

Cloud Infrastructure Management Software V1.2.0



User's Guide

Windows

J2UL-1404-03ENZ0(00)
June 2011

Preface

Purpose of This Document

This document presents an overview of the functions of Cloud Infrastructure Management Software (hereafter referred to as "this product"), and explains how to install, set up and operate this product.

Intended Readers

This document is intended for administrators who will use this product to operate the entire infrastructure for private clouds and data centers, as well as service providers who will use this product to provide services on private clouds.

Service users who will receive the services provided and conduct business activities on private clouds should refer to the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Users" that comes with this product.

Structure of This Document

This document is organized as follows:

Heading	Content
Chapter 1: Overview	This chapter presents an overview of this product.
Chapter 2: Operating Environment	This chapter explains the operating environment for this product.
Chapter 3: Installation and Uninstallation	This chapter explains how to install and uninstall this product.
Chapter 4: Operation and Management	This chapter explains how to operate and manage this product.
Appendix A: ICT Resource Management Functions	This appendix explains the management functions for the ICT resources managed by this product.
Appendix B: Managed Objects	This appendix explains the objects managed by this product.
Appendix C: Preparations and Checks before Installation	This appendix explains the preparation and check procedures that are required before this product is installed.
Appendix D: Port Numbers	This chapter explains the port numbers used by this product.
Appendix E: Tuning System Parameters	This appendix explains the tuning for Linux system parameters that is required when this product is used.
Appendix F: Creating and Setting up Interstage Single Sign-On Environments, and Cancelling the Setup	This appendix explains how to create and set up an Interstage Single Sign-On environment to be used with this product, and how to cancel the setup.
Appendix G: Command Reference	This appendix provides detailed information about the commands used with this product.
Appendix H: Registered Software IDs	This appendix explains the registered software IDs.
Appendix I: Registering and Deregistering Managed Servers	This appendix explains how to register and deregister Managed Servers.
Appendix J: Messages	This appendix explains the messages that are output or displayed by this product.
Glossary	This glossary explains the terms used in this product. Refer to this glossary when necessary.

Conventions Used in This Document

The conventions used in this document are as follows.

- Specific information is provided separately as below where functions differ according to the operating system required when this product is used.

[Windows]	Article relevant to Windows
[Linux]	Article relevant to Linux
[VMware]	Article relevant to VMware
[Hyper-V]	Article relevant to Hyper-V
[Windows/Linux]	Article relevant to Windows or Linux
[Manager]	Article relevant to the Manager
[Managed Server Resource Agent]	Article relevant to the Manager Server Resource Agent
[Business Server Agent]	Article relevant to the Business Server Agent
[Web Client]	Article relevant to the Web Client
[Admin Client]	Article relevant to the Admin Client
[User department]	Article relevant to the user department

- Unless otherwise specified, "blade servers" in this document refers to the PRIMERGY BX series.
- References are enclosed in double quotes (" ").
- Phrases and numbers that require particular emphasis are written in ***bold italics***.
- Window names, dialog names, menu names, and tab names are shown enclosed by square brackets ([]).
- Button names are shown enclosed by **bold angle brackets** (<>).
- The order of selecting menus is indicated using []-[].
- Text to be entered by the user are enclosed in angle brackets (<>).
- Some menu items are followed by an ellipse ("...") indicating that another window will be opened for entering settings or performing operations, but these ellipses are omitted when these menu items are referred to in this manual.
- In usage examples, prompts are denoted using the Windows prompt symbol ">". For Linux, replace this symbol with "#".
- The terms "folder" and "directory" are sometimes used interchangeably. For Windows, both of these terms can be interpreted as meaning "folder", whereas for Linux both terms can be interpreted as meaning "directory".

Website for Cloud Infrastructure Management Software

The website for Cloud Infrastructure Management Software publishes the latest manuals and technical information.

It is recommended that you refer to the website for Cloud Infrastructure Management Software before using this product. The URL address is as follows:

```
http://www.fujitsu.com/global/services/software/cims/ (as of June 2011)
```

Related Manuals

This product comes bundled with the following products:

- ServerView Resource Orchestrator V2.3.0
- Systemwalker Software Configuration Manager V14g
- Systemwalker Runbook Automation V14g
- Systemwalker Service Catalog Manager V14g

To refer to the content of the manuals that come with this product, view the manuals stored in the following locations on the product installation disks.

DISK1: Product manuals for ServerView Resource Orchestrator (Windows/Linux)

```
<DVD drive>:\DISK1\packages\ROR\Common>manual\en
```

DISK2: Product manuals for Systemwalker Software Configuration Manager V14g (Windows/Linux)

```
<DVD drive>:\DISK2\packages\CFMG>manual\CFMG
```

DISK2: Product manuals for Systemwalker Runbook Automation V14g (Windows/Linux)

```
<DVD drive>:\DISK2\packages\CFMG>manual\RBA
```

DISK3: Product manuals for Systemwalker Service Catalog Manager V14g (Windows/Linux)

```
<DVD drive>:\DISK3\packages\CTMG\unified\Discl\CT-MG\Manual
```

Note that functions other than those provided by Cloud Infrastructure Management Software cannot be used although there is a description in the related product manuals.

Refer also to the following manuals as necessary.

- When using VMware
 - vSphere Basic System Administration
 - vSphere Resource Management Guide
 - Guest Operating System Installation Guide
- When performing detailed operations using ICT resources
 - ServerView Resource Coordinator VE Installation Guide
 - ServerView Resource Coordinator VE Setup Guide
 - ServerView Resource Coordinator VE Operation Guide
 - ServerView Resource Coordinator VE Command Reference
 - ServerView Resource Coordinator VE Message Guide

Abbreviations

The abbreviations used in this document are as follows:

Abbreviation	Product
Windows	Microsoft(R) Windows Server(R) 2008 Standard
	Microsoft(R) Windows Server(R) 2008 Enterprise
	Microsoft(R) Windows Server(R) 2008 R2 Standard
	Microsoft(R) Windows Server(R) 2008 R2 Enterprise
	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
	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
	Windows(R) 7 Professional
	Windows(R) 7 Ultimate
	Windows Vista(R) Business
	Windows Vista(R) Enterprise
	Windows Vista(R) Ultimate
	Microsoft(R) Windows(R) XP Professional operating system

Abbreviation	Product
Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter
Windows 2008 x86 Edition	Microsoft(R) Windows Server(R) 2008 Standard (x86) Microsoft(R) Windows Server(R) 2008 Enterprise (x86)
Windows 2008 x64 Edition	Microsoft(R) Windows Server(R) 2008 Standard (x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x64)
Windows Server 2003	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
Windows 2003 x64 Edition	Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
Windows 7	Windows(R) 7 Professional Windows(R) 7 Ultimate
Windows Vista	Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate
Windows XP	Microsoft(R) Windows(R) XP Professional operating system
Linux or Red Hat Enterprise Linux	Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64)
ESC	ETERNUS SF Storage Cruiser
GLS	PRIMECLUSTER GLS
MSFC	Microsoft Failover Cluster
SCVMM	System Center Virtual Machine Manager 2008 R2
VMware	VMware vSphere(TM) 4 VMware vSphere(TM) 4.1
RCVE	ServerView Resource Coordinator VE
ROR	ServerView Resource Orchestrator
CMDB	Configuration Management DataBase
IBPMA	Interstage Business Process Manager Analytics
CIMS	Cloud Infrastructure Management Software

Export Restriction

Fujitsu documentation may contain specific technologies that apply to foreign exchange and foreign trade control laws. When such specific technology is described in the document, and that document is either exported or provided to a non-resident, permission based on these laws is required.

Trademarks

- Adobe, Adobe Reader, and Flash are trademarks or registered trademarks of Adobe Systems Incorporated in the United State and other countries.
- Interstage, ServerView, Symfoware, and Systemwalker are registered trademarks of FUJITSU LIMITED.
- Linux is a trademark or registered trademark of Mr. Linus Torvalds in the United States and other countries.

- Microsoft, Windows, Windows XP, Windows Server, Windows Vista, Windows 7, Excel, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- NetApp is a registered trademark of Network Appliance, Inc. in the United States and other countries. Data ONTAP, Network Appliance, and Snapshot are trademarks of Network Appliance, Inc. in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States and other countries.
- Red Hat, RPM and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. 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/or other jurisdictions.
- Other company names and product names are trademarks or registered trademarks of respective companies.

Note that system names and product names in this document are not accompanied by trademark symbols such as (TM) or (R).

Issue Date and Version

June 2011: Third Edition

Copyright Notice

No part of the content of this manual may be reproduced without the written permission of Fujitsu Limited.

The contents of this manual may be changed without notice.

Copyright 2011 FUJITSU LIMITED.

Contents

Chapter 1 Overview.....	1
1.1 Features.....	1
1.2 Functional Overview.....	1
1.3 System Configuration.....	4
Chapter 2 Operating Environment.....	7
2.1 Hardware Environment.....	7
2.1.1 Static disk capacity.....	7
2.1.2 Dynamic disk capacity.....	7
2.1.3 Memory capacity.....	7
2.2 Software Environment.....	8
2.2.1 Software Configuration.....	8
2.2.2 Software Requirements.....	8
2.2.2.1 Operating system.....	8
2.2.2.2 Required patches.....	10
2.2.2.3 Required software.....	11
2.2.2.4 Conflicting software.....	13
Chapter 3 Installation and Uninstallation.....	18
3.1 Installing on the Admin Server.....	18
3.1.1 Preparing for Installation.....	18
3.1.2 Installing the Required Software.....	20
3.1.2.1 Downloading and Setting Up the Required Software.....	20
3.1.3 Installing the Manager.....	21
3.1.3.1 Installing on Windows systems [Windows].....	25
3.1.4 Setup.....	25
3.1.4.1 Creating and Setting up Interstage Single Sign-On Environments.....	25
3.1.4.2 Registering Users, Groups and Organizational Units.....	26
3.1.4.2.1 Registering User Information with the Interstage Directory Service.....	26
3.1.4.2.2 Registering users for service providers (configuration management function).....	31
3.1.4.2.3 Registering users for service providers (Self Service Portal).....	32
3.1.4.3 Setting up the Connection to the LDAP Server.....	34
3.1.4.4 Setting up the CMDB.....	34
3.1.4.5 The User Allowed to Access the Database.....	34
3.1.4.6 Setting up the Automatic Operation Function [Windows].....	35
3.1.4.7 Registering the Mail Server.....	38
3.1.4.8 Setting up the Catalog Function.....	40
3.1.4.9 Tuning the Desktop Heap [Windows].....	40
3.1.4.10 Restarting the Operating System.....	41
3.1.5 Post-setup Tasks.....	41
3.1.5.1 Starting the Web Servers.....	42
3.1.5.2 Setting up Mail and Accounting Information.....	42
3.1.5.3 Setting up Information for Interstage Single Sign-On.....	45
3.1.5.4 Register the Application Process.....	48
3.1.5.5 Registering Managed Servers for the Cloud Infrastructure Administrator Dashboard.....	51
3.2 Installing on Managed Servers.....	51
3.2.1 Preparing for Installation.....	51
3.2.2 Installing the Required Software.....	52
3.2.3 Installing Managed Server Resource Agents.....	52
3.2.3.1 Installing Managed Server Resource Agents [VMware].....	52
3.2.3.2 Installing Managed Server Resource Agents [Hyper-V].....	53
3.3 Installing on the VM Server.....	53
3.3.1 Preparing for Installation.....	53
3.3.2 Installing the Required Software.....	54
3.3.3 Installing Business Server Agents.....	54

3.3.3.1	Installing Business Server Agents [Windows]	54
3.3.3.2	Installing Business Server Agents [Linux]	55
3.4	Uninstalling the Manager from the Admin Server	56
3.4.1	Tasks to Perform Before Cancelling the Setup	56
3.4.2	Canceling the Setup	56
3.4.2.1	Canceling the Setup of the Automatic Operation Function [Windows]	57
3.4.2.2	Canceling the Setup for the CMDB	57
3.4.2.3	Canceling the Setup for the Manager	57
3.4.3	Tasks to Perform After Cancelling the Setup	57
3.4.4	Uninstalling the Manager	58
3.4.4.1	Uninstalling the Manager [Windows]	58
3.4.5	Tasks to Perform After Uninstallation	58
3.4.5.1	Uninstalling the Fujitsu XML Processor [Windows]	58
3.4.5.2	Deleting the User Information for Accessing the Database	59
3.4.5.3	Files that Remain After Uninstallation	59
3.4.5.4	Groups that Remain After Uninstallation	60
3.5	Uninstalling Managed Server Resource Agents from Managed Servers	60
3.5.1	Uninstalling Managed Server Resource Agents	60
3.5.1.1	Uninstalling Managed Server Resource Agents [Hyper-V]	60
3.5.1.2	Uninstalling Managed Server Resource Agents [VMware]	61
3.6	Uninstalling Business Server Agents from VM Servers	61
3.6.1	Uninstalling Business Server Agents	61
3.6.1.1	Uninstalling Business Server Agents [Windows]	61
3.6.1.2	Uninstalling Business Server Agents [Linux]	61
3.6.2	Post-uninstallation Tasks	62
3.6.2.1	Uninstalling SMEE [Linux]	62
3.6.2.2	Uninstalling the Securecrypto Library Runtime [Linux]	62
3.6.2.3	Files that Remain After Uninstallation	62
3.6.2.4	Notes to Observe After Uninstalling SMEE and the Securecrypto Library Runtime [Linux]	63
3.7	Uninstalling "Uninstall (middleware)"	63
Chapter 4	Operation and Management	66
4.1	User Management	66
4.2	Overview of Service Operations	67
4.3	Operation Procedures for Service Providers	69
4.3.1	Registering Resources	69
4.3.2	Registering Resources in Resource Pools	69
4.3.2.1	VM host resources	70
4.3.2.2	Storage resources	70
4.3.2.3	Network resources	71
4.3.2.4	Virtual Image resources	75
4.3.3	Creating and Managing L-Server Templates	75
4.3.4	Creating and Managing L-Servers	76
4.3.4.1	Creating an L-Server	76
4.3.4.2	Managing L-Servers	77
4.3.5	Creating, Registering and Deleting System Templates	77
4.3.6	Publishing and Deleting Services	80
4.4	Applying to Use Services and Returning Services (for Service Users)	81
4.5	Approving and Checking Applications to Use Services	82
4.6	Visualizing ICT Resources	83
4.7	Managing Accounting Information	84
4.8	Backing up or Restoring the Admin Server	85
4.8.1	Notes on Backing up and Restoring the Admin Server	85
4.8.2	Backing up the Admin Server	86
4.8.2.1	Stopping the CIMS Systems	86
4.8.2.2	Backing up the CIMS Resources (Resources for the Self Service Portal)	87
4.8.2.3	Backing up the CIMS Resources (Configuration Management Resources)	87

4.8.2.4 Backing up the CIMS Resources (Application Process Resources).....	87
4.8.2.5 Backing up the CIMS Resources (Interstage Single Sign-On Resources).....	87
4.8.2.6 Backing up the CIMS Resources (Resource Pool Management Resources).....	88
4.8.2.7 Starting the CIMS System.....	89
4.8.3 Restoring the Admin Server.....	90
4.8.3.1 Stopping the CIMS System.....	90
4.8.3.2 Restoring the CIMS Resources (Resource Pool Management Resources).....	90
4.8.3.3 Restoring the CIMS Resources (Application Process Resources and Interstage Single Sign-On Resources).....	91
4.8.3.4 Restoring the CIMS Resources(Configuration Management Resources).....	92
4.8.3.5 Restoring the CIMS Resources (Resources for the Self Service Portal).....	92
4.8.3.6 Starting the CIMS System.....	93
4.8.3.7 Updating the CMDB for CIMS.....	93
Appendix A ICT Resource Management Functions.....	94
A.1 Resource Pools.....	94
A.2 Logical Servers (L-Servers).....	95
A.3 L-Server Templates.....	96
A.4 RC Console.....	96
Appendix B Managed Objects.....	100
B.1 Users of This Product.....	100
B.2 ICT Resources.....	100
B.3 Templates.....	102
B.4 Services.....	102
Appendix C Preparations and Checks before Installation.....	103
C.1 Preparations and Checks Before Installation.....	103
Appendix D Port Numbers.....	104
D.1 List of Port Numbers.....	104
D.2 Procedure for Changing Ports.....	107
D.2.1 Procedure for Changing Port Numbers for the Dynamic Resource Management Server.....	107
D.2.2 Procedure for Changing Port Numbers for the Self Service Portal/Configuration Management.....	108
Appendix E Tuning System Parameters.....	112
E.1 Tuning Values for System Parameters.....	112
E.2 Tuning Procedure.....	113
Appendix F Creating and Setting up Interstage Single Sign-On Environments, and Cancelling the Setup.....	115
F.1 Creating and Setting up Interstage Single Sign-On Environments.....	115
F.1.1 Creating an SSL Communication Environment.....	115
F.1.2 Setting up Interstage Single Sign-On.....	120
F.2 Canceling the Setup for Interstage Single Sign-On.....	124
Appendix G Command Reference.....	127
G.1 Environment Setup and Control Commands.....	127
G.1.1 Overview of the Environment Setup and Control Commands.....	127
G.1.2 Manager Control Commands.....	127
G.2 Template Management Commands.....	129
G.2.1 Overview of the Template Management Commands.....	130
G.2.2 Software Information Manipulation Commands.....	132
G.2.3 Image Information Manipulation Commands.....	136
G.2.4 Segment Information Manipulation Commands.....	144
G.2.5 Template Information Manipulation Commands.....	149
G.3 Interstage Single Sign-On Management Commands.....	158
G.3.1 Overview of Interstage Single Sign-On Management Commands.....	158
G.3.2 Interstage Single Sign-On System Creation Command.....	159
G.3.3 Interstage Single Sign-On System Deletion Command.....	161
G.3.4 Interstage Single Sign-On Start and Stop Command.....	163

G.3.5 Interstage Single Sign-On Backup Command.....	164
G.3.6 Interstage Single Sign-On Restore Command.....	166
Appendix H Registered Software IDs.....	169
Appendix I Registering and Deregistering Managed Servers.....	171
I.1 Registering VM Hosts.....	171
I.1.1 Setting up Resource Information Collection from the VM Host.....	171
I.1.2 Registering the VM Host on the Admin Server.....	173
I.2 Registering Devices for which Eco Information is Collected.....	174
I.2.1 Setting up the Devices for which Eco Information is Collected.....	174
I.2.2 Registering Devices on the Admin Server.....	175
I.3 Applying Registered Information.....	175
I.4 Deregistering VM Hosts.....	176
I.5 Deregistering Devices for which Eco Information is Collected.....	177
Appendix J Messages.....	179
J.1 Messages during Installation.....	179
J.2 Messages during Command Execution.....	179
J.3 How to Collect Investigation Data.....	181
Glossary.....	182

Chapter 1 Overview

This chapter presents an overview of this product.

1.1 Features

In order to optimize customers' ICT systems, it is important to use virtualization to integrate ICT resources (such as servers, storage, and networks) so that they can be used efficiently.

There is also a demand for self-service functions that enable virtual platforms to be provided to users as soon as they are required. Cloud Infrastructure Management Software is a software product that manages ICT resources in a private cloud environment by grouping them into pools and automatically deploys ICT resources in response to user requests.

This product also supports efficient usage by visualizing the usage status of ICT resources.

This product has the following features.

Private cloud systems can be created easily

Cloud systems that deploy everything from infrastructure systems (Fujitsu PRIMERGY servers, storage and networks) through to operating systems can be provided quickly.

ICT resources can be utilized efficiently according to how much they are used

Visualizing ICT resources allows users to track their usage status, which makes it possible to utilize ICT resources flexibly.

The private cloud can start small

This product allows users to start off small by purchasing only a single server and then expand to full-scale operations later.

The private cloud can be expanded in the future

By installing the following related software products, Cloud Infrastructure Management Software can be used as internal service infrastructure where everything up to the middleware level has been deployed, or can be used to create private clouds for multi-vendor server environments. For each of these related software products, a new license must be purchased.

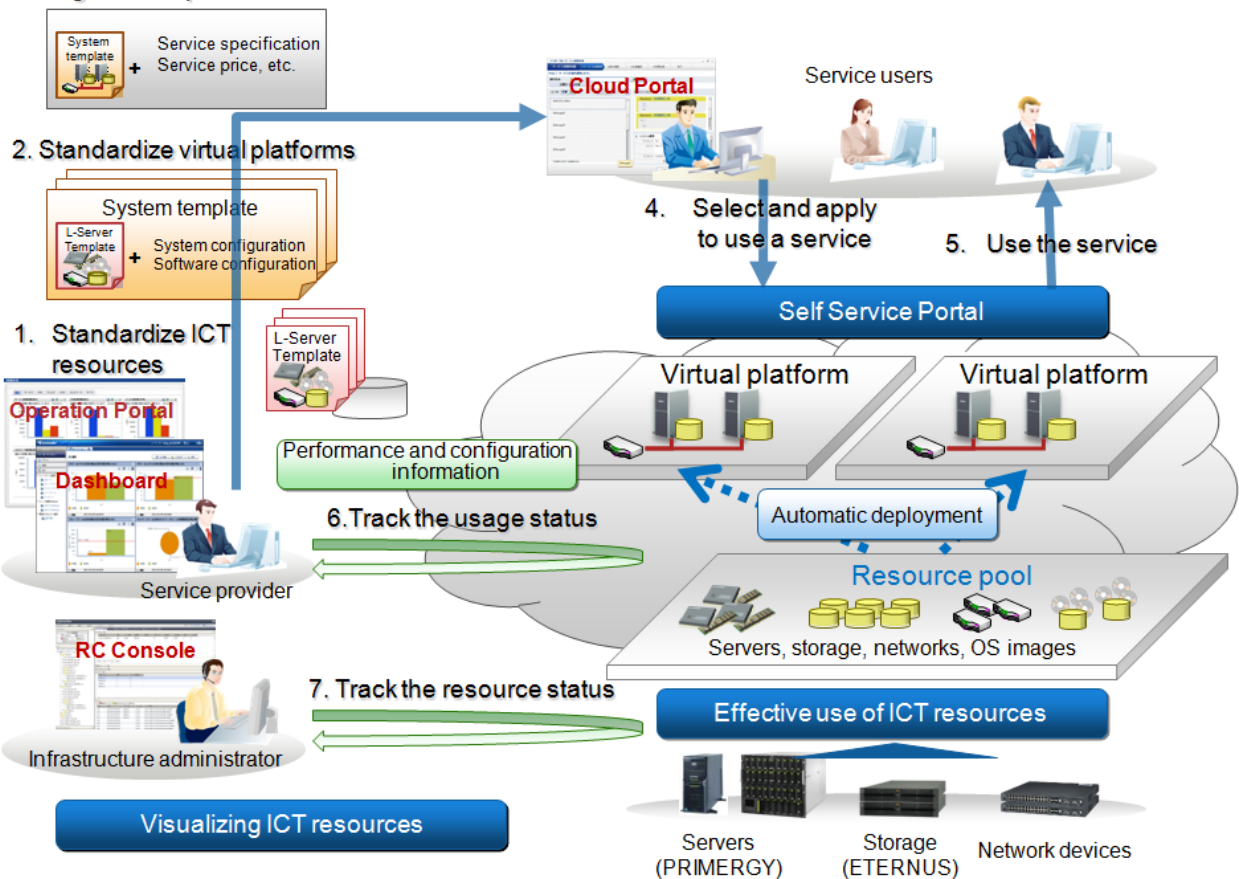
Table 1.1 Related software

Item No.	Software name	Software functions
1	Systemwalker Service Catalog Manager V14g (14.1.0)	This product converts applications to services, and enables various self-service management functions to be used from user applications via APIs.
2	Systemwalker Software Configuration Manager V14g (14.1.0)	This product automatically deploys software (business applications and middleware) including parameter settings.
3	Systemwalker Runbook Automation V14g (14.1.0)	This product automates administrative procedures.
4	ServerView Resource Orchestrator V2.3.0	This product centrally manages ICT resources (such as servers, storage and networks) including multi-vendor servers.

1.2 Functional Overview

This section explains the roles of people that use this product, as well as the functions corresponding to each role.

3. Register and publish the lease service



Infrastructure administrator

This product installs Logical Servers (L-Servers), which define the logical specifications (such as the number of CPUs, memory capacity, disk capacity, and the number of NICs) for the ICT resources (such as servers, storage, and networks) in the private cloud. Systems where L-Servers have been layered are referred to as *"virtual platforms"*.

Infrastructure administrators manage the ICT resources (such as servers, storage, and networks) in the private cloud, as well as the operating systems that run on virtual platforms.

As well as using this product to centrally manage ICT resources by grouping them into pools, infrastructure administrators also keep track of the load on ICT resources so that they can add, replace or maintain resources as necessary.

Infrastructure administrators can perform sequences of operations using the *"RC Console"*.

- RC Console

The RC Console allows infrastructure administrators to manage the environment for reading and writing L-Server Templates and managing ICT resources.

Service provider

Service providers provide services to service users. Service providers prepare templates for pre-patterned virtual platform environments according to service users' purposes, and then make these templates available to service users as services.

In some cases, service providers also accept applications from service users and assess the content of these applications, in accordance with an application process.

Service providers can also monitor operations and check the status of how service users are using their service. This monitoring and status checking is performed using the **[Operation Portal]**.

- Operation Portal

The Operation Portal enables service providers (the managers of provider departments) to check the status of how service users are using the service, monitor the operation, and assess application processes.

- Cloud infrastructure administrator dashboard

The cloud infrastructure administrator dashboard is a function for collecting and centrally displaying the information required for administration in a cloud environment. The cloud infrastructure administrator dashboard can be used by selecting [**Operation Monitor**] from the menu of the [**Operation Portal**].

Service user

A service user is a user who receives a service from a service provider. Service users apply to use a virtual platform that can be used as a service, and then use a virtual platform that has been configured according to the application submitted.

If approval from the person in charge of the department using the service is required when the application is made, the service user makes a request for approval to the person in charge in accordance with the application process.

Service users can use the "Cloud Portal" to apply to use a service, and to check the virtual systems that make up the services that they are using.

- Cloud Portal

The Cloud Portal enables service users (the managers of user departments) to perform sequences of operations, such as applying to use services in MyPortal, managing users, checking application processes to see whether applications to use services have been approved, and checking the usage status of services.

- MyPortal

MyPortal is linked to the Cloud Portal in order to make applications to use services for operations to be performed by each service user, manage systems and display event logs.

Table 1.2 Roles

Item No.	Service utilization procedure	Description	People concerned
1	Standardizing ICT resources (L-Server Templates (*1))	Service providers create L-Server Templates by patterning (standardizing) configurations of ICT resources and operating systems.	Service provider
2	Standardizing virtual platforms (system templates)	Service providers create system templates by patterning (standardizing) multi-layer system configurations and logical configurations for operating systems.	Service provider
3	Registering and publishing a service	Service providers define system templates plus information such as price settings according to usages, and publish them as services.	Service provider
4	Selecting and applying to use a service	Service users search through the services that have been published, select a virtual platform that meets the usage purpose, and then apply to use that virtual platform. Applications to return virtual platforms that are no longer required can be performed in the same way. Service users can start, stop, and take snapshots of the virtual platforms with which they have been provided.	Service user
5	Using the service	The virtual platforms corresponding to the services that service users have applied to use are lease or returned automatically by this product. Processing is also performed automatically by this product according to instructions for operations such as starting and stopping virtual servers, and taking snapshots.	Service user

Item No.	Service utilization procedure	Description	People concerned
6	Tracking the usage status	Service providers track the usage status of each service (such as CPU, memory, disk usage, and time). Service providers can also monitor the billing information for the use of their services.	Service provider
7	Tracking the resource status	Infrastructure administrators can monitor the lease on each resource based on the usage status of resources, and make decisions about using ICT resources efficiently or adding more resources when there are not enough resources.	Infrastructure administrator

*1: Refer to "[A.2 Logical Servers \(L-Servers\)](#)" and "[A.3 L-Server Templates](#)" for details on L-Servers and L-Server Templates, respectively.

This product provides the following functions and function ranges.

Self Service Portal

Service users can use services (such as virtual platform environment creation (*1)) on demand, by selecting services from the Self Service Portal and applying to use them.

All of the processing from applying to use a service through to actually using the service is executed automatically. Some services require the approval of the person in charge before they can be used. For these services, the approval flow (from requesting approval through to receiving approval) is executed automatically.

Effective use of ICT resources

ICT resources such as servers (*2), storage and networks can be managed by grouping them into resource pools, so that ICT resources can be utilized effectively according to changing levels of use.

Refer to "[Appendix A ICT Resource Management Functions](#)" for details.

Visualizing ICT resources

The usage status of ICT resources can be tracked easily using the dashboard.

The dashboard allows users to monitor information such as resource information for virtual servers and the availability status of resource pools. It also allows users to specify thresholds for the monitored data, so that alerts are notified automatically when the thresholds are exceeded.

*1: Additional "[Table 1.1 Related software](#)" is required to create environments for software (middleware and business applications).

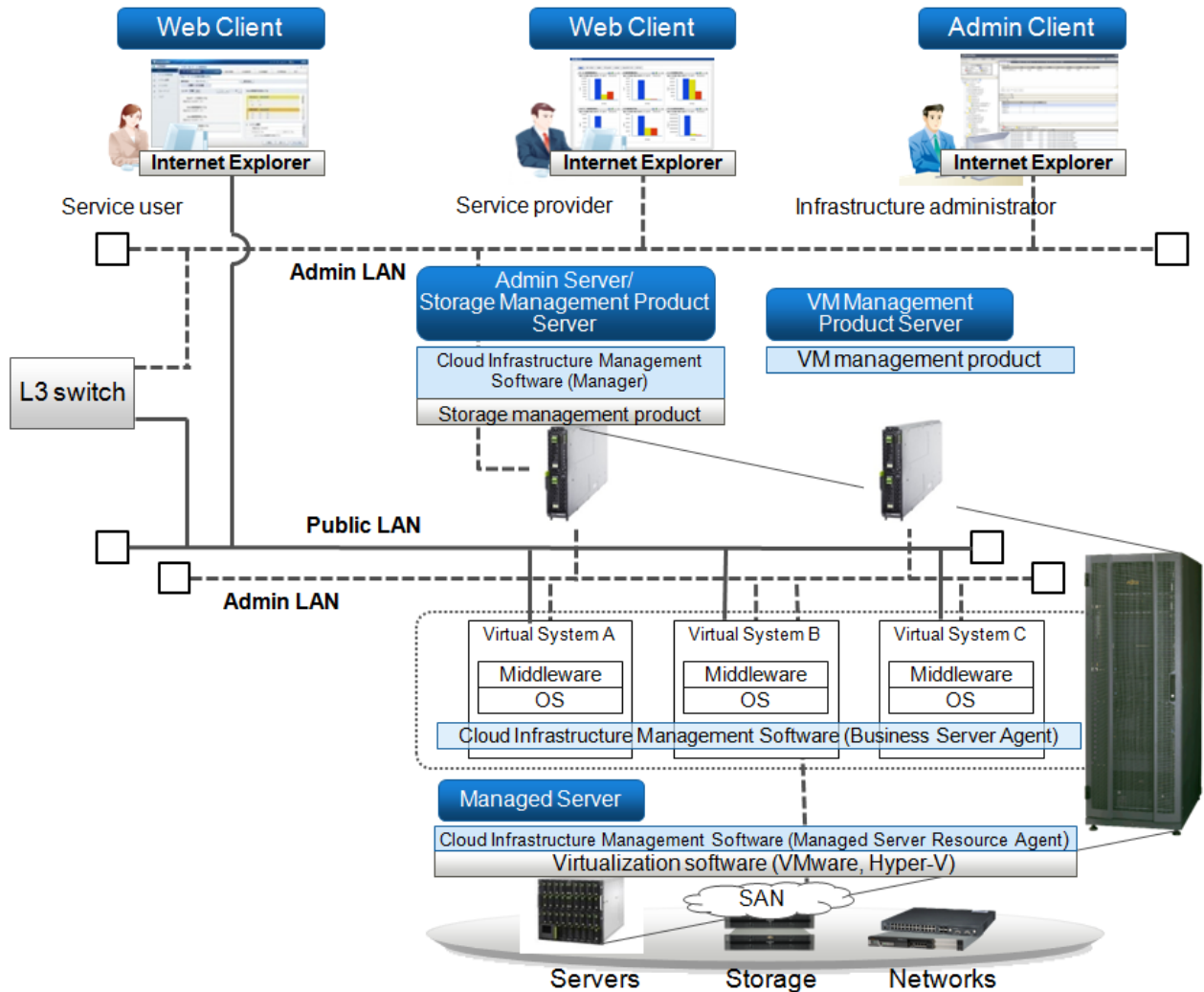
*2: ServerView Resource Orchestrator is required for multi-vendor servers other than Fujitsu PRIMERGY servers.

Refer to "[Appendix B Managed Objects](#)" for details on the resources and users handled by this product.

1.3 System Configuration

This section explains the system configuration for this product, using an example.

Figure 1.1 System configuration example



Admin Server

The Admin Server is a server that manages multiple Managed Servers. The Admin Server can run in either a Windows environment or a Linux environment.

The Manager function of Cloud Infrastructure Management Software is installed on the Admin Server.

By using a virtual environment, it is possible to use high-reliability configurations for virtualization software (such as VMware-HA).

For Windows, the Admin Client can be located on the same machine as the Admin Server.

Note that it is not possible to monitor or operate on the Admin Server itself by installing the Agent function on the Admin Server.

Manager

The Manager is a function that is installed on the Admin Server in order to centrally manage the data handled by Cloud Infrastructure Management Software. The Manager issues processing requests to the Agent function installed on the Managed Servers to which virtual platforms have been deployed.

Managed Server

Managed Servers are servers where the server virtualization software product runs. The Agent function of Cloud Infrastructure Management Software is installed on Managed Servers. The server virtualization software receives deployment instructions from the Manager function on the Admin Server, and virtual platforms are deployed on Managed Servers.

Managed Server Resource Agent

The Managed Server Resource Agent is installed on the operating systems for Managed Servers. It receives deployment instructions from the Manager, and then links to the server virtualization software product on the Managed Server to create a virtual platform.

VM Server

VM Servers are Business Servers (virtual servers) that are deployed as virtual platforms on Managed Servers by Cloud Infrastructure Management Software. VM Servers are managed by the Manager on the Admin Server.

Business Server Agent

Business Server Agents are installed on the virtual images that are the basis for VM Servers. They collect information such as the usage status of virtual platforms, and notify this information to the Manager.

Web Client

The Web Client is a client terminal that service providers and service users use to perform operations such as defining various services and applying to use services.

Admin Client

The Admin Client is a client terminal that is connected to the Admin Server in order to check and control the status or configuration of the entire system via a GUI.

Admin Clients run in Windows environments.

Storage Management Product Server

The Storage Management Product Server is a server for running a storage management product (such as ETERNUS SF Storage Cruiser) that manages multiple storage devices. The Storage Management Product Server must be located on the same machine as the Admin Server. Note that the machine that hosts both the Admin Server and the storage management product must have enough resources to run both products.

VM Management Product Server

The VM Management Product Server is a server for running a VM management product (such as VMware vCenter Server or System Center Virtual Machine Manager) that manages multiple server virtualization software products in an integrated fashion. The VM Management Product Server can be located on the same machine as the Admin Server.

If the VM Management Product Server and the Admin Server are installed on the same machine, that machine must have enough resources to run both the Admin Server and the VM management product.

Admin LAN

The admin LAN is a LAN for managing Managed Servers and storage devices from the Admin Server.

The admin LAN is set up separately from the public LAN that is used to perform jobs on Managed Servers.

The admin LAN and the public LAN can be made redundant by using network redundancy software on servers. Set up the network redundancy software manually.



Information

The first NIC that is available for the admin LAN can be changed.

For details, refer to "6.1.3.1 Registering Blade Servers and Partition Model Servers" in the "ServerView Resource Coordinator VE Setup Guide".

Public LAN

The public LAN is a LAN for business activities, to which Business Servers (VM Servers) are connected.

It is recommended that the public LAN be connected to the admin LAN via an L3 switch, and that a firewall that uses an access control list (ACL) be set up.

It is also possible to use an L3 switch to completely separate the public LAN from the admin LAN. However, if the two LANs are separated, the following operations cannot be performed:

- Visualizing the resource usage status
- Submitting applications from service users on the public LAN

Chapter 2 Operating Environment

This chapter explains the operating environment for this product.

2.1 Hardware Environment

The hardware conditions described below must be met when using Cloud Infrastructure Management Software.

2.1.1 Static disk capacity

The following static disk capacity is required to make a new installation for this product. The disk capacity varies slightly according to differences in the environments being checked.

Static disk capacity (not including the operating system)

[Manager]

OS type	Folder	Disk capacity (in MB)
Windows	Installation folder (*1)	5037

[Managed Server Resource Agent]

OS type	Folder	Disk capacity (in MB)
VMware	/opt	325
	/etc	15
	/var	2
Hyper-V	Installation folder (*1)	330

*1: This is the name of the installation folder that is specified when the software is installed.

2.1.2 Dynamic disk capacity

When this product is used, each folder requires the following disk capacity in addition to the static disk capacity. Refer to the following manuals for details.

- "1.1.2.5 Dynamic disk capacity" in the "ServerView Resource Coordinator VE Installation Guide"
- "3.1.2 Disk Capacity Required" in the "Systemwalker Service Catalog Manager V14g Technical Guide"
- "2.1.4 Disk Capacity Required" in the "Systemwalker Service Catalog Manager V14g Cloud Operation Management Dashboard User's Guide"
- "3.1 Required Hardware" in the "Systemwalker Software Configuration Manager V14g Technical Guide"

2.1.3 Memory capacity

The following memory capacity is required to use this product.

Memory capacity (not including the operating system)

[Manager]

OS type	Memory capacity (in MB)
Windows	10400 or more

*1: In addition to the values above, memory for Interstage Application Server and Systemwalker Service Quality Coordinator is also required. Refer to the "Interstage Application Server Tuning Guide" and the "Systemwalker Service Quality Coordinator Installation Guide" for details.

[Managed Server Resource Agent]

Virtual environment	Memory capacity (in MB)
VMware	32
Hyper-V	32

[Business Server Agent]

Virtual environment	Memory capacity (in MB)
Windows	400
Linux	400

*1: In addition to the values above, memory for Systemwalker Service Quality Coordinator (Agent) is also required. Refer to the "Systemwalker Service Quality Coordinator Installation Guide" for details.

2.2 Software Environment

This product consists of the following DVDs:

- Cloud Infrastructure Management Software (the media pack includes a DVD for the Windows version and a DVD for the Linux version)

2.2.1 Software Configuration

This product consists of the following software programs.

Software name	Functional overview
Cloud Infrastructure Management Software V1.2.0 Manager	This software automatically deploys virtual platforms and manages self-service functions (such as starting and stopping virtual servers, taking snapshots, and restoring virtual servers from snapshots).
Cloud Infrastructure Management Software V1.2.0 Agent	- Managed Server Resource Agent This software runs on Managed Servers, and deploys the virtual platforms that service users have applied to use.
	- Business Server Agent This software runs on the virtual platforms that are deployed to Managed Servers, and collects information about resources (CPU, memory and disks) and about the usage status of the virtual platform.

2.2.2 Software Requirements

This section explains the software requirements for installing this product.

2.2.2.1 Operating system

The following operating system is required to use this product.

[Manager]

Operating system type	Operating system	Remarks
Windows	Microsoft(R) Windows Server(R) 2008 R2 Standard (*) Microsoft(R) Windows Server(R) 2008 R2 Enterprise (*)	The Server Core installation option is not supported.

*: Runs as a 32-bit application on the WOW64 (Windows 32-bit On Windows 64-bit) subsystem.

[Managed Server Resource Agent]

Virtual environment	Virtualization software	Remarks
VMware	VMware vSphere(TM) 4 VMware vSphere(TM) 4.1	Install the Managed Server Resource Agent on VMware ESX hosts.
Hyper-V	Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	The Server Core installation option is not supported. Turn the Hyper-V role on. Add Microsoft Failover Cluster (MSFC). Only the Windows Manager is supported.

[Business Server Agent]

Operating system type	Operating system	Remarks
Windows	Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64) Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise	The Server Core installation option is not supported.
	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	SP2 or higher is supported.
Linux	Red Hat(R) Enterprise Linux(R) 5.5 (for x86) Red Hat(R) Enterprise Linux(R) 5.5 (for Intel64)	Prepare any required software such as driver kits and update kits. For information on required software, refer to the manuals for each server, and to the Linux installation guides.

 Note

- Some of the functions of the server virtualization software product used by this product are not supported by this product. Do not use these functions.

Server virtualization software product	Functions that do not support use with this product
VMware vSphere (TM) 4 VMware vSphere (TM) 4.1	VMware Storage VMotion VMware vNetwork Distributed Switch and Cisco Nexus 1000V virtual switch VMware vStorage Thin Provisioning
Microsoft(R) System Center Virtual Machine Manager 2008 R2	- Memory area migration - Migration that involves changing the storage location of a virtual machine - Storing in libraries for virtual machines

[Hyper-V]

- If Managed Servers use Hyper-V, only Windows is supported as the operating system of the Admin Server.

- SCVMM can manage VMware ESX via VMware vCenter Server. However, with this product, VMware ESX cannot be managed via SCVMM. To manage VMware ESX with this kind of configuration, register VMware vCenter Server with this product.
- If a Windows image is specified when an L-Server is created, server-specific information will be reset using Sysprep (which is available from Microsoft) when the image is deployed. User information and operating system settings are also initialized when Sysprep is executed.
For information on Sysprep, refer to the information provided by Microsoft.
- If the Manager is stopped and restarted while processing is being executed, the processing will be re-executed after the Manager starts. Wait until the processing that is being executed completes before performing any new operations on the same resources.
- If the operating system for the image uses MAK license authentication for the activation method (as is the case with Windows Server 2008, for example), the total number of times that Sysprep can be executed will be limited to only three times. Sysprep is executed when an L-Server is created by specifying an image, or when a cloning master is taken, which means that these operations (taking cloning masters and creating L-Servers by specifying images) cannot be performed more than three times. For this reason, it is recommended that cloning masters be taken from a dedicated master server, rather than from L-Servers to which cloning masters have been distributed. Note that Sysprep is also executed when a guest operating system is customized using the template function with VMware, or when templates are created using SCVMM, and that these Sysprep executions are counted in the total number of executions.

[Windows][VMware]

- If an L-Server has been created by specifying a Windows image, use Sysprep to reset the server-specific information when the L-Server is started for the first time after being created. When the L-Server Console is opened from the management window for the server virtualization software product after the L-Server has been started and the server-specific information has been reset, the Administrator will be automatically logged into the L-Server Console, so it is recommended that you log off from the L-Server Console.
- Note the following points when taking a cloning master from an L-Server that has been created using a cloning master.
 - When L-Servers have never been started since they were created, and when server-specific information has not been set up, an L-Server creation may fail if a cloning master taken from such an L-Server is used to create another L-Server. To take a cloning master from such an L-Server, be sure to start the target L-Server at least once so that the server-specific information will be set up for the L-Server.

.....

The software for this product does not need to be installed on the Admin Client, but the following operating system is required.

[Admin Client]

Operating system	Remarks
Microsoft(R) Windows(R) 7 Professional Microsoft(R) Windows(R) 7 Ultimate	-
Microsoft(R) Windows Vista(R) Business Microsoft(R) Windows Vista(R) Enterprise Microsoft(R) Windows Vista(R) Ultimate	SP1 or higher is supported.
Microsoft(R) Windows(R) XP Professional operating system	SP3 or higher is supported.
Microsoft(R) Windows Server(R) 2008 Standard (x86, x64) Microsoft(R) Windows Server(R) 2008 Enterprise (x86, x64) Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	The Server Core installation option is not supported.
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	SP2 or higher is supported.

2.2.2.2 Required patches

The following patch programs are required to use this product.

[Manager]

Operating system type	Operating system	Patch ID/Batch update
Windows	PRIMECLUSTER GLS	TP002714XP-06

[Managed Server Resource Agent]

Virtual environment	Operating system	Patch ID/Batch update
VMware	None	-
Hyper-V	None	-

[Business Server Agent]

Virtual environment	Operating system	Patch ID/Batch update
VMware	None	-
Hyper-V	None	-

2.2.2.3 Required software

The following software programs are required to use this product.

[Manager]

Operating system type	Required software	Version and level	Remarks
Windows	ServerView Operations Manager for Windows (Formerly, "ServerView Console for Windows")	V4.20.25 or later	This software is required to call the Web UI for the server management software from the RC Console. Refer to the information about settings for ServerView Operations Manager for Windows in the "ServerView Resource Coordinator VE Installation Guide".
		V5.10.03 or later	This software is required to call the console window for the server from the RC Console. Use a version of ServerView Operations Manager that supports calling of the server console window. If the console window is to be called, ServerView Operations Manager must be installed on the same machine as this product's manager. Also specify the IP address of the iRMC server when registering the monitored server in the ServerView Operations Manager.
	Microsoft(R) LAN Manager module	-	Download this software from the Microsoft FTP site. (*1)
	BACS or Intel PROSet or PRIMECLUSTER GLS for Windows	-	One of these software programs is required to make the admin LAN for the Admin Server redundant.
	ServerView RAID	-	This software is required when local disks (*2) use RAID configurations.
	VMware vCenter Server (Formerly, "VMware VirtualCenter")	4.0 4.1	[VMware] This software is required to manage VM guests and VM hosts. This software can either be placed on the same

Operating system type	Required software	Version and level	Remarks
			Admin Server as the Manager, or on a different server.
	SNMP Trap Service	-	-
	Microsoft(R) System Center Virtual Machine Manager 2008 R2	-	[Hyper-V] This software is required to manage VM guests and VM hosts. This software can either be placed on the same Admin Server as the Manager, or on a different server. It is also possible to create multiple library servers. Refer to "SCVMM Server MaxShellPerUser Settings " in "G.2.2 Pre-setup Preparations " in the "ServerView Resource Orchestrator Users' Guide " and specify settings so that up to six sessions can be controlled concurrently.
	Windows PowerShell	2.0	[Hyper-V] This software is required to manage VM guests and VM hosts.

[Managed Server Resource Agent]

Virtual environment	Required software	Version and level	Remarks
VMware	ServerView Agent for VMware	V4.30-20 or later	-
	ServerView RAID	-	This software is required when local disks (*2) use RAID configurations.
Hyper-V	ServerView Agent for Windows	V4.50.05 or later	-

*1: Download this software from the following Microsoft FTP site.

Microsoft FTP site

URL: <ftp://ftp.microsoft.com/bussys/clients/msclient/DSK3-1.EXE> (as of June 2011)

*2: "Local disks" include both internal disks for the server and storage blades.

[Business Server Agent]

Operating system type	Required software	Version and level	Remarks
Windows	VMware Tools	-	[VMware] This is necessary when the virtualization software is VMware.
Linux	sysstat package	-	This package is included in the installation media for the operating system.

[Admin Client]

Required software	Version and level	Remarks
Microsoft(R) Internet Explorer	7 8	-
Java(TM) 2 Runtime Environment Standard Edition	(*1)	This software is required to display the ServerView Operations Manager management window or the VM management window on the Admin Client.

Required software	Version and level	Remarks
VMware vSphere(TM) Client	4.0 4.1	[VMware] This software is required to use functions that link to the VM management product or the VMware for Managed Servers on the Admin Client.
Hyper-V Manager	-	[Hyper-V] This software is required to use functions that link to the Hyper-V for Managed Servers on the Admin Client. This software is not supported for Windows XP or Windows 2003.
Microsoft(R) System Center Virtual Machine Manager 2008 R2 Administrator Console	-	[Hyper-V] This software is required to use functions that link to VM management products on the Admin Client.
Adobe Flash Player	10	-
Adobe Reader	9	-

*1: To display the management window for ServerView Operations Manager, refer to the manuals for ServerView Operations Manager.

To display the VM management window, Version 1.5 or later is required.

[Web Client]

Required software	Version and level	Remarks
Microsoft(R) Internet Explorer	7 8	-
Adobe Flash Player	10	-
Adobe Reader	9	-

2.2.2.4 Conflicting software

This product cannot be used with the following products.

[Manager]

Operating system type	Item No.	Product name	Version and level	Remarks
Windows	1	INTERSTAGE	All versions	Here "INTERSTAGE" includes the following products: - INTERSTAGE - INTERSTAGE Standard Edition - INTERSTAGE Enterprise Edition
	2	Interstage Apcoordinator	All versions	-
	3	Interstage Application Server	All versions	Here "Interstage Application Server" includes the following products: - INTERSTAGE Application Server Standard Edition - INTERSTAGE Application Server Enterprise Edition

Operating system type	Item No.	Product name	Version and level	Remarks
				<ul style="list-style-type: none"> - INTERSTAGE Application Server Web-J Edition - Interstage Application Server Standard Edition - Interstage Application Server Standard-J Edition - Interstage Application Server Enterprise Edition - Interstage Application Server Plus - Interstage Application Server Plus Developer - Interstage Application Server Web-J Edition
	4	Interstage Apworks	All versions	-
	5	Interstage Business Application Server	All versions	<p>Here "Interstage Business Application Server" includes the following products:</p> <ul style="list-style-type: none"> - Interstage Business Application Server Standard Edition - Interstage Business Application Server Enterprise Edition
	6	Interstage Business Process Manager	All versions	-
	7	Interstage Business Process Manager Analytics	All versions	-
	8	Interstage BPM Flow	All versions	-
	9	Interstage Service Integrator	All versions	-
	10	Interstage Shunsaku Data Manager	All versions	-
	11	Interstage Studio	All versions	-
	12	Interstage Traffic Director	All versions	-
	13	INTERSTAGE WEBCOORDINATOR	All versions	-
	14	Systemwalker Centric Manager (x64)	All versions	<p>Here "Systemwalker Centric Manager" includes the following products:</p> <ul style="list-style-type: none"> - SystemWalker/CentricMGR - SystemWalker/CentricMGR-M - SystemWalker/CentricMGR GEE - SystemWalker/CentricMGR EE - SystemWalker/CentricMGR SE - Systemwalker Centric Manager Global Enterprise Edition - Systemwalker Centric Manager Enterprise Edition

Operating system type	Item No.	Product name	Version and level	Remarks
				- Systemwalker Centric Manager Standard Edition
	15	Systemwalker IT Change Manager	All versions	Here "Systemwalker IT Change Manager" includes the following products: <ul style="list-style-type: none"> - Systemwalker IT Change Manager Enterprise Edition - Systemwalker IT Change Manager Standard Edition
	16	Systemwalker IT Process Master	All versions	-
	17	Systemwalker Operation Manager	V13.3 or earlier	Here "Systemwalker Operation Manager" includes the following products: <ul style="list-style-type: none"> - SystemWalker/OperationMGR Global Enterprise Edition - SystemWalker/OperationMGR Enterprise Edition - SystemWalker/OperationMGR Standard Edition - SystemWalker OperationMGR Global Enterprise Edition - SystemWalker OperationMGR Enterprise Edition - SystemWalker OperationMGR Standard Edition - Systemwalker OperationMGR Global Enterprise Edition - Systemwalker OperationMGR Enterprise Edition - Systemwalker OperationMGR Standard Edition
	18	Systemwalker PKI Manager	All versions	-
	19	Securecrypto Library	All versions	-
	20	Systemwalker Resource Coordinator	All versions	Here "Systemwalker Resource Coordinator" includes the following products: <ul style="list-style-type: none"> - Systemwalker Resource Coordinator - Systemwalker Resource Coordinator Base Edition - Systemwalker Resource Coordinator Virtual server Edition
	21	Systemwalker Runbook Automation (Linked Server/Relay Server/Business Server)	All versions	-
	22	Systemwalker Service Quality Coordinator	All versions except V13.4.0	-

Operating system type	Item No.	Product name	Version and level	Remarks
	23	SystemcastWizard	All versions	-
	24	SystemcastWizard Professional	All versions	-
	25	SystemcastWizard Lite	All versions	-
	26	ServerView Installation Manager (*1)	All versions	-
	27	ServerView Resource Coordinator VE	All versions	-
	28	ServerView Resource Orchestrator	All versions	-
	29	TeamWARE Office Server	All versions	-
	30	TRADE MASTER	All versions	-

*1: Because the Manager for this product includes a PXE server, this product cannot be used with the PXE server that is required for ServerView Installation Manager remote installations.

Note

- The Admin Server for this product can manage ServerView Resource Coordinator VE V2.2 Agents. In this case, these Agents can be used within the functional range of ServerView Resource Coordinator VE.
- The Admin Server for this product cannot manage the same resources as the Admin Server for ServerView Resource Coordinator VE.

[Managed Server Resource Agent]

Virtual environment	Product name	Version and level	Remarks
VMware	-	-	-
Hyper-V	Server System Manager	All versions	-
	SystemcastWizard	All versions	-
	SystemcastWizard Professional	All versions	-
	SystemcastWizard Lite	All versions	-

[Business Server Agent]

Operating system type	Item No.	Product name	Version and level	Remarks
Windows	1	Systemwalker Runbook Automation (Management Server/Linked Server/Relay Server)	All versions	-
	2	Systemwalker Service Quality Coordinator	All versions except V13.4.0	-
	3	ETERNUS SF Disk Space Monitor	All versions	-
Linux	1	Systemwalker Runbook Automation (Management Server/Linked Server/Relay Server)	All versions	-
	2	Systemwalker Service Quality Coordinator	All versions except V13.4.0	-
	3	ETERNUS SF Disk Space Monitor	All versions	-

 Note

- The Admin Server for this product cannot manage the same resources as the Admin Server for ServerView Resource Coordinator VE.
- The Manager for this product includes a DHCP server function and a PXE server function. This means that other products or services with DHCP or PXE server functions should not be placed on the admin LAN.

Examples of products that include DHCP servers or PXE servers

- Windows Deployment Services (WDS) for Windows Server 2008
- Boot Information Negotiation Layer(BINLSVC)
- ServerStart (when the remote installation function is used).

Chapter 3 Installation and Uninstallation

This chapter explains how to install and uninstall this product.

3.1 Installing on the Admin Server

This section explains how to install the Manager on the Admin Server.

The procedure for installing and setting up the Manager is as follows:

1. Preparing for installation
2. Installing the required software
3. Installing the Manager
4. Registering users, groups and organizational units
5. Setup
6. Post-setup tasks

3.1.1 Preparing for Installation

Configuration of the target server for installation

This section explains how to create a new Admin Server. It explains the procedure for installing the Manager on a new server where only the operating system has been installed.

Before installing the Manager on an existing server, perform the procedure in "[Appendix C Preparations and Checks before Installation](#)".

Setting up the firewall

To install this product on an environment where a firewall function is being used, settings need to be specified so that the firewall function allows communications via the necessary ports.

Refer to the operating system manual for information on how to set up the firewall so as to allow communications to the necessary ports. Refer to "[D.1 List of Port Numbers](#)" for information on the ports used by this product. Connections must be allowed for "List of port numbers that need to receive packets from external servers".



The following note applies when the operating system is Windows Server 2008:

The Windows firewall function is enabled by default, and so firewall exceptions must be specified for the port numbers and protocols that are to be used.

Checking the host name

The host name must be specified in order for the Admin Server to run correctly. Either enter a host name in the "hosts" file using no more than 256 characters, or specify DNS settings so that the host name can be resolved.

Setting up the Hosts file

[Windows]

```
<System drive>\Windows\System32\drivers\etc\hosts
```



Note the following points when registering the local host in the "hosts" file.

When setting the local host name for "127.0.0.1", be sure to first enter an IP address that can be looked up remotely. Alternatively, do not set the local host name for "127.0.0.1".

In the following example, the host name "remote1" is set with "10.10.10.10" for the IP address.

```
10.10.10.10 remote01
127.0.0.1 remote01 localhost.localdomain localhost
```

Checking the SMTP server

This product uses an email function. Set up the SMTP server to create an environment where email can be used.

Checking the system time

Specify settings so that the Admin Server and the Managed Servers both use the same system time.

If the times are different, it will not be possible to display the correct values for usage statuses in the Operation Portal and the Cloud Portal.

Setting up a server virtualization software product

The settings differ depending on the server virtualization software product used.

If a server virtualization software product is used, refer to the article for the server virtualization software product being used under "Appendix G Configuring Server Virtualization Software" in the "ServerView Resource Orchestrator Users' Guide" for details.

Determining the storage configuration

Determine the storage configuration required for the system.

The following table shows the storage configurations supported by this product.

Table 3.1 Supported storage configurations

Server type	L-Server system disk	L-Server data disk
Vmware	Complies with the environment that can be used by VMware.	
Hyper-V	SAN storage	SAN storage

Setting up the storage environment

If a server virtualization software product is used, refer to the article for the server virtualization software product being used under "Appendix G Configuring Server Virtualization Software" in the "ServerView Resource Orchestrator Users' Guide" for details.

Setting up the network environment

To ensure security during operations, the following networks must be created in such a way that they are physically separated.

Refer to the article for network configurations in the "ServerView Resource Coordinator VE Installation Guide" for information on how to determine the network configuration.

- Admin LAN

Connect to admin LAN when performing management tasks such as installing or maintaining L-Servers, or performing operations on the Manager.

Systems can be operated with greater safety by setting up the operating system firewall function or installing a firewall on the admin LAN in accordance with the port list in the "ServerView Resource Coordinator VE Installation Guide".

- Public LAN

The public LAN is a network that general users connect to when using business applications and so on.

The following VLAN IDs are automatically set by this product in order to prevent L-Servers that perform independent jobs from connecting to one another:

- The VLAN ID for the internal port of the LAN switch blade (for blade servers)
The VLAN ID for external ports must be set in advance.
- The VLAN ID for the virtual switch

3.1.2 Installing the Required Software

Install the software indicated in "[2.2.2.3 Required software](#)" on the Admin Server.

The following sections explain the settings where care is required with some of the required software programs.

3.1.2.1 Downloading and Setting Up the Required Software

- Download and extract the Microsoft LAN Manager module

Download the Microsoft LAN Manager module from the following FTP site:

URL: <ftp://ftp.microsoft.com/bussys/clients/msclient/dsk3-1.exe> (as of June 2011)

[Windows]

After downloading the module, place the module in a work folder for the system where the module will be installed (such as "C:\temp") and then extract the module.

The Microsoft LAN Manager module can be installed even if it is not extracted first.

The module is for x86 CPU architecture. The module cannot be extracted on systems that use x64 CPU architecture. To extract the module, it must be extracted on a system with x86 CPU architecture.

Use the following method to extract the module.



Example

When dsk3-1.exe is placed in C:\temp

```
> cd /d c:\temp <RETURN>
> dsk3-1.exe <RETURN>
> Expand c:\temp\protman.do_ /r <RETURN>
> Expand c:\temp\protman.ex_ /r <RETURN>
```

After the module has been extracted, transfer the following files to a work folder on the machine where the module will be installed. Use upper-case for the names of the files that have been transferred.

- PROTMAN.DOS
- PROTMAN.EXE
- NETBIND.COM

Setting up the software required for Windows [Windows]

- ServerView Operations Manager 4.x for Windows Settings

In order for Resource Orchestrator to operate correctly, ensure that the following settings are made when installing ServerView Operations Manager for Windows.

- Do not select **IIS (Microsoft Internet Information Server)** for Web Server selection.

For details on how to configure the settings, refer to the ServerView Operations Manager 4.X for Windows manual.

- SNMP Service Settings

In order for Resource Orchestrator to operate correctly, the following settings for the standard Windows **SNMP trap service** are required.

Open *Service* from [Administrative Tools] on the Windows [Control Panel], and configure the following settings on the *security tab* of *SNMP service* in the [Services] window.

- SNMP community name
- Trap community name
- Community privileges
- SNMP trap destination
- SNMP Trap Service Settings

In order for Resource Orchestrator to operate correctly, the following settings for the standard Windows SNMP trap service are required.

- Open *Services* from [Administrative Tools] on the Windows [Control Panel], and then configure the startup type of *SNMP Trap service* as *Manual* on the [Services] window. Set the service status to *Started*.
- DHCP server installation

Installation of the Windows standard DHCP Server is necessary when managed servers belonging to different subnets from the admin server are to be managed. Install the DHCP Server following the procedure below:

1. Add DHCP Server to the server roles. For the addition settings, refer to the manual for Windows.
2. Open *Services* from [Administrative Tools] on the Windows [Control Panel], and then configure the startup type of DHCP Server service as *Manual* on the [Services] window.
3. From the [Services] window, stop the DHCP Server service. When an admin server is a member of a domain, perform 4.
4. Authorize DHCP servers.
 - a. Open DHCP from [Administrative Tools] from the Windows [Control Panel], and then select [Action] - [Managed authorized servers] from DHCP.
The [Manage Authorized Servers] window will be displayed.
 - b. Click <Authorize> on the [Manage Authorized Servers] window.
The [Authorize DHCP Server] window will be displayed.
 - c. Enter the admin IP address of the admin server in *Name or IP address* and click <OK>.
The [Confirm Authorization] window will be displayed.
 - d. Check the *Name* and *IP address*, and click <OK>.
The server will be displayed in the *Authorized DHCP servers* of the [Manage Authorized Servers] window.

3.1.3 Installing the Manager

To install the Manager, design and check the following parameters in advance.

Default values are listed for some of the parameters in the following table ("Parameters specified during installation"). For these parameters, it is recommended that the default values be used.

Parameters specified during installation

[Windows]

Item No.	Window	Input item	Description
1	Select the installation folder.	Installation Folder	This is the installation folder for this product. (*1) Default value: C:\Fujitsu The installation folder must be specified using no more than 10 characters long, including the driver letter and the "\" symbol.

Item No.	Window	Input item	Description
2	Administrative User Creation	User Account	This is the name of the user account for logging into this product as a privileged user. The string should be no more than 16 characters long, where the first character must be a letter and the remaining characters can consist of alphanumeric characters, underscores ("_"), hyphens ("-") or periods ("."). The value is case-sensitive.
		Password	This is the password for the privileged user.
		(Retype password)	This is a string consisting of no more than 16 alphanumeric characters and symbols.
3	Admin LAN Selection	Network to use the admin LAN	This is the network to be used as admin LAN. This network can be selected from a list box.
4	Admin LAN Selection	Folder containing the LAN Manager module	This is the folder that was expanded in "Download and extract the Microsoft LAN Manager" under "Downloading and Setting up the Required Software".
5	Port number setting	The port number of the namangement function	This is the port number used by the management function of this product. Default value: 8013
		The port number of the database	This is the port number of the database for this product. Default value: 5438
6	Environment settings for mailing function	Host name or IP address for SMTP server	This is the host name or IP address that was verified in " Checking the SMTP server ".
		Port number for SMTP server	This is the port number of the SMTP server. Default value: 25
		Sender address	This is the sender email address (the "from" address) when email is sent.
7	Port number setting	Interstage Management Console	This is the port number of the Interstage Management Console. Default value: 12000
		Web server (Interstage HTTP Server)	This is the port number of the Web server. Default value: 80
		CORBA Service	This is the port number of the CORBA Service used by this product. Default value: 8002
8	Select the installation folder for CMDB.	Installation folder for CMDB Manager database	This is the installation folder for the CMDB of this product. Default value: C:\Fujitsu\Systemwalker\CMDB
9	Setting user password	User password /	This is the password for the user ("swrbadbuser") that is required to start Job Execution Control. (*2)
		(Retype Password)	
10	Setting user password	User password	This is the password for the user ("swrbajobuser") that is required to start the process management database. (*2)
		(Retype Password)	
11	Admin server settings	FQDN for the admin server	This is the host name that was verified in " Checking the host name ".
12	Portal server settings	Port number of the cloud portal server	This is the port number of the portal server used by this product.

Item No.	Window	Input item	Description
			Default value: 3500
13	Database settings	Port number of the database for user management	This is the port number of the user management database for this product. Default value: 5440
		Port number of the database for access control	This is the port number of the access control database for this product. Default value: 5439
		Port number of the database for accounting	This is the port number of the accounting database for this product. Default value: 5441
		Port number of the database dashboard	This is the port number of the database for the cloud infrastructure administrator dashboard. Default value: 5442
14	Interstage single sign-on SSO repository settings	FQDN of the SSO repository server	This is the FQDN of the SSO repository used by Interstage Single Sign-On. For the FQDN of the SSO repository, use the FQDN of the Admin Server. The FQDN must be no more than 256 characters long, and it must be possible to resolve the name.
		Port number of the SSO repository server	This is the port number of the SSO repository. Default value: 389
		Administrator's DN of the SSO repository server	This is the administrator DN of the SSO repository. Default value: cn=manager,ou=interstage,o=fujitsu,dc=com
		Administrator's password for the SSO repository	The password for the administrator DN of the SSO repository must be no more than 128 characters, including alphanumeric characters, commas (","), plus signs ("+") or equals signs ("=").
		(Retype password)	
15	Authentication server settings	FQDN of the authentication server	This is the FQDN of the authentication server used by this product. For the FQDN of the authentication server, use the FQDN of the Admin Server. The FQDN must be no more than 256 characters long, and it must be possible to resolve the name.
		Port number of the authentication server	This is the port number of the authentication server. Default value: 10443
16	User management settings	Enable user management by user department - on - off	If user management is to be performed by the user department, select "on". If user management is to be performed by the provider department administrator, select "off".
17	MyPortal settings	Allow the service specification modification	This checkbox must be selected if changes to the service specifications are allowed.
18	MyPortal settings	Enable application process	This checkbox must be selected if application processes are enabled.
19	MyPortal settings	Application process to be used	When Application process is enabled, a window is displayed to select the application to be used.

Item No.	Window	Input item	Description
			Select the required checkbox to use the following application processes: <ul style="list-style-type: none"> - Default (Approver and Judge) - ApproverOnly - JudgeOnly Initial value: Default
20	MyPortal settings	Select the application process settings.	After the above window, another window appears. Select the checkbox to choose the timing of the application process: <ul style="list-style-type: none"> - Use the application process subscribing to the service - Use the application process canceling the subscription - Use the application process modifying the service specification (This selection is only displayed in the windows if the "17.MyPortal settings" has been selected.)
21	CMDB and Interstage Bussiness Process Manager Analytics settings	Port number of CMDB and BPM-A	This is the port number of Interstage Business Process Analytics and the CMDB used by this product. Default value: 80
22	Virtualization software settings	Type of virtualization software <ul style="list-style-type: none"> - Hyper-V - VMware - Hyper-V + VMware 	This is the virtualization software that is installed on Managed Servers. A checkbox for virtualization software must be selected according to the environment used.

*1: Install the Manager on an NTFS format disk.

*2: Password settings for "swrbajobuser" and "swrbaduser"

- An error will occur with the installation processing if either "swrbajobuser" or "swrbaduser" (or both) have been registered already. In this case, delete the user(s) that caused the error (either "swrbajobuser" or "swrbaduser" or both), and then perform the installation again.
- The strings that can be specified for passwords must start with a letter or number and be between 1 and 250 characters long. Also, the following characters cannot be used in passwords:
 - \ (backslash)
 - " (double quote)
 - Spaces
 - Tab character.
- Depending on the security policy settings for the operating system, a certain degree of complexity may be demanded for the strings that can be used as passwords. With the default settings for Windows 2008, in particular, a fairly high degree of complexity is demanded for the strings that can be used as passwords.
Specify a password, taking the following rules into account:
 - The password must not contain all or part of the user name ("swrbajobuser" or "swrbadbuser").
 - The password must contain at least one letter, at least one number and at least one symbol
 - Passwords must be at least eight characters long.

*3: To adopt the default value, simply press the <Enter> key without entering any values.

3.1.3.1 Installing on Windows systems [Windows]

Cautions Prior to Installing

- If a terminal server is installed, execute the following command to change the terminal service to install mode:

```
CHANGE USER /INSTALL
```

Installation

Use the following procedure to install the Manager.

1. Log in with Administrator privileges.
2. Start the installer.
The installer will start automatically when the DVD-ROM(DISK1) is inserted in the DVD drive. If the installer does not start automatically, start it manually by executing *cimssetup.exe*.
3. Click "**Installation of Admin Serevr function**".
Thereafter, proceed with the installation by entering the parameters that were designed and verified in "[Parameters specified during installation](#)" as appropriate, in accordance with the instructions displayed in the installation wizard.
4. When prompted, insert the DVD-ROM(DISK2) or the DVD-ROM(DISK3) to DVD drive to proceed 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 the product again.

Notes on the Post-installation Procedure

- If a terminal server is installed, execute the following command to change the terminal service to execute mode:

```
CHANGE USER /EXECUTE
```

- The following user is added:

User name	swrbadbuser
-----------	-------------

swrbadbuser is the OS account used to start the process management database service. Do not delete this account while CIMS is still installed.

3.1.4 Setup

This section explains how to set up the Manager.

3.1.4.1 Creating and Setting up Interstage Single Sign-On Environments

When registering users to the Interstage Single Sign-on authentication infrastructure, refer to "[F.1 Creating and Setting up Interstage Single Sign-On Environments](#)" for information on how to first create and set up the Interstage Single Sign-on environment.



See

Refer to the "Interstage Application Server Single sign-on Operator's Guide" for details on Interstage Single Sign-On.

3.1.4.2 Registering Users, Groups and Organizational Units

Register the organizational units and users that are required to use this product. Register these organizational units and users with either the authentication infrastructure or an LDAP environment. Register user information according to the directory service being used.

Note

- The step where users, groups and organizational units are registered with the LDAP directory only needs to be performed for the initial setup after installation. This step is not required when the setup is canceled and then performed again.
- There is no need to create organizational units if operations are to be performed using organizational units that have already been created.
- The users and groups created in this chapter are the users and groups that are required for Cloud Infrastructure Management Software to run. Be sure to create these users and groups.
- It is not recommended to create LDIF files by copying samples from this manual. This is because linefeed characters may be skipped or duplicated, depending on the Web browser or display program being used. It is recommended that you use the samples in accordance with the procedures in this manual.

If you have to copy the samples from this manual for particular reasons, carefully check to see that the linefeed characters appear exactly as shown in this manual before creating LDIF files.

3.1.4.2.1 Registering User Information with the Interstage Directory Service

This section explains the procedure for registering users with the Interstage Directory Service.

It explains how to register users by using LDIF files, as one of the user registration methods.

Note

Refer to the "Interstage Application Server Directory Service Operator's Guide" for details on LDIF files.

Information

User information can also be registered by using the GUI-based "Entry Management Tool". Refer to the "Interstage Application Server Directory Service Operator's Guide" for details.

Registering users for service providers (automatic operation function)

Location of sample LDIF files

Sample LDIF files are stored in the following location.

[Windows]

```
<CIMS installation folder>\Systemwalker\swrbam\etc\sample\ldif
```

LDIF file	Description
swrba_sso_sample.ldif	This LDIF file creates organizational units, users and groups, and adds users to groups. Use this sample file if the Interstage Single Sign-On authentication infrastructure is used.
swrba_no_sso_sample.ldif	This LDIF file creates organizational units, users and groups, and adds users to groups. Use this sample file if the Interstage Single Sign-On authentication infrastructure is not used.

The definitions in the sample file and how to edit them

This sample file assumes the following LDAP configuration.

Edit this sample file to match the LDAP environment for the actual operation. Be sure to change the password for the process control user.

Public directory	Note: The value is fixed as below. ou=interstage,o=fujitsu,dc=com
Organizational unit for storing users	ou=User
Organizational unit for storing groups	ou=Group
Process control user	swrbaadmin
Password for the process control user	systemwalker#1

How to register sample files

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

 Example

Administrator DN: cn=manager

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

Password for the administrator DN: password

Host name of the repository: The host name of the Admin Server (Interstage Directory Service)

Port number: 389

[Windows]

```
> ldapmodify -H ldap://< }Host name of the Admin Server>:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f <Name of the edited LDIF file>
```

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 files

This section explains how to create LDIF files to register the user information (shown below) with the LDAP directory.

Note that three separate LDIF files are created here, but it is also possible to group all three files into a single LDIF file and register that file with the LDAP directory.

LDIF file for creating organizational units

This section explains the definitions for registering the organizational units shown in the following table with the LDAP directory.

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.

Create an LDIF file to register organizational units according to the setting examples.

Example 1: Using "User" as a group for managing users.

The "User" group is created automatically when the repository is created.

To use the "User" group as the group for managing users, prepare an LDIF file that registers only "Group", as follows:

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

Example 2: Using a group other than "User" as a group for managing users.

To use a group with a name other than "User" as the group for managing users, prepare an LDIF file that registers two groups (a group for managing groups and a group for managing users) as follows:

```
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 table below.

List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	Public directory: 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.

 **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

This section explains the definitions for registering the users shown in the following table with the LDAP directory.

User name	Password	Description
swrbaadmin (*1)	systemwalker#1 (*2)	This user is required for Cloud Infrastructure Management Software to control processes internally. (Mandatory user.)

***1:** This is the recommended user name, but any name can be specified.

***2:** "systemwalker#1" is the default value. This password can be changed to any password.

Create an LDIF file to register users according to the setting example.

Settings example

```
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

```

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

List of replacement elements

Replacement symbol	Setting after replacement
%DOMAIN%	Public directory: 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 has been changed, specify the new name.) Example: User. Note: To execute the setup after creating an LDAP directory, specify ou=< Value of %USER%> for the organizational unit settings for storing the LDAP user account when the setup is executed.

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

This section explains the definitions for registering the groups shown in the following table.

Group name	Members
AdminRole(*1)	- swrbaadmin
IflowUsers	- swrbaadmin
IflowGroups(*1)	- AdminRole - swrba_Exe - Role
swrba_Exe(*1)	- swrbaadmin
Role(*1)	- swrbaadmin

***1:** These are the recommended group names. Arbitrary prefixes can be added to the front of the group names, without actually changing the group name itself.

Note

Do not assign users other than the swrbaadmin user to the swrba_Exe group.

Otherwise, problems may occur with the behavior of Automated Operation Processes.

Create an LDIF file for registering groups and adding users in accordance with the setting example below.

Setting example

```

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

dn: cn=IflowUsers,ou=%GROUP%,%DOMAIN%
changetype: add
objectclass: groupOfNames
objectclass: top
cn: IflowUsers
member: uid=swrbaadmin ,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 table 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 has been changed, specify the new name.) Example: User. Note: To execute the setup after creating an LDAP directory, ou=< Value of %USER %> must be specified for the organizational unit settings for storing the LDAP user account when the setup is executed.
%GROUP%	The "Group" organizational unit (OU) (If the name of the OU has been changed, specify the new name.) Example: Group.

Replacement symbol	Setting after replacement
	Note: To execute the setup after creating an LDAP directory, ou=< Value of %GROUP %> must be specified for the LDAP organizational unit settings when the setup is executed.

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".

The following example shows how to register entry data using the ldapmodify command and an LDIF file.

Example

Administrator DN: cn=manager

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

Password for the administrator DN: password

Host name of the repository: The host name of the Admin Server (Interstage Directory Service)

Port number: 389

[Windows]

```
> ldapmodify -H ldap://<Host name of the Admin Server>:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -w password -a -f <Name of the created LDIF file>
```

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

3.1.4.2.2 Registering users for service providers (configuration management function)

Registering the required organizational unit

Register the following organizational unit user (required to use this product) with the Interstage Directory Service.

Organizational unit	Parent object
Operators	User

1. Prepare the following LDIF file.

```
dn: ou=Operators, ou=User, ou=interstage, o=fujitsu, dc=com (*1)
changetype: add
objectClass: organizationalUnit
ou: Operators
```

*1: For the underlined section, make changes according to the domain name specified in the public directory for the repository created in "F.1 Creating and Setting up Interstage Single Sign-On Environments".

2. Open a command prompt with Administrator privileges.
3. Register the organizational unit by executing the following command.

[Windows]

```
> ldapmodify -H ldap://<Host name of the Admin Server>:389 -D "<Administrator DN>" -w
<Password for the administrator DN> -a -f <Name of the created LDIF file>
```

Registering the required user

Register the following user (required to use this product) with the Interstage Directory Service.

User ID	Role	Organization name	Password
cfmgadm	System administrator	cfmgadm	Required

1. Prepare the following LDIF file.

```
dn: cn=cfmgadm, ou=Operators, ou=User, ou=interstage, o=fujitsu, dc=com (*1)
changetype: add
objectClass: ssoUser
objectClass: inetOrgPerson
cn: cfmgadm
sn: cfmgadm
uid: cfmgadm
userPassword: <Password>
ssoRoleName: CFMGSystemAdmin
mail: <Email address>
```

*1: For the underlined section, make changes according to the domain name specified in the public directory for the repository created in "F.1 Creating and Setting up Interstage Single Sign-On Environments".

2. Open a command prompt with Administrator privileges.
3. Register the user by executing the following command.

[Windows]

```
> ldapmodify -H ldap://<Host name of the Admin Server>:389 -D "<Administrator DN>" -w
<Password for the administrator DN> -a -f <Name of the created LDIF file>
```

3.1.4.2.3 Registering users for service providers (Self Service Portal)

Authentication for the Operation Portal is performed using Interstage Single Sign-On. Provider department administrators who will use the Operation Portal must be registered with the repository for Interstage Single Sign-On using an LDIF file. Use the following procedure to register provider department administrators.

1. Create provider department administrators.
2. Add provider department administrators as members of the "IflowUsers" group.



Provider department administrators who have not been registered in the "IflowUsers" group cannot conduct assessment in application processes.

Also, if no provider department administrators have been registered in the "IflowUsers" group, the following error message will be displayed after users forward applications from the forward destination selection window when they apply to use a service.

```
PCS1002
An error occurred while processing application.
Please contact the system operation manager
```

Each of these registration procedures is explained below.

Creating provider department administrators

The procedure for creating provider department administrators is as follows:

1. Create an LDIF file

Create an LDIF file by editing a sample LDIF file. A sample LDIF file is shown below.

```
# Entry: User: ctmg_provider001
dn: cn=ctmg_provider001,ou=Operators,ou=User,ou=interstage,o=fujitsu,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: ssoUser
uid: ctmg_provider001
userPassword: ctmg_provider001
mail: ctmgprovider001@example.com
ssoRoleName: CTMGProviderAdmin
ssoAuthType: basicAuth
sn: 001
givenName: provider
cn: ctmg_provider001
```

2. Execute the ldapmodify command

[Windows]

Execute the ldapmodify command specifying the LDIF file that has been created.

```
> ldapmodify -H ldap://<Host name of the Admin Server>:389 -D "<Administrator DN>" -w
<Password for the administrator DN> -a -f <Name of the created LDIF file>
```

An execution example is shown below.

```
c:\> ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w
admin -a -f c:\ldif\adduser.ldif
adding new entry "cn=ctmg_provider001,ou=Operators,ou=User,ou=interstage,o=fujitsu,dc=com"
```



Note

Enter the command on a single line without inserting any line breaks midway through.

For the host name of the Interstage Directory Service, the port number, the administrator DN, and the password for the administrator DN, enter the values that were specified during installation. Refer to the "Systemwalker Service Catalog Manager V14g Installation Guide" for details.

Adding provider department administrators to the "IflowUsers" group

Use the following procedure to add provider department administrators as members of the "IflowUsers" group.

1. Create an LDIF file

Create an LDIF file by editing a sample LDIF file. A sample LDIF file is shown below.

```
# Add ctmg_provider001 to IflowUsers
dn: cn=IflowUsers,ou=group,ou=interstage,o=fujitsu,dc=com
changetype: modify
add: member
member: cn=ctmg_provider001,ou=Operators,ou=User,ou=interstage,o=fujitsu,dc=com
```

2. Execute the ldapmodify command

[Windows]

Execute the ldapmodify command specifying the LDIF file that has been created.

```
> ldapmodify -H ldap://<Host name of the Admin Server>:389 -D "<Administrator DN>" -w
<Password for the administrator DN> -f <Name of the created LDIF file>
```

An execution example is shown below.

```
c:\> ldapmodify -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -w
admin -f c:\ldif\adduser2group.ldif
modifying entry "cn=IflowUsers,ou=group,ou=interstage,o=fujitsu,dc=com"
```

Note

Enter the command on a single line without inserting any line breaks midway through.

For the host name of the Interstage Directory Service, the port number, the administrator DN, and the password for the administrator DN, enter the values that were specified during installation. Refer to the "Systemwalker Service Catalog Manager V14g Installation Guide" for details.

3.1.4.3 Setting up the Connection to the LDAP Server

Set up the connection to the LDAP server by checking and modifying the content of the following file.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWCFMG\config\vsys_config.xml
```

Check the following properties, and make modifications if necessary.

Property	Value	Can this be omitted?	Default value
ldap-server	Host name of the directory server	No	ldap://localhost:389
ldap-admin-password	Password for the administrator DN specified in " F.1 Creating and Setting up Interstage Single Sign-On Environments "	No	(Blank)

3.1.4.4 Setting up the CMDB

Use the following procedure to set up the CMDB.

1. Stop the CMDB.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbstop.bat
```

1. Set up the CMDB.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbsetupenv.bat -k MGR
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbsetupenv.bat -k
AGT_CFMG
```

1. Start the CMDB.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbstart.bat
```

3.1.4.5 The User Allowed to Access the Database

The user (cfmgdb) and group (cfmgdb) for starting the database process are added during installation.

Use this user to access and manage the database.



Do not delete this user while this product is being used.

Changing the password

The following password is registered immediately after installation:

```
cfmg14db! (for Windows)
```

Because it is insecure to use the default password, use the following procedure to change the password.

[Windows]

How to Change the Operating System User Password

Change the password using the following procedure:

1. Select **[Start] - [Control Panel]** to open **[Control Panel]**.
2. Click **User Accounts**.
3. Click **Manage another account**.
4. Click the **cfmgdb** user.
5. Click **Reset the password**.
6. Enter the new password, and then click the **<OK>** button.
Alternatively, set it on the command line as follows:

```
> net user cfmgdb <New password>
```

How to Change the Service Setup Password

The database service is started as the DB startup user (cfmgdb).

Upon starting the login password is required, which is set to service.

When the DB startup user (cfmgdb) password is changed, the service settings must also be changed. Use the following procedure:

1. Select **[Start] - [Control Panel] - [Administrative Tools]**, then open **[Services]**.
2. Select **Systemwalker Software Configuration Manager DB Service** from the list of services, then open that property.
3. Click the **[Log on]** tab.
4. In **[Password]** and **[Confirm password]** fields, set a string that matches the password set in "How to Change the Operating System User Password", and then click the **<OK>** button.
5. This password will be effective the next time the service is started.

3.1.4.6 Setting up the Automatic Operation Function [Windows]

1. Log in to the Admin Server as a user with Administrator privileges.
2. Execute the following command to start the setup:

```
> <CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_setup -s
```



If the operating system is Windows Server 2008, execute the command above as an administrator.

3. The setup tool for the automatic operation function will start.

Check the settings that are 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 Admin Server from the following options: - Standalone Server (normal operations)

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. 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
Type of The Authentication Server to Use	Specify the type of the authentication server to be used. - Interstage Single Sign-On Authentication Server
LDAP Used	Specify the type of LDAP directory to be used. - Interstage Directory Service
Interstage Single Sign-On environment setting Business system name	Specify the business system name of the Interstage Single Sign-On environment. default: 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	Specify the public directory. Note: The value is fixed as below. ou=interstage,o=fujitsu,dc=com  Note Separate public directory levels with commas(.). Example: If the public directory is ou=interstage,o=fujitsu,dc=com itm.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 LDAP repository administrator. Format: cn=<Administrator DN> Note: The value is fixed as below. cn=manager
Password for Administrator DN	Specify the password for the LDAP repository administrator.

 **Note**

.....
After performing the procedure above, check whether this user can authenticate with the LDAP server.

If the LDAP authentication test fails, an error message will be displayed. In this case, review the settings.
.....

8. Set up user information.

Enter each setting, and then click the <Next> button.

Item name	Input value
User for Process Control	Specify the user that is required for Cloud Infrastructure Management Software to control processes internally. "swrbaadmin" is the recommended value, but any value can be specified. This user must have been registered in the LDAP directory beforehand.
Password for the User for Process Control	Specify the password for the user for process control.

Note

After performing the procedure above, check whether this user can authenticate with the LDAP server.

If the LDAP authentication test fails, an error message will be displayed. In this case, review the settings. Check the following as well:

- There may be a problem with the settings for the LDAP server, so return to the previous window and check whether the information has been set up correctly.
- Check for any problems with the user or group information registered with the LDAP server.

9. The settings will be displayed.

Check that the displayed values are correct, and then click the **<Next>** button. The setup will commence.

10. A window will be displayed indicating the setup progress.

11. 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 command for the automatic operation function fails for any reason, be sure to cancel the setup.

3.1.4.7 Registering the Mail Server

To send email notifications when tasks are allocated during operations that use Automated Operation Processes, mail server information must be registered on the Admin Server.

Note

- In the initial state following the setup, the automatic operation function runs on the assumption that a mail server has been created on the Admin Server. Email notifications will not be performed if a mail server has not been created on the Admin Server.

List of setting items

The following table lists the items that can be set up as mail server information.

Item name	Description	Default value
SMTPServerHost	Specify the host name or IP address of the SMTP server that is used to send emails.	Localhost
SMTPServerPort	Specify the port number of the SMTP server that is used to send emails.	25
SMTPUserName	Specify the user name that is used to authenticate with the SMTP server when emails are sent. If the user name is not to authenticate with the SMTP server when emails are sent, specify " " (the backslash character followed by a space).	None
SMTPPassword	Specify the password for the user that is used to authenticate with the SMTP server when emails are sent. If the user name is not to authenticate with the SMTP server when emails are sent, specify " " (the backslash character followed by a space).	None

ServerEmailAddress	Specify the email address that is assigned as the "sender" (the "from" address). Note that the email address specified by this item will also be the destination for emails that are returned when the destination is unknown. Specify the address of a person who can rapidly respond to problems.	postmaster@example.com
ServerEmailBaseURL	Specify the URL of the Admin Server (which will appear in emails) using the following format: - http://<Host name of the Admin Server>:<80 (Port number of the Web server)>/console/ Be sure to specify a URL that can be accessed externally. For environments that use Interstage Single Sign-On, in particular, be sure to specify the host name in FQDN format.	http://< Host name of the Admin Server>:<80 (Port number of the Web server)>/console/

Setup procedure

Log in as a system administrator and register mail server information on the Admin Server using the following procedure.

It is recommended that a backup be taken before you perform this procedure, in case something goes wrong.

1. Check the startup status of the automatic operation function.

Use the `swrba_status` command to check the startup status of the automatic operation function. If the automatic operation function is not running, start it using the `swrba_start` command.

2. To authenticate with the SMTP server when emails are sent, encrypt the password for the user that is used to authenticate with the SMTP server. Use the following command to encrypt the password.

This step can be skipped if authentication with the SMTP server is not performed when email is sent.

[Windows]

```
> <CIMS installation folder>\Systemwalker\IBPM\client\samples\configuration
\EncryptPassword.bat -e "<Password>"
-----ENCRYPTED PASSWORD-----
<Encrypted password>
```

3. Prepare a mail server definition file and a mail sender definition file.

Create the following two types of file. These files can be created in any desired location.

- a. SMTP server configuration file (`smtpserver.conf`)

Sample configuration file for authenticating with the SMTP server when email is 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/
```

Sample configuration file for not authenticating with the SMTP server when email is 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: Be sure to insert a space after the backslash character("\ ").

- b. Mail sender configuration file (emailaddress.conf)

```
ServerEmailAddress=swrbamailuser@swrba.mail.server
```

4. Register the information for the mail server and the mail sender with the automatic operation function. Register the mail server definition and the mail sender definition.

- a. Register the SMTP server.

[Windows]

```
> <CIMS installation folder>\Systemwalker\IBPM\server\deployment\bin  
\importProperties.bat smtpserver.conf <Account for accessing the process management  
database> <Password for the account for accessing the process management database>
```

- b. Register the mail sender.

[Windows]

```
> <CIMS installation folder>\Systemwalker\IBPM\server\deployment\bin  
\importProperties.bat emailaddress.conf <Account for accessing the process management  
database> <Password for the account for accessing the process management database> Default
```

Be sure to specify the "Default" option at the end.

5. Restart the automatic operation function.

To reflect the information that has been set up, first use the swrba_stop command to stop the automatic operation function, and then use the swrba_start command to start it.

- a. Stop the automatic operation function.

[Windows]

```
> <CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_stop
```

- b. Start the automatic operation function.

[Windows]

```
> <CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_start
```

3.1.4.8 Setting up the Catalog Function

This section explains how to set up the catalog function.

1. Log in to the Admin Server as a superuser.
2. Execute the following command to start the setup for the automatic operation function.

[Windows]

```
> <CIMS installation folder>\Systemwalker\SWCTMG\bin\setup\swctmg_service_setup /s
```

3.1.4.9 Tuning the Desktop Heap [Windows]

Use the following procedure to tune the desktop heap.



Note

- Edit the registry as a user with Administrator privileges.
- When editing the registry, be sure to take a backup first, and be very careful when making the changes.

- If the value of the SharedSection registry key has been changed, restart the system for the changes to take effect.

1. Open the registry editor.

Select **[Run]** from the **[Start]** menu. Enter "regedt32", and then click the **<OK>** button.

2. Move to the SubSystems key.

Move to the following key from the **HKEY_LOCAL_MACHINE** subtree.

```
\System\CurrentControlSet\Control\Session Manager\SubSystems
```

3. Select the value for the **[Windows]** key.

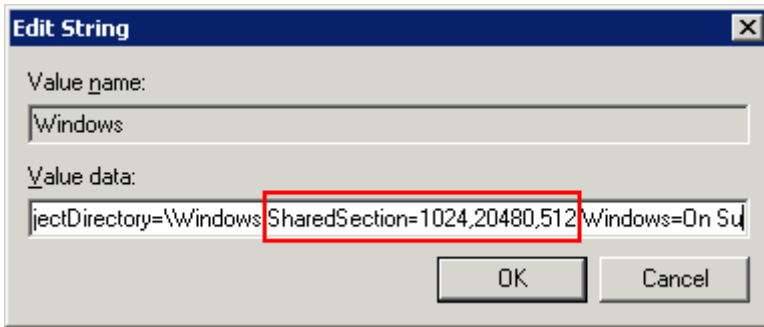
4. Select **[Modify]** from the **[Edit]** menu to display the **[Edit String]** dialog box.

5. Increase the desktop heap by changing the value of the SharedSection parameter.

Increase the value of the third item ("zzzz") to 3072.

```
SharedSection=xxxx,yyy,zzzz
```

Note: There is no need to change the first and second values ("xxxx" and "yyyy").



- Example: Before change.

```
SharedSection=1024,20480,512
```

- Example: After change.

```
SharedSection=1024,20480,3072
```

Information

For details on how to expand the desktop heap by modifying the registry, refer to document number 126962 on the "Microsoft Support Online" website published by Microsoft for details. Refer to Article 184802 on the Microsoft Support website for information on the desktop heap.

3.1.4.10 Restarting the Operating System

Restart the operating system.

[Windows]

Restart the operating system from the **Start** menu.

3.1.5 Post-setup Tasks

This section explains the tasks to be performed after the Manager has been set up.

After setting up the Manager, perform the following tasks:

1. Starting the Web servers
2. Setting up mail and accounting information
3. Setting up information for Interstage Single Sign-On
4. Registering application processes

3.1.5.1 Starting the Web Servers

Start the Web servers for Interstage Application Server.

Use the following procedure to start the Web servers.

1. Start the Interstage Management Console.
Use the following procedure to start the Interstage Management Console.

[Windows]

Select the [All Programs] - [Interstage] - [Application Server], and then [Interstage Management Console] from the [Start] menu.

2. Start the Web servers.

Select [Interstage Management Console] - [Interstage Application Server] - [System] - [Service] - [Web Server] - [List].

If any of the following Web servers have stopped, start them.

- FJapache
- ctmg-http-int
- ctmg-https-ext

3.1.5.2 Setting up Mail and Accounting Information

This section explains how to set up mail and accounting information.

Mail settings

The operating environment files for this product must be modified in order to send emails to users in the user departments to notify that processing has completed or failed when they use MyPortal to apply to use a service, change service specifications or cancel a service contract.

The following operating environment files need to be modified:

- vsys_config.xml
- mail_config.xml

These two files are stored on the server where this product has been installed. The modification procedure is explained below.

Setting up the "vsys_config.xml" file

1. Open the following operating environment file.

[Windows]

<CIMS installation folder>\Systemwalker\SWCFMG\config\vsys_config.xml

2. Set the following items in the operating environment file.

Item	Description
ctmg-host	Specify the FQDN for the server where this product has been installed.
ctmg-port	Specify the port number of the API for linking to this product (fixed as 3551).

A setting example is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
  <entry key="super-org-id">cfmgadm</entry>
  ... (Omitted) ...
  <entry key="ctmg-host">aaa.bbb.fujitsu.co.jp</entry>
  <entry key="ctmg-port">3551</entry>
  <entry key="mail-config-file">/etc/opt/FJSVcfmg/config/mail_config.xml</entry>
  <entry key="locale">ja</entry>
</properties>
```

Note

- When editing the "vsys_config.xml" file, do not change any settings other than ctmg-host and ctmg-port.
- Back up the "vsys_config.xml" file before editing it. If any settings other than ctmg-host and ctmg-port have been changed, restore the file from the backup.

Specifying settings in "mail_config.xml"

If environment setup for the mail transmission function was not performed when this product was installed, the host name (or IP address), port number and email address that were entered with the mail settings specified during installation on Windows or Linux systems must be reflected to the operating environment files for this product. The procedure is explained below.

1. Open the following operating environment file.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWCFMG\config\mail_config.xml
```

2. Change the following items in the operating environment file in accordance with the settings for this product.

Item	Description
enable-email	Set this item to "true".
smtp-host	Specify the host name or IP address of the SMTP server.
smtp-port	Specify the port number of the SMTP server.
from-email	Set the source (sender) email address.
from-name	Set the name of the sender.

A setting example is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
  <entry key="enable-email">>true</entry>
  ... (Omitted) ...
  <entry key="smtp-host">smtp.example.com</entry>
  <entry key="smtp-port">25</entry>
  ... (Omitted) ...
  <entry key="from-email">cloud-master@example.com</entry>
  <entry key="from-name">Support Office</entry>
</properties>
```

Note

- When editing the "mail_config.xml" file, do not change any settings other than smtp-host, smtp-port, from-email, and from-name.
- Back up the "mail_config.xml" file before editing it. If any settings other than smtp-host, smtp-port, from-email, and from-name have been changed, restore the file from the backup.

Accounting information settings

The operating environment files must be modified so that the user of the user department can display accounting information on the service specification list displayed on the service specification search window using MyPortal.

The following operating environment files need to be modified:

- vsys_config.xml
- custom_config.xml

These two files are stored on the server where this product has been installed. The modification procedure is explained below.

Setting up the "vsys_config.xml" file

1. Open the following operating environment file.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWCFMG\config\vsys_config.xml
```

2. Set the following items in the operating environment file.

Item	Description
use-charge	Set this item to "yes" to use the accounting information display function, or "no" otherwise.
use-charge-log	Set "yes" to use the accounting information display function. Set "no" not to use the function.

A setting example is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
  <entry key="super-org-id">cfmgadm</entry>
  ... (Omitted) ...
  <entry key="use-charge">yes</entry>
  <entry key="charge-host">localhost</entry>
  <entry key="charge-port">3550</entry>
  <entry key="charge-uri">/resource/ver1.0</entry>
  <entry key="use-charge-log">yes</entry>
  <entry key="charge-log-host">localhost</entry>
  <entry key="charge-log-port">3550</entry>
  <entry key="charge-log-uri">/resource/ver1.1</entry>
  ... (Omitted) ...
</properties>
```

Note

- When editing the vsys_config.xml file, do not modify setting items other than use-charge, and use-charge-log.
- Backup the vsys_config.xml file before editing it. If setting items other than use-charge, and use-charge-log are modified, restore the backup file.

Specifying settings in "custom_config.xml"

1. Open the following operating environment file.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWCTMG\MyPortal\config\custom_config.xml
```

2. Set the following items in the operating environment file.

Item	Description
estimation-mode	Set "3" to display the Monthly Charges (Approximate) applicable to that subscription. Set "0" not to display it. If "yes" was specified for "use-charge" of "vsys_config.xml settings", set "3". If "no" was specified, set "0".

A setting example is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>  
<properties>  
  <entry key="estimation-mode">3</entry>  
  ... (Omitted) ...  
  <entry key="custom-01">false</entry>  
</properties>
```

Note

- When editing the "custom_config.xml" file, do not change any settings other than estimation-mode.
- Back up the "custom_config.xml" file before editing it. If any settings other than estimation-mode have been changed, restore the file from the backup.

Restart the CFMG_VSYS WorkUnit.

1. Start the Interstage Management Console.
Refer to "3.1.5.1 Starting the Web Servers" for information on the procedure for starting the Interstage Management Console.
2. Re-start the [CFMG_VSYS] WorkUnit by specifying [System] - [WorkUnit] - [View WorkUnit Status].

3.1.5.3 Setting up Information for Interstage Single Sign-On

Registering site definitions

Use the Interstage Management Console to specify the public URL for the Admin Server, as described below.

1. Start the Interstage Management Console.
Follow the steps below to start the Interstage Management Console:
[Windows]
From the [Start] menu, select [All programs] - [Interstage] - [Application Server] - [Interstage Management Console].
2. Specify the public URL of the Admin Server.
Select the [System] - [Security] - [Single Sign-on] - [Authentication infrastructure] - [Repository server] - [Protection resource] - [Create a New Site configuration] tab. Enter FQDN and the port number of the admin server in [Site Configuration Settings] - [FQDN and Port number:3500(The port number of the Cloud Portal)]. Click the <Create> button.

Register Protection Path

Use the Interstage Management Console and follow the steps below to register the protection path:

1. Start the Interstage Management Console.

Refer to "[Registering site definitions](#)" for the procedure to start the Interstage Management Console.

2. Register protected resource.

Select the [System] - [Security] - [Single Sign-on] - [Authentication infrastructure] - [Repository server] - [Protection resource] - [<Admin server FQDN>:<Admin server port number>] - [Protection path] - [Create a New Path configuration] tab.

Set as follows and click the <Create> button.

Path definition		Role / role set (select the following items)
Protected path	Notification of extended user information	
/portala/ctrl/	-	sop_delegated_manager sop_resource_manager sop_restricted_user
/portala/personalInfo/	-	sop_delegated_manager sop_resource_manager
/portala/rManagerInfo/	-	sop_delegated_manager sop_resource_manager
/portala/userManagerMenu/	-	sop_delegated_manager sop_resource_manager

Create the Business system setup file

Use the Interstage Management Console and follow the steps below to create the Business system setup file:

1. Start the Interstage Management Console.

Refer to "[Registering site definitions](#)" for the procedure to start the Interstage Management Console.

2. Set the Public URL and the password in the business system setup file.

Select the [System] - [Security] - [Single Sign-on] - [Authentication infrastructure] - [Business system setup file] tab.

Set the Business system Information as follows. Enter the password (6 or more characters), and click <Download>.

Item	Description
Public URL	http://<Host name of the Admin Server>:<3500(Port number of the Cloud Portal)>/
Linkage with Interstage Portalworks?	No

3. Save the downloaded business system setup file.

Registering the Admin Server

Use the Interstage Management Console and follow the steps below to register the admin server:

1. Start the Interstage Management Console.

Refer to "[Registering site definitions](#)" for the procedure to start the Interstage Management Console.

2. Stop the Web server.

Select the [System] - [Services] - [Web Server] - [ctmg-https-ext]. Display [ctmg-https-ext:Web Server Status], and click the <Stop> button.

3. Set the business system setup file and the password.

Select the [System] - [Security] - [Single Sign-on] - [Business system] - [Addition of Business server] tab.

Set the "*Business system setup file*" downloaded as directed in Create the "*Business system setup file*" and the password in "*Business system setup file*" and Password of file, and then click the <Next> button.

4. Add a Admin Server.

Set the following values in General Settings, and click the <Add> button.

Item	Settings
Business system Name	Business system name (any name)
Web server name to Web Server used	ctmg-https-ext
Host to Web Server used	<Host name of the Admin Server>:<3500 (Port number of the Cloud Portal)>
When Updating Access Control Information?	Execute manually as needed (Execute when Business server is added)
Use Single Sign-on JavaAPI?	Yes

5. Modify the configuration.

Select [System] - [Security] - [Single Sign-on] - [Business system] - [Business system Name]. Enter the business system name specified in step 4 in "*Business system Name*".

Select the [Settings] tab and click [Detailed settings] - [Show]. Modify the configuration as follows and then click the <Update> button.

Item	Settings
Access Log Settings	Maximum size: 1024
Enable Client IP address Check?	No
Notify User Information?	Yes
Cache size	2
Cache count	100

6. Start the Web server.

Select the [System] - [Services] - [Web Server] - [ctmg-https-ext]. Display [ctmg-https-ext:Web Server Status], and click the <Start> button.

Prevention of Caching of Contents

Follow the steps below to enable the Web browser cache settings.

1. Start the Interstage Management Console

Refer to "[Registering site definitions](#)" for the procedure to start the Interstage Management Console.

2. Stop the Web server

Select the [System] - [Services] - [Web Server] - [ctmg-https-ext]. Display [ctmg-https-ext:Web Server Status], and click the <Stop> button.

3. Update the Environment Configuration File of the business server.

Update the Environment Configuration File of the business server using the Editor.

The location and file name of the Environment Configuration File for the business server is shown below:

[Windows]

```
<CIMS installation folder>\Systemwalker\IAPS\F3FMss0\ssoatzag\conf\ssoatzag.conf
```

Edit the above file as shown below:

Add `http-cache-cntl=NO` to the line following the business system name `business-system-name = <Business system name specified in "Register the Admin Server">` of the business server that inhibits cache.

An example using the business name of `Business001` is shown below:

```
ServerPort=80
...<Omitted>...
business-system-name=Gyomu001
http-cache-cntl=NO
```

4. Start the Web server.

Select the [System] - [Services] - [Web Server] - [ctmg-https-ext]. Display [ctmg-https-ext:Web Server Status], and click the <Start> button.

Update Access Control Information

Use the Interstage Management Console and follow the steps below to update the access control information:

1. Start the Interstage Management Console.
Refer to "[Registering site definitions](#)" for the procedure to start the Interstage Management Console.
2. Select [System] - [Security] - [Single Sign-on] - [Business system] - [<Business system Name>]. Click the <Update> button on the [Update access control information] tab.



Note

Continue working because there is no operational problem though the message of `sso04718` might be output when you update access control information.

3.1.5.4 Register the Application Process

To use application processes with this product, a mail server must be registered and a BAR file must be registered with the server for this product.



Information

- Refer to the "Systemwalker Runbook Automation V14g Operation Guide" for details on how to register application processes.



Note

If emails are not sent from the application process function during operations, check whether the mail server for this product has been registered correctly.

Change the following settings to match the settings specified when the mail server for this product was registered.

Item	Description
SMTPServerHost	Specify the host name or IP address that was verified in " Checking the SMTP server ".
SMTPServerPort	Specify "25" (the port number of the mail server).
ServerEmailAddress	Specify the source (sender) email address. The source (sender) email address is the email address in Item 6 of " Parameters specified during installation ".

Use the following procedure to use application processes by registering BAR files with the server for this product.

1. Use a Web browser to access the following URL, and log in as a user with system administrator privileges.

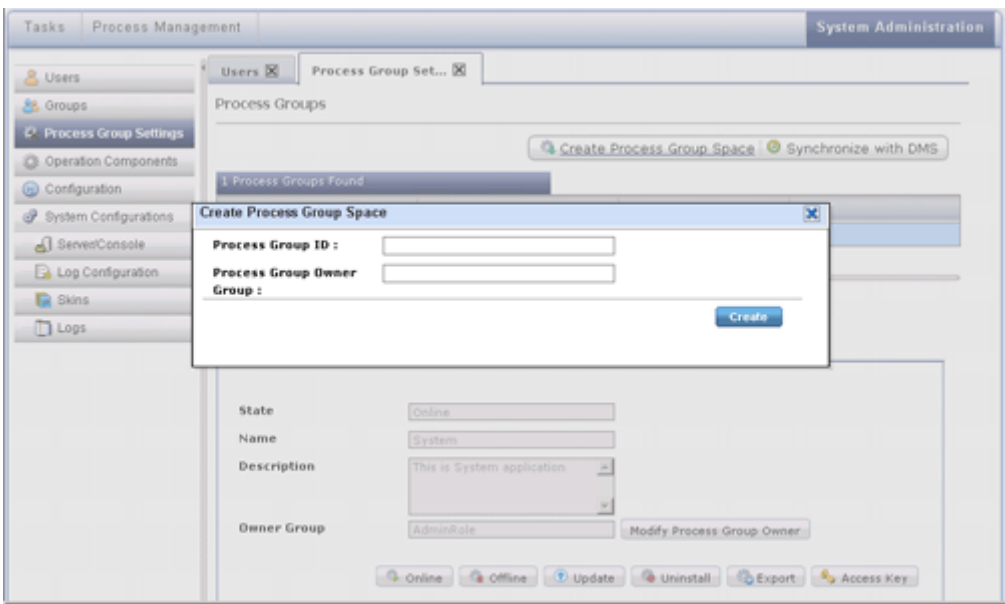
`http://<Host name of the Admin Server>:<80 (Port number of the Web Console)>/console/Default/`

2. Create the process group.

On the process group selection window, select **System** from [Process Group Name] and click the <OK> button.

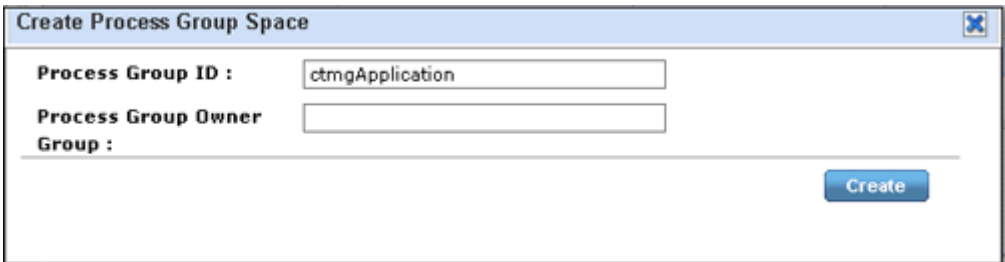


Select [Process Group Settings] on the System Administration tab window, and display the process group setting window. Then, select [Create Process Group Space].



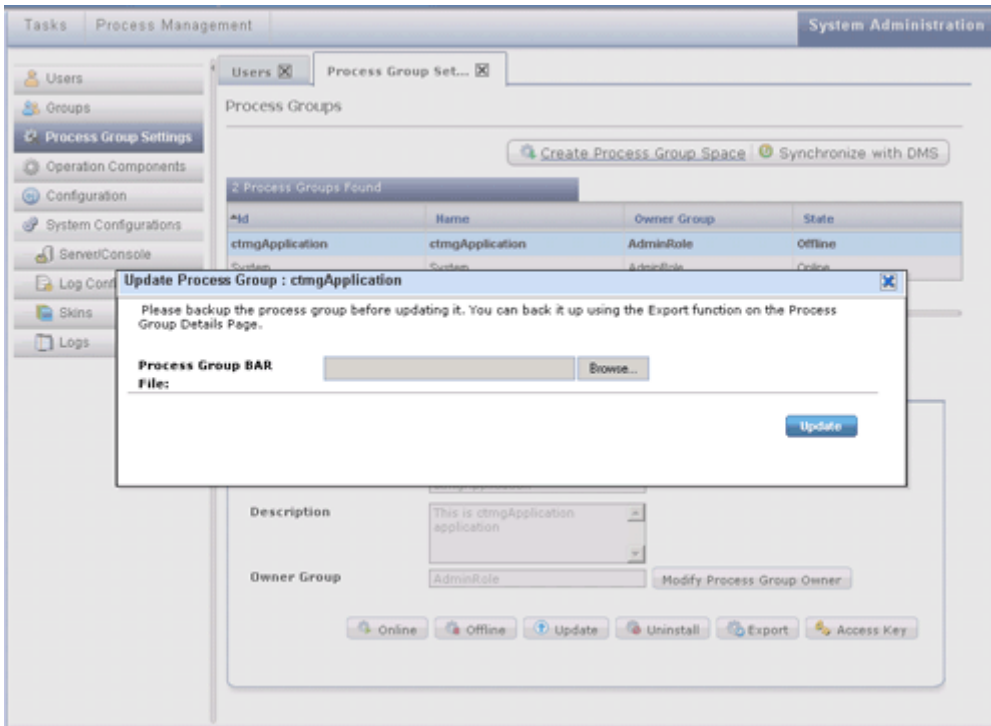
3. Enter the process group ID.

Enter **ctmgApplication** in [Process Group ID] on the [Create Process Group Space] dialog box, and click the <Create> button.



4. Update the process group.

Select the application **ctmgApplication** created in step 3, and click the <Update> button on the lower pane.

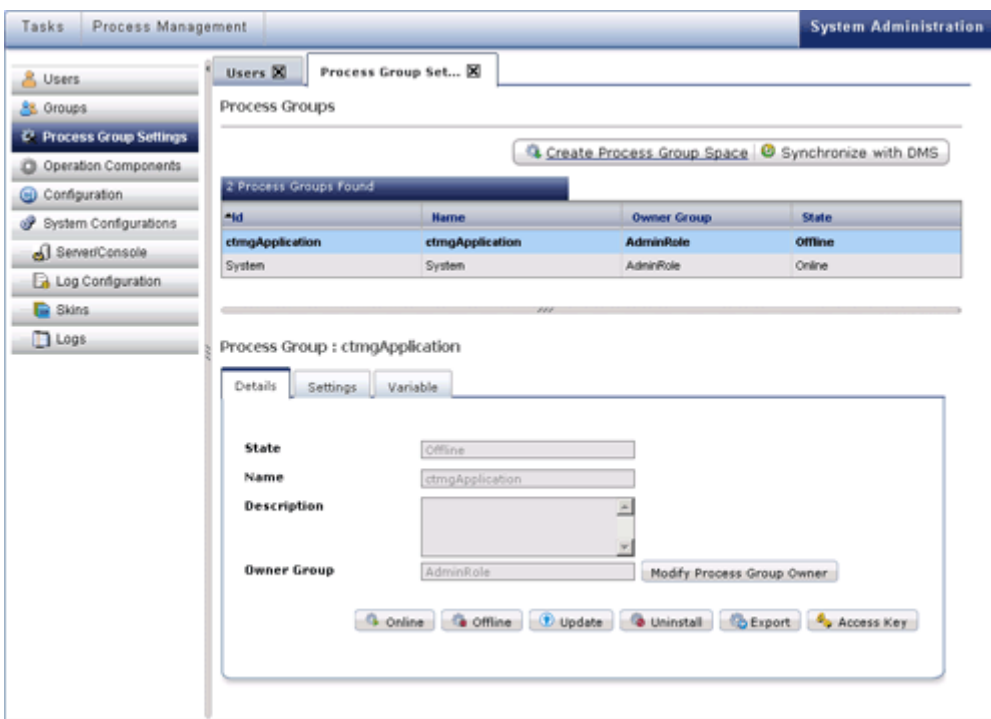


Copy the ctmgApplication.bar file below in the Admin Server onto the environment in which the browser has been opened.

[Windows]

<CIMS installation folder>\Systemwalker\SWCTMG\MyPortal\pkg\ctmgApplication.bar

Click the <Browse> button on the [Update Process Group] dialog box. Select the ctmgApplication.bar file that was copied, and click the <Update> button.

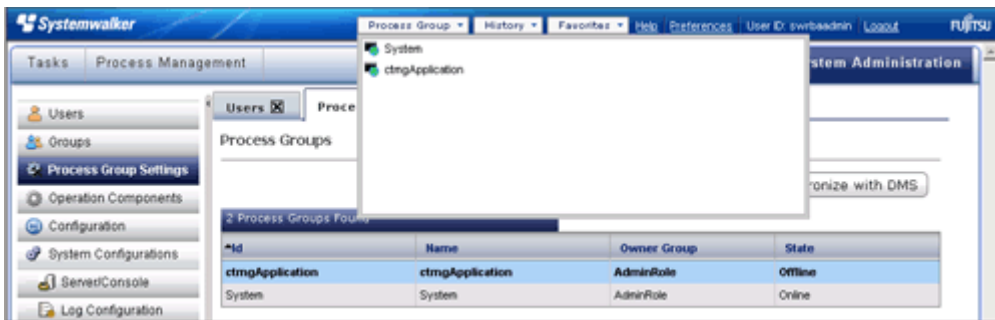


5. Change the process group to an online status.

Select the created process group *ctmgApplication*, and click the <Online> button on the lower pane.

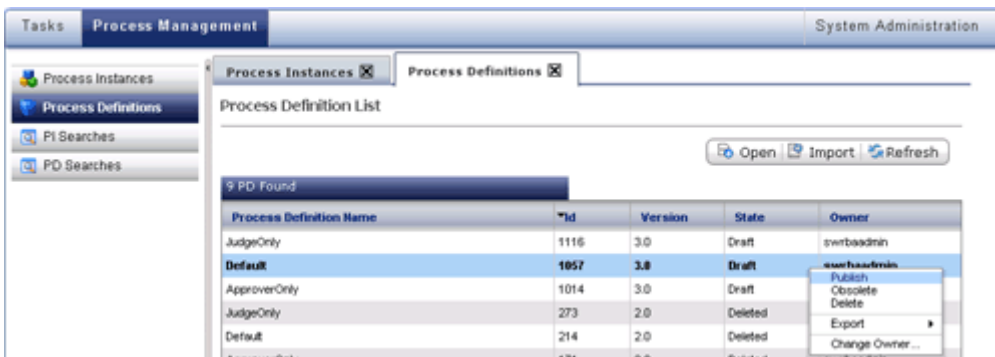
6. Select the process definition and enable it.

Refresh the window by selecting [System Administration] tab, and display the *ctmgApplication* in [Process Group]. Select *ctmgApplication* from [Process Group].



Select [Process Definitions] on the [Process Management] tab window.

Select from the process definition list the process definition to be used. Select **Publish** on the context menu.



3.1.5.5 Registering Managed Servers for the Cloud Infrastructure Administrator Dashboard

To use the cloud infrastructure administrator dashboard with this product, the Managed Servers to be monitored with the dashboard must be registered.

Refer to "[Appendix I Registering and Deregistering Managed Servers](#)" for information on how to register Managed Servers.

3.2 Installing on Managed Servers

This section explains how to install the Managed Server Resource Agent on Managed Servers.

The procedure for installing and setting up Managed Server Resource Agents is as follows:

1. Preparing for installation
2. Installing the required software
3. Installing Managed Server Resource Agents

3.2.1 Preparing for Installation

Configuration of the target server for installation

This section explains the procedure for creating a new Managed Server and installing a Managed Server Resource Agent on the Managed Server where only the virtualization software has been installed.

To install a Managed Server Resource Agent on an existing server, perform the procedure in "[Appendix C Preparations and Checks before Installation](#)" before installing the Managed Server Resource Agent.

Setting up the firewall

To install this product on an environment where a firewall function is being used, settings need to be specified so that the firewall function allows communications via the necessary ports.

Refer to the operating system manual for information on how to set up the firewall so as to allow communications to the necessary ports. Refer to "[D.1 List of Port Numbers](#)" for information on the ports used by this product. Connections must be allowed for the port numbers that need to receive communications from external servers.

Note

The following note applies when the operating system is Windows Server 2008:

The Windows firewall function is enabled by default, and so firewall exceptions must be specified for the port numbers and protocols that are to be used.

Checking the system time

Specify settings so that the Admin Server and the Managed Servers both use the same system time.

3.2.2 Installing the Required Software

Install the software indicated in "[2.2.2.3 Required software](#)" on the Managed Server.

The following sections explain the settings where care is required with some of the required software.

Setting up the required software

- Setting up ServerView Agent

Enter the settings for the SNMP service that are required to install a ServerView Agent.

Refer to the ServerView Agent manuals for details on how to set up the SNMP service.

- For the SNMP community name, set the same value as the SNMP community name that has been set for the management blade.
- Set **Read (reference rights)** or **Write (reference and update rights)** for the SNMP community name.
- For the hosts for which SNMP packets will be accepted, either select **Accept SNMP packets from any host** or select **Accept SNMP packets from these hosts**, and then specify the IP address of the admin LAN for the Admin Server.
- For the SNMP trap destination, specify the IP address of the Admin Server.

If the Admin Server that is the destination for SNMP traps has multiple NICs, specify the IP address of the admin LAN to which the Managed Server is connected.

3.2.3 Installing Managed Server Resource Agents

To install the Managed Server Resource Agent, design and check the following parameters in advance.

Parameters specified during installation

Item No.	Window	Input item	Description
1	Admin Server INformation Registration	Admin Server Address	This is the IP address of the Admin Server. If the Admin Server has multiple IP addresses, specify an IP address with which the Managed Server can communicate.

3.2.3.1 Installing Managed Server Resource Agents [VMware]

Use the following procedure to install a Managed Server Resource Agent.

1. Start the Managed Server (where this product is to be installed) in multi-user mode, and log in to the system as root.

2. Insert the DVD-ROM(DISK1) for this product in the DVD drive, and execute the following command.

```
# cd <Mount point for the DVD-ROM>/DISK1/packages/ROR/Linux/agent
```

Move to the directory where the installer is stored.

3. Execute the installation command (rcxagtinstall).

```
# ./rcxagtinstall
```

4. Proceed with the installation by entering the parameters that were designed and verified in "[Parameters specified during installation](#)" as appropriate, in accordance with the interactive messages given by the installer.

3.2.3.2 Installing Managed Server Resource Agents [Hyper-V]

Use the following procedure to install a Managed Server Resource Agent.

1. Log on with Administrator privileges.

2. Start the installer.

The installer will start automatically when the DVD-ROM(DISK1) is inserted in the DVD drive. If the installer does not start automatically, start it manually by executing *cimssetup.exe*.

3. Click "**Installation of Server Resource Management Agent**".

Thereafter, proceed with the installation by entering the parameters that were designed and verified in "[Parameters specified during installation](#)" as appropriate, in accordance with the instructions displayed in the installation wizard.

For the license authentication information for Windows volume licenses, click the <Next> button without selecting Use the "**cloning feature of this product**".

3.3 Installing on the VM Server

This section explains how to install a Business Server Agent on the VM server.

To create a VM server, a system template, the basis for the VM server, must be created.

Refer to "Chapter 3 Creating and Registering System Templates" in "Systemwalker Software Configuration Manager V14g Operation Guide" for information on how to create and register system templates.

Do the following steps to install the business server agent on the VM server. (These steps are also performed when creating the L-Server when creating system templates.)

Before starting the installation, check that the procedure in "[Appendix C Preparations and Checks before Installation](#)" has been performed.

Use the following procedure to install and set up Business Server Agents.

1. Preparing for installation
2. Installing the required software
3. Installing Managed Server Resource Agents

3.3.1 Preparing for Installation

Setting up the operating system property definition file

To deploy Linux operating system virtual servers, the virtual server DNS search path must be set in the OS property definition file.

Refer to "L-Server Parameter Details" in the "ServerView Resource Orchestrator User's Guide" for information on how to set this path.



.....
The DNS search path is specified using the operating system property definition file. For the operating system property definition file, edit the following file that is common to both Windows and Linux operating systems.

[Windows]

```
<CIMS installation folder>\Resource Orchestrator\Manager\etc\customize_data\os_setting.rcxprop
```

[Linux]

```
/etc/opt/FJSVrcvnr/customize_data/os_setting.rcxprop
```

Setting system parameters [Linux]

Tune the system parameters for the VM server. Refer to "[Appendix E Tuning System Parameters](#)" for details on tuning settings.

Setting up the firewall

To install this product on an environment where a firewall function is being used, settings need to be specified so that the firewall function allows communications via the necessary ports.

Refer to the operating system manual for information on how to set up the firewall so as to allow communications to the necessary ports. Refer to "[D.1 List of Port Numbers](#)" for information on the ports used by this product. Connections must be allowed for the port numbers that need to receive communications from external servers.



Note

The following note applies when the operating system is Windows Server 2008:

The Windows firewall function is enabled by default, and so firewall exceptions must be specified for the port numbers and protocols that are to be used.

Setting the software ID for the software information in the system template

The software ID for the software information in the system template for the VM server must be set. Set the following for the software ID. Refer to "Registered Software IDs" for details.

Registered software ID	Software	OS	Version
SW00000091	Systemwalker Service Quality Coordinator Enterprise Edition	Windows	V13.4
SW00000093	Systemwalker Service Quality Coordinator Enterprise Edition	Linux	V13.4

3.3.2 Installing the Required Software

Install the software indicated in "[2.2.2.3 Required software](#)" on the Business Server Agent.

3.3.3 Installing Business Server Agents

This section explains how to install Business Server Agents.

3.3.3.1 Installing Business Server Agents [Windows]

This section explains how to install Business Server Agents when the VM server is running Windows.

- Installing Business Server Agents

1. Log in with Administrator privileges.

2. Start the installer.

The installer will start automatically when the DVD-ROM(DISK1) is inserted in the DVD drive. If the installer does not start automatically, start it manually by executing *cimssetup.exe*.

3. Select either "*Installation of Job Server Agent function (32bit)*" or "*Installation of Job Server Agent function (64bit)*".

4. Specify the installation folder and then start the installation.

5. Specify the host name or IP address of the Admin Server to connect to.
6. When prompted, insert the DVD-ROM(DISK2) or the DVD-ROM(DISK3) to DVD drive to proceed 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 the product again.

3.3.3.2 Installing Business Server Agents [Linux]

This section explains how to install Business Server Agents when the VM server is running Linux.

- Installing Business Server Agents

Perform the following procedure.

1. Log in as a superuser (root).
2. Insert the DVD-ROM(DISK1) in the DVD drive.
3. Mount the DVD-ROM by executing the following command. If the DVD-ROM is automatically mounted by the automount daemon (autofs), the installer will fail to start because "noexec" is specified for the mount option.

```
# mount /dev/hdc <Mount point for the DVD-ROM>
```

4. Execute the installation command (cimssetup.sh).

```
# <Mount point for the DVD-ROM>/cimssetup.sh
```

5. Perform the installation in accordance with the interactive messages given by the installer.
Select either "**Job server agent function(32bit)**" or "**Job server agent function(64bit)**" in the server selection window.
6. Enter the host name or IP address of the Admin Server to connect to.
7. A message will be output prompting for the disks to be swapped.
8. Open another terminal (such as a Gnome terminal) and use a command to eject the DVD-ROM.

```
# eject (<Mount point for the DVD-ROM>)
```

9. Insert the DVD-ROM(DISK2) and wait for automount to complete.
10. Remount the DVD-ROM.

```
# umount <Mount point for the DVD-ROM>  
# mount /dev/hdc <Mount point for the DVD-ROM>
```

11. Press the <Enter> key to continue the installation.
12. Regarding to DVD-ROM(DISK3), continue the installation process by following steps 9 to 11.

Note

- Do not set the current directory to the DVD or else it will not be possible to replace the disk.

For single user mode, X Window will not be running, so one of the following actions is required.

- Switching the virtual console (switch using the CTL+ALT+PFn key)
- Running the command in the background

- 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 the product again.

3.4 Uninstalling the Manager from the Admin Server

This section describes how to cancel the setup for the Manager on the Admin Server and uninstall the Manager.

1. Tasks to perform before cancelling the setup
2. Canceling the setup
3. Uninstalling the Manager.

3.4.1 Tasks to Perform Before Cancelling the Setup

Be sure to stop this product before canceling the setup for the Manager.

If this product is running when the setup is canceled, the setup will not be canceled properly.

Stop this product by executing the following command.

[Windows]

1. Log in with Administrator privileges.
2. Execute the stop command.

```
> <CIMS installation folder>\CIMS\Manager\bin\cims mgrctl stop
```

Canceling the settings for Interstage Single Sign-On

Use the Interstage Management Console to cancel the setup for the Interstage Single Sign-On environment for this product.

Use the following procedure to cancel the setup for the Interstage Single Sign-On environment.

1. Start the Interstage Management Console.

Use the following procedure to start the Interstage Management Console.

[Windows]

Select All Programs, Interstage, Application Server, and then Interstage Management Console from the Start menu.

2. Display the list of business systems.

Select **[System] - [Security] - [Single sign-on] - [Business system]**, and open **[Business system: List]**.

3. Delete the public URL.

After confirming the value set in **Public URL** of the business system where **ctmg-https-ext** is set as the Web server name, select the checkbox, and click the **<Delete>** button.

4. Display the protected resources.

Select **[System] - [Security] - [Single sign-on] - [Authentication infrastructure] - [Repository server] - [Protection resource]**, and open **[Protection resource: List]**.

5. Delete the site definitions.

Check the check box of the site definition that matches FQDN and the port number of the Public URL confirmed at step 3 of the procedure, and click the **<Delete>** button.

3.4.2 Canceling the Setup

This section explains how to cancel the setup for the Manager.

3.4.2.1 Canceling the Setup of the Automatic Operation Function [Windows]

1. Log in as a user with Administrator privileges for the Management Server.
2. Execute the following command to start cancelling the setup.

```
> <CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_setup -u
```

3. The setup cancellation tool for the automatic operation function will start.
Check the settings that are displayed, and then click the <Next> button.
4. A confirmation dialog box is displayed. Click the <Yes> button when going ahead with deletion of the operating environment to start the setup cancellation process. Click the <No> button to cancel setup cancellation.
5. After setup cancellation is complete, the completion window will be displayed. Check the settings that are displayed, and then click the <Finish> button.

3.4.2.2 Canceling the Setup for the CMDB

Use the following procedure to cancel the setup for the CMDB.

1. Stop the CMDB.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbstop.bat
```

1. Cancel the setup for the CMDB.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbunsetupenv.bat -k  
AGT_CFMG
```

1. Start the CMDB.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbstart.bat
```

3.4.2.3 Canceling the Setup for the Manager

This section explains how to cancel the setup for the Manager.

Canceling the setup [Windows]

This section explains the procedure for canceling the setup for the Manager.

Executing the setup cancellation command

1. Log in with Administrator privileges.
2. Use the following command to cancel the setup.

```
> <CIMS installation folder>\Systemwalker\SWCTMG\bin\setup\swctmg_service_setup /u
```

3. Use the following command to cancel the setup.

```
> <CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_setup -u
```

3.4.3 Tasks to Perform After Cancelling the Setup

After canceling the setup for the Manager, be sure to perform the following tasks:

- Canceling the setup for Interstage Single Sign-On

This product uses the Interstage Single Sign-On function for user authentication.

Cancel the setup for Interstage Single Sign-On in order to delete the Interstage Single Sign-On environment that has been created.

Refer to "F.2 Canceling the Setup for Interstage Single Sign-On" for details.

3.4.4 Uninstalling the Manager

This section explains how to uninstall the Manager. If necessary, back up environment resources before uninstallation.

Refer to "4.8.2 Backing up the Admin Server" for details.

3.4.4.1 Uninstalling the Manager [Windows]

Use the following procedure to uninstall the Manager.

1. Log in with Administrator privileges.
2. Execute the following command.

```
> %F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl stop
```

3. Start the uninstaller.

From the [Start] menu, select [Programs] or [All Programs], then select [Fujitsu], then select [Uninstall (middleware)].

4. Select "*Cloud Infrastructure Management Software (Admin Server)*", then click the <Remove> button.
5. Once the uninstallation has completed, click the <Exit> button to exit the uninstaller.
6. Restart the system.



The user account that was created in the "Administrative User Creation" window (shown in the table under "[Parameters specified during installation](#)") during the installation is not deleted automatically.

If this account is not required, delete it manually. However, do not delete this account if it is being used for another purpose.

The installation folder (default: C:\Fujitsu) will still remain after the uninstallation. If this folder is not required, delete it manually.

- How to delete Windows user accounts

Open [Management] from [Administrative Tools] on the Windows [Control Panel], and then select [Local Users and Groups] - [Users].

Right-click the user account to be deleted, and select [Delete].

3.4.5 Tasks to Perform After Uninstallation

This section explains the tasks to be performed after the Manager has been uninstalled.

3.4.5.1 Uninstalling the Fujitsu XML Processor [Windows]

This section explains the procedure for uninstalling the Fujitsu XML Processor.



Make sure 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.



See

Refer to the "Fujitsu XML Processor Software Release Note" for details. The Software Release Note can be viewed by selecting **[Fujitsu XML Processor V5.2]** and then **[Software Release Note]** from the **[Start]** menu.

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

Select **[Control Panel]** and then **[Add or Remove Programs]** from the **[Start]** menu.

Select **[Fujitsu XML Processor V5.2.4]** and then click the **[Remove]** button.



Note

If the operating system is Windows Server 2008, select **[Control Panel]** and then **[Programs and Features]** from the **[Start]** menu, and run the uninstaller as an administrator.

3. A message will be displayed confirming whether to continue with the uninstallation processing.
To continue with the uninstallation, click the **<OK>** button. Otherwise click the **<No>** button to cancel the uninstallation.
4. Execute the uninstallation.
The program removal window will be displayed, and the program will be deleted, together with the information registered in the registry.

3.4.5.2 Deleting the User Information for Accessing the Database

[Windows]

Use the following procedure to delete the user profile and user account for accessing the database.



Note

This procedure must be performed by a user with Administrator privileges in administrator mode.

1. Open the **[Control Panel]** from the **[Start]** menu.
2. Open the **[System]** window from the **[Control Panel]**.
3. Click the **[Advanced system settings]** to open the **[System Properties]** dialog box.
4. Click on the **[Settings]** button in the **[User Profiles]** section of the **[Advanced]** tab.
5. If the list of user profiles contains a profile corresponding to cfmgdb, select it and click the **[Delete]** button.

Use the following command to delete the account for the user.

This example uses the "net user" command.



Example

```
net user cfmgdb /delete
```

3.4.5.3 Files that Remain After Uninstallation

After the uninstallation, some files and directories may still remain. Delete the following files and folders (including any files and subfolders in these folders) manually.

[Windows]

- CMDBDB
- CMDBM
- SWCTMG
- SWRBAM
- SWOMGR
- IBPM
- IAPS
- IBPMA
- IBPMA_DATA
- SQC_DATA
- SQCM
- Resource Orchestrator
- %SystemDrive%\ProgramData\Fujitsu\SystemwalkerCF-MG



Note

Any files that have been locked may fail to be deleted. In this case, delete these files manually after restarting the operating system.

The "%SystemDrive%\ProgramData" folder is normally not displayed because it is a hidden folder.

Accordingly, use either of the following methods to view the content of this folder.

- Specify "%SystemDrive%\ProgramData" directly as the folder name.
- Select **[Folder and Search Options]** from the **[Organize]** menu of Explorer to display the **[Folder Options]** dialog box. Select the **[View]** tab, then select **[Hidden files and folders]** and **[Show hidden files] - [folders and drives]** and apply the settings.

3.4.5.4 Groups that Remain After Uninstallation

The swadmin group has been created. If this group is not required, delete it manually.

3.5 Uninstalling Managed Server Resource Agents from Managed Servers

This section explains how to uninstall Managed Server Resource Agents from Managed Servers.

3.5.1 Uninstalling Managed Server Resource Agents

This section explains how to uninstall Managed Server Resource Agents.

3.5.1.1 Uninstalling Managed Server Resource Agents [Hyper-V]

Use the following procedure to uninstall Managed Server Resource Agents.

1. Log in with Administrator privileges.
2. Open the **[Add and Remove Programs]** window from the **[Control Panel]**, and then remove "ServerView Resource Orchestrator Agent".



Information

For Windows Server 2008, open the **[Programs and Functions]** window from the **[Control Panel]**.

3.5.1.2 Uninstalling Managed Server Resource Agents [VMware]

Use the following procedure to uninstall Hypervisor Agents.

1. Log in as a superuser (root).
2. Execute the uninstallation command (rcxagtuninstall).

```
# /opt/FJSVrcxat/bin/rcxagtuninstall
```

3. Perform the uninstallation in accordance with the interactive messages output by the uninstaller.
4. If the uninstallation fails, use the "rpm" command to remove the package displayed in the message, and then repeat the procedure from Step 1.

```
# rpm -e <Package name> <RETURN>
```

3.6 Uninstalling Business Server Agents from VM Servers

This section explains how to uninstall Business Server Agents from VM servers.

It explains how to uninstall Business Server Agents from the virtual images that are the basis of VM servers.

3.6.1 Uninstalling Business Server Agents

This section explains how to uninstall Business Server Agents.

3.6.1.1 Uninstalling Business Server Agents [Windows]

1. Log in with Administrator privileges.
2. Use the stop command to stop the Business Server Agent if it is running.

```
> %F4AN_INSTALL_PATH%\F4ANswnc\bin\swncctrl stop
```

3. Start the uninstaller.

From the **[Start]** menu, select **[Programs]** or **[All Programs]**, then select **[Fujitsu]**, then select **[Uninstall (middleware)]**.

4. Select **"Cloud Infrastructure Management Software (Job Server)"**, then click the **<Remove>** button.
Perform the uninstallation in accordance with the wizard for the uninstaller.

5. Restart the server.

Be sure to restart the server after the Business Server Agent has been uninstalled.

3.6.1.2 Uninstalling Business Server Agents [Linux]

1. Log in as a superuser (root).
2. Use the stop command to stop the Business Server Agent if it is running.

```
# /opt/FJSVswnc/bin/swncctrl stop
```

3. Execute the uninstallation command (cimanager.sh).

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

4. Perform the uninstallation in accordance with the interactive messages output by the uninstaller.

3.6.2 Post-uninstallation Tasks

This section explains the tasks to be performed after the Business Server Agent has been uninstalled.

3.6.2.1 Uninstalling SMEE [Linux]

This section explains the procedure for uninstalling SMEE.



Make sure that no other products are using SMEE before uninstalling it.

1. Log in to the system as a superuser.
2. Use the rpm command to uninstall the package.

- For the 32 bit version

```
# rpm -e FJSVsmee
```

- For the 64 bit version

```
# rpm -e FJSVsmee64
```

3.6.2.2 Uninstalling the Securecrypto Library Runtime [Linux]

This section explains the procedure for uninstalling the Securecrypto Library Runtime.



Make sure that no other products are using the Securecrypto Library Runtime before uninstalling it.

1. Log in to the system as a superuser.
2. Use the rpm command to uninstall the package.

- For the 32 bit version

```
# rpm -e FJSVsc1r
```

- For the 64 bit version

```
# rpm -e FJSVsc1r64
```

3.6.2.3 Files that Remain After Uninstallation

The following folders where the Business Server Agent was installed may still remain after uninstallation. Delete these folders manually.

Note that these folders may contain files and folders that have been left over, so delete these files and folders as well.

[Windows]

- SWCTMGA
- SWCTMGAV
- SWRBAA



Any files that have been locked may fail to be deleted. In this case, delete these files manually after restarting the operating system.

[Linux]

- /etc/opt/FJSVcmdba
- /etc/opt/FJSVctmg
- /etc/opt/FJSVlnkbs
- /etc/opt/FJSVswrbaa
- /etc/opt/FJSVswrbac
- /opt/FJSVcmdba
- /opt/FJSVctmg
- /opt/FJSVlnkbs
- /opt/FJSVswrbaa
- /opt/FJSVswrbac
- /var/opt/FJSVcmdba
- /var/opt/FJSVlnkbs
- /var/opt/FJSVswrbaa
- /var/opt/FJSVswrbac

3.6.2.4 Notes to Observe After Uninstalling SMEE and the Securecrypto Library Runtime [Linux]

The following folders will still remain after SMEE and the Securecrypto Runtime Library have been uninstalled. Check that these folders are not being used by other products, and delete them manually if they are not required.

Note that these folders may contain files and folders that have been left over, so delete these files and folders as well.

- For the 32 bit version
 - /opt/FJSVsmee
 - /etc/opt/FJSVsclr
- For the 64 bit version
 - /opt/FJSVsmee64
 - /etc/opt/FJSVsclr64

3.7 Uninstalling "Uninstall (middleware)"

It manages installed Fujitsu middleware products and launches uninstallers of those.

This product supports Uninstall (middleware).

Uninstall (middleware) will be installed by default when this product is installed. Uninstall (middleware) controls the installation and uninstallation of Fujitsu middleware products. Note that the installation process will not be performed if Uninstall (middleware) has already been installed.

This section explains how to uninstall "Uninstall (middleware)", and the points that should be noted.



- To uninstall this product, be sure to uninstall it from the [**Uninstall (Middleware)**] tool.

- This tool manages information for other Fujitsu middleware products as well as for this product. Do not uninstall this tool unless it is absolutely necessary.

If this tool is uninstalled accidentally, use the following procedure to reinstall it.

[Windows]

1. Log in with Administrator privileges to the machine where the tool is to be installed.
2. Insert the DVD (DISK1) in the DVD drive.
3. Execute the installation command.

```
<DVD drive>\DISK1\CIR\cirinst.exe
```

[Linux]

1. Become a superuser on the system.
2. Insert the DVD (DISK1) in the DVD drive.
3. Mount the DVD by executing the following command. If the DVD is automatically mounted by the automount daemon (autofs), the installer will fail to start because "noexec" is specified for the mount option.

```
# mount /dev/hdc <Mount point for the DVD-ROM>
```

4. Execute the installation command.

```
# <Mount point for the DVD-ROM>/DISK/CIR/cirinst.sh
```

To uninstall *Uninstall (middleware)*, perform the following procedure:

1. Start *Uninstall (middleware)* and check whether other Fujitsu middleware products are still remaining. The method to start the tool is as follows:

[Windows]

Click the [Start] - [All Programs] - [Fujitsu] - [Uninstall (middleware)].

[Linux]

```
# /opt/FJSVcir/cir/bin/cimanager.sh [-c]
```

-c: Command interface



The tool will fail to start if the command path contains blank spaces. Do not change to a directory that contains blank spaces.



To start the tool in command mode, specify the "-c" option. If this "-c" option is not specified, the command will run in GUI mode if there is a GUI environment and in command mode if there is no GUI environment.

2. If no Fujitsu middleware products have been installed, execute the following uninstallation command.

[Windows]

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

[Linux]

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

3. The following message will be displayed: *"This software is a tool that is shared by all Fujitsu middleware products. Is it OK to delete it? [y/n]:"*. Enter 'y' to continue.

Uninstallation will be complete in a few seconds.

4. After the uninstallation completes, the following directories and the files under them will still remain, so delete them manually.

[Windows]

- %SystemDrive%\FujitsuF4CR

[Linux]

- /var/opt/FJSVcir

Chapter 4 Operation and Management

This chapter explains how to operate and manage systems using Cloud Infrastructure Management Software.

- User management
- Service operations
- Visualizing ICT resources
- Managing accounting information
- Backing up and restoring the Admin Server

4.1 User Management

User management involves managing information about users and organizations, which change as a result of personnel changes and organizational restructuring.

User management methods

There are two methods for user management: "*User management by the service provider department*", and "*User management by the service user department*".

User management by the service provider department

With this method, the system administrator uses user management commands to manage users and organizations.

User management by the service user department

With this method, the administrator of the service user department uses GUI operations to manage the administrators and general users in the user department within the organization.

User management functions

User management can be broadly classified into three types, as follows:

- Organization management
- User management
- Service management

The following table shows which roles have permission to perform which type of user management operation:

	Overview	User management by the service provider department			User management by the service user department		
		System administrator	Service provider department administrator	General user	System administrator	Service user department administrator	General user
Organization management	Register new organizations	Yes	No	No	Yes	No	No
	Delete organizations	Yes	No	No	Yes	No	No
	Change organization names	Yes	No	No	Yes	No	No
	List organization information	Yes	No	No	Yes	No	No
User management	Register users	Yes	No	No	Yes (*1)	Yes (*3)	No

	Overview	User management by the service provider department			User management by the service user department		
		System administrator	Service provider department administrator	General user	System administrator	Service user department administrator	General user
	Delete users	Yes	No	No	Yes (*1)	Yes (*3)	No
	Change user information	Yes	Yes (*2)	Yes (*2)	Yes (*1)	Yes (*3)	Yes (*2)
	Move users	Yes	No	No	Yes	No	No
	List user information	Yes	No	No	Yes	Yes (*3)	No
Service management	Change service management source	Yes	No	No	Yes	No	No

Yes: Operation allowed, No: Operation not allowed.

*1: Because users are managed by the service user department, commands should be used only when necessary.

*2: Users can only change their own information from the user management window.

*3: Operations relating to general users and user department administrators can be performed from the user management window.

Note

- A single user ID cannot be registered with multiple organizations.
- Organizations cannot be layered.
- In order to ensure user uniqueness, a user ID cannot be used again once its user has been deleted.

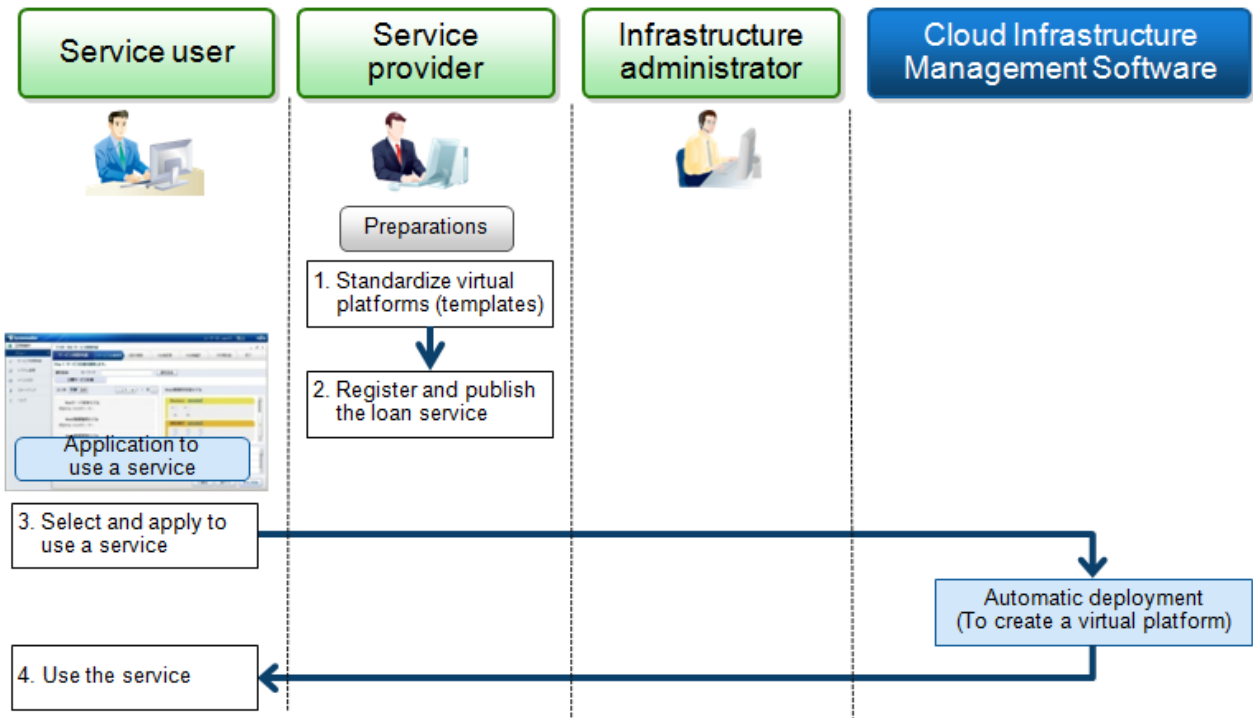
Refer to "Chapter 4 User Management" , "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide" for Administrators for details on managing organizations and users, and operations involving personnel changes and organizational restructuring.

4.2 Overview of Service Operations

This section explains the flow of operations for the users who use this product. Note that the minimal users required for this product to run are registered when the product is installed.

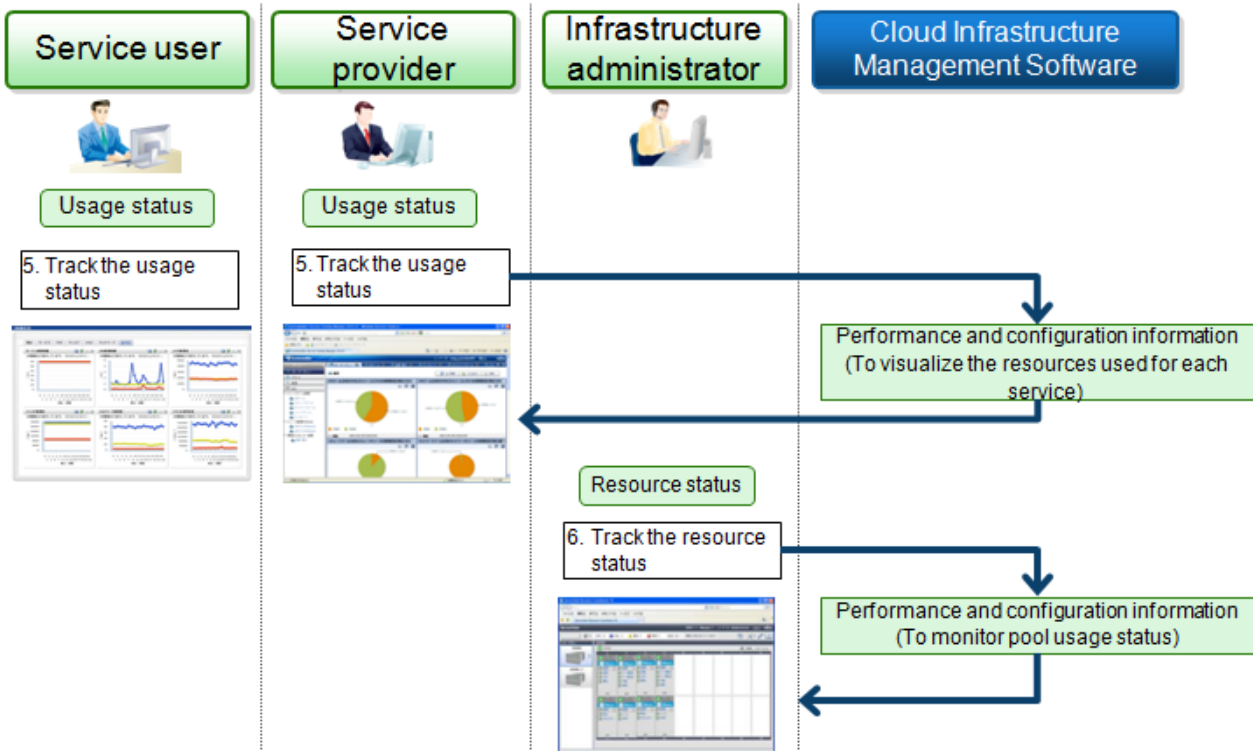
From registering and publishing a service through to applying to use the service

The following flowchart shows the general flow whereby service providers register ICT resources as a service, publish that service, and then service users apply to use the service.



Tracking the usage status of services and resources

The following flowchart shows the general flow for tracking the usage status of a service during system operations and tracking the status of ICT resources.



The following explains how to start the RC Console, the Operation Portal and the Cloud Portal, which are used in these operation methods.

- RC Console

To connect to the RC Console, the infrastructure administrator starts a Web browser and specifies the URL of the RC Console. If the port number has been changed, specify the new port number.

```
URL: https://<Host name or IP address of the Admin Server>:23461(Port number of the RC Console)/
```

Alternatively, in environments where the Admin Server is running on Windows and the Manager has been installed, the RC Console can also be started by selecting **[Start] - [All Programs] - [Resource Coordinator VE] - [RC consol]**.

Refer to "[A.4 RC Console](#)" for details on the RC Console.

- Operation Portal

To connect to the Operation Portal, the service provider (the administrator of the service provider department) starts a Web browser and specifies the URL of the Operation Portal.

```
URL: http://<Host name of the Admin Server>:<80 (Port number of the Web server)>/op_portal
```

- Cloud Portal

To connect to the Cloud Portal, the service user (the administrator of the user department) starts a Web browser and specifies the URL of the Cloud Portal.

```
URL: http://<Host name of the Admin Server>:<80(Port number of the Cloud Portal)>/portal/ctrl/top/
```

The following sections explain operating methods, following the flows described above.

4.3 Operation Procedures for Service Providers

This section explains the preparation tasks that service providers perform to lease virtual platforms (ICT resources) to service users, as well as the operations for standardizing virtual platforms as templates.

- Registering resources
- Registering resources in resource pools
- Creating and managing L-Server Templates
- Creating and managing L-Servers
- Creating, registering and deleting system templates
- Publishing and deleting services

4.3.1 Registering Resources

Register ICT resources with this product. The registration method depends on the type of server virtualization software being used.

Refer to the following procedures in "ServerView Resource Orchestrator User's Guide" details for each server virtualization software products.

[VMware]

Section 1, Register resources of "G.1.4 Setup"

[Hyper-v]

Section 1, Register resources of "G.2.4 Setup"

4.3.2 Registering Resources in Resource Pools

This section explains how to register the ICT resources managed by this product in resource pools.

"Resource pools" are a type of resource folder displayed on the orchestration tree of RC Console, which stores the resources for selection when creating or adding L-Servers.

A resource pool type is specified when creating a resource pool, and only resources of a specific type are stores in each type of resource pool. When installing this product, one resource pool is created for each resource pool type.

This section explains how to register resource pool types or resources to a resource pool.

Table 4.1 Registering resources in resource pools for each resource type

Type of resource pool	Type of resources stored in the resource pool	How to register resources in resource pools	Registration required?
VM pool	VM host resources	Refer to " VM host resources ".	Yes
Server pool	Physical server resources	Not supported by this product	No
Storage pool	Virtual storage resources	Refer to " Storage resources ".	Yes
Network pool	Network resources	Refer to " Network resources ".	Yes
Address pool	Address set resources	Not supported by this product	No
Image pool	Virtual image resources - Either images that use templates used by the VM management product to create VM guests, or images of cloning masters taken from L-Servers	Refer to " Virtual Image resources ".	Yes (*1)

Yes: Required

No: Not required

*1: If the template is used, register them to the image pools.

4.3.2.1 VM host resources

This section explains how to register VM hosts in VM pools.

Use the following procedure to register VM hosts in a VM pool.

1. In the RC console orchestration tree, right-click the target VM pool, and select the **[Register Resources]** from the context menu. The **[Register Resources]** dialog box will be displayed.
2. Select the VM host to be registered. The list of the VM hosts that can be registered is displayed in the resource list. Select the VM host that you want to register using the **[Select]** checkbox, or select all VM host resources displayed in the resource list by checking **[Select all]**.
3. Click the **<OK>**. The VM host resource is registered.

4.3.2.2 Storage resources

This section explains how to register a storage resource in a storage pool.

Use the following procedure to register a storage resource.

1. In the RC console orchestration tree, right-click the target storage pool, and select **[Register Resources]** from the popup menu. The **[Register Resources]** dialog is displayed.
2. Select the storage resource to register from **[Resources]**.

Resources

Virtual storage

When creating a specified size of disk automatically from the virtual storage during L-Server creation, select **[Virtual storage]**.

When **[Virtual Storage]** is selected, the virtual storage resources which can be registered will be displayed in the resource list.

Select the virtual storage resource which you want to register using the **[Select]** checkbox of the resources, or select all registered virtual storage resources by checking **[Select all]**.

Note

Virtual storage resources cannot be selected for EMC storage.

Disk resource

When using a disk that has been created in advance as an L-Server, select [**Disk resource**].

When the following items are specified as search conditions, the list for the relevant disk resources which can be registered is displayed.

Virtual storage

Select a virtual storage where there is a disk that has been created in advance.

Size

Enter the size of the disk resource.

Minimum value

Enter the lowest value of the disk size to be searched as a number with up to one decimal place, in units of gigabytes. Check the [**Minimum value**] checkbox, and enter a value lower than the maximum value.

Maximum value

Enter the highest value of the disk size to be searched as a number with up to one decimal place, in units of gigabytes. Check the [**Maximum value**] checkbox, and enter a value higher than the minimum value.

Depending on the value of the second decimal place of the disk size, matching disks may not be able to be displayed in the result. For search conditions, specify a size allowing for errors.

Select the disk resource which you want to register using the "Select" checkbox of the displayed disk resources, or select all registered disk resources by checking [**Select all**].

3. Click the <OK>.

The storage resource is registered.

Note

When using a LUN that has been created in advance and a LUN for iSCSI boot as a disk resource, if the L-Server is deleted or disks are deleted from L-Servers, the content of disks will remain (is not deleted).

When the disk resource is registered in a global pool, it is possible to be allocated to unspecified users, so caution is necessary.

When using a LUN that has been created in advance as a disk resource, it is recommended to operate the LUN in a local pool, and delete data on the disk during deletion of L-Servers or detachment of disks.

Use the following methods to delete the data on disks.

- Using an OS, perform disk formatting while the L-Server is connected
- Using a function of the storage, perform disk formatting (For ETERNUS)
- Create a LUN again

4.3.2.3 Network resources

This section explains how to create network resources and register them in network pools.

Use the following procedure to create a network resource.

- Create a new network resource

Refer to "[Create a new network resource](#)" for details.

- Create a network resource using the registered admin LAN subnet

Refer to "[Create a network resource using the registered admin LAN subnet](#)" for details.

Create a new network resource

Use the following procedure to create a new network resource and register it in a network pool.

1. In the RC console orchestration tree, right-click the target network pool, and select **[Create Resource] - [New]** from the popup menu. The **[Create a network resource]** dialog is displayed.
2. Enter the items below, and click the **<OK>**.

Network resource name

Enter a name for the network resource.

If "Admin LAN" was selected as the type, enter a string that is no more than 16 characters long, where the first character is a number or letter (either upper- or lower-case) and the remaining characters are alphanumeric characters (either upper- or lower-case), underscores (" _ "), periods (".") and hyphens ("-").

If "Admin LAN" was not selected as the type, enter a string that is no more than 32 characters long, where the first character is a number or letter (either upper- or lower-case) and the remaining characters are alphanumeric characters (either upper- or lower-case), underscores (" _ "), periods (".") and hyphens ("-").

Types

The network resource type that will be created is set using the following radio buttons:

- Public LAN
- Admin LAN
- iSCSI boot (Although this will be displayed, it cannot be used in this product)

Note

To create the public LAN, the network resource name and VLAN ID must both be entered.

To create the admin LAN, the network resource name, VLAN ID, subnet address and subnet mask must all be entered.

VLAN/External Connection Port Settings

Set the VLAN ID and external connection ports.

Clicking **[Setting]** displays the **[Define VLAN ID/Uplink port settings]** dialog.

Specify the VLAN ID to allocate to the LAN switch blade and virtual switch. Select a VLAN ID allocated to the external port of the LAN switch blade, or enter a number. Specify a pre-designed VLAN ID.

Enter an integer between "1" and "4094".

- For external networks that include blade servers
Select from a list of VLAN IDs with external ports.
- For internal networks, or external networks with only rack-mounted servers

Enter a VLAN ID.

When selecting the "Filter ports by VLAN ID" checkbox with an ID specified, the next time an external connection port is configured, the displayed information is filtered.

Uplink port settings (VLAN ID/Chassis/LAN Switch/Port/VLAN type) (Optional)

When an L-Server is connected to an external network, set up the virtual switch and the internal port for the LAN switch blade, so that the L-Server can communicate with the specified ports.

Clicking **<Settings>** displays the **[Define VLAN ID/Uplink port settings]** dialog.

Specify the external connection ports that are used when external networks that include blade servers are automatically set up.

Select the checkboxes for the external connection ports that have been designed and set up in advance. Select two ports that will form a pair. If there are multiple chassis, select all of the ports that the chassis will use.

To specify a port for a link aggregation configuration, perform the following tasks:

- First check the settings for the LAN switch blade, and then select at least one port for which link aggregation has been set up.
- If the target port is not displayed in the external connection port list, clear the "Filter ports by VLAN ID" checkbox. Regardless of the VLAN ID, the ports available for external connections on the LAN switch blade are displayed.

Do not specify these settings for internal networks or for external networks with only rack-mounted servers.

Subnet settings

This setting can be omitted if "Public LAN" is specified for the type.

Enter if you want to automatically set a network and IP address for the NIC connected to the network resource when deploying an image on an L-Server. IP addresses included in subnet addresses are allocated to L-Servers, but it is possible to specify a range of addresses to exclude. Clicking <Add> will display the **[Define start and end IP addresses]** dialog, specify the range of IP addresses to exclude, and click <Add>. To reactivate excluded IP addresses, check the appropriate checkboxes on the list, and click the <Delete>. Clicking the <OK> displays the original dialog with the entered settings.

Network addresses and broadcast addresses are automatically excluded.

Information

If a subnet address has been specified for a network resource, IP addresses can be set up automatically when images are distributed to L-Servers.

If a subnet address has not been specified, the DHCP settings will be used.

Subnet address/mask

Enter the subnet address and subnet mask to be set up using "xxx.xxx.xxx.xxx" format.

The maximum value for the subnet mask is "255.255.255.255" (32-bit mask), and the minimum value is "255.255.0.0" (16-bit mask). However, "255.255.255.254" cannot be specified.

Note

When creating a physical L-Server, specify a different subnet to the admin LAN subnet for the public LAN subnet.

When the physical L-Server is created, the admin LAN will be created by default after this product is installed. Register the default admin LAN IP address as an IP address that will not be a target of allocation. If this is not registered, it may overlap with the IP address of a device that is not a management target of this product.

Default gateway (Optional)

This can be omitted if Admin LAN was not selected as the type.

Enter the IP address for the default gateway to be used when communicating outside the subnet.

Exclusion IP range (Optional)

This item can be used to specify IP addresses that should not be automatically allocated to L-Servers. Reasons for not automatically allocating to an L-Server include because the IP addresses are being used by another device, because there is a plan to use them in future, or for some other reason.

Note

For the IP addresses specified in the subnet addresses and subnet masks, the following addresses are automatically excluded from allocation. They cannot be specified as target IP addresses.

Admin Server

Managed Servers

Network addresses and broadcast addresses

To exclude other IP addresses (such as VM management product or LAN switch blade admin IP addresses), set these as non-target IP addresses.



Information

One admin LAN network resource will be created automatically for the admin network that is specified when this product is installed.

To use two or more admin networks, create two or more admin LAN network resources.

Note that there is no need to register a server resource tree admin LAN subnet.

For details on how to register admin LAN subnets, refer to "6.1.7 Registering Admin LAN Subnets [Windows]" in the "ServerView Resource Coordinator VE Setup Guide".



Label (Optional)

Assign an alias to the network resource that is easy to understand (based on what is used for, for example).

Enter a string that is no more than 32 characters long.

Comment(Optional)

For a comment, you can freely enter information about the network resource. For example, the comment can include detailed information about what the network resource is used for, or what to do if a fault occurs, so that the fault can be resolved quickly.

Enter a string that is no more than 256 characters long.

3. The network resource will be created and registered in the network pool.

Create a network resource using the registered admin LAN subnet

Use the following procedure to create a network resource using the registered admin LAN subnet and register it in a network pool.

1. In the RC console orchestration tree, right-click the target network pool, and select [Create Resource]-[Using existing admin subnet] from the popup menu.

The [Create a network resource] dialog is displayed.

2. Enter the items below, and click <OK>.

Network resource name

Clicking <Select> displays the [Select a subnet for the admin LAN] dialog.

Select an already configured admin LAN subnet.

When the selected admin LAN subnet has no name, enter the name of a network resource for "*Network resource name*".

Enter up to 32 characters beginning with an alphanumeric character (upper or lower case), and including alphanumeric characters (upper or lower case), underscores ("_"), periods ("."), or hyphens ("-").

Click the <OK>.

Type

"Admin LAN" is displayed.

VLAN ID/Uplink port settings

Refer to "VLAN/External" Connection Port Settings" of "[Create a new network resource](#)" for details.

Subnet settings (Optional)

Refer to "Subnet settings" of "[Create a new network resource](#)" for details.

Label (Optional)

Refer to "Label" of "[Create a new network resource](#)" for details.

Comment (Optional)

Refer to "Comment" of "[Create a new network resource](#)" for details.

3. The network resource will be created and registered in the network pool.

4.3.2.4 Virtual Image resources

This section explains how to register the cloning master in the image pool.

If the image (template) has already been created in the VM management product, use the following procedure to register it in the image pool.

1. In the RC console orchestration tree, right-click the target image pool, and select [**Register Resources**] from the popup menu. The [**Register Resources**] dialog box will be displayed.
2. Select the cloning image to register and click the <OK>. The cloning master will then be registered.



For an image (template) that has already been created in the VM management product, change the template name as shown below so that it can be handled in this product.

- Delete everything except the alphanumeric characters and underscores ("_").
- Where the first character is not an alphanumeric character, delete the characters up to the first alphanumeric character.

4.3.3 Creating and Managing L-Server Templates

L-Server Templates are templates that define the specifications for an L-Server in advance (such as the number of CPUs, memory capacity, disk capacity, and the number of NICs). L-Server Templates are marked up in XML format.

To create an L-Server Template, export the sample L-Server Template that comes with this product as a standard template, and then edit the L-Server Template that is output. When the edited L-Server Template is imported, a new L-Server Template will be created.



Use "UTF-8" as the character encoding for L-Server Templates.

Exporting L-Server Templates

Use the following procedure to export an L-Server Template.

1. Select the RC console orchestration tree..
On the [**Template List**] tab, right-click the L-Server template to export and select [**Export**] from the popup menu.
Displays the [**File Download**] dialog
2. Click the <Save>.
The L-Server Template will be exported.

Editing L-Server Templates

Edits an L-Server template. For details on the XML definition of L-Server template, refer to "2.2 L-Server Template" in the "ServerView Resource Orchestrator Reference Guide".

If a template is imported without editing the L-Server template name (L-Server Template name) of the L-Server template file, the content

of the existing L-Server template is overwritten. If an L-Server template is imported after the name is edited from when it was exported, the L-Server template is added.

Importing L-Server Templates

Use the following procedure to import an L-Server Template.

1. Select [**File**] - [**L-Server Template**] - [**Import**] from the RC console menu.
2. Specify the file name, and click the <**OK**>.
The L-Server template is imported.

When a registered L-Server template name is included in the specified file, a warning dialog is displayed to confirm whether or not to overwrite the L-Server template.

When overwriting it, click the <**OK**>.

When not overwriting it, click the <**Cancel**> and return to the dialog to specify the file name.

Deleting L-Server Templates

L-Server Templates that are no longer required can be deleted (including the standard L-Server Templates that are provided with this product).

Use the following method to delete the unnecessary L-Server Templates.

On the [**Template List**] tab, right-click the L-Server template to delete, and select [**Delete**] from the popup menu.

From the command-line, execute `rcxadm template delete`.

4.3.4 Creating and Managing L-Servers

This section explains how to create and manage the L-Server.

4.3.4.1 Creating an L-Server

L-Servers are created using L-Server Templates. Separate explanations are given for each of the following cases.

- If a cloning master is not stored in an image pool, or if a cloning master that has already been registered is not used, use the following procedure. For the image, specify <None>.

1. Create the L-Server
2. Install the operating system manually
3. Install the business server agent
4. Take the cloning master

- If a cloning master is stored in an image pool

For the image, specify the cloning master to be distributed. An L-Server will be created based on the cloning master distributed.

1. Create the L-Server

[VMware]

For steps 1, 2 and 4, refer to "G.1.5 Creating L-Server" in the "ServerView Resource Orchestrator User's Guide" and then create the L-Server.

For step 3, refer to "[3.3 Installing on the VM Server](#)".

[Hyper-V]

For steps 1, 2 and 4, refer to "G.2.5 Creating L-Server" in the "ServerView Resource Orchestrator User's Guide" and then create the L-Server.

For step 3, refer to "[3.3 Installing on the VM Server](#)".

4.3.4.2 Managing L-Servers

The L-Server that has been created can be viewed from the RC Console. This means that the RC Console can also be used to reconfigure or delete the L-Servers that have been created. For details, refer to "6.3 Modification" and "6.5 Deleting an L-Server" in the "ServerView Resource Orchestrator User's Guide" that comes with this product.

4.3.5 Creating, Registering and Deleting System Templates

Next, create and register verified system configurations as system templates, which are required to create systems.

Note that system templates can be manipulated using the GUI in the Manager View, as well as using commands.

Refer to the "Systemwalker Software Configuration Manager User's Guide (template Manager Edition) " for information on operations using the GUI in the Manager View.

System template registration procedure

The service provider makes the system template usable by registering various types of information as required.

The following information is registered:

- [Software information](#)
- [Image information](#)
- [Segment information](#)
- [Template information](#)



Point

Perform the following operations to check whether information has been correctly registered or set up using the information registration or setup commands.

- Check the return value of the command.

If the return value is 0, the command has terminated normally.

If the return value is other than 0, the command has terminated abnormally and an error message is output.

- Check using the corresponding display command in the following table.

Registration or setup command	Display command
Software information registration command (cfmg_addsoft)	Software information list display command (cfmg_listsoft)
Image information registration command (cfmg_addimageinfo)	Image information list display command (cfmg_listimageinfo)
Segment registration command (cfmg_addnetinfo)	Segment list display command (cfmg_listnetinfo)
Template information registration command (cfmg_addtemplate)	Template information list display command (cfmg_listtemplate)

Software information

Use the following procedure to register the software information included in the image that is used by the system template if it has not been registered yet.

1. Create a software information file (an XML file) that marks up configuration information for the software included in the image.

It is also possible to use a software information file that has already been registered. Refer to "[Appendix H Registered Software IDs](#)" for details.

Refer to "[Detailed explanation of software information](#)" for details on software information.

2. Use the software information registration command (cfmg_addsoft) to register the software information file.

A separate software information file is registered for each type of software. (If there is more than one type of software, create a file for each type of software.)

Image information

Use the following procedure to register image information if it has not been registered with the virtual image that is used by the system template.

1. Use the virtual image list display command (cfmg_listvmimage) to check the virtual image where the image information will be registered.
2. Create an image information file (an XML file).
Samples are available, so refer to these samples when creating the file.
Refer to "[Detailed explanation of image information](#)" for details on image information and the location where the samples are stored.
3. Use the image information registration command (cfmg_addimageinfo) to register the image information.

Segment information

To restrict the virtual networks used by this product, use the following procedure to register segment information.

1. Use the virtual network list display command (cfmg_listvnet) to check the virtual network where the segment information will be registered.
Take note of the resource ID recorded in the <networks>/<network>/<id> tag.
2. Create a segment information file (an XML file).
In the <id> tag, specify the resource ID that was noted in Step 1.
Refer to "[Detailed explanation of segment information](#)" for details on segment information.
3. Use the segment registration command (cfmg_addnetinfo) to register the segment information.



Note

- If segment information is not registered, all of the virtual networks registered with Cloud Infrastructure Management Software will be deployed.
If [**automatically select**] is specified for the deployment destination virtual network, the deployment destination will be selected from all of the virtual networks.
- When registering segment information, register segment information for all of the virtual networks used by the system template.
If [automatically select] is specified for the deployment destination virtual network, the deployment destination will be selected from the virtual networks for which "**business segment**" has been specified.

Template information

Use the following procedure to register template information.

1. Use the following commands to check the information used by the template.
 - Segment information: Segment list display command (cfmg_listnetinfo)
 - Image information: Image information list display command (cfmg_listimageinfo)
2. Create a template information file (an XML file).
Samples are available, so refer to these samples when creating the file.
Refer to "[Detailed explanation of template information](#)" for details on template information and the location where the samples are stored.
3. Use the template information registration command (cfmg_addtemplate) to register the template information.

4. The default publication setting for system templates is **Hidden**.

To make a system template available to system users, use the system template publication setting command (cfmg_showtemplate) to change the publication settings.

Refer to "[System template publication setup command](#)" for details on this command.

Note

- A virtual systems that has already been deployed is not affected even if the publication setting for the system template that it uses is changed to **Hidden**.
- It is also possible to change the publication setting to **Hidden** if you do not want users to deploy virtual systems using the target system template.

Deleting system templates

Service providers can delete various types of information as necessary.

- [Template information](#)
- [Segment information](#)
- [Image information](#)
- [Software information](#)

Note

- If the following information files have been associated with multiple template information files, all of the template information files associated with these information files must be deleted before each of these information files can be deleted.
 - Image information
 - Segment information
- Before deleting a software information file, delete all of the image information files with which that software information file has been associated.
- Do not delete template information files that are being used in a deployed system.

Point

Perform the following operations to check whether information has been correctly deleted using the deletion command for each information type.

- Check the return value of the command.
 - If the return value is 0, the command has terminated normally.
 - If the return value is other than 0, the command has terminated abnormally and an error message is output.
- Check using the corresponding display command in the following table.

Deletion command	Display command
Template information deletion command (cfmg_deletetemplate)	Template information list display command (cfmg_listtemplate)
Segment deletion command (cfmg_deletenetinfo)	Segment list display command (cfmg_listnetinfo)
Image information deletion command (cfmg_deleteimageinfo)	Image information list display command (cfmg_listimageinfo)

Deletion command	Display command
Software information deletion command (cfmg_deletesoft)	Software information list display command (cfmg_listsoft)

Template information

Use the following procedure to delete template information.

1. Check the template name displayed in Manager View, "*System Manager*", "*System list*", and ensure that the template information to be deleted is not being used in a deployed system.

Use the Template information list display (cfmg_listtemplate) command, and take a note of the name of the template ID that corresponds to the template name in step 1.

2. If the publications setting is **Published**, the template information cannot be deleted.

In this case, the publication setting must be changed to **Hidden** using the system template publication setting command (cfmg_showtemplate).

Refer to "[System template publication setup command](#)" for details on this command.

3. Use the template information deletion command (cfmg_deletetemplate) to delete the template information by specifying the template ID that was noted in Step 1.

Segment information

Use the following procedure to delete segment information.

1. Use the Template information list display (cfmg_listtemplate -v) command to output a list of template information, and use this to see if the segment configuration information to be deleted is associated with template information in the "`<template>/<vnets>/<vnet>/<id>`" tag.
2. Use the segment deletion command (cfmg_deletenetinfo) to delete the segment information.

Image information

Use the following procedure to delete image information.

1. Use the template information list display command (cfmg_listtemplate -v) to output a list of template information, and check the `<template>/<servers>/<server>/<imageId>` tag to see that the image information to be deleted is not associated with the template information.
2. Use the image information deletion command (cfmg_deleteimageinfo) to delete the image information.

Software information

Use the following procedure to delete software information.

1. Use the image information list display command (cfmg_listimageinfo -v) to output a list of image information, and check the "`<image>/<softwares>/<software>/<id>`" tag to see that the software information to be deleted is not associated with the image information.
2. Use the software information deletion command (cfmg_deletesoft) to delete the software information.

4.3.6 Publishing and Deleting Services

This section explains how to publish and delete services that are leased to service users.

The definitions that clarify the content and status of a service to be leased to service users are referred to as the "service specification".

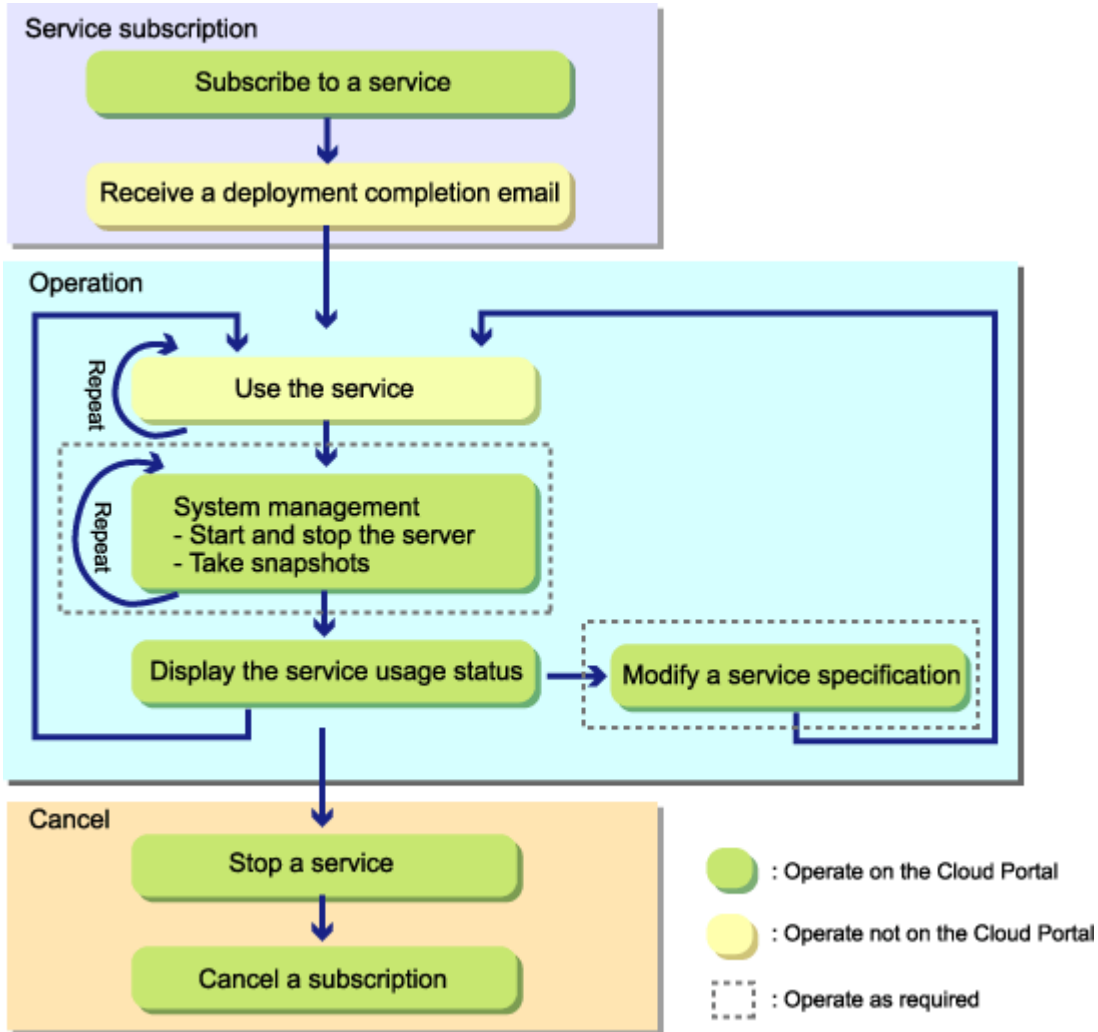
To publish a service specification, register and publish the system template information.

To display prices for the service specifications that are displayed in the **[Search service]** page of MyPortal, it is necessary to register accounting information using the product master maintenance command provided by this product.

System templates can be registered using the `cfmg_addtemplate` command, published as service specifications using the `cfmg_showtemplate` command, and deleted using the `cfmg_deletetemplate` command.

4.4 Applying to Use Services and Returning Services (for Service Users)

This section explains the flow of operations performed using the Cloud Portal ranging from service subscription through to subscription cancellation.



1. Apply to use the service
Service users use the MyPortal function of the Cloud Portal to apply to use services.
For details, refer to "2.2 Subscribe to a Service" in the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Users" that comes with this product.
2. Receiving deployment completion emails
When the service that the service user has applied to use has been deployed, a deployment completion email is sent to that user. Deployment completion emails contain the information required to access the service.
3. Use the service
Access and use the service in accordance with the information in the deployment completion email.
4. Manage the system
If necessary, use the MyPortal function of the Cloud Portal to start and stop the virtual servers that make up the service being used, or to take snapshots.
For details, refer to "2.3 System Management" in the "Systemwalker Service Catalog Manager V14g Infrastructure service Function Operation Guide for Users" that comes with this product.

5. Display the service usage status
Use the Cloud Portal to check the usage status of the service being used.
For details, refer to "Chapter 5 Usage Status" in the "Systemwalker Service Catalog Manager V14g Infrastructure service Function Operation Guide for Users" that comes with this product.
6. Change the service specification
Change the service specification for the service being used according to the service usage status. For example, if there is not enough disk space, use the MyPortal function of the Cloud Portal to change the service specification by adding disks. Refer to "2.3.7 Modify s Specification" in the "Systemwalker Service Catalog Manager V14g Infrastructure service Function Operation Guide for Users" that comes with this product.
7. Stop the service
Use the MyPortal function of the Cloud Portal to stop the virtual servers that make up services that are no longer required.

Refer to "2.3.4 Start and Stop the Virtual Server" in the "Systemwalker Service Catalog Manager V14g Infrastructure service Function Operation Guide for Users" that comes with this product.
8. Cancel the service
Use the MyPortal function of the Cloud Portal to cancel the service that is no longer required.

Refer to "2.3.8 Cancel a Subscription" in the "Systemwalker Service Catalog Manager V14g Infrastructure service Function Operation Guide for Users" that comes with this product.

4.5 Approving and Checking Applications to Use Services

When applications to use services are submitted, it is possible to have the administrator of the service user department approve the application, and to have the service provider (the administrator of the service provider department) to assess the application.

Operations that approve and assess applications are provided as an "application process" service by the service provider that lease ICT resources.

1. Select the forwarding destinations for application processes.

Once an application process has been correctly registered with the system and enabled, forwarding destinations can be selected from the **[License Agreement]** window for applying to use the service, and notifications can be sent to approvers.

For details on how to select forwarding destinations for application processes, refer to "2.5 Select Forward Destination of Application Process" in the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Users" that comes with this product.

2. Approve the applications.

The approver approves the application process. The *approver* is the administrator of the service user department that was specified as the forwarding destination when the application was made.



Point

.....
If the application process has been set up so that approval is required, the approver will need to approve the application process. When the application process is forwarded, an approval request email is sent to the approver.
.....

For details, refer to "4.3 Approve Application" in the "Systemwalker Service Catalog Manager V14g Infrastructure service Function Operation Guide for Users" that comes with this product.

3. Assess the applications.

The assessor assesses the application process. The *assessor* is the service provider (the administrator of the service provider department).



Point

.....
If the application process has been set up so that assessment is required, the assessor will need to assess the application process. When the application process is forwarded, an assessment request email is sent to the assessor.
.....

For details, refer to "8.2 Application Assessment" in the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Administrators" that comes with this product.

4. Check the status of the applications to use services.

The service user who made the application to use the service can check the status of the application.

To check the status, log in and then select [**Application list**] from either the Operation menu or the toolbar for the Cloud Portal. For details, refer to "4.1 Check Application Status" in the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Users" that comes with this product.

The service provider can check the status of the applications to use services.

To check the status, log in and then select [**Assessment**] from the Operation menu for the Operation Portal. For details, refer to "8.1 Check Assessment Status" in the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Administrators" that comes with this product.

4.6 Visualizing ICT Resources

This section explains the information that infrastructure administrators, service providers and service users can look up.

Tracking the resource status for infrastructure administrators

Infrastructure administrators can use the RC Console to check the status of resources.

Refer to "[A.4 RC Console](#)" for details on the RC Console.

Tracking the resource status for service providers

Service providers can use the cloud infrastructure administrator dashboard function to monitor information such as the availability status of resource pools and resource information about virtual platforms (VMs). This function allows users to specify thresholds for the monitored data, so that alerts are notified automatically when the thresholds are exceeded.

For details, refer to "Appendix A To Customize the Cloud Operation Management Dashboard" of the "Systemwalker Service Catalog Manager V14g Cloud Operation Management Dashboard User's Guide" that comes with this product.

Metering the resources for service providers

As a way of metering ICT resources, service providers can use the Operation Portal to check how long resources have been used for and how much has been consumed. Service providers can also quantify the amount of service that service users have used. Reports can be generated by tallying how many servers have been used, and how much CPU, disk and memory resources have been consumed.

To display the Operation Portal, perform the following operations:

1. Start a Web browser.
2. Specify the URL of the Operation Portal.

The URL format is shown below.

```
URL: http://<Host name or IP address of the Admin Server>:<80 (Port number of the Web server)>/op_portal
```

The top page of the Operation Portal will be displayed.

For details, refer to "Chapter 7 Usage Status" in the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Administrators" that comes with this product.

Tracking the usage status for service users

Service users can display and check the usage status of the services that they are using, by logging in and then selecting [**Usage Status**] from either the Operation menu or the toolbar for the Cloud Portal. The following information can be looked up:

- Service usage time
- CPU usage time
- Disk usage

- Memory usage
- Network usage

For details, refer to "Chapter 5 Usage Status" in the "Systemwalker Service Catalog Manager V14g Infrastructure Service Function Operation Guide for Users" that comes with this product.

4.7 Managing Accounting Information

This section explains the accounting information that is managed and operated by CIMS.

"Accounting information" is the information that is required to display prices for service specifications in MyPortal.

The following functions are available for managing accounting information for this product.

- Managing accounting information for service specifications

This function manages accounting information for the service specifications.

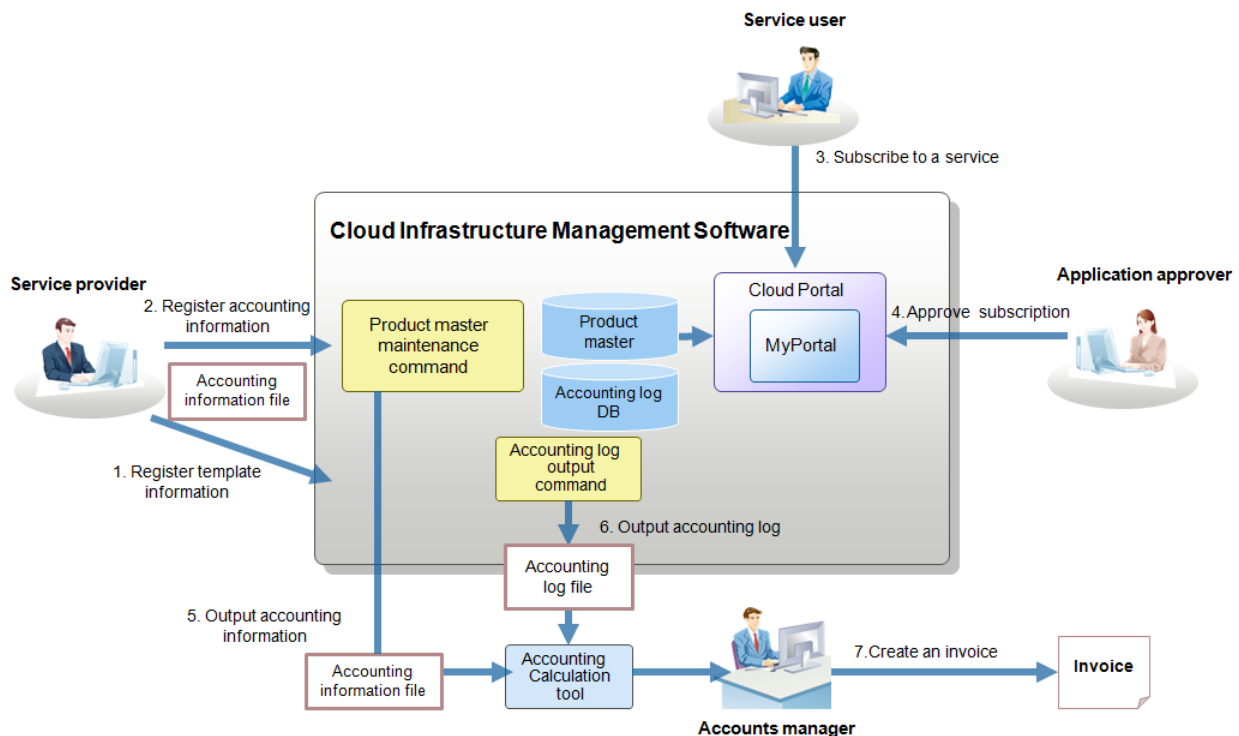
The database that stores accounting information for service specifications is referred to as the *product master*.

- Outputting change histories for service specifications

This function outputs change histories for virtual servers, disks, and configuration information for the virtual systems in service specifications.

Overview of operations

The following diagram presents an overview of operations that manage accounting information for CIMS.



Accounts manager: A user in charge of checking the charges regularly and performs tasks such as sending an invoice to the user department.
Accounting calculation tool: Tool prepared by the provider department.

Management and operation of accounting information by the provider department administrator

1. The provider department administrator registers template information using the template management command supplied by CIMS.
2. The provider department administrator registers the accounting information using the product master maintenance command supplied by CIMS.

Operation in the user department

3. The subscriber references the monthly charges (approximate) of the service specifications displayed on MyPortal of CIMS, and apply to use the service.
4. The approver references to the monthly charges (approximate) of the service specifications displayed in the subscription list on Cloud Portal of CIMS, then approves or rejects the subscription.

Accounting calculation by the accounts manager

5. The accounts manager obtains the accounting information file using output function of product master maintenance command.
6. The accounts manager obtains the accounting log files using accounting log output command..
7. The account manager creates billing statements based on the accounting information file and the accounting log file regularly by using the accounting calculation tool provided by the provider department, and sends them to the user departments.



Point

About the accounting calculation tool

The accounting calculation tool is a tool to calculate the amount charged to each user department based on the accounting information file

and accounting log file. It is recommended to customize it so that it suits to the accounting policy, by not charging to CPUs and memories.

For details, refer to "Chapter 9 Accounting" in the "Systemwalker Service Catalog Manager V14gInfrastructure service Function Operation Guide for Administrators" that comes with this product.

4.8 Backing up or Restoring the Admin Server

This section explains the methods for backing up and restoring the Admin Server.

4.8.1 Notes on Backing up and Restoring the Admin Server

This section provides notes on executing backup and restore.

- Notes on the environment in which backup and restore are executed
- Treatment of backup resources
- Treatment of restore resources



Note

System administrator (superuser) privileges are required to execute the commands.

Notes on the environment in which backup and restore are executed

- The backup and restore environment must meet the following requirements to execute backup and restore:
 - The operating systems are the same.
However, the version of the operation systems may not be the same.
 - The host information (host name and IP addresses) is the same.
 - The character codings are the same.
 - The repository servers are the same.
 - The directories storing the CMDB database are the same.
- The items set by using the set menu on the screen of the Cloud Operation Management Dashboard are not backed up and not restored.

Treatment of backup resources

- To move the backup resources, move the folders(directories) specified as the backup destination and all the folders(directories) and files located under those folders(directories).
- Do not delete the backup resources located under the folders(directories) specified as the backup destination until the restore operation is completed.
- The backup command cannot be used to save data to the following media:
 - Saving data to an optical disk such as CD-R or DVD-R
To save data to an optical disk, save the data to a local disk, then, write the saved data to the media using a dedicated writer etc.
 - Saving data to a folder(directory) that contains a space

Treatment of restore resources

The restore command cannot be used to restore data from the following media:

- Restoring data from a directory that contains a space

4.8.2 Backing up the Admin Server

Before backing up, CIMS System (Manager) must be stopped.

At this point, also back up the Interstage Single Sign-On resources that manage user information. The following tasks apply:

1. Stopping the CIMS Systems
2. Backing up CIMS Resources
 - a. Backing up the CIMS Resources (Resources for the Self Service Portal)
 - b. Backing up the CIMS Resources (Configuration Management Resources)
 - c. Backing up the CIMS Resources (Application Process Resources)
 - d. Backing up the CIMS Resources (Interstage Single Sign-On Resources)
 - e. Backing up the CIMS Resources (Resource Pool Management Resources)
3. Starting the CIMS System

4.8.2.1 Stopping the CIMS Systems

Stop the CIMS System (the Manager) by executing the following command.

[Windows]

```
<CIMS installation folder>\cims\Manager\bin\cims mgrctl stop
```

The processing results are output to the standard output. If the return value is 0, the command has terminated normally and the system has stopped.

Processing result	Return value
Normal termination	0
Error	Other than 0

Checking the system status

Check that the Manager and the service from this product have stopped. Refer to "[G.1.2 Manager Control Commands](#)" for information on how to check the status.

4.8.2.2 Backing up the CIMS Resources (Resources for the Self Service Portal)

Backup the databases and various definition files relating to resources for the Self Service Portal function by executing the following command. Create a new directory (folder) to store the resources, making sure that the directory name does not include spaces.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWCTMG\bin\swctmg_backup.bat <Storage folder>
```

4.8.2.3 Backing up the CIMS Resources (Configuration Management Resources)

Backing up the configuration management resources

Back up the various definition files and the database relating to configuration management resources by executing the following command. For the storage directory (folder), specify a directory that does not exist.

[Windows]

1. Stop the database.

```
net stop "Systemwalker Software Configuration Manager DB Service"
```

2. Perform a backup.

```
<CIMS installation folder>\Systemwalker\SWCFMG\bin\cfmg_backup <Storage folder>
```

3. Start the database.

```
net start "Systemwalker Software Configuration Manager DB Service"
```

4.8.2.4 Backing up the CIMS Resources (Application Process Resources)

Backing up the application process resources

[Windows]

The following example shows the operations for backing up resources to the folder "X:\Backup\swrba".

1. Create the following folder.

```
mkdir X:\Backup\swrba
```

2. Execute the following command to back up the resources.

```
<CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_backup X:\Backup\swrba
```

4.8.2.5 Backing up the CIMS Resources (Interstage Single Sign-On Resources)

Backing up the Interstage Single Sign-On resources

[Windows]

1. Stop the Interstage Single Sign-On

```
<CIMS installation folder>\Systemwalker\SWRBAM\sso\bin\ssoclservicectl stop
```

2. Execute the following command to back up the resources.

```
<CIMS installation folder>\Systemwalker\SWRBAM\sso\bin\ssoclbakup <Storage folder>
```

3. Start the Interstage Single Sign-On

```
<CIMS installation folder>\Systemwalker\SWRBAM\sso\bin\ssoclservicectl start
```

4.8.2.6 Backing up the CIMS Resources (Resource Pool Management Resources)

Note

- For second and subsequent backups, the folders and configuration definition information from previous backups can be safely deleted after the new backup has been taken. Delete these folders and definition information to free up disk space if necessary
- Do not perform backups while backing up or restoring system images, or while taking or distributing cloning masters

- Backing up the configuration definition information.

Export configuration definition information by executing the following command.

Use the "-dir" option to specify the storage directory to which the configuration definition information and version information XML file is to be exported.

If the storage directory does not exist, a new directory will be created.

If the storage directory already exists and the "-overwrite" option is specified, the XML file will be overwritten. An error will occur if "-overwrite" is not specified.

[Windows]

```
<CIMS installation folder>\Resource Orchestrator\Manager\bin\rcxbackup -dir <Storage folder> [-  
overwrite]
```

Note

Specify the absolute path to the command.

Note the following when specifying directories.

- Do not specify the system installation directory for the "-dir" option.
- Do not specify directories that include the following symbols for the "-dir" option:

```
""", "|", ":", "!", " ", "?", " /", " .", "<", ">", " ", "%", "&", "^", "=", "!", " ", "#", " ", "+", "[", "]", "{", " }"
```

When transferring the backup data (the directory specified by the "-dir" option) to an FTP server or some other destination, first use ZIP or some other method to compress the backup data into a single file before transferring it.

When restoring from the backup data, note that all of the configuration definition information and definition files must have been backed up at the same time. It is recommended that the backup data be stored together in a directory with a name that indicates the date and time when the backup was taken.

- Execution conditions

Configuration definition information cannot be backed up while operations are being performed on resources such as L-Servers, resource pools, and resource folders. Stop the Manager before executing backups.

Note that the following information is not restored as part of the restoration process. Take the appropriate action that matches the information below.

- Maintenance mode status

Maintenance mode will be canceled after restoration. If you take a backup when maintenance mode has been set up, record the maintenance mode status for each Managed Server before taking the backup.

- Power consumption data for power monitoring devices

Power consumption data for power monitoring devices cannot be restored. It is recommended that power consumption data be output before reinstalling the Manager. Refer to the article on power consumption data output in the "ServerView Resource Coordinator Ve Operation Guide" for information on the operation method.

- Backing up SystemcastWizard-related information

[Windows]

Back up the following data to any desired folder.

For files and databases, simply copy the data to the folder. For registries, use the registry editor to export all of the following keys.

No	Type	Backup/restoration target
1	Registry (*1)	HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard(32bitOS) HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard(64bitOS)
2	Database	<CIMS installation folder>\Resource Orchestrator\ScwPro\scwdb\scwdb1.mdb <CIMS installation folder>\Resource Orchestrator\ScwPro\scwdb\scwdb1.mdw
3	DHCP settings file	<CIMS installation folder>\Resource Orchestrator\ScwPro\bin\ipTable.dat
4	IP address settings file	<CIMS installation folder>\Resource Orchestrator\ScwPro\bin\localipaddress.txt
5	AWWN definition file	<CIMS installation folder>\Resource Orchestrator\ScwPro\tftp\rcbooting _awwn_XXX.XXX.XXX.XXX.cfg (*2) <CIMS installation folder>\Resource Orchestrator\ScwPro\tftp\rcbooting _awwn_XXX.XXX.XXX.XXX.cfg (*2)

*1: For 64-bit operating systems, this registry redirects to Wow6432Node.

*2: Here "XXX.XXX.XXX.XXX" represents an IP address.

- Backing up various definition files

The various definition files that were created when this product was used will be erased during uninstallation.

If necessary, back up (copy) the following folder to another folder before uninstalling this product.

[Windows]

```
<CIMS installation folder>\Resource Orchestrator\Manager\etc\customize_data
```

4.8.2.7 Starting the CIMS System

Start this product (the Manager) by executing the following command.



Note

- The Manager starts automatically when the Admin Server is started.

[Windows]

```
<CIMS installation folder>\cims\Manager\bin\cims mgrctl start
```

The processing results are output to the standard output. If the return value is 0, the command has terminated normally and the system has started.

Processing result	Return value
Normal termination	0
Error	Other than 0

Checking the system status

Check the startup status of the Manager. Refer to "[G.1.2 Manager Control Commands](#)" for details.

4.8.3 Restoring the Admin Server

This section explains how to restore backed up resources.

1. Stopping the CIMS System
2. Restore the CIMS Resources
 - a. Restoring the CIMS Resources (Resource Pool management Resources)
 - b. Restoring the CIMS Resources (Application Process Resources and Interstage Sigle Sign-On Resources)
 - c. Restoring the CIMS Resources(Configuration Management Resources)
 - d. Restoring the CIMS Resources (Resources for the Self Service Portal)
3. Starting the CIMS System
4. Updating the CMDB for CIMS

4.8.3.1 Stopping the CIMS System

Use the command for stopping the system in the same way as when the Admin Server is backed up. Refer to "[G.1.2 Manager Control Commands](#)" for details.

4.8.3.2 Restoring the CIMS Resources (Resource Pool Management Resources)

Restoring SystemcastWizard-related information

[Windows]

Restore the backup data (that was backed up to an arbitrary folder) to the following locations.

For files and databases, simply copy the data. For registries, use the registry editor to import the registry file data that was backed up.

No	Type	Backup/restoration target
1	Registry (*1)	HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\SystemcastWizard(32bitOS) HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Fujitsu\SystemcastWizard(64bitOS)
2	Database	<CIMS installation folder>\Resource Orchestrator\ScwPro\scwdb\scwdb1.mdb <CIMS installation folder>\Resource Orchestrator\ScwPro\scwdb\scwdb1.mdw
3	DHCP settings file	<CIMS installation folder>\Resource Orchestrator\ScwPro\bin\ipTable.dat
4	IP address settings file	<CIMS installation folder>\Resource Orchestrator\ScwPro\bin\localipaddress.txt
5	AWWN definition file	<CIMS installation folder>\Resource Orchestrator\ScwPro\tftp\rcbooting \awwn_XXX.XXX.XXX.XXX.cfg (*2) <CIMS installation folder>\Resource Orchestrator\ScwPro\tftp\rcbooting _awwn_XXX.XXX.XXX.XXX.cfg (*2)

*1: For 64-bit operating systems, this registry redirects to Wow6432Node.

*2: Here "XXX.XXX.XXX.XXX" represents an IP address.

Restoring configuration definition information

Restore the configuration definition information that was backed up using the procedure in "Backing up configuration definition information" under "[4.8.2.6 Backing up the CIMS Resources \(Resource Pool Management Resources\)](#)".

Execute the following command.

[Windows]

```
<CIMS installation folder>\Resource Orchestrator\Manager\bin\rcxrestore -dir <Storage folder>
```

Note

Specify the absolute path to the command.

Restoring various definition files

Restore various definition files.

Restore the backup data (that was backed up to an arbitrary folder) to the following locations.

[Windows]

```
<CIMS installation folder>\Resource Orchestrator\Manager\etc\customize_data
```

Note

- Do not perform restoration while backing up or restoring system images, or while taking or distributing cloning masters.
- For the configuration definition information and various definition files, restore data that was backed up at the same time.
- Restorations can be performed only if the following hardware settings and configurations have not been changed since the backup was taken.
 - Chassis, the LAN switch blades, Managed Servers, or the power monitoring devices (Hardware replacement)
 - NICs for Managed Servers (NIC replacement)
 - The LAN connection between Managed Servers and the LAN switch blade
 - Ongoing operations following server failover (*1)
- *1: Restoration can be performed if the operation has failed back to the original server after the failover.
- Maintenance mode settings will not be restored after restoration. Set up maintenance mode in accordance with the information that was recorded before the back up was taken.
- Information for the LAN switches and the connections on the network map cannot be backed up. Collect LAN switch registration and connection information, by referring to the article on network map preparations in the "ServerView Resource Coordinator VE Operation Guide".

4.8.3.3 Restoring the CIMS Resources (Application Process Resources and Interstage Single Sign-On Resources)

Canceling the setup for application process resources

Cancel the setup in order to restore the application process resources.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_setup -u
```

Restoring the Interstage Single Sign-On resources

This section explains the procedure for restoring Interstage Single Sign-On resources.

[Windows]

1. Stop the Interstage Sigle Sign-On

```
<CIMS installation folder>\Systemwalker\SWRBAM\sso\bin\ssoclservicectl stop
```

2. Execute the following command to restore the resources.

```
<CIMS installation folder>\Systemwalker\SWRBAM\sso\bin\ssoclrestore <Storage folder>
```

3. Start the Interstage Sigle Sign-On

```
<CIMS installation folder>\Systemwalker\SWRBAM\sso\bin\ssoclservicectl start
```

Setting up application process resources

Execute the setup to create application process resources. For the parameters that are set during setup, set the same parameters as for when the backup was taken.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_setup -s
```

Restoring application process resources

[Windows]

The following example shows the operations for restoring the resources that have been backed up to the folder: "X:\Backup\swrba".

1. Stop the application process function.

```
<CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_stop
```

2. Execute the following command to restore the resources. When the restoration processing has completed successfully, a completion message is displayed.

```
<CIMS installation folder>\Systemwalker\SWRBAM\bin\swrba_restore X:\Backup\swrba
```

4.8.3.4 Restoring the CIMS Resources(Configuration Management Resources)

Restore the various definition files and the database relating to configuration management resources by executing the following command.

[Windows]

1. Stop the configuration management function. Be sure to execute the commands in the following order.

```
isstopwu CFMG_ManagerView  
isstopwu CFMG_VSYS
```

2. Stop the database.

```
net stop "Systemwalker Software Configuration Manager DB Service"
```

3. Perform restoration.

```
<CIMS installation folder>\Systemwalker\SWCFMG\bin\cfmg_restore <Storage folder>
```

4. Start the database.

```
net start "Systemwalker Software Configuration Manager DB Service"
```

4.8.3.5 Restoring the CIMS Resources (Resources for the Self Service Portal)

Restore the databases and various definition files relating to resources for the Self Service Portal function by executing the following command. Paths that contain spaces cannot be specified for the storage directory.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWCTMG\bin\swctmg_restore.bat <Storage folder>
```

4.8.3.6 Starting the CIMS System

Use the command for starting the system, in the same way as when the Admin Server is backed up. Refer to "[G.1.2 Manager Control Commands](#)" for details.

4.8.3.7 Updating the CMDB for CIMS

Update the CMDB data by executing the following command.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin\cmdbrefresh.exe -a -q
```

Appendix A ICT Resource Management Functions

This appendix explains the ICT resource management functions.

A.1 Resource Pools

A resource pool is a bundle of all resources of the same type (such as virtual servers, storage, networks, or images).


Introducing resource pools has the following benefits.


Until now, it was necessary to purchase new resources such as servers, storage, and networks every time a business activity was expanded or a new business activity was introduced. This involves a lot of effort, first to get approval for the purchase, then to arrange to purchase the resources, then to create environments, and so on. By introducing this product, servers can be created by simply pulling the necessary resources out of resource pools. This eliminates the need for the time and effort discussed above, and allows infrastructure environments to be created and operated according to plan.

Resource pool management is a function for utilizing resources effectively without waste. There are several types of resource pool, as shown below. Pre-registering the resources controlled by this product in resource pools makes it possible to create servers (including storage and networks) rapidly by pulling out the appropriate resources from resource pools in response to user requests. If a server is no longer required, the resources can be released and set aside for reuse.

Multiple resource pools can be created, according to the operation requirements (such as separate resource pools for different hardware types, security levels or resource management units). If a resource pool runs out of resources, new resources can be added or resources can be moved from other resource pools.

Table A.1 Types of resource pool

Type of resource pool	Overview
VM	<p>VM pools are resource pools for storing the VM hosts that are used when new servers (VMs) are created.</p> <p>VM pools can store VM hosts for different server virtualization software products.</p> <p>With VM pools that include a mix of different server virtualization software products, if you specify a VM type when creating an L-Server, the appropriate VM host will be selected to create the L-Server.</p> <p>In environments in which multiple cluster groups have been registered in the same VM pool, it is only possible to migrate the L-Server between VM hosts belonging to the same cluster.</p>
Server	<p>Server pools are resource pools for storing the physical servers that are used when new servers are created.</p> <p> Note</p> <p>.....</p> <p>Although displayed as a resource pool, this resource pool type cannot be used in Cloud Infrastructure Management Software.</p> <p>.....</p>
Storage	<p>Manages virtual storage resources and disk resources in this product.</p> <p>'Virtual storage resources' refers to the file system that is used for VM guests which are controlled by VM management products such as RAID groups, which themselves are controlled by the storage management products.</p> <p>These can be managed as virtual storage resources using a common operation.</p> <p>'Disk resources' refers to the disk that is allocated to the server.</p> <p>In the case of the VM guest, this is equivalent to the virtual disk.</p> <p>In this product, disk resources are allocated to the L-Server using the following methods:</p> <ul style="list-style-type: none"> - Pulling out disk resources of the required size from the virtual storage resources and then allocating them to the L-Server.

Type of resource pool	Overview
	<ul style="list-style-type: none"> - Assigning the disk that has already been created on the storage management product to the L-Server. <p>The following virtual storage resources are stored in the storage pool:</p> <ul style="list-style-type: none"> - Storage for VMs File systems for creating VMs and virtual disks, such as VMFS (data store) file systems for VMware and cluster shared volumes for Hyper-V
Network	<p>Network pools are resource pools for storing network resources that define the networks to be connected to servers.</p> <p>Refer to Section 1.2.6, "Simplifying Network Settings" in the "ServerView Resource Orchestrator User's Guide" for details on network resources.</p>
Address	<p>The following resources are stored in this type of resource pool.</p> <ul style="list-style-type: none"> - MAC addresses - WWN <p> Note</p> <hr style="border-top: 1px dotted orange;"/> <p>Although displayed as a resource pool, this resource pool type cannot be used in Cloud Infrastructure Management Software.</p> <hr style="border-top: 1px dotted orange;"/>
Image	<p>The following resources are stored in this type of resource pool.</p> <ul style="list-style-type: none"> - Cloning master

A.2 Logical Servers (L-Servers)

Logical Servers define the logical specifications for servers including storage and networks, such as the number of CPUs, memory capacity, disk capacity, and the number of NICs. Logical Servers are referred to as "L-Servers".

Resources are allocated to L-Servers according to predefined specifications. Once resources have been allocated to an L-Server, the L-Server can be operated in the same way as a normal server.

The users of an L-Server can operate the L-Server without having to be aware of the actual nature of the resources that have been allocated. Rather, they only have to be aware of the specifications that have been defined for the L-Server.

Using L-Servers has the following benefits:

- Simple, rapid server creation

By automatically allocating the resources stored in resource pools according to the specifications defined for L-Servers, servers with optimum configurations can be created easily and quickly.

- Lower management costs

Server users do not need to manage the resources that have been allocated to the L-Server. Management costs can be further reduced as a result of having resource management performed intensively by a specialized administrator known as an "infrastructure administrator".

Information

Resources can be allocated to L-Servers automatically from resource pools or by manually allocating particular resources.

A.3 L-Server Templates

L-Server Templates are templates that predefine the specifications for an L-Server (such as the number of CPUs, memory capacity, disk capacity, and the number of NICs).

Using L-Server Templates has the following benefits:

- Reducing the steps for creating L-Servers

The usage specification can be easily specified by simply selecting an L-Server Template from a list of available templates.

L-Servers can be easily created by selecting only three items: an L-Server Template, a cloning master, and the network that the L-Server will connect to.

- Standardizing configurations

Because L-Servers can be created using the same standardized configuration as the L-Server Template, there will be no mistakes in the work of creating servers and management costs can be reduced.

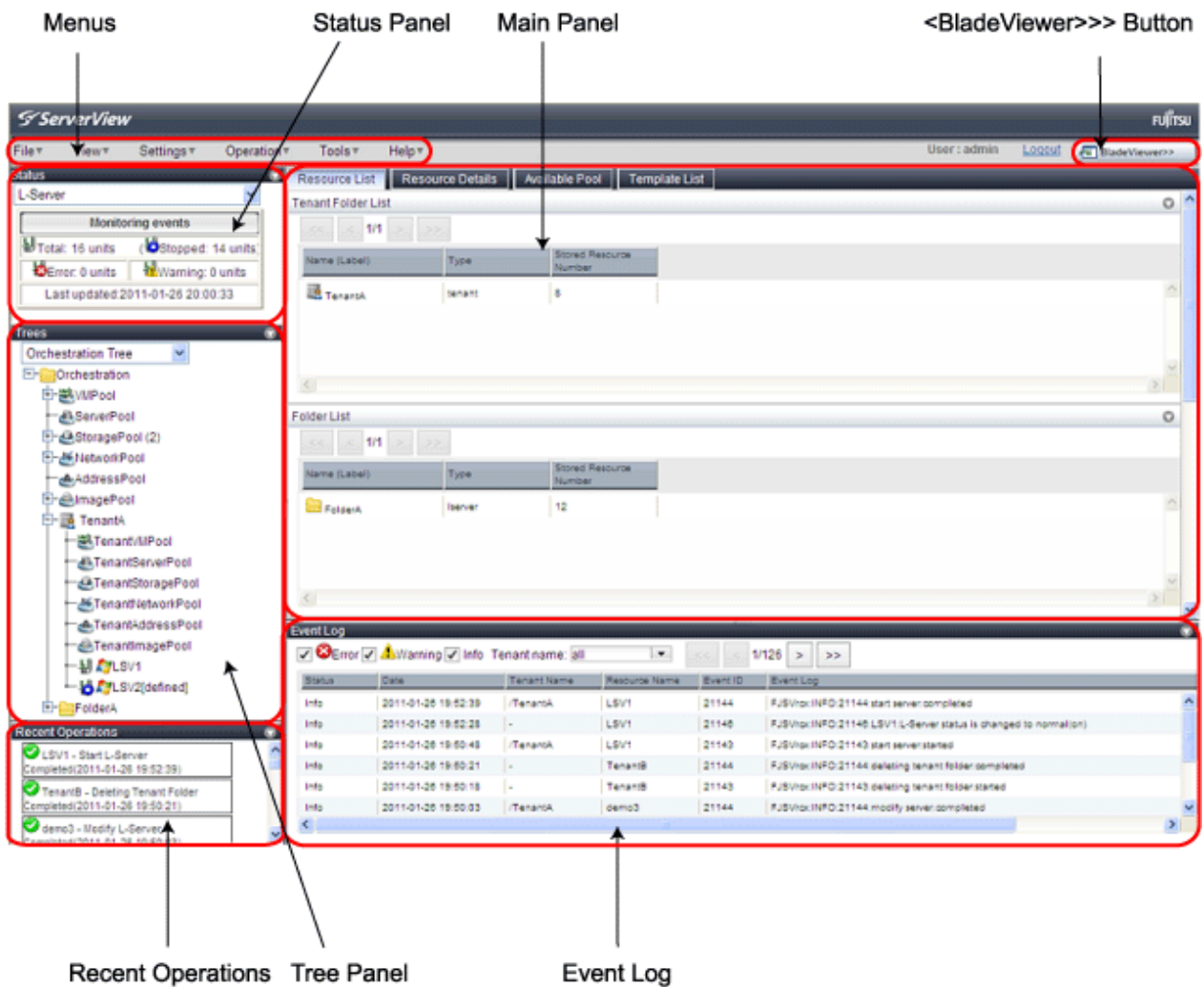
L-Server Templates can be exported and imported using XML files. This enables L-Server Templates to be designed at a different location from the Admin Server. It also allows configurations to be standardized between different systems.

This product comes with sample L-Server Templates. You can use these sample templates as they are, or you can edit them to your own requirements.

Refer to "Section 2.2.2 For Virtual L-Servers" in the "ServerView Resource Orchestrator Reference Guide" for details on L-Server Templates.

A.4 RC Console

The RC Console is used by the infrastructure administrator to register ICT resources in resource pools, release resources from resource pools, create L-Servers, and check the status of resources.



Menus

Operations can be performed either from the menu bar or popup menus. The RC console menu is described below. For details regarding menus not listed below, refer to "Chapter 2 User Interface" of the "ServerView Resource Coordinator VE Setup Guide".

Table A.2 Menu Item List

Menu bar	Menu	Submenu	Function
File	L-Server Template	Import	Imports an L-Server template.
		Export	Exports an L-Server template.
Settings	Pool	Register	Registers a resource in the selected resource pool.
		Unregister	Deregisters the selected resource from a resource pool.
	Create	Folder	Creates a resource folder in the server tree or orchestration tree.
		Tenant	Creates a tenant folder in the orchestration tree.
		Pool	Creates a resource pool in the orchestration tree.
		L-Server	Creates an L-Server.
		Network Resource (New)	Creates a new network resource.

Menu bar	Menu	Submenu	Function	
		Network Resource (Using existing admin subnet)	Creates a network resource from an admin LAN subnet.	
	Move to Folder	-	Moves a resource pool, resource folder, or a resource to another resource folder.	
	Move to Pool	-	Moves a resource to another resource pool.	
	User Accounts	-	Creates, modifies, or deletes a user account.	
	User Groups	-	Creates, modifies, or deletes a user group.	
	Change Password	-	Change the password of the logged-in user.	
	Modify	Basic Information		Modifies the basic information of a resource pool, resource folder, or a resource.
		Specification		Change L-Server or network resource specifications.
		Attach Disk		Attaches disks to an L-Server.
		Detach Disk		Detaches disks from an L-Server.
		Network Configuration		Changes the network configuration of an L-Server.
	Definition		Modifies L-Server definition information.	
Operation	Snapshot	Collect	Collects a snapshot of the L-Server.	
		Restore	Restores a snapshot to the L-Server.	
		Delete	Deletes a snapshot.	
	Console Screen	-	Opens the L-Server console.	
	Install VM Tool	-	Connects the ISO images for installing VMware Tools to an L-Server.	
	Backup/Restore	Backup	Backs up L-Server system images.	
		Restore	Restores L-Server system images.	
Delete		Deletes backup system images.		

Status Panel

The Status Panel displays the status of managed servers.

Only the L-Server status is displayed for the following users:

- Users with a role that only allows use of L-Servers
- Users with restricted access

If a warning or error event occurs on a managed server, the status monitoring area starts to blink.

If you click the blinking area, the server's information is displayed on the main panel.

For details of the status, refer to "2.3 Status Panel" in the "ServerView Resource Coordinator VE Setup Guide".

Tree Panel

CIMS displays the orchestration tree and storage tree in addition to the trees provided by ServerView Resource Coordinator VE. If resource folders have been created in the server tree, these resource folders are also displayed.

Only the orchestration tree is displayed for the following users:

- Users with a role that only allows use of L-Servers
- Users with restricted access

The resources displayed are restricted according to the access rights of the logged in user.

Orchestration Tree

Manages and operates L-Servers and resource pools.

All resources authorized for access by the logged in user are displayed. The resources displayed differ depending on the role and access rights of the user.

The statuses of the following resources are shown in a tree view:

- Resource folders and L-Servers
- Resource pools and the resources registered in resource pools

The top-level resource folder of each tree is called a root folder. The standard tree consists of only the root folder.

The orchestration tree displays the following information:

- Resource List

Displays information on resources related to the resource selected in the resource tree.

- Resource Details

Displays detailed information for the resource selected in the resource tree. Additionally, external software can be opened.

- Available Pool

A list of resource pools available for use is displayed.

- Template List

A list of L-Server templates available for use is displayed.

Using an L-Server template, an L-Server can be created.

Server resource tree

The server resource tree displays all chassis, servers, VM hosts, VM guests, and LAN switches managed in Resource Orchestrator, in a tree view.

Network resource tree

The network resource tree displays all LAN switches other than LAN switch blades managed in Resource Orchestrator, in a tree view.

Storage tree

The storage resource tree displays all storage management software, storage units, RAID groups, LUNs, and virtual disks of VM guests managed in CIMS, in a tree view.

Resources displayed in the server resource tree and network resource tree are represented by an icon and their resource name.

For details on icons and their resource names, refer to "Chapter 2 User Interface" of the "ServerView Resource Coordinator VE Setup Guide", and "5.2 Resource Status" in the "ServerView Resource Coordinator VE Operation Guide".

Main panel

The Main Panel displays information on resources selected in the tree.

Recent Operations

Displays the progress statuses and results of operations performed in Resource Orchestrator according to the user's scope of access.

Event log

Information about the events that occurred is displayed.

Events for ServerView Resource Coordinator VE are displayed in the event log, in addition to the events for this product.

Histories of the events that have occurred with managed resources are displayed as a list.

The resources displayed are restricted according to the role and access range for the user that is logged in.

<BladeViewer>>> button

BladeViewer is a management interface specially designed for blade servers. It can only be used in conjunction with PRIMERGY BX servers registered as managed servers.

Appendix B Managed Objects

This product manages the following objects.

Table B.1 Managed objects

Managed object	Overview
Users of this product	Service provider departments/service providers, service user departments/service users
ICT resources	Servers, storage, networks, etc.
Templates	L-Server Templates, system templates
Services	Leasing/returning Starting/stopping virtual platforms Taking snapshots

B.1 Users of This Product

This section explains users of this product.

Table B.2 Users of this product

User	Content	
Service provider department/service provider	Provider department administrator	This is the administrator who uses this product to provide a service to user departments. The provider department administrator can provide service specifications to service users, monitor the usage status of services, assess applications from user departments, and manage accounting information for service specifications.
Service user department/service user	Organization	Organizations represent the organizational groups to which the users of this product belong.
	User department administrator	This is a user belonging to the organization that uses the Cloud Portal for this product, and who has been given management privileges for the users that belong to that organization. Multiple user department administrators can be registered within a given organization. User department administrators can manage the users within their organization, apply to use services, and manage systems for the services within the organization.
	General user	This is a user belonging to the organization that uses the Cloud Portal for this product. Multiple general users can be registered within a given organization. General users can apply to use services, and manage systems for the services that they themselves have applied to use.

B.2 ICT Resources

This section explains the ICT resources that are managed by this product.

Refer to "Chapter 3 System Design and Initial Setup" of the "ServerView Resource Coordinator VE Setup Guide" for information on managing chassis, VM hosts, VM management products and LAN switches,

Table B.3 ICT resources

Resource	Content
Chassis	The chassis of a blade server that houses one or more server blades. This product can monitor the status of chassis, display information about chassis, and manipulate the power to chassis.
VM host	<p>A server virtualization software product that runs on a server in order to enable Virtual Machines(Virtual Server) to run. Examples of VM hosts are VMware ESX by VMware, and Windows Server 2008 R2 with a Hyper-V role added.</p> <p>This product can monitor VM hosts, display information about VM hosts, and perform server switching operations.</p> <p>When a VM host is registered, the VM guests running on the VM host are automatically detected and displayed.</p>
VM management product	<p>A product that performs integrated management for multiple server virtualization software products. Examples of VM management products are VMware vCenter Server for VMware and SCVMM for Hyper-V.</p> <p>Registering and linking VM management products with this product enables their functions to be used on VM guests.</p>
LAN switch	<p>The term "LAN switch" refers to both the LAN switches that are installed in the chassis of blade servers (which are known as "LAN switch blades") and to the LAN switches that these LAN switch blades are connected to.</p> <p>This product can monitor the status of LAN switch blades, display information about LAN switch blades and set up VLANs.</p> <p>This product can display the following information about LAN switch blades and other LAN switches via the RCVE network map function. Refer to "Chapter 12 Network Map" in the "ServerView Resource Coordinator VE Operation Guide" for details.</p> <ul style="list-style-type: none"> - The network configuration within a virtual server (the virtual switch and the VM guest) - The network connection status between resources - The VLAN setup status within virtual servers
VM guest	<p>The operating system that runs on a Virtual Machine(Virtual Server).</p> <p>This product can monitor the status of VM guests, display information about VM guests, and manipulate the power to VM guests. In addition to the functions of ServerView Resource Coordinator VE, this product provides functions such as creating new VM guests as L-Servers, and creating snapshots.</p>
Virtual switch	<p>A virtual LAN switch that is used to manage the networks for VM guests running on a VM host.</p> <p>With Hyper-V, this concept is expressed by the term "virtual network".</p> <p>This product supports both Hyper-V virtual networks and VMware virtual switches (provided as a standard VMware function). This product does not support VMware vNetwork Distributed Switches or Cisco Nexus 1000V virtual switches.</p>
Disk resource	Disk resources that are allocated to servers. An example of a disk resource is a virtual disk.
Virtual storage resource	<p>A resource that enables disk resources to be pulled out dynamically. An example of a storage resource is the file system for creating virtual machines (such as VMFS data stores by VMware).</p> <p>Disk resources can be created from RAID groups of ETERNUS storage and file systems for creating VM.</p>
Network resource	Resources that define information about the networks that L-Servers use.

Resource	Content
	<p>By connecting an NIC for an L-Server to a network resource, physical and virtual network switches are set up so that the L-Server can communicate.</p> <p>If an IP address range has been specified for a network resource, IP addresses can be set up automatically when images are distributed to L-Servers.</p>
Virtual image resource	An image that is created using a template from a VM management software for VM guest creation, or that is collected as a cloning image from an L-Server.

B.3 Templates

This section explains templates.

Table B.4 Templates

Type	Content
L-Server Template	<p>Templates that predefine the specifications for an L-Server (such as the number of CPUs, memory capacity, disk capacity, and the number of NICs).</p> <p>Refer to the articles on L-Servers and L-Server Templates in "Appendix A ICT Resource Management Functions" for details.</p>
System template	Templates that define the logical configuration of ICT resources and software.

B.4 Services

This section explains services.

A "service" is a unit for managing the business systems and ICT resources that are consolidated in data centers so that they can be provided or leased to users efficiently and on demand.

Service users can use services by selecting which services they require and applying to use them.

Appendix C Preparations and Checks before Installation

This appendix explains the preparations and checks that need to be performed before installing this product.

C.1 Preparations and Checks Before Installation

Checking for conflicting software

Check that neither the Manager for this product nor any of the software listed under "[2.2.2.4 Conflicting software](#)" has been installed on the target system.

Preparing and checking the required software

Check that the software programs listed under "[2.2.2.3 Required software](#)" have been installed on the system. If not, install them in advance.

Checking the ports used by this product

Check that the port numbers used by this product are not being used by another application.

Execute the following command to output the usage status of port numbers.

```
> netstat -an
```

Refer to "[D.1 List of Port Numbers](#)" for information on the port numbers used by this product and what to do if there are conflicts.



Note

When opening holes in the firewall for the ports used by this product:

To install this product on a system where a firewall has been enabled, open holes in the firewall for the port numbers used by this product so that the Manager and the Agent can communicate without any problems.

How to set up the Windows firewall

For Windows Server 2008 (but not Windows Server 2008 R2), use the following procedure to set up the Windows firewall.

1. Open the [**Windows Firewall**] dialog box from the [**Control Panel**], and then select the [**Exceptions**] tab.
2. Click the <**Add Port**> button in the [**Exceptions**] tab to display the [**Add Port**] dialog box.
3. Enter an arbitrary name and a port number in the [**Add Port**] dialog box, and select the protocol (either TCP or UDP).
4. Click the <**OK**> button to close the [**Add Port**] dialog box.
5. Click the <**OK**> button to close the [**Windows Firewall**] dialog box.

Preparing the installation folder and checking the free space

Decide the installation folder for this product.

However, folders on removable disks cannot be specified.

Check that there are no files or folders in the installation folder.

Check that the installation drive has enough free space.

Refer to "[2.1.1 Static disk capacity](#)" and "[2.1.2 Dynamic disk capacity](#)" for information on the disk space required by this product.

Checking the status of the admin LAN and the NICs

Decide the network (IP addresses) to be used as the admin LAN.

Check that the NIC on the admin LAN side has been enabled.

Appendix D Port Numbers

After being installed, this product uses the communication paths indicated in this appendix.

[Windows]

```
<System drive>\Windows\system32\drivers\etc\services
```

[Linux]

```
/etc/services
```

These port numbers must be unique within the network. If the port numbers shown in "[List of Port Numbers](#)" are already being used, the following actions are required.

For port numbers that can be changed

Change the port number by following the procedure in "[D.2 Procedure for Changing Ports](#)".

For port numbers that cannot be changed

Change the port number for the other software program that is using the port.

D.1 List of Port Numbers

This section shows the port numbers that are used by the functions of this product.

Note that if a firewall has been set up, connections must be allowed for the port numbers that need to receive packets from external servers, so that this product can run properly.

Admin Server

Table D.1 List of port numbers that need to receive packets from external servers

Function	Function details	Port number/Protocol	Changeable?
Dynamic resource management	RC Console	23461/tcp	Yes
	ServerView Operations Manager	3169/tcp	No
		3170/tcp	No
	Monitoring and controlling resources	161/udp	No
		162/udp	No
		623/udp	No
		23/tcp	No
	Backups, restorations, and cloning	4972/udp	No
		4973/udp	No
		67/udp	No
		4011/udp	No
		69/udp	No
	ServerView Agent	161/tcp	No
		161/udp	No
162/udp		No	
VMware ESX, vCenter Server	443/tcp	No	
System Center Virtual Machine Manager	80/tcp 443/tcp	No	
Self Service Portal/ configuration management	Connecting LDAP servers	389/tcp	Can be changed only during setup

Function	Function details	Port number/Protocol	Changeable?
	SSO authentication server	10443/tcp	No
	Process management	9657/tcp	Can be changed only during setup
	CORBA Service	8002/tcp	Can be changed only during installation
	Web server (Interstage HTTP Server) Operation Portal	80/tcp	No
	Authentication server	10443/tcp 10550/tcp 10555/tcp	No
	Collecting usage status information	2344/tcp	No
	Cloud Portal	80/tcp	No
		3500/tcp	Can be changed during installation or setup
	Interstage Management Console	12000/tcp	Yes
	Mail server	25/tcp	Can be changed only during installation
	CMDB	18443/tcp 18444/tcp	No
	File transfer infrastructure	9664/tcp	Yes

Table D.2 List of port numbers used internally

Function	Function details	Port number/Protocol	Changeable?
Dynamic resource management	ServerView Remote Connector Service	3172/tcp	No
	Active Directory	636/tcp	Yes
	Backups, restorations, and cloning	4971/tcp	No
Self Service Portal/ configuration management	CORBA Service	8002/tcp	Can be changed only during installation
	Web server (Interstage HTTP Server) Operation Portal	80/tcp	No
	Authentication server	10443/tcp 10550/tcp 10555/tcp	No
	Cloud Portal	3500/tcp	Can be changed only during installation
	Application process rule engine	40320/tcp	No
	Access control database	5439/tcp	Can be changed only during installation

Function	Function details	Port number/Protocol	Changeable?
	Usage management database	5440/tcp	Can be changed only during installation
	Accounting information database (product master)	5441/tcp	Can be changed only during installation
	Cloud infrastructure administrator dashboard database	5442/tcp	Can be changed only during installation
	IIOP	8002/tcp	No
	Servlet container	This function uses 10 vacant port numbers, starting from 9000/tcp.	No
	Internal APIs	3550/tcp 3551/tcp	No
	Interstage Management Console	12000/tcp	Yes
	CMDB	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	No
	Communications infrastructure	18005/tcp 18009/tcp	No
	Database	5438/tcp	Can be changed only during installation

Managed Servers

Table D.3 List of port numbers that need to receive packets from external servers

Function	Function details	Port number/Protocol	Changeable?
Dynamic resource management	Monitoring and controlling resources	23458/tcp	Yes
		161/tcp 161/udp	No
		162/udp	No
		623/udp	No
		23/tcp	No
	Backups, restorations, and cloning	4973/udp	No
	ServerView Agent	161/tcp 161/udp	No
162/udp		No	

Function	Function details	Port number/Protocol	Changeable?
	VMware ESX, vCenter Server	443/tcp	No
	Hyper-V	135/tcp 137/tcp 137/udp 138/udp 139/tcp 445/tcp 445/udp	No

VM servers

Table D.4 List of port numbers that need to receive packets from external servers

Function	Function details	Port number/Protocol	Changeable?
Self Service Portal/ configuration management	File transfer infrastructure	9664/tcp	Yes
	SSH	22/tcp	No
	IPMI	623/udp	No
	SNMP	161/udp	No

Table D.5 List of port numbers used internally

Function	Function details	Port number/Protocol	Changeable?
Self Service Portal/ configuration management	Communication infrastructure	18005/tcp 18009/tcp	No



Note

If the firewall function is enabled, firewall exceptions must be specified for the port numbers and protocols that are shown in the table above.

D.2 Procedure for Changing Ports

D.2.1 Procedure for Changing Port Numbers for the Dynamic Resource Management Server

This section explains the procedures for changing port numbers for the dynamic resource management function.

Procedure for changing the port number of the Admin Server

Refer to the ServerView Operations Manager manuals for details on how to change port numbers for ServerView Operations Manager. SNMP and the server startup control are standard protocols, and their port numbers are fixed by the hardware and cannot be changed.

For systems where the operating system firewall has been enabled, and environments where a firewall has been placed on the network, change the firewall settings so that communications to the modified ports can be performed without any problems.

Use the following procedure to change the port number of the Admin Server, which is used by the Manager itself.

1. Stop the Manager.

[Windows]

1. Log in with Administrator privileges.

2. Execute the stop command.

```
> <CIMS installation folder>\CIMS\Manager\bin\cims mgrctl stop
```

2. Execute the rcxadm mgrctl modify command by specifying the name of the port to be changed and the new port number.

Refer to "5.7 rcxadm mgrctl" in the "ServerView Resource Coordinator VE Command Reference" for details on the rcxadm mgrctl modify command.

[Windows]

```
> <CIMS installation folder>\Resource Orchestrator\Manager\bin\rcxadm mgrctl modify -port  
name=number <RETURN>
```

3. Restart the Manager.



If the port number of the RC Console has been changed, change the following port numbers to the same value.

- Admin Client

Change the port number of the URL specified in the Web browser to the port number of the RC Console.

If URLs have been saved in the "Favorites" for the Web browser, change the port numbers of these URLs as well.

Procedure for changing the port numbers of Managed Servers

Use the following procedure to change the port numbers of Managed Servers.

[VMware]

1. Change the following line in the "/etc/services" file using the vi command or some other method.

```
# Service name Port number/Protocol name  
nfagent      23458/tcp
```

2. Restart the server for which the port number has been changed.

[Hyper-V]

1. Use a text editor (such as Notepad) to change the following line in the "<system drive>\WINDOWS\system32\drivers\etc\service" file.

```
# Service name Port number/Protocol name  
nfagent      23458/tcp
```

2. Restart the server for which the port number has been changed.

D.2.2 Procedure for Changing Port Numbers for the Self Service Portal/ Configuration Management

This section explains the procedure for changing the port numbers for the Admin Server.

This section explains the procedures for changing port numbers for the Self Service Portal/configuration management function.

Procedure for changing the port number of the Interstage Management Console

Use the Interstage Management Console to change the port number of the Interstage Management Console. Refer to the help for the Interstage Management Console for details on the change procedure.

Settings required when the port number for the file transfer infrastructure is duplicated

Changing the port number of the VM server

The file transfer infrastructure uses port number 9664. This port number must be changed if it already exists in a VM server environment. Make the change on the Admin Server that is linked to the VM server to be changed.

[Windows]

Change the following port number specified in the "<System drive>\WINDOWS\system32\drivers\etc\services" file to a vacant port number.

[Linux]

Change the following port number specified in the "/etc/services" file to a vacant port number.

```
dtranf02    9664/tcp                # FJSVlnkbs
```

The port number can be a value between 1 and 65535.

Changing the port number of the Admin Server

For the port number specified in the network definition file for the file transfer infrastructure, specify the same value as the port number that has been set for the VM server.

1. Edit the following network definition file.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\FJSVlnkbs\lnk02\gen\network_def.txt
```

2. After the network definition file has been edited, apply the definition information as below.

[Windows]

```
<CIMS installation folder>\Systemwalker\SWRBAM\FJSVlnkbs\lnk02\bin\f3jtlxgentrn.exe -i 02  
<CIMS installation folder>\Systemwalker\SWRBAM\FJSVlnkbs\lnk02\gen\network_def.txt
```

3. Restart the file transfer infrastructure.

[Windows]

Restart the "Systemwalker File Transfer Library Control" service.

Changing the port number of the server for the Cloud Portal

Use the following procedure to change the port number.

1. Stop the Manager by executing the following command.

[Windows]

- a. Log in with Administrator privileges.
- b. Execute the stop command.

```
> <CIMS installation folder>\CIMS\Manager\bin\cims mgrctl stop
```

2. Change the "portal.properties" file.

[Windows]

- a. Open the following file.

```
<CIMS installation folder>\SWCTMG\SecurityManagement\conf\portal.properties
```

Change the port numbers specified in the following URLs:

- portalSsl.url

- authedPortal.url
- userManager.url
- personalInfo.url
- rManagerInfo.url
- orgInfo.url
- portala.logout.url
- pki.url
- aControl.url
- community.url
- sendmail.auth.url

- b. Close the file that was opened in Step a.
- c. Open a command prompt.
- d. Execute the following command from the command prompt.

```
<CIMS installation folder>\SWCTMG\SecurityManagement\conf\bin\ctsec_bstrip.bat
```

- e. Check that "Success" is displayed at the command prompt.
- f. Close the command prompt.

3. Start the Interstage Management Console.

Use the following procedure to start the Interstage Management Console.

[Windows]

Select the [All Programs] - [Interstage] - [Application Server] - [Interstage Management Console] from the [Start] menu.

4. Modify the port number.

Select the [System] - [Services] - [Web server] - [ctmg-https-ext] - [Web Server Settings], and modify the port number.

5. Change the port number for protected resources.

Select the [System] - [Security] - [Single Sign-on] - [Authentication infrastructure] - [Repository server] - [Protection resource] - [<FQDN, Port Number>], and modify the port number.

6. Output the business system configuration file.

Select the [System] - [Security] - [Single Sign-on] - [Authentication infrastructure] - [Business system setup file tab].

Set the [Business] - [system information] as follows, input password (within 6 characters or more) and then click <Download>.

Item	Description
public URL	http://< FQDN of the Admin Server>:<3500(Port number of the Cloud Portal)>/
Linkage with Interstage Portalworks?	No

7. Delete the business system.

Display a list by the [System] - [Security] - [Single Sign-on] - [Business system].

Delete the business system of the port number set (Change).

Delete the business system corresponding to the port number to be changed (the port number that is already set up).

8. Register an Admin Server.

Register an Admin Server by referring to "[Registering the Admin Server](#)".

9. Enable content cache suppression.

Use the business system configuration file that was downloaded in Step 6 and the password to enable content cache suppression by referring to "[Prevention of Caching of Contents](#)".

10. Update access control information.

Update access control information by referring to "[Update Access Control Information](#)".

11. Restart the Manager.

[Windows]

```
<CIMS installation folder>\CIMS\Manager\bin\cims mgrctl start
```

The processing results are output to the standard output. If the return value is 0, the command has terminated normally and the system has stopped.

Processing result	Return value
Normal termination	0
Error	Other than 0

Appendix E Tuning System Parameters

Refer to "E.1 Tuning Values for System Parameters" below 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 default 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 default value or the previous setting). Check the upper limit for the system before setting the parameter to the result of the addition. If the result of the addition is greater than the upper limit for the system then set the parameter to the upper limit for the system.

Refer to the Linux manuals or other documents for details.

E.1 Tuning Values for System Parameters

Admin Server

- Shared memory

Parameter	Description	Settings	Type
kernel.shmmax	Maximum segment size for shared memory	2684354560	Maximum
kernel.shmall	Total amount of shared memory available	655360	Maximum
kernel.shmmni	Maximum number of shared memory segments	156	Addition

- Semaphores

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

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

Parameter	Description	Settings	Type
para1	Maximum number of semaphores per semaphore identifier	512	Maximum
para2	Number of semaphores for the entire system	23481	Addition
para3	Maximum number of operators per semaphore call	50	Maximum
para4	Number of semaphore operators for the entire system	2763	Addition

- Message queues

Parameter	Description	Settings	Type
kernel.msgmax	Maximum size of messages	16384	Maximum
kernel.msgmnb	Maximum number of messages that can be held in a single message queue	114432	Maximum
kernel.msgmni	Maximum number of message queue IDs	1566	Addition

VM 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 operators for the entire system	2	Addition

- Message queues

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

E.2 Tuning Procedure

1. Use the following command to check the current settings for the system parameters.

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

Example

```
# /sbin/sysctl -a
...
(omitted)
...
kernel.sem = 256 32000 32 128
kernel.shmmax = 68719476736
kernel.shmall = 4294967296
kernel.shmmni = 4096
...
kernel.msgmax = 65536
kernel.msgmnb = 65536
kernel.msgmni = 16
...
(omitted)
...
```

2. Refer to "E.1 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 the /etc/sysctl.conf file as shown in the following example.

Example

```
kernel.sem = 512 55481 50 2891
kernel.shmmni = 4252
kernel.msgmnb = 114432
kernel.msgmni = 1582
```

4. Use the following command to check that the changes have been applied to the /etc/sysctl.conf file.

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

5. To enable the settings entered in Step 3, perform either of the following methods.

- Apply the settings by rebooting the system.

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

- Apply the settings by executing the "/sbin/sysctl -p" command.

```
# /sbin/sysctl -p /etc/sysctl.conf (*)
```

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

6. The output of the following command can be used to check whether the specified system parameters have been updated.

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

Example

```
# /sbin/sysctl -a
...
(omitted)
...
kernel.sem = 512 55481 50 2891
kernel.shmmax = 68719476736
kernel.shmall = 4294967296
kernel.shmmni = 4252
...
kernel.msgmax = 65536
kernel.msgmnb = 114432
kernel.msgmni = 1582
...
(omitted)
...
```

Appendix F Creating and Setting up Interstage Single Sign-On Environments, and Cancelling the Setup

This appendix explains how to create and set up Interstage Single Sign-On environments and how to cancel the setup.

F.1 Creating and Setting up Interstage Single Sign-On Environments

This section explains how to create and set up an Interstage Single Sign-On environment, which is required for the Admin Server after installation.



Point

This product uses Interstage Single Sign-On for user authentication. This section explains the environment setup for Interstage Single Sign-On.

Use the following procedure to create and set up Interstage Single Sign-On environments.

- Creating an SSL communication environment
- Setting up Interstage Single Sign-On

F.1.1 Creating an SSL Communication Environment

Create an SSL communication environment as preparation for setting up Interstage Single Sign-On.

Use the following procedure to create an SSL communication environment.

1. Set up access permissions for the Interstage certificate environment.
2. Create an Interstage certificate environment and an application form for acquiring the certificates used for SSL communications.
3. Register the certificates used for SSL communications.
4. Enter settings for SSL communications.



Information

Refer to "Setting and Use of the Interstage Certificate Environment" in the *Interstage Application Server Security System Guide* for details on how to create an SSL environment.

Creating an Interstage certificate environment and an application form for acquiring the certificates used for SSL communications

Use the `scsmakeenv` command (the certificate signing request (CSR) creation command) to create an Interstage certificate environment and to create a CSR for applying to acquire the certificates used for SSL communications.

The creation procedure and an execution example are shown below.

Creation procedure:

1. Specify the installation path to the JDK or JRE in the `JAVA_HOME` environment variable.

This step is only required for Linux. There is no need to set the `JAVA_HOME` environment variable for Windows.

1. Execute the scsmakeenv command.

[Windows]

```
scsmakeenv -n <Nickname of the private key> -f <Name of the file where the CSR is output>
```

[Linux]

```
scsmakeenv -n <Nickname of the private key> -f <Name of the file where the CSR is output> -g  
<Group that allows access to the Interstage certificate environment>
```

If necessary, change the name of the file where the CSR is output.

Note

The nickname of the private key that is specified with the scsmakeenv command is required when the site certificate that is acquired from the certificate authority is registered.

Information

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

2. Enter the password for accessing the Interstage certificate environment.

The password is required to access the Interstage certificate environment.

3. Enter an identifier.

For the "What is your first and last name?" prompt, the FQDN of the server for which the certificate application is to be made must be specified as the host name of the Web server.

4. Enter the following items, in the same way as with Step 4.

- organizational unit
- Organization
- City or Locality
- State or Province
- Country code

5. Check the values that have been entered.

To create a CSR using the values that have been entered, enter "yes". To enter the values all over again, enter "no".

6. Send the CSR to the certificate authority to request that a certificate be issued.

If the scsmakeenv command terminates normally, a CSR will be output to the output file for the CSR that was specified with the "-f" option of the scsmakeenv command. Send this file to the certificate authority to request that a certificate be issued. Follow the request method used by the certificate authority.

Example

[Windows]

The command execution example below uses the following settings:

```
- Nickname of the site certificate: SERVERCERT  
- Output file name for the CSR: C:\temp\ssocert.txt  
- First and last name: ssoserver.example.com  
- Organizational unit: FUJITSU TOKYO  
- Organization: FUJITSU
```

```
- City or locality: Shinjuku
- State or province: Tokyo
- Country code: jp
```

```
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>
```

[Linux]

The command execution example below uses the following settings:

```
- Nickname of the site certificate: SERVERCERT
- Output file name for the CSR: /tmp/ssocert.txt
- Group that allows access to the Interstage certificate environment: iscertg
- First and last name: ssoserver.example.com
- Organizational unit: FUJITSU TOKYO
- Organization: FUJITSU
- City or locality: Shinjuku
- State or province: Tokyo
- Country code: jp
```

The execution example creates a new Interstage certificate environment with access permissions set by the *iscertg* group, and also creates a CSR. If an Interstage certificate environment has already been created, set the access permissions for the Interstage certificate environment as necessary.

The execution example below uses a Bourne shell.

```
# JAVA_HOME=/opt/FJJSVawjbc/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

If an Interstage certificate environment has already been created, there will be a prompt asking you to enter the password for the Interstage certificate environment, so enter the password that was specified when the Interstage certificate environment was created.

Information

Test site certificates can be used for test environments. Use test site certificates for test environments only and not for actual operations.

Refer to "[Creating test site certificates](#)" for information on how to create test site certificates.

Registering the certificates used for SSL communications

Obtain the site certificate issued by the certificate authority, as well as the CA certificate for the certificate issuer, and then register these certificates using the `scscenter` command (the certificate/CRL registration command).

Information

Depending on the certificate authority, it may be necessary to register an intermediate CA certificate as well. Refer to "Registering Certificates and CRL" in the "Interstage Application Server Security System Guide" for details.

This step is not required if a test site certificate has been created.

Creation procedure:

1. Use the `scscenter` command to register the CA certificate.

```
scscenter -n <Nickname of the CA certificate> -f <CA certificate>
```

Information

Refer to "SSL Environment Setting Commands" in the "Interstage Application Server Reference Manual (Command Edition)" for details on the `scscenter` command.

2. Enter the password for accessing the Interstage certificate environment.

Enter the password for accessing the Interstage certificate environment that was specified in the `scsmakeenv` command.

3. Use the `scscenter` command to register the site certificate.

```
scscenter -n <Nickname of the site certificate> -f <Site certificate> -o
```

To register the site certificate obtained from the certificate authority, specify the nickname that was specified for the private key using the `scsmakeenv` command.

Be sure to specify the "-o" option when registering site certificates.

4. Enter the password for accessing the Interstage certificate environment.

Enter the password for accessing the Interstage certificate environment that was specified in the `scsmakeenv` command.



Example

[Windows]

The command execution example below uses the following settings:

```
- CA certificate: c:\temp\ca-cert.cer
- Nickname of the CA certificate: CACERT
- Site certificate: C:\temp\server-cert.cer
- Nickname of the site certificate: SERVERCERT
```

If necessary, change the file names of the CA certificate and the site certificate that have been obtained.

```
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:\>
```

[Linux]

The command execution example below uses the following settings:

```
- CA certificate: /tmp/ca-cert.cer
- Nickname of the CA certificate: CACERT
- Site certificate: /tmp/server-cert.cer
- Nickname of the site certificate: SERVERCERT
```

If necessary, change the file names of the CA certificate and the site certificate that have been obtained. The execution example uses a Bourne shell.

```
# JAVA_HOME=/opt/FJSVawjbc/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.
#
```

Setting up for SSL communications

Use the Interstage Management Console to create SSL definitions.

1. Start the Interstage Management Console.

Use the following procedure to start the Interstage Management Console.

[Windows]

Select the **[All Programs]**, **[Interstage, Application Server]**, and then **[Interstage Management Console]** from the **[Start]** menu.

[Linux]

- a. Start a Web browser.
- b. Specify the URL of the Interstage Management Console.

The URL format is shown below.

(For communications without SSL encryption)

```
http://<Host name of the Admin Server>:<12000 (Port number of the Interstage Management Console)>/IsAdmin/
```

(For communications with SSL encryption)

```
http://<Host name of the Admin Server>:<12000 (Port number of the Interstage Management Console)>/IsAdmin/
```

c. Log in to the Interstage Management Console.

2. Create SSL definitions

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 click the **<Create>** button.

Item	Settings
Configuration name	<p>Specify a name to identify the SSL definitions.</p> <p>The definition name specified here must be specified when Interstage Single Sign-On is set up.</p> <p>The definition name can be up to 32 characters long, including alphanumeric characters and the following symbols.</p> <ul style="list-style-type: none">- Hyphen "-"- Parenthesis "()"- Bracket "[]"- Underscore "_"
Site Certificate Nickname	<p>Select the nickname that was specified when the site certificate was registered with the Interstage certificate environment in "Registering the certificates used for SSL communications". The site certificate that was selected can be checked in the [System] - [Security] - [Certificates] - [Site Certificates] window of the Interstage Management Console.</p>
Protocol Version	<p>Select "SSL 3.0" and "TLS 1.0".</p>
Verify Client Certificate?	<p>Select "No".</p>
Encryption Method	<p>If necessary, change the encryption method by referring to the help for the Interstage Management Console.</p>
CA Certificate Nickname	<p>If necessary, change the nickname of the CA certificate by referring to the help for the Interstage Management Console.</p>

F.1.2 Setting up Interstage Single Sign-On

Use the `ssocsetup` command (the Interstage Single Sign-On setup command) to set up Interstage Single Sign-On.

By executing the `ssocsetup` command, the following servers (which are required for Interstage Single Sign-On) will be created.

- Repository server (update system)
- Authentication server
- Business Server

The information set up by the `ssocsetup` command is as follows:

Item	Settings
Public directory	ou=interstage,o=fujitsu,dc=com
Administrator DN	cn=manager
Authentication Web server name	SSOauth
Authentication server port number	10443 10550 10555
Idle monitoring time	30 minutes
Re-authentication interval	480 minutes
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 `ssocsetup` command:

(Mandatory)

- Server FQDN
- SSL definitions

(Optional)

- SSO repository name
- Port number of the SSO repository

For the server FQDN, specify the FQDN of the Admin Server that was specified when it was installed.

For the SSL definitions, specify the SSL definitions that were created in "[Setting up for SSL communications](#)".

For the SSO repository name, specify up to eight alphanumeric characters. If this option is omitted, "rep001" will be specified.

For the port number of the SSO repository, specify the port number of the SSO repository that was specified during installation.

Refer to "[G.3.2 Interstage Single Sign-On System Creation Command](#)" for details on the `ssocsetup` command.

When the `ssocsetup` command is executed, the password for the administrator DN will need to be entered, so enter the value that was specified during installation.

Creation procedure:

1. Execute the `ssocsetup` command.

[Windows]

```
ssocsetup FQDN SSLConfName [-rn RepositoryName] [-lp LDAPPort]
```

[Linux]

```
/opt/FJSVcfmg/sso/bin/ssocsetup FQDN SSLConfName [-rn RepositoryName] [-lp LDAPPort]
```

2. Enter the password for the administrator DN of the SSO repository.

Example

[Windows]

The command execution example below uses the following settings:

```
- Server FQDN: ssoSERVER.example.com
- SSL definition name: AuthSSL
```

Change the server FQDN and SSL definition name as necessary.

```
ssoc1setup ssoSERVER.example.com AuthSSL
Please input SSO Repository administrator DN password
Password:
Retype:
IREP: INFO: irep10815: Password file was created.
file=C:\INTERS~3\F3FMss\soatcsv\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.
```

[Linux]

The command execution example below uses the following settings:

```
- Server FQDN: ssoSERVER.example.com
- SSL definition name: AuthSSL
```

Change the server FQDN and SSL definition name as necessary.

The execution example uses a Bourne shell.

```
# /opt/FJSVcfmg/sso/bin/ssoc1setup 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.
```

Creating test site certificates

Test site certificates can be used only when testing needs to be conducted before using a site certificate issued by a certificate authority. The following example shows how to create a test site certificate.

Note

Test site certificates can only be used for test environments.

Do not use test site certificates in actual operations.

Example

The command execution example below uses the following settings:

```
- Nickname of the test site certificate: testCert
- First and last name: ssoserver.example.com
- Organizational unit: FUJITSU TOKYO
- Organization: FUJITSU
- City or locality: Shinjuku
- State or province: Tokyo
- Country code: jp
```

The password that is entered is not displayed. For the first time, you will register the password. Enter "yes" to create a certificate using the information displayed to confirm the password that has been entered. Enter "no" to enter the information again.

[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.example.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 execution example uses a Bourne shell.

```
# JAVA_HOME=/opt/FJSVawjbc/jdk5;export JAVA_HOME
# scsmakeenv -n testCert
Password:

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

If an Interstage certificate environment has already been created, there will be a prompt asking you to enter the password for the Interstage certificate environment, so enter the password that was specified when the Interstage certificate environment was created.

F.2 Canceling the Setup for Interstage Single Sign-On

This section explains the procedure for canceling the setup for Interstage Single Sign-On.

Note

Cancel the setup for CIMS before canceling the setup for Interstage Single Sign-On.

Use the `ssoclunsetup` command (the Interstage Single Sign-On setup cancelation command) to cancel the setup for Interstage Single Sign-On.

By executing the `ssoclunsetup` command, the following resources for Interstage Single Sign-On will be deleted:

- The following servers for Interstage Single Sign-On
 - Repository server (update system)
 - Authentication server
 - Business Servers (*1)
- The SSO repository that the repository server (the update system) refers to
- The Web server (*2) for which the repository server (the update system) and the authentication server have been created

*1: All of the Business Servers for Interstage Single Sign-On that have been created on the machine where the `ssoclunsetup` command is executed will be deleted. However, the Web servers themselves will not be deleted.

*2: Only the Web server with the Web server name "SSOAuth" (for which the repository server (the update system) and the authentication server have been created) will be deleted. Other Web servers will not be deleted.

Note

Refer to "[G.3.2 Interstage Single Sign-On System Creation Command](#)" for details on the `ssoclsetup` command.

Deletion procedure:

1. Execute the `ssoclunsetup` command.

[Windows]

```
ssoclunsetup
```

The `ssoclunsetup` command is stored in the following folder.

```
<CIMS installation folder>\Systemwalker\SWCTMG\SecurityManagement\sso\bin
```

[Linux]

```
# /opt/FJSVctsec/sso/bin/ssoclunsetup
```

2. Confirm whether to delete Interstage Single Sign-On

When the ssoclunsetup command is executed, a message will be displayed confirming whether to delete Interstage Single Sign-On. To delete Interstage Single Sign-On, enter "yes". If a value other than "yes" is entered, "Command canceled" will be displayed and Interstage Single Sign-On will not be deleted.

3. The status of resources will be displayed as a message.

4. When the ssoclunsetup command has been executed, the status of the resources to be deleted will be displayed as a message. The meaning of each resource is shown below:

Resource name	Resource description
Repository Server	Repository server (update system)
Authentication Server	Authentication server
Business Server	Business Server
Web Server (<Web server name>)	The Web server for which the repository server (the update system) and the authentication server have been created. The Web server name is fixed as <i>SSOauth</i> .
SSO Repository (<Repository name>)	The SSO repository that the repository server (the update system) refers to

5. The status of resources will be displayed as the following messages:

Messages	Resource status
Exist	The resource exists
Not exist	The resource does not exist

 Note

- After the ssoclunsetup command has completed, the Web server (Interstage HTTP Server) to which Business Servers have been added will not be started.
- The ssoclunsetup command will terminate normally even if it is executed when the resources to be deleted do not exist.

 Example

[Windows]

```
> ssoclunsetup
Repository Server      : Exist
Authentication Server  : Exist
Business Server        : Exist
Web Server (SSOauth)   : ExistSSO 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/FJSVtsec/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]
```


Appendix G Command Reference

This appendix presents the command reference for this product.

G.1 Environment Setup and Control Commands

This section explains the environment setup and control commands.

G.1.1 Overview of the Environment Setup and Control Commands

These commands are used to set up an environment for the Admin Server and to control it.

Command location

The storage location of the control and environment setup commands is shown below.

```
[Windows]
  <CIMS installation folder>\CIMS\Manager\bin\
```

Format of command description

This section explains the description format for the environment setup and control commands.

Synopsis

This section explains the synopsis for the commands.

```
"Command name" "Subcommand name" ["Option"] [...]
```

The following table explains each item of the command.

Item	Description
Command name	This is a command name.
Subcommand name	This is a subcommand name.
[Option]	This is an option name, or an option name plus a parameter. Options in square brackets can be omitted.
[...]	This indicates that multiple options can be entered. However, these additional options can be omitted.

Description

This section explains the function of a command.

Subcommands

This section explains subcommands.

Options

This section explains options.

Cautions

This section explains important points to note when using the command.

Return values

This section explains the values that are returned when the command terminates.

G.1.2 Manager Control Commands

Synopsis

cims mgrctl start

cims mgrctl stop

Description

The cims mgrctl command starts and stops the Manager.



Note

The Manager starts automatically when the Admin Server is started.

This section explains how to check the startup status of the Manager.

[Windows]

The Manager is made up of the following Windows services and Interstage WorkUnits.

- The Manager itself (Windows services)
 - Resource Coordinator Manager
 - Resource Coordinator Task Manager
 - Resource Coordinator Web Server(Apache)
 - Resource Coordinator Sub Web Server(Mongrel)
 - Resource Coordinator Sub Web Server(Mongrel2)
 - Resource Coordinator DB Server(PostgreSQL)
- The Manager itself (Interstage WorkUnits)
 - CMDB_Gui
 - CMDB_Manager
 - CTMG_MyPortal
 - CTMG_OpPortal
 - CtmgConfidential
 - PDP
 - REST
 - SopConfidential
 - SopGetConfidential
 - SopUserManager
 - portal
 - portala
 - portals
 - CFMG_VSYS
 - CFMG_ManagerView
 - WUibpmcon
 - WUibpmsv
 - IBPMMServer

- Related services
 - Deployment Service
 - TFTP Service
 - PXE Services
 - Systemwalker SQC DCM
 - Systemwalker MpMjes

For the Manager itself (Windows services) and related services, the status of each service can be checked using the [Services] window that is opened by selecting [Administrative Tools] from the Windows [Control Panel].

The status of the Manager itself (Interstage WorkUnits) can be checked using the following procedure.

[Check method]

- Checking the startup status of Interstage
 - Use the isstat command (the Interstage startup status display command) to check that the *status* is *execute* (already running).
- Checking the startup status of WorkUnits
 - Use the islistwu command (the WorkUnit list display command) to check that the *status* of the WorkUnits above is *execute* (already running).



Subcommands

start

Starts the Manager.

stop

Stops the Manager.

Options

None

Cautions

[Windows]

Execute the command as an Administrator.

Execution environment

Admin Server.

Return values

The following values are returned.

0

The command has been processed successfully.

Other than 0

An error has occurred.

For messages that are output or displayed when a value other than zero is returned, perform checks and take action by referring to "[Messages for the cims mgrctl command](#)".

G.2 Template Management Commands

This section explains the Template Management Commands.

G.2.1 Overview of the Template Management Commands

The Template Management Commands provide functions for listing, registering, and deleting the various files that make up the system template.

The Template Management Commands can only be used by service providers.

Structure of Template Management Commands

The following table shows how the Template Management Commands are organized.

Type	Function name	Command name	Description
Software information manipulation commands	Software information list display command	cfmg_listsoft	This command outputs a list of the software information that has been registered.
	Software information registration command	cfmg_addsoft	This command registers software information.
	Software information deletion command	cfmg_deletesoft	This command deletes software information.
Image information manipulation commands	Virtual image list display command	cfmg_listvmimage	This command outputs a list of the virtual images that have been registered.
	Image information list display command	cfmg_listimageinfo	This command outputs a list of the image information that has been registered.
	Image information registration command	cfmg_addimageinfo	This command registers image information.
	Image information deletion command	cfmg_deleteimageinfo	This command deletes image information.
Segment information manipulation commands	Virtual network list display command	cfmg_listvnet	This command outputs a list of the virtual networks that have been registered.
	Segment list display command	cfmg_listnetinfo	This command outputs a list of the segments that have been registered.
	Segment registration command	cfmg_addnetinfo	This command registers segments.
	Segment deletion command	cfmg_deletenetinfo	This command deletes segments.
Template information manipulation commands	Template information list display command	cfmg_listtemplate	This command outputs a list of the template information that has been registered.
	Template information registration command	cfmg_addtemplate	This command registers template information.
	System template publication setup command	cfmg_showtemplate	This command publishes or delists system templates.
	Template information deletion command	cfmg_deletetemplate	This command deletes template information.

Command location

The storage location of the Template Management Commands is shown below.

```
[Windows]
<CIMS installation folder>\Systemwalker\SWCFMG\bin\
```

Input files

This section explains the file configuration used by Template Management Commands.

The following types of files are used as input files for these commands.

- Software information files
- Image information files
- Segment information files
- Template information files

The sections relating to each command explain the relationship between these input files.



For the values of the setting items in the input files, the strings cannot contain control characters such as linefeed or tab characters.

Each tag (everything between <tag name> and </tag name>) must be entered on a single line.

Also, these strings cannot contain the following characters:

< > & ' "

Nor can these strings contain the following strings, which are entity references to the characters above:

< > & " '

Return values and error messages

For the execution results of Template Management Commands, check the return values.

If the return value is 0, the command has terminated normally.

If the return value is other than 0, the command has terminated abnormally and an error message is output.

The following example shows how to check return values.

[Windows]

```
C:\Users\Administrator>cfmg_deletesoft -f -id SW00000003  
C:\Users\Administrator>echo %errorlevel%  
0  
C:\Users\Administrator>
```

Description format

This section explains the description format for Template Management Commands.

Synopsis

This section explains the synopsis for the commands.

```
"Command name" "Option" "Option 1" | "Option 2" [Option] [...]"
```

The following table explains each item of the command.

Item	Description
Command name	This is a command name.
Option	This is an option name, or an option name plus a parameter.
Option 1 Option 2	Select either option 1 or option 2.
[Option]	Options in square brackets can be omitted.

Item	Description
[...]	This indicates that multiple options can be entered. However, these additional options can be omitted.

Description

This section explains the function of a command.

Options

This section explains options.

Output format

This section explains the format of the data output when the command terminates normally.

Cautions

This section explains important points to note when using the command.

Example

This section shows examples of how the command is used.

The examples in the explanations here are based on the Linux version.

G.2.2 Software Information Manipulation Commands

This section explains the commands for manipulating software information.

It is also possible to use a software information file that has already been registered.

Refer to "[Appendix H Registered Software IDs](#)" for details.

Displaying Software information

Synopsis

```
cfmg_listsoft [-v] [-utf8]
```

Description

This command outputs an XML file that contains a list of the software information that has been registered.

Options

Option	Description
-v	This option outputs the list in detailed format. If this option is omitted, the list is output in the simple format.
-utf8	This option outputs the list in UTF-8 format. This option is only valid for the Windows version. For the Windows version, the list is output in ISO-8859-1 format if this option is omitted.

Output format

This command uses the following format to output all of the software information that has been registered.

Detailed format	Simple format	Output format
*	*	<pre><?xml version="1.0" encoding="UTF-8"?> <softwares> <software> <id>[Software ID]</id> <name>[Software name]</name></pre>
*	*	
*	*	
*	*	

Detailed format	Simple format	Output format
*	*	<category>[Software category]</category>
*	*	<osCategory>[Operating system category]</osCategory>
*	-	<version>[Version]</version>
*	-	<officialVersion>[Official version]</officialVersion>
*	-	<patch>[Patch version]</patch>
*	-	<license>[License information]</license>
*	-	<support>[Support information]</support>
*	-	<productId>[Model number]</productId>
*	-	<productName>[Product name]</productName>
*	-	<price>[Unit price]</price>
*	-	<chargeType>[Billing method]</chargeType>
*	-	<expectedUsage>[Expected monthly usage]</expectedUsage>
*	-	</software>
*	*	...
-	-	</softwares>
*	*	

*: Indicates information that is output.

-: Indicates information that is not output.

Cautions

This command outputs the following data if no software information has been registered.

```
<?xml version="1.0" encoding="UTF-8"?>
<softwares />
```

Example

```
# /opt/FJSVcfmg/bin/cfmg_listsoft
<?xml version="1.0" encoding="UTF-8"?>
<softwares>
  <software>
    <id>SW00000011</id>
    <category>OS</category>
    <name>Red Hat Enterprise Linux 5 (for Intel64)</name>
  </software>
</softwares>
```

Registering Software information

Synopsis

```
cfmg_addsoft [-name <Software name>] -xml <Path to the software information file>
```

Description

This command registers software information.

Options

Option	Description
-name	This option specifies the name of the software to be registered in the software information file, using a string made up of up to 85 printable ASCII characters long. Enclose the string in double quotes (") if it contains blank spaces. If this option is specified, the value specified for this option takes precedence over the information in the software information file. If this option is omitted, the software name in the software information file takes effect. An error will occur if this option is omitted and a software name has not been entered in the software information file.

Option	Description
-xml	This option specifies the absolute or relative path to the software information file, using a string made up of printable ASCII characters. Enclose the string in double quotes (") if it contains blank spaces.

Output format

The software ID that has been allocated is output using the following XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
  <id>[Software ID]</id>
</result>
```

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_addsoft -xml /tmp/template_test/software/software.xml
<?xml version="1.0" encoding="UTF-8"?>
<result>
  <id>SW00000003</id>
</result>
```

Deleting Software information

Synopsis

```
cfmg_deletesoft [-f] -id <Software ID>
```

Description

This command deletes software information.

Options

Option	Description
-f	This option executes the deletion without confirmation. If this option is omitted, a confirmation prompt will be output before the deletion takes place.
-id	This option specifies the software ID of the software information to be deleted.

Output format

None.

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_deletesoft -id SW00000011
Do you want to delete the software information? (Y/N) y
```

Detailed explanation of software information

This section provides detailed software information.

Software information

Software information files are XML documents that list configuration information for the software (the operating system and middleware) contained in the virtual image.

Create and register one software information file for each item of software.

Because software information for main Fujitsu middleware products and operating systems comes with the product, there is normally no need for service providers to create these software information files.

Refer to "[Appendix H Registered Software IDs](#)" for details on the software information files that come with this product.

When license information and so on is required, the service provider will need to modify the content of the files.

Refer to "Software infoemation Details" for details on the items (tags).

To register software such as OSS, a new software information file must be created.

Sample software information files are stored in the following directory.

The service provider must create software information files by referring to these samples.

```
[Windows]
<CIMS installation folder>\Systemwalker\SWCFMG\templates\softwares\
```

Software information Details

Software information files use the following XML format.

```
<?xml version="1.0" encoding="UTF-8" ?>
<software version="1.1">
  <id>[Software ID]</id>
  <lcid>[Locale ID]</lcid>
  <name>[Software name]</name>
  <category>[Software category]</category>
  <osCategory>[Operating system category]</osCategory>
  <version>[Version]</version>
  <officialVersion>[Official version]</officialVersion>
  <patch>[Patch version]</patch>
  <license>[License information]</license>
  <support>[Support information]</support>
  <productId>[Model number]</productId>
</software>
```

The following table shows descriptions of each of these items (tags), as well as their settings.

Modify software information files as necessary, by referring to the information in this table.

The square brackets enclosing some of the tag names indicate that these tags can be omitted.

Tag name	Type	Setting range	Description	Required?	Settings
[id]	-	-	This item sets the ID that is allocated when the software information is registered.	U	
[lcid]	string ASCII	Select	This item specifies the locale for software information.	M	Select one of the following values: - "ja": Japanese version - "en": English version
[name]	string UTF-8	Up to 85 characters	This item specifies the name of the software. Specify this item when registering software information.	O	
category	string ASCII	Select	This item specifies the category of the software.	M	Select the following value: - "OS": Operating system

Tag name	Type	Setting range	Description	Required?	Settings
osCategory	string ASCII	Select	This item specifies the software category of the operating system.	M	Select one of the following values: - "windows": Windows - "linux": Linux - "windows64": Windows (64bit) - "linux64": Linux (64bit)
version	string ASCII	1 to 10 bytes	This item specifies the version of the software.	M	Specify the version. Example: 9.2.0
officialVersion	-	-	This item specifies the official version.	U	
patch	-	-	This item represents patch information.	U	Specify information about the patches that have been applied in the image information files.
license	string UTF-8	Up to 85 characters	This item specifies license information for the software.	O	If "OS" was selected for the "category" item, specify the product key for the Windows operating system. This item cannot be specified for Linux operating systems. - If the virtualization software is Vmware: For Windows Server 2003, specify the product key for the Windows operating system. Example: XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX For operating systems other than Windows Server 2003, specify an empty string. - If the virtualization software is Hyper-V: Specify the product key for the Windows operating system. Example: XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX
support	string UTF-8	Up to 85 characters	This item specifies support information for the software.	O	
productId	-	-	This item specifies the product ID of the software.	U	

The symbols in the "Required?" column have the following meaning:

M: If the tag is specified, be sure to specify a value.

O: The value can be omitted.

U: There is no need to set a value. Only the tag itself is specified.

G.2.3 Image Information Manipulation Commands

This section explains the commands for manipulating image information.

Displaying a Virtual Image List

Synopsis

```
cfmg_listvmimage [-utf8]
```

Description

This command outputs an XML file that contains a list of the virtual images that have been registered.

Options

Option	Description
-utf8	This option outputs the list in UTF-8 format. This option is only valid for the Windows version. For the Windows version, the list is output in ISO-8859-1 format if this option is omitted.

Output format

This command uses the following format to output all of the virtual images that have been registered.

```
<?xml version="1.0" encoding="UTF-8"?>
<images>
  <image>
    <id>[Image ID]</id>
    <name>[Image name]</name>
    <comment>[Comment]</comment>
    <type>[Image type]</type>
    <version>[Image version]</version>
    <time>[Date and time when the image was created]</time>
  </image>
  ...
</images>
```

Cautions

This command outputs the following data if no virtual image information has been registered.

```
<?xml version="1.0" encoding="UTF-8"?>
<images />
```

Example

```
# /opt/FJSVcfmg/bin/cfmg_listvmimage
<?xml version="1.0" encoding="UTF-8"?>
<images>
  <image>
    <id>ST01-M_896</id>
    <name>RHELx64_IMG </name>
    <comment />
    <type>cloning</type>
    <version>1</version>
    <time>2010-11-17-15:20:17+09:00 </time>
  </image>
</images>
```

Displaying Image Information

Synopsis

```
cfmg_listimageinfo [-v] [-utf8]
```

Description

This command outputs an XML file that contains a list of the image information that has been registered.

Options

Option	Description
-v	This option outputs the list in detailed format. If this option is omitted, the list is output in the simple format.
-utf8	This option outputs the list in UTF-8 format. This option is only valid for the Windows version. For the Windows version, the list is output in ISO-8859-1 format if this option is omitted.

Output format

This command uses the following format to output all of the image information that has been registered.

Detailed format	Simple format	Output format
*	*	<pre><?xml version="1.0" encoding="UTF-8"?> <images> <image> <id>[Image ID]</id> <name>[Image name]</name> <ownerOrg>[Owner organization]</ownerOrg> <ownerUser>[Owner user]</ownerUser> <publicCategory>[Publication category]</publicCategory> <serverCategory>[Server type]</serverCategory> <serverApplication>[Server usage]</serverApplication> <serverType>[Default server type]</serverType> <cpuBit>[Number of CPU bits]</cpuBit> <sysvolSize>[Size of the system disk]</sysvolSize> <numOfNIC>[Number of NICs]</numOfNIC> <maxCpuPerf>[Maximum CPU performance]</maxCpuPerf> <numOfMaxCpu>[Maximum number of CPUs]</numOfMaxCpu> <maxMemorySize>[Maximum memory size]</maxMemorySize> <numOfMaxDisk>[Maximum number of disks]</numOfMaxDisk> <maxDiskSize>[Maximum disk capacity]</maxDiskSize> <icon>[Icon type]</icon> <virtualization>[Virtualization method]</virtualization> <showFlag>[Show flags]</showFlag> <softwares> ... </softwares> </image> </images></pre>
*	*	
*	*	
*	*	
*	-	
*	-	
*	-	
*	-	
*	*	
*	-	
*	-	
*	-	
*	-	
*	-	
*	-	
*	-	
*	-	
*	-	
*	-	
*	-	
*	*	
*	*	

*: Indicates information that is output.

-: Indicates information that is not output.

Cautions

This command outputs the following data if no image information has been registered.

```
<?xml version="1.0" encoding="UTF-8"?>
<images />
```

Example

```
# /opt/FJSVcfmg/bin/cfmg_listimageinfo -v
<?xml version="1.0" encoding="UTF-8"?>
<images>
  <image>
    <id>ST01-M_896</id>
    <name>RHELx64_IMG</name>
    <ownerOrg>cfmgadm</ownerOrg>
    <ownerUser>cfmgadm</ownerUser>
    <publicCategory>PUBLIC</publicCategory>
    <serverCategory>GENERAL</serverCategory>
    <serverApplication>AP</serverApplication>
    <serverType>extra_small</serverType>
    <cpuBit>32</cpuBit>
    <sysvolSize>15.0</sysvolSize>
    <numOfNIC>2</numOfNIC>
    <maxCpuPerf>10.0</maxCpuPerf>
    <numOfMaxCpu>1</numOfMaxCpu>
    <maxMemorySize>10.0</maxMemorySize>
    <numOfMaxDisk>10</numOfMaxDisk>
    <maxDiskSize>30.0</maxDiskSize>
    <numOfMaxNic>1</numOfMaxNic>
    <icon>unit_tag_web.png</icon>
    <virtualization>hvm</virtualization>
    <showFlag>0</showFlag>
    <softwares>
      <software>
        <name>Red Hat Enterprise Linux 5 (for Intel64)</name>
        <id>SW00000011</id>
        <category>OS</category>
        <osCategory>linux64</osCategory>
        <version>5.5</version>
        <officialVersion />
        <patch />
        <license />
        <support />
        <productId />
        <productName />
        <price />
        <chargeType />
        <expectedUsage />
      </software>
    </softwares>
  </image>
</images>
```

Image information registration command

Synopsis

```
cfmg_addimageinfo -xml <Path to the image information file>
```

Description

This command registers image information.

Options

Option	Description
-xml	This option specifies the absolute or relative path to the image information file, using a string made up of printable ASCII characters. Enclose the string in double quotes (") if it contains blank spaces

Output format

None.

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_addimageinfo -xml /tmp/template_test/images/sample.xml
```

Image information deletion command

Synopsis

```
cfmg_deleteimageinfo [-f] -name <Image name>
```

Description

This command deletes image information.

Options

Option	Description
-f	This option executes the deletion without confirmation. If this option is omitted, a confirmation prompt will be output before the deletion takes place.
-name	This option specifies the image name of the image information file to be deleted.

Output format

None.

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_deleteimageinfo -name RHELx64_IMG
Do you want to delete the image information? (Y/N) y
```

Detailed explanation of image information

This section provides detailed image information.

Image information

Image information files are XML documents that list configuration information for virtual images.

Create and register a separate image information file for each virtual image.

Sample image information files are stored in the following directory.

The service provider must create software information files by referring to these samples.

```
[Windows]
<CIMS installation folder>\Systemwalker\SWCFMG\templates\images\
```

Refer to "Detailed image information" for details on the items (tags).

For information on the software ID contained in the image information, the software ID (which is assigned when the software information is registered) must be entered in the image information file.

Detailed image information

Image information files use the following XML format.

```

<?xml version="1.0" encoding="UTF-8" ?>
<image version="1.1">
  <id>[Image ID]</id>
  <name>[Image name]</name>
  <ownerOrg>[Owner organization]</ownerOrg>
  <ownerUser>[Owner user]</ownerUser>
  <publicCategory>[Publication category]</publicCategory>
  <serverCategory>[Server type]</serverCategory>
  <serverApplication>[Server usage]</serverApplication>
  <serverType>[Default server type]</serverType>
  <cpuBit>[Number of CPU bits]</cpuBit>
  <sysvolSize>[Size of the system disk]</sysvolSize>
  <numOfNic>[Number of NICs]</numOfNic>
  <maxCpuPerf>[Maximum CPU performance]</maxCpuPerf>
  <numOfMaxCpu>[Maximum number of CPUs]</numOfMaxCpu>
  <maxMemorySize>[Maximum memory size]</maxMemorySize>
  <numOfMaxDisk>[Maximum number of disks]</numOfMaxDisk>
  <maxDiskSize>[Maximum disk capacity]</maxDiskSize>
  <initialPassword>[Default password]</initialPassword>
  <icon>[Icon type]</icon>
  <virtualization>[Virtualization method]</virtualization>
  <softwares>
    <software>
      <id>[Software ID]</id>
      <order>[Display order]</order>
      <patches>
        <patch>
          <id>[Patch ID]</id>
          <locale>
            <lcid>[Locale ID]</lcid>
            <componentName>[Component name]</componentName>
            <description>[Description]</description>
          </locale>
          ...
        </patch>
        ...
      </patches>
    </software>
    ...
  </softwares>
</image>

```

The following table shows descriptions of each of these items (tags), as well as their settings.

Modify image information files as necessary, by referring to the information in this table.

The square brackets enclosing some of the tag names indicate that these tags can be omitted.

Tag name	Type	Setting range	Description	Required?	Settings
Id	string ASCII	1 to 32 bytes	This item specifies the image ID.	M	Specify the image ID that was verified using the <code>cfmg_listvmimage</code> command (described in " Displaying a Virtual Image List ").
name	string ASCII	1 to 32 bytes	This item specifies the image name.	M	Specify the image name that was verified using the <code>cfmg_listvmimage</code> command (described in " Displaying a Virtual Image List ").
ownerOrg	string ASCII	Fixed value	This item specifies the organization ID of the	M	The value is fixed as "cfmgadm".

Tag name	Type	Setting range	Description	Required?	Settings
			organization to which the image belongs.		
ownerUser	string ASCII	Fixed value	This item specifies the user ID of the user who registers the image.	M	The value is fixed as "cfmgadm".
publicCategory	string ASCII	Fixed value	This item selects the category of the image.	M	The value is fixed as "PUBLIC". The image is available to all users.
serverCategory	string ASCII	Fixed value	This item selects the category of the server included in the image.	M	The value is fixed as "GENERAL". The server is a generic server.
serverApplication	string ASCII	Select	This item selects the usage of the server included in the image.	M	One or more values can be selected from the following: - "WEB": Web server - "AP": Application server - "DB": Database server Separate each value with "/" when specifying more than one value. Values can be specified in any order. Example: WEB/AP, AP/WEB/DB, etc.
serverType	string ASCII	0 to 32 bytes	This item specifies the server type.	O	Specify the name of an L-Server Template that has been set up and will be selected as the default L-Server Template when this image is used.
cpuBit	integer	Select	This item selects the number of bits used in the CPU of the server included in the image.	M	Select one of the following values: - "32": 32 bits - "64": 64 bits
sysvolSize	decimal	In decimal notation, to one decimal place	This item specifies the size of the system disk for a server included in the image.	M	Specify this value in GB.
numOfNic	integer	1 to 99	This item specifies the number of NICs.	M	Specify the number of NICs for the server included in the image.
[maxCpuPerf]	decimal	In decimal notation, to one decimal place (0.1 to 99999.9)	This item specifies the limit for the CPU performance that can be specified for the server.	M	Specify the limit for the CPU performance that can be specified for the server using the Manager View. Specify the value in GHz.
[numOfMaxCpu]	integer	1 to 99	This item specifies the limit for the number of CPUs that can be specified for the server.	M	This value will be the maximum number of CPUs that users can specify with the Manager View.
[maxMemorySize]	decimal	In decimal notation, to one decimal place (0.1 to 99999.9)	This item specifies the limit for the memory size that can be specified for the server.	M	Specify the limit for the memory size that can be specified for the server using the Manager View. Specify the value in GB.
[numOfMaxDisk]	integer	0 to 99	This item specifies the maximum number of expansion disks that can be added to the server.	M	This value will be the maximum number of disks that can be specified.

Tag name	Type	Setting range	Description	Required?	Settings
[maxDiskSize]	decimal	In decimal notation, to one decimal place (0.1 to 99999.9)	This item specifies the limit for the disk capacity that can be specified for expansion disks.	M	Specify this value in GB. This value will be the maximum size of expansion disks that can be specified.
initialPassword	string UTF-8	Up to 85 characters	This item specifies the default password for the operating system.	M	[Windows] - If the virtualization software is Vmware: Specify the password for the user name "Administrator". - If the virtualization software is Hyper-V: Specify the password for the local administrator account used by the L-Server to be created. [Linux] Specify the password for the superuser.
icon	string UTF-8	Select	This item selects the icon for the server included in the image.	M	Select one of the following icons, corresponding to server usages (as specified by the "serverApplication" item). - "unit_tag_web.png": Web server - "unit_tag_ap.png": Application server - "unit_tag_db.png": Database server - "unit_tag_webap.png": Web/application servers - "unit_tag_webdb.png": Web/database servers - "unit_tag_apdb.png": Application/database servers - "unit_tag_webapdb.png": Web/application/database servers - "unit_tag_blank.png": Other
virtualization	string ASCII	Fixed value	This item specifies the virtualization method.	M	The value is fixed as "hvm".
softwares	-	-	This item specifies the software installed on the server.	U	This tag is mandatory.
software	-	One or more	This item is specified for each software program installed on the server.	U	
Id	string ASCII	1 to 32 bytes	This item specifies the software ID of the software.	M	Specify the software ID that is displayed in the registration results of the cfmg_addsoft command (described in " Registering Software information ") or in the output results of the cfmg_listsoft command.
order	integer	0 or more	This item specifies the order in which software programs are to be displayed.	M	Specify the software programs in order, starting from "0". Make sure that the operating system is listed first.

Tag name	Type	Setting range	Description	Required?	Settings
patches	-	-	This item specifies patch information for the software.	U	
[patch]	-	One or more	This item is specified for each patch or update that needs to be applied.	U	This item is required only when patch information exists.
Id	string ASCII	1 to 32 bytes	This item specifies the patch ID for the patch.	M	Specify the update number and so on. It is not possible to specify the same patch ID more than once for a single software ID.
locale	-	One or more	This item specifies patch information for each locale.	U	
lcid	string ASCII	Select	This item specifies the locale for patch information.	M	Select one of the following values: - "ja": Japanese version - "en": English version
componentName	string UTF-8	Up to 85 characters	This item specifies the name of the component to which the patch is to be applied.	O	Specify an empty string if the patch specification does not include the concept of components. If patch information has already been registered with exactly the same software ID, patch ID and locale, the existing information will be updated by the newly registered information.
description	string UTF-8	Up to 85 characters	This item contains a description for the patch.	O	If patch information has already been registered with exactly the same software ID, patch ID and locale, the existing information will be updated by the newly registered information.

The symbols in the "Required?" column have the following meaning:

M: If the tag is specified, be sure to specify a value.

O: The value can be omitted.

U: There is no need to set a value. Only the tag itself is specified.

G.2.4 Segment Information Manipulation Commands

This section explains the commands for manipulating segment information.

Virtual network list display command

Synopsis

```
cfmg_listvnet [-utf8]
```

Description

This command outputs an XML file that contains a list of the virtual networks that have been registered.

Options

Option	Description
-utf8	This option outputs the list in UTF-8 format. This option is only valid for the Windows version.

Option	Description
	For the Windows version, the list is output in ISO-8859-1 format if this option is omitted.

Output format

This command uses the following format to output all of the virtual networks that have been registered.

```
<?xml version="1.0" encoding="UTF-8"?>
<networks>
  <network>
    <id>[Resource ID]</id>
    <name>[Network name]</name>
    <category>[Network type]</category>
    <extid>[VLANID]</extid>
    <addrset>
      <name>[Address set name]</name>
      <subnet>[Subnet address]</subnet>
      <mask>[Net mask]</mask>
      <start>[Start address]</start>
      <end>[End address]</end>
    </addrset>
    <exclude>
      <range>
        <start>[Beginning of the excluded addresses]</start>
        <end>[End of the excluded addresses]</end>
      </range>
      ...
    </exclude>
    <status>
      <num>[Number of addresses]</num>
      <used>[Number of reserved addresses]</used>
      <avail>[Number of vacant addresses]</avail>
    </status>
  </network>
  ...
</networks>
```

Cautions

This command outputs the following data if no virtual network has been registered.

```
<?xml version="1.0" encoding="UTF-8"?>
<networks />
```

Example

```
# /opt/FJSVcfmg/bin/cfmg_listvnet
<?xml version="1.0" encoding="UTF-8"?>
<networks>
  <network>
    <id>cloud-st-03_641</id>
    <name>cloudst_net1</name>
    <category>BUSINESS</category>
    <extid>70</extid>
    <addrset>
      <name>192.168.xxx.xxx</name>
      <subnet>192.168.xxx.xxx</subnet>
      <mask>255.255.xxx.xxx</mask>
      <start>192.168.xxx.xxx</start>
      <end>192.168.xxx.xxx</end>
    </addrset>
    <exclude>
      <range>
```

```

        <start>192.168.xxx.xxx</start>
        <end>192.168.xxx.xxx</end>
    </range>
</exclude>
<status>
    <num>30</num>
    <used>9</used>
    <avail>21</avail>
</status>
</network>
</networks>

```

Segment list display command

Synopsis

```
cfmg_listnetinfo [-v] [-utf8]
```

Description

This command outputs an XML file that contains a list of the segments that have been registered.

Options

Option	Description
-v	This option outputs the list in detailed format. If this option is omitted, the list is output in the simple format.
-utf8	This option outputs the list in UTF-8 format. This option is only valid for the Windows version. For the Windows version, the list is output in ISO-8859-1 format if this option is omitted.

Output format

This command uses the following format to output all of the segments that have been registered.

Detailed format	Simple format	Output format
*	*	<?xml version="1.0" encoding="UTF-8"?>
*	*	<networks>
*	*	<network>
*	*	<id>[Resource ID]</id>
*	*	<name>[Network name]</name>
*	*	<category>[Network type]</category>
*	-	<extid>[VLANID]</extid>
*	-	<addrset>
*	-	<name>[Address set name]</name>
*	-	<subnet>[Subnet address]</subnet>
*	-	<mask>[Net mask]</mask>
*	-	<start>[Start address]</start>
*	-	<end>[End address]</end>
*	-	</addrset>
*	-	<exclude>
*	-	<range>
*	-	<start>[Beginning of the excluded addresses]</start>
*	-	<end>[End of the excluded addresses]</end>
*	-	</range>
-	-	...
*	-	</exclude>
*	-	<status>
*	-	<num>[Number of addresses]</num>

Detailed format	Simple format	Output format
*	-	<used>[Number of reserved addresses]</used>
*	-	<avail>[Number of vacant addresses]</avail>
*	-	</status>
*	*	</network>
-	-	...
*	*	</networks>

*: Indicates information that is output.

-: Indicates information that is not output.

Cautions

This command outputs the following data if no segment has been registered.

```
<?xml version="1.0" encoding="UTF-8"?>
<networks />
```

Example

```
# /opt/FJSVcfmg/bin/cfmg_listnetinfo -v
<?xml version="1.0" encoding="UTF-8"?>
<networks>
  <network>
    <id>ST01-M_1446</id>
    <name>gyomu-3</name>
    <category>BUSINESS</category>
    <extid>10</extid>
    <addrset>
      <name>192.168.xxx.xxx</name>
      <subnet>192.168.xxx.xxx</subnet>
      <mask>255.255.xxx.xxx</mask>
      <start>192.168.xxx.xxx</start>
      <end>192.168.xxx.xxx</end>
    </addrset>
    <exclude>
      <range>
        <start>192.168.xxx.xxx</start>
        <end>192.168.xxx.xxx</end>
      </range>
    </exclude>
    <status>
      <num>20</num>
      <used>8</used>
      <avail>12</avail>
    </status>
  </network>
</networks>
```

Segment registration command

Synopsis

```
cfmg_addnetinfo -xml <Path to the segment information file>
```

Description

This command registers segments.

Options

Option	Description
-xml	This option specifies the absolute or relative path to the segment information file, using a string made up of printable ASCII characters. Enclose the string in double quotes (") if it contains blank spaces

Output format

None.

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_addnetinfo -xml /tmp/template_test/networks/sample.xml
```

Segment deletion command

Synopsis

```
cfmg_deletenetinfo [-f] -id <Resource ID>
```

Description

This command deletes segments.

Options

Option	Description
-f	This option executes the deletion without confirmation. If this option is omitted, a confirmation message will be output before the deletion takes place.
-id	Specify the resource ID of the segment to be deleted.

Output format

None.

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_deletenetinfo -id ST01-M_1446
Do you want to delete the segment? (Y/N) y
```

Detailed explanation of segment information

This section provides detailed segment information.

Segment information

Segment information files are XML documents that list configuration information for virtual networks.

Create and register a separate segment information file for each segment.

Refer to "Detailed segment information" for details on the items (tags).

Sample segment information files are stored in the following directory.

The service provider must create segment information files by referring to these samples.

```
[Windows]
<CIMS installation folder>\Systemwalker\SWCFMG\templates\networks\
```

```
[Linux]
/opt/FJSVcfmg/templates/networks/
```

Detailed segment information

Segment information files use the following XML format.

```
<?xml version="1.0" encoding="UTF-8" ?>
<network version="1.0">
  <id>[Resource ID]</id>
  <category>[Network type]</category>
</network>
```

The following table shows descriptions of each of these items (tags), as well as their settings.

Modify segment information files as necessary, by referring to the information in this table.

Tag name	Type	Setting range	Description	Required?	Settings
Id	string ASCII	1 to 32 bytes	This item specifies the resource ID.	M	Specify the resource ID corresponding to the virtual network that was verified using the <code>cfmg_listvnet</code> command (described in " Virtual network list display command ").
category	string ASCII	Select	This item specifies the category.	M	Select one of the following values: - MANAGEMENT : Management Segment - BUSINESS : Business segment

G.2.5 Template Information Manipulation Commands

This section explains the commands for manipulating template information.

Template information list display command

Synopsis

```
cfmg_listtemplate [-v] [-utf8]
```

Description

This command outputs an XML file that contains a list of the template information that has been registered.

Options

Option	Description
-v	This option outputs the list in detailed format. If this option is omitted, the list is output in the simple format.
-utf8	This option outputs the list in UTF-8 format. This option is only valid for the Windows version. For the Windows version, the list is output in ISO-8859-1 format if this option is omitted.

Output format

This command uses the following format to output all of the template information that has been registered.

Detailed format	Simple format	Output format
*	*	<?xml version="1.0" encoding="UTF-8"?>
*	*	<templates>
*	*	<template>
*	*	<id>[Template ID]</id>
*	*	<name>[Template name]</name>
*	-	<baseTemplateId>[Base template ID]</baseTemplateId>
*	-	<baseTemplateName>[Base template name]</baseTemplateName>
*	*	<ownerOrg>[Owner organization]</ownerOrg>
*	*	<ownerUser>[Owner user]</ownerUser>
*	*	<publicCategory>[Publication category]</publicCategory>
*	-	<designSheetPath>[Path to the design sheet]</designSheetPath>
*	-	<releaseDate>[Release date]</releaseDate>
*	-	<numOfMaxVnet>[Maximum number of VNETs]</numOfMaxVnet>
*	-	<numOfMaxVm>[Maximum number of VMs]</numOfMaxVm>
*	*	<description>[Description]</description>
*	-	<keyword>[Search keyword]</keyword>
*	*	<estimate>[Estimated amount]</estimate>
*	*	<license>[License information]</license>
*	*	<support>[Support information]</support>
*	*	<productId>[Model number]</productId>
*	*	<productName>[Product name]</productName>
*	*	<price>[Unit price]</price>
*	*	<chargeType>[Billing method]</chargeType>
*	*	<expectedUsage>[Expected monthly usage]</expectedUsage>
*	*	<showFlag>[Show flags]</showFlag>
*	-	<vnets>
*	-	<vnet>
*	-	<id>[Network ID]</id>
*	-	<name>[Name]</name>
*	-	<numOfMaxVm>[Maximum number of VMs]</numOfMaxVm>
*	-	<resourceId>[Resource ID]</resourceId>
*	-	<category>[Network type]</category>
*	-	</vnet>
*	-	...
*	-	</vnets>
*	-	<servers>
*	-	<server>
*	-	<no>[Server serial number]</no>
*	-	<imageId>[Image ID]</imageId>
*	-	<name>[Server name]</name>
*	-	<serverType>[Server type]</serverType>
*	-	<vmPool>[Resource name of the VM pool]</vmPool>
*	-	<storagePool>[Resource name of the storage pool]</storagePool>
*	-	<vnics>
*	-	<management>[Control NIC]</management>
*	-	<vnic>
*	-	<no>[NIC serial number]</no>
*	-	<networkId>[Connection destination network ID]</
*	-	networkId>
-	-	</vnic>
*	-	...
*	-	</vnics>
*	-	<vdisks>
*	-	<vdisk>
*	-	<no>[Disk serial number]</no>
*	-	<diskSize>[Disk capacity]</diskSize>
*	-	<storagePool>[Resource name of the storage pool]</
-	-	storagePool>
*	-	</vdisk>
*	-	...

Template information registration command

Synopsis

```
cfmg_addtemplate [-id <Template ID>] [-name <Template name>] - xml <Path to the template information file>
```

Description

This command registers template information.

Options

Option	Description
-id	This option specifies the template ID, using a string made up of up to 32 printable ASCII characters long. A registration error will occur if the template ID is already being used. If this option is specified, the value specified for this option takes precedence over the information in the template information file. If this option is omitted, a template ID is generated automatically.
-name	This option specifies the template name, using a string made up of up to 85 printable ASCII characters long. Enclose the string in double quotes (") if it contains blank spaces. If this option is specified, the value specified for this option takes precedence over the information in the template information file. If this option is omitted, the template name in the template information file takes effect. An error will occur if this option is omitted and a template name has not been entered in the template information file.
-xml	This option specifies the absolute or relative path to the template information file, using a string made up of printable ASCII characters. Enclose the string in double quotes (") if it contains blank spaces

Output format

The template ID that has been allocated is output using the following XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
  <id>[Template ID]</id>
</result>
```

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_addtemplate -xml /tmp/template_test/sample1.xml
<?xml version="1.0" encoding="UTF-8"?>
<result>
  <id>template-12c95768de8</id>
</result>
```

System template publication setup command

Synopsis

```
cfmg_showtemplate -id <Template ID> -on | off
```

Description

This command publishes and delists system templates.

Options

Option	Description
-id	This option specifies the ID of the template to be published or delisted.
-on	This option publishes the system template.
-off	This option delists the system template.

Output format

None.

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_showtemplate -id template-12c95768de8 -on
```

Template information deletion command

Synopsis

```
cfmg_deletetemplate [-f] -id <Template ID>
```

Description

This command deletes template information.

Options

Option	Description
-f	This option executes the deletion without confirmation. If this option is omitted, a confirmation prompt will be output before the deletion takes place.
-id	This option specifies the template ID for the template information file to be deleted.

Output format

None.

Cautions

None.

Example

```
# /opt/FJSVcfmg/bin/cfmg_deletetemplate -id template-12c95768de8  
Do you want to delete the template? (Y/N) y
```

Detailed explanation of template information

This section provides detailed template information.

Template information

Template information files are XML documents that list configuration information for system templates.

Create and register a separate template information file for each system template.

Sample template information files are stored in the following directory.

The service provider must create template information files by referring to these samples.

```
[Windows]  
Storage location: <CIMS installaton folder>\Systemwalker\SWCFMG\templates\templates\  
The following sample files are stored:
```

```
sample1.xml (for single server configurations)
sample2.xml (for two-tier server configurations)
sample3.xml (for three-tier server configurations)
```

[Linux]

Storage location: /opt/FJSVcfmg/templates/templates/

The following sample files are stored:

```
sample1.xml (for single server configurations)
sample2.xml (for two-tier server configurations)
sample3.xml (for three-tier server configurations)
```

Refer to "Detailed template information" for details on the items (tags).

For the image ID in the template information file, enter the image ID of a virtual image that has been registered.

Detailed template information

Template information files use the following XML format.

```
<?xml version="1.0" encoding="UTF-8" ?>
<template version="1.1">
  <id>[Template ID]</id>
  <lcid>[Locale ID]</lcid>
  <name>[Template name]</name>
  <baseTemplateId>[Base template ID]</baseTemplateId>
  <ownerOrg>[Owner organization]</ownerOrg>
  <ownerUser>[Owner user]</ownerUser>
  <publicCategory>[Publication category]</publicCategory>
  <designSheetPath>[Path to the design sheet]</designSheetPath>
  <releaseDate>[Release date]</releaseDate>
  <numOfMaxVnet>[Maximum number of VNETs]</numOfMaxVnet>
  <numOfMaxVm>[Maximum number of VMs]</numOfMaxVm>
  <productId>[Model number]</productId>
  <description>[Description]</description>
  <keyword>[Search keyword]</keyword>
  <estimate>[Estimated amount]</estimate>
  <license>[License information]</license>
  <support>[Support information]</support>
  <vnets>
    <vnet>
      <id>[Network ID]</id>
      <name>[Name]</name>
      <numOfMaxVm>[Maximum number of VMs]</numOfMaxVm>
      <resourceId>[Network resource ID]</resourceId>
    </vnet>
    ...
  </vnets>
  <servers>
    <server>
      <no>[Server serial number]</no>
      <imageId>[Image ID]</imageId>
      <imageName>[Image name]</imageName>
      <name>[Server name]</name>
      <serverType>[Server type]</serverType>
      <vmPool>[Resource name of the VM pool]</vmPool>
      <storagePool>[Resource name of the storage pool]</storagePool>
      <vnics>
        <management>[Control NIC]</management>
        <vnic>
          <no>[NIC serial number]</no>
          <networkId>[Connection destination network ID]</networkId>
        </vnic>
        ...
      </vnics>
    </server>
    ...
  </servers>
  <vdisks>
```

```

        <vdisk>
            <no>[Disk serial number]</no>
            <diskSize>[Disk capacity]</diskSize>
            <storagePool>[Resource name of the storage pool]</storagePool>
        </vdisk>
        ...
    </vdisks>
</server>
...
</servers>
</template>

```

The following table shows descriptions of each of these items (tags), as well as their settings.

Modify template information files as necessary, by referring to the information in this table.

The square brackets enclosing some of the tag names indicate that these tags can be omitted.

Tag name	Type	Setting range	Description	Required?	Settings
[id]	string ASCII	0 to 32 bytes	This item specifies the ID to be allocated to the template.	O	If this item is omitted, IDs will be assigned automatically.
[lcId]	string ASCII	Select	This item specifies the locale for template information.	M	Select one of the following values: - "ja": Japanese version - "en": English version
[name]	string UTF-8	Up to 85 characters	This item specifies the name of the template.	O	
baseTemplat Id	-	-	This item specifies the name of the base template.	U	
ownerOrg	string ASCII	Fixed value	This item specifies the organization ID of the organization to which the template belongs.	M	The value is fixed as "cfmgadm".
ownerUser	string ASCII	Fixed value	This item specifies the user ID of the user who registers the template.	M	The value is fixed as "cfmgadm".
publicCatego ry	string ASCII	Fixed value	This item specifies the category of the template.	M	The value is fixed as "PUBLIC". The template is available to all users.
designSheet Path	-	-	This item specifies the directory where the design sheet is stored.	U	
releaseDate	string ASCII	0 to 10 bytes	This item specifies the date when the template is to be published.	O	The format is "yyyy/mm/dd".
numOfMax Vnet	integer	1 to 99	This item specifies the maximum number of segments that can be used by the system in the template.	M	
numOfMax Vm	integer	0 to 10	This item specifies the maximum number of servers that can be used by the system in the template.	M	

Tag name	Type	Setting range	Description	Required?	Settings
productId	-	-	This item specifies a product ID for the template that will be used for billing purposes.	U	
description	string UTF-8	Up to 85 characters	This item contains a description of the template, explaining the system that the template produces, the content of the template, and so on.	O	
keyword	string UTF-8	Up to 85 characters	This item specifies a search keyword for the template.	O	The function for searching templates uses this keyword to find the template.
estimate	decimal	Fixed value	This item specifies the price of the template.	M	The value is fixed as "0".
license	string ASCII	Select	This item specifies whether a license has been assigned to the template.	M	Select the following value: - 0: No license assigned - 1: License assigned
support	string ASCII	Select	This item specifies whether support has been assigned to the template.	M	Select one of the following values: - 0: No support assigned - 1: Support assigned
vnets	-	-	This item specifies a segment for the system.	U	
[vnet]	-	One or more	This item specifies a separate segment information tag for each segment.	U	This item is required only when segment information exists.
Id	string ASCII	1 to 20 bytes	This item specifies an ID for identifying the segment within the template.	M	Specify a unique ID within the template. The value specified here is also specified as the value of the <networkId> tag under the <vnic> tag.
name	string ASCII	0 to 20 bytes	This item specifies the name of the segment.	O	
numOfMax Vm	integer	0 to 10	This item specifies the maximum number of servers that can be used by adding them to the segment.	M	
[resourceId]	string ASCII	1 to 32 bytes	This item specifies the resource ID of the virtualization network to be allocated to the segment.	M	Use the <code>cfmg_listvnet</code> command (described in " Virtual network list display command ") to verify resource IDs.
servers	-	-	This item specifies a server for the system.	U	
server	-	One or more	This item is for server information and specified for each server.	M	
No	integer	0 to 9	This item specifies the number of the server.	M	Specify a serial number for the server that is unique within the template.
imageId	-	-	This item specifies the image ID for the image to be deployed to the server.	U	It is necessary to register the image information and check the image ID beforehand.

Tag name	Type	Setting range	Description	Required?	Settings
imageName	string ASCII	1 to 32 bytes	This item specifies the image name of the image to be deployed to the server.	M	It is necessary to register the image information and check the image name in advance.
name	string UTF-8	Up to 85 characters	This item specifies the name of the server.	M	This is a name that is used to distinguish servers within the template, and is not the host name.
serverType	string ASCII	1 to 32 bytes	This item specifies the name of an L-Server Template that has been set up and will be selected as the default L-Server Template.	M	Specify the same value as was specified in the image information file.
[vmPool]	string ASCII	1 to 32 bytes	This item specifies the resource name of the VM pool where the server will be deployed. Specify the resource name in a format starting with "/". Example: /vmPool_2	O	If this option is omitted, the first VM pool will be selected. The VM pool can also be changed at deployment time.
[storagePool]	string ASCII	1 to 32 bytes	This item specifies the resource name for the storage pool where the server will be deployed.	O	If this option is omitted, the first storage pool will be selected. The storage pool can also be changed at deployment time.
vnic	-	-	This item specifies a NIC.	U	
[management]	integer	1 or more	This item specifies the number of the NIC to be specified as the control NIC.	M	Specify the value that was specified for the <no> tag under the <vnic> tag. This tag is required when multiple NICs have been specified. This tag can be omitted if there is only one NIC.
[vnic]	-	One or more	This item is specified for each NIC.	U	
No	integer	1 to 99	This item specifies the number of the NIC.	M	Specify a number for the NIC that is unique within the server.
networkId	string ASCII	1 to 20 bytes	This item specifies the segment ID for the segment to connect to.	M	Specify the value that was specified for the <id> tag under the <vnet> tag.
vdisk	-	-	This item specifies the expansion disk for the server.	U	
[vdisk]	-	One or more	This item is specified for each disk.	U	This item is required only when expansion disks exist. [Windows] - If the virtualization software is Hyper-V: Up to three <vdisk> tags can be specified.
[no]	integer	1 or more	This item specifies a number for the disk that is unique within the server.	M	For the shared disk, the same value must be specified for all servers.

Tag name	Type	Setting range	Description	Required?	Settings
[diskSize]	decimal	In decimal notation, to one decimal place	This item specifies the size of the disk.	M	Specify this value in GB. For the shared disk, the same value must be specified for all servers.
[storagePool]	string ASCII	1 to 32 bytes	This item specifies the resource name for the storage pool where the expansion disk will be deployed. Specify the resource name in a format starting with "/". Example: /StoragePool_2	O	If this item is omitted, the first storage pool is selected. The storage pool can also be changed at deployment time.

The symbols in the "Required?" column have the following meaning:

M: If the tag is specified, be sure to specify a value.

O: The value can be omitted.

U: There is no need to set a value. Only the tag itself is specified.

G.3 Interstage Single Sign-On Management Commands

This section explains the Interstage Single Sign-On Management Commands.

G.3.1 Overview of Interstage Single Sign-On Management Commands

The Interstage Single Sign-On Management Commands provide functions for creating and deleting Interstage Single Sign-On systems.

These commands can only be used by system administrators.

Structure of Interstage Single Sign-On Management Commands

The following table shows how the Interstage Single Sign-On Management Commands are organized.

Function name	Command name	Description
Interstage Single Sign-On system creation command	ssocsetup	This command creates Interstage Single Sign-On systems.
Interstage Single Sign-On system deletion command	ssoclunsetup	This command deletes Interstage Single Sign-On systems.
Interstage Single Sign-On start and stop command	ssocservicectl	This command starts and stops Interstage Single Sign-On.
Interstage Single Sign-On backup command	ssocbackup	This command backs up Interstage Single Sign-On.
Interstage Single Sign-On restore command	ssocrestore	This command restores Interstage Single Sign-On.

Command location

The storage location of the Interstage Single Sign-On Management Commands is shown below.

```
[Windows]
<CIMS installation folder>\Systemwalker\SWCTMG\SecurityManagement\sso\bin
```


Return values and error messages

For the results of Interstage Single Sign-On Management Commands, check the return values.

If the return value is 0, the command has terminated normally.

If the return value is other than 0, the command has terminated abnormally and an error message is output.

Refer to "Interstage Single Sign-on Management Commands Messages" in the "Systemwalker Software Configuration Manager V14g Message Guide" for details on return value and error messages.

The following example shows how to check return values.

[Windows]

```
C:\Users\Administrator>ssoclnsetup
C:\Users\Administrator>echo %errorlevel%
0
C:\Users\Administrator>
```

Description format

This section explains the description format for Interstage Single Sign-On Management Commands.

Synopsis

This section explains the synopsis for the commands.

```
"Command name" "Option" ["Option"] [...]
```

The following table explains each item of the command.

Item	Description
<Command name>	This is a command name.
<Option>	This is an option name, or an option name plus a parameter.
[<Option>]	Options in square brackets can be omitted.
[...]	This indicates that multiple options can be entered. However, these additional options can be omitted.

Description

This section explains the function of a command.

Options

This section explains options.

Cautions

This section explains important points to note when using the command.

Example

This section shows examples of how the command is used.

The examples in the explanations here are based on the Linux version.

G.3.2 Interstage Single Sign-On System Creation Command

Synopsis

```
ssoclnsetup <FQDN> <SSLConfName> [-rn <RepositoryName>] [-lp <LDAPPort>]
```

Description

This command creates Interstage Single Sign-On systems. The Interstage Single Sign-On system that is created is configured as below.

- This command creates or adds the following servers for Interstage Single Sign-On on a single server machine.
 - Repository server (update system)
 - Authentication server
 - Business Servers

The repository server (update system) and the authentication server are both created on the same Web server (Interstage HTTP Server).

Options

Option	Description
FQDN	Specify the FQDN (host name + domain name) of the server where this command is to be executed. This option cannot be specified using the following formats: <ul style="list-style-type: none"> - Host name only - IP address
SSLConfName	Specify the name of the SSL definition used by the Web server (Interstage HTTP Server) where the servers for the authentication infrastructure (the repository server (update system) and the authentication server) are to be created. The SSL definition name specified here must be created in advance. The SSL definition name can be between 1 and 32 characters long, including alphanumeric characters and the following symbols. <ul style="list-style-type: none"> - "-", "()", "[]", "_"
-rn RepositoryName	Specify the repository name of the SSO repository. If this option is omitted, "rep001" is specified as the default value. The repository name can be between 1 and 8 characters long, including alphanumeric characters and the underscore "_". However, note the following points when specifying a repository name: <ul style="list-style-type: none"> - The first character must be a letter. - If upper-case letters are specified, they will be converted into their lower-case equivalents. Note that this command uses the specified repository name to create a new SSO repository. For this reason, do not specify the name of an existing repository for this option.
-lp LDAPPort	Specify the port number of the SSO repository to be created. If this option is omitted, "389" is specified as the default value.

Cautions

After the command executes, a message will be displayed asking you to enter the password of the administrator DN for the SSO repository, so enter the password of the administrator DN. If "Retye" is displayed, enter the same password again.

The password can be between 1 and 128 characters long, including alphanumeric characters and the following symbols.

- ",", "+", "=", "-", ".", "_"

[Windows]

Execute the command as an Administrator.

Example

```
$ su -  
Password: <Password for the superuser>  
# /opt/FJSVcfmg/sso/bin/ssoclsetup FQDN SSLConfName
```

Note

- The Interstage Single Sign-On system that is created by this command uses the following ports. Accordingly, do not use these ports for other applications on the server where this command is executed.
 - 10443
 - 10550
 - 10555
- When this command executes, the service ID file for Interstage Single Sign-On is updated. An "sso00204" message is output to the system log when the service ID file is updated. Refer to the "Interstage Application Server Messages" for information on the sso00204 message.
- If processing is interrupted after this command has been executed but before the processing has completed, an Interstage Single Sign-On environment will be created in a state where the setup has not completed normally. In such cases, execute the ssoclunsetup command (described in "[G.3.3 Interstage Single Sign-On System Deletion Command](#)") and then execute this command again.

G.3.3 Interstage Single Sign-On System Deletion Command

Synopsis

```
ssoclunsetup
```

Description

This command deletes Interstage Single Sign-On systems.

Specifically, the following resources will be deleted.

- The following servers for Interstage Single Sign-On:
 - Repository server (update system)
 - Authentication server
 - Business Servers (*1)
- The SSO repository that the repository server (the update system) refers to
- The Web servers (Interstage HTTP Server) (*2) for which the servers for the authentication infrastructure (the repository server (update system) and the authentication server) have been created

Note

*1: All of the Business Servers for Interstage Single Sign-On that have been created on the machine where this command is executed will be deleted. However, the Web servers themselves will not be deleted.

*2: Only the Web server with the Web server name "SSOauth" (for which the servers for the authentication infrastructure (the repository server (update system) and the authentication server) have been created) will be deleted. Other Web servers will not be deleted.

Options

None.

Cautions

When the command is executed, the status of the resources to be deleted will be displayed as a message. The meaning of each resource is shown in the following table.

Resource name	Resource description
Repository Server	Repository server (update system)
Authentication Server	Authentication server
Business Server	Business Server
Web Server (<Web server name>) (*1)	The Web servers for which the servers for the authentication infrastructure (the repository server (update system) and the authentication server) have been created
SSO Repository (<Repository name>)	The SSO repository that the repository server (update system) refers to

The status of resources will be displayed as the following messages.

Message	Resource status
Exist	The resource exists.
Not Exist	The resource does not exist.

*1: The Web server name is fixed as "SSOAuth".

[Windows]

Execute the command as an Administrator.

Example

```
$ su -
Password: <Password for the superuser>
# /opt/FJSVcfmg/sso/bin/ssoclunsetup
```

Note

- This command does not back up resources before deleting the Interstage Single Sign-On system. Accordingly, if the resources for the Interstage Single Sign-On system are required, back up them before executing this command.
- This command stops the SSO repository that the repository server (update system) and the individual Interstage Single Sign-On servers refer to, and then deletes the Interstage Single Sign-On system. After the command has completed, the Web server (Interstage HTTP Server) to which Business Servers have been added will not be started.
- When the command is executed, a message will be displayed confirming whether to delete the Interstage Single Sign-On system. To delete the system, enter "yes". If a value other than "yes" is entered, "Command canceled." will be displayed and the Interstage Single Sign-On system will not be deleted.
- The command will terminate normally even if it is executed when the resources to be deleted do not exist. However, because there are no resources to be deleted, the resource deletion processing will not be performed.
- After this command has been executed, the Web server (Interstage HTTP Server) to which Business Servers for Interstage Single Sign-On have been added may fail to be deleted using the Interstage Management Console. In this case, delete the Web server by executing the `ihsdelete` command with the `-c` option specified. Refer to "ihsdelete" in the "Interstage Application Server (Command Edition)" for information on the `ihsdelete` command.

G.3.4 Interstage Single Sign-On Start and Stop Command

Synopsis

```
ssoclservicectl [start|stop]
```

Description

This command starts and stops the following Interstage Single Sign-On services.

- Interstage Management Console
- Interstage HTTP Server (*1)
- Interstage directory service repository (*2)
- *1: All Web servers configured on the machine where this command is executed will be started or stopped.
- *2: Only the SSO repository is started or stopped. Check the SSO repository name by selecting **[System] - [Security] - [Single Sign-on] - [Authentication infrastructure] - [Repository server] - [Settings tab] - [Repository server detailed settings]** from the Interstage Management Console. Note that it will not be possible to check the name if the Interstage Management Console has been stopped. Start the Interstage Management Console to check the name.

Options

Option	Description
start	Specify when starting a service. This option cannot be set at the same time as the stop option.
stop	Specify when stopping a service. This option cannot be set at the same time as the start option.

Cautions

[Windows]

Execute the command as an Administrator.

Example

- When starting a service

```
$ su -  
Password: <Password for the superuser>  
# /opt/FJSCVcfmg/sso/bin/ssoclservicectl start
```

- When stopping a service

```
$ su -  
Password: <Password for the superuser>  
# /opt/FJSCVcfmg/sso/bin/ssoclservicectl stop
```

Note

- Do not execute more than one of these commands at the same time.
- Execute this command in an environment that has been created with the Interstage Single Sign-On system creation command (ssocsetup).
- The Interstage Management Console also stops when this command is used to stop the service.
- If there are services that fail to stop or start after executing this command, refer to the messages output or to the messages output to the syslog, solve the problem, and then execute the command again.
- If the service started with this command is already running, a message to that effect is output.

- If the service stopped with this command is already stopped, a message to that effect is output.

G.3.5 Interstage Single Sign-On Backup Command

Synopsis

```
ssoclbackup <BackupDirectory>
```

Description

This command backs up an environment created with the Interstage Single Sign-On system creation command (ssoclsetup). Refer to "Interstage Single Sign-On System Creation Command" for information on the ssoclsetup command.

The following table shows the resources, files, and locations backed up by this command.

Backed up resources	Backed up files (*1)	Locations (*2)
Interstage Single Sign-On	Repository server definition file	<BackupDirectory>\ssoroot\SSO\sv_back
	• Authentication server definition file • Message files displayed in the authentication server's Web browser	<BackupDirectory>\ssoroot\SSO\ac_back
	• Business server definition file • Message files displayed in the business server's Web browser	<BackupDirectory>\ssoroot\SSO\az_back
Interstage HTTP Server	The following files for all Web servers • Interstage HTTP Server environment definition file • Password file Public root directory	<BackupDirectory>\ssoroot\IHS\
Interstage directory service	The following files in the repository being used as the SSO repository • Repository environment • Repository data • Access logs	<BackupDirectory>\ssoroot\IDS\rep_back\
Interstage certificate environment	• Certificate environment files • SSL definition File	<BackupDirectory>\ssoroot\SCS\

Information about the environment that was backed up is also stored in the following files.

Information stored	Details	Location ([Windows] above, [Linux] below)
SSO repository name	The name of the backed up SSO repository is stored as text.	<BackupDirectory>\ssoroot\info\rep_name.txt
SSO repository configuration information	Configuration information about the backed up SSO repository.	<BackupDirectory>\ssoroot\info\rep_config.txt
A list of the Interstage HTTP Server's Web server names	A list of the names of the backed up Web servers is stored as text.	<BackupDirectory>\ssoroot\info\web_server_list.txt

*1: Refer to "Maintenance (Resource Backup)" - "Backing Up and Restoring Resources" - "Resources that can be Backed Up and Restored" in the "Interstage Application Server Operator's Guide" for details on files.

*2: This is a destination to store each backup resource. Specify this path when only a part of resources is restored individually. Refer to "Maintenance (Resource Backup)" - "Backing Up and Restoring Resources" in the "Interstage Application Server Operator's Guide" for information on restoring individually.

Options

Option	Description
BackupDirectory	<p>Specify the directory where the resources are to be backed up, using a full path. Specify the path using no more than 100 bytes.</p> <p>If the specified backup directory does not exist, the directory is created.</p> <p>[Windows]</p> <p>The following characters cannot be used in the backup directory name. The colon can be used to indicate the drive letter and the backslash can be used as the directory separator.</p> <div style="border: 1px solid black; padding: 2px; width: fit-content;"> <p>: ; / * ? \ < > " ,</p> </div>

Cautions

[Windows]

Execute the command as an Administrator.

Example

If the backup destination is /backup

```
$ su -
Password: <Password for the superuser>
# /opt/FJSVcfmg/sso/bin/ssoclbackup /backup
```

 Note

- Do not execute more than one of these commands at the same time.
- Backup and restore can only be performed on the same operating systems.
- Do not perform backup if backup or restore is being performed on the same server.
- Before backing up, use the ssoclservicectl command to stop all services connected to Interstage Single Sign-On. Refer to "Interstage Single Sign-On Start and Stop Command" for information on the ssoclservicectl command.
- This command will end with an error if backup resources ("ssoroot" directory) already exist in the backup directory.
- Execute this command in an environment that has been created with the Interstage Single Sign-On system creation command (ssoclsetup).
When the single sign-on system created by not using configuration command is backed up, back up referring to "Maintenance (Resource Backup)"-" Backing Up and Restoring Resources" in the "Interstage Application Server Operator's Guide".
- If there are contents or CGI outside of the directories specified by the Interstage HTTP Server DocumentRoot directive, use one of the following methods to back these up separately.

[Windows]

copy command or Explorer

- If processing is interrupted after this command has been executed but before the processing has completed, backup will not have been completed. If this occurs, delete the backup directory and then execute the command again.

G.3.6 Interstage Single Sign-On Restore Command

Synopsis

```
ssoclrestore <BackupDirectory>
```

Description

This command restores Interstage Single Sign-On environments that have been backed up with the ssoclbackup command.

The following are restored:

- The following Interstage Single Sign-On servers:
 - Repository server
 - Authentication server
 - Business Server
- SSO repository
- Interstage HTTP Server
- Interstage certificate environment

When executing this command, one of the situations below must apply to the SSO repository and Interstage HTTP Server.

- SSO repository (*1)
 - A repository with the same name as the SSO repository that was backed up exists and it has the same configurations for the following (*2):
 - Database storage directory
 - Public directory
 - User password encryption scheme
 - A repository with the same name as the SSO repository that was backed up does not exist
- Interstage HTTP Server (*3)
 - The backed up operating environment, number of Web servers, and the names of the Web servers all match (*4)
 - No Web servers exist
 - Immediately after installing the product

*1: Check the status of the repository configuration in **[System] - [Services] - [Repository] - [repository name] - [Settings]** in Interstage Management console

*2: Refer to information which was saved when the ssoclbackup command was executed for information on SSO repository name of SSO repository and the setting information when they were backed up..

*3: Check the status of Interstage HTTP Server configuration by the ihdisp command. Refer to "Web Server Operation Edition" in the "Interstage Application Server Reference Manual (Command Edition)" for information on the ihdisp command.

*4: Refer to the list of Web server names for the Interstage HTTP Server saved when the ssoclbackup command was executed to find out the configuration status of the Interstage HTTP Server that was backed up.

Options

Option	Description
BackupDirectory	Specify the directory where the resources were backed up using the ssoclbackup command, using a full path. Specify the path using no more than 100 bytes. [Windows] The following characters cannot be used in the backup directory name. The colon can be used to indicate the drive letter and the backslash can be used as the directory separator.

Option	Description
	:;/*?\<> ",

Cautions

[Windows]

Execute the command as an Administrator.

Example

If the backup destination is /backup

```
$ su -
Password: <Password for the superuser>
# /opt/FJSVcfmg/sso/bin/ssoclrestore /backup
```

Note

- Do not execute more than one of these commands at the same time.
- Backup and restore can only be performed on the same operating systems.
- Specify the same LANG environment variable as when the backup was made.
- Do not restore if backup or restore is being performed on the same server.
- Before restoring, use the ssoclservicectl command to stop all services connected to Interstage Single Sign-On. Refer to "Interstage Single Sign-On Start and Stop Command" for information on the ssoclservicectl command.
- This command will end with an error if there are insufficient backup resources in the backup directory. Refer to "Interstage Single Sign-On Backup Command" for information on the backup resources.
- When restoring a backed up repository, the repository name, database storage directory, and access log storage directory will be the same as the original environment where the backup was made. If there is no path to the database storage directory and access log storage directory, create the paths before restoring.
- If there are contents or CGI outside of the directories specified by the Interstage HTTP Server DocumentRoot directive, use one of the following methods to restore these separately.

[Windows]

copy command or Explorer

- When restoring using this command after reinstalling this product, follow the precautions below:
 - The ssocsetup command does not need to be used for setup.
 - Install the product on a machine that has the same disk configuration as when the backup was made
 - Install the product using the same path as when the backup was made.
- If there are services that fail to be restored after executing this command, refer to the messages output, solve the problem, and then execute the command again.
- If processing is interrupted after this command has been executed but before the processing has completed, restore will not have been completed. If this occurs, execute the command again.
- A list of the backup resources in the backup directory will be displayed as follows when this command is executed. Then a message will be displayed asking whether to proceed with the restoration. Confirm the items in the list, then enter "yes" to proceed. The meaning of each resource is shown in the following table.

Resource name	Resource description
Repository Server	Repository server resources
Authentication Server	Authentication server resources

Resource name	Resource description
Business Server	Business Server resources
Web Server	Interstage HTTP Server resources
SSO Repository (Repository name)	SSO repository resources
Interstage Certificate Environment	Interstage certificate environment resources

Appendix H Registered Software IDs

The following software information is included in this product.

Use this information when necessary.

Storage location

The storage location is shown below.

```
[Windows]
<CIMS installation folder>\Systemwalker\SWCFMG\templates\softwares\
```

Registered software IDs

The following table shows the software IDs that have already been registered with this product.

Registered software ID	Software name	OS	Version
SW00000003	Windows Server 2008 Standard (32bit)	Windows	6.0
SW00000004	Windows Server 2008 Standard (64bit)	Windows64	6.0
SW00000005	Windows Server 2008 Enterprise (32bit)	Windows	6.0
SW00000006	Windows Server 2008 Enterprise (64bit)	Windows64	6.0
SW00000008	Windows Server 2008 R2 Standard	Windows64	6.1
SW00000009	Windows Server 2008 R2 Enterprise	Windows64	6.1
SW00000010	Red Hat Enterprise Linux 5 (for x86)	Linux	5.5
SW00000011	Red Hat Enterprise Linux 5 (for Intel64)	Linux64	5.5
SW00000091	Systemwalker Service Quality Coordinator Enterprise Edition	Windows	V13.4
SW00000093	Systemwalker Service Quality Coordinator Enterprise Edition	Linux	V13.4
SW00000113 (Note)	Systemwalker Software Configuration Manager (Agent)	Windows	V14.1
SW00000114 (Note)	Systemwalker Software Configuration Manager (Agent)	Windows64	V14.1
SW00000115 (Note)	Systemwalker Software Configuration Manager (Agent)	Linux	V14.1
SW00000116 (Note)	Systemwalker Software Configuration Manager (Agent)	Linux64	V14.1

Note: This is the reserved software ID that has already been registered using "Systemwalker Software Configuration Manager (Agent)" that was installed as the Business Server Agent for this product. There is no need to set these software IDs that have already been registered, on the system template.

Software IDs have not been registered for the following operating systems. Templates for registering these operating systems are provided as shown below. Use these operating systems by entering the product key for the Windows operating system in the <license> tag and registering the software information.

Software name	OS	Version	Software information file name
Windows Server 2003 R2, Standard	Windows	5.2	WS2003R2_SE.xml

Software name	OS	Version	Software information file name
Windows Server 2003 R2, Enterprise	Windows	5.2	WS2003R2_EE.xml
Windows Server 2003 R2, Standard x64 Edition	Windows64	5.2	WS2003R2_SE_x64.xml
Windows Server 2003 R2, Enterprise x64 Edition	Windows64	5.2	WS2003R2_EE_x64.xml

Appendix I Registering and Deregistering Managed Servers

This appendix explains the procedures for registering and deregistering Managed Servers during operations.

Registering and deregistering Managed Servers involves the following two steps:

- Registering or deregistering the VM hosts for which resource information is to be collected
- Registering or deregistering the devices for which eco information (temperature and power consumption information) is to be collected

Each of these steps is explained below.

I.1 Registering VM Hosts

The flow for registering VM hosts is as follows:

1. Setting up resource information collection from the VM host
2. Registering the VM host on the Admin Server

I.1.1 Setting up Resource Information Collection from the VM Host

Resource information collection must be set up for the VM host on a Managed Server. A VM host is a server virtualization software product that runs on a server in order to operate virtual machines. An example of a VM host is VMware ESX for VMware.

The setup procedure varies depending on which virtualization software is used. Perform the setup procedure by referring to the article on the virtualization software being used.

For VMware

1. Use the VMware vSphere Client to log in directly to the managed VMware ESX. For the **IP address / Name** field, enter the host name or IP address for VMware ESX. Enter **root** for User name and the password for the root account for Password, and then click the **<Login>** button.
2. If a **[Security Warning]** window regarding certificates appears, click the **<Ignore>** button.
3. In the **[VMware vSphere Client]** window, select the **[Users and Groups]** tab (for Version 4.1 of VMware this will be Local Users and Groups), and then click **<Users>**.
4. Right-click on the user table and then select **Add**.
5. In the **[Add New User]** dialog box, enter "sqcsqc001" (the default value) for Login, User Name and Password. Then, select the **[Grant shell access to this user]** checkbox, and click the **<OK>** button.

The user "sqcsqc001" will be added to the user table.



For Version 4.1 of VMware, access permissions for using ssh must be set up for the "sqcsqc001" user that was added above. Use the following procedure to set up access permissions.

1. Use the VMware vSphere Client to change the settings for the SSH server to automatic execution.
 - a. Select the **[Configuration]** tab of the VMware vSphere Client.
 - b. Select **[Software]** and then **[Security Profile]** on the left-hand side of the window.
 - c. Click **[Properties]** at the top right-hand corner of the window.

- d. The **[Firewall Properties]** dialog box will open, so select the **SSH Server** row and then select the checkbox to the left of **SSH Server**.
 - e. With the **SSH Server** row selected, click the **<Options>** button at the bottom right of the dialog box.
 - f. The **SSH server (sshd) option** dialog box will open, so select **Start automatically when a port opens and stop when all ports close in Activation policy**. Start the service by clicking **Start at Service command**. If the service has already started, **Start** is grayed out, but this is not a problem and you can continue the operation.
 - g. Click the **<OK>** button to close the **SSH server (sshd) option** dialog box and the **[Firewall Properties]** dialog box.
2. Log in to VMware ESX with the root account.
 3. Open the "/etc/pam.d/sshd" file and add the following entry to the last line.

```
account    required    pam_access.so
```

4. Open the "/etc/security/access.conf" file and add the following line.

```
+:<Name of the user that has been added>:<IP address of the Admin Server>.
```

 **Note**

- If an "-:ALL:ALL" line already exists, be sure to add the new line before the "-:ALL:ALL" line. If the new lines are added after the "-:ALL:ALL" line, the settings will not take effect.
- Be sure to add a period (".") after the IP address.

```
(Example of the file before the changes)
+:root:ALL
+:vpxuser:ALL
+:vslauser:ALL
-:ALL:ALL

(Example of the file after the changes: The underlined section has been added)
Note: When the added user is sqcsqc001, and the IP address of the Admin Server is
192.168.1.142
+:root:ALL
+:vpxuser:ALL
+:vslauser:ALL
+:sqcsqc001:192.168.1.142.
-:ALL:ALL
```

6. Log in to VMware ESX (mentioned above) with the root account.
7. Execute the visudo command to edit the sudoers file.

Add the following line to the end of the sudoers file, and then save the file. In the following example, the connection account is "sqcsqc001" (the default value). Change the value to match the actual connection account.

[Setting example]

```
sqcsqc001 ALL=(ALL) NOPASSWD: /usr/bin/esxtop
sqcsqc001 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-vmhbadevs
sqcsqc001 ALL=(ALL) NOPASSWD: /usr/sbin/vdf
sqcsqc001 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-nics
sqcsqc001 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-vswitch
sqcsqc001 ALL=(ALL) NOPASSWD: /bin/egrep
sqcsqc001 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-scsidevs
```

Information

If the environment allows you to log in to Managed Servers from the Admin Server, you can check whether the sudoers file has been edited correctly by logging in to the Managed Server with the connection account (e.g. "sqcsqc001") from the Admin Server and executing the "sudo -l" command. If the following window is displayed, the sudoers file has been edited correctly.

[Execution result example]

```
$ sudo -l
User sqcsqc001 may run the following commands on this host:
(ALL) NOPASSWD: /usr/bin/esxstop
(ALL) NOPASSWD: /usr/sbin/esxcfg-vmhbadevs
(ALL) NOPASSWD: /usr/sbin/vdf
(ALL) NOPASSWD: /usr/sbin/esxcfg-nics
(ALL) NOPASSWD: /usr/sbin/esxcfg-vswitch
(ALL) NOPASSWD: /bin/egrep
(ALL) NOPASSWD: /usr/sbin/esxcfg-scsidevs
```

For Hyper-V

With this version, information cannot be collected from Hyper-V.

I.1.2 Registering the VM Host on the Admin Server

Execute the VM host registration command on the machine where the Admin Server for CIMS has been created.

[Windows]

Open a command prompt, and execute the following command.

```
> cd <CIMS installation folder>\Systemwalker\SWCTMG\Dashboard\bin
> addVMHostInfo -h <host_address> -u <username> -p <password> -v <vm_type>
```

Parameters

Parameter	Description
-h <host_address>	Specify the IP address or host name of the VM host for the Managed Server.
-u <username>	Specify the user name that was added in " I.1.1 Setting up Resource Information Collection from the VM Host ".
-p <password>	Specify the password for the user name that was added in " I.1.1 Setting up Resource Information Collection from the VM Host ".
-v <vm_type>	Specify the virtualization software type for the Managed Server. Specify either of the following values according to the virtualization software type used. - For VMware: VMWARE - For Hyper-V: HYPERV Note: "HYPERV" can only be specified with the Windows version.

Example:

[Windows]

```
> cd <CIMS installation folder>\Systemwalker\SWCTMG\Dashboard\bin
> addVMHostInfo -h 192.168.1.100 -u sqcsqc01 -p sqcsqc01 -v VMWARE
```

Note

After executing the commands, be sure to apply the registered information by using the procedure described in "I.3 Applying Registered Information". If the information is not applied, information about the registered devices will not be displayed in the dashboard.

I.2 Registering Devices for which Eco Information is Collected

The "eco information" discussed in this section refers to information about the temperature and power consumption for devices.

The following procedure is used to register the devices for which eco information is to be collected.

1. Setting up the devices for which eco information is to be collected
2. Registering the devices on the Admin Server

Note

- This product can collect eco information for the following devices:
 - PRIMERGY BX600
 - PRIMERGY BX900
 - PRIMERGY RX200
 - PRIMERGY RX300
- Only temperature information can be collected from PRIMERGY BX600 and BX900. Power consumption information will not be collected.
- This product supports SNMP versions v2 and v2c.

I.2.1 Setting up the Devices for which Eco Information is Collected

To collect eco information, SNMP traps must be set up for the target device. Specifically, set up the following items:

- Set the IP address of the Admin Server as the SNMP trap destination
- Set the SNMP community to "public"

The procedure for setting up SNMP traps varies depending on the target device type. Refer to the manuals for each device for details.

This section explains the procedure for setting up SNMP traps, using the PRIMERGY BX900 as an example.

1. Open the Web User Interface window for the ServerView management blade for the target device.

Use a Web browser to access the Web User Interface for the ServerView management blade.

- For HTTP

http://[<IP address of the ServerView management blade>]:[<Port number (default: 80)>]

- For HTTPS

https://[<IP address of the ServerView management blade>]:[Port number (default: 443)>]

2. A window for entering the password will be displayed, so enter the user name and password that have been specified for the ServerView management blade.
3. The start page for the ServerView management blade will be displayed. Select the [**Settings**] - [**System Unit**] and then **SNMP** from the menu on the left.
4. Select **SNMP Setting** in the tab on the right.
5. Check that the **Enable SNMP** checkbox has been selected in the **Enable SNMP** settings. If this checkbox has not been selected, select it and click the <Apply>.

6. Check that there is a "public" entry in the *SNMP community* settings. If not, use *Add community* below the *SNMP community* and specify "public" for *Community* and "read only" for the user privileges. Then click the <Apply>.
7. Add the IP address of the Admin Server to the *SNMP trap destination* settings. Use *Event type of New trap destination* below that to set *Destination address/server name* to the IP address of the Admin Server, *Community* to "public" and *Type of Event* to "AllEvent", and then click the <Apply>.
8. Confirm that the IP address of the Admin Server has been added to the *SNMP trap destination* settings as shown in the window
9. Close the window by signing out from the Web User Interface for the ServerView management blade.

I.2.2 Registering Devices on the Admin Server

On the machine where the Admin Server for CIMS has been created, execute the command for registering devices for which eco information is to be collected.

[Windows]

Open a command prompt, and execute the following command.

```
> cd <CIMS installation folder>\Systemwalker\SWCTMG\Dashboard\bin
> addEcoInfo -s <snmp_address> -m <machine_type>
```

Parameters

Parameter	Description
-s <snmp_address>	Specify the IP address or host name of the device for which eco information is to be collected.
-m <machine_type>	Specify the model name of the device for which eco information is to be collected. The following shows the models for which eco information can be collected, as well as how to specify the model names. <ul style="list-style-type: none"> - PRIMERGY BX600: BX600 - PRIMERGY BX900: BX900 - PRIMERGY RX200: RX200 - PRIMERGY RX300: RX300

Execution example:

[Windows]

```
> cd <CIMS installation folder>\Systemwalker\SWCTMG\Dashboard\bin
> addEcoInfo -s 192.168.1.101 -m RX300
```



Note

After executing the commands, be sure to apply the registered information by using the procedure described in "I.3 Applying Registered Information". If the information is not applied, information about the registered devices will not be displayed in the dashboard.

I.3 Applying Registered Information

After performing the operations in "I.1.2 Registering the VM Host on the Admin Server" or "I.2.2 Registering Devices on the Admin Server", apply the registered information by executing the following command at least 15 minutes after the registration operations have completed. If multiple VM hosts or devices have been registered consecutively, execute the CMDB refresh command at least 15 minutes after the last registration operation completed.

[Windows]

```
> cd <CIMS installation folder>\Systemwalker\SWRBAM\CMDB\FJSVcmdbm\bin  
> cmbdbrefresh -q
```



Note

Note that it sometimes takes a while (10 to 20 minutes) before the results of executing the CMDB refresh command are actually applied.

I.4 Deregistering VM Hosts

To deregister a VM host, delete the information for the corresponding Managed Server from the connection account definition file and the remote monitoring definition file, and then execute the update command. Refer to "3.2 Virtual Resource Management" and "3.2.3 Settings for Monitoring Servers" in the "Systemwalker Service Quality Coordinator User's Guide" for details on each file.

Use the following procedure to deregister VM hosts from the Admin Server.

1. Log in to the Admin Server.
2. Delete information for the Managed Server by editing the connection account definition file. The connection account definition file contains an entry corresponding to the IP address of the Managed Server as shown in the following example, so delete the entry.

- File storage location

[Windows]

```
<CIMS installation folder>\Systemwalker\SQL_DATA\control\remoteAccount.txt
```

- File format

".ini" file format

- Example: If the IP address of the Managed Server is 192.168.103.65

```
[192.168.103.65]  
CONNECTTYPE=SSH  
USER=sqcsqc001  
PASSWORD=/PPDcezlmhgTUjXYbKdpfA==
```

3. Delete information for the Managed Server by editing the remote monitoring definition file. The remote monitoring definition file contains an entry corresponding to the IP address of the Managed Server as shown in the following example, so delete the entry.

- File storage location

[Windows]

```
<CIMS installation folder>\Systemwalker\SQL_DATA\control\remoteAgent.txt
```

- File format

".ini" file format

- Example: If the IP address of the Managed Server is 192.168.103.65

```
[192.168.103.65]  
HOSTNAME=192.168.103.65  
VMATYPE=VMWARE  
ACCOUNT=192.168.103.65  
CONNECTION=ON
```

4. Execute the update command for Systemwalker Service Quality Coordinator.

[Windows]

Open a command prompt, and execute the following command.

```
> cd <CIMS installation folder>\Systemwalker\SWCTMG\Dashboard\bin
> updateSQC.bat
(Example: If the installation folder is C:\Fujitsu)
> cd C:\Fujitsu\Systemwalker\SWCTMG\Dashboard\bin
> updateSQC.bat
```

Information

To continue using the VM host even after it has been deregistered, restore the setup operations performed on the VM host in "[I.2.1 Setting up the Devices for which Eco Information is Collected](#)" as necessary. Specifically, this involves the following tasks:

- Delete the user that has been added (e.g., "sqcsqc001").
- Cancel the automatic execution settings for the SSH server.
- Delete the line that was added to /etc/pam.d/sshd.
- Delete the line that was added to /etc/security/access.conf.
- Delete the line that was added to the sudoers file.

I.5 Deregistering Devices for which Eco Information is Collected

To deregister a device for which eco information is to be collected, delete the information about the corresponding Managed Server from the configuration information file for SNMP Agents, and then execute the update command. Refer to "12.3.3 Setting the SNMP Agent Configuration Information File" in the "Systemwalker Service Quality Coordinator User's Guide" for details on each file.

Use the following procedure to deregister the target devices (for which eco information is to be collected) from the Admin Server.

1. Log in to the Admin Server.
2. Delete information for the Managed Server by editing the configuration information file for SNMP Agents. The configuration information file contains an entry corresponding to the IP address of the Managed Server as shown in the following example, so delete the entry.

- File storage location

[Windows]

```
<CIMS installation folder>\Systemwalker\SQC_DATA\control\ecoAgentInfo.txt
```

- File format

".ini" file format

- Example: If the IP address of the Managed Server is 192.168.103.65

```
192.168.103.65,v2c,public,BX600
```

3. Execute the update command for Systemwalker Service Quality Coordinator.

[Windows]

Open a command prompt, and execute the following command.

```
> cd <CIMS installation folder>\Systemwalker\SWCTMG\Dashboard\bin
> updateSQC.bat
```

Information

To continue using the device (for which eco information is to be collected) even after it has been deregistered, restore the setup operations performed on the device in "[I.2.1 Setting up the Devices for which Eco Information is Collected](#)" as necessary. Specifically, this involves the following task:

- Delete the Admin Server from the SNMP trap destinations.
-

Appendix J Messages

This appendix explains the messages that are output or displayed by this product.

J.1 Messages during Installation

This section explains the messages that are output or displayed while this product is being installed.

Messages for the Manager

The file already exists at the installation destination.

Description

The specified installation directory already contains files.

Action

The uninstallation may not have completed. Either perform the uninstallation again, or delete the files in the installation directory. Then make sure that there are no files in the installation directory, and try again.

The error occurred.

Description

An error has occurred with the command.

Action

Collect the message in question, and then contact Fujitsu technical support.



Note

Contact Fujitsu technical support if messages other than the message above are output or displayed.

J.2 Messages during Command Execution

This section explains the messages that are output or displayed when the commands for this product are executed.

Messages for the cims mgrctl command

67101

FJSVcims:ERROR:67101:not privileged

Description

The execution user is not an administrator for the operating system.

Action

Perform the operation with administrator privileges for the operating system.

For Windows Server 2008, users with administrator privileges other than the *Administrator* user cannot execute commands with administrator privileges by starting [Command Prompt] from the [Start] menu.

Such users should perform operations after right-clicking on the [Command Prompt] item in the [Start] menu and then selecting [Run as Administrator] from the context menu to open a command prompt.

67124

FJSVcims:ERROR:67124:not enough memory

Description

The command cannot run because there is not enough memory.

Action

Check whether there is enough memory.

Close any unnecessary programs, and then try again.

67146

FJSVcims:ERROR:67146:<filename>:file not found

Description

The *filename* file for this product does not exist.

Action

In either of the following cases, restore the whole system or reinstall this product.

- If the corresponding file has been deleted
- If the corresponding file has been deleted as a result of system failure or an error with the disk or file system

In all other cases, collect this message and the [Investigation data](#), and contact Fujitsu technical support.

67147

FJSVcims:ERROR:67147:<filename>:permission denied

Description

The *filename* file for this product cannot be accessed.

Action

Collect this message and the [Investigation data](#), and then contact Fujitsu technical support.

67198

FJSVcims:ERROR:67198:command execution error.<detail>

Description

An error has occurred with a command for the Manager.

Action

Detailed information about the message is indicated in the *<detail>* section.

Take action according to the content indicated in the *<detail>* section.

- If "registry access error" is indicated in the *<detail>* section

Use the following procedure to check whether the installation for this product (Cloud Infrastructure Management Software) has completed.

[Windows]

Select the [Start] - [Programs] or [All Programs] - [Fujitsu] - [Uninstall (middleware)].

- If "syscall=" is indicated in the *<detail>* section

Collect the message in question and the [Investigation data](#), and then contact Fujitsu technical support.

67244

FJSVcims:ERROR:67244:another command is running

Description

This command may already be executing.

Action

Wait until the command has executed, and then try again.

67999

FJSVcims:ERROR:67999:internal error, <details>

Description

An error has occurred with the command.

Action

- If this message was output after the command execution had been canceled using "Ctrl+C" or some other method, the command has been canceled normally, and there is no need to take any action.

In other cases, collect the message in question and the [Investigation data](#), and then contact Fujitsu technical support.

J.3 How to Collect Investigation Data

Collect the following data as investigation data for this product.

Investigation data

[Windows]

```
<CIMS installation folder>\Manager\var\log\cims_cli.log*
```

Glossary

Admin Server

The server where CIMS runs. Services are centrally managed on the Admin Server.

application process

A process that defines the procedures for approval and assessment processing for the application processing performed by users. Application processes are executed only when they have been enabled. Application processes are set up by the service provider department.

assessment

The act of assessing applications from service users.

Business Segment

A network segment for performing communications for business purposes.

cloud

An expression that abstracts the virtualization technology for platforms ranging from servers through to applications.

cloud computing

A configuration that allows ICT resources to be accessed from anywhere via connected devices.

control NIC

The NIC for virtual servers that perform communications with the Admin Server.

Information and Communication Technology (ICT)

A generic term relating to information and communications technology.
The hardware and software that make up a system are referred to as "ICT resources".

Intelligent Blade Panel (IBP)

One of the operating modes for PRIMERGY LAN switch blades.

This mode can be used by linking to ServerView Virtual I/O Manager (VIOM), and associations between server blades and the LAN switch blade can be set up easily and safely.

L-Server

A logical platform configured by combining various individual resources.

L-Server Template

A template defining specifications such as the number of CPUs, memory capacity and disk capacity for the resources to be allocated to an L-Server.

Managed Server

The server where the Agent for CIMS runs. Services that are automatically deployed also run on Managed Servers.

Manager Segment

A network segment for performing communications for administration and other purposes.

Manager View

A GUI for performing the following functions provided by this product.

- Provisioning Management
- Patch management
- Taking snapshots and restoring from snapshots

organization

An department or division to which system users or system administrators belong.

private cloud

Refers to a configuration where a company constructs a cloud computing system within its private network, so that it can provide services to departments within the company and subsidiaries and so on. This kind of environment is also referred to as a "private cloud environment".

In contrast, configurations where services are provided to general users via the Internet are referred to as "public clouds".

Provisioning Management

A function that follows system templates to deploy virtual platforms, automatically deploy various software programs (only operating systems in the case of CIMS), and automatically set up parameters.

service specifications

A specification that defines service usage in order to clarify the content and status of the services to be provided to users.

single sign-on

A function that enables (allows) access to multiple Web servers with a single sign-on (authentication).

system administrator

The person responsible for creating and administrating systems using Cloud Infrastructure Management Software. System administrators also manage service users, and the organizations to which they belong.

system template

Information that defines the logical configuration of ICT resources and software.

Template Management

A function for creating virtual platforms by enabling users to create and register the various resources that make up a system template, and to create system templates by combining these resources.

Template Management Commands

The commands that provide functions for registering, listing, updating and deleting the various files that make up a system template.

virtual platform

A concept whereby virtual servers, virtual storage and virtual networks make up a single virtual system.