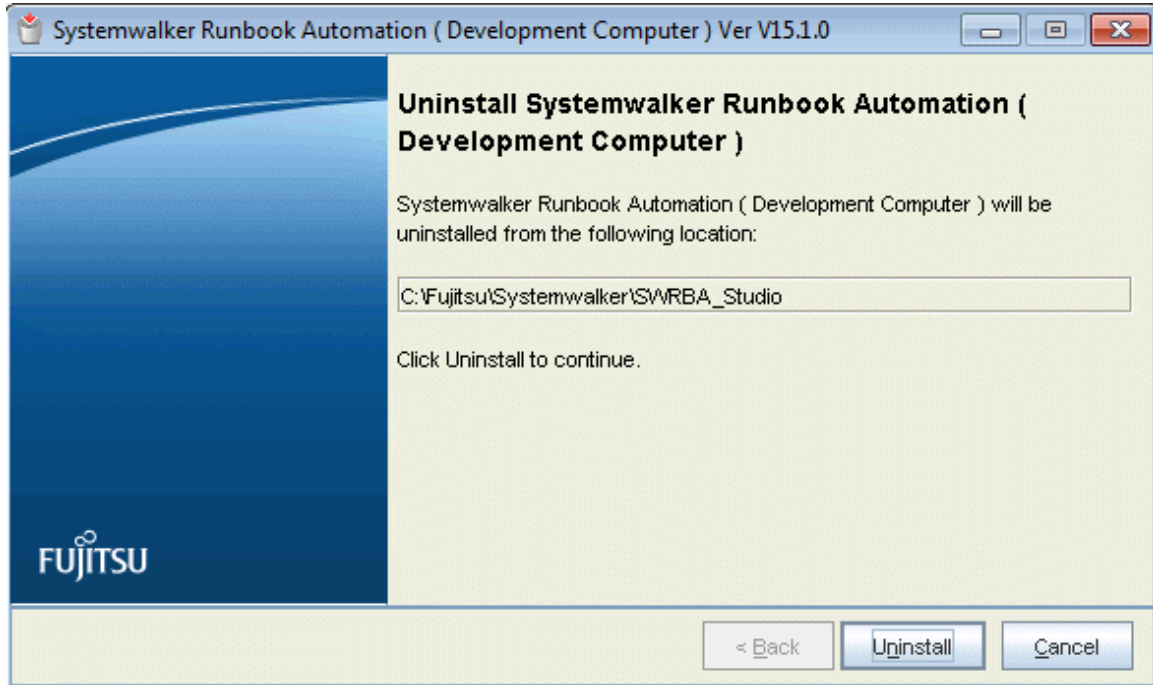
4. After the uninstallation is complete, click the **Exit** button to exit the uninstaller.
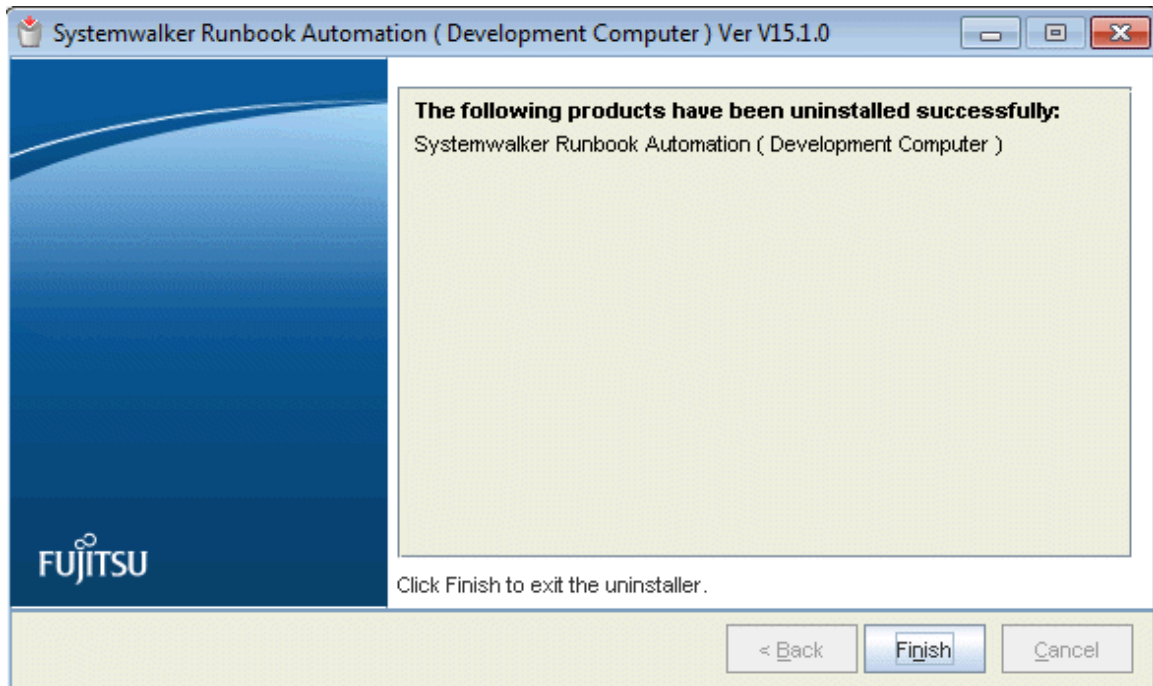
5. Restart the system.

   Click the **Yes** button.
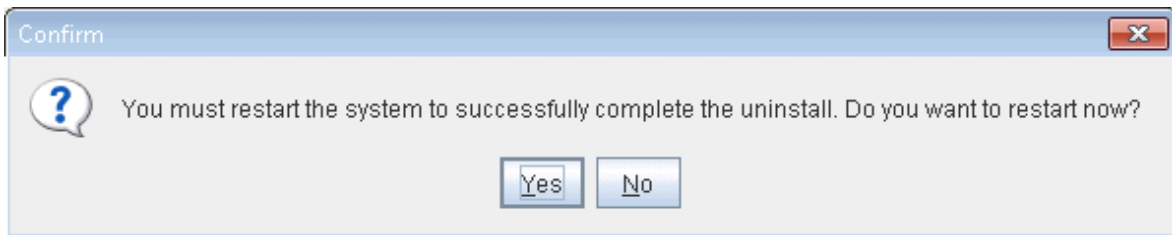
7.2.3 Uninstalling the Linked Server/Relay Server

This section describes how to uninstall the Agent from Linked Servers and Relay Servers.

7.2.3.1 Uninstalling Systemwalker Runbook Automation

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the uninstaller as an administrator.

[Linux]

- System administrator (superuser) privileges are required.

Uninstallation procedure

[Windows]

1. If the Agent is running, then stop it:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
   ```

2. Start the uninstaller.

   Select either **Programs** or **All Programs** from the **Start** menu, and select **Fujitsu**, and then, **Uninstall (middleware)**

![Note]

When uninstalling Systemwalker Runbook Automation because of installation failure or for some other reason, Systemwalker Runbook Automation may be displayed in the **Incomplete install** tab. If Systemwalker Runbook Automation is not displayed in the **Currently installed products** tab, click the **Incomplete install** tab to check that Systemwalker Runbook Automation is displayed there. The subsequent uninstallation procedure is the same even if Systemwalker Runbook Automation is displayed in the **Incomplete install** tab.

3. Select **Systemwalker Runbook Automation (Linked Server/Relay Server)**, and click the **Remove** button.
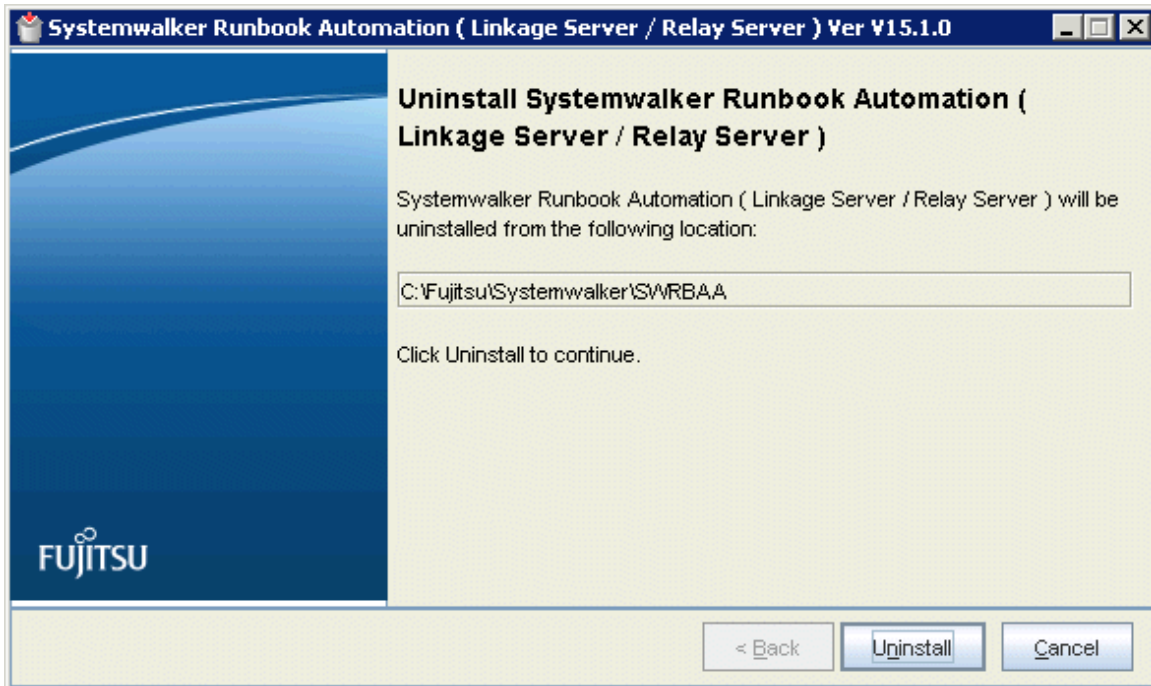
   Click the **Uninstall** button.

4. Uninstallation will complete.
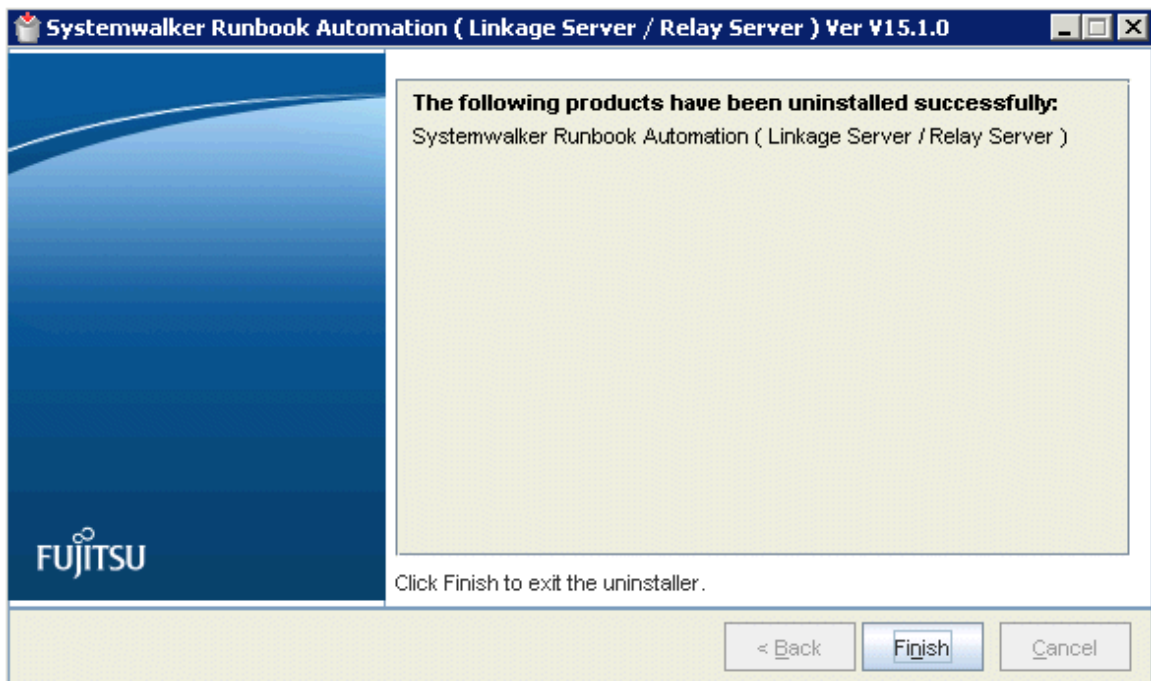
   Click the **Exit** button.

5. Restart the system.

   Click the **Yes** button.

[Linux]

1. If the Agent is running, then stop it:

```
# /opt/FJSVswnc/bin/swncctrl stop
```

2. Start the uninstaller:

```
# /opt/FJSVcir/cir/bin/cimanager.sh
```
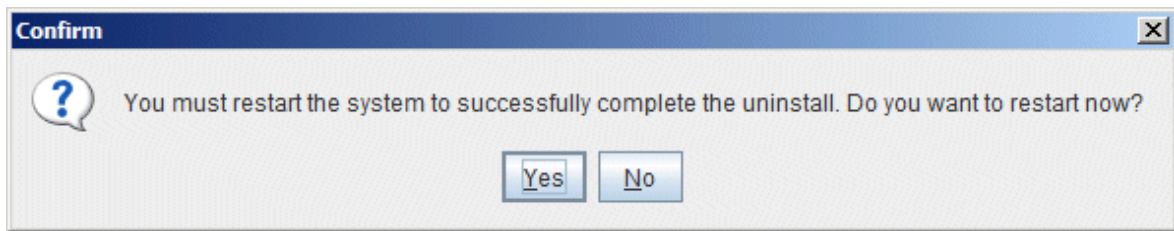
3. At the prompt for software number, enter "1":

```
Loading the Software Uninstallation and Management function.


Installed software
1. Systemwalker Runbook Automation (Linked Server/Relay Server) V15.1.0

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

4. Check the installation settings.

   Ensure that the settings are correct, and then, enter "y". If a setting must be corrected, then enter "b" to go back to the previous window.

```
Systemwalker Runbook Automation (Linked Server/Relay Server)
    Description: Systemwalker Runbook Automation (Linked Server/Relay Server)
    Version: V15.1.0
    Company name: Fujitsu Limited
    Installation directory: /opt
    Installation date: 2012-6-9


Uninstallation will start. Are you sure?
[y,b,q]
=>y
```

5. Uninstallation will start.

   The message below will be displayed:

```
Uninstallation in progress
```

6. Uninstallation will complete.

   The message below will be displayed:

```
The following software has been uninstalled:
    Systemwalker Runbook Automation (Linked Server/Relay Server)
```

```
Closing the Software Uninstallation and Management function
```

7.2.3.2 Uninstalling SMEE [Linux]

This section describes how to uninstall SMEE.

📖 Note

....

Ensure that no other products are using SMEE before uninstalling it.

....

1. Log in as a superuser on the system.

2. Uninstall the package.

   - For the 32-bit version:

   ```
   # rpm -e FJSVsmee
   ```

   - For the 64-bit version:

   ```
   # rpm -e FJSVsmee64
   ```

7.2.3.3 Uninstalling Securecrypto Library RunTime [Linux]

This section describes how to uninstall Securecrypto Library RunTime.

📖 Note

....

Ensure that no other products are using Securecrypto Library RunTime before uninstalling it.

....

1. Log in as a superuser on the system.

2. Uninstall the package.

   - For the 32-bit version:

   ```
   # rpm -e FJSVsclr
   ```

   - For the 64-bit version:

   ```
   # rpm -e FJSVsclr64
   ```

7.2.4 Uninstalling the Business Server

This section describes how to uninstall the Agent for the Business Server.

7.2.4.1 Uninstalling Systemwalker Runbook Automation

Privileges required for execution

[Windows]

- Administrator privileges are required. If the operating system being used is Windows Server 2008, execute the uninstaller as an administrator.

[Linux] [Solaris]

- System administrator (superuser) privileges are required.

Uninstallation procedure

[Windows]

1. Start the uninstaller.

   Select either **Programs** or **All Programs** from the **Start** menu, and select **Fujitsu**, and then, **Uninstall (middleware)**.
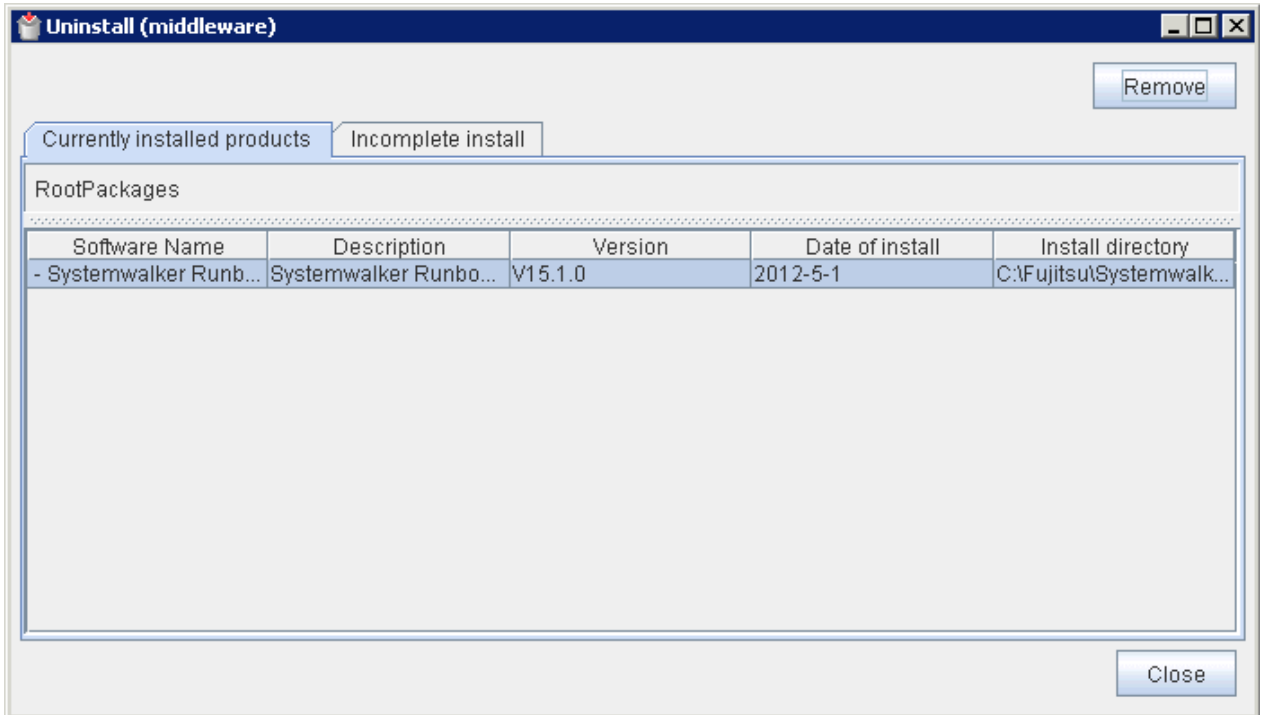
📑 Note

When uninstalling Systemwalker Runbook Automation because of installation failure or for some other reason, Systemwalker Runbook Automation may be displayed in the **Incomplete install** tab. If Systemwalker Runbook Automation is not displayed in the **Incomplete install** tab, click the **Incomplete install** tab to check that Systemwalker Runbook Automation is displayed there. The subsequent uninstallation procedure is the same even if Systemwalker Runbook Automation is displayed in the **Incomplete install** tab.

2. Select **Systemwalker Runbook Automation (Business Server)**, and click the **Remove** button.
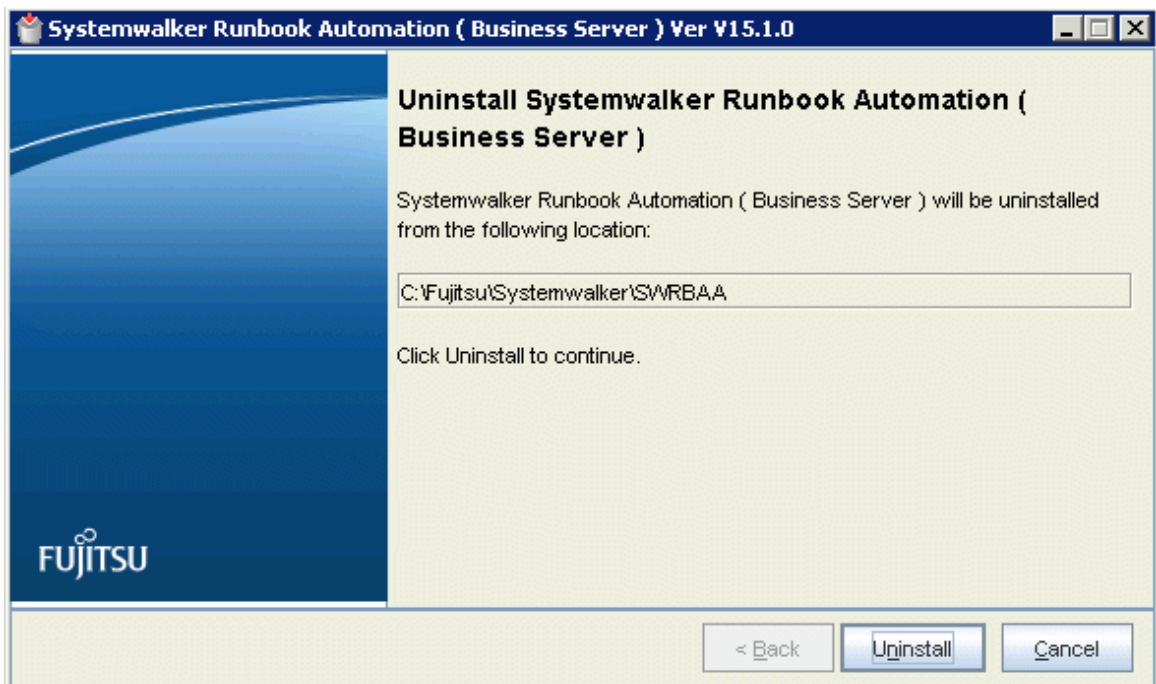
   Click the **Uninstall** button.

3. Uninstallation will complete.

   Click the **Exit** button.
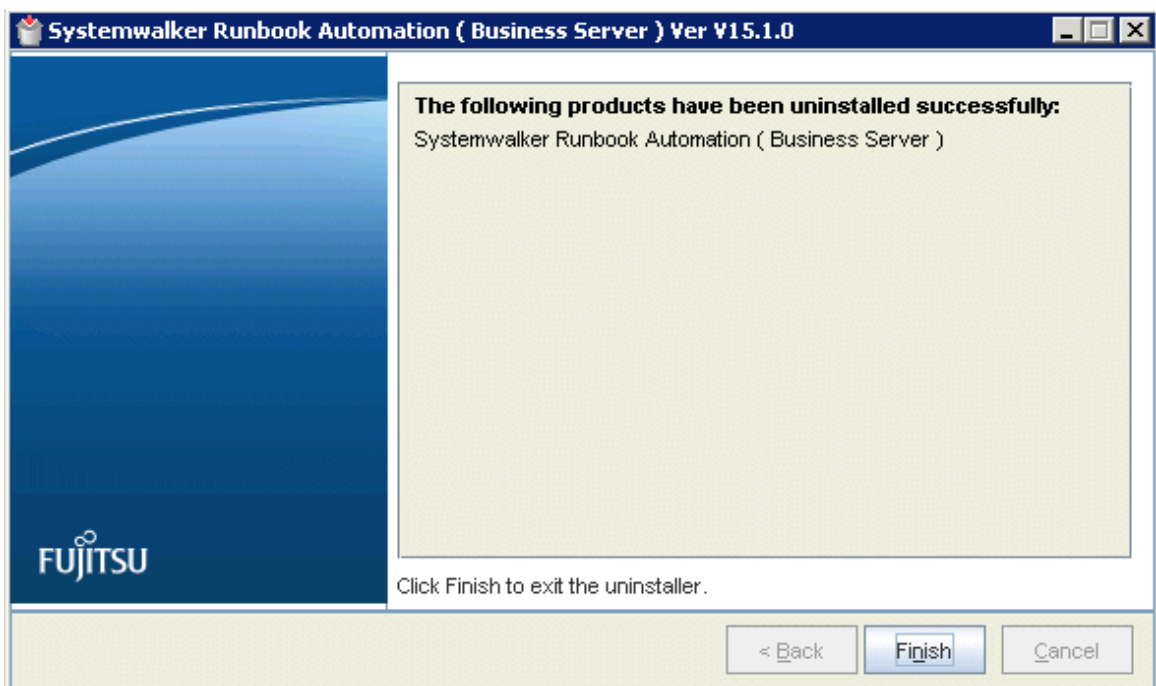
4. Restart the system.

   Click the **Yes** button.

[Linux] [Solaris]

1. Start the uninstaller.

   ```
   # /opt/FJSVcir/cir/bin/cimanager.sh -c
   ```
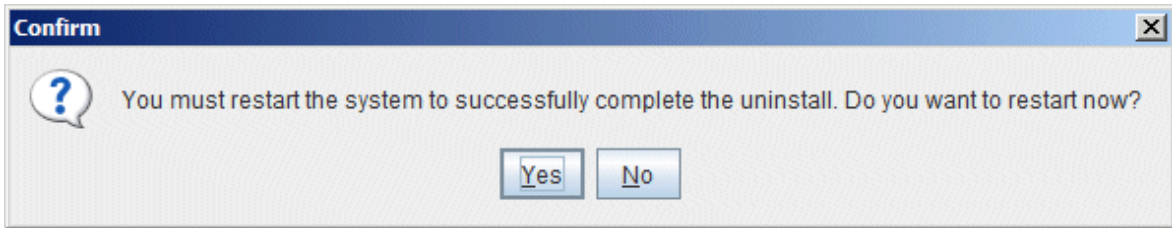
2. The select window of uninstallation products will be displayed.

   Select Systemwalker Runbook Automation (Business Server). If enter "q", uninstaller will be quit.

   ```
   Loading the Software Uninstallation and Management function.


   Installed software
   1. Systemwalker Runbook Automation (Business Server) V15.1.0

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

3. Check the installation settings.

   Ensure that the settings are correct, and then, enter "y". If a setting must be corrected, then enter "b" to go back to the previous window.

   ```
   Systemwalker Runbook Automation (Business Server)
       Description: Systemwalker Runbook Automation (Business Server)
       Version: V15.1.0
       Company name: Fujitsu Limited
       Installation directory: /opt
       Installation date: 2012-6-9


   The uninstallation process will start. Are you sure?
   [y,b,q]
   =>y
   ```

4. Uninstallation will start.

   The message below will be displayed:

   ```
   Uninstallation in progress
   ```

5. Uninstallation will complete.

   The message below will be displayed:

   ```
   The following software has been uninstalled:
       Systemwalker Runbook Automation (Business Server)


   Closing the Software Uninstallation and Management function
   ```

7.3 Post-uninstallation Notes

This section describes points to note after uninstalling Systemwalker Runbook Automation.

7.3.1 Points to Note after Uninstalling the Management Server

This section describes points to note after uninstalling the Management Server.

7.3.1.1 Points to Note after Uninstalling Systemwalker Runbook Automation

Files and directory that remain after uninstallation

Some data may remain after the uninstallation (if the files in the following directories were locked during uninstallation, for example). In this case, manually delete the files in the following directories after restarting the system.

- Systemwalker Catalog Manager

- Systemwalker Centric Manager

[Windows]

Some data may remain after the uninstallation (if the files in the following directories were locked during the uninstallation, for example). In this case, manually delete the files in the following directories after restarting the system.

- Systemwalker Runbook Automation Management Server installation directory

- Interstage Application Server installation directory

- Interstage Business Process Manager installation directory

- Systemwalker Operation Manager installation directory
  Database storage directory for the CMDB Manager

-

- If some file is looked and to not delete directory, delete it after restart operating system.

[Linux]

The directories and files below will remain after uninstallation. If they are not being used by other products and are not required, then manually delete them.

- <*root account home directory*>/InstallShield

- /etc/opt/FJSVawjbk

- /etc/opt/FJSVcmdba

- /etc/opt/FJSVcmdbm

- /etc/opt/FJSVejb

- /etc/opt/FJSVextp

- /etc/opt/FJSVihs

- /etc/opt/FJSVirep

- /etc/opt/FJSVisas

- /etc/opt/FJSVisgui

- /etc/opt/FJSVisjee

- /etc/opt/FJSVispw

- /etc/opt/FJSVisscs

- /etc/opt/FJSVj2ee

- /etc/opt/FJSVjms

- /etc/opt/FJSVjs2su

- /etc/opt/FJSVlnkbs

- /etc/opt/FJSVod

- /etc/opt/FJSVsoap

- /etc/opt/FJSVssoac

- /etc/opt/FJSVssoaz

- /etc/opt/FJSVssofs

- /etc/opt/FJSVssosv

- /etc/opt/FJSVtd

- /opt/FJSVawjbk

- /opt/FJSVcmdba

- /opt/FJSVcmdbm

- /opt/FJSVejb

- /opt/FJSVena

- /opt/FJSVextp

- /opt/FJSVibpm

- /opt/FJSVihs

- /opt/FJSVirep

- /opt/FJSVirepc

- /opt/FJSVisas

- /opt/FJSVisgui

- /opt/FJSVisjee

- /opt/FJSVispw

- /opt/FJSVj2ee

- /opt/FJSVjms

- /opt/FJSVjs2su

- /opt/FJSVlnkbs

- /opt/FJSVmqd

- /opt/FJSVod

- /opt/FJSVsoap

- /opt/FJSVssoac

- /opt/FJSVssoaz

- /opt/FJSVssocm

- /opt/FJSVssofs

- /opt/FJSVssosv

- /opt/FJSVtd (*1)

- /var/opt/FJSVawjbk

- /var/opt/FJSVcmdba

- /var/opt/FJSVcmdbm

- /var/opt/FJSVejb

- /var/opt/FJSVena

- /var/opt/FJSVextp

- /var/opt/FJSVihs

- /var/opt/FJSVirep

- /var/opt/FJSVirepc

- /var/opt/FJSVisas

- /var/opt/FJSVisgui

- /var/opt/FJSVisjee

- /var/opt/FJSVisjmx

- /var/opt/FJSVispw

- /var/opt/FJSVj2ee

- /var/opt/FJSVjms

- /var/opt/FJSVisjmx

- /var/opt/FJSVjs2su

- /var/opt/FJSVlnkbs

- /var/opt/FJSVod

- /var/opt/FJSVsoap

- /var/opt/FJSVssoac

- /var/opt/FJSVssoaz

- /var/opt/FJSVssocm

- /var/opt/FJSVssofs

- /var/opt/FJSVssosv

- /var/opt/FJSVswrbam

- /etc/opt/FJSVswrbac

- /var/opt/FJSVswrbac

- /var/opt/FJSVtd

- /etc/opt/FJSVlnkbs

- /opt/FJSVlnkbs

- /var/opt/FJSVlnkbs

- /etc/opt/FJSVisscs

- /etc/opt/FJSVtd

- /var/opt/FJSVtd

- /opt/FJSVtd

Note: If the Systemwalker Centric Manager Operation Management Server has not been installed, then /opt/FJSVtd/var/IRDB cannot be deleted.

Accounts and groups that remain after the uninstallation

- If the swadmin group is not required, then delete it.

7.3.1.2 Points to Note after Uninstalling SMEE and Securecrypto Library RunTime [Linux]

The directories and files below will remain after uninstallation. If they are not being used by other products and are not required, then manually delete them.

- /opt/FJSVsmee

- /etc/opt/FJSVsclr

7.3.2 Post-uninstallation Notes for Linked Servers, and Relay Servers

This section describes the points to note after uninstalling the Agents from the Linked Servers and Relay Servers.

7.3.2.1 Points to note after uninstalling Systemwalker Runbook Automation

[Windows]

The directory where the Agent was installed may still remain after uninstallation. If this is the case, delete it manually.

[Linux]

The following directories may remain. If this is the case, delete them manually.

- /etc/opt/FJSVcmdba

- /etc/opt/FJSVlnkbs

- /etc/opt/FJSVswrbaa

- /etc/opt/FJSVswrbac

- /opt/FJSVcmdba

- /opt/FJSVlnkbs

- /opt/FJSVswrbaa

- /opt/FJSVswrbac

- /var/opt/FJSVcmdba

- /var/opt/FJSVlnkbs

- /var/opt/FJSVswrbaa

- /var/opt/FJSVswrbac

7.3.2.2 Points to Note after Uninstalling SMEE and Securecrypto Library RunTime [Linux]

The following files and directories will still remain after SMEE and Securecrypto Library RunTime have been uninstalled. Check that these files and directories are not being used by other products, and delete them manually if they are not required.

For 32 bit version

- /opt/FJSVsmee

- /opt/FJSVsmee64

For 64 bit version

- /etc/opt/FJSVsclr

- /etc/opt/FJSVsclr64

7.3.3 Points to Note after Uninstalling from the Business Server

Points to note after uninstalling the Agent on the Business Server are explained below.

7.3.3.1 Points to Note after Uninstalling Systemwalker Runbook Automation

[Windows]

The directories that the Agents were installed in may still remain. Delete these directories manually.

Note that files or directories under these directories may also still remain, so delete them as well.

The files will have been locked, and therefore, any attempt to delete them may fail. In this case, restart the operating system then delete them.

[Linux] [Solaris]

The following directories may still remain. Delete them manually.

Note that files or directories under these directories may also still remain, so delete them as well.

- /etc/opt/FJSVlnkbs

- /etc/opt/FJSVswrbaa

- /etc/opt/FJSVswrbac

- /opt/FJSVlnkbs

- /opt/FJSVswrbaa

- /opt/FJSVswrbac

- /var/opt/FJSVlnkbs

- /var/opt/FJSVswrbaa

- /var/opt/FJSVswrbac

Note

The references above are for installations using default values. If changing the installation destination, such as when installing to Solaris or other OS, load to the changed installation destinations.

7.3.4 Points to Note after Uninstalling for Development Computer

This section describes the points to note after uninstalling the Systemwalker Runbook Automation Studio from the Development Computer.

7.3.4.1 Points to Note after Uninstalling Systemwalker Runbook Automation Studio

Workspaces created with Systemwalker Runbook Automation Studio and using the default location are created in Studio installation directory. Such directory still remains after uninstalling Studio.

After you delete the workspace, delete Studio installation directory.

7.3.5 Uninstalling the Uninstallation and Management (middleware)

This section describes how to uninstall the Uninstallation and Management (middleware).

- To uninstall Systemwalker Runbook Automation, uninstall from Uninstallation and Management(middleware)

- This tool has managed another Fujitsu middleware products even if Systemwalker Runbook Automation. Do not uninstall this tool, unless you really need it. If you have accidentally uninstalled it, re-install it following the steps below.

    [Windows]

    1. Log in as a user who belongs to the Administrators group on the installed machine, change management authority use account.

2. Insert the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc " DVD-ROM in the drive " Systemwalker Runbook Automation

3. Execute the install command.

```
DVD-ROM mount point\CIR installer root\cirinst.exe
```

[Linux] [Solaris]

1. Log in as a user who belongs to the Administrators group on the installed machine, change management authority use account.

2. Insert the "Systemwalker Runbook Automation Media Pack (15.1.0) Disc " DVD-ROM in the drive " Systemwalker Runbook Automation

3. Execute the install command.

```
# DVD-ROM mount point/CIR installer root/cirinst.sh
```

📂 Point

. . . .

If reinstalling "Uninstallation and Management (middleware)", either DVD-ROM "Disc No 1 of 2" or "Disc No 2 of 2" can be used.

. . . .

- If you uninstall this tool, execute as following steps.

1. Start the tool and check whether there are any other Fujitsu middleware products left on the system.

   [Windows]

   Start menu:

   Select **Start** >> **All Programs** >> **Fujitsu** >> **Uninstall (middleware)**

   [Linux] [Solaris]

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

   -c: Command interface

   Note: The command will fail if its path includes spaces, so do not move it to a directory with spaces in its name.

2. If no Fujitsu middleware products have been installed, then issue the command below:

   [Windows]

   ```
   C:\FujitsuF4CR\bin\cirremove.exe
   ```

   [Linux] [Solaris]

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

3. At the uninstallation confirmation prompt, enter "y":

```
"This software is a tool that is shared with other Fujitsu products. Are you sure you want to
remove this software? [y/n]"
```

4. Uninstallation will start.

   The process will take a few seconds.

5. Uninstallation will complete.

   The directories below and its files will still remain, and must be manually deleted:

   [Windows]

   %SystemDrive%\FujitsuF4CR

   [Linux] **[Solaris]**

/var/opt/FJSVcir

Chapter 8 Maintenance

This chapter describes operations that need to be performed when Systemwalker Runbook Automation is operated.

8.1 Logs

This section describes the logs generated by the product.

- Process instance audit logs

- CMDB audit logs

8.1.1 Process Instance Audit Logs

The process instance start time, end time, starter and status information is output as an audit log.

Settings

There is no particular need to configure settings for the collection of process instance audit logs. The settings will be complete at the point when the installation and setup of the Systemwalker Runbook Automation Management Server are complete.

Usage

To obtain the process instance audit logs, execute the get process instance audit information command (swrba_audit). Refer to the *Systemwalker Runbook Automation Reference Guide* for information on the swrba_audit command.

Example)

```
swrba_audit
```

The process instance audit information that can be obtained using the swrba_audit command without any options will be the process instance information that was complete after the swrba_audit command was executed without any options the previous time.

Output Location

The process instance audit log is output to the following process instance audit information file. Refer to the *Systemwalker Runbook Automation Reference Guide* for information on the process instance audit information file.

[Windows]

```
[Systemwalker Runbook Automation Management Server installation directory] \var\audit\swrba_audit.log
```

```
/opt/FJSVswrbam/var/audit/swrba_audit.log
```

- 10 generations of the process instance audit information file are managed, each generation being 10MB.

- The trigger for the generation switchover is when the file exceeds 10MB.

- A number between 1 and 9 is added to the ' swrba_audit' part of the file name each time there is a generation switchover, so the file name becomes swrba_audit.log --> swrba_audit1.log --> swrba_audit2.log... --> swrba_audit9.log.

- Once 10 generations (100MB) is exceeded, the oldest file (swrba_audit9.log) is deleted.

Log Output Format

The audit log is output in the following format. One process instance information is displayed as one record.

```
"process instance start time","process instance starter","process instance name","process instance status","process instance end time","activity name","transition date and time","person responsible","task status","selection result",...,"exit node"
```

- Process instance start time: The time at which the process instance was started is displayed.

- Process instance starter: The user ID of the user that started the process instance is displayed.

- Process instance name: The process instance name is displayed.

- Process instance status: The process instance status is displayed.

   - closed

  Only "closed" is displayed. Except of "closed", such as "aborted", or "error" status is not displayed.

- Process instance end time: The time at which the process instance was ended is displayed.

- Activity name: The activity name is displayed.

- Transition date and time: The date and time of the transition are displayed for the activity. If processing is not translated to activity, blank string is displayed.

- Person responsible: The user ID for the assigned task is displayed. If processing is not translated to activity, blank string is displayed.

- Task status: The task status is displayed.

   - COMPLETED

   - INITIAL: The processing is translated to activity.

- Selection result: The selected arrow name is displayed

- End node: The end node name is displayed.

Example of the output

The example below shows the output of the audit information for the process instance with the name "Sample-1".

```
"2011-05-11 14:50:32.460","swrbaadmin","Sample-1","closed","2011-05-11
14:53:27.161","Activity1","2011-05-11 14:53:27.033","swrbaadmin","COMPLETED","Arrow2","Exit1"
```

Example of the operation

The example below shows the recommended operation.

1. Using an operating system feature such as Task Scheduler (Windows) or cron (Linux), configure the settings so that the get process instance audit information command is executed at fixed intervals. The get process instance audit information command is executed without any options.

   When this command is executed without any options, any process instance audit logs output between the previous time the command was executed without any options and when the command is executed this time will be collected.

2. After the command was executed, create another directory using a name such as the date, create the process instance audit information file (if there are multiple files, create all of them) then back up the file (or files) in the directory that was created.

3. Delete the process instance audit information file that was output in 1. (if there are multiple files, delete all of them).

4. Repeat steps 2 and 3. Each time the command is executed.

P Point

· ·

- The process instance audit information file content is managed as 10MB x 10 generations. Design so that the execution of the get process instance audit information command once does not result in 100MB being exceeded.

- Execute test operations, and check/adjust the get interval.

- By specifying the -closedafter and -closedbefore options in the command, it will be possible to get the process instance audit logs separately at specified intervals.

· ·

8.1.2 CMDB Audit Logs

Operations performed on the CMDB via Agents, commands or GUI operations are logged into audit log files.

The file name and location are displayed below:

[Windows]

<CMDB Manager directory>\FJSVcmdbm\var\log\audit\audit.log

[Linux]

/opt/FJSVcmdbm/var/log/audit/audit.log

- Up to 10 generations of audit log files are kept, named "audit.log", "audit.log.1", "audit.log.2", up to "audit.log.9". Each audit log is 5 MB. Once the maximum number of audit log files is reached, the oldest one (audit.log.9) is deleted.

Log output format

"date/time", "operation location", "execution host", "operator", "operation type", "operation target", "operation content", "execution result", "component", "additional information", "reserved area"

- Date/time: Operation's date and time, in "date time time-difference" format.

- Operation location: IP address of the machine where the operation was performed

- Execution host: Host name of the machine where the operation was performed (the machine hosting the CMDB Manager).

- Operator: Information on the Agent or command that performed the operation:

    - If performed by an Agent: Agent ID or type name (if it was the first operation and the Agent ID has not been set up).

    - If performed by a command: OS user name for the user that executed the command.

- Operation type: Operation name.

- Operation target: Target and result of the operation, in "name=value;" format.

- Operation content: Content of the operation. If the execution result is failure, this item indicates error details.

- Execution result: "S" if the operation succeeded, "F" if the operation failed.

- Component: Literal text "FSERV".

- Additional information: Additional information for the operation, in "name=value;" format.

- Reserved area: Not used.

Output example

"2009/09/18 16:54:20.093 +0900","192.0.2.10","ITCM-GSV1","MDR Service for Interstage Application Server","addMDR","id=mdr000000000004;","addMDR","S","FSERV","",""

"2009/09/18 16:54:24.375 +0900","192.0.2.10","ITCM-GSV1","mdr000000000004","addEntities","id=gid000000000004; type=InterstageApplicationServer; record=observed; version=1;","addEntity","S","FSERV","",""

"2009/09/18 16:54:26.656 +0900","192.0.2.10","ITCM-GSV1","mdr000000000004","addEntities","id=gid000000000005; type=ISWorkUnit; record=observed; version=1;","addEntity","S","FSERV","",""

"2009/09/18 16:54:26.843 +0900","192.0.2.10","ITCM-GSV1","mdr000000000004","addEntities","id=gid000000000001; type=LogicalServer; record=observed; version=1;","updateEntity","S","FSERV","",""

"2009/09/19 15:24:48.187 +0900","192.0.2.20","ITCM-GSV1","SYSTEM","addEntity","id=gid000000000016; type=ChangeRecord; record=expected; version=1;","addEntity","S","FSERV","",""

"2009/09/19 15:29:33.890 +0900","192.0.2.20","ITCM-
GSV1","SYSTEM","addEntities","id=gid000000000027; type=MasterPackage; record=expected;
version=1;","addEntity","S","FSERV","",""

8.2 Adding, Changing and Deleting Users

This section describes how to add, change and delete users when user authentication is performed using LDAP.

Add and remove users according to their LDAP types.

Adding users

To add a new user, follow the steps below:

1. Add the user to the LDAP directory.

   Refer to "Registering user in Directory Service" in the *Systemwalker Runbook Automation Operation Guide* for details.

2. Assign the user to groups.

   Refer to "Registering Local Group and Adding User" in the *Systemwalker Runbook Automation Operation Guide* for details.

Note

. . . .

- If the users and groups in the organization are already managed by using the LDAP directory as a directory service, Systemwalker Runbook Automation can use the existing directory structure. In this case, specify the LDAP users as IflowUsers and Role users.

- It may take up to 90 minutes for the registration results to be reflected in the LDAP directory. To reflect the registration results immediately, restart Systemwalker Runbook Automation.

. . . .

Changing user passwords

To change a user's password, change the password for the user that has been registered with each LDAP directory. The procedure depends on the type of the LDAP being used (refer to the manual for the LDAP directory used).

Deleting users

1. Check whether all tickets for the user can be deleted.

2. Delete the user from Systemwalker Runbook Automation.

8.3 Backup and Restoration

This section describes how to back up and restore the Management Server.

Note that Agents do not have backup or restoration functions, they have to be reinstalled.

8.3.1 Notes on Backup and Restoration

This section describes points that require attention when performing backups or restorations:

- Notes on operations that use coexistence with Systemwalker Operation Manager

- Notes on the environments where backups and restorations are performed

- Notes on the timing of backups and restorations

- Handling backup resources

- Operations during backups and restorations

Notes on operations that use coexistence with Systemwalker Operation Manager

Systemwalker Runbook Automation backup/restore is executed at the same time as Systemwalker Operation Manager backup/restore.

In order to use operations that use coexistence with Systemwalker Operation Manager, backup/restore Systemwalker Operation Manager using the same backup/restore procedure that is used for Systemwalker Runbook Automation. Do not execute backup/restore on the standalone Systemwalker Operation Manager.

Notes on the environments where backups and restorations are performed

The backup and restoration environments must follow the criteria below:

- When OS are different in from backup and to restore
  However, execution will be possible if the operating system versions of the same vendor are different.

- When the product installation directories are different [Windows]

- When the host information (host name/IP address) is different

- When the code types are different

- When the LDAP servers are different

- When the Process Management database storage directories are different

- When the CMDB database storage directories are different

- When the sub system number with using scheduling are different

- When the Web server (Interstage HTTP Server), message broker, and server function port numbers are different

Notes on the timing of backups and restorations

- When backup and restore are executed, it will be necessary to stop, and then, restart Systemwalker Runbook Automation. Additionally, at the time of restore Systemwalker Operation Manager is stopped, and then, restarted. For this reason, the operator should execute backup and restore in a time zone that does not use Systemwalker Runbook Automation and Systemwalker Operation Manager.

- The status of the Automated Operation Process will be restored exactly as it was at the point when the backup was executed. For this reason, if the restoration was executed using the backup resources of the Automated Operation Process while it was running, the activity of the Automated Operation Process will be restarted. It is recommended that you first check that there are no Automated Operation Processes which are running, before executing the backup.

  Additionally, any user assets that are used, such as File Listener, will not be targets of backup/restore. These should be backed up if necessary.

- If backup is executed while a Systemwalker Operation Manager job/job net/group is running, and that information is then restored, the job/job net/group that is running will end abnormally with the exit code 239. It is recommended that you execute this operation in a time zone in which the job/job net/group are not executed.

Handling backup resources

- When moving backup resources to the restoration target, move the directory specified as the backup directory and all its files.

- Do not delete the backup resources in the directory specified as the backup directory until the restoration completes.

- The backup command cannot be used to back up data to the following types of media:

  - Optical disks such as CD-Rs and DVD-Rs
    To save user assets to optical disks, first back up the data to the local disk, and then, write it to the media using a dedicated optical disk writer, for example.

  - Network paths [Windows]

- Directories whose pathnames include spaces [Windows]

- For the backup destination directory name, only alphanumeric characters can be specified. The name cannot include symbols or blank spaces.

- The backup directory name can contain up to the following number of characters:

32 characters

- If the specified directory does not exist, it will be created by the backup command.

Operations during backups and restorations

Do not operate the following middleware products during backups or restorations:

- Interstage Application Server

- Systemwalker Operation Manager

- Systemwalker Centric Manager

- Systemwalker Runbook Automation

Handling restoration resources

- The restore command cannot be used to restore data from the following type of media:

  - Directories whose pathnames contain spaces

  - Restore frpm network path [Windows]

- For the backup destination directory name, only alphanumeric characters can be specified. The name cannot include symbols or blank spaces.

- The backup directory name can contain up to the following number of characters:

32 bytes

8.3.2 Backing up Systemwalker Runbook Automation

This section describes how to back up the Systemwalker Runbook Automation environment.

Back up as following steps

Backup Interstage Single Sign-On resources

Backup LDAP

Common processing

Start and finish
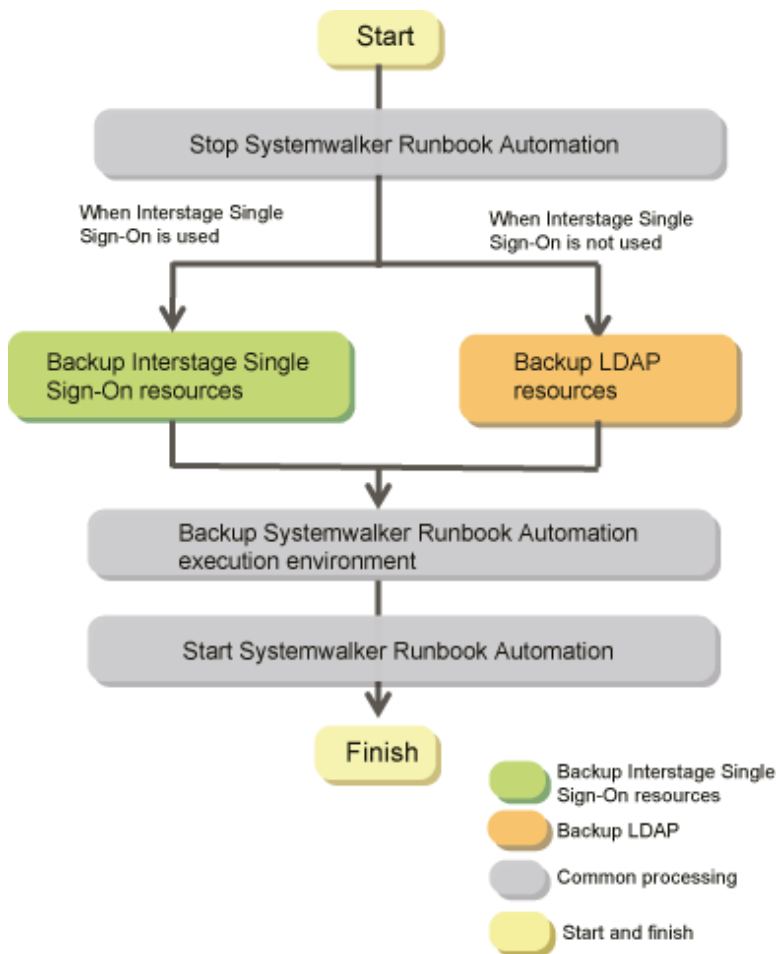
8.3.2.1 Stop Systemwalker Runbook Automation

Stop Systemwalker Runbook Automation Management Server by swrba_stop command.

[Windows]

```
[Systemwalker Runbook Automation Management Server install directory]\bin\swrba_stop
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_stop
```

8.3.2.2 Backup the Interstage Single Sign-On Resources

This section explains the procedure for backing up the Interstage Single Sign-On resources.

You do not need to execute this procedure in the environment of not using Interstage Single Sign-On authentication foundation.

📝 Note

- Here, the Interstage Single Sign-On resources constructed by using the ssoclsetup command are backed up.

  For the Interstage Single Sign-On resources constructed by not using the ssoclsetup, refer to the *Interstage Application Server Operator's Guide* and backup the resources.

- Execute procedure in this section as an administrator authority.

8.3.2.2.1 Stop the Interstage Single Sign-On

The Interstage Single Sign-On is stopped by using the ssoclservicectl command. Refer to the *Systemwalker Runbook Automation Reference Guide* for the ssoclservicectl command

[Windows]

```
[Systemwalker Runbook Automation Management Install Directory]\sso\bin\ssoclservicectl stop
```

[Linux]

```
/opt/ FJSVswrbam /sso/bin/ssoclservicectl stop
```

8.3.2.2.2 Backup the Interstage Single Sign-On Resources

The Interstage Single Sign-On resources can be backed up by using the ssoclbackup command. Refer to the *Systemwalker Runbook Automation Reference Guide* for the ssoclbackup command.

[Windows]

1. Create directory for back up

```
mkdir X:\Backup\sso
```

2. Back up with ssoclbackup command.

```
 [Systemwalker Runbook Automation Management Server Install Directory]\sso\bin\ssoclbackup X:
\Backup\sso
```

[Linux]

1. Create directory for back up

```
mkdir /backup/sso
```

2. Back up with ssoclbackup command

```
/opt/FJSVswrbam/sso/bin/ssoclbackup /backup/sso
```

Note

Here, the following resources are backed up. Refer to *Systemwalker Runbook Automation Reference Guide*

- Interstage Single Sign-On resources

- Interstage HTTP Server resources

- Interstage Directory Service resources

- Interstage Certificate Environment resources

- SSO repository name

8.3.2.2.3 Start the Interstage Single Sign-On

The Interstage Single Sign-On is started by using the ssoclservicectl command. Refer to *Systemwalker Runbook Automation Reference Guide* for the ssoclservicectl command.

[Windows]

```
[Systemwalker Runbook Automation Management Server Install Directory]\sso\bin\ssoclservicectl start
```

[Linux]

```
/opt/FJSVswrba/sso/bin/ssoclservicectl start
```

8.3.2.3 Backing up LDAP Resources

This section explains how to back up the LDAP resources.

If you use Interstage Single Sign-On authentication infrastructure, you do not execute this steps.

If Active Directory or OpenLDAP is used for LDAP, refer to the LDAP manual before performing the backup tasks.

In the backup method explained here, the Interstage Directory Service is used and a standard database is used for the repository database.

[Windows]

In the following example, the repository "rep001" is backed up to the backup directory "X:\Backup\rep001".

1. Log in as the system administrator.

2. Stop Interstage directory service.

   Stop "Interstage Directory Service(rep001)" from **Control Panel**- **Administrative tool**-**Service.** Or stop it by the following command.

   ```
   net stop "Interstage Directory Service(rep001)"
   ```

3. Execute the backup command.

   Delete the rep001 directory if it exists in 'X:\Backup', otherwise the command will fail.

   ```
   [Interstage Application Server installation directory]\bin\irepbacksys -d X:\Backup\rep001 -R
   rep001
   ```

4. Start the Interstage Directory Service, if it is used.

   Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services.** From the displayed list of services, right-click **Interstage Directory Service(rep001)** and click **Start**.

   Alternatively, start the Interstage Directory Service using the following command:

   ```
   net start "Interstage Directory Service(rep001)"
   ```

[Linux]

In the following example, the repository "rep001" is backed up to the backup files "/backup/rep001".

1. Log in as the system administrator.

2. Stop Interstage directory service by irepstop command.

   ```
   /opt/FJSVirep/bin/irepstop -R rep001
   ```

3. Execute the backup command.

   ```
   /opt/FJSVirep/bin/irepbacksys -f /backup/rep001 -R rep001
   ```

4. If the Interstage Directory Service is used, start it.

   ```
   /opt/FJSVirep/bin/irepstart -R rep001
   ```

Information

Refer to "Interstage back up Interstage Directory Service" in the *Interstage Application Server Operation Guide* for information on how to back up the Interstage Directory Service.

8.3.2.4 Back up Systemwalker Runbook Automation execution environment

This section describes how to back up the Systemwalker Runbook Automation environment.

Checking the space available in the backup directory

Backing up resources

Checking the space available in the backup directory

To check how much free space is required for the backup directory, it is necessary to check the space required for the backup directory for Systemwalker Runbook Automation and the space required for the backup directory for the CMDB.

Guides to the amount of free space required in the backup directory are as follows.

Checking the space available in the backup directory

[Windows]

> Space required for the backup directory =
> Amount of backup resources for the Process Management Database (*1)
> + Total size of the files and directories under the installation directory for the Systemwalker Runbook
> Automation Management Server
> + Total capacity in the Systemwalker Operation Manager installation directory
> + 1 MB

*1:

Process Management Database directory size specified during setup

[Linux]

> Space required for the backup directory =
> Amount of backup resources for the Process Management Database (*1) +
> +Total size of the files and directories under the /etc/opt/FJSVswrbam directory +
> +Total size of the files and directories under the /var/opt/FJSVswrbam directory +
> + Total capacity in /var/opt/FJSVJMCMN/etc
>
> + Total capacity in /var/opt/FJSVjmcal
>
> + Total capacity in /var/opt/FJSVJOBSC
>
> + Total capacity in /var/opt/FJSVfwseo/config/JM (*2)
>
> + Total capacity in /opt/FJSVJOBSC/bin
>
> + Total capacity in /etc/mjes
>
> + Total capacity in /var/spool/mjes
>
> + 1 MB

*1:

Database directory size specified during setup

*2:

In the following cases, "FJSVfwseo" will be "FJSVfwsec".

- When Systemwalker Centric Manager V13.4.0 is installed after Systemwalker Runbook Automation

- When a version later than Systemwalker Centric Manager V13.4.0 is installed (this has nothing to do with the order of installation with regard to Systemwalker Runbook Automation)

Checking the space available in the CMDB backup directory

As a guide to the amount of free space required for the backup directory, check the size of the directories below:

[Windows]

```
Space required for the backup directory =
<CMDB Manager database directory>\FJSVcmdbm \Shunsaku\directorData
+ <CMDB Manage database directory r>\FJSVcmdbm\fcmdb\file
+100MB
```

[Linux]

```
Space required for the backup directory =
/opt/FJSVcmdbm/var/Shunsaku/directorData
+/opt/FJSVcmdbm/var/fcmdb/file
+100MB
```

Backing up resources

[Windows]

Describes the steps for backing up backup directory X:\Backup\swrba

1. Login as a system administrator

2. Create back up directory

   ```
   mkdir X:\Backup\swrba
   ```

3. Execute back up command

   Back up the resources

   ```
   [Systemwalker Runbook Automation Management Server install directory]\bin\swrba_backup X:\Backup
   \swrba
   ```

4. Backup will start.

   The message below will be displayed:

   > Systemwalker Runbook Automation backup has started.
   >
   > Database backup has started.
   >
   > Database backup has completed successfully.
   >
   > File backup has started.
   >
   > File backup has completed successfully.
   >
   > Backup of the Scheduling is starting.
   >
   > Backup of the Scheduling has finished.
   >
   > Starting to back up the CMDB Manager.
   >
   > Finished backing up the CMDB Manager.
   >
   > Systemwalker Runbook Automation backup has completed successfully.

5. E Backup will complete

   The message below will be displayed:

   > Systemwalker Runbook Automation backup has completed successfully.

[Linux]

1. Log in as a superuser on the system.

2. Create back up directory

   ```
   mkdir /backup/swrba
   ```

3. Back up the resources

> 1. /opt/FJSVswrbam/bin/swrba_backup /backup/swrba.

4. Backup will start.

   The message below will be displayed:

   > Systemwalker Runbook Automation backup has started.
   >
   > Database backup has started.
   >
   > Database backup has completed successfully.
   >
   > File backup has started.
   >
   > File backup has completed successfully.
   >
   > Backup of the Scheduling is starting.
   >
   > Backup of the Scheduling has finished.
   >
   > Starting to back up the CMDB Manager.
   >
   > Finished backing up the CMDB Manager.
   >
   > Systemwalker Runbook Automation backup has completed successfully.

5. Backup will complete.

   The message below will be displayed:

   > Systemwalker Runbook Automation backup has completed successfully.

8.3.2.5 Start Systemwalker Runbook Automation

start Systemwalker Runbook Automation Management Server by swrba_start command.

[Windows]

```
[Systemwalker Runbook Automation Management Server install directory]\bin\swrba_start
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_start
```

8.3.3 Restoring Systemwalker Runbook Automation

This section describes how to restore the Systemwalker Runbook Automation environment.
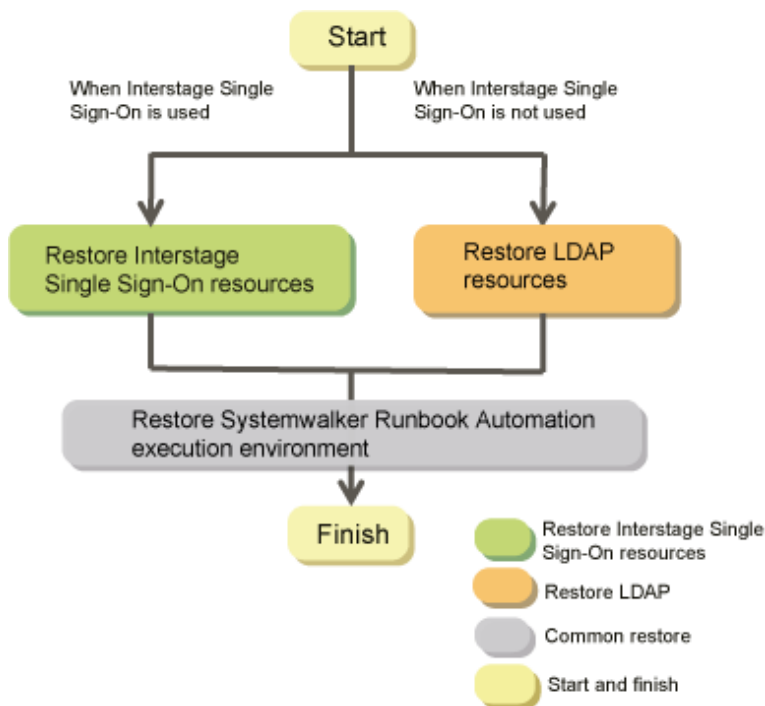
8.3.3.1 Restore the Interstage Single Sign-On Resources

This section explains the procedure for restoring the Interstage Single Sign-On resources.

You do not need to execute this procedure if you do not use Interstage Single Sign-On authentication infrastructure

![Note icon] **Note**

. . . .

- Here, the Interstage Single Sign-On resources constructed by using the ssoclbackup command are restored.

  For the Interstage Single Sign-On resources constructed by not using the ssoclbackup, refer to the "*Interstage Application Server Operator's Guide*" and restore the resources.

- Execute procedure in this section as an administrator authority.

. . . .

8.3.3.1.1 Stop the Interstage Single Sign-On

The Interstage Single Sign-On is stopped. Refer to the "*Systemwalker Runbook Automation Reference Guide*" for information on how to stop the Interstage Single Sign-On.

[Windows]

```
[Systemwalker Runbook Automation Management Server Install Directory]\sso\bin\ssoclservicectl stop
```

[Linux]

```
/opt/FJSVswrba/sso/bin/ssoclservicectl stop
```

8.3.3.1.2 Restore the Interstage Single Sign-On Resources

The Interstage Single Sign-On is restored by using the ssoclrestore command. Refer to the *Systemwalker Runbook Automation Reference Guide* for the ssoclrestore command.

[Windows]

When the backup target directory is X:\Backup\sso

```
[Systemwalker Runbook Automation Management Server Install Directory]\sso\bin\ssoclrestore X:\Backup
\sso
```

[Linux]

When the backup target directory is \Backup\sso

```
/opt/FJSVswrbam/sso/bin/ssoclrestore /backup/sso
```

Note

. . . .

Here, the following resources are restored. Refer to the ssoclrestore command in the "*Systemwalker Runbook Automation Reference Guide*".

- Interstage Single Sign-On resources

- Interstage HTTP Server resources

- Interstage Directory Service resources

- Interstage Certificate Environment resources

- SSO repository name

. . . .

8.3.3.1.3 Start the Start the Interstage Single Sign-On

Start Interstage Single Sign-On with using ssoclservicectl command. For the detail of ssoclservicectl command Refer to the "*Systemwalker Runbook Automation Reference Guide*"

[Windows]

```
[Systemwalker Runbook Automation Management Server install directory]\sso\bin\ssoclservicectl start
```

[Linux]

```
/opt/FJSVswrbam/sso/bin/ssoclservicectl start
```

8.3.3.2 Restoring LDAP Resources

This section explains how to restore the LDAP resources.

If you use Interstage Single Sign-On authentication infrastructure, you do not execute this steps

If Active Directory or OpenLDAP is used for LDAP, refer to the LDAP manual before performing the backup tasks.

In the restore method explained here, the Interstage Directory Service is used and a standard database is used for the repository database.

In case using database except standard database , refer to the "*Restore Interstage Directory Service resource*" in the "*Interstage Application Server Operation Guide(Basic)*".

[Windows]

Back up directory: X:\Backup\rep001

Repository Name: rep001

1. Delete the rep001 directory if it exists in 'X:\Backup',

2. Recovery repository by the following command.

   ```
   [Interstage Application Server Install directory]\bin\ireprestsys -d X:\Backup\rep001 -R rep001
   ```

3. Start the Interstage Directory Service, if it is used.

   Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**. From the displayed list of services, right-click **Interstage Directory Service(rep001)** and click **Start**.

   Alternatively, start it using the following command:

```
net start "Interstage Directory Service(rep001)"
```

[Linux]

Back up file: /backup/rep001.tar.gz

Repository name: rep001

1. Delete the rep001 repository if it exists

2. Recovery repository by the following command

```
/opt/FJSVirep/bin/irepstart -R rep001
```

3. Recovery repository by the following command

```
/opt/FJSVirep/bin/irepstart -R rep001
```

Information

. . . .

How to perform backups when the Interstage Directory Service is used

If the Interstage Directory Service is used for the LDAP directory, back up resources by referring to "*Back up Interstage Directory Service Resource*" in the "*Interstage Application Server Operation Guide*".

. . . .

Note

. . . .

- You may not restore if repository exists . Delete repository from Interstage Management Console.
  Delete as "**Interstage Management Console** >> **Interstage Application Server** >> **System** >> **Service** >> **Repository** >> **state**"

. . . .

8.3.3.3 Restoring Systemwalker Runbook Automation execution environment

This section explains how to restore the Systemwalker Runbook Automation execution environment

[Windows]

1. If the setup of Systemwalker Runbook Automation is complete, stop Systemwalker Runbook Automation Management Server.

   Stop Systemwalker Runbook Automation Management Server by swrba_stop command

   ```
   [Systemwalker Runbook Automation Management Server Install directory]\bin\swrba_stop
   ```

2. Restore the resources:

   In case of Back up directory X:\Backup\swrba

   ```
   <Installation directory for the Systemwalker Runbook Automation Management Server>\bin
   \swrba_restore < X:\Backup\swrba
   ```

   If the command is executed in a state in which the setup of Systemwalker Runbook Automation is complete, the following message will be displayed.

   ```
   Systemwalker Runbook Automation restore has started.
   Initialization of the restoration destination directory will start.
   Initialization of the restoration destination directory has finished.
   Database restore has started.
   Database restore has completed successfully.
   File restore has started.
   File restore has completed successfully.
   Restore of the Scheduling is starting.
   Restore of the Scheduling has finished.
   ```

```
Starting to restore the Interstage Business Process Manager.
Finished restoring the Interstage Business Process Manager.
Starting to restore the CMDB Manager.
Finished restoring the CMDB Manager.
Systemwalker Runbook Automation restore has completed successfully.
```

If the command is executed in a state in which the setup of Systemwalker Runbook Automation is not complete, the following message will be displayed.

```
Systemwalker Runbook Automation restore has started.
The Systemwalker Runbook Automation environment build to the restoration destination management
server will start.
Starting the Process Management Database build.
Creating the Process Management Database has completed.
Starting to set up the environment for Systemwalker Runbook Automation.
Setting up the environment for Systemwalker Runbook Automation has completed.
The CMDB environment setup will start.
The CMDB environment setup is now complete.
The Systemwalker Runbook Automation environment build to the restoration destination management
server has finished.
Systemwalker Runbook Automation restore has started.
Initialization of the restoration destination directory will start.
Initialization of the restoration destination directory has finished.
Database restore has started.
Database restore has completed successfully.
File restore has started.
File restore has completed successfully.
Restore of the Scheduling is starting.
Restore of the Scheduling has finished.
Starting to restore the Interstage Business Process Manager.
Finished restoring the Interstage Business Process Manager.
Starting to restore the CMDB Manager.
Finished restoring the CMDB Manager.
Systemwalker Runbook Automation restore has completed successfully.
```

If the command is executed in a state in which the previous setup of Systemwalker Runbook Automation ended abnormally, the following message will be displayed.

```
Systemwalker Runbook Automation restore has started.
Deletion of the Systemwalker Runbook Automation environment from the restoration destination
management server will start.
The CMDB environment deletion will start.
Deletion of the CMDB environment is now complete.
Canceling the environment settings for Systemwalker Runbook Automation.
The environment settings for Systemwalker Runbook Automation have been canceled.
Deletion of the Process Management Database is about to start.
Deletion of the Process Management Database is now complete.
Deletion of the Systemwalker Runbook Automation environment from the restoration destination
management server has finished.
Systemwalker Runbook Automation restore has started.
Initialization of the restoration destination directory will start.
Initialization of the restoration destination directory has finished.
Database restore has started.
Database restore has completed successfully.
File restore has started.
File restore has completed successfully.
Restore of the Scheduling is starting.
Restore of the Scheduling has finished.
Starting to restore the Interstage Business Process Manager.
Finished restoring the Interstage Business Process Manager.
Starting to restore the CMDB Manager.
Finished restoring the CMDB Manager.
Systemwalker Runbook Automation restore has completed successfully.
```

Restoration will complete.

The message below will be displayed:

```
 Systemwalker Runbook Automation restore has completed successfully.
```

3. Start Systemwalker Runbook Automation Management Server by the following command.

```
[Systemwalker Runbook Automation Management Server Install Directory]\bin\swrba_start
```

4. Update CMDB information by cmdbrefresh command as below.

```
[Systemwalker Runbook Automation Management Server Install directory]\CMDB\FJSVcmdbm\bin
\cmdbrefresh.exe -a -q
```

The message below will be displayed:

```
Updating MDRs.
Command successful!
```

> **Note**
> ....
> When updating CMDB information, confirm the product, which collected configuration information be started.
>
> To confirm the product, which collected configuration information by mdradmin.exe -l command.
>
> For the detail mdradmin command, Refer to the *mdradmin* in the *Systemwalker Runbook Automation Reference Guide*
> ....

[Linux]

1. Log in as a superuser on the system.

2. If the setup of Systemwalker Runbook Automation is complete, stop Systemwalker Runbook Automation.

   Stop Systemwalker Runbook Automation Management Server by swrba_stop command.

```
/opt/FJSVswrbam/bin/swrba_stop
```

3. Execute Restore command

   With executing the following command, rstore Systemwalker Runbook Automation resource

   In case of backup directory/backup/swrba

```
 /opt/FJSVswrbam/bin/swrba_restore /backup/swrba
```

   If the command is executed in a state in which the setup of Systemwalker Runbook Automation is complete, the following message will be displayed.

```
Systemwalker Runbook Automation restore has started.
Initialization of the restoration destination directory will start.
Initialization of the restoration destination directory has finished.
Database restore has started.
Database restore has completed successfully.
File restore has started.
File restore has completed successfully.
Restore of the Scheduling is starting.
Restore of the Scheduling has finished.
Starting to restore the Interstage Business Process Manager.
Finished restoring the Interstage Business Process Manager.
Starting to restore the CMDB Manager.
Finished restoring the CMDB Manager.
Systemwalker Runbook Automation restore has completed successfully.
```

If the command is executed in a state in which the setup of Systemwalker Runbook Automation is not complete, the following message will be displayed.

```
Systemwalker Runbook Automation restore has started.
The Systemwalker Runbook Automation environment build to the restoration destination management
server will start.
Starting the Process Management Database build.
Creating the Process Management Database has completed.
Starting to set up the environment for Systemwalker Runbook Automation.
Setting up the environment for Systemwalker Runbook Automation has completed.
The CMDB environment setup will start.
The CMDB environment setup is now complete.
The Systemwalker Runbook Automation environment build to the restoration destination management
server has finished.
Systemwalker Runbook Automation restore has started.
Initialization of the restoration destination directory will start.
Initialization of the restoration destination directory has finished.
Database restore has started.
Database restore has completed successfully.
File restore has started.
File restore has completed successfully.
Restore of the Scheduling is starting.
Restore of the Scheduling has finished.
Starting to restore the Interstage Business Process Manager.
Finished restoring the Interstage Business Process Manager.
Starting to restore the CMDB Manager.
Finished restoring the CMDB Manager.
Systemwalker Runbook Automation restore has completed successfully.
```

If the command is executed in a state in which the previous setup of Systemwalker Runbook Automation ended abnormally, the following message will be displayed.

```
Systemwalker Runbook Automation restore has started.
Deletion of the Systemwalker Runbook Automation environment from the restoration destination
management server will start.
The CMDB environment deletion will start.
Deletion of the CMDB environment is now complete.
Canceling the environment settings for Systemwalker Runbook Automation.
The environment settings for Systemwalker Runbook Automation have been canceled.
Deletion of the Process Management Database is about to start.
Deletion of the Process Management Database is now complete.
Deletion of the Systemwalker Runbook Automation environment from the restoration destination
management server has finished.
Systemwalker Runbook Automation restore has started.
Initialization of the restoration destination directory will start.
Initialization of the restoration destination directory has finished.
Database restore has started.
Database restore has completed successfully.
File restore has started.
File restore has completed successfully.
Restore of the Scheduling is starting.
Restore of the Scheduling has finished.
Starting to restore the Interstage Business Process Manager.
Finished restoring the Interstage Business Process Manager.
Starting to restore the CMDB Manager.
Finished restoring the CMDB Manager.
Systemwalker Runbook Automation restore has completed successfully.
```

Restoration will complete .

The message below will be displayed:

```
Systemwalker Runbook Automation restore has completed successfully.
```

4. Start Systemwalker Runbook Automation by the following command.

```
/opt/FJSVswrbam/bin/swrba_start
```

5. Update CMDB information by executing cmdbrefresh command

```
/opt/FJSVcmdbm/bin/cmdbrefresh.sh -a -q
```

The message below will be displayed:

```
Updating MDRs.
Command successful!
```

📝 Note

When updating CMDB information, confirm the product, which collected configuration information be started.

To confirm the product, which collected configuration information by mdradmin.exe -l command.

For the detail mdradmin command, refer to the *mdradmin* in the *Systemwalker Runbook Automation Reference Guide*

8.4 Changing the Environment for Systemwalker Runbook Automation

This section describes how to change the environment for Systemwalker Runbook Automation.

- Changing the mail server information registered on the Management Server

- Changing the Management Server's host name/IP address

- Changing Host Name and IP Address of Linked Servers and Relay Servers

📝 Note

The host name and IP address of the Management Server cannot be changed if it has been installed on top of a cluster system.

Uninstall the product before changing the host name or IP address, and then, reinstall it.

8.4.1 Changing the Mail Server Information Registered on the Management Server

If the mail server information (such as the host name or port number of the SMTP server) has changed, the information registered on the Management Server must be changed.

This section explains the procedure for changing information about the mail server (SMTP server).

📝 Note

- Refer to "Setting Up Mail Notification" in the *Systemwalker Runbook Automation Operation Guide* for information on email notification.

List of setting items

The following table lists the items that can be set up as the mail server information.

Item name	Description
SMTPServerHost	Specify the host name or IP address for the SMTP server for sending e-mail messages.
SMTPServerPort	Specify the port number for the SMTP server for sending e-mail messages.
SMTPUserName	Specify the name of the user responsible for authenticating with the SMTP server when e-mail messages are sent. If you do not perform authentication with the SMTP server when e-mail messages are sent, specify "\ " (a backslash followed by a space).
SMTPPassword	Specify the password of the user responsible for authenticating with the SMTP server when e-mail messages are sent. If you do not perform authentication with the SMTP server when e-mail messages are sent, specify "\ " (a backslash followed by a space).
ServerEmailAddress	Specify the sender (the "from" address), who will be assigned to the e-mail messages that are sent, using the e-mail address format. Note that this address will be used as the address for receiving error e-mail messages when the notification e-mails that are sent bounce because the recipient cannot be found. Specify the e-mail address of someone who can respond to problems promptly.
ServerBaseURL	Specify the URL for the Web console. Specify the URL using the following format: - http://*<host name of the Management Server>*:*<port number for the Management Server (Web server)>*/console/ Ensure you specify a URL that can be accessed externally. Specifically, for environments that use the Interstage Single Sign-On, ensure you specify the host name in the FQDN format.
ServerEmailBaseURL	Specify the URL for the Management Server that will appear in e-mail messages. Set the same value as the ServerBaseURL.

Setup procedure

Log in as a system administrator, and use the following procedure to register information on the Management Server.

It is recommended that a backup be taken before starting this procedure. Refer to "8.3 Backup and Restoration" for information on the backup method.

1. Check the operational status of Systemwalker Runbook Automation.

   Check the operational status of Systemwalker Runbook Automation by executing the swrba_status command. If Systemwalker Runbook Automation is not running, start it using the swrba_start command.

   Refer to the *Systemwalker Runbook Automation Reference Guide* for information on the swrba_status and swrba_start commands.

2. To authenticate with the SMTP server when email messages are sent, encrypt the password of the user responsible for authenticating with the SMTP server. Use the following command to encrypt the password.

This step is not required if authentication with the SMTP server is not performed when email messages are sent, or if the password is not to be changed.

[Windows]

```
> [Interstage BPM installation directory]\client\samples\configuration\EncryptPassword.bat -e
"password"
-------ENCRYPTED PASSWORD-------
Encrypted password
```

[Linux]

```
# /opt/FJSVibpm/client/samples/configuration/EncryptPassword.sh -e "password"
-------ENCRYPTED PASSWORD-------
Encrypted password
```

3. Prepare definition files for the mail server and mail sender.

Create the following two types of files. The files can be created in any location. In these files, specify only the items that will be changed. In the following example, all the parameters will be changed.

1. Configuration file for the SMTP server (smtpserver.conf)

Example of configuration file settings for authenticating with the SMTP server when email messages are sent.

```
SMTPServerHost=swrba.mail.server
SMTPServerPort=25
SMTPUserName=swrbamailuser
SMTPPassword=encrypted password
ServerBaseURL=http://ssoserver.example.com:80/console/
ServerEmailBaseURL=http://ssoserver.example.com:80/console/
```

Example of configuration file settings for not performing the authentication with the SMTP server when email messages are sent.

```
SMTPServerHost=swrba.mail.server
SMTPServerPort=25
SMTPUserName=\ (*1)
SMTPPassword=\ (*1)
ServerBaseURL=http://ssoserver.example.com:80/console/
ServerEmailBaseURL=http://ssoserver.example.com:80/console/
```

*1: Ensure you insert a space after the "\" symbol.

2. Configuration file for the mail sender (emailaddress.conf)

```
ServerEmailAddress=swrbamailuser@swrba.mail.server
```

4. Register the mail server and mail sender information with Systemwalker Runbook Automation. Register both the mail server and mail sender definitions.

1. Registering the SMTP server:

[Windows]

```
> [Interstage BPM installation directory]\server\deployment\bin
\importProperties.batsmtpserver.conf [the account for accessing the Process Management Database]
[password for the account for accessing the Process Management Database]
```

[Linux]

```
# /opt/FJSVibpm/server/deployment/bin/importProperties.sh smtpserver.conf [the account for
accessing the Process Management Database] [password for the account for accessing the Process
Management Database]
```

5. Registering the mail sender:

[Windows]

```
> [Interstage BPM installation directory]\server\deployment\bin
\importProperties.batemailaddress.conf [the account for accessing the Process Management
Database] [password for the account for accessing the Process Management Database] Default
```

[Linux]

```
# /opt/FJSVibpm/server/deployment/bin/importProperties.sh emailaddress.conf [the account for
accessing the Process Management Database] [password for the account for accessing the Process
Management Database] Default
```

Ensure you specify the "Default" option at the end.

6. Restart Systemwalker Runbook Automation.

To reflect the information that has been set up, stop Systemwalker Runbook Automation using the swrba_stop command, and then, restart it again using the swrba_start command.

1. Stopping Systemwalker Runbook Automation:

[Windows]

```
> [Installation directory for the Systemwalker Runbook Automation Management Server]\bin
\swrba_stop
```

[Linux]

```
# /opt/FJSVswrbam/bin/swrba_stop
```

2. Starting Systemwalker Runbook Automation:

[Windows]

```
> [Installation directory for the Systemwalker Runbook Automation Management Server]\bin
\swrba_start
```

[Linux]

```
# /opt/FJSVswrbam/bin/swrba_start
```

8.4.2 Changing the Management Server's host name/IP address

To change the host name/IP address of the server running the Management Server, follow the steps below.

📛 Note

. . . .

- Before preforming this task, confirm that own host name is not specified in host file. If it is specified, delete it. Redefine deleted item after finishing this task.

. . . .

🅿 Point

. . . .

- Before performing this task, it is recommended that you back up files in case any abnormalities occur. Refer to "8.3 Backup and Restoration" for information on how to back up files.

- To change the host name/IP address of the server running the Management Server, one writable empty directory will be needed as a work area. Do not delete this work area while changing work will be completed.

- It is necessary to change the settings of the Linked Server/Relay Server in accordance with the changed host name/IP address of the server running the Management Server. Refer to "8.4.3 Changing Host Name and IP Address of Linked Servers and Relay Servers" for details.

- If either Systemwalker Centric Manager or Systemwalker Operation Manager has been installed and is running on the server operating Management Server, it is necessary to change the host name/IP address changes of these products (refer to the *Systemwalker Centric Manager Installation Guide* or *Systemwalker Operation Manager Installation Guide* for details). However, it is not necessary to execute the Interstage system information export/import mentioned in *Systemwalker Centric Manager Installation Guide*.

・・

1. To change the host name/IP address, one writable empty directory will be needed as a work area. Create empty directory of the absolute path within 25 alphanumeric characters. The rough amount of space for work area is as follows.

> The requisite amount of work area =
>
> Total amount of under install directory of Interstage Application Server (*1) x 1.2

(*1) The install directory of Interstage Application Server is as below.

[Windows]

It is **any** of the following directory.

- If standard install
  C:\Fujitsu\Systemwalker\IAPS

- If custom istall
  [The directory specified as install direction]\IAPS

[Linux]

It is total amount of the following directory

/var/opt/FJSVejb	/var/opt/FJSVena	/var/opt/FJSVes
/var/opt/FJSVextp	/var/opt/FJSVihs	/var/opt/FJSVisas
/var/opt/FJSVisgui	/var/opt/FJSVisjee	/var/opt/FJSVisjmx
/var/opt/FJSVisscs	/var/opt/FJSVj2ee	/var/opt/FJSVjms
/var/opt/FJSVjs2su	/var/opt/FJSVjs5	/var/opt/FJSVod
/var/opt/FJSVots	/var/opt/FJSVporb	/var/opt/FJSVshs
/var/opt/FJSVssoac	/var/opt/FJSVssoaz	/var/opt/FJSVssocm
/var/opt/FJSVssofs	/var/opt/FJSVssosv	/var/opt/FJSVtd
/etc/opt/FJSVejb	/etc/opt/FJSVes	/etc/opt/FJSVextp
/etc/opt/FJSVihs	/etc/opt/FJSVisas	/etc/opt/FJSVisgui
/etc/opt/FJSVisjee	/etc/opt/FJSVisjmx	/etc/opt/FJSVisscs
/etc/opt/FJSVj2ee	/etc/opt/FJSVjms	/etc/opt/FJSVjs2su
/etc/opt/FJSVjs5	/etc/opt/FJSVod	/etc/opt/FJSVots
/etc/opt/FJSVporb	/etc/opt/FJSVsclr	/etc/opt/FJSVshs
/etc/opt/FJSVssoac	/etc/opt/FJSVssoaz	/etc/opt/FJSVssofs
/etc/opt/FJSVssosv	/etc/opt/FJSVtd	

2. Stop Systemwalker Runbook Automation.
   [Windows]

```
<Systemwalker Runbook Automation Management Server installation directory>\bin\swrba_stop
```

   [Linux]

```
/opt/FJSVswrbam/bin/swrba_stop
```

3. If Systemwalker Centric Manager Operation Management Server is installed, then stop all Systemwalker Centric Manager functions.
   [Windows]

   ```
   <Systemwalker Centric Manager installation directory>\MPWALKER.DM\bin\pcentricmgr /a
   ```

   [Linux]

   ```
   /opt/systemwalker/bin/pcentricmgr -a
   ```

4. Execute the host name/IP address pre-change command.
   [Windows]

   ```
   <Systemwalker Runbook Automation Management Server installation directory>\bin
   \swrba_pre_chghostinf -i <pre-change IP address> -d <work area>
   ```

   [Linux]

   ```
   /opt/FJSVswrbam/bin/swrba_pre_chghostinf -i <pre-change IP address> -d <work area>
   ```

5. Change the host name/IP address of servers running Management Server according to the OS operation method.

   P Point
   . . . .
   When the server host name is changed in Windows, it is also necessary to restart the server. If Systemwalker Centric Manager Operation Management Server is installed, stop all Systemwalker Centric Manager functions after start:

   ```
   <Systemwalker Centric Manager installation directory>\MPWALKER.DM\bin\pcentricmgr /a
   ```
   . . . .

6. Execute the host name/IP address post-change command.
   [Windows]

   ```
   <Systemwalker Runbook Automation Management Server installation directory>\bin
   \swrba_post_chghostinf -host <name> -i <IP address>
   ```

   [Linux]

   ```
   /opt/FJSVswrbam/bin/swrba_post_chghostinf - h <host name> -i <IP address>
   ```

7. If Systemwalker Centric Manager Operation Management Server is installed, then start all Systemwalker Centric Manager functions.
   [Windows]

   ```
   <Systemwalker Centric Manager installation directory>\MPWALKER.DM\bin\scentricmgr /a
   ```

   [Linux]

   ```
   /opt/systemwalker/bin/scentricmgr -a
   ```

8. Start Systemwalker Runbook Automation.
   [Windows]

   ```
   <Systemwalker Runbook Automation Management Server installation directory>\bin\swrba_start
   ```

   [Linux]

   ```
   /opt/FJSVswrbam/bin/swrba_start
   ```

Note
. . . .

- Mail Server (SMTP Server) information recorded on the Management Server cannot be changed with this procedure. If a mail server has been built on the server running the Management Server, it is necessary to execute "8.4.1 Changing the Mail Server Information Registered on the Management Server".

- If Interstage Single Sign-On is used as the authentication infrastructure, perform "8.4.2.1 Changing Interstage Single Sign-On Host Names" after this procedure.

8.4.2.1 Changing Interstage Single Sign-On Host Names

To change the Interstage Single Sign-On host name of the server used to run the Management Server, follow the steps below.

Note

- This procedure is not necessary in environments in which the Interstage Single Sign-On authentication infrastructure is not used.

1. Stop the Web server.

   Execute the following command as a user with administrator privileges:

   [Windows]

   ```
   ihsstop -all
   ```

   [Linux]

   ```
   /opt/FJSVihs/bin/ihsstop -all
   ```

2. Change the FQDN in the configuration file.

   - [Interstage HTTP Server] (Authentication Server)

     [Windows]

     ```
     <Systemwalker Runbook Automation Management Server installation directory>\IAPS\F3FMihs
     \servers\SSOauth\conf\httpd.conf
     ```

     [Linux]

     ```
     /var/opt/FJSVihs/servers/SSOauth/conf/httpd.conf
     ```

     - Edit the ServerName directive:

       ```
       ServerName <new FQDN>
       ```

   - [Interstage Single Sign-On Authentication Server

     [Windows]

     ```
     <Systemwalker Runbook Automation Management Server installation directory>\IAPS\F3FMsso
     \ssoatcag\conf\ssoatcag.conf
     ```

     [Linux]

     ```
     /etc/opt/FJSVssoac/conf/ssoatcag.conf
     ```

     - Edit the authentication infrastructure URL:

       ```
       authenticate-url=https://<new FQDN>:10443
       ```

   - [Interstage Single Sign-On Repository Server]

     [Windows]

     ```
     <Systemwalker Runbook Automation Management Server installation directory>\IAPS\F3FMsso
     \ssoatcsv\conf\ssoatcsv.conf
     ```

     [Linux]

```
/etc/opt/FJSVssosv/conf/ssoatcsv.conf
```

- Edit the authentication infrastructure URL:

```
authenticate-url=https://<new FQDN>:10443
```

- [Interstage Single Sign-On Session Management Server]

[Windows]

```
<Systemwalker Runbook Automation Management Server installation directory>\IAPS\F3FMsso
\ssoatcsv\conf\ssossmgr.conf
```

[Linux]

```
/etc/opt/FJSVssosv/conf/ssossmgr.conf
```

- Edit the authentication infrastructure URL:

```
authenticate-url=https://<new FQDN>:10443
```

- [Interstage Single Sign-On Business Server

[Windows]

```
<Systemwalker Runbook Automation Management Server installation directory>\IAPS\F3FMsso
\ssoatzag\conf\ssoatzag.conf
```

[Linux]

```
/etc/opt/FJSVssoaz/conf/ssoatzag.conf
```

- Edit the Business Server public URL, the authentication infrastructure URL, the repository server FQDN, and the authentication server URL:

```
FQDN=http://<new FQDN>:80
AuthServerURL=https://<new FQDN>:10443/ssoatcag
repository-server=<new FQDN>:10550
authserver-connect-url=https://<new FQDN>:10443/ssoatcag
```

3. Change the site certificate.

   1. Create the site certificate.

      Refer to "3.1.3.1.2 Creating the Interstage Certificate Environment and the Application to Obtain the Certificate that is used for SSL Communication" for details. At the prompt "What is your first and last name?", specify the post-change host name FQDN (Fully Qualified Domain Name).

   2. Register the new site certificate.

      Refer to "3.1.3.1.3 Registering Certificates used in SSL Communication" for details.

   3. Using the Interstage Management Console, update the SSL definition.

      1. Enter the following URL in the browser to start the Interstage Management Console login window.

         ```
         http://<Management Server host name>:<Interstage Management Console port number>/
         IsAdmin
         ```

         Note that, in environments in which Systemwalker Service Catalog Manager is installed, the URL (https) may be as follows:

         ```
         https://<Management Server host name>:<Interstage Management Console port number>/
         IsAdmin
         ```

2. Enter the following login ID and password in the login window, then click the **Login** button.

[Windows]

User ID	Password
Administrator	Password for the administrator

[Linux]

User ID	Password
root	Password for the root account

3. Click **System** >> **Security** >> **SSL** >> **<*SSL name*>** >> **SSL Settings**, and change the site certificate nickname to the new site certificate nickname.

4. As a user with administrator privileges, delete the pre-change site certificate (specify the old nickname).

[Windows]

```
scsdelete -n <old nickname>
```

[Linux]

Before executing the command, set the JDK or JRE installation path in the JAVA_HOME environment variable.

```
JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
scsdelete -n <old nickname>
```

4. As a user with administrator privileges, update the encrypted information for the repository server.

[Windows]

```
ssoupsid
```

[Linux]

```
/opt/FJSVssosv/bin/ssoupsid
```

5. Using the Interstage Management Console, download the authentication infrastructure file.

Click **System** >> **Security** >> **Single Sign-on** >> **Authentication Infrastructure** >> **Authentication infrastructure setup file**, set the **Password**, then click the **Download** button.

Refer to "Constructing a Repository Server (One Server or Update System)" in the *Interstage Application Server Single Sign-on Operator's Guide* for details.

6. As a user with administrator privileges, update the encrypted information for the authentication server.

Specify the full path of the authentication infrastructure configuration file downloaded in 5. Note that the file must be deleted after the command is executed.

[Windows]

```
ssoimpac <authentication infrastructure configuration file>
```

[Linux]

```
/opt/FJSVssoac/bin/ssoimpac <authentication infrastructure configuration file>
```

7. Using the Interstage Management Console, update the site definition.

Click **System** >> **Security** >> **Single Sign-on** >> **Authentication Infrastructure** >> **Repository Server** >> **Protection resource** >> **Old FQDN:80** >>**Settiongs** >>**Site Definition**. In **FQDN Port number**, change the FQDN as follows:

```
<new FDQN>:80
```

8. Using the Interstage Management Console, download the business system configuration file.

   Click **System** >> **Security** >> **Single Sign-on** >> **Authentication Infrastructure** >> **Business system setup file**, then click the **Download** button.

   Refer to "Preparations for Setting up a Business System" in the *Interstage Application Server Single Sign-on Operator's Guide* for details.

9. As a user with administrator privileges, import the business server settings:

   Specify the full path of the business system configuration file downloaded in 8. Note that the file must be deleted after the command is executed.

   [Windows]

   ```
   ssoimpaz <business system configuration file>
   ```

   [Linux]

   ```
   /opt/FJSVssoaz/bin/ssoimpaz <business system configuration file>
   ```

10. As a user with administrator privileges, start the Web server.

    [Windows]

    ```
    ihsstart -all
    ```

    [Linux]

    ```
    /opt/FJSVihs/bin/ihsstart -all
    ```

11. Try to log in to the Web console.

8.4.3 Changing Host Name and IP Address of Linked Servers and Relay Servers

If the host name or port number of a Management Server, Linked Server or Relay Server has been changed, then follow the steps below:

1. Edit cmdbsetup.ini.

   If the host name or port number of the Management Server has been changed:

   ```
   [InfoFederation]
   FedIp=<Management Server new host name>
   FedPort=<Management Server new port number (default: 80)>
   ```

   If the host name or port number of the Agent has been changed:

   ```
   [InfoMDR]
   MdrIp=<Agent new host name>
   MdrPort=<Agent new port number (default: 18444)>
   ```

   The file name and location are displayed below:

   [Windows]

   ```
   <Agent installation directory>\CMDB\cmdbsetup.ini
   ```

   [Linux]

   ```
   /opt/FJSVcmdba/resources/cmdbsetup.ini
   ```

2. Set up any Linked Servers or Relay Servers.

   Refer to the 3.2 Setting up Linked Servers or 3.3 Setting up Relay Servers for details on the Agent setup procedure. Note that there is no need to cancel the settings for the Agent first. The setup procedure can be performed even if the Agent has already been set up.

📝 **Note**

. . . .

- The changes to the host name or port number of the Linked Server or Relay Server are notified to the CMDB Manager when update information is next collected and reflected to the CMDB Manager.

. . . .

8.5 Applying Updates to Systemwalker Runbook Automation

This section describes how to apply updates to Systemwalker Runbook Automation.

Use UpdateAdvisor to apply updates to Systemwalker Runbook Automation. Refer to UpdateSite for information on updates to be applied to Systemwalker Runbook Automation.

8.5.1 Checking Updates

Systemwalker Runbook Automation has many software products.

So check if the updates are released for all software products used by Systemwalker Runbook Automation.

Show the checking product list must be checked. To check updates, use update site.

Management Server

Product Name	Version Level
Systemwalker Runbook Automation	V15.1.0
Interstage Application Server Enterprise Edition	V10.0.0
Systemwalker Operation Manager Enterprise Edition	**[Windows]** V13.4.0B **[Linux]** V13.4.1A

Relay Server/Linked Server

Product Name	Version Level
Systemwalker Runbook Automation	V15.1.0

Business Server

Product Name	Version Level
Systemwalker Runbook Automation	V15.1.0

Deployment Computer

Product Name	Version Level
Systemwalker Runbook Automation	V15.1.0

8.5.2 Applying Updates to the Management Server

This section describes how to apply updates to the Management Server.

P Point

• •

[Linux]

Apply the updates in single-user mode. Return to multi-user mode after the updates have been applied.

• •

[Windows]

To stop the services, apply the updates and restart the services, follow the steps below:

Stopping Systemwalker Runbook Automation

⬇

Stopping Agents (*1)

⬇

Stopping Systemwalker Operation Manager

⬇

Stopping Interstage (*1)

⬇

Stopping the CMDB Manager service

⬇

Stopping the Interstage Directory Service

⬇

Stopping the Java EE Service (*1)

⬇

Stopping the Interstage Management Console (*1)

⬇

Stopping the file transfer infrastructure

⬇

Applying updates

⬇

Starting the file transfer infrastructure

⬇

```
┌─────────────────────────────────────────────────┐
│ Starting the Java EE Service (*1)               │
└─────────────────────────────────────────────────┘

                    ⬇

┌─────────────────────────────────────────────────┐
│ Starting the Interstage Management Console (*1) │
└─────────────────────────────────────────────────┘

                    ⬇

┌─────────────────────────────────────────────────┐
│ Starting the Interstage Directory Service       │
└─────────────────────────────────────────────────┘

                    ⬇

┌─────────────────────────────────────────────────┐
│ Starting the CMDB Manager service               │
└─────────────────────────────────────────────────┘

                    ⬇

┌─────────────────────────────────────────────────┐
│ Starting Interstage (*1)                        │
└─────────────────────────────────────────────────┘

                    ⬇

┌─────────────────────────────────────────────────┐
│ Starting Systemwalker Operation Manager         │
└─────────────────────────────────────────────────┘

                    ⬇

┌─────────────────────────────────────────────────┐
│ Starting Agents (*1)                            │
└─────────────────────────────────────────────────┘

                    ⬇

┌─────────────────────────────────────────────────┐
│ Starting Systemwalker Runbook Automation        │
└─────────────────────────────────────────────────┘
```

*1: Only these services need to be stopped and restarted if the Management Server has not been set up.

Stopping Systemwalker Runbook Automation

If the Systemwalker Runbook Automation Manager service is running, use the Services feature of Windows, as a user with administrator privileges, to stop the service.

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**. Doing this displays a list of services available on the system.

2. If the status of the Systemwalker Runbook Automation Manager is **Started**, right-click the service and click **Stop**.

If this service is not running, execute the command to stop Systemwalker Runbook Automation. Refer to 4.1.2 Stopping Systemwalker Runbook Automation for details.

Stopping Agents

1. Issue the command below as a user with administrator privileges:

   ```
   "%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
   ```

Stopping Systemwalker Operation Manager

1. Issue the command below as a user with administrator privileges:

```
poperationmgr
```

Stopping Interstage

1. Issue the command below as a user with administrator privileges:

```
isstop -f
```

Stopping the CMDB Manager service

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools,** and then, double-click **Services**.

2. Right-click the following services, and click the **Stop** button.

    - Shunsaku Director contents

    - Shunsaku Director metadata

    - Shunsaku Searcher cmdbs01

    - Shunsaku Searcher cmdbs02

    - Shunsaku Searcher cmdbs03

Stopping the Interstage Directory Service

P Point

. . . .

Only follow the steps below if the Interstage Directory Service is selected as the LDAP directory to be used and the Interstage Directory Service is used on the Management Server

. . . .

1. Open the login window for the Interstage Management Console by entering the following URL in a Web browser.

```
http://<Interstage Directory Service host name>:[port number for the Interstage Management Console]/IsAdmin
```

2. If installed Systemwalker Service Catalog Manager, it will be shown the following URL

```
https://<Interstage directory service host name>:[port number for the Interstage Management Console]/IsAdmin
```

3. Specify the following login ID and password in the login window, and then, click the **Login** button.

User ID	Password
Administrator	Password for the administrator

4. Open the repository window by selecting **System** >> **Service** >> **repository** from the tree view (the pane on the left-hand side of the window).

5. Select the repository being used, and then, click the **Stop** button. Check the message indicating that the repository has stopped.

6. Log out.

Stopping the Interstage Management Console

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select **Interstage Operation Tool** in the **Services** dialog box, and click the **Stop** button.

3. Select **Interstage Operation Tool(FJapache)**, and click the **Stop** button.

4. Select **Interstage JServlet(OperationManagement)**, and click the **Stop** button.

Stopping the Java EE Service

Use the following procedure to stop the Java EE Service.

1. Use the Windows(R) Services function, as a user with administrator privileges, and stop the message broker.

   Select the Interstage Message Queue Broker Service in the **Services** dialog box (opened from **Administrative Tools** under **Control Box**), and then, click the **Stop** button.

2. Stop the Interstage Java EE Node Agent Service by executing the following command as a user with administrator privileges:

   ```
   ijnastop
   ```

3. Stop the Interstage Java EE DAS Service by executing the following command as a user with administrator privileges:

   ```
   ijdasstop
   ```

Stopping the file transfer infrastructure

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select **Systemwalker File Transfer Library Control** in the **Services** dialog box, and click the **Stop** button.

Applying updates

Refer to the update information file to apply the updates.

Starting the file transfer infrastructure

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select **Systemwalker File Transfer Library Control** in the **Services** dialog box and click the **Start** button.

Starting the Java EE Service

Use the following procedure to start the Java EE Service.

1. Start the Interstage Java EE DAS Service by executing the following command as a user with administrator privileges:

   ```
   ijdasstart
   ```

2. Start the Interstage Java EE Node Agent Service by executing the following command as a user with administrator privileges:

   ```
   ijnastart
   ```

3. Start the message broker as a user with administrator privileges.

   Use the Windows(R) Services function to start the message broker.

   Select the Interstage Message Queue Broker Service in the **Services** dialog box (opened from **Administrative Tools** under **Control Box**), and then, click the **Start** button.

Starting the Interstage Management Console

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select **Interstage Operation Tool** in the **Services** dialog box, and click the **Start** button.

Starting the Interstage Directory Service

Only follow the steps below if the Interstage Directory Service is selected as the LDAP directory to be used and the Interstage Directory Service is used on the Management Server.

1. Open the login window for the Interstage Management Console by entering the following URL in a Web browser.

   http://<*Interstage Directory Service host name*>:[*port number for the Interstage Management Console*]/IsAdmin

2. If installed Systemwalker Service Catalog Manager, it will be shown the following URL

   https://<*Interstage directory service host name*>:[*port number for the Interstage Management Console*]/IsAdmin

3. Specify the following login ID and password in the login window, and then, click the **Login** button.

User ID	Password
Administrator	Password for the administrator

4. Open the repository window by selecting **System** >> **Service** >> **repository** from the tree view (the pane on the left-hand side of the window).

5. Select the repository being used, and then, click the **Start** button. Check the message indicating that the repository has started.

6. Log out.

Starting the CMDB Manager service

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select the following services in the dialog box, and click the **Start** button.

   - Shunsaku Director contents

   - Shunsaku Director metadata

   - Shunsaku Searcher cmdbs01

   - Shunsaku Searcher cmdbs02

   - Shunsaku Searcher cmdbs03

   - Shunsaku Conductor cmdbc

   - Shunsaku Sorter cmdbo01

Starting Interstage

1. Issue the command below as a user with administrator privileges:

   ```
   isstart
   ihsstart -all
   ```

Starting Systemwalker Operation Manager

1. Issue the command below as a user with administrator privileges

   ```
   soperationmgr
   ```

Starting Agents

1. Issue the command below as a user with administrator privileges:

"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start

Starting Systemwalker Runbook Automation

Refer to "4.1.1 Starting Systemwalker Runbook Automation" for details.

8.5.3 Applying Updates to Linked Servers and Relay Servers

This section describes how to apply updates to Linked Servers, Relay Servers, and Business Servers.

🅿 Point

. . . .

[Linux]

Apply the updates in single-user mode. Return to multi-user mode after the updates have been applied.

. . . .

[Windows]

To stop the services, apply the updates, and restart the services, follow the steps below:

Stopping Agents

⬇

Stopping the file transfer infrastructure

⬇

Applying updates

⬇

Starting the file transfer infrastructure

⬇

Starting Agents

Stopping Agents

1. Issue the command below as a user with administrator privileges:

"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop

Stopping the file transfer infrastructure

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select **Systemwalker File Transfer Library Control** in the **Services** dialog box, and click the **Stop** button.

Applying updates

Refer to the update information file to apply the updates..

Starting the file transfer infrastructure

Follow the steps below as a user with administrator privileges:

1. Click **Start** >> **Control Panel** >> **Administrative Tools,** and then, double-click **Services**.

2. Select **Systemwalker File Transfer Library Control** in the **Services** dialog box, and click the **Start** button.

Starting Agents

1. Issue the command below as a user with administrator privileges:

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
```

8.5.4 Applying Updates to the Business Server

The procedure used to apply updates to the Business Server is shown below.

Point

[Linux] [Solaris]

Apply the updates in single user mode. Restore the multi user mode after the updates have been applied.

[Windows]

Use the following procedure to stop the services, apply the updates, and restart the services.

Stopping file transfer infrastructure

Applying updates

Starting file transfer infrastructure

Stopping file transfer infrastructure

Stop the file transfer infrastructure.

Use the services feature of Windows to stop the services with a user that has administrator privileges.

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select **Systemwalker File Transfer Library Control**, and click the **Stop** button.

Applying updates

Apply the updates according to the explanations for the updates to be applied.

Starting file transfer infrastructure

Start the file transfer infrastructure.

Use the services feature of Windows to start the services with a user that has administrator privileges.

1. Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**.

2. Select **Systemwalker File Transfer Library Control**, and click the **Start** button.

8.5.5 Applying Updates to the Development Computer

This section describes how to apply updates to Development Computers.

Stopping Systemwalker Runbook Automation Studio

Applying updates

Starting Systemwalker Runbook Automation Studio

Stopping Systemwalker Runbook Automation Studio

Refer to the *Systemwalker Runbook Automation BPM Studio User's Guide* for details.

Applying updates

Refer to the update information file to apply the updates.

Starting Systemwalker Runbook Automation Studio

Refer to the *Systemwalker Runbook Automation BPM Studio User's Guide* for details.

8.6 Changing the Password for Users that Systemwalker Runbook Automation Uses for Internal Control

This section describes how to change the password for users that Systemwalker Runbook Automation uses internally.

Follow these steps in accordance with the security policy for the organization installing Systemwalker Runbook Automation.

- User for accessing the database required to manage processes (the access account for the Process Management Database)

- User required to manage the LDAP directory (the LDAP administrator DN)

- User required to control processes (the user for process control)

- User required to start a schedule (user for schedule startup)

8.6.1 Changing the Password for the Account Used to Access the Process Management Database

This section describes how to change the password for the account used to access the databases that are required for Systemwalker Runbook Automation to manage processes internally.

When Systemwalker Runbook Automation is set up for the first time, the following user is created by default:

Account name	swrbadb

Follow the steps below to change the password:

1. Stop Systemwalker Runbook Automation.

2. Change the password for the account used to access the database.

3. Start Systemwalker Runbook Automation.

Stopping Systemwalker Runbook Automation

Refer to "4.1.2 Stopping Systemwalker Runbook Automation" for information on how to stop the Management Server.

Change the password for the account used to access the database.

Follow the steps below:

1. Issue the command below:

    [Windows]

<Systemwalker Runbook Automation installation directory>\bin\swrba_db_change_password

    [Linux]

/opt/FJSVswrbam/bin/swrba_db_change_password

    Refer to "swrba_db_change_password" in the *Systemwalker Runbook Automation Reference Guide* for details.

Starting Systemwalker Runbook Automation

Refer to "4.1.1 Starting Systemwalker Runbook Automation" for details.

8.6.2 Changing the Password for the LDAP Administrator DN

This section describes how to change the password for the LDAP administrator DN, which is required for Systemwalker Runbook Automation to update the LDAP directory.

This section assumes the following:

Administrator DN	cn=manager,ou=interstage,o=fujitsu,dc=com

See

Refer to " Registering Users, Groups and Organizational Units with the LDAP Directory" for information on how to create users.

Follow the steps below:

1. Stop Systemwalker Runbook Automation.

2. Change the LDAP information.

3. Change the environment for Systemwalker Runbook Automation.

4. Start Systemwalker Runbook Automation.

Stopping Systemwalker Runbook Automation

Refer to "4.1.2 Stopping Systemwalker Runbook Automation" for details.

Changing the LDAP information

Refer to the manuals for the LDAP directory being used.

Changing the environment for Systemwalker Runbook Automation

Follow the steps below to register the password:

1. Issue the command below:

   [Windows]

   > *<Systemwalker Runbook Automation installation directory>*\bin\swrba_regist_password

   [Linux]

   > /opt/FJSVswrbam/bin/swrba_regist_password

   Refer to the *Systemwalker Runbook Automation Reference Guide* for details on the command.

At the dialog box, specify the user for process control and register the password.

Starting Systemwalker Runbook Automation

Refer to "4.1.1 Starting Systemwalker Runbook Automation" for details on how to start the Management Server.

8.6.3 Changing the Password for Process Control User/Schedule Startup

This section describes how to change the password for the user that Systemwalker Runbook Automation uses to control processes internally and the user that is required to start a schedule.

This section assumes that each user ID is the following:

User ID for process control	swrbaadmin
User ID for schedule startup	swrbasch

🔖 See
....
Refer to Registering Users, Groups and Organizational Units with the LDAP Directory" for information on how to create users.
....

Follow the steps below:

1. Stop Systemwalker Runbook Automation.

2. Change the LDAP information.

3. Change the environment for Systemwalker Runbook Automation.

4. Start Systemwalker Runbook Automation.

Stopping Systemwalker Runbook Automation

Refer to "4.1.2 Stopping Systemwalker Runbook Automation" for details on how to stop the Management Server.

Changing the LDAP information

Refer to the manuals for the LDAP directory being used.

Changing the environment for Systemwalker Runbook Automation

Follow the steps below to register the password:

1. Issue the command below:

   Note that, since an enquiry window will be displayed when the user is changed, specify the user type to be changed ("process control user" or "schedule startup user") then register the password.

   [Windows]

   ```
   <Systemwalker Runbook Automation installation directory>\bin\swrba_regist_password
   ```

   [Linux]

   ```
   /opt/FJSVswrbam/bin/swrba_regist_password
   ```

   Refer to the *Systemwalker Runbook Automation Reference Guide* for details on the command.

At the dialog box, specify the User for Controlling Processes and register the password.

Starting Systemwalker Runbook Automation

Refer to "4.1.1 Starting Systemwalker Runbook Automation" for details on how to start the Management Server.

8.7 Changing Operating System User Passwords Used by Systemwalker Runbook Automation

Systemwalker Runbook Automation registers and uses the following users as the operating system users for starting the services. This section explains how to change the passwords for these users.

This task should be performed in accordance with the security policies of the organization installing Systemwalker Runbook Automation.

[Windows]

- swrbadbuser

- swrbajobuser

[Linux]

- swrbadbuser

Use the following procedure for changing the password:

1. Stop Systemwalker Runbook Automation.

2. Stop the Java EE Service.

   1. As a user with administrator privileges, use the **Services** feature of Windows to stop the message broker.

      Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**. From the displayed list of services, right-click the **Interstage Message Queue Broker** service and click the **Stop** button.

   2. Use the following command to stop the Interstage Java EE Node Agent Service.

      ```
      ijnastop
      ```

   3. Use the following command to stop the Interstage Java EE DAS Service.

      ```
      ijdasstop
      ```

3. Change the password in accordance with the method for the operating system.

4. For Windows, change the password for the service startup account in accordance with the method for the operating system. Passwords must be changed for the following services:

 - Services for which the password must be changed when the password for swrbajobuser is changed:

   - Systemwalker MpMjes*n* (*1)

     *1: "*n*" represents the subsystem number specified in the **Advanced Setup for Scheduling** window during installation. The default value is 9.

   - Interstage Java EE Node Agent

 - Services for which the password must be changed when the password for swrbadbuser is changed:

   - Systemwalker Runbook Automation DB Service

5. Start the Java EE Service.

   1. As a user with administrator privileges, use the following command to start the Interstage Java EE DAS Service:

   ```
   ijdasstart
   ```

   2. Use the following command to start the Interstage Java EE Node Agent Service.

   ```
   ijnastart
   ```

   3. Start the message broker.

      Use the Services feature of Windows to start the message broker.

      Click **Start** >> **Control Panel** >> **Administrative Tools**, and then, double-click **Services**. From the displayed list of services, select the **Interstage Message Queue Broker** service and click the **Start** button.

6. Start Systemwalker Runbook Automation.

8.8 Deleting Process Instances

If large numbers of unnecessary process instances have accumulated because a certain period of time has elapsed since the completion of processing, it will cause the Process Management Database area to become compressed and will cause performance to decline. These process instances can be deleted using swrba_admin (the admin command).

🛈 Note

- When this task is performed, the process instance information will be deleted from the database. Before the process instances are deleted, the swrba_admin (admin command) option for obtaining the process instance detailed information can be used to obtain the process instance history information in XML format. Because of this history information, the process instance history information can be checked even after the process instance has been deleted from the database.

- When deleting large numbers of process instances, consider the effect on process instances in progress by performing this task outside operating hours. By using the swrba_admin (admin command) option for searching process instances, you can check how many deletion target process instances there are.

Execution example

Examples of the command execution to delete process instances for which a certain period of time has elapsed are shown below.

In these examples, process instances having the status "closed" that were started through 2010 are deleted.

[Windows]

```
[Systemwalker Runbook Automation installation directory]\bin\swrba_admin pi-delete -user swrbaadmin -
password systemwalker#1  -startedafter 2010-01-01 -startedbefore 2010-12-31 -state closed
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_admin pi-delete -user swrbaadmin -password systemwalker#1  -startedafter
2010-01-01 -startedbefore 2010-12-31 -state closed
```

Refer to the *Systemwalker Runbook Automation Reference Guide* for information on swrba_admin (the admin command).

8.9 Checking Installation Status of Systemwalker Runbook Automation

To check instllation status of Systemwalker Runbook Automation, execute the following procedure.

[Windows]

1. Select **Fujitsu** >> **Uninstall (middleware)** from **Programs** of **Start** menu or **All Programs.**

   Uninstall (middleware) window will be displayed. The following is an example for Management Server.

Currently installed products tab

In **Currently installed products** tab, check installed products.

The meaning of item is shown in tab are below.

- Software Name

  The name of installed software will be displayed. You can confirm installed Fujitsu middleware products by using Cloud Infrastructure Management Software.

- Description

  The description of installed software will be displayed.

- Version

  The version and level of installed software will be displayed.

- Date of install

  The date when software was installed will be displayed.

- Install directory

    The directory where software has been installed will be displayed.

Incomplete install tab

    In Incomplete install tab, the information of unsuccessful installation of software will be displayed.

    The shown item and meaning are same with of **Currently installed products** tab.

2. When finish to confirm, click **Close** button, and then **Uninstall (middleware)** window will be closed.

[Linux]

1. Execute the following command.

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

2. **Uninstall (middleware)** window will be displayed. The following is an example for Management Server.

```
Uninstall (middleware) has been download...


Currently installed products
1. Systemwalker Runbook Automation ( Management Server )  V15.1.0

Input uninstalled software number
[number,q]
=>q
```

Currently installed products

    The name of installed software and version level will be displayed. You can confirm installed Fujitsu middleware products by using Cloud Infrastructure Management Software and version and level.

Incomplete install

    If there are unsuccessful installation of software, the software and version level of unsuccessful installation of software will be displayed.

3. Click "q" and close window.

Chapter 9 Port Numbers

Systemwalker Runbook Automation uses the communication paths described in this chapter after it is installed. When Systemwalker Runbook Automation is installed or configured, entries are added to the following "services" file for the TCP/UDP ports in the "9.1 Port Numbers" table shown in the "Service name" column.

[Windows]

C:\Windows\system32\drivers\etc\services

[Linux]

/etc/services

Each port number must be unique within the network. If a port number, refer to "9.1 Port Numbers", is already in use by another application, the following actions must be taken:

- If the port number can be changed

  Change the port number using the procedure described in "9.2 How to Change Port Numbers".

- If the port number cannot be changed

  Change the port number used by the other application to a port number that does not conflict with Systemwalker Runbook Automation.

9.1 Port Numbers

Management Server

Port numbers that should accept from external server

Function	Port number/protocol used	Configurable
Web server (Interstage HTTP Server)	80/tcp	Only during installation
For LDAP connection	389/tcp	Only during setup
For SSO Authentication Server (*1)	10443/tcp	No
For Interstage Management Console	12000/tcp	Yes
HTTP listener for operation management	12001/tcp	Yes
File transfer infrastructure	9664/tcp	Yes
For CMDB	18443/tcp 18444/tcp	No
SNMP	161/udp	No

*1: This function is used when an authentication server for Interstage Single Sign-On is used.

Port numbers used internal

Function	Port number/protocol used	Configurable
CORBA Service	8002/tcp	Yes
HTTP listener	28080/tcp	Yes
IIOP	23600/tcp	Yes
IIOP_SSL	23601/tcp	Yes

Function	Port number/protocol used	Configurable
IIOP_MUTUALAUTH	23602/tcp	Yes
JMX_ADMIN	8686/tcp	Yes
Message broker	7676/tcp	Only during setup
Process management	9657/tcp	Only during setup
Those used with the server function	23700/tcp	Only during setup
Scheduling	9690/tcp 9691/tcp	Yes
For SSO Authentication Server (*1)	10550/tcp 10555/tcp	No
For CMDB	13300/tcp 13301/tcp 13321/tcp 13322/tcp 13323/tcp 13324/tcp 13325/tcp 13326/tcp 13327/tcp 13328/tcp 13331/tcp 13332/tcp 13333/tcp	No
JMX Service	12200/tcp 12210/tcp	Yes
Communication infrastructure	18005/tcp 18009/tcp	Yes
RSH and REXEC	1014/tcp 1015/tcp 1016/tcp 1017/tcp 1018/tcp 1019/tcp 1020/tcp 1021/tcp 1022/tcp 1023/tcp	No

*1: This function is used when an authentication server for Interstage Single Sign-On is used

Linked Server/Relay Server

Port numbers that should accept from external server

Function	Port number/protocol used	Configurable
File transfer infrastructure	9664/tcp	Yes
For CMDB	18443/tcp 18444/tcp	No
SSH	22/tcp	No
IPMI	623/udp	No

Function	Port number/protocol used	Configurable
SNMP	161/udp	No
Telnet	23/tcp	No
FTP	20/tcp 21/tcp	No
RSH	514/tcp	No
REXEC	512/tcp	No

Port numbers used internal

Function	Port number/protocol used	Configurable
Communication infrastructure	18005/tcp 18009/tcp	Yes

Business Server

Port numbers that should accept from external server

Function	Port number/protocol used	Configurable
File transfer infrastructure	9664/tcp	Yes
SSH	22/tcp	No
IPMI	623/udp	No
SNMP	161/udp	No
Telnet	23/tcp	No
FTP	20/tcp 21/tcp	No
RSH	514/tcp	No
REXEC	512/tcp	No

📝 **Note**

. . . .

If Windows Server 2008 is being used as the operating system of the server of communication destination, the Windows firewall function is enabled by default, therefore firewall exceptions need to be specified for the port numbers and protocols used shown in the above list.

. . . .

9.2 How to Change Port Numbers

Changing the port number of the Web server (Interstage HTTP Server)

The port number for the Web server (Interstage HTTP Server) cannot be changed. Uninstall the product and then install it again. During the reinstallation, specify the port number for the Web server (Interstage HTTP Server).

Changing the port number of the Interstage Management Console

The port number used by the Interstage Management Console is changed via the Interstage Management Console. Refer to the Interstage Management Console help file for more details on this procedure.

Changing the port number for the HTTP listener for operation management

The port number for the HTTP listener for operation management can be changed using the "asadmin set" subcommand. Refer to the *Interstage Application Server* "System Design Guide" for information on the procedure for changing the port number.

Setting when the port number of the file transfer infrastructure overlaps

In the file transfer infrastructure, the port number: 9664 is used. If the overlap of the port number occurred in the Business Server environment, it is necessary to change the port number. Execute the changing to the Management Server that links with Business Server that is changed, or all of the Business Server that is link target of the relay server.

Changing the port number of the Business Server

[Windows]

The following port numbers that have been described to "Installation directory of Windows system\SYSTEM32\DRIVERS\ETC\SERVICES" are changed to an empty port number.

[Linux] [Solaris]

The following port numbers that have been described to "/etc/services" are changed to an empty port number.

```
dtranf02    9664/tcp           # FJSVlnkbs
```

The port number can be specified between 1-65535.

Changing the network definition of the Management Server or relay server

Specify the same value as the port number that has been described to the network definition file of the file transfer infrastructure and the port number that set to Business Server.

1. Network definition file

   [Windows]

   - Management Server

   ```
   [Installation directory of Systemwalker Runbook Automation Management Server]\SWRBAM
   \FJSVlnkbs\lnk02\gen\network_def.txt
   ```

   - Relay server

   ```
   [Installation directory of Systemwalker Runbook Automation relay server]\SWRBAA\FJSVlnkbs
   \lnk02\gen\network_def.txt
   ```

   [Linux]

   ```
   /opt/FJSVlnkbs/lnk02/GEN/network_def.txt
   ```

2. Reflect the definition information after the network definition file is changed.

   [Windows]

   - Management Server

   ```
   [Installation directory of Systemwalker Runbook Automation Management Server]\SWRBAM
   \FJSVlnkbs\lnk02\bin\f3jtlxgentrn.exe -i 02 [Installation directory of Systemwalker
   Runbook Automation Management Server]\SWRBAM\FJSVlnkbs\lnk02\gen\network_def.txt
   ```

   - Relay server

   ```
   [[Installation directory of Systemwalker Runbook Automation Relay Server]\SWRBAA\FJSVlnkbs
   \lnk02\bin\f3jtlxgentrn.exe -i 02 [[Installation directory of Systemwalker Runbook
   Automation Relay Server]\SWRBAA\FJSVlnkbs\lnk02\gen\network_def.txt
   ```

   [Linux]

```
/opt/FJSVlnkbs/lnk02/bin/f3jtlxgentrn -i 02 /opt/FJSVlnkbs/lnk02/GEN/network_def.txt
```

3. Restart the file transfer infrastructure

   [Windows]

   Restart the "Systemwalker File Transfer Library Control" service.

   [Linux]

```
# service FJSVlnkbs stop
# service FJSVlnkbs start
```

Changing the port number for the HTTP listener

The port number for the HTTP listener can be changed using the "asadmin set" subcommand. Refer to the *Interstage Application Server* "System Design Guide" for information on the procedure for changing the port number.

Changing the port number for IIOP

The port number for IIOP can be changed using the "asadmin set" subcommand. Refer to the *Interstage Application Server* "System Design Guide" for information on the procedure for changing the port number.

Changing the port number for IIOP_SSL

The port number for IIOP_SSL can be changed using the "asadmin set" subcommand. Refer to the *Interstage Application Server* "System Design Guide" for information on the procedure for changing the port number.

Changing the port number for IIOP_MUTUALAUTH

The port number for IIOP_MUTUALAUTH can be changed using the "asadmin set" subcommand. Refer to the *Interstage Application Server* "System Design Guide" for information on the procedure for changing the port number.

Changing the port number for JMX_ADMIN

The port number for JMX_ADMIN can be changed using the "asadmin set" subcommand. Refer to the *Interstage Application Server* "System Design Guide" for information on the procedure for changing the port number.

Changing the port number for schedules

The port number that Systemwalker Runbook Automation uses with schedules can be specified at installation. To change the port number after the installation, use the following procedure:

1. Stop Systemwalker Runbook Automation.
   Execute the following command.

```
<Systemwalker Runbook Automation Management Server installation directory>\bin\swrba_stop
```

2. [Windows]

   Change the following port number in the "<*installation directory for the Windows system*>\SYSTEM32\DRIVERS\ETC \SERVICES" file to a free port number.

   [Linux]

   Change the following port number in the "/etc/services" file to a free port number.

```
jobsch_winn (*1)      9690/tcp   #SWRBA Jobsch subsystem
mjsnetn (*1)          9691/tcp   #SWRBA MpMjes subsystem
```

*1: Here "*n*" is the subsystem number used by Systemwalker Runbook Automation (which is "9" by default).

*1: Here "*n*" is the subsystem number used by Systemwalker Runbook Automation (which is "9" by default).

1. Start Systemwalker Runbook Automation.
   Execute the following command.

```
<Systemwalker Runbook Automation Management Server installation directory>\bin\swrba_start
```

Changing the port number for the JMX service

The port number for the JMX service can be changed by editing the environment definition file shown below (refer to the *Interstage Application Server Operator's Guide System Design Guide* for details) .

[Windows]

```
<Interstage Application Server installation directory>\jmx\etc\isjmx.xml
```

Note: The default Interstage Application Server installation directory is "C:\Fujitsu\Systemwalker\IAPS".

[Linux]

```
/etc/opt/FJSVisjmx/isjmx.xml
```

Changing the port number for the communications infrastructure

To change the port number for the communications infrastructure, follow the steps below.

1. In the case of the Management Server, stop Systemwalker Runbook Automation.

   [Windows]

```
<Systemwalker Runbook Automation Management Server installation directory>\bin\swrba_stop
```

   [Linux]

```
/opt/FJSVswrbam/bin/swrba_stop
```

2. Stop the agent.

   [Windows]

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" stop
```

   [Linux]

```
/opt/FJSVswnc/bin/swncctrl stop
```

3. Change the port number.

   - To change the default value of 18005 to 19005:

     [Windows]

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncconf" --dtrans -a 19005
```

     [Linux]

```
/opt/FJSVswnc/bin/swncconf --dtrans -a 19005
```

   - To change the default value of 18009 to 19009:

     [Windows]

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncconf" --dtrans -c 19009
```

     [Linux]

```
/opt/FJSVswnc/bin/swncconf --dtrans -c 19009
```

4. Check the results.

[Windows]

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncconf" --dtrans -v
```

[Linux]

```
/opt/FJSVswnc/bin/swncconf --dtrans -v
```

In the example below, the port numbers specified in step 3 are displayed.

Example:

```
>swncconf --dtrans -v
Port number (HTTP server)       : 18444
Port number (JServlet)          : 19005
Port number (connector)         : 19009
...
(omitted)
...
```

5. Start the agent.

[Windows]

```
"%F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl" start
```

[Linux]

```
/opt/FJSVswnc/bin/swncctrl start
```

6. In the case of the Management Server, restart Systemwalker Runbook Automation.

[Windows]

```
<Systemwalker Runbook Automation  Management Server installation directory>\bin\swrba_start
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_start
```

Appendix A Installing Operation Management Products on the Systemwalker Runbook Automation Management Server

This appendix describes the installation procedure and notes to consider when the product below is installed on the Systemwalker Runbook Automation Management Server:

- Systemwalker Centric Manager

- Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager

- ServerView Resource Orchestrator Cloud Edition

A.1 Installing Systemwalker Centric Manager

The CORBA Service (ObjectDirector) bundled with the Systemwalker Runbook Automation Management Server is also included in Systemwalker Centric Manager (this document refers to Systemwalker/CentricMGR, Systemwalker CentricMGR and Systemwalker Centric Manager as "Systemwalker Centric Manager"). For this reason, care must be taken when installing both a Systemwalker Centric Manager Operation Management Server and a Systemwalker Runbook Automation Management Server on the same computer.

Refer to the Systemwalker Centric Manager manuals for details on the environment setup procedure, commands, and so on.

These notes apply to the Systemwalker Centric Manager Operation Management Server.

If Systemwalker Runbook Automation and Systemwalker Centric Manager are installed on the same system, they can only be used with the same operating system.

Note also that the following versions of Systemwalker Centric Manager cannot be installed on the same computer as a Systemwalker Runbook Automation Management Server:

- Windows version Systemwalker CentricMGR before V10.0L21

- Windows version Systemwalker/CentricMGR V5.0Lxx

System parameter[Linux]

- Do the tuning of system parameter when Systemwalker Centric Manager and Systemwalker Runbook Automation are installed in the same server. If the tuning is not done the installer will fail.

- Please refer to *"2.1.1 Tuning System Parameters [Linux] [Solaris]"* for the setting of system parameter of Systemwalker Runbook Automation. Please refer to *"Systemwalker Centric Manager User's Guide - Running Interstage, Symfoware and ObjectDirector"* for the setting of system parameter of Systemwalker Centric Manager.

A.1.1 When a Systemwalker Centric Manager Operation Management Server is installed on a computer where a Systemwalker Runbook Automation Management Server has already been installed

Follow the steps below to install a Systemwalker Centric Manager Operation Management Server:

1. Stop Systemwalker Runbook Automation and install Systemwalker Centric Manager

1. If the Systemwalker Runbook Automation Management Server, then stop it.

   Refer to "4.1.2 Stopping Systemwalker Runbook Automation" for details.

2. Enable auto-start of service.

   [**Windows**]

   Using Windows(R) service function, change **Startup type** of the following **manual** to **auto.**

   - Systemwalker MpAosfB

- Systemwalker MpAosfP

- Systemwalker MpAosfX

3. Stop Interstage.

Method 1: Via the Interstage Management Console.

Method 2: Via the command line:

[Windows]

```
C:\> isstop -f
```

[Linux]

```
# isstop -f
```

4. Install a Systemwalker Centric Manager Operation Management Server.

Refer to the *Systemwalker Centric Manager Installation Guide* for details.

5. Restart the computer.

6. Perform steps 1 and 2 again.

2. Create an environment and start Systemwalker Centric Manager

Create an environment for Systemwalker Centric Manager.

[Windows]

👉 Note

⋯⋯⋯

Environments in which a Systemwalker Runbook Automation Management Server has been installed already have an ObjectDirector environment, so there is no need to recreate it. Refer to the *Systemwalker Centric Manager User's Guide - Running Interstage, Symfoware and ObjectDirector* for details (provided from Systemwalker CentricMGR V10.0L20 and later).

⋯⋯⋯

1. Start the Operation Environment Maintenance Wizard.

2. Select "Create Operation Environment" to create a Systemwalker Centric Manager environment.
(Click **No** when prompted to confirm whether to rebuild the environment)

3. Start the Systemwalker Centric Manager service:

```
C:\><Systemwalker Centric Manager installation directory>\MPWALKER.DM\bin\scentricmgr
```

[Linux]

1. Set up Systemwalker Centric Manager:

/opt/systemwalker/bin/MpFwSetup -mix

- In the setup menu, enter "1" to create a Systemwalker Centric Manager environment.

- In the Connection environment check result window, enter "2" to continue processing without recreating the Systemwalker Centric Manager environment.

- In the setup menu, enter "3" to start each daemon for Systemwalker Centric Manager.

3. Start Interstage and Systemwalker Runbook Automation

1. Start Interstage.

Method 1: Via the Interstage Management Console.

Method 2: Via the command line:

[Windows]

```
C:\> isstop -f
```

[Linux]

```
# isstop -f
```

2. Start the Systemwalker Runbook Automation Management Server:

```
swrba_start
```

If a Management Server has been set up, then start it. Refer to "4.1.1 Starting Systemwalker Runbook Automation" for details.

A.1.2 When a Systemwalker Runbook Automation Management Server is installed on a computer where a Systemwalker Centric Manager Operation Management Server has already been installed

Follow the steps below to install a Systemwalker Runbook Automation Management Server.

1. Stop Systemwalker Centric Manager and delete its environment

[Windows]

1. Stop all Systemwalker Centric Manager functions:

```
C:\><Systemwalker Centric Manager installation directory>\MPWALKER.DM\bin\pcentricmgr
```

2. Start the Operation Environment Maintenance Wizard.

3. Select Backup Operation environment to back up the Systemwalker Centric Manager environment.

4. Select Delete Operation environment to delete the Systemwalker Centric Manager environment.

[Linux]

1. Stop all Systemwalker Centric Manager functions:

```
 # /opt/systemwalker/bin/pcentricmgr
```

2. Back up Systemwalker Centric Manager.

   Refer to the Systemwalker Centric Manager manuals for details.

3. Delete the Systemwalker Centric Manager environment:

```
 # /opt/systemwalker/bin/MpFwSetup
```

In the setup menu, enter "2".

2. Uninstall the packages

[Windows]

1. Uninstall the ObjectDirector that was installed alongside Systemwalker Centric Manager.

2. Open the **Services** dialog box from **Administrative Tools** under the **Control Panel** and stop the "OD_start" service.

3. Open the **Add or Remove Programs** dialog box from the **Control Panel**, and uninstall ObjectDirector Server.

4. Restart the computer.

5. Stop all Systemwalker Centric Manager functions:

```
C:\><Systemwalker Centric Manager installation directory>\MPWALKER.DM\bin\pcentricmgr
```

[Linux]

1. Stop ObjectDirector that was installed alongside Systemwalker Centric Manager:

```
# /opt/FJSVod/bin/OD_stop
```

2. Uninstall the FJSVod, FJSVsclr and FJSVsmee packages:

```
# rpm -e FJSVod FJSVsclr FJSVsmee
```

3. Install Systemwalker Runbook Automation and stop Interstage

1. Install a Systemwalker Runbook Automation Management Server.

2. Restart the computer.

3. Stop Interstage.

   Method 1: Via the Interstage Management Console.

   Method 2: Via the command line:

   [Windows]

```
C:\> isstop -f
```

   [Linux]

```
# isstop -f
```

4. Enable automatic startup for the service.

   [Windows]

   Using the Windows(R) Services function, change **Startup Type** for the following services from **Manual** to **Automatic**.

   - Systemwalker MpAosfP

   - Systemwalker MpAosfX

4. Restore the environment and start Systemwalker Centric Manager

Restore the environment and start Systemwalker Centric Manager

[Windows]

Note

. . . .

Environments in which a Systemwalker Runbook Automation Management Server has been installed already have an ObjectDirector environment, so there is no need to recreate it. Refer to the *Systemwalker Centric Manager User's Guide - Running Interstage, Symfoware and ObjectDirector* for details (provided from Systemwalker CentricMGR V10.0L20 and later).

. . . .

1. Start the Operation Environment Maintenance Wizard.

2. Restore the Systemwalker Centric Manager environment. Select **Restore operation environment**.
   (In the window that prompts for confirmation to rebuild the environment, click **No**.)

3. Start the Systemwalker Centric Manager service:

```
C:\><Systemwalker Centric Manager installation directory>\MPWALKER.DM\bin\scentricmgr
```

[Linux]

1. Create an environment for Systemwalker Centric Manager (for restoration):

```
# /opt/systemwalker/bin/MpFwSetup -mix
```

   - In the setup menu, enter "5" to display the maintenance menu.

- In the maintenance menu, enter "2" to create an environment.

- In the connection environment check result window, enter "2" to continue without recreating the environment.

2. Restore Systemwalker Centric Manager.

Refer to the Systemwalker Centric Manager manuals for details.

3. Start the Systemwalker Centric Manager service:

```
# /opt/systemwalker/bin/scentricmgr
```

5. Start Interstage and set up Systemwalker Runbook Automation

1. If using Windows Management server, start Interstage HTTP Service by ihsstart command. If using Linux Management server , you do not execute this procedure.

```
C:\> ihsstart -all
```

2. Start Interstage.

Method 1: Via the Interstage Management Console.

Method 2: Via the command line:

[Windows]

```
C:\> isstart
```

[Linux]

```
# isstart
```

3. Set up Systemwalker Runbook Automation.
Refer to "3.1 Setting up the Management Server" for details.

A.2 Installing Cloud Infrastructure Management Software/ Systemwalker Software Configuration Manager

Some of the Systemwalker Runbook Automation Management Server features are included in Cloud Infrastructure Management Software/ Systemwalker Software Configuration Manager, therefore care is required when the Systemwalker Runbook Automation Management Server is used in the same server as Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager.

This section explains the procedure and points to note when the following software and the Systemwalker Runbook Automation Management Server are used in the same server.

- Cloud Infrastructure Management Software V1.2.0

- Systemwalker Software Configuration Manager V14.1.0A

📌 Note

. . . .
- As a safeguard against errors occurring when the Systemwalker Runbook Automation Management Server is installed, Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager must always be backed up before this procedure is performed.

. . . .

Order of Installation

The procedure that is used to install the Systemwalker Runbook Automation Management Server in an environment in which Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager have already been installed is explained below.

Systemwalker Runbook Automation Management Server Installation Procedure

The procedure that is used to install the Systemwalker Runbook Automation Management Server is as follows:

![Note]

. . . .

- When the Systemwalker Runbook Automation Management Server installation procedure has started, do not operate any other products that are installed in the same environment until the installation is complete.

- An empty directory that can be written to as the working area will be required to install the Systemwalker Runbook Automation Management Server. Additionally, the working area data will be required to re-execute after an error has occurred in the installation. For this reason, do not delete the working area data until the Systemwalker Runbook Automation Management Server installation and behavior confirmation are complete.

- If the installation cannot be performed, for example because the working area has been corrupted, reinstall Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager then restore the product from the backup.
  Then, perform the Systemwalker Runbook Automation Management Server installation procedure.

- 600MB of free area is required for the Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager installation destination directory. If there is insufficient area for the installation destination directory, extend the installation destination directory area before installing Systemwalker Runbook Automation. Use the following procedure to extend the installation destination directory area:
  1) Back up the product
  2) Uninstall the product
  3) Extend the installation destination directory area
  4) Install the product
  5) Restore the product

. . . .

![See]

. . . .

- Refer to "*Backing up or Restoring the Admin Server*" in the "*Cloud Infrastructure Management Software User's Guide*" for information on how to back up and restore Cloud Infrastructure Management Software environment resources. Refer to "*Installation and*

Uninstallation" in the *"Cloud Infrastructure Management Software User's Guide"* for information on how to install and uninstall the product.

- Refer to "*Backing up the Admin Server"* and "*Restoring the Admin Server"* in the *"Systemwalker Software Configuration Manager Operation Guide*" for information on how to back up and restore Systemwalker Software Configuration Manager environment resources. Refer to *"Installation"* and *"Uninstallation"* in the *"Systemwalker Software Configuration Manager Operation Guide"* for information on how to install and uninstall the product.

A.2.1 Preparation

An empty directory that can be written to as the working area will be required to install the Systemwalker Runbook Automation Management Server. Create an empty directory using a maximum of 25 alphanumeric characters as the absolute path. A rough estimate of the size required for the working area is shown below.

```
Working area requirement=

Total capacity in the Process Management database storage directory

+ Total capacity in the Systemwalker Runbook Automation Management Server installation directory
(*2)

+ Total capacity in the Interstage Application Server installation directory (*2)

+ Total capacity in the Systemwalker Operation Manager installation directory (*2)

+ Total capacity under the directory specified in "Repository Database" of Interstage Directory Service
(*1)

+ 100MB
```

(*1) This is added when Interstage Directory Service is used for LDAP.

(*2) In Linux the total size of following directories is required.

/var/opt/FJSVJMCMN	/var/opt/FJSVJOBSC	/var/opt/FJSVMJS
/var/opt/FJSVcmdba	/var/opt/FJSVcmdbi	/var/opt/FJSVcmdbm
/var/opt/FJSVejb	/var/opt/FJSVena	/var/opt/FJSVes
/var/opt/FJSVextp	/var/opt/FJSVftlo	/var/opt/FJSVfwseo
/var/opt/FJSVfwtco	/var/opt/FJSVihs	/var/opt/FJSVirep
/var/opt/FJSVirepc	/var/opt/FJSVisas	/var/opt/FJSVisgui
/var/opt/FJSVisjmx	/var/opt/FJSVisscs	/var/opt/FJSVj2ee
/var/opt/FJSVjmcal	/var/opt/FJSVjms	/var/opt/FJSVjmweb
/var/opt/FJSVjs2su	/var/opt/FJSVjs5	/var/opt/FJSVlnkbs
/var/opt/FJSVod	/var/opt/FJSVots	/var/opt/FJSVporb
/var/opt/FJSVshnsk	/var/opt/FJSVshs	/var/opt/FJSVssoac
/var/opt/FJSVssoaz	/var/opt/FJSVssocm	/var/opt/FJSVssofs
/var/opt/FJSVssosv	/var/opt/FJSVstem	/var/opt/FJSVsvmon
/var/opt/FJSVswaic	/var/opt/FJSVswnc	/var/opt/FJSVswrbac
/var/opt/FJSVswrbam	/var/opt/FJSVtd	/etc/opt/FJSVMJS
/etc/opt/FJSVcmdba	/etc/opt/FJSVcmdbm	/etc/opt/FJSVejb
/etc/opt/FJSVes	/etc/opt/FJSVextp	/etc/opt/FJSVftlo
/etc/opt/FJSVihs	/etc/opt/FJSVirep	/etc/opt/FJSVisas
/etc/opt/FJSVisgui	/etc/opt/FJSVisjmx	/etc/opt/FJSVisscs
/etc/opt/FJSVj2ee	/etc/opt/FJSVjms	/etc/opt/FJSVjs2su

/etc/opt/FJSVjs5	/etc/opt/FJSVlnkbs	/etc/opt/FJSVod
/etc/opt/FJSVots	/etc/opt/FJSVporb	/etc/opt/FJSVsclr
/etc/opt/FJSVshnsk	/etc/opt/FJSVshs	/etc/opt/FJSVssoac
/etc/opt/FJSVssoaz	/etc/opt/FJSVssofs	/etc/opt/FJSVssosv
/etc/opt/FJSVsvmon	/etc/opt/FJSVswaic	/etc/opt/FJSVswnc
/etc/opt/FJSVswrbac	/etc/opt/FJSVswrbam	/etc/opt/FJSVtd

A.2.2 Registering Required Users in Systemwalker Runbook Automation

Register the user information that will be required for the Systemwalker Runbook Automation Management Server in the authentication infrastructure that is currently used.

Storage location of sample LDIF files

The LDIF files that are required to register the user information are stored as follows:

[Windows]

```
[DVD-ROM mount point]\tool\inst\ldif\swrba_sample_swrbasch.ldif
```

[Linux]

```
[DVD-ROM mount point]/tool/inst/ldif/swrba_sample_swrbasch.ldif
```

Definition content in the samples, and how to edit this content

This sample assumes the LDAP configuration shown below.

Edit the files according to the LDAP environment that will be used for operations. The password must also be changed.

Public directory	ou=interstage,o=fujitsu,dc=com
Organizational unit that stores the users	ou=User
Organizational unit that stores the groups	ou=Group
User for Schedule Startup	swrbasch
Password of User for Schedule Startup	systemwalker#2

How to define the samples

Use the ldapmodify command to register the LDIF file definition information in LDAP.

[Windows]

```
ldapmodify -H ldap://<Interstage Directory Service host name>:<port number> -D "<Administrator DN>" -w <Administrator DN password> -a -f <edited LDIF file name>
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://<Interstage Directory Service host name>:<port number> -D "<Administrator DN>" -w <Administrator DN password> -a -f <edited LDIF file name>
```

Example

. . . .

Interstage Directory Service host name: hostname

Port number: 389

Administrator DN: cn=manager,ou=interstage,o=fujitsu,dc=com

Administrator DN password: password

Edited LDIF file name: rbauser.ldif

[Windows]

```
ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f rbauser.ldif
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w password
-a -f rbauser.ldif
```

Refer to "*Interstage Directory Service Operation Command*" in the "*Interstage Application Server/Interstage Web Server Reference(Command)*" for information on the ldapmodify command.

A.2.3 Stopping Middleware Products

Before installing the Systemwalker Runbook Automation Management Server, stop the following products:

- Cloud Infrastructure Management Software V1.2.0

- Systemwalker Software Configuration Manager V14.1.0A

See

- Refer to "*Manager Control Commands*" in the "*Cloud Infrastructure Management Software User's Guide*" for information on how to stop Cloud Infrastructure Management Software.

- Refer to "*Starting and Stopping Systemwalker Software Configuration Manager*" in the "*Systemwalker Software Configuration Manager Operation Guide*" for information on how to stop Systemwalker Software Configuration Manager.

A.2.4 Upgrading Systemwalker Runbook Automation

Execute the upgrade as a user with administrator privileges. Mount disc No.1 of 2 from the Systemwalker Runbook Automation Media pack (V15.1.0) and start the installation.

Refer to "C.2.5 Upgrading Systemwalker Runbook Automation" for details.

Note

After the upgrade, the ServerView Resource Orchestrator and Systemwalker Runbook Automation environment settings are updated and the operating system will restart. For this reason, although reboot is mentioned in the upgrade procedure, there is no need for carry it out at this stage.

A.2.5 Changing the Cloud Infrastructure Management Software/ Systemwalker Software Configuration Manager Settings

Change the Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager settings.

After changing the settings, restart the operating system. Operations can be started once the restart of the operating system is complete.

Procedure for changing the settings

1. Log in as a user with administrator privileges, open the following file by text editor.

   [Windows]

   ```
   %SWCMDB_INSTALL_PATH%\FJSVcmdba\resources\MDBAD_SQC.xsl
   ```

[Linux]

```
/opt/FJSVcmdba/resources/MDBAD_SQC.xsl
```

2. Modify the following parts, and save the file.

   [Before]

   ```
   <xsl:param name="create_logical_server">false</xsl:param>
   ```

   [After]

   ```
   <xsl:param name="create_logical_server">true</xsl:param>
   ```

3. Log in as a user with administrator privileges, execute the following command from the command prompt.

   ```
   C:\> copy "%SWCMDB_INSTALL_PATH%\FJSVcmdbm\CMDBConsole\WEB-INF\resources
   \web.xml" "%SWCMDB_INSTALL_PATH%\FJSVcmdbm\CMDBConsole\WEB-INF\web.xml"
   ```

4. Execute the following command from the command prompt, and display the IIOP port number.

   [Windows]

   [Command that is executed]

   ```
   findstr "IBPMSRV_IIOP_PORT" [Systemwalker Runbook Automation Management Server
   installation directory]\etc\share\config\setup.ini
   ```

   [Command execution example (where 23700 is the IIOP port number)]

   ```
   c:\> findstr "IBPMSRV_IIOP_PORT" C:\Fujitsu\Systemwalker\SWRBAM\etc\share\config\setup.ini

   IBPMSRV_IIOP_PORT=23700
   ```

   [Linux]

   [Command that is executed]

   ```
   # grep "IBPMSRV_IIOP_PORT" /etc/opt/FJSVswrbam/share/config/setup.ini
   ```

   [Command execution example (where 23700 is the IIOP port number)]

   ```
   # grep "IBPMSRV_IIOP_PORT" /etc/opt/FJSVswrbam/share/config/setup.ini

   IBPMSRV_IIOP_PORT=23700
   ```

5. From the Web Console, connect to the Interstage Management Console.
   Log in as the operating system administrator.

   [Interstage Management Console URL]

   ```
   http://[Management Server host name]:[Interstage Management Console port number]/IsAdmin
   ```

   or,

   ```
   https://[Management Server host name]:[Interstage Management Console port number]/IsAdmin
   ```

6. From the Web Console, select **Interstage Management Console** >> **Interstage Application Server** >> **System** >> **WorkUnit** >>
   CTMG_MyPortal, then click the **Stop** button.

7. Once CTMG_Myportal has stopped completely, click the **Settings** tab to display **WorkUnit Settings**.

8. Add the following content as the fixed application library paths of **WorkUnit Settings**:

   [Windows]

```
[Interstage Application Server installation directory]\F3FMisjee\imq\lib\jms-ref-lib.jar

[Interstage Application Server installation directory]\F3FMisjee\lib\appserv-rt-client.jar

[Interstage Application Server installation directory]\F3FMisjee\lib\appserv-ext.jar

[Interstage Application Server installation directory]\F3FMisjee\lib\install\applications\jmsra
\imqjmsra.jar

[Interstage Application Server installation directory]\F3FMisjee\lib\appserv-admin.jar

[Interstage Application Server installation directory]\F3FMisjee\imq\lib\jms.jar
```

Note: The default Interstage Application Server installation directory is "C:\Fujitsu\Systemwalker\IAPS".

[Definition example (default installation destination)]

```
C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\imq\lib\jms-ref-lib.jar

C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\appserv-rt-client.jar

C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\appserv-ext.jar

C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\install\applications\jmsra\imqjmsra.jar

C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\appserv-admin.jar

C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\imq\lib\jms.jar
```

[Linux]

```
/opt/FJSVisjee/imq/lib/jms-ref-lib.jar

/opt/FJSVisjee/lib/appserv-rt-client.jar

/opt/FJSVisjee/lib/appserv-ext.jar

/opt/FJSVisjee/lib/install/applications/jmsra/imqjmsra.jar

/opt/FJSVisjee/lib/appserv-admin.jar

/opt/FJSVisjee/imq/lib/jms.jar
```

9. Add the following option as the JavaVM option of **WorkUnit Settings**.
   Leave a space after the existing option then specify **WorkUnit Settings**.

```
-Dcom.sun.appserv.iiop.endpoints=localhost:[IIOP port number]
```

[Definition example (IIOP port number is 23700)]

```
-Dcom.sun.appserv.iiop.endpoints=localhost:23700
```

10. Click the **Apply** button at the bottom of the window to save the WorkUnit settings.

11. From the Web Console, select **Interstage Management Console** >> Interstage Application Server >> **System** >> **WorkUnit** >> CFMG_API, then click the **Stop** button. Note that, if there are no CFMG_API WorkUnits, there is no need to do these steps from 11 to 14. Start with step 15.

12. Once CFMG_API has stopped completely, click the **Settings** tab to display **WorkUnit Settings**.

13. Add the following option as the JavaVM option of **WorkUnit Settings**.
    Leave a space after the existing option then specify **WorkUnit Settings**..

```
-Djavax.xml.transform.TransformerFactory=org.apache.xalan.xsltc.trax.TransformerFactoryImpl
```

14. Click the **Apply** button at the bottom of the window to save the WorkUnit settings.

15. Restart the operating system.

16. After restarting the operating system, log in as a user with administrator privileges, execute the following command.

```
"%SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\cmdbrefresh" -q type=AGT_SQC
```

A.3 Installing ServerView Resource Orchestrator Cloud Edition

Some of the Systemwalker Runbook Automation Management Server features are included in ServerView Resource Orchestrator Cloud Edition, therefore care is required when the Systemwalker Runbook Automation Management Server is used in the same server as ServerView Resource Orchestrator Cloud Edition.

This section explains the procedure and points to note when the following software and the Systemwalker Runbook Automation Management Server are used in the same server are explained.

- ServerView Resource Orchestrator Cloud Edition V3.0.0

- ServerView Resource Orchestrator Cloud Edition V3.1.0

Note

- As a safeguard against errors occurring when the Systemwalker Runbook Automation Management Server is installed, ServerView Resource Orchestrator must always be backed up before this procedure is performed.

Order of Installation

This section explains the procedure to install the Systemwalker Runbook Automation Management Server in an environment in which ServerView Resource Orchestrator has already been installed.

Systemwalker Runbook Automation Management Server Installation Procedure

The procedure that is used to install the Systemwalker Runbook Automation Management Server is as follows:

Note

- When the installation procedure has started, do not operate any other products that are installed in the same environment until the installation of the Systemwalker Runbook Automation Management Server is complete.

- An empty directory that can be written to as the working area will be required to install the Systemwalker Runbook Automation Management Server. Additionally, the working area data will be required to re-execute after an error has occurred in the installation.

For this reason, do not delete the working area data until the Systemwalker Runbook Automation Management Server installation and behavior confirmation are complete.

- If the installation cannot be performed, for example because the working area has been corrupted, reinstall ServerView Resource Orchestrator then restore the product from the backup.
  Then, perform the Systemwalker Runbook Automation Management Server installation procedure.

- 600MB of free area is required for the ServerView Resource Orchestrator installation destination directory. If there is insufficient area for the installation destination directory, extend it before installing Systemwalker Runbook Automation. Use the following procedure to extend the installation destination directory area:
  1) Back up the product
  2) Uninstall the product
  3) Extend the installation destination directory area
  4) Install the product
  5) Restore the product

See

- Refer to the "*ServerView Resource Orchestrator Operation Guide*" for information on how to back up and restore ServerView Resource Orchestrator environment resources. Refer to the "*ServerView Resource Orchestrator Installation Guide*" for information on how to install and uninstall the product.

A.3.1 Preparation

Follow the steps to install the Systemwalker Runbook Automation Management server. Please refer to *"A.3.1 Preparation"*.

A.3.2 Stopping ServerView Resource Orchestrator

Before installing the Systemwalker Runbook Automation Management Server, stop ServerView Resource Orchestrator.

See

- Refer to *"Starting and Stopping the Manager"* in the "*ServerView Resource Orchestrator Installation Guide"* for information on how to stop ServerView Resource Orchestrator.

A.3.3 Upgrading Systemwalker Runbook Automation

Execute the upgrade as a user with administrator privileges. Mount disc No.1 of 2 from the Systemwalker Runbook Automation Media pack (V15.1.0) and start the installation.

Refer to "C.2.5 Upgrading Systemwalker Runbook Automation" for details.

Note

After the upgrade, the ServerView Resource Orchestrator and Systemwalker Runbook Automation environment settings are updated and the operating system will restart. For this reason, although reboot is mentioned in the upgrade procedure, there is no need for carry it out at this stage.

A.3.4 Changing the ServerView Resource Orchestrator/Systemwalker Runbook Automation Settings

Change the ServerView Resource Orchestrator and Systemwalker Runbook Automation Management Server settings.

When the following software and the Systemwalker Runbook Automation Management Server are used in the same server, execute this procedure.

- ServerView Resource Orchestrator Cloud Edition V3.0.0

After changing the settings, restart the operating system. When the operating system has been restarted, the Systemwalker Runbook Automation Management Server and ServerView Resource Orchestrator can both be used.

Procedure that is used to change the Systemwalker Runbook Automation Management Server settings

1. From the Web Console, connect to the Interstage Java EE Management Console.
   Log in as the operating system administrator.

   [Interstage Management Console URL]

   ```
   http://[Management Server host name]:[Operation Management HTTP listener port number]/
   javaee_admin
   ```

   or,

   ```
   https://[Management Server host name]:[Operation Management HTTP listener port number]/
   javaee_admin
   ```

2. From the Web Console, select **Common Tasks** >> **Clusters** >> IJCLibpmcon", then display the **Web Server Connector** settings window.

3. "RCXCT-ext2" is displayed in the list of Web servers. Select the check box, then click the **Save** button in the top right of the window.

4. From the Web Console, select **Common Tasks** >> **Clusters** >> IJCLibpmsv", then display the **Web Server Connector** settings window.

5. "RCXCT-ext2" is displayed in the list of Web servers. Select the check box, then click the **Save** button in the top right of the window.

Procedure that is used to change the ServerView Resource Orchestrator settings

1. Log in as a user with administrator privileges, execute the following command from the command prompt, and display the IIOP port number.

   [Windows]

   [Command that is executed]

   ```
   findstr "IBPMSRV_IIOP_PORT" [Systemwalker Runbook Automation Management Server
   installation directory]\etc\share\config\setup.ini
   ```

   [Command execution example (where 23700 is the IIOP port number)]

   ```
   c:\> findstr "IBPMSRV_IIOP_PORT" C:\Fujitsu\Systemwalker\SWRBAM\etc\share\config\setup.ini
   IBPMSRV_IIOP_PORT=23700
   ```

   [Linux]

   [Command that is executed]

   ```
   # grep "IBPMSRV_IIOP_PORT" /etc/opt/FJSVswrbam/share/config/setup.ini
   ```

   [Command execution example (where 23700 is the IIOP port number)]

   ```
   # grep "IBPMSRV_IIOP_PORT" /etc/opt/FJSVswrbam/share/config/setup.ini
   IBPMSRV_IIOP_PORT=23700
   ```

2. From the Web Console, connect to the Interstage Management Console.
   Log in as the operating system administrator.

   [Interstage Management Console URL]

> http://[Management Server host name]:[Interstage Management Console port number]/IsAdmin

or,

> https://[Management Server host name]:[Interstage Management Console port number]/IsAdmin

3. From the Web Console, select **Interstage Management Console** >> Interstage Application Server >> **System** >> **WorkUnit** >> RCXCT_MyPortal", then click the **Stop** button.

4. Once RCXCT_MyPortal has stopped completely, click the **Settings** tab to display **WorkUnit Settings.**

5. Add the following content as the fixed application library paths of **WorkUnit Settings.**

   [Windows]

   > [Interstage Application Server installation directory]\F3FMisjee\imq\lib\jms-ref-lib.jar
   >
   > [Interstage Application Server installation directory]\F3FMisjee\lib\appserv-rt-client.jar
   >
   > [Interstage Application Server installation directory]\F3FMisjee\lib\appserv-ext.jar
   >
   > [Interstage Application Server installation directory]\F3FMisjee\lib\install\applications\jmsra\imqjmsra.jar
   >
   > [Interstage Application Server installation directory]\F3FMisjee\lib\appserv-admin.jar
   >
   > [Interstage Application Server installation directory]\F3FMisjee\imq\lib\jms.jar

   Note: The default Interstage Application Server installation directory is "C:\Fujitsu\Systemwalker\IAPS".

   [Definition example (default installation destination)]

   > C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\imq\lib\jms-ref-lib.jar
   >
   > C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\appserv-rt-client.jar
   >
   > C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\appserv-ext.jar
   >
   > C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\install\applications\jmsra\imqjmsra.jar
   >
   > C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\lib\appserv-admin.jar
   >
   > C:\Fujitsu\Systemwalker\IAPS\F3FMisjee\imq\lib\jms.jar

   [Linux]

   > /opt/FJSVisjee/imq/lib/jms-ref-lib.jar
   >
   > /opt/FJSVisjee/lib/appserv-rt-client.jar
   >
   > /opt/FJSVisjee/lib/appserv-ext.jar
   >
   > /opt/FJSVisjee/lib/install/applications/jmsra/imqjmsra.jar
   >
   > /opt/FJSVisjee/lib/appserv-admin.jar
   >
   > /opt/FJSVisjee/imq/lib/jms.jar

6. Add the following option as the JavaVM option of **WorkUnit Settings.**
   Leave a space after the existing option then specify **WorkUnit Settings.**

   > -Dcom.sun.appserv.iiop.endpoints=localhost:[IIOP port number]

   [Definition example (IIOP port number is 23700)]

   > -Dcom.sun.appserv.iiop.endpoints=localhost:23700

7. Click the **Apply** button at the bottom of the window to save the WorkUnit settings.

8. From the Web Console, select **Interstage Management Console** >> Interstage Application Server >> **System** >> **WorkUnit** >> RCXCF_API, then click the **Stop** button.

9. Once RCXCF_API has stopped completely, click the **Settings** tab to display **WorkUnit Settings.**

10. Add the following option as the JavaVM option of **WorkUnit Settings**.
    Leave a space after the existing option then specify **WorkUnit Settings.**.

    ```
    -Djavax.xml.transform.TransformerFactory=org.apache.xalan.xsltc.trax.TransformerFactoryImpl
    ```

11. Click the **Apply** button at the bottom of the window to save the WorkUnit settings.

12. Restart the operating system.

A.3.5 Notes on Operations

Points to note when ServerView Resource Orchestrator and the Systemwalker Runbook Automation Management Server are used in the same server are explained below.

Notes on Setting Up/Canceling the Setup of the Systemwalker Runbook Automation Management Server

When ServerView Resource Orchestrator and the Systemwalker Runbook Automation Management Server are used in the same server, use the setup/cancel the setup of ServerView Resource Orchestrator to set up/cancel the setup of the Systemwalker Runbook Automation Management Server respectively.

Use the setup/cancel the setup of ServerView Resource Orchestrator to set up/cancel the setup of the Systemwalker Runbook Automation Management Server respectively.

Notes on Setting Up ServerView Resource Orchestrator

To set up ServerView Resource Orchestrator again in a state where the Systemwalker Runbook Automation V15.1.0 Management Server has been installed, re-execute the procedure described in *"ServerView Resource Orchestrator/Systemwalker Runbook Automation Settings"*.

Port number that is used when ServerView Resource Orchestrator is being set up

The following fixed port numbers are used when ServerView Resource Orchestrator is set up again:

Port number for the message broker	7676
Port number for the server function	23700

If it is necessary to change the port number, for example because these port numbers are already being used, create the following files again before performing the ServerView Resource Orchestrator setup.

[Windows]

```
%SWRBA_HOME%\etc\config\setup\silent_setup.ini
```

[Linux]

```
/opt/FJSVswrbam/etc/config/setup/silent_setup.ini
```

File Format

```
[SETUP]

MESSAGE_BROKER_PORT=7676

SERVER_PORT=23700
```

Explanation of the SETUP section

Item name	Key name
Port number for the message broker	MESSAGE_BROKER_PORT

Item name	Key name
Port number for the server function	SERVER_PORT

Appendix B Creating Test Site Certificates

The test site certificate can only be used for testing before the site certificate issued by the CA is used. Examples of how to create the test site certificate are shown below:

Note

. . . .

The test site certificate can only be used in a test environment.
Do not use the test site certificate in actual operations.

. . . .

The command execution examples shown below use the following values:

```
- Test site certificate nickname: testCert
- First and last name: ssoserver.example.com
- Name of organizational unit: FUJITSU TOKYO
- Name of organization: FUJITSU
- Name of City or Locality: Shinjuku
- Name of State or Province: Tokyo
- Two-letter country code for this unit:jp
```

The password that was entered will not be displayed. The password will be registered the first time it is entered. To create the certificate using the information displayed for the confirmation of the password that was entered, enter "yes". To enter a different password, enter "no".
[Windows]

```
scsmakeenv -n testCert
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]: ssoserver.example.com
What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
  [Unknown]: FUJITSU
What is the name of your City or Locality?
  [Unknown]: Shinjuku
What is the name of your State or Province?
  [Unknown]: Tokyo
What is the two-letter country code for this unit?
  [Un]: jp

Is <CN=ssoserver.fujitsu.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
  [no]: yes
SCS: INFO: scs0102: Self-sign certificate was issued
```

[Linux]

The Bourn shell has been used in the execution example.

```
# JAVA_HOME=/opt/FJSVawjbk/jdk5;export JAVA_HOME
# scsmakeenv -n testCert
New Password:
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]: ssoserver.example.com
What is the name of your organizational unit?
  [Unknown]: FUJITSU TOKYO
What is the name of your organization?
```

```
   [Unknown]: FUJITSU
What is the name of your City or Locality?
   [Unknown]: Shinjuku
What is the name of your State or Province?
   [Unknown]: Tokyo
What is the two-letter country code for this unit?
   [Un]: jp


Is <CN=ssoserver.example.com, OU=FUJITSU TOKYO, O=FUJITSU, L=Shinjuku, ST=Tokyo,C=jp> correct?
   [no]: yes
UX:SCS: INFO: scs0102: Self-sign certificate was issued
#
```

🔶 Note

You will be prompted to input password for Interstage certificate environment if Interstage certificate environment is already configured.
In this case, input the password that was set when you configured Interstage certificate environment.

Appendix C Upgrading from a Previous Version/Level

This appendix describes the procedure for upgrading Systemwalker Runbook Automation in environments running Systemwalker Runbook Automation Management Server to V15.1.0.

Upgrade from the following versions/levels is supported:

- Systemwalker Runbook Automation V14g V14.1.0 Management Server

- Systemwalker Runbook Automation V14g V14.1.0A Management Server

- Systemwalker Runbook Automation V15.0.0 Management Server

Note

- Back up Systemwalker Runbook Automation before upgrading, in case an error occurs (refer to *Systemwalker Runbook Automation V14g Installation Guide* or the *Systemwalker Runbook Automation Installation Guide* for details).

- There is no need to upgrade the Business Server and Linkage/Relay Servers, therefore no upgrade installation procedure has been provided. If a previous version/level of the Business Server or Linkage/Relay Servers was uninstalled as part of a software switch, install a new version/level of the Business Server or Linkage/Relay Server.

- If the Management Server is running in a cluster environment, perform a clean Systemwalker Runbook Automation V15.1.0 installation and setup for the new cluster environment, and not the upgrade shown in this appendix.

C.1 Upgrade Flow

The figure below illustrates the procedure used to upgrade the Systemwalker Runbook Automation Management Server:

 Note

    - Once the upgrade has started, do not operate any other product installed in the same environment until Systemwalker Runbook Automation V15.1.0 installation is complete.

    - To perform the upgrade, an empty directory with write privileges will be required, to be used as the working area. In case of error, date written to this directory will be required, therefore do not delete it until the Systemwalker Runbook Automation V15.1.0 installation and behavior confirmation are complete.

    - If the upgrade cannot be performed (for example, because the working area has been corrupted), reinstall the product of the previous version/level, then restore the product from the backup, and then upgrade.

    - The Management Server installation directory must have at least 600MB free. If that is not the case, then extend it:
      1) Back up the product.
      2) Uninstall the product.
      3) Extend the installation directory area.
      4) Install the product.
      5) Restore the product.

C.2 Details of the Upgrade Procedure

C.2.1 Preparation

An empty directory with write privileges is required to upgrade, to be used as the working area (the absolutepath can have up 25 alphanumeric characters). A rough estimate of the required size is displayed below:

Working area requirement =

Total capacity in the Process Management database directory +

Total capacity in the Systemwalker Runbook Automation Management Server directory +(*2)

Total capacity in the Interstage Application Server directory +(*2)

Total capacity in the Systemwalker Operation Manager directory +(*2)

Total capacity under the directory specified in "Repository Database" of Interstage Directory Service (*1) +

100MB

(*1) This is added when Interstage Directory Service is used for LDAP.

(*2) In Linux the total size of following directories is required.

/var/opt/FJSVJMCMN	/var/opt/FJSVJOBSC	/var/opt/FJSVMJS
/var/opt/FJSVcmdba	/var/opt/FJSVcmdbi	/var/opt/FJSVcmdbm
/var/opt/FJSVejb	/var/opt/FJSVena	/var/opt/FJSVes
/var/opt/FJSVextp	/var/opt/FJSVftlo	/var/opt/FJSVfwseo
/var/opt/FJSVfwtco	/var/opt/FJSVihs	/var/opt/FJSVirep
/var/opt/FJSVirepc	/var/opt/FJSVisas	/var/opt/FJSVisgui
/var/opt/FJSVisjmx	/var/opt/FJSVisscs	/var/opt/FJSVj2ee
/var/opt/FJSVjmcal	/var/opt/FJSVjms	/var/opt/FJSVjmweb
/var/opt/FJSVjs2su	/var/opt/FJSVjs5	/var/opt/FJSVlnkbs
/var/opt/FJSVod	/var/opt/FJSVots	/var/opt/FJSVporb
/var/opt/FJSVshnsk	/var/opt/FJSVshs	/var/opt/FJSVssoac
/var/opt/FJSVssoaz	/var/opt/FJSVssocm	/var/opt/FJSVssofs

/var/opt/FJSVssosv	/var/opt/FJSVstem	/var/opt/FJSVsvmon
/var/opt/FJSVswaic	/var/opt/FJSVswnc	/var/opt/FJSVswrbac
/var/opt/FJSVswrbam	/var/opt/FJSVtd	/etc/opt/FJSVMJS
/etc/opt/FJSVcmdba	/etc/opt/FJSVcmdbm	/etc/opt/FJSVejb
/etc/opt/FJSVes	/etc/opt/FJSVextp	/etc/opt/FJSVftlo
/etc/opt/FJSVihs	/etc/opt/FJSVirep	/etc/opt/FJSVisas
/etc/opt/FJSVisgui	/etc/opt/FJSVisjmx	/etc/opt/FJSVisscs
/etc/opt/FJSVj2ee	/etc/opt/FJSVjms	/etc/opt/FJSVjs2su
/etc/opt/FJSVjs5	/etc/opt/FJSVlnkbs	/etc/opt/FJSVod
/etc/opt/FJSVots	/etc/opt/FJSVporb	/etc/opt/FJSVsclr
/etc/opt/FJSVshnsk	/etc/opt/FJSVshs	/etc/opt/FJSVssoac
/etc/opt/FJSVssoaz	/etc/opt/FJSVssofs	/etc/opt/FJSVssosv
/etc/opt/FJSVsvmon	/etc/opt/FJSVswaic	/etc/opt/FJSVswnc
/etc/opt/FJSVswrbac	/etc/opt/FJSVswrbam	/etc/opt/FJSVtd

C.2.2 Registering Users in LDAP

To upgrade from the following versions or levels, register the user information that will be required for Systemwalker Runbook Automation V15.1.0 in the authentication infrastructure currently used.

🏫 Note
. . . .

- Only follow this procedure when upgrading from the following version/level:

    - Systemwalker Runbook Automation V14g V14.1.0

- This procedure assumes that the user information required by Systemwalker Runbook Automation V15.1.0 is registered in the authentication infrastructure currently used.

- Refer to the *Systemwalker Runbook Automation Installation Guide* for information on how to register users.
. . . .

- When Interstage Directory Service is used (when the sample LDIF files are used)

- When Interstage Directory Service is used (when new LDIF files are created and then registered)

- When ActiveDirectory is used

- When OpenLDAP is used

[When Interstage Directory Service is used (when the sample LDIF files are used)]

Location of sample LDIF files

[Windows]

```
ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f rbauser.ldif
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w
password -a -f rbauser.ldif
```

Content in the samples, and how to edit this content

This sample assumes the LDAP configuration shown below.

Edit the files according to the LDAP environment that will be used for operations. The password must also be changed.

Public directory	ou=interstage,o=fujitsu,dc=com
Organizational unit that stores the users	ou=User
Organizational unit that stores the groups	ou=Group
User for Schedule Startup	swrbasch
Password of User for Schedule Startup	systemwalker#2

Refer to " [When Interstage Directory Service is used (when new LDIF files are created)]" for information on the content defined in the LDIF files.

How to define the samples

Register the LDIF file definition information in LDAP using the ldapmodify command (refer to "*Interstage Directory Service Operation Command*" in the "*Interstage Application Server/Interstage Web Server Reference Manual (Command)"* for details):

[Windows]

```
ldapmodify -H ldap://<Interstage Directory Service host name>:<port> -D "<Administrator DN>" -w
<password> -a -f <edited LDIF file>
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://<Interstage Directory Service host name>:<port> -D "<Administrator
DN>" -w <password> -a -f <edited LDIF file>
```

📖 Information
. . . .

Interstage Directory Service host name: hostname

Port number: 389

Administrator DN: cn=manager,ou=interstage,o=fujitsu,dc=com

Administrator DN password: password

Edited LDIF file name: rbauser.ldif

[Windows]

```
ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f
swrba_swrbasch.ldif
```

[Linux]

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w
password -a -f swrba_swrbasch.ldif
```
. . . .

For the detail of ldapmodify command, refer to "Interstage directory service operation command" in the *Interstage Application Server/Interstage Web Server Reference Guide (Command).*

[When Interstage Directory Service is used (when new LDIF files are created)]

This section explains example of replacement string for actual case with using below.

Replacement string	Settings value after replacement
%DOMAIN%	Public directory (Example) ou=interstage,o=fujitsu,dc=com
%USER%	Organizational Unit (OU) "User" (if this name was changed, this will be the Organizational Unit (OU) of the name that was changed)

Replacement string	Settings value after replacement
	(Example) User
%GROUP%	Organizational Unit (OU) "Group" (if this name was changed, this will be the Organizational Unit (OU) of the name that was changed)
	(Example) Group

Registering the User for Schedule Startup

Register the user required by Systemwalker Runbook Automation to start the Automated Operation Process according to a schedule. The following user name and password are used in the example below. The following user name is the suggested value, however this can be changed to any name. Note that the value set here is specified in the parameter input file when the installation preparation command is executed.

User name	Password
swrbasch	systemwalker#2

Following the settings example shown below, create the LDIF file for registering the user, then register the user in LDAP using the ldapmodify command (refer to "Interstage Directory Service Operation Command" in the "*Interstage Application Server/ Interstage Web Server Reference(Command)*" for details).

Settings example

```
dn: uid=swrbasch,ou=%USER%,%DOMAIN%

changetype: add

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

objectClass: top

objectClass: ssoUser

cn: swrbasch

sn: swrbasch

givenName: swrbasch

userPassword: systemwalker#2

uid: swrbasch

dn: cn=AdminRole,ou=%GROUP%,%DOMAIN%

changetype: modify

member: uid=swrbasch,ou=%USER%,%DOMAIN%

dn: cn=IflowUsers,ou=%GROUP%,%DOMAIN%

changetype: modify

member: uid=swrbasch,ou=%USER%,%DOMAIN%
```

[When Active Directory is used]

Register the user shown below in Active Directory.

Last name	First name	Initial	User logon name	Password	Will there be a check mark in the enter password window? (*1)	User's group	Description
swrbasch (Note 2)	Blank	Blank	swrbasch (Note 2)	systemwalker#2 (Note 3)	A: User must change password at next logon B: User cannot change password C: Password never expires A: Account is disabled	AdminRole IflowUsers	User for Schedule Startup

*1A: The check mark has been removed **B**: There may be a check mark **C**: There is a check mark

*2 Recommended value, can be changed to any value.

*3Initial value, can be changed to any value.

To register the user, follow the steps below:

1. From the start menu, click **Control Panel** >> **Administrative Tools** >> **Active Directory Users and Computers**.

2. Right-click the name in Organizational Unit (OU) "User" (if the name was changed in "Creating an organizational unit (OU)", this will be the Organizational Unit (OU) of the name that was changed), then select **New** >> **User**.

3. The **New Object - User** window will be displayed.
   As shown in the above table, enter **Last name**, **First name**, **Initials**, and **User logon name**, then click **Next**.

4. The password window will be displayed.
   As shown in the above table, set the password and check boxes, then click **Next**.

5. The confirmation window will be displayed.
   If the content is correct, click **OK**.

6. Right-click the user registered to open the properties window.

7. Select the **Member Of** tab, then click **Add**.

8. In the **Enter the object names to select** text box, enter the name of the owner group shown in the above table, then click **OK**.

9. Click the **OK** button of the properties window.

[When OpenLDAP is used]

This section explains example of replacement string for actual case with using below.

Replacement target string	Settings value after replacement
%DOMAIN%	Public directory (Example) ou=interstage,o=fujitsu,dc=com
%USER%	Organizational Unit (OU) "User" (if this name was changed, this will be the Organizational Unit (OU) of the name that was changed) (Example) User
%GROUP%	Organizational Unit (OU) "Group" (if this name was changed, this will be the Organizational Unit (OU) of the name that was changed) (Example) Group

Registering the User for Schedule Startup

Register the user required by Systemwalker Runbook Automation to start the Automated Operation Process according to a schedule. The following user name and password are used in the example below. The following user name is the suggested value, however this can be changed to any name. Note that the value set here is specified in the parameter input file when the installation preparation command is executed.

User name	Password
swrbasch	systemwalker#2

Following the settings example shown below, create the LDIF file for registering the user, then use the ldapadd command to register the user in LDAP.

Settings example

```
dn: uid=swrbasch,ou=%USER%,%DOMAIN%
changetype: add
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: swrbasch
sn: swrbasch
givenName: swrbasch
userPassword: systemwalker#2
uid: swrbasch

dn: cn=AdminRole,ou=%GROUP%,%DOMAIN%

changetype: modify

member: uid=swrbasch,ou=%USER%,%DOMAIN%

dn: cn=IflowUsers,ou=%GROUP%,%DOMAIN%

changetype: modify

member: uid=swrbasch,ou=%USER%,%DOMAIN%
```

C.2.3 Preparation when Systemwalker Centric Manager Operation Management Server has been installed

If the Systemwalker Centric Manager Operation Management Server has already been installed, use the following procedure.

[Windows]

1. Stop all Systemwalker Centric Manager features:

```
C:\> [Systemwalker Centric Manager installation path]\MPWALKER.DM\bin\pcentricmgr
```

2. Start the **Operation Environment Maintenance Wizard**.

3. Select **Backing up the operation environment** to back up the Systemwalker Centric Manager environment.

4. Select **Deleting the operation environment** to delete the Systemwalker Centric Manager environment.

[Linux]

1. Stop all Systemwalker Centric Manager features:

```
# /opt/systemwalker/bin/pcentricmgr
```

2. Back up Systemwalker Centric Manager.

   Refer to the Systemwalker Centric Manager manuals for details.

3. Stop all Systemwalker Centric Manager features:

```
# /opt/systemwalker/bin/pcentricmgr
```

4. Delete the Systemwalker Centric Manager environment.

```
# /opt/systemwalker/bin/MpFwSetup
```

In the setup menu (initial menu), enter "2" to delete the Systemwalker Centric Manager environment.

C.2.4 Stopping the Systemwalker Runbook Automation Management Server

Use the following procedure to stop Systemwalker Runbook Automation.

1. Login to the Management Server as a user with administrator privileges.

2. Stop Systemwalker Runbook Automation:

   [Windows]

   ```
   [Systemwalker Runbook Automation Management Server directory]\bin\swrba_stop
   ```

   [Linux]

   ```
   # /opt/FJSVswrbam/bin/swrba_stop
   ```

Note

If the operating system used is Windows Server 2008, execute the above command as an Administrator.

See

Refer to "4.1.2 Stopping Systemwalker Runbook Automation" for details.

C.2.5 Upgrading Systemwalker Runbook Automation

Perform upgrade of Systemwalker Runbook Automation.

Systemwalker Runbook Automation upgrades must be executed by a user with administrator privileges.

Point

Follow the steps described in this section, even if the Systemwalker Runbook Automation Management Server is to be installed in environments in which the following software is already installed.

- Cloud Infrastructure Management Software V1.2.0

- Systemwalker Software Configuration Manager V14.1.0A

- ServerView Resource Orchestrator Cloud Edition V3.0.0

- ServerView Resource Orchestrator Cloud Edition V3.1.0

Note that if any of the software above is already installed, the environment settings will have to be changed after installation, without restarting the operating system (refer to "Changing the Cloud Infrastructure Management Software/Systemwalker Software Configuration Manager Settings" and "Changing the ServerView Resource Orchestrator/Systemwalker Runbook Automation Settings" for details).

C.2.5.1 Upgrading in Windows

This section describes how to upgrade Systemwalker Runbook Automation installed on a Windows Management Server.

Note

- If a terminal server is installed, change the terminal service to install mode:

```
CHANGE USER /INSTALL
```

- A random password will be generated for OS user "swrbajobuser" used by Systemwalker Runbook Automation - change it after the upgrade if required (refer to "Changing Operating System User Passwords Used by Systemwalker Runbook Automation").

- When Systemwalker Runbook Automation will be installed in the environment that following software have benn installed, Stop these software in advance.

    - Cloud Infrastructure Management Software

    - Systemwalker Software Configuration Manager

    - ServerView Resource Orchestrator Cloud Edition

    - Systemwalker Service Quality Coordinator

    - Systemwalker Service Catalog Manager

  For how to stop, refer to the following.

    - For stopping Cloud Infrastructure Management Software, refer to "Manager control command" in the *Cloud Infrastructure Management Software User's Guide*.

    - For stopping Systemwalker Software Configuration Manager, refer to "Stop/Start Systemwalker Software Configuration Manager" in the *Systemwalker Software Configuration Manager Operation Guide*.

    - For stopping ServerView Resource Orchestrator, refer to "Start and stop Manager" in the *ServerView Resource Orchestrator Installation Guide*.

    - For stopping Systemwalker Service Quality Coordinator, refer to "Stop and Start resident process" in the *Systemwalker Service Quality Coordinator Installation Guide*.

- Before executing to upgrade, confirm whether event viewer has been displayed. If it is displayed, close it before upgrading.

· ·

1. Login using an account belonging to the Administrators group.

2. Start the installer.

   Place the DVD-ROM below in the DVD-ROM device - installation will start automatically (if it does not, execute swsetup.exe):

     - Systemwalker Runbook Automation Media Pack (15.1.0) Disc No. 1/2

Note

· ·

If the system runs Windows Server 2008, execute as administrator.

· ·

In the displayed window, select **Install Management Server.**
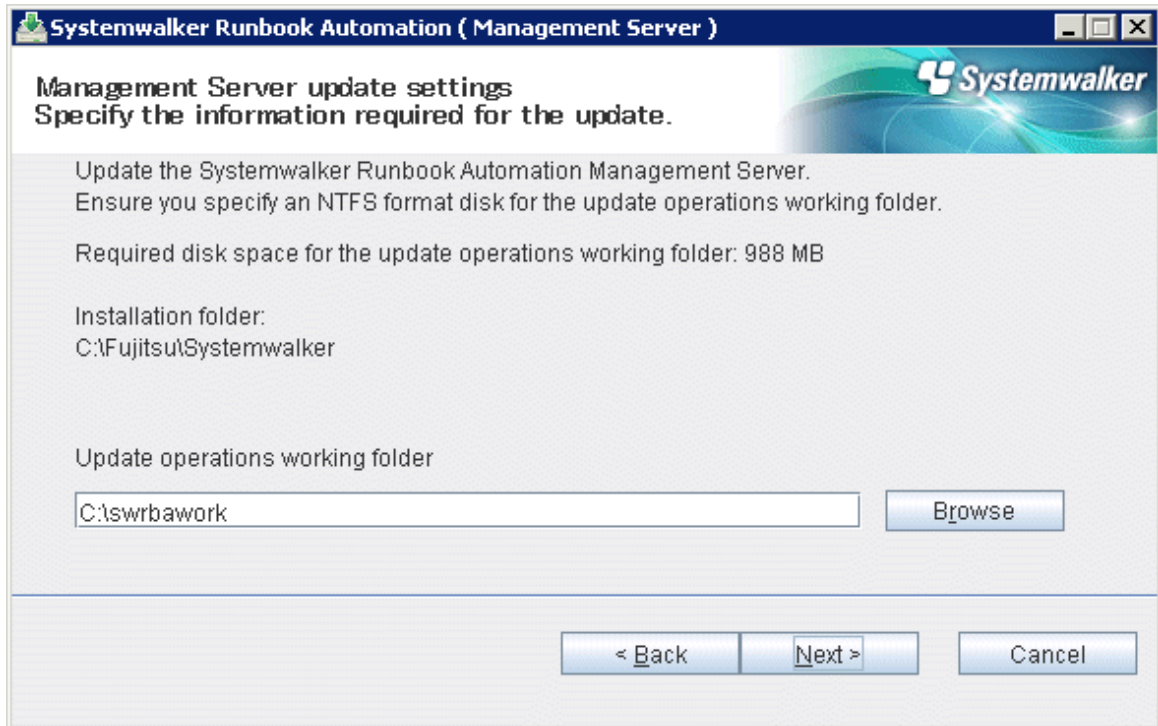

3. The **Welcome** dialog box will be displayed.

   Make sure that the contents are correct, then click the **Next** button.

4. Specify the operation folder required for Systemwalker Runbook Automation update tasks.

   Specify a directory that has enough disk space for the update operations.

![Note]

- The update operation folder name can be up to 25 characters long.

- Specify an NTFS disk for the update operation folder.

- A relative path or a path beginning with "\\" cannot be specified.

- Only half-width alphanumeric characters can be specified for the directory name.

- Files and directories may exist in the work area when restarting after an error, but specify the same directory without deleting them. Refer to "If an error occurs" for details.

5. If you use Interstage Single Sign-On as authentication mechanism, or any of these are already installed, this windows is displayed.

   - Cloud Infrastructure Management Software V1.2.0

   - Systemwalker Software Configuration Manager V14.1.0A

Specify the SSO repository used by Interstage Single Sign-On that is built into the current environment.

![P] **Point**

. . . .

Check the SSO repository information using the Interstage Management Console by clicking **System** > **Security** > **Single Sign-on** > **Authentication Infrastructure** > **Repository Server** > **Settings**.

Alternatively, click **System** > **Security** > **Single Sign-on** > **Authentication Infrastructure** > **Repository Server** > **Protected resource**, and confirm the FQDN.

. . . .

6. The window below will be displayed if upgrading from one of these versions:

   - Systemwalker Runbook Automation V14g.V14.1.0 Management Server

   - Systemwalker Runbook Automation V14g.V14.1.0A Management Server

   The window might also be displayed if any of these are already installed:

   - Cloud Infrastructure Management Software V1.2.0

   - Systemwalker Software Configuration Manager V14.1.0A

   - ServerView Resource Orchestrator Cloud Edition V3.0.0

Specify the port number used by Systemwalker Runbook Automation.

> **Note**
> ....
> - Do not specify the port number currently operating - use the command below to check:
>
> | > netstat -a -n |
> |---|
>
> - The specified port number may be in use elsewhere even if it is not currently operating (refer to "9.1 Port Numbers" for details).
> ....

7. The window below will be displayed if upgrading from this version:

   - Systemwalker Runbook Automation V14g.V14.1.0 Management Server

   The window might also be displayed if any of these are already installed:

   - Cloud Infrastructure Management Software V1.2.0

   - Systemwalker Software Configuration Manager V14.1.0A

Specify the subsystem number, port number, or user used by the Scheduling.

![Note icon] **Note**

....

- Specify the port number if the default port number used by the schedule function is in use elsewhere.

- Do not specify the port number currently operating - use the command below to check:

  ```
  > netstat -a -n
  ```

- The specified port number may be in use elsewhere even if it is not currently operating (refer to "9.1 Port Numbers" for details).

....

8. The window below will be displayed if upgrading from this version and executing Management Server setup:

   - Systemwalker Runbook Automation V14g.V14.1.0 Management Server

   - Systemwalker Runbook Automation V14g.V14.1.0A Management Server

   The window might also be displayed if any of these are already installed:

   - Cloud Infrastructure Management Software V1.2.0 (Note)

   - Systemwalker Software Configuration Manager V14.1.0A (Note)

   - ServerView Resource Orchestrator Cloud Edition V3.0.0

   Note: The applications process is used

Specify the port number used by Systemwalker Runbook Automation.

🈁 **Note**

. . . .

- Do not specify the port number currently operating - use the command below to check:

```
> netstat -a -n
```

- The specified port number may be in use elsewhere even if it is not currently operating (refer to "9.1 Port Numbers" for details).

. . . .

9. Confirm installation.

In the **Confirm Installation** window, make sure that the contents are correct, then click the **Confirm** button - installation will start (note that this window is only displayed when the parameter has actually been specified).

10. After installation is completed, the window below will be displayed.

Click the **Finish** button.

11. Reboot the machine.

    Click the **Yes** button

    ```
    Confirmation                                              ⊠
       (?)   The system must be restarted to complete the installation. Restart the system now?

                        [ Yes ]    [ No ]
    ```

If an error occurs

- Act according to the displayed message, then restart the installer and execute the upgrade. Do not delete files and directories in the work area.

C.2.5.2 Upgrading in Linux

This section describes how to upgrade Systemwalker Runbook Automation installed on a Linux Management Server.

> 📄 **Note**
> ....
>
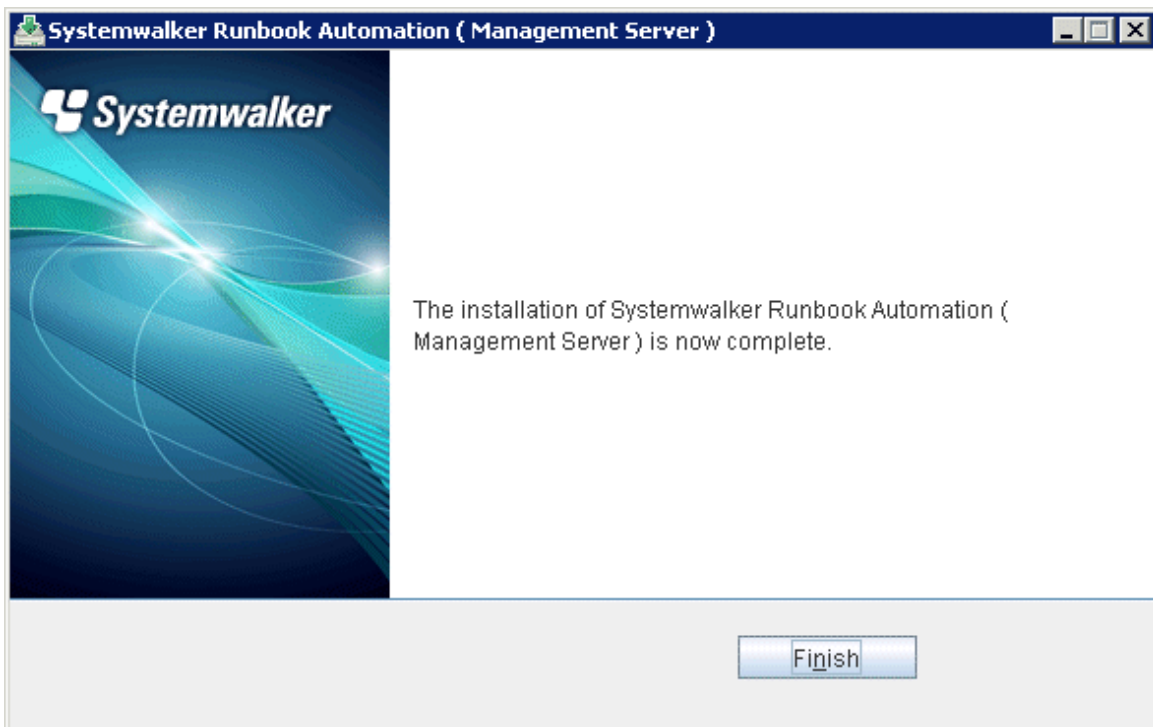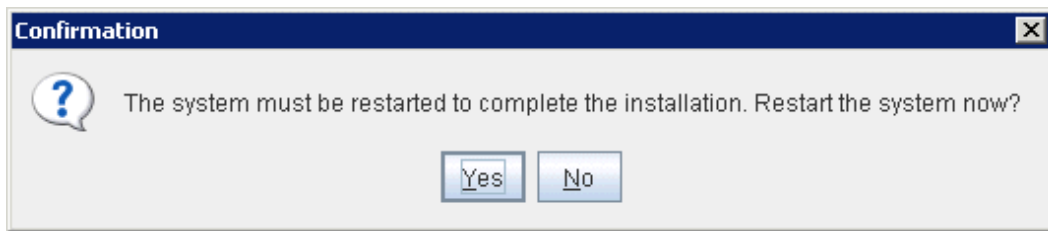> - If the operating system that supports the installation media (DVD-ROM) and the operating system for the installation destination are different, "Management Server" is not displayed in the select server window of the installation destination. Use an installation media type that is supported on the operating system used to install Systemwalker Runbook Automation.
>
> ....

1. Log in to the system as superuser.

2. Place the DVD-ROM media in the DVD-ROM device.

   Place the "Systemwalker Runbook Automation Media pack (15.1.0) Disc No. 1/2".

3. Mount the DVD-ROM.

   Use the command below.

   If the DVD-ROM is mounted automatically using the automatic mount daemon (autofs), because "noexec" is set in the mount options, attempts to start the installer will fail.

   ```
   # mount -t iso9660 -r /dev/mnt <DVD-ROM mount point>
   ```

4. Start the installer.

   Execute the install command (provided with this software) to install multiple packages at once.

   ```
   # <DVD-ROM mount point>/swsetup
   ```

5. The **Welcome** window will be displayed - press **Enter** key.

   ```
   ================================================================================
                       Systemwalker Runbook Automation Setup
                                      V15.1.0
              All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
   ================================================================================


   Welcome to Systemwalker Setup!
   Setup will install Systemwalker Runbook Automation.


   Press ENTER.
   ```

6. The server selection window for the installation folder will be displayed - type "**1**" to select **Management Server**.

```
================================================================================
                    Systemwalker Runbook Automation Setup
                                     V15.1.0
          All Rights Reserved, Copyright(c) FUJITSU LIMITED 2010-2012
================================================================================
<<Select the installation folder>>


1. Management Server


================================================================================
Select one of the items above.
[q,number]
=>1
```

7. Type "y" to start the Management Server installer.

```
Preparing to install.
Please wait.
Systemwalker Runbook Automation (Management Server)
Do you want to start installation?
[y,n]
=> y
```

8. Specify the directory required for Systemwalker Runbook Automation update tasks.
    Specify a directory with more disk space than the update operations working folder.

```
===<Information required for update tasks>===
Updating installed Systemwalker Runbook Automation.
Specify a directory that has more disk space than the update operations working folder.
Disk space required for the update operations: 1024MB
[ENTER:/var/tmp/swrbawork]
=>
```

![Note icon] **Note**
. . . .

-   The update task directory name can be up to 25 characters long.

-   A relative path cannot be specified.

-   Only half-width alphanumeric characters can be specified for the directory name.

-   Files and directories may exist in the work area when restarting after an error, but specify the same directory without deleting them. Refer to "Strategies for abnormal operations" for details.
. . . .

9. If you use Interstage Single Sign-On as authentication mechanism, or any of these are already installed, this message is displayed.

-   Cloud Infrastructure Management Software V1.2.0

-   Systemwalker Software Configuration Manager V14.1.0A

Specify the environment information of the SSO repository used by Interstage Single Sign-On that is built into the current environment.

```
=== Interstage Single Sign-On settings  ===
Input SSO repository FQDN
=> ssoserver.example.com

=== Interstage Single Sign-On settings  ===
Input SSO repository repository name
[ENTER:rep001]
=>
```

```
=== Interstage Single Sign-On settings  ===
Input SSO repository port number
[ENTER:389]
=>


=== Interstage Single Sign-On settings  ===
Input SSO repository administrator DN
[ENTER:cn=manager,ou=interstage,o=fujitsu,dc=com]
=>


=== Interstage Single Sign-On settings  ===
Input SSO repository administrator DN password
=>
```

Point

• •

Check the SSO repository information using the Interstage Management Console from the repository server advanced settings by clicking **System** > **Security** > **Single Sign-on** > **Authentication Infrastructure** > **Repository Server** > **Settings**.

Alternatively, click **System** > **Security** > **Single Sign-on** > **Authentication Infrastructure** > **Repository Server** > **Protected resource**, and confirm the FQDN.

• •

10. The prompts below will be displayed if upgrading from this version:

   - Systemwalker Runbook Automation V14g.V14.1.0 Management Server

   The prompts might also be displayed if any of these are already installed:

   - Cloud Infrastructure Management Software V1.2.0

   - Systemwalker Software Configuration Manager V14.1.0A

   - ServerView Resource Orchestrator Cloud Edition V3.0.0

   Specify the port number used by Systemwalker Runbook Automation.

```
=== <Systemwalker Runbook Automation port> ===
Enter the HTTP listener port number.
[ENTER:28080]
=>


=== <Systemwalker Runbook Automation port> ===
Enter the operation management HTTP listener port number.
[ENTER:12001]
=>


=== <Systemwalker Runbook Automation port> ===
Enter the IIOP port number.
[ENTER:23600]
=>


=== <Systemwalker Runbook Automation port> ===
Enter the IIOP_SSL port number.
[ENTER:23601]
=>


=== <Systemwalker Runbook Automation port> ===
Enter the IIOP_MUTUALAUTH port number.
[ENTER:23602]
=>


=== <Systemwalker Runbook Automation port> ===
Enter the JMX_ADMIN port number.
```

```
[ENTER:8686]
=>
```

📖 **Note**

. . . .

- Do not specify the port number currently operating - use the command below to check:

```
> netstat -a -n
```

- The specified port number may be in use elsewhere even if it is not currently operating (refer to "9.1 Port Numbers" for details).

. . . .

11. The prompts below will be displayed if upgrading from this version:

   - Systemwalker Runbook Automation V14g.V14.1.0 Management Server

   The prompts might also be displayed if any of these are already installed:

   - Cloud Infrastructure Management Software V1.2.0

   - Systemwalker Software Configuration Manager V14.1.0A

   Sets the subsystem number, port number, or user used by the schedule function.

```
=== <Systemwalker Runbook Automation Schedule Function Advanced Setup> ===
Enter the subsystem number.
[ENTER:9]
=>

=== <Systemwalker Runbook Automation Schedule Function Advanced Setup> ===
Enter the job scheduler port number.
[ENTER:9690]
=>

=== <Systemwalker Runbook Automation Schedule Function Advanced Setup> ===
Enter the Job Execution Control port number.
[ENTER:9691]
=>

=== <Systemwalker Runbook Automation Schedule Function Advanced Setup> ===
Enter the scheduled start user.
[ENTER:swrbasch]
=>

=== <Systemwalker Runbook Automation Schedule Function Advanced Setup> ===
Enter the password of the scheduled start user
.=>
```

📖 **Note**

. . . .

- Specify the port number if the default port number used by the schedule function is in use elsewhere.

- Do not specify the port number currently operating - use the command below to check:

```
> netstat -a -n
```

- The specified port number may be in use elsewhere even if it is not currently operating (refer to "9.1 Port Numbers" for details).

. . . .

12. The prompts below will be displayed if upgrading from this version and executing Management Server setup:

   - Systemwalker Runbook Automation V14g.V14.1.0 Management Server

   The prompts might also be displayed if any of these are already installed:

- Cloud Infrastructure Management Software V1.2.0 (Note)

- Systemwalker Software Configuration Manager V14.1.0A (Note)

- ServerView Resource Orchestrator Cloud Edition V3.0.0

Note: The applications process is used

Specify the port number used by Systemwalker Runbook Automation.

```
=== <Port numbers used by Systemwalker Runbook Automation setup> ===
Enter the message broker port number.
[ENTER:7676]
=>

=== <Port numbers used by Systemwalker Runbook Automation setup> ===
Enter the port number for the server function.
[ENTER:23700]
=>
```

📖 Note

- Do not specify the port number currently operating - use the command below to check:

```
> netstat -a -n
```

- The specified port number may be in use elsewhere even if it is not currently operating (refer to "" for details).

13. Confirm installation.

In the **Confirm Installation** window, make sure that the contents are correct, then click the **Confirm** button - upgrade will start. If updating installation information, enter the item numbers that will perform the updates. (note that this window is only displayed when the parameter has actually been specified).

```
=== <Installation destination directory> ===
Program deployment destination (cannot be changed): /opt
Setup files deployment destination (cannot be changed): /etc/opt
Work files deployment destination (cannot be changed): /var/opt
===<Information required for update tasks>===
1. Update operations working directory: /var/tmp/swrbawork
=== <SSO repository environment information> ===
2. SSO repository FQDN: ssoserver.example.com
3. SSO repository name: rep001
4. SSO repository number: 389
5. SSO repository administrator DN: cn=manager,ou=interstage,o=fujitsu,dc=com
=== <Systemwalker Runbook Automation port> ===
7. HTTP Listener port number: 28080
8. Administrator HTTP listener port number: 12001
9. IIOP port number: 23600
10. IIOP_SSL port number: 23601
11. IIOP_MUTUALAUTH port number: 23602
12. JMX_ADMIN port number: 8686
=== <Detailed Scheduling settings for Systemwalker Runbook Automation> ===
13. Subsystem Number: 9
14. Job Scheduler Port Number: 9690
15. Job Execution Control Port Number: 9691
16. User for Schedule Startup: swrbasch
=== <Port numbers used by Systemwalker Runbook Automation setup> ===
17. Port number for the message broker: 7676
18. Server function port number: 23700

Install with these settings? If not, enter the number of the item to change.
```

```
[y,q,number]
=>y
```

14. Start the installation.

When preparation for the installation is ready, the prompt below will be displayed and installation will start.

```
Installation in p;rogress.
```

15. Reboot the system.

After installation is completed, the window below will be displayed - enter "y" to reboot.

```
Installation of Systemwalker Runbook Automation (Management Server) is complete.
Reboot now?
[y,n]=>y
```

If an error occurs

- Act according to the displayed message, then restart the installer and execute the upgrade. Do not delete files and directories in the work area.

C.2.6 Subsequent operation when Systemwalker Centric Manager Operation Management Server has been installed

If the Systemwalker Centric Manager Operation Management Server has already been installed, restore and start the Systemwalker Centric Manager environment.

1. Stop Systemwalker Runbook Automation and Interstage

The start of Systemwalker Runbook Automation might not be completed immediately after reboot of OS. Please execute the this step after confirming the following messages in syslog (If the Windows, event log).n

```
FSP_SW/RB-A_BASE: INFO: 00407: Systemwalker Runbook Automation has started.
```

[Windows]

1. Stop Systemwalker Runbook Automation:

```
C:\> [Systemwalker Runbook Automation Management Server directory]\bin\swrba_stop
```

2. Stop Interstage:

```
C:\> isstop -f
```

[Linux]

1. Stop Systemwalker Runbook Automation:

```
# /opt/FJSVswrbam/bin/swrba_stop
```

2. Stop Interstage:

```
# isstop -f
```

2. Restore and start the Systemwalker Centric Manager environment

Follow the steps below:

[Windows]

1. Stop all Systemwalker Centric Manager features:

```
C:\> [Systemwalker Centric Manager installation path]\MPWALKER.DM\bin\pcentricmgr
```

2. Start the **Operation Environment Maintenance Wizard**.

3. Restore the Systemwalker Centric Manager environment. Select **Confirm ObjectDirector environment**.
   (In the window that asks you to confirm whether you want to rebuild the environment, click **No**.)

4. Start the Systemwalker Centric Manager service:

```
 C:\> [Systemwalker Centric Manager installation path]\MPWALKER.DM\bin\scentricmgr
```

[Linux]

1. Stop all Systemwalker Centric Manager features:

```
 # /opt/systemwalker/bin/pcentricmgr
```

2. Build the Systemwalker Centric Manager environment (for restore):

```
# /opt/systemwalker/bin/MpFwSetup -mix
```

   - In the setup menu (initial menu), enter "5" to display the maintenance menu.

   - In the maintenance menu, enter "2" to create the Systemwalker Centric Manager environment for restore.

   - In the **RESULT OF COMMUNICATION ENVIRONMENT CHECK** window, enter "2" to continue processing without the Systemwalker Centric Manager environment rebuild.

3. Restore Systemwalker Centric Manager.

   Refer to the Systemwalker Centric Manager manuals for details.

4. Start the Systemwalker Centric Manager service:

```
 # /opt/systemwalker/bin/scentricmgr
```

3. Start Systemwalker Runbook Automation and Interstage

Follow the steps below:

[Windows]

1. Start Interstage:

```
C:\> isstart
C:\> ihsstart -all
```

2. Start Systemwalker Runbook Automation:

```
C:\> [Systemwalker Runbook Automation Management Server directory]\bin\swrba_start
```

3. Restart CMDB.

```
C: \> [Systemwalker Runbook Automation Management Server directory] \SWRBAM\CMDB\FJSVcmdbm\bin
\cmdbstop
C: \> [Systemwalker Runbook Automation Management Server directory] \SWRBAM\CMDB\FJSVcmdbm\bin
\cmdbstart
```

[Linux]

1. Start Interstage:

```
# isstart
```

2. Start Systemwalker Runbook Automation:

```
# /opt/FJSVswrbam/bin/swrba_start
```

3. Restart CMDB.

```
# /opt/FJSVcmdbm/bin/cmdbstop.sh
# /opt/FJSVcmdbm/bin/cmdbstart.sh
```