

Systemwalker Service Quality Coordinator

A decorative horizontal band with a dark blue background and abstract, glowing green and cyan wave-like patterns and light streaks.

User's Guide (Website Management Functions Edition)

Windows/Solaris/Linux

J2X1-7664-01ENZ0(00)
July 2012

Preface

Purpose of this manual

This manual explains how to use the Website administration functions of Systemwalker Service Quality Coordinator.

Target audience

Systemwalker Service Quality Coordinator is designed to visually express the quality of the various services provided by IT systems, and optimize business costs. This manual is aimed at individuals who use Systemwalker Service Quality Coordinator to manage Websites.

Organization of Systemwalker Service Quality Coordinator manuals

The Systemwalker Service Quality Coordinator manuals are organized as follows:

- Systemwalker Service Quality Coordinator Technical Guide
Provides an overview of the functions of Systemwalker Service Quality Coordinator.
- Systemwalker Service Quality Coordinator Installation Guide
Explains how to install and set up Systemwalker Service Quality Coordinator.
- Systemwalker Service Quality Coordinator User's Guide
Explains how to use the functions of Systemwalker Service Quality Coordinator.
- Systemwalker Service Quality Coordinator User's Guide (Console Edition)
Explains how to use those functions related to console windows.
- Systemwalker Service Quality Coordinator User's Guide (Dashboard Edition)
Explains how to use dashboard functions.
- Systemwalker Service Quality Coordinator Reference Guide
Explains commands, data formats, messages and so on.
- Systemwalker Service Quality Coordinator Troubleshooting Guide
Explains how to handle any problems that may occur.
- Systemwalker Service Quality Coordinator User's Guide (Website Management Functions Edition)
Explains the Systemwalker Service Quality Coordinator functions that relate to analyzing Web usage and monitoring Web content tempering.
- Systemwalker Service Quality Coordinator User's Guide (Systemwalker User Management and Single Sign-On Edition)
Explains how to install and use the Systemwalker User Management and Systemwalker Single Sign-On functions when Systemwalker Service Quality Coordinator is to be used.
- Systemwalker User's Guide - Systemwalker User Management and Single Sign-On
Explains how to install the Systemwalker User Management function and the Systemwalker Single Sign-On function.
- Systemwalker Service Quality Coordinator Glossary
This manual explains Systemwalker Service Quality Coordinator terminology.

Positioning of this document

This manual is common to the following Systemwalker Service Quality Coordinator products for Windows, Linux and Oracle Solaris:

- Systemwalker Service Quality Coordinator Enterprise Edition V15.0.0
- Systemwalker Service Quality Coordinator Standard Edition V15.0.0

Abbreviations

- The term "Windows Server 2008" refers to the following products:
 - Microsoft(R) Windows Server(R) 2008 R2 Foundation
 - 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) 2008 Foundation
 - Microsoft(R) Windows Server(R) 2008 Standard
 - Microsoft(R) Windows Server(R) 2008 Enterprise
 - Microsoft(R) Windows Server(R) 2008 Datacenter
 - Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM)
 - Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM)
 - Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM)
 - Microsoft(R) Windows Server(R) 2008 Standard Server Core
 - Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Server Core
 - Microsoft(R) Windows Server(R) 2008 Enterprise Server Core
 - Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Server Core
 - Microsoft(R) Windows Server(R) 2008 Datacenter Server Core
 - Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) Server Core
- The term "Windows Server 2003" refers to the following products:
 - 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, Datacenter Edition
 - Microsoft(R) Windows Server(R) 2003, Standard Edition
 - Microsoft(R) Windows Server(R) 2003, Enterprise Edition
 - Microsoft(R) Windows Server(R) 2003, Datacenter Edition
- The term "Windows 7" refers to the following products:
 - Windows(R) 7 Home Premium
 - Windows(R) 7 Professional
 - Windows(R) 7 Enterprise
 - Windows(R) 7 Ultimate

- The term "Windows Vista" refers to the following products:
 - Windows Vista(R) Home Basic
 - Windows Vista(R) Home Premium
 - Windows Vista(R) Business
 - Windows Vista(R) Enterprise
 - Windows Vista(R) Ultimate
- The term "Windows XP" refers to the following products:
 - Microsoft(R) Windows(R) XP Home Edition
 - Microsoft(R) Windows(R) XP Professional Edition
- Microsoft(R) SQL Server(TM) is abbreviated as "SQL Server".
- Microsoft(R) Cluster Server is abbreviated as "MSCS".
- Oracle Solaris might be described as Solaris, Solaris Operating System, or Solaris OS.
- Oracle WebLogic Server is abbreviated as "WebLogic Server".
- Oracle Database is abbreviated as "Oracle".
- Systemwalker Centric Manager is abbreviated as "Centric Manager".
- Systemwalker Resource Coordinator is abbreviated as "Resource Coordinator".
- Interstage Application Server is abbreviated as "Interstage".
- Symfoware Server is abbreviated as "Symfoware".
- VMware(R) ESX(R) is abbreviated as "VMware ESX" or "ESX".
- VMware(R) ESXi(TM) is abbreviated as "VMware ESXi" or "ESXi".
- VMware(R) vCenter(TM) is abbreviated as "VMware vCenter" or "vCenter".
- VMware vSphere(R) is abbreviated as "VMware vSphere".
- Versions of Systemwalker Service Quality Coordinator that operate under Windows are referred to as "Windows versions".
- Versions of Systemwalker Service Quality Coordinator that operate under Solaris are referred to as "Solaris versions".
- Versions of Systemwalker Service Quality Coordinator that operate under Linux are referred to as "Linux versions".
- Solaris and Linux versions of Systemwalker Service Quality Coordinator are referred to collectively as "UNIX versions".
- The term "Agent" is used to refer to articles common to both Agent for Server and Agent for Business.

Conventions used in this document

- Edition-specific information

This manual deals mainly with the Standard Edition and Enterprise Edition of Systemwalker Service Quality Coordinator. The following symbols appear in the title or text of an article to distinguish between the Standard Edition (standard specification) and the Enterprise Edition.

EE

This indicates that the article relates specifically to Systemwalker Service Quality Coordinator Enterprise Edition.

SE

This indicates that the article relates specifically to Systemwalker Service Quality Coordinator Standard Edition.

- Information specific to Windows or UNIX versions

This document contains information common to both Windows versions and UNIX versions of Systemwalker Service Quality Coordinator. Information specific to only the Windows versions and information specific to only the UNIX versions are distinguished from common information by attaching the following symbols:

[Windows]

This indicates that the article relates specifically to Windows versions.

[UNIX]

This indicates that the article relates specifically to UNIX versions.

The symbols **[Solaris]**, **[Linux]**, **[AIX]**, and **[HP-UX]** are used to distinguish Solaris, Linux, AIX, and HP-UX versions of Systemwalker Service Quality Coordinator.

If notice should be paid, the information is distinguished from common information by attaching the following symbols:



This indicates that the article relates specifically to Solaris versions.

Symbols

The symbols used with commands are explained below.

[Entry example]

```
[ PARA = { a | b | c | ... } ]
```

[Meaning of each symbol]

Symbol	Meaning
[]	Items enclosed in square brackets are optional.
{ }	Select one of the items enclosed in braces ({ }).
_	When all optional items enclosed in square brackets ([]) are omitted, the default value indicated by an underscore (_) is used.
	Select one of the items separated by vertical bars.
...	The item immediately before the ellipsis (...) can be repeatedly specified.

Export Restriction

If this document is to be exported or provided overseas, confirm the regulations of Foreign Exchange and Foreign Trade Control laws adhere to all legal requirements according to those laws.

Trademarks

- Adobe, Adobe Reader, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Apache and Tomcat are trademarks or registered trademarks of The Apache Software Foundation.
- HP-UX is a registered trademark of the Hewlett-Packard Company.

- IBM, IBM logo, AIX, AIX 5L, HACMP, Power, and PowerHA are trademarks of International Business Machines Corporation in the United States and other countries.
- Intel and Itanium are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.
- Linux is a trademark or registered trademark of Mr. Linus Torvalds in the United States and other countries.
- Microsoft, Windows, Windows Server and the titles or names of other Microsoft products are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.
- Oracle Solaris might be described as Solaris, Solaris Operating System, or Solaris OS.
- Red Hat, RPM, and all the trademarks and logos based on Red Hat are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- VMware, the VMware logo, Virtual SMP and VMotion are trademarks or registered trademarks of VMware, Inc. in the United States and other countries.
- Other company names and product names are trademarks or registered trademarks of respective companies.
- The company names, system names, product names and other proprietary names that appear in this document are not always accompanied by trademark symbols (TM or (R)).

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

Acknowledgement

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

July 2012

Copyright 2003-2012 FUJITSU LIMITED

Contents

Part 1 Overview.....	1
Chapter 1 Overview.....	2
1.1 Overview of Each Function.....	2
1.1.1 Trend Viewer.....	2
1.1.1.1 Supported log formats.....	5
1.1.1.2 Functional configuration.....	7
1.1.1.2.1 Usage Analysis Function components.....	8
1.1.1.2.2 SQC extended log.....	9
1.1.2 Contents Tampering Monitor.....	9
1.1.2.1 Function overview and features.....	9
1.1.2.2 Function configuration.....	10
Chapter 2 SQC operating configurations.....	11
2.1 Basic Form.....	11
2.1.1 Locating methods of the analysis data.....	11
2.1.1.1 Operation of the Managed Server.....	11
2.1.1.2 Operation of the Management Server.....	12
2.1.2 Group Operation.....	13
2.1.2.1 Server grouping.....	13
2.1.3 Configuration for tampering monitoring.....	14
Part 2 Installation (Basic).....	15
Chapter 3 General Procedure for Basic Installation.....	16
3.1 System Configuration.....	16
3.2 Environment Settings procedures.....	17
3.3 Estimating Resources.....	19
3.3.1 Management Server.....	19
3.3.1.1 Usage Analysis.....	19
3.3.1.1.1 Space estimation in the Usage DB.....	19
3.3.1.1.2 Space estimation of the CSV format log file.....	19
3.3.1.1.3 Space estimation of SQC extended log.....	19
3.3.1.2 Tamper Monitor.....	20
3.3.2 Managed Server.....	20
3.3.2.1 Trend Viewer.....	20
Chapter 4 Environment Settings for the Managed Server.....	21
4.1 Settings for Web Server.....	21
4.1.1 Microsoft(R) Internet Information Services 6.0.....	21
4.1.2 Apache HTTP Server 1.3.26.....	22
4.1.3 Netscape(R) Enterprise Server 3.0.....	24
4.1.4 InfoProvider Pro (packaged with Interstage Application Server).....	25
4.2 Environment Settings for Usage Analysis.....	26
4.2.1 Defining httpd.conf.....	27
4.2.2 Defining the usage DB environment definition file.....	27
4.2.3 Enhancing public Web server security.....	30
4.3 Settings for service start.....	31
Chapter 5 Environment Settings for the Management Server.....	32
5.1 Settings for Web Server.....	32
5.1.1 Windows.....	32
5.1.1.1 Setting virtual directories.....	32
5.1.1.2 Handler mapping settings.....	34
5.1.1.3 Setting virtual directories property.....	34
5.1.1.4 Setting of basic attestation.....	35

5.1.2 UNIX.....	36
5.2 Environment Settings for Usage Analysis.....	39
5.3 Registering System Configuration.....	42
5.4 Settings for Service Start.....	42
Chapter 6 Environment Settings for the Report Server.....	43
6.1 Setting a virtual directory.....	43
6.2 Setting a virtual directory property.....	44
Chapter 7 Configuring the Operating Environment.....	45
7.1 Registering a Management Server.....	45
7.1.1 Web Site Management.....	46
7.2 Registering a Managed Server.....	48
7.2.1 Managed server information.....	48
7.2.1.1 Registering a Managed Server.....	48
7.2.2 Registering an Analysis Target Server.....	51
7.2.2.1 Registering a usage service.....	52
7.3 Registering a Group.....	54
7.3.1 Group Information.....	55
7.4 Registering a Report Server.....	58
Chapter 8 Checking Operation.....	60
8.1 Displaying the Usage Analysis Window.....	60
8.2 Displaying a Report.....	62
Part 3 Installation(Application).....	70
Chapter 9 Web Marketing.....	71
9.1 Determining an Analysis Method and Configuration.....	71
9.1.1 Overview of analysis type.....	71
9.1.1.1 Traffic display.....	72
9.1.1.2 Response analysis page.....	72
9.1.2 Analyzing cyclic transition.....	73
9.1.3 Analysis that identifies users.....	73
9.1.4 Analysis using CSV output.....	74
9.1.4.1 Analysis using the analysis window and analysis using CSV output.....	74
9.1.5 Integrated analysis with data on the backbone system.....	74
9.1.5.1 Overview of integrated analysis with data on the backbone system.....	74
9.1.5.2 Method of integrated analysis with data on the backbone system.....	75
9.1.6 If you would like to analyze response.....	76
9.1.6.1 SQC Extended Log Collectin.....	76
9.1.6.2 Response logs.....	76
9.1.6.2.1 Outline.....	76
9.1.6.2.2 Making settings for log collection.....	77
9.1.6.2.3 Stopping log collection.....	81
9.1.6.2.4 Log format.....	81
9.1.6.3 SQC extended log file.....	82
9.1.6.3.1 File name.....	82
9.1.6.3.2 Capacity estimation.....	83
9.1.6.3.3 Switching the SQC extended log file.....	83
9.1.6.4 Setting an extended log environment definition file.....	83
9.1.6.4.1 File storage location.....	84
9.1.6.4.2 Example of definition.....	84
9.1.6.5 Setting a usage DB environment definition file.....	85
9.1.6.6 Analysis using the usage analysis window.....	86
9.1.6.7 Analyzing response using the management server.....	87
9.1.7 If you would like to analyze user types.....	90
9.1.7.1 Specifying users.....	91

9.1.7.2 Environment settings.....	91
9.1.7.2.1 Setting a Web server log output.....	91
9.1.7.2.2 Setting a usage DB environment definition file.....	93
9.1.7.3 Analysis using the usage analysis window.....	94
9.1.8 If you would like to make analysis in subnetwork units.....	95
9.1.8.1 Environment settings.....	95
9.1.8.1.1 Setting an option definition file.....	95
9.1.8.2 Analysis using the usage analysis window.....	96
9.1.9 If you would like to make analysis with specific subnetworks excluded.....	97
9.1.9.1 Environment settings.....	97
9.1.9.1.1 Setting an option definition file.....	98
9.1.9.2 Analysis using the usage analysis window.....	98
9.1.10 If you would like to make analysis with specific URLs excluded.....	99
9.1.10.1 Environment settings.....	99
9.1.10.1.1 Setting an option definition file.....	99
9.1.10.2 Analysis using the usage analysis window.....	100
9.2 Notes.....	100
9.2.1 Date and time.....	100
9.2.2 Operation when moving to other URL.....	100
9.2.3 Extension name display.....	101
9.2.4 Host name/IP address display when DNS conversion is not possible.....	101
9.2.5 Handling of the URL name to be analyzed.....	101
9.2.6 Notes on selecting the URL based breakdown from the analysis method box.....	101
9.2.7 Notes on selecting the URL extension based breakdown from the analysis method box.....	101
9.2.8 Notes on displaying analysis results of mass log data.....	101
Chapter 10 Monitoring for Tampering with Web Contents.....	102
10.1 Overview of Monitoring.....	102
10.2 Environment Settings.....	104
10.2.1 Setting the send environment for tampering detection reports.....	105
10.3 Registering Monitoring Requirements.....	105
10.3.1 Specifying a content publish location.....	106
10.3.2 Specifying an execution frequency for tampering inspection.....	108
10.3.3 Specifying a tampering detection reporting destination.....	109
10.4 Registering Contents.....	111
10.4.1 Distributing a content publish notifier.....	113
10.4.2 Notifying content publish (contents administrator job).....	113
Part 4 User's Guide.....	114
Chapter 11 Analyzing Web Site Usage.....	115
11.1 Usage DB Engine.....	115
11.1.1 Usage DB Registration Engine.....	115
11.1.1.1 Outline.....	115
11.1.1.2 Start operation.....	115
11.1.1.3 Stop operation.....	116
11.1.1.4 Start up time.....	117
11.1.1.5 URL extensions valid for analysis.....	118
11.1.1.6 Space estimation in the Usage DB.....	118
11.1.1.7 Usage DB switching.....	119
11.1.1.8 Notes on use of Usage DB Registration Engine.....	119
11.1.2 Usage DB Reference Engine.....	120
11.1.2.1 Outline.....	120
11.1.2.2 Start operation.....	120
11.1.2.3 Usage DB reference port number.....	125
11.1.2.4 Stop operation.....	125
11.1.3 Usage DB backup and restore.....	128
11.1.3.1 Backing up the Usage DB.....	128

11.1.3.2 Restoring the Usage DB.....	128
11.1.3.3 Deleting the Usage DB.....	129
11.2 Analysis Window.....	130
11.2.1 Outline.....	130
11.2.2 Start operation.....	130
11.2.2.1 Before startup.....	131
11.2.2.2 Start Operation.....	131
11.2.3 Stop operation.....	131
11.2.4 Configuring the analysis window.....	131
11.2.4.1 Analysis window features.....	132
11.2.5 Analysis window options.....	135
11.2.5.1 Traffic display.....	136
11.2.5.2 Response analysis page.....	136
11.2.6 Operation of analysis page.....	137
11.2.6.1 Performing data analysis.....	137
11.2.7 Notes.....	143
11.2.7.1 Date and time.....	143
11.2.7.2 Operation when moving to other URL.....	144
11.2.7.3 Extension name display.....	144
11.2.7.4 Host name/IP address display when DNS conversion is not possible.....	144
11.2.7.5 Handling of the URL name to be analyzed.....	145
11.2.7.6 Notes on selecting the URL based breakdown from the analysis method box.....	145
11.2.7.7 Notes on selecting the URL extension based breakdown from the analysis method box.....	145
11.2.7.8 Notes on displaying analysis results of mass log data.....	145
11.3 CSV Output.....	145
11.3.1 Outline.....	145
11.3.2 Start operation.....	145
11.3.2.1 Startup.....	145
11.4 SQC Extended Log Collection.....	146
11.4.1 Response log.....	146
11.4.1.1 Outline.....	146
11.4.1.2 Making settings for log collection.....	147
11.4.1.3 Stopping log collection.....	151
11.4.1.4 Log format.....	151
11.5 Navigation Guide for the Usage Analysis Window.....	152
11.5.1 Analyzing changes in the number of Web site visitors.....	152
11.5.1.1 Analysis using the usage analysis window.....	153
11.5.2 If you would like to make analysis in page units.....	154
11.5.2.1 Analysis using the usage analysis window.....	154
11.5.3 Analyzing site navigation.....	155
11.5.3.1 Analyzing site navigation for an entire Web site.....	155
11.5.3.2 Analyzing site navigation for a specific customer.....	156
11.5.3.3 Analyzing site navigation for a specific URL.....	158
Chapter 12 Evaluating the Usage.....	161
12.1 Registered Report Window.....	161
12.1.1 OutLine.....	161
12.1.2 Start operation.....	161
12.1.3 Quit operation.....	162
12.1.4 Window configuration.....	163
12.2 Registry of report Window.....	165
12.2.1 OutLine.....	165
12.2.2 Start operation.....	165
12.2.3 Quit operation.....	166
12.2.4 Window configuration.....	166
12.3 Generate of report window.....	168
12.3.1 OutLine.....	168

12.3.2 Start operation.....	168
12.3.3 Quit operation.....	169
12.3.4 Window configuration.....	169
12.4 History of Reports Window.....	171
12.4.1 OutLine.....	171
12.4.2 Start operation.....	171
12.4.3 Quit operation.....	171
12.4.4 Window configuration.....	171
12.5 Report paramters.....	173
12.5.1 Category and Report type.....	173
12.5.2 Other report parameters.....	176
12.5.2.1 Common items.....	176
12.5.2.2 Report Object and Select Condition.....	177
12.5.3 Report contents.....	178
Chapter 13 Using the Contents Tampering Monitor.....	181
13.1 Viewing the Environment Settings Window.....	181
13.1.1 Contents Tampering Monitor window (menu window).....	181
13.1.2 Tamper Monitor URL Entry window.....	183
13.1.3 Tamper Monitor URL Modify window.....	185
13.1.4 Confirm URL Delete window.....	187
13.1.5 Environment Properties window.....	187
13.1.6 Action Statement window.....	188
13.2 Tampering Detection Notice.....	190
13.2.1 E-mail notice.....	190
13.3 Customization.....	192
13.3.1 If you would like to make tampering inspection with a shorter interval.....	192
13.3.2 If you would like to make tampering inspection at an optional time.....	193
Part 5 References.....	194
Chapter 14 Setting the Web Site Management Window.....	195
14.1 Environment Settings Window.....	196
14.1.1 Management Server Settings window.....	198
14.1.2 Managed server setting window.....	200
14.1.2.1 Managed Server Information window.....	203
14.1.2.2 Usage service information window.....	205
14.1.3 Report Server Settings window.....	208
14.1.4 Group Settings window.....	209
14.1.4.1 Group Information window.....	210
14.1.5 Notes.....	212
14.1.5.1 Deleting unnecessary temporary files.....	212
Chapter 15 SQC file types.....	214
15.1 List of SQC file types.....	214
15.2 SQC Definition Files.....	214
15.2.1 Usage DB Environment Definition File.....	215
15.2.1.1 File storage location.....	215
15.2.1.2 File internal configuration.....	216
15.2.1.3 File internal format (basic).....	217
15.2.1.4 File internal format (analysis target server definition block).....	217
15.2.1.5 File internal format (log definition block to be analyzed).....	222
15.2.2 Extended Log Environment Definition File.....	232
15.2.2.1 File storage location.....	232
15.2.2.2 File internal configuration.....	233
15.2.2.3 File internal format (basic).....	233
15.2.2.4 File internal format (extended log definition block).....	233
15.2.3 Option Definition File.....	235

15.2.3.1 File storage location.....	235
15.2.3.2 File internal configuration.....	236
15.2.3.3 File internal format (analysis definition block for each subnetwork).....	236
15.2.3.4 File internal format (definition block with analysis of a specific subnetwork omitted).....	238
15.2.3.5 File internal format (definition block with analysis of a specific URL omitted).....	239
15.2.4 Usage DB Output file.....	240
15.2.4.1 Usage DB Output file format.....	240
15.2.4.2 Capacity estimation.....	243
15.2.5 SQC extended log file.....	244
15.2.5.1 File name.....	244
15.2.5.2 Capacity estimation.....	244
15.2.5.3 Switching a SQC extended log file over to another.....	245
15.2.6 Usage Log file.....	245
15.2.6.1 Usage Log file format.....	245
15.2.6.2 Capacity estimation.....	249
15.2.6.3 Deleting a Usage Log file.....	249
15.3 Report data file.....	251
15.3.1 Report data file.....	251
15.3.1.1 Report data file format.....	252
Chapter 16 Troubleshooting.....	259
16.1 Usage Analysis.....	259
16.2 Report Display.....	262
16.3 Contents Tampering Monitor.....	265
Chapter 17 Messages.....	268
17.1 Contents Tampering Monitor messages.....	268
17.1.1 Contents Tampering Monitor - settings windows.....	268
17.1.2 Content publish notifier.....	268
17.1.3 Tampering inspection program.....	269
17.2 Usage Analysis Function.....	270
17.2.1 Usage DB Registration Engine.....	270
17.2.2 Usage DB Reference Engine.....	272
17.2.3 Analysis window.....	274
17.2.4 CSV output command.....	275
17.2.5 Common messages.....	276
Chapter 18 Command Reference.....	278
18.1 Contents Tampering Monitor.....	278
18.1.1 Contents Tampering Monitor.....	278
18.1.1.1 Content publish notifier.....	278
18.1.1.1.1 MpupdtCntnts command location.....	278
18.1.1.1.2 MpupdtCntnts command specifications.....	278
18.1.1.1.3 Content list file format.....	281
18.2 Usage Analysis Function.....	282
18.2.1 Trend Viewer.....	282
18.2.1.1 dbprt.....	282
Chapter 19 Environment Maintenance.....	286
19.1 Management Server Resources.....	286
19.1.1 Database.....	286
19.1.1.1 Usage DB.....	286
19.2 Managed Server Resources.....	286
19.2.1 Database.....	286
19.2.1.1 Usage DB.....	286

Part 1 Overview

Part 1 gives an overview of the SQC Website Management functionality and the modes in which Systemwalker Service Quality Coordinator Usage Analysis can operate.

Chapter 1 Overview	2
Chapter 2 SQC operating configurations	11

Chapter 1 Overview

Chapter 1 gives an overview of the Systemwalker Service Quality Coordinator Website Management functionality.

1.1 Overview of Each Function

1.1.1 Trend Viewer

The Web Site Trend Viewer is used for analyzing the usage of systems that are comprised of Web servers and proxy servers.

On the Web server and Proxy server, access information from the user is accumulated in the log file. From this log file, the Web site Trend Viewer can extract and analyze such details as URL, user (user name, IP address, host name, and ID set in Cookie), and time. This user-access analysis enables timely decision-making on the services constructed on your Internet/ Intranet.



.....
If, for example, a page on employment information is published using the Internet, you can use the Web site Trend Viewer to readily find out which schools the students referencing the recruit page attend.

If a Proxy server is set up to reduce the network load, it is easy to determine whether the Proxy server setting is effective by analyzing the cache hit rate and traffic.

.....
The Trend Viewer provides the following functions:

- Site access analysis
Usage in terms of access to Web sites, such as the extent of access to Web sites, such as which pages are popular, who accesses Web pages and how often, and which links are used.
- Site navigation analysis
Usage in terms of customer behavior, such as which page the customers view, how long they view each page, and how they navigate through pages.

The Web site Trend Viewer edits data on the usage of the Web server and Proxy server and displays it on the Web browser (Web page) in table or graph form. It can be used on any Web browser connected to the Web server and network.

Data types and periods can be analyzed from a variety of viewpoints; buttons on the Web page enable you to switch views easily. An advanced-analysis function is also provided so you can carry out analyses focused on specific URLs and clients.

The usage of the Web site Trend Viewer is roughly classified into the following two modes:

1. Display trend data by switching the analysis window according to the analysis type.
2. Use the regular report function to report regular analysis results such as daily reports and monthly reports.

The Web site Trend Viewer displays the results by switching the analysis window depending on the analysis type. For example, you can use the Trend Viewer to make the following analyses:

Web server

Analysis type	Analyzed Data type to be used
to view a usage summary for the entire server	View a summary of the analysis results. The summary displays the following report data:

Analysis type	Analyzed Data type to be used
	<ul style="list-style-type: none"> - Session count (total) - Request count (total) - Traffic (total) - Cache hit count (total) - Error count (total)
To find how popular the Web service is	View the session report. In the session report, the number of people who visited the site can be checked. Multiple accesses to a page from the same person are counted as one person.
To find which page of the Web service is most popular	View the request report. In the request report, which pages are popular and which types of user view such pages can be checked.
To find the order the Web services pages accessed by the user	View the page navigation report. In the page navigation report, you can see the order in which Web service pages are accessed.
To find whether any unauthorized access or site link disconnection has occurred	View the error report. Errors detected by the server include access by unauthorized persons and missing links when such links are referenced on the site. Checking for the occurrence of such errors can enable uses to find of whether any unauthorized access or site link disconnection has taken place. Contents of errors that have occurred are displayed on the analysis window in the error report.

Proxy server

Analysis type	Analyzed data type to be used
To view a usage summary for the entire server	View a summary of the analysis results. The summary displays the following report data: <ul style="list-style-type: none"> - Session count (total) - Request count (total) - Traffic (total) - Cache hit count (total) - Error count (total)
To know the validity of the number of sessions	View the session report. You can learn how many users in the Proxy server access external servers at one time
To know the validity of URL for caching	View the request report. You can observe which external pages are accessed from within the Proxy server and who accesses most often.
To know the validity of the caching amount	View the traffic report. You can observe how much data is received in response to accessing of external servers from within the Proxy server. Based on this result, you can decide whether improvement is required if the caching amount on the server is small.
If you want to know caching effects	View the cache report. You can determine how effectively the cache definition on the server is working.

Analysis type	Analyzed data type to be used
	You can examine the hit rate for cache information held by the Proxy server with respect to access to external servers from within the Proxy server or access from outside the Proxy server.

You can make more detailed analyses by carrying out the above analyses focusing on the following methods:

Analysis method type	Description
Client host name	Analyses are carried out using the host name obtained by converting the client IP address by using DNS as a key. Any IP address that cannot be converted by DNS is displayed as is without conversion. The client here is the following: <ul style="list-style-type: none"> - In the Web server analysis, any user who accesses the Web service. - In the Proxy server analysis, any user who accesses external servers from within the Proxy server. However, in the case of the Proxy server in reverse operation, the client has the same meaning as that of the Web server.
Client IP address	Analyses are made using the client IP address as a key.
Authorization user name	If the Web server or Proxy server performs authorization, the user name for the authorization is used for analysis.
User agent	Analyses are made using the browser used by the user to access the Web server or Proxy server as a key.
Referrer host name	Analyses are made regarding through which links the constructed Web service is reached, using the referrer host name as a key.
Referrer IP address	Analyses are made regarding through which links the constructed Web service is reached, using the referrer IP address as a key.
Remote host name	Analyses are made on the Proxy server using the host name of the page accessed from within the Proxy server as a key. In the case of a Proxy server in reverse operation, to which Web server a request was made from outside is analyzed, using the host name as a key.
Remote IP address	Analyses are made on the Proxy server using the IP address of the page accessed from within the Proxy server as a key. In the case of a Proxy server in reverse operation, to which Web server a request was made from outside is analyzed, using the IP address as a key.
URL	Analyses are made using the URL name accessed from the client as a key.
Entry URL	Analyses are made using URL as an entry point of the URL accessed from the client as a key.
Exit URL	Analyses are made using URL as an exit point of the URL accessed from the client as a key.
Referrer URL	Analyses are made regarding through which links the constructed Web service is reached, using the referrer URL as a key.

Analysis method type	Description
URL extension	Analyses are made regarding which extension is accessed most often, using the extension as a key.
Access ID	Analyses are made using ID set in Cookie as a key. If the user is authenticated by CGI on the Web server, setting ID in Cookie can make analyses in which users are identified.
Subnet	Analyses are made using a subnet, which groups client IP addresses, as a key.



For details on how to specify the analyzed data type and analysis method type, refer to "11.2 Analysis Window".

The Trend Viewer can output collected/accumulated information in the CSV file format. By entering this information for such OLAP/mining tool as "SymfoWARE e-Business Intelligence Suite", information can be utilized at a higher level; for example, analyses can be executed that combine data on the backbone system, enabling the more effective use of Web sites by your business.

The analysis results can also be printed for reference.

1.1.1.1 Supported log formats

The Web site Trend Viewer supports the following log formats. Other logs can be analyzed if their log formats are defined.

For information on how to define log formats, refer to "4.2 Environment Settings for Usage Analysis" (Managed server) and "5.2 Environment Settings for Usage Analysis" (Management server)

No	Log format	Server name
1	W3C (CERN) Common log format	W3C httpd (CERN httpd)
2	Apache Common log format	Apache Web Server
3	Apache Custom log format	Apache Web Server
4	Microsoft IIS log format	Microsoft Internet Information Services
5	NCSA Common log format	Microsoft Internet Information Services
6	W3C Extended log format	Microsoft Internet Information Services
7	Netscape Enterprise Server Common log format	Netscape Enterprise Server
8	Netscape Enterprise Server Flexible log format	Netscape Enterprise Server
9	Netscape Enterprise Server Custom log format	Netscape Enterprise Server
10	Fujitsu InfoProvider Pro Common log format	Fujitsu InfoProvider Pro
11	Fujitsu InfoProvider Pro Extended log format	Fujitsu InfoProvider Pro

No	Log format	Server name
12	Netscape Proxy Server Common log format	Netscape Proxy Server
13	Netscape Proxy Server Extended log format	Netscape Proxy Server
14	Netscape Proxy Server Extended2 log format	Netscape Proxy Server
15	Netscape Proxy Server Flexible log format	Netscape Proxy Server
16	Netscape Proxy Server Custom log format	Netscape Proxy Server
17	Squid Common log format	Squid
18	Squid Native log (version 1.1) format	Squid
19	DeleGate Common log format	DeleGate
20	DeleGate Custom log format	DeleGate
21	DeleGate Default log format	DeleGate
22	Fujitsu InfoProxy Common log format	Fujitsu InfoProxy
23	Fujitsu InfoProxy Common log format	Fujitsu InfoProxy
24	Microsoft Proxy Server Webproxy log format	Microsoft Proxy Server
25	SQC Extended log format	Systemwalker Service Quality Coordinator

Note

"SQC Extended log format" in No. 25 is a format of log files accumulated by collecting the SQC extended logs. For more details, refer to "[11.4 SQC Extended Log Collection](#)".

The Web Site Trend Viewer saves the log with the character code and LF(line feed) code according to the operating OS where it runs. The combinations are as follows:

[Windows]

Character Code	LF code
ASCII	CR + LF

[UNIX]

Character Code	LF code
ASCII	LF

Note

Normal operation is not guaranteed if the combination differs the above combinations. Notice should be paid especially when network file on a remote network is involved.

1.1.1.2 Functional configuration

Web Trend Viewer is composed of the Web service analysis function and the extended log collector.

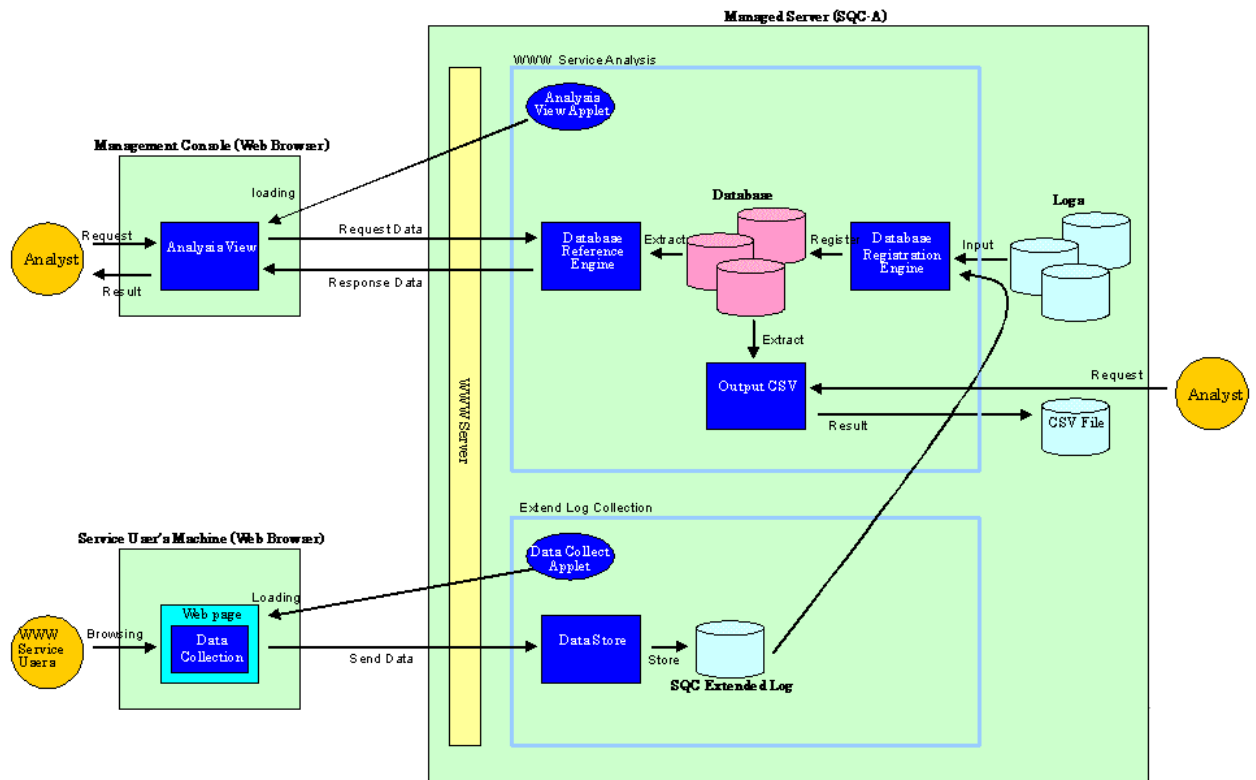
As shown in the following figures, two functional configurations of the Web site Trend Viewer are available; one for analyses made on the Managed Server, and one for analyses made on the Management Server.

Carry out analyses on the Management Server in the following types of operation:

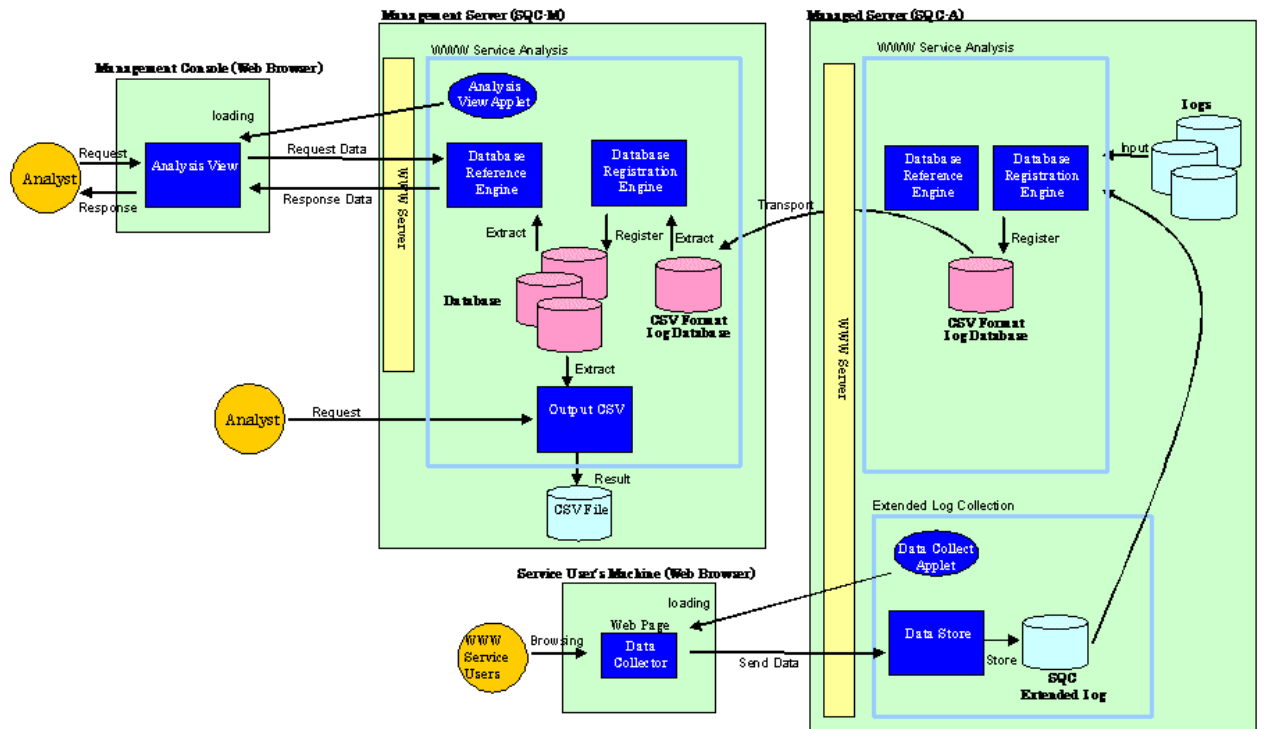
- The Web site is configured using multiple Web servers and the entire Web site should be analyzed.
- Analyses should not be made in the DMZ.
- Load on the Web server due to analyses should be avoided.

In the following figures, a Web server or Proxy server machine on which Agent for Business(SQC-A) is installed is called a "Managed Server", a machine on which Manager(SQC-M) is installed is called a "Management Server", and a person who carries out analyses is called an "analyzer".

Analyses made on the Managed Server



Analyses made on the Management Server



See

For information on the operational methods to use to make analyses on the Management Server, refer to "[Chapter 3 General Procedure for Basic Installation](#)".

1.1.1.2.1 Usage Analysis Function components

Web Site Trend Viewer is used to perform availability analyses of Web services based on logs related to the Web service.

Web Site Trend Viewer includes the following features:

Usage DB Registration Engine

An engine on the Managed Server or Management Server that extracts data from various logs related the Web server and stores it in the database or Usage DB specific to this product.

Usage DB Reference Engine

An engine on the Managed Server or Management Server that retrieves data from the Usage DB. This engine provides the interface (using HTTP communication) to extract data from the Usage DB in response to a request from the "analysis window".

Analysis window

A GUI, running in a Web browser on the client machine, used to carry out data analyses and display results. Usage DB data edited in the interface of "Usage DB Reference Engine" is obtained and displayed in graph or table form.

Analysis report

A function used to display or output analysis results as regular reports. Clicking the "Trend Reporter" button on the "Web Site Management" window on the Management Server and then selecting a Trend Viewer report can use this function.

CSV output

A command, running on the Managed Server or Management Server, used to output Usage DB data to a file in the CSV format.

1.1.1.2.2 SQC extended log

SQC extended log, a specific log adopted by this product, contains data on the response time of the CGI program viewed from the Web browser. Since the SQC extended log is one of a number of logs handled by the "Usage DB registration engine", its data can be referenced by "analysis window" and by "CSV output".

SQC extended log can be used, for example, when the search service via the CGI program is provided on the Web page, and the analyst needs to find out how long it takes to return search results to the Web page user.

Data collection function

A Java™ applet for collecting the SQC extended logs. The applet is set for each Web page for which a SQC extended log is to be collected.

Data accumulation function

A CGI program for accumulating SQC extended logs. This function is called by using the data collection function to accumulate SQC extended logs.

1.1.2 Contents Tampering Monitor

This section provides an overview of the Contents Tampering Monitor.

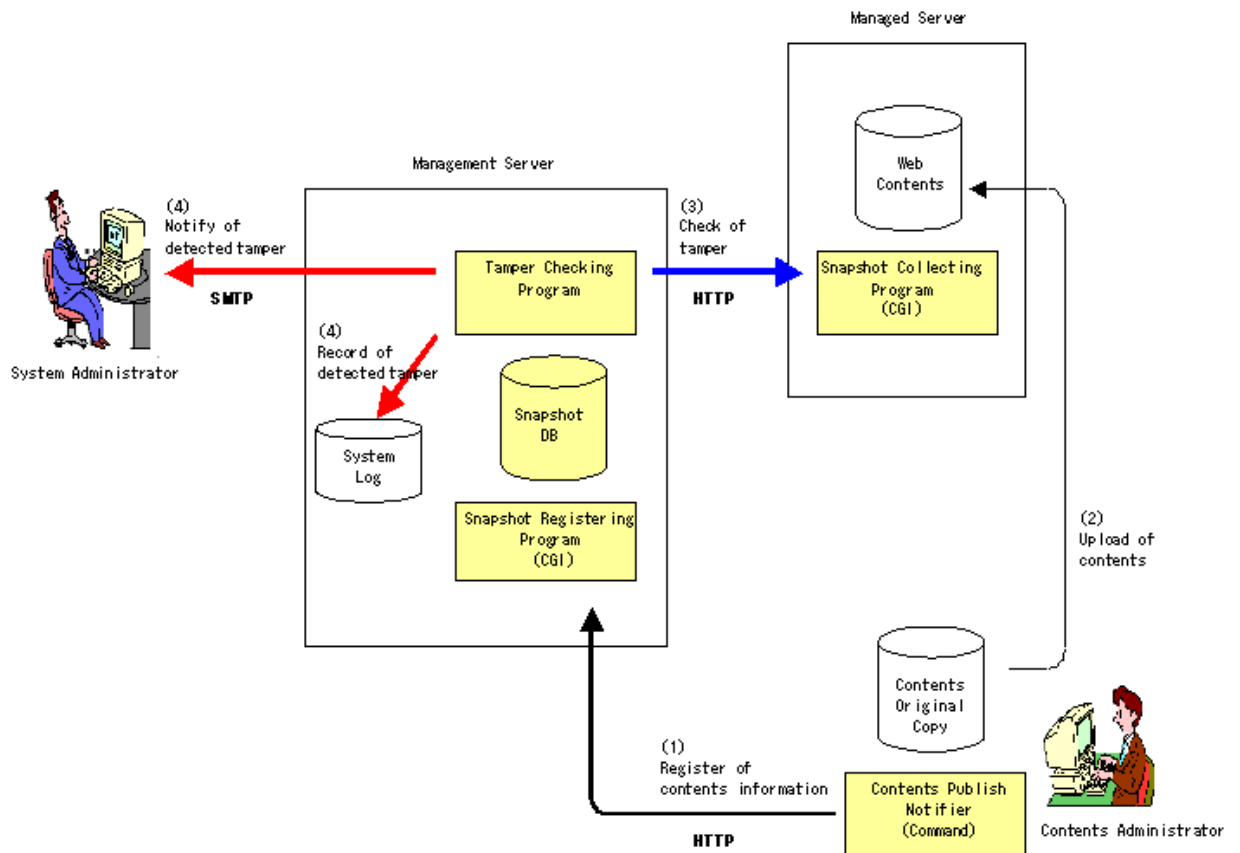
1.1.2.1 Function overview and features

The Contents Tampering Monitor detects tampering with Web content at an early stage and reports it to the system administrator. Early detection minimizes the damage, such as loss of credibility and loss of business opportunities, that can result from security problems on a Web site.

- Highly accurate detection of tampering
In addition to checking the consistency between published Web content and original content, this function distinguishes between content that has failed publication and content that has been tampered with.
- Tamper detection on a remote server
Web server load is minimized because only data on public Web content on a remote Web server is collected and checked for tampering.
- Tamper monitoring on multiple servers
Data on Web content is collected from multiple Web servers and placed on a remote server where it is checked for tampering.
- Alert with e-mail and system logs (event log and syslog)
An alert function is supported so that the system administrator can quickly recognize tampering of open Web contents and take quick action.

1.1.2.2 Function configuration

The following diagram shows the configuration of the Contents Tampering Monitor.



Content Tamper Monitoring system

Data on Web content from the Content Tamper Monitoring system on the Managed Server is collected and tampering with Web content is monitored on the Management Server.

Content Publish Notifier

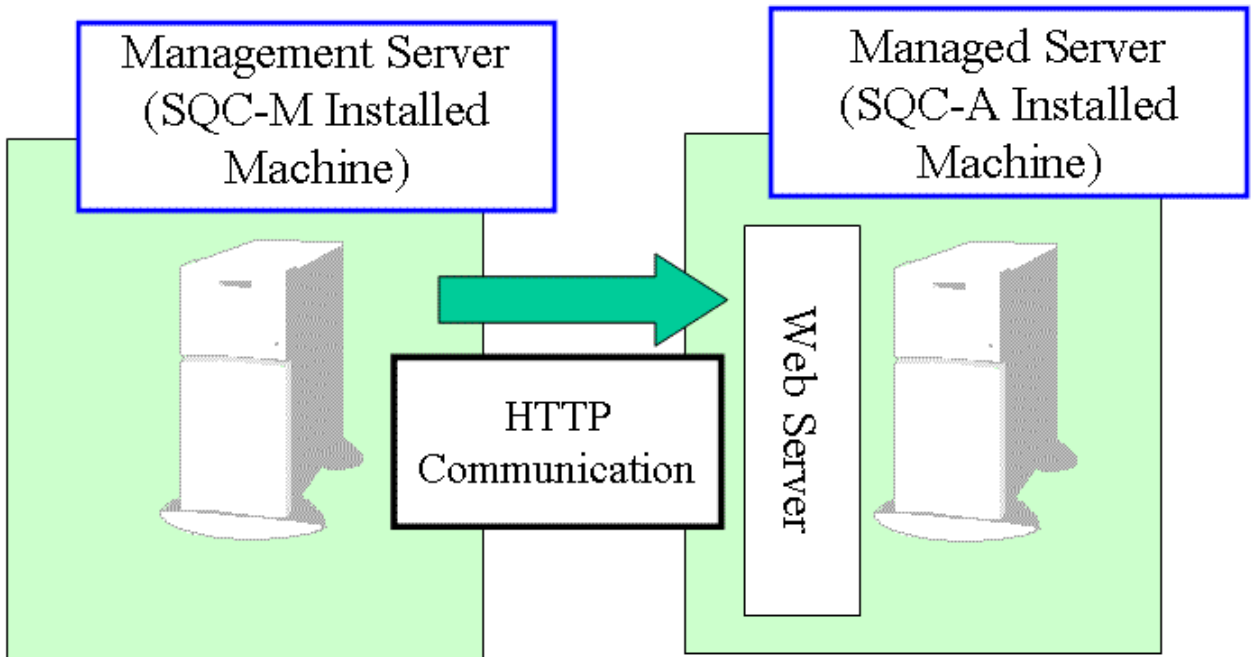
The Content Publish Notifier is executed on the site where content is created. This registers, on the Managed Server, data regarding the Web content that is to be published.

Chapter 2 SQC operating configurations

Chapter 2 gives an overview of configurations for SQC operation.

2.1 Basic Form

Web Site Management Functionality enables the Management Server in which the Manager(SQC-M) is installed to manage Managed Servers (Web server and proxy servers) in which an Agent for Business(SQC-A) is installed.



Because the HTTP protocol is used to perform communication between the management and Managed Servers, no special settings are required to perform it in the DMZ environment.

2.1.1 Locating methods of the analysis data

The Systemwalker Service Quality Coordinator analysis data is located in the following two methods.

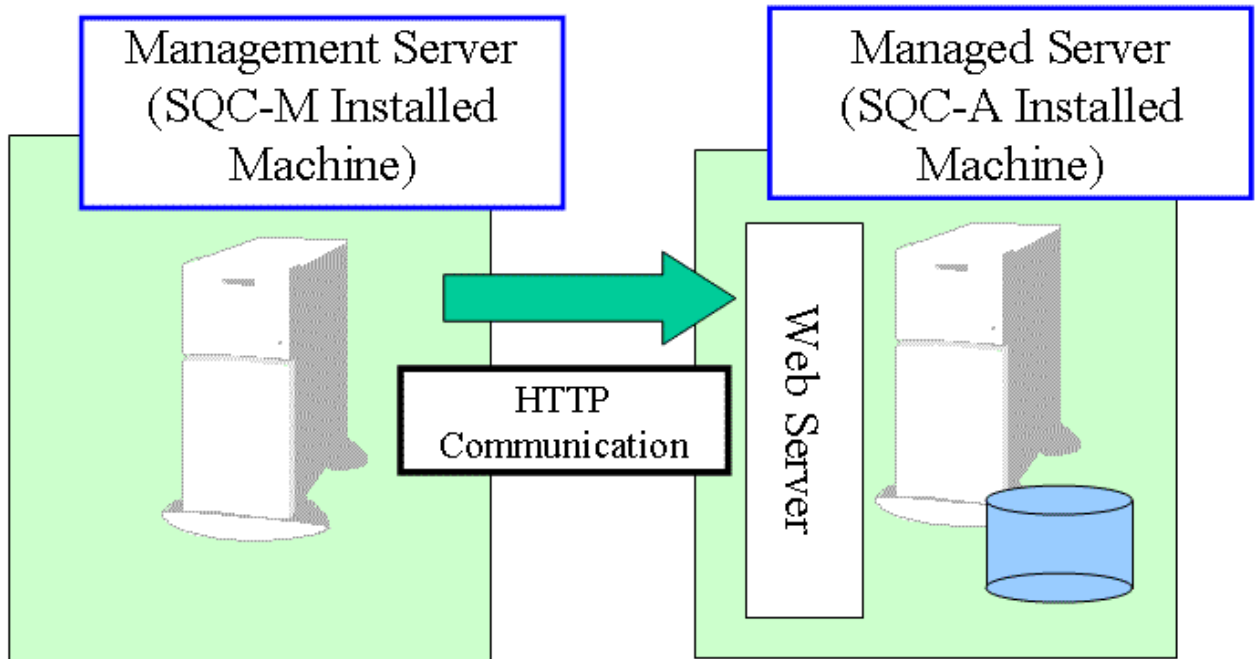
Managed Server Operation	When analysis data is located on the Managed Server
Management Server Operation	When analysis data of the Managed Server is located on the Management Server

When you execute Usage Analysis, select one of operation of the Managed Server or operation of the Management Server.

The following explains the operation for each case.

2.1.1.1 Operation of the Managed Server

The following is the configuration when the Usage Analysis is executed in form of the operation of Managed Server.

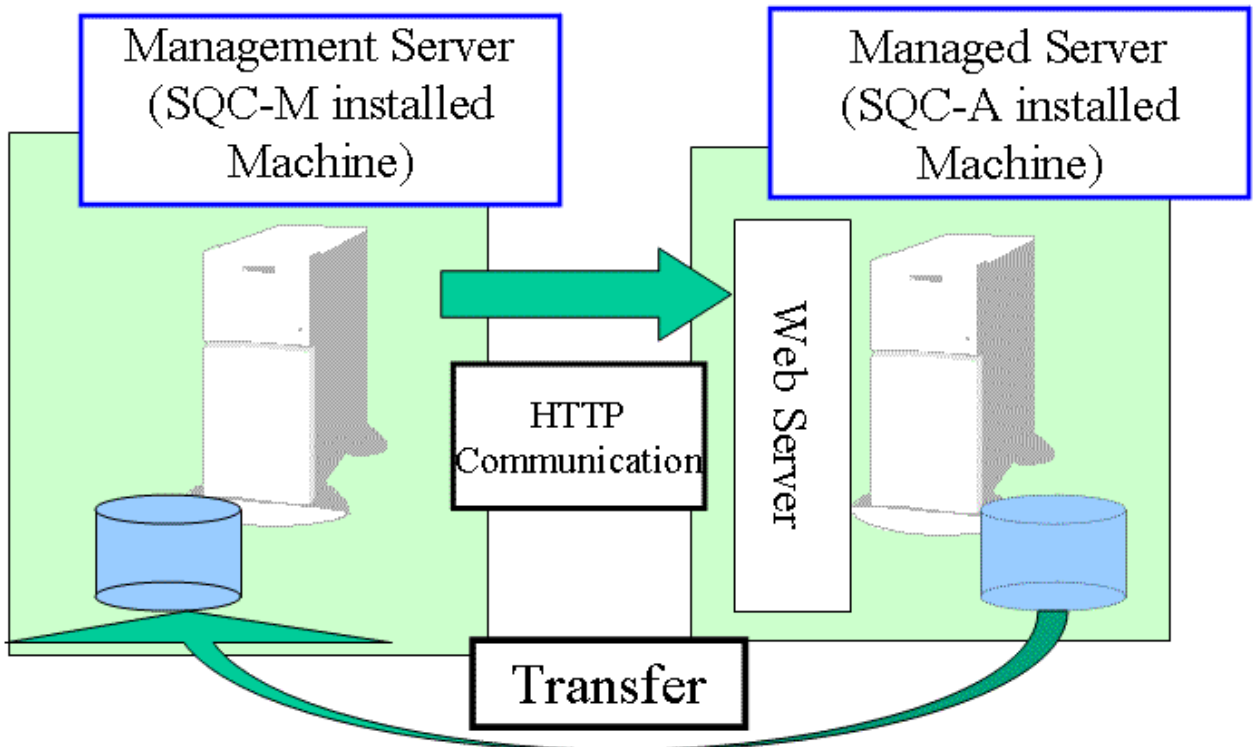


When the Managed Server is operated, data extracted from log information of Web Server is cumulated on Usage Analysis DB of the Managed Server. The Managed Server is used to analyze usage status.

When the Managed Server is accessed from the Web Site Management Window, it is accessed on demand and displayed on the screen.

2.1.1.2 Operation of the Management Server

The following is the configuration when the Usage Analysis is executed in form of the operation of Management Server.



When the Management Server is operated, log information of Web server is transferred to the Management Server and data extracted from log information cumulated on the Usage Analysis DB of the Management Server. The Management Server is used to analyze usage status.

Use this operation to avoid placing on the Web server loads caused by the analysis.

2.1.2 Group Operation

Systemwalker Service Quality Coordinator groups two or more management targets together to manage them collectively

Generally, the following two grouping methods are available.

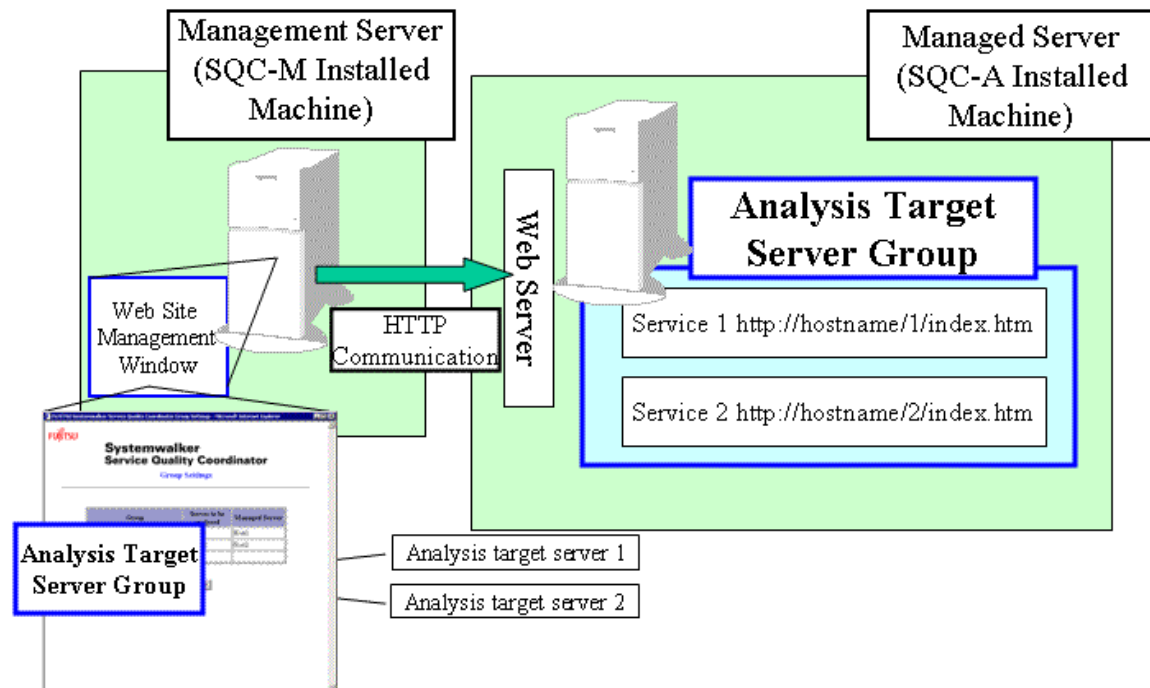
Grouping unit	Management method	Example
Server	When two or more physical Managed Servers (Web and Proxy servers) are managed, they are grouped into one.	Environment where loads are distributed in logical Server units using the load balancer. Example: Hosting environment where more than one domain is operated on one server

Read the following for details.

2.1.2.1 Server grouping

In virtual host and hosting environment, more than 1 domain can be managed by grouping them into a group.

By registering the servers in domain unit and defining the group, Systemwalker Service Quality Coordinator enables this feature.

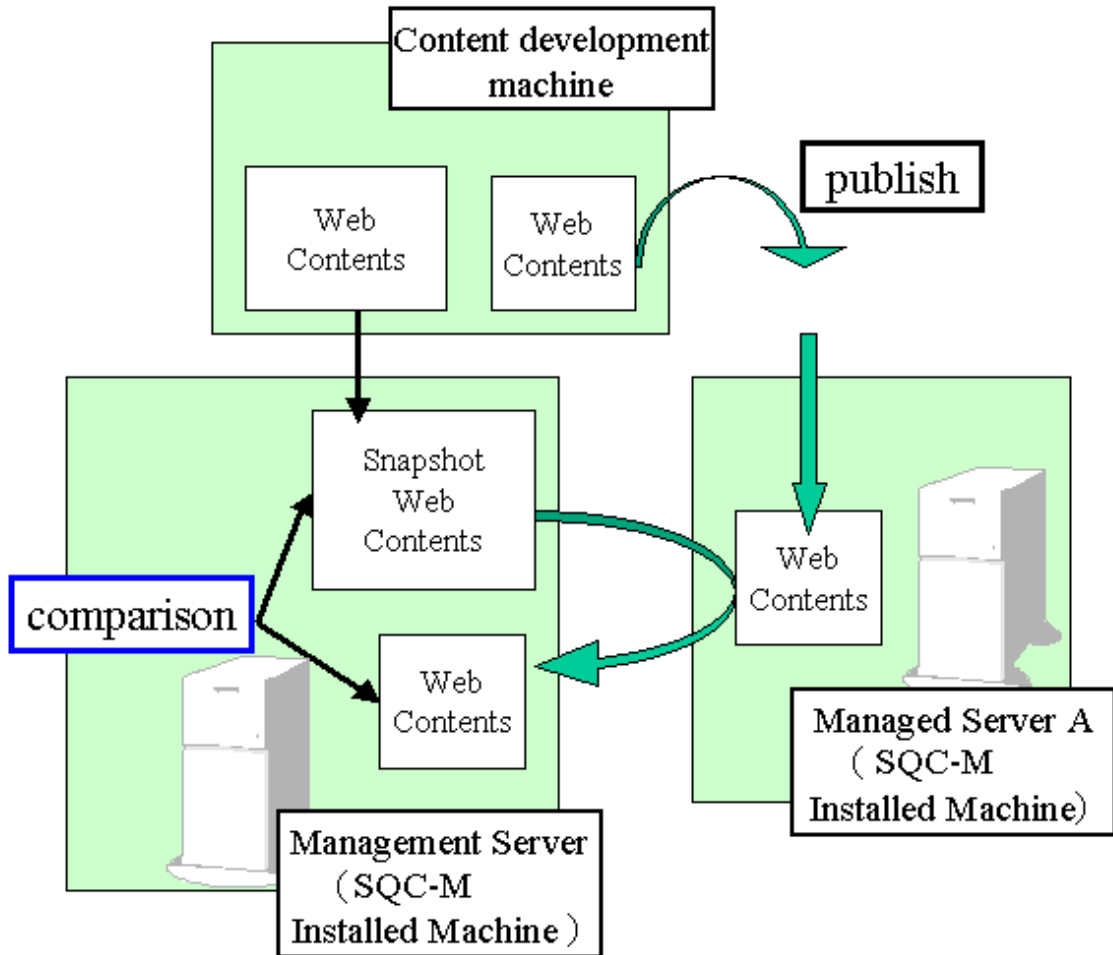


 See

For details on grouping servers together, refer to "14.1.4 Group Settings window" and "7.3 Registering a Group".

2.1.3 Configuration for tampering monitoring

The following shows the system configuration when tampering monitoring operation is performed.



Part 2 Installation (Basic)

Part II provides examples of specific systems to explain the installation procedures used when the basic operation is performed.

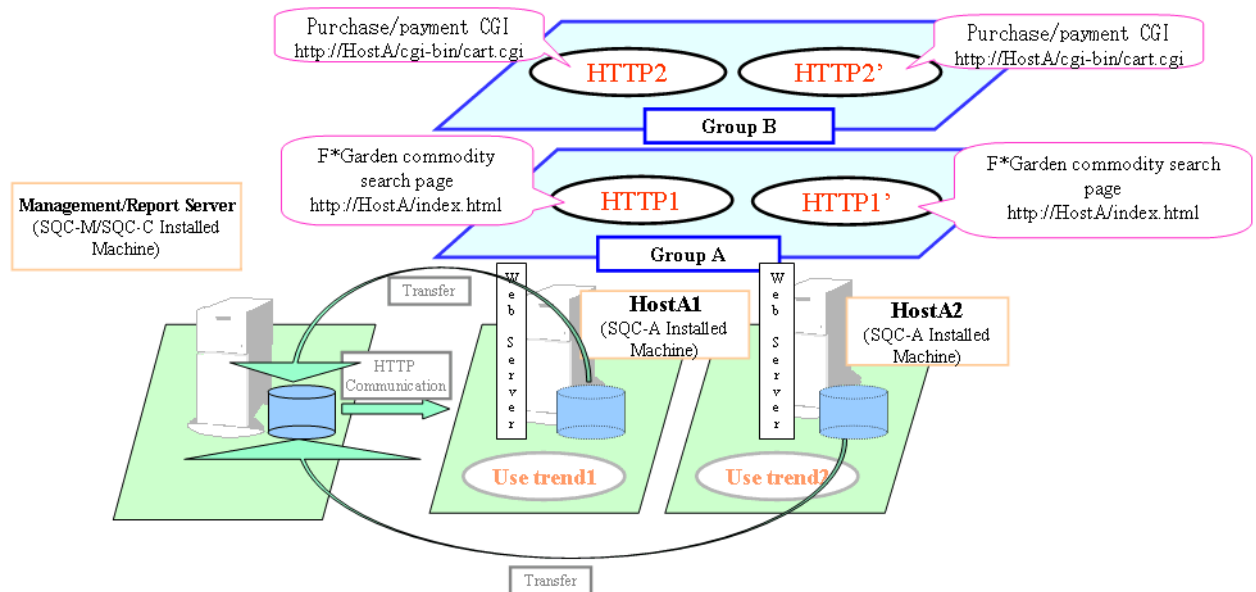
Chapter 3 General Procedure for Basic Installation.....	16
Chapter 4 Environment Settings for the Managed Server.....	21
Chapter 5 Environment Settings for the Management Server.....	32
Chapter 6 Environment Settings for the Report Server.....	43
Chapter 7 Configuring the Operating Environment.....	45
Chapter 8 Checking Operation.....	60

Chapter 3 General Procedure for Basic Installation

From Chapter 3 to Chapter 7, specific system examples are provided to explain the method of environment settings for the Systemwalker Quality Coordinator Web Site Management Functionality.

3.1 System Configuration

Part 2 explains the procedure for the Web Site Management Functionality operation assuming that it is operated on the following system for the F*Garden flower arrangement site.



At the F*Garden flower arrangement site, loads are distributed over two Web servers, HostA1 and HostA2. HostA1 and HostA2 are operating article search page, purchase/payment CGI, and the server for usage analysis. The following lists management server and managed server environments.

Management server

Item	Assumed contents
Host name	Manager
IP address	192.0.2.1
Platform	Windows Server 2008
Web Site Management window URL	http://Manager/SQC/default.htm

Managed server 1

Item	Assumed contents
Host name	HostA1
IP address	192.0.2.2

Item	Assumed contents
SQC-A URL	http://HostA1/SQC/
Platform	Solaris 7
Web server	Apache
Article search page URL	http://HostA1/index.html
Purchase/payment CGI URL	http://HostA1/cgi-bin/cart.cgi

Managed server 2

Item	Assumed contents
Host name	HostA2
IP address	192.0.2.3
SQC-A URL	http://HostA2/SQC/
Platform	Solaris 7
Web server	apache
Article search page URL	http://HostA2/index.html
Purchase/payment CGI URL	http://HostA2/cgi-bin/cart.cgi

The settings for managing this site in management server operation are explained from Chapter 3 to Chapter 7.




By grouping the load-distributing servers, the entire servers can be managed as a whole.

3.2 Environment Settings procedures

Environment settings are made in the sequence, managed server, management server, and report server.

The following lists the setting sequences, explanation locations in the online manual, and setting points.

Item No	Explanation location in online manual	Setting point
1	Chapter 4 Environment Settings for the Managed Server	<p>The following settings need to be consistent:</p> <ul style="list-style-type: none"> - Web server settings - Usage DB environment definition files <p>Here, settings need to be made for HostA1 and HostA2.</p> <p>Explanation is given with HostA1 used as an example.</p>

Item No	Explanation location in online manual	Setting point
		Replace the host name and IP address with the actual ones of your Web server.
2	Chapter 5 Environment Settings for the Management Server	The following settings need to be consistent: <ul style="list-style-type: none"> - Settings for managed server usage analysis - Settings for management server usage analysis  Note In case of cluster operation, apply the settings on the node where management business is in operating. In case of double-operation of Manager, apply the settings for each server.
3	Chapter 6 Environment Settings for the Report Server	Settings for virtual directory properties.

When all settings from Item No. 1 to No. 3 are finished, check the following points to see whether the settings are made correctly.

Item No	Check point	Viewpoint
1	Web server settings are completed.	-
2	Environment settings for usage analysis are completed on the management and managed servers.	Make a check, paying attention to the following points: Check if the DB environment definition file for usage of the managed and the management servers are specified for management server operation setting.
3	Management server settings are completed.	Check the environment settings related to the managed server.
4	Report server settings are completed.	Check that the property settings for a virtual directory are correct.

 **Note**

-
- Execution environment and execution permission for Java™ applets is required. For systems where Java VM is not included, (Windows Server 2003, etc), Java VM should be installed.
 - If the level of Microsoft(R) Win32 Virtual Machine for Java™ (called JavaVM in this document) used on Microsoft(R) Internet Explorer is not 5.00.3167 or later, the analysis window may not be displayed normally.
If the analysis window is not displayed normally and the JavaVM level satisfies this condition, obtain the update patch from the Microsoft site and apply it.
The JavaVM level can be checked using one of the following methods:
 - If the use of the Java console is enabled, select Java Console from the View menu. The JavaVM level is displayed in the first line of the Java console.
 - Retrieve msjava.dll from the directory of the system and open the properties. The JavaVM level is displayed in the Version field.

- If Java™ Plug-in is enabled, the analysis window is not normally displayed under the following conditions:
 - The Proxy server and Proxy exceptions are set on the Web browser, and
 - The Proxy server is set so that the Web browser settings are used in Java™ Plug-in, and
 - The machine on which this product is installed corresponds to the Proxy exception.

3.3 Estimating Resources

This section explains resources required for operating the Web Site Management Functionality.

3.3.1 Management Server

This section explains resources required for operating the Web Site Management Functionality in management server operation.

3.3.1.1 Usage Analysis

3.3.1.1.1 Space estimation in the Usage DB

In management server operation, space in the Usage DB on the management server is the summary of the space in the Usage DB's for all the managed servers.

 See

For the detailed information on the space in one usage DB, refer to "[11.1.1.6 Space estimation in the Usage DB](#)".

3.3.1.1.2 Space estimation of the CSV format log file

This section includes an example of space estimation under the conditions shown below. When you estimate, you should use the actual period of the CSV format log file and other actual conditions.

Conditions

Data type	Visit information
Size per line	About 250 bytes (may change depending on the length of the client host name and URL)
Access count	About 10,000/day

Approximate maximum size per day

About 250 bytes * about 10,000 = About 2.5 MB (/day)

3.3.1.1.3 Space estimation of SQC extended log

The formula for estimating the space per day is as follows. Characters shown in blue indicate variables.

$$(\text{Space per day}) = (50 + A + B) * C$$

Symbol	Meaning
A	Average number of bytes of the client field
B	Average number of bytes of the document field
C	Average access count to the document per day

3.3.1.2 Tamper Monitor

The product stores setting information and notice data used for the tamper monitor function in the following locations.

[Windows]

Under <Installation directory (variable)>\etc\seq\dat

[UNIX]

Under /etc/opt/FJSVssqc/seq/dat

The following table lists the formulas for estimating capacity. The value obtained by each following formula is the maximum value of capacity required.

Information type	Formula
Setting information	5.3 KB * number of registered URLs
Notice data	1.2 KB * number of notified URLs

3.3.2 Managed Server

This section explains resources required for operating the Web Site Management Functionality in managed server operation.

3.3.2.1 Trend Viewer

Refer to "[3.3.1.1 Usage Analysis](#)".

Chapter 4 Environment Settings for the Managed Server

Point

The following provides a point on this chapter:

- The log settings for the usage DB environment definition file must be the same as those for the Web server.

Chapter 4 explains how to set the environment for the managed server.

Do the settings for every server.

Use the following procedure to set the environment for the managed server.

Item No	Reference
1	4.1 Settings for Web Server
2	4.2 Environment Settings for Usage Analysis
3	4.3 Settings for service start

4.1 Settings for Web Server

To communicate with the Management Server, a virtual directory must be registered with the Web server.

This subsection explains the registration procedures, using the four Web servers as examples:

4.1.1 Microsoft(R) Internet Information Services 6.0

[Windows]

1. Start the Internet Service Manager from the Windows' Start menu.

[Start]

-> [Programs]

-> [Control Tools]

-> [Microsoft Internet Information Server]

-> [Internet Service Manager]

Note

If your environment is different from the above, change it so that it matches.

2. Create a virtual directory.

Right-click the Web site to which a virtual directory is to be added, and from the shortcut menu select New -> [Virtual directory].

The wizard for creating a new virtual directory is started. Make the following settings:

Alias: SQC

Physical path: Installation directory\www

Access right: Read access is permitted

3. Set the execution right of the CGI program to the directory cgi-bin under the created virtual directory.

Right-click the directory cgi-bin, and from the shortcut menu select [Properties]. The Properties window is displayed. Make the following setting in [Application settings]

Access right: Execution (including the scripts)

4.1.2 Apache HTTP Server 1.3.26

[Windows]

1. Open the configuration file.

For example, in the standard Apache installation.

[Start]

-> [Programs]

-> [Apache HTTP Server]

-> [Configure Apache Server]

-> [Edit the Apache httpd.conf Configuration File]



Note

.....
If your environment is different from the above, change it so that it matches.
.....

2. Set a virtual directory.

Add the following lines to the end of the file:

```
# Systemwalker Service Quality Coordinator Agent
```

```
ScriptAlias /SQC/cgi-bin/ "C:/Program Files/SystemwalkerSQC/www/cgi-bin/"
```

```
<Directory "C:/Program Files/SystemwalkerSQC/www/cgi-bin">
```

```
Options ExecCGI
```

```
AllowOverride None
```

```
Order allow,deny
```

```
Allow from all
```

```
</Directory>
```

```
Alias /SQC/ "C:/Program Files/SystemwalkerSQC/www/"
```

```
<Directory "C:/Program Files/SystemwalkerSQC/www">
```

```
Options None
```

```
AllowOverride None
```

```
Order allow,deny
```

```
Allow from all
```

```
</Directory>
```

Note

The above has three references to C:/Program Files/SystemwalkerSQC. This is the default installation directory for this product.

If your installation directory is different, change the references to match your installation directory. Also, change such settings as the access rights, as required.

See

Setup of virtual directory depends on versions of Apache. For details, please refer to the manual of Apache.

3. Make settings so that a file with the extension cgi is started as a CGI program.
If the following line in the file is marked as a comment, remove the comment mark.
AddHandler cgi-script .cgi
4. Apply the new settings.
Close the editor after updating the entries. If Apache HTTP Server is active, stop the server and then restart it.

[UNIX]

1. Open the configuration file using a text editor.
2. Set a virtual directory.
Add the following lines to the end of the file:

```
# Systemwalker Service Quality Coordinator
ScriptAlias /SQC/cgi-bin/ "/opt/FJSVssqc/www/cgi-bin/"
<Directory "/opt/FJSVssqc/www/cgi-bin">
Options ExecCGI
AllowOverride None
Order allow,deny
Allow from all
</Directory>
Alias /SQC/ "/opt/FJSVssqc/www/"
<Directory "/opt/FJSVssqc/www">
Options None
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

Note

Change such settings as the access rights as required.



See

Virtual directory settings depend on the Apache version. Refer to the Apache manuals for details.

3. Make settings so that a file with the extension `cgi` is started as a CGI program.
If the following line in the file is marked as a comment, remove the comment mark.
`AddHandler cgi-script .cgi`
4. Apply the new settings.
Close the editor after updating the entries. If Apache HTTP Server is active, stop the server and then restart it.

4.1.3 Netscape(R) Enterprise Server 3.0

[Windows]

1. Start the Netscape(R) Enterprise Server 3.0 from the Windows' Start menu.

For example, in the standard Netscape Server installation:

[Start]

-> [Programs]

-> [Netscape SuiteSpot]

-> [Administration]



Note

If your environment is different from the above, change it so that it matches.

2. Select the server to which a virtual directory is to be added and display the server manager page.

Create a virtual directory.

Click the [Content Management] button and then click [Additional Document Directories] in the list on the left. The [Additional Document Directories] page is displayed.

Make the settings shown below:

URL Prefix: `SQC`

Map To Directory: `Installation directory\www`

Click OK. The [Save and Apply Changes] page is displayed. Click the [Save and Apply] button.

3. Set the execution rights of the CGI program to the directory `cgi-bin` under the created virtual directory.

Click the [Programs] button and then click [CGI Directory] in the list on the left. The [CGI Directory] page is displayed.
Make the settings shown below:

URL Prefix : `SQC/cgi-bin`

CGI Directory: `Installation directory\www\cgi-bin`

Click [OK]. The [Save and Apply Changes] page is displayed. Click the [Save and Apply] button.

4.1.4 InfoProvider Pro (packaged with Interstage Application Server)

[Windows]

1. Open the environment definition file of InfoProvider Pro using a text editor.
2. Set a virtual directory.
Add the following lines to the end of the file:

```
# Systemwalker Service Quality Coordinator Agent V12.0L10  
cgi-path-idnt: C:\PROGRA~1\SYSTEM~1\www\cgi-bin SQC/cgi-bin  
link: SQC C:\PROGRA~1\SYSTEM~1\www
```

Point

.....
The above has a reference to C:\PROGRA~1\SYSTEM~1 (8.3format) is the default installation setting. If your installation setting is different, change the references to match.
.....

3. Apply the new settings.
Close the editor after updating the entries. If InfoProvider Pro is active, close it down and then restart it.

Note

.....
If your InfoProvider Pro is older than the one bundled in Interstage Standard Edition V2.0L20, the above settings are not possible due to functional restrictions. Instead, make the settings shown below:
.....

1. Create a virtual directory equivalent to the above one.

Create a new directory SQC under the top directory published by the Web server, and then copy to this new directory all files under the directory www under the installation directory of this product, excluding cgi-bin. Open viewer.html at the copy destination using a text editor and then add the <PARAM> tag between the <APPLET> tags as shown below:

```
<APPLET codebase="./classes/" archive="viewer.jar" code="Viewer.class" width=950 height=512>  
<PARAM name="CGI" value=http://xxx.yyy.com/SQC-cgi-bin/dbref.cgi>  
</APPLET>
```

Note

.....
Replace the term *xxx.yyy.com* above with the actual host address of your Web server.
.....

2. Open the environment definition file of InfoProvider Pro using a text editor and add the following lines to the end of the file:

```
# Systemwalker Service Quality Coordinator Agent  
cgi-path-idnt: C:\PROGRA~1\SYSTEM~1\www\cgi-bin SQC-cgi-bin
```

Note

.....
The above has a reference to C:\PROGRA~1\SYSTEM~1 (8.3 format), which is the default installation setting. If your installation setting is different, change the references to match.
.....

3. Apply the new settings.
Close the editor after updating the entries. If InfoProvider Pro is active, close it down and then restart it

[Solaris]

1. Open the environment definition file of InfoProvider Pro using a text editor.
2. Set a virtual directory.
Add the following lines to the end of the file:

```
# Systemwalker Service Quality Coordinator Agent  
  
cgi-path-idnt: /opt/FJSVssqc/www/cgi-bin SQC/cgi-bin  
  
link: SQC /opt/FJSVssqc/www/cgi-bin
```
3. Apply the settings.
Close the editor after updating the entries. If InfoProvider Pro is active, close it down and then restart it.

Note

.....
If your InfoProvider Pro is older than the one bundled in INTERSTAGE Standard Edition 3.0, the above settings are not possible due to functional restrictions. Instead, make the settings shown below:
.....

1. Create a virtual directory equivalent to the above one.
Create a new directory SQC under the top directory published by the Web server, and then copy to this new directory all files under the directory www under the installation directory of this product, excluding cgi-bin.
Open viewer.html at the copy destination using an editor and then add the <PARAM> tag between the <APPLET> tags as shown below:

```
<APPLET codebase="/classes/" archive="viewer.jar" code="Viewer.class" width=950 height=512>  
<PARAM name="CGI" value=http://xxx.yyy.com/SQC-cgi-bin/dbref.cgi>  
</APPLET>
```

Note

.....
Replace the term *xxx.yyy.com* above with the actual host address of your Web server.
.....

2. Open the environment definition file of InfoProvider Pro using a text editor and then add the following lines to the end of the file:

```
# Systemwalker Service Quality Coordinator Agent 12.0  
cgi-path-idnt: /opt/FJSVssqc/www/cgi-bin SQC-cgi-bin
```
3. Apply the new settings.
Close the editor after updating the entries. If InfoProvider Pro is active, close it down and then restart it.

4.2 Environment Settings for Usage Analysis

The following settings need to be made on the managed server to make usage analysis:

1. Log setting of Web server

2. Settings for usage DB environment definition file

The following explains how to make these settings:

4.2.1 Defining httpd.conf

The following shows httpd.conf file settings when the managed server is Apache HTTP Server.

Example

The following shows an example of definition.

```
CustomLog /usr/local/apache/logs/access_log common
```

Point

.....
If the CustomLog specification in httpd.conf is changed, the log for Web servers needs to be re-created.
.....

The following provides the procedure for re-creating the log for Web servers.

1. Shutdown the Web server.

```
# /usr/local/apache/bin/apachectl stop
```

2. Save the log for the Web server before the log format is changed.

```
# mv /usr/local/apache/logs/access_log /tmp/access_log.back
```

3. Start up the Web server.

```
# /usr/local/apache/bin/apachectl start
```

Note

.....
When the Web server is other than Apache HTTP Server, set the log format to the purpose, refer to "[15.2.1.5 File internal format \(log definition block to be analyzed\)](#)".

When the Web server is IIS, not all required tokens are logged out by the default setting. Changed the default setting to make IIS log out all required tokens specified in "[15.2.1.5 File internal format \(log definition block to be analyzed\)](#)".
.....

4.2.2 Defining the usage DB environment definition file

Use the following sample files to create and store usage DB environment definition files.

[UNIX]

When you set the environment in "[3.1 System Configuration](#)", refer to the following table.

File	Path
Sample file	/opt/FJSVssqc/sample/ DatabaseConfig

File	Path
Storage destination of usage DB environment definition file	/etc/opt/FJSVssqc/DatabaseConfig

[Windows]

When the managed server is Window, refer to the following table.

File	Path
Sample file	<installation directory>\DatabaseConfig
Storage destination of usage DB environment definition file	<installation directory(variable)>\control \DatabaseConfig

The following gives a definition example of the usage DB environment definition file.

Example:

The definition example is shown below.

<pre>[Server] Symbol = HostA1 Name = HostA1 Type = web Domain = xxx.yyy.com DatabaseInterval = week(sun) SearchDNS = yes RequestURLSuffix = "html,htm,shtml,shtm,stm,cgi,asp,pl,tcl,sh" DatabaseMode = both [Log] Symbol = HostA1 Name = HostA1 Path = /usr/local/apache/logs/access_log Format = Common Region = +0900</pre>
--

Note

Note the following settings.

Setting item	Remarks
Name	Use Name under [Server] to specify the name of the analysis target server that is defined in the environment setting window for the managed server.
Format	Accord to the log format of the Web server. When the Web server is Apache HTTP Server, accord to the log format specified in httpd.conf CustomLog.
Domain	Defines the domain name of the analysis target server.

Setting item	Remarks
	For details, refer to " 15.2.1.4 File internal format (analysis target server definition block) ".

See

See "[15.2.1 Usage DB Environment Definition File](#)" in the online manual for details on setting the usage DB definition file.

Point

After the settings above have been made, check that the usage DB registration engine starts.

[UNIX]

Use the following procedure to check whether the settings have been made correctly:

1. Execute the command.

```
/opt/FJSVssqc/bin/dbregmng
```

2. Check the log.
Check the output message of the following log file.

```
/var/opt/FJSVssqc/log/dbreg.log
```

If the following message is displayed after the command is executed, the usage DB has been created correctly.

```
dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1098 103001001i
"[server=HostA1][log=HostA1]Database register engine started"

dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1853 103001002i
"[server=HostA1][log=HostA1]Database register engine stopped."
```

Check that:

- A pair of messages shown above is displayed.
- No error message is displayed between the first and second messages.

See

If the usage DB is not correctly created, see this section and "[11.1.1.2 Start operation](#)" to review the settings.

[Windows]

In case of Windows, check as follows:

1. Execute the command.

```
1. <installation directory>\bin\dbregmng.exe
```

2. Check the log.
Check the output message of the following log file.

```
1. <installation directory(variable)>\log\dbreg.log
```

If the following message is displayed after the command is executed, the usage DB has been created correctly.

```
dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1098 103001001i  
"[server=HostA1][log=HostA1]Database register engine started"  
  
dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1853 103001002i  
"[server=HostA1][log=HostA1]Database registration engine stopped."
```

Check that:

- A pair of messages shown above is displayed.
- No error message is displayed between the first and second messages.



If the usage DB is not correctly created, see this section and "[11.1.1.2 Start operation](#)", to review the settings.

4.2.3 Enhancing public Web server security

[Windows]

If this product is installed on an Internet public Web server or Proxy server, you can enhance security by changing the access authority to the installed resources. Follow the procedure below.



Using the following command can change the access authority. However, this command is valid only for NTFS.

Access authority to directories/files

Change the access authority by using the sqcSetFileSec.exe command.

```
<Installation directory>\bin\sqcSetFileSec.exe <installation directory (variable)>
```

By executing the above command, the access authority to the installed resources is changed as follows:

Administrators: Full control

Everyone: Read/execute authorities only

SQC extended log

If the access authority is changed by the method, no SQC extended log can be collected.

If the SQC extended log needs to be collected, restore the access authority to the state when installed by following the method below. (However, security risks will be greater.)

```
<installation directory>\bin\sqcSetFileSec.exe -u <installation directory(variable)>\extend-log
```

```
<installation directory>\bin\sqcSetFileSec.exe -u <installation directory(variable)>\log
```

[UNIX]

Access authority to directories and files

The access authorities for the installed resources are set during installation as shown below:

Super user: Read/Write/Execute authorities

Others: Read/Execute authorities only

SQC extended log

After the installation, the SQC extended log cannot be collected.

If the SQC extended log needs to be collected, log in as a super user and then change the access authority by following the method below. (However, security risks will become greater.)

```
# chmod 777 /var/opt/FJSVssqc/extend-log
```

```
# chmod 777 /var/opt/FJSVssqc/log
```

4.3 Settings for service start

For the service start, refer to "[11.1.1.2 Start operation](#)".

Chapter 5 Environment Settings for the Management Server

Point

The points of this chapter are as follows:

- Make consistent settings for usage analysis between the management server and Managed Servers.
- Make the following settings consistent between the setting window on the Managed Server and use trend database environment definition file:
 - "Agent URL" in the setting window on the Managed Server
 - "Name" of definition block for the server to be analyzed in DatabaseConfig

The management server environment is set up according to the following procedure:

No.	Reference
1	5.1 Settings for Web Server
2	5.2 Environment Settings for Usage Analysis
3	5.3 Registering System Configuration
4	5.4 Settings for Service Start

5.1 Settings for Web Server

On the Management Server, a virtual directory for the Web server of the installation must be set.

A virtual directory is set so that the Web Site Management Window can be displayed from the Web browser.

The following explains how to set the virtual directories.

5.1.1 Windows

[Windows]

For Windows, virtual directories must be set.

Also set up basic authentication for the environment setup window if access to the environment setup window must be restricted.

5.1.1.1 Setting virtual directories

Virtual directory is not set automatically when the Management Server is installed. If necessary, execute the following IIS command to build an environment.

Before performing this procedure

The WWW service (World Wide Web Publishing Service) must be running before the following setup command is executed. Also check that a site designated as "Existing Web site" exists.

Note

The commands referred to below may generate an error if any of the following conditions exist:

- IIS is not installed
- Windows Scripting Host is not assigned (Microsoft(R) Internet Information Services 6.0)
- The command line management tool (appCmd.exe) is not installed (Microsoft(R) Internet Information Services 7.0/7.5)
- The setup procedure has already been performed

Command to execute

Run the following command to set up the virtual directory:

```
<Installation directory>\bin\sqcSetIISreg.exe -m
```

For Microsoft(R) Internet Information Services(IIS)6.0

When using Microsoft(R) Internet Information Services 6.0, run the command shown below after sqcSetIISreg.exe. IIS 6.0 is bundled as a standard feature with Windows Server 2003.

Note

Switch the current directory to <installation directory>\bin before running the following command:

```
Installation directory\bin\sqcmsetc.bat
```

For Microsoft(R) Internet Information Services(IIS)7.0/7.5

When using Microsoft(R) Internet Information Services 7.0/7.5, run the command shown below after sqcSetIISreg.exe.

Note

Switch the current directory to <installation directory>\bin before running the command.

Note that in Windows Vista and Windows Server 2008, this command must be executed using administrator privileges. To do so, select [Programs] and then [Accessories] from the [Start] menu and then right-click on [Command Prompt] and select [Run as Administrator] from the pop-up menu that appears. Enter the following command in the [Command Prompt] window that appears.

```
Installation directory\bin\sqcmsetc_iis7.bat
```

This creates the following virtual directories in Microsoft(R) Internet Information Services.

Service	Setting item	Settings
WWW service	Alias	SQC
	Directory	<Installation directory>\www Example) C:\Program Files\SystemwalkerSQC\www
	Access right	Reading Execution (including scripts)

Make the above settings also when virtual directories are set manually.



See

For details on how to set the virtual directory, refer to the online documentation for Microsoft(R) Internet Information Services.

5.1.1.2 Handler mapping settings

Handler mapping settings are required when using Microsoft(R) Internet Information Services 7.0/7.5.

Before performing this procedure

In order to set up handler mapping, it is necessary for [CGI] to be enabled in the [Application Development Function] of the [World Wide Web Service] component of the Internet Information Services.

Before performing this procedure, check the status of the [CGI] setting and enable it if is not enabled.

Procedure

1. Select the virtual directory name "SQC" in the Microsoft(R) Internet Information Services setup window.
2. Double click [Handler Mapping] in the function view on the right.
3. [Add Module Map] from the operation menu on the right.
4. Specify the following information in the [Add Module Map] dialog box and click the [OK] button:
 - Request path: *.cgi
 - Module: CgiModule
 - Name: CGI-.cgi

5.1.1.3 Setting virtual directories property

Procedure

For Microsoft(R) Internet Information Services(IIS) 6.0

In Microsoft(R) Internet Information Services 6.0, the setup procedure is as follows:

1. Select the virtual directory name "SQC" in the Microsoft(R) Internet Information Services setup window.
2. Click the [Directory Security] tab in the [Properties] window of the above virtual directory.

3. Set an account that has administrator privileges (the account used when installing the Operation Management Client) as the account that will be used for anonymous access.
4. Clear the [Basic authentication] check box if authenticated access is to be used.

For Microsoft(R) Internet Information Services(IIS)7.0/7.5

In Microsoft(R) Internet Information Services 7.0/7.5, the setup procedure is as follows:

1. Select the virtual directory name "SQC" in the Microsoft(R) Internet Information Services setup window.
2. Double click [Authentication] in the function view.
3. Check that [Anonymous Authentication] is enabled, then click [Anonymous Authentication] and select [Edit] from the operation menu on the right.
4. When the [Edit Anonymous Authentication Credentials] dialog box appears, select [Specific user] and click the [Set] button.
5. Specify the user name and password of a user with administrator privileges in the [Set Credentials] dialog box.

After the above settings are made, the Web Site Management Window can be displayed by specifying the following URL on the Web browser:

If the management server is Windows:

<code>http:// management server's host name/SQC/default.htm</code>
--

5.1.1.4 Setting of basic attestation

Procedure

1. Register a user account with Windows

Register a user account for accessing the Management Console startup HTML or the user startup HTML.

- The user who will access the Management Console can use the account with administrator privileges that is normally used or create a new account.
- There are no special restrictions on the account type (access rights) that is created when creating a new account to access the Management Console or when creating an account to access the user startup HTML, as long as the account is able to grant read permissions to the file specified in set in Step 2 "Set file access control" below.

Register users referring to the Windows help file.

2. File security settings in IIS

The following procedure is used to specify file security settings in IIS:

1. Select the virtual directory name "SQC" in the Microsoft(R) Internet Information Services setup window.
2. Select "EnvSetting_jp.html" and "EnvSetting_en.html" in the window on the right, click the right mouse button, and then select [Properties] from the pop-up menu to open the [Properties] window.
3. Click the [File Security] tab and then click the [Edit] button for [Anonymous Access and Authentication Control].

4. Clear the [Anonymous access] check box and select the [Basic authentication] check box in the [Authenticated Access] field. If any check boxes relating to other authentication methods are selected, clear them.
5. Click the [OK] button to apply the definition.

The above settings will cause an authentication window to appear when the environment setup window is displayed.

5.1.2 UNIX

This subsection explains the setting procedure using, as an example, the following Web server configuration:

- Apache HTTP Server 1.3.14
- Sun WebServer
- InfoProvider Pro (bundled in Interstage Application Server V3.0)

[Solaris/Linux]

Apache HTTP Server

1. Open httpd.conf using an editor. httpd.conf is located at the following:
 - Apache supplied as standard with Solaris: Under /etc/Apache
 - Apache supplied as standard with Linux: Under /etc/httpd/conf
 - Apache other than the above: Under /usr/local/apache/conf
2. Set the virtual directory. Add the following record to the end of the file:

```
# Systemwalker Service Quality Coordinator
#
Alias /SQC/cgi-bin/ "/opt/FJSVssqc/www/cgi-bin/"
<Directory "/opt/FJSVssqc/www/cgi-bin">
Options ExecCGI
AllowOverride None
Order allow,deny
Allow from all
</Directory>
#
Alias /SQC/ "/opt/FJSVssqc/www/"
<Directory "/opt/FJSVssqc/www">
Options None
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

3. Make settings so a file with extension cgi is started as a CGI program. If the following line in the file is marked as a comment, remove the comment mark.

```
AddHandler cgi-script .cgi
```


4. There is a possibility of causing the garble in the state of the first stage of Apache2.0.

Please set it in the following if necessary.

5. Save the file and then close the editor.

6. If apache HTTP Server is active, stop the server and then restart it.

After the above settings are made, the Web Site Management Window can be displayed by specifying the following URL on the Web browser:

When the management server is Solaris, Linux:

```
http://<management_server_hostname>/SQC/index.html
```

[Solaris]

Sun WebServer

1. Open httpd.conf using the editor. You can find httpd.conf at the following location:

- Under /etc/http/

2. Set a virtual directory:

Add a virtual directory to the following section in the file:

[Correction section]

```
server {  
}
```

or

```
url virtual server URL{  
}
```

server{ } : Set for all servers by default. You can make this setting if you do not perform virtual server operation.

url{ } : Set for specific virtual servers only. If you operate Systemwalker Service Quality Coordinator on a virtual server, set for the applicable section of the virtual server to be operated.

[Setting Record]

```
cgi_enable "yes"  
map /SQC/ /opt/FJSVssqc/www/  
map /SQC/cgi-bin/ /opt/FJSVssqc/www/cgi-bin/ cgi
```

cgi_enable: If the record already exists, rewrites the value only without adding the record.

map: Add "cgi" to the end so that the extension cgi can be recognized as a CGI program.

3. Save the file and then close the editor.
4. If Sun Web Server is active, stop the server and then restart it.

After the above settings are made, the Web Site Management Window can be displayed by specifying the following URL on the Web browser:

If management server is Solaris:

```
http://<management_server_hostname> /index.html
```

[Solaris]

InfoProvider Pro

1. Open HTTPD.conf using the editor. You can find HTTPD.conf at the following location:
 - Under /etc/opt/FSUNprovd/
2. Set a virtual directory. Add the following record to the end of the file.

```
# Systemwalker Service Quality Coordinator  
cgi-path-idnt: /opt/FJSVssqc/www/cgi-bin SQC-A/cgi-bin  
link: /opt/FJSVssqc/www
```

3. Save the file and then close the editor.
4. If InfoProvider Pro is running, stop the server and then restart it.

Note

If your InfoProvider Pro is older than the one bundled in INTERSTAGE Standard Edition V2.0L20, then functional restrictions prevent the above settings. Instead, use the symbolic link function of the UNIX file system as shown below:

1. Open HTTP.conf from the editor: You can find httpd.conf at the following location:
 - Under /etc/opt/FSUNprovd/
2. Set the directory in which the CGI application is stored. Add the following record to the end of the file.

```
# Systemwalker Service Quality Coordinator  
cgi-path-idnt: /opt/FJSVssqc/www/cgi-bin SQC/cgi-bin
```

3. Check the public directory defined by "acstop".
4. Save the file and then close the editor.
5. Execute the following command:

```
cd public directory defined by "acstop"
ln -s /opt/FJSVssqc/www SQC
```

6. If InfoProvider Pro is active, stop the server and then restart it.

After the above settings are made, the Web Site Management Window can be displayed by specifying the following URL on the Web browser:

If management server is Solaris:

```
http://management server's host name/index.html
```

5.2 Environment Settings for Usage Analysis

Use the following sample file to create a use trend database environment definition file and store it in the file show below:

[Windows]

When you set the environment according to "3.1 System Configuration", refer to this table.

File	Path
Sample file	<Installation directory>\sample \DatabaseConfig
Storage destination of use trend database environment definition file	<Installation directory (variable)>\control \DatabaseConfig

[UNIX]

File	Path
Sample file	/opt/FJSVssqc/sample/ DatabaseConfig
Storage destination of use trend database environment definition file	/etc/opt/FJSVssqc/DatabaseConfig

An example of the use trend database environment definition file is shown below.

Example

A sample definition is shown below:

```
[Server]
Symbol = HostA1
Name = HostA1
Type = web
Domain = xxx.yyy.com
```

```

DatabaseInterval = week(sun)
SearchDNS = yes
RequestURLSuffix = "html,htm,shtml,shtm,stm,cgi,asp,pl,tcl,sh"
DatabaseMode = db
[Log]
Symbol = HostA1
Name = HostA1
Path = "C:\SystemwalkerSQC\database\csv\HostA1\*.csv"
Format = SQC-CSV
Region = +0000
[Server]
Symbol = HostA2
Name = HostA2
Type = web
Domain = xxx.yyy.com
DatabaseInterval = week(sun)
SearchDNS = yes
RequestURLSuffix = "html,htm,shtml,shtm,stm,cgi,asp,pl,tcl,sh"
DatabaseMode = db
[Log]
Symbol = HostA2
Name = HostA2
Path = "C:\SystemwalkerSQC\database\csv\HostA2\*.csv"
Format = SQC-CSV
Region = +0000

```

 **Note**

Note the following settings:

Name	For "Name" under [Server], specify the name of the server to be analyzed defined in the Managed Server setting window for environment settings.
Path	<Installation directory (variable)>\database\csv\<server>\db*.csv
Format	Accord the format to the log format specified by CustomLog of Httpd.conf. When you operate the Management Server, specify "SQC-CSV"
Region	Here, specify the region of time by the time difference from GMT (Greenwich Mean Time). When you operate the Management Server: Specify "+0000" as the Region definition of the Management Server side. Specify "+0900" as the Region definition of the Managed Server side.



Note

However, in case of IIS, specify "+0000" as the Region definition of the Managed Server side.



See

For detail of the setting of a use trend database environment definition file, refer to "[15.2.1.5 File internal format \(log definition block to be analyzed\)](#)".



Point

After the above settings are finished, check whether the settings are correct according to the following procedure:



Note

In order to check the settings, the system configuration must be registered. For details on registering system configuration, refer to "[5.3 Registering System Configuration](#)".

[Windows]

1. Check that the use trend database registration engine starts normally.
2. Enter the command
Enter the following command:

```
<Installation directory>\bin\dbregmng.exe
```

3. Check the log file
Check the output messages in the following log file:

```
<Installation directory (variable)>\log\dbreg.log
```

If the following messages are output as the result of the command, the use trend database was created normally.

```
dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1098 103001001i  
"[server=HostA1][log=HostA1]The database registration engine started."  
  
dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1853 103001002i  
"[server=HostA1][log=HostA1] The database registration engine ended."
```

Check that no error messages are output between the above 2 messages.



See

.....
If the use trend database was not normally created, check the settings while referring to "[Chapter 4 Environment Settings for the Managed Server](#)".
.....

[UNIX]

When the Managed Server is Solaris, check whether the setting is proper or not according to the following procedure.

1. Enter the command

```
/opt/FJSVssqc/bin/dbregmng
```

2. Check the log
Check the following log file output message.

```
/var/opt/FJSVssqc/log/dbreg.log
```

If the following messages are output as the result of the command, the use trend database was created normally.

```
dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1098 103001001i  
"[server=HostA1][log=HostA1]The database registration engine started."  
  
dd/mmm/yyyy:hh:mm:ss +0900 dbreg[22262] DBReg_Main:1853 103001002i  
"[server=HostA1][log=HostA1]The database registration engine ended."
```

Check from the following points of view:

- Above messages were outputted in pairs.
- No error message was output between the first message and the second message.



See

.....
If the use trend database was not normally created, check the settings while referring to "[Chapter 4 Environment Settings for the Managed Server](#)".
.....

5.3 Registering System Configuration

For information on registering system configuration, refer to "[Chapter 7 Configuring the Operating Environment](#)".

5.4 Settings for Service Start

For information on service start, refer to "[11.1.1.2 Start operation](#)".

Chapter 6 Environment Settings for the Report Server

The report server environment is set up according to the following procedure:

Note

Web Site Management Functionality uses the Operation Management Client as report server.

Web Site Management Functionality uses the Operation Management Client as report server.

No.	Reference
1	6.1 Setting a virtual directory
2	6.2 Setting a virtual directory property

6.1 Setting a virtual directory

Commonly, the virtual directory is automatically set during the installation of the report server.

If the report server is installed into an environment where Microsoft(R) Internet Information Services is not installed, you should install the Microsoft(R) Internet Information Services, and then run the following IIS setting command to build the environment.

```
<installation directory of the Operation Management Client>\bin\sqlSetIISreg.exe -c
```

Note

Before performing installation or executing the IIS setting command, the WWW service (World Wide Web Publishing Service) must be started. If the version of Microsoft(R) Internet Information Services is 6.0, check whether a site set as "defined Web site" exists.

This creates the following virtual directories in Microsoft(R) Internet Information Services.

Service	Setting item	Settings
WWW service	Alias	SSQC
	Directory	<Installation directory of operation management client> \www Example) C:\Program Files\SystemwalkerSQL-C\www
	Access right	Read Execution (including scripts)

Make the above settings also when a virtual directory is set manually.

See

For details on how to set the virtual directory, refer to the online documentation for the Microsoft(R) Internet Information Services.

6.2 Setting a virtual directory property

It is necessary to set up the property of a virtual directory manually.

Set an account with the Administrator authority to be used for anonymous access. Please make the following settings:

1. Select the virtual directory name SSQC from the setting window of Microsoft(R) Internet Information Services.
2. Make the following directory security settings in the Properties window of the above virtual directory:
 1. Select the "Anonymous access" check box.
 2. Set an account with the Administrator authority to be used for anonymous access.
 3. Clear the "Basic authentication" check box.

Point

After the report server environment is set to this stage, check the settings are correct according to the following procedure

1. [Check whether reports can be displayed from the Web Site Management Window.

Click the [Trend Reporter] button on the Web Site Management Window to check whether the registered reports list can be displayed.

See

If the registered reports list can not be displayed, check the settings while referring to "[16.2 Report Display](#)" in the *Troubleshooting Guide*.

Chapter 7 Configuring the Operating Environment

This chapter explains how to configure the Web Site Management Functionality operating environment with the Web Site Management Window, using the system in "3.1 System Configuration" as an example.

Operations for configuring the Web Site Management Functionality operating environment

The following operations must be performed before the Web Site Management Functionality can be used.

Operation	Reference section	Remarks
Registering a management server	7.1 Registering a Management Server	Required Registering with the "7.1.1 Web Site Management" window is required.
Registering managed server	7.2 Registering a Managed Server	Required "7.2.1.1 Registering a Managed Server" and "7.2.2 Registering an Analysis Target Server" are required.
Registering a group	7.3 Registering a Group	Register a group if it is needed to manage multiple servers together. Make settings here.
Registering a report server	7.4 Registering a Report Server	Register a report server if it is needed to use report. Make settings here.

Starting the Web Site Management window

[Web Site Management] windows can be started by visiting the following URL with a Web browser.

[Windows]

If management server is Windows:

```
http://management server's host name/SQC/default.htm
```

[UNIX]

If management server is Solaris, Linux:

```
http://management server's host name/SQC/index.html
```

Starting the Console

Console can be started by visiting the following URL with a Web browser.

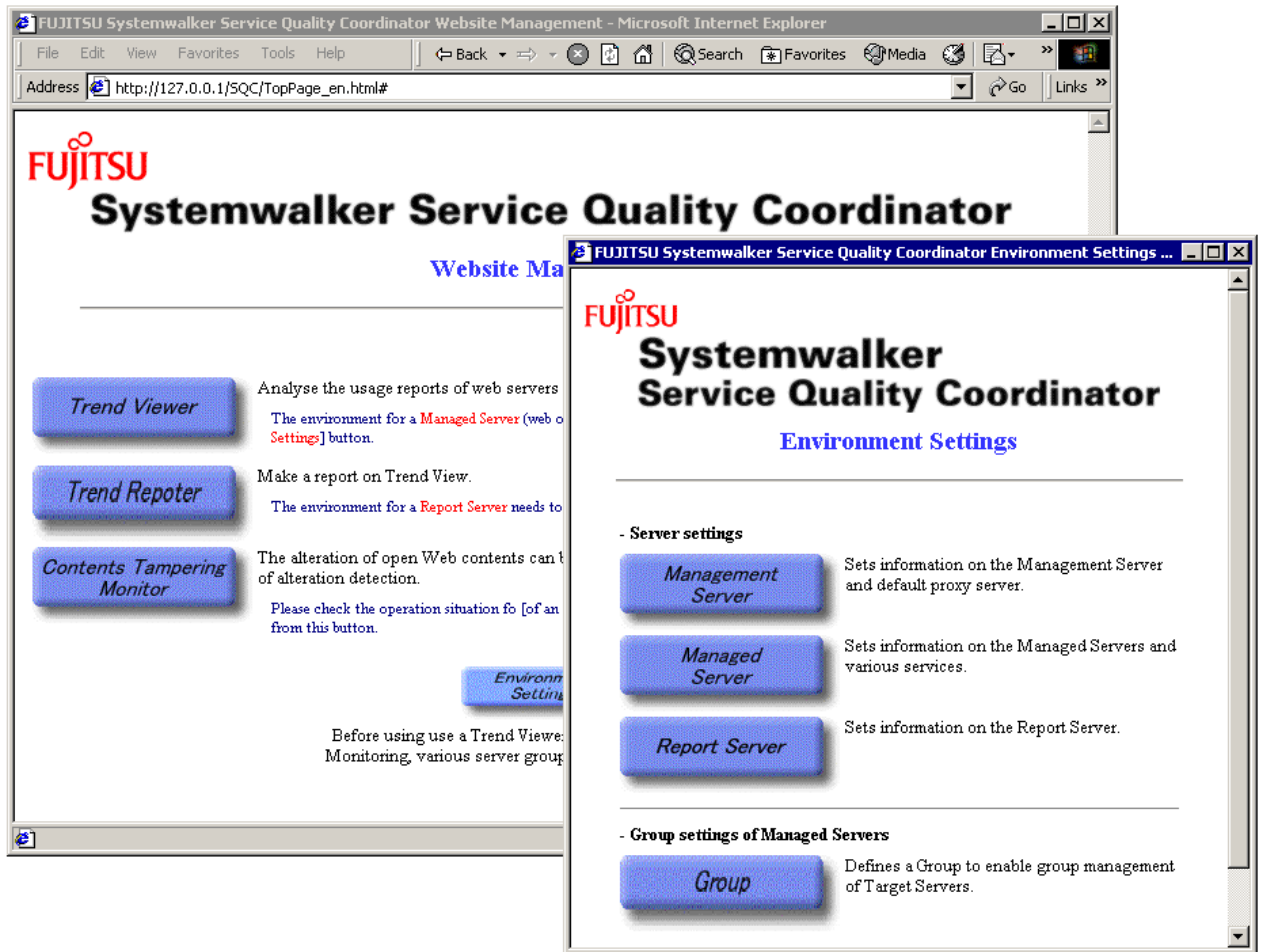
```
http://operation management client's host name/SSQC/console.html
```

7.1 Registering a Management Server

Management server can be registered with the following windows.

7.1.1 Web Site Management

Click the [Environment Setting] button on the [Web Site Management] window to open the environment settings pages.



Click the [Management Server] button on the environment settings pages to display the [Management Server Settings] windows. Set data for the management server.

FUJITSU Systemwalker Service Quality Coordinator Management Server ...

FUJITSU
Systemwalker
Service Quality Coordinator
Management Server Settings

Management Server

Address

Port

Default Proxy Server

Default proxy server used for communication between the manager and agent.

Address

Port

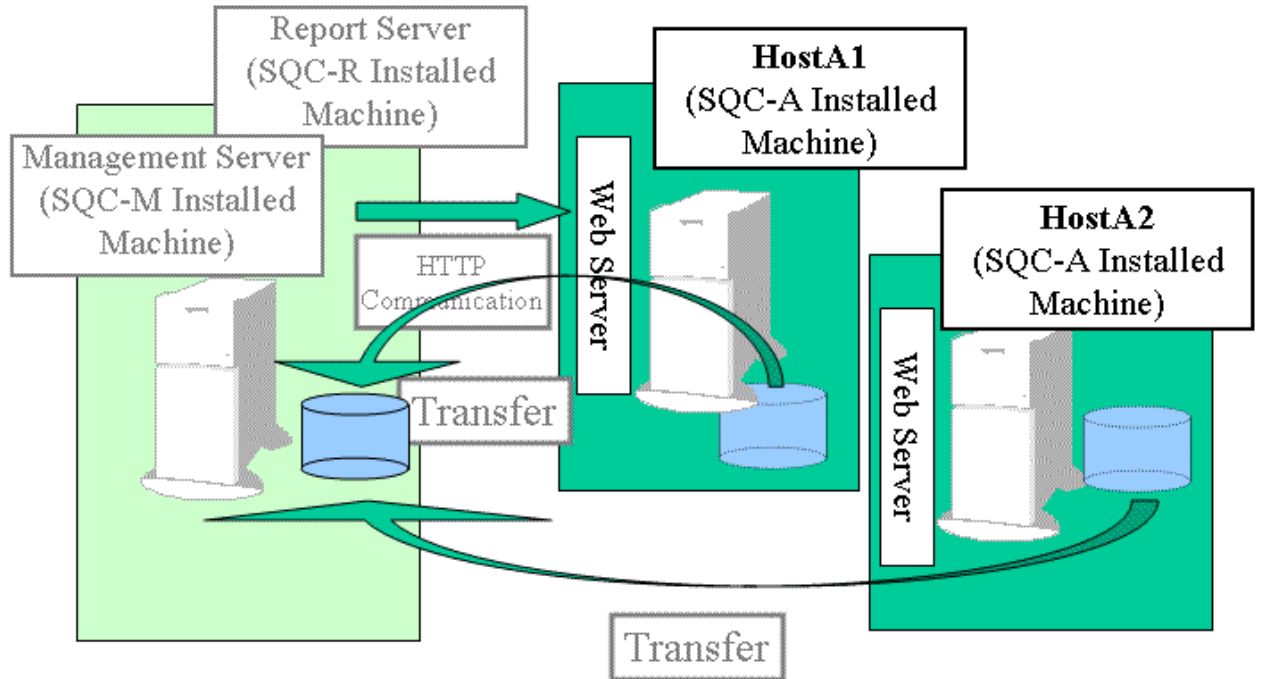
Setting item	Example of settings	Content of settings
Management Server	192.0.2.1	Specify the IP address or host name for the management server.
Port	Not specified	Specify the port number for the Web server used by the management server. This can be omitted if the default port 80 is used.
Proxy server	Not specified	If a default proxy is used in the environment managed by the Systemwalker Service Quality Coordinator, set the data for the following items: Address Specify the host name or IP address of the proxy server. Port Specify the port number for the proxy server.

7.2 Registering a Managed Server

This section explains how to register a Managed Server and management target: analysis target server.

It is required that Agent for Business(SQC-A) is installed on the managed server.

Here, it is required those two servers: HostA1 and HostA2 be registered.



7.2.1 Managed server information

The following types of information need to be registered for registration of a Managed Server

1. Information on the Managed Server
2. Information on the Analysis Target Server

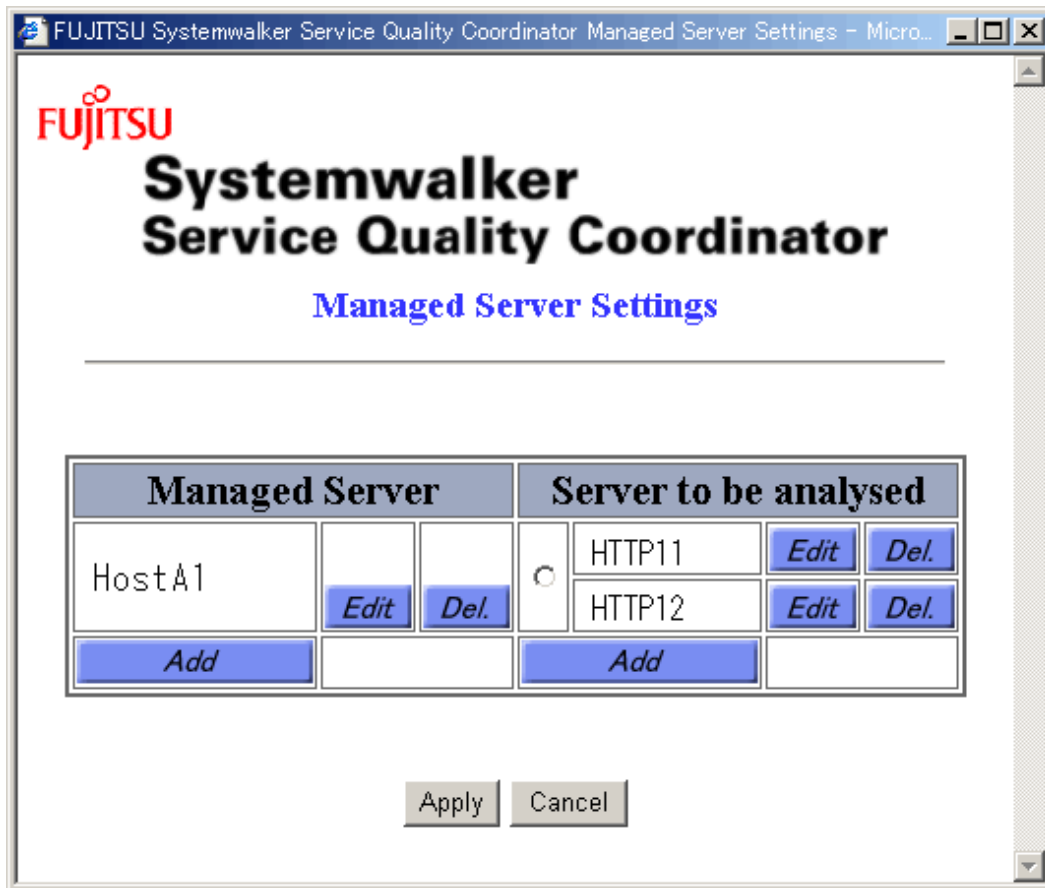
This section explains how to register information on the manager server.

7.2.1.1 Registering a Managed Server

Click the [Managed Server] button on the Environment Settings page, and set information on the Managed Server.

Click the [Add] button below the Managed Server field. The [Managed Server Information] window appears. Add information by repeating this operation, as many times as there are Managed Servers.

Here, HostA1, and HostA2 must be added.



FUJITSU

Systemwalker Service Quality Coordinator

Managed Server Information

- Basic information

Server name

IP address

Subnet mask

Proxy Server

If the proxy server check box is selected, communication between the manager and agent is performed via the proxy server.
Specify the proxy server address and port below; otherwise, the default proxy server defined in the Management Server settings window is used.

Address

Port

- Attributes of Managed Server

Service Quality Coordinator Agent

Server where the Agent is installed.

Agent URL

The following explains the information to be set, using the case of adding HostA1 as an example.

[Basic information]

Setting item	Examples of settings	Contents of settings
Server name	HostA1	Specify the entry name for the Managed Server . Each server name must be unique among all Managed Servers.
IP address	192.0.2.2	Specify the IP address of the Managed Server .
Subnet mask	255.255.255.0	Specify the subnet mask of the Managed Server .

Setting item	Examples of settings	Contents of settings
Proxy server	Not checked	If communication between the manager and agent is performed via a proxy server, select the check box.
Proxy server address	Not specified	If the proxy server check box is selected, specify the address of the proxy server.
Proxy server port	Not specified	If the proxy server check box is selected, specify the port of the proxy server.

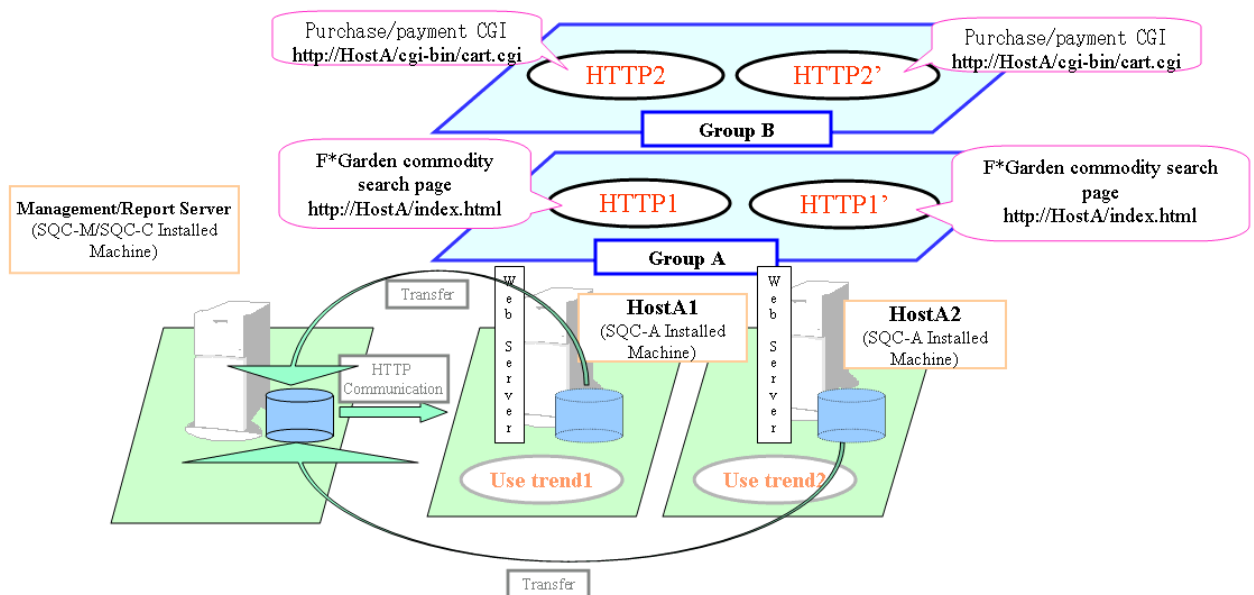


For more information, see "14.1.2 Managed server setting window".

[Attributes of Managed Server]

Setting item	Example of settings	Contents of settings
Systemwalker Service Quality Coordinator agent	Select the check box.	-
Agent URL	http://192.0.2.2/SQC/	Specify the URL of agent. The format is as following: "http://host[:port]/alias/" For the "host", specify the IP address or host name (with domain name). Match the setting with "Name" two lines below [Server] in the use trend database environment definition file.

7.2.2 Registering an Analysis Target Server

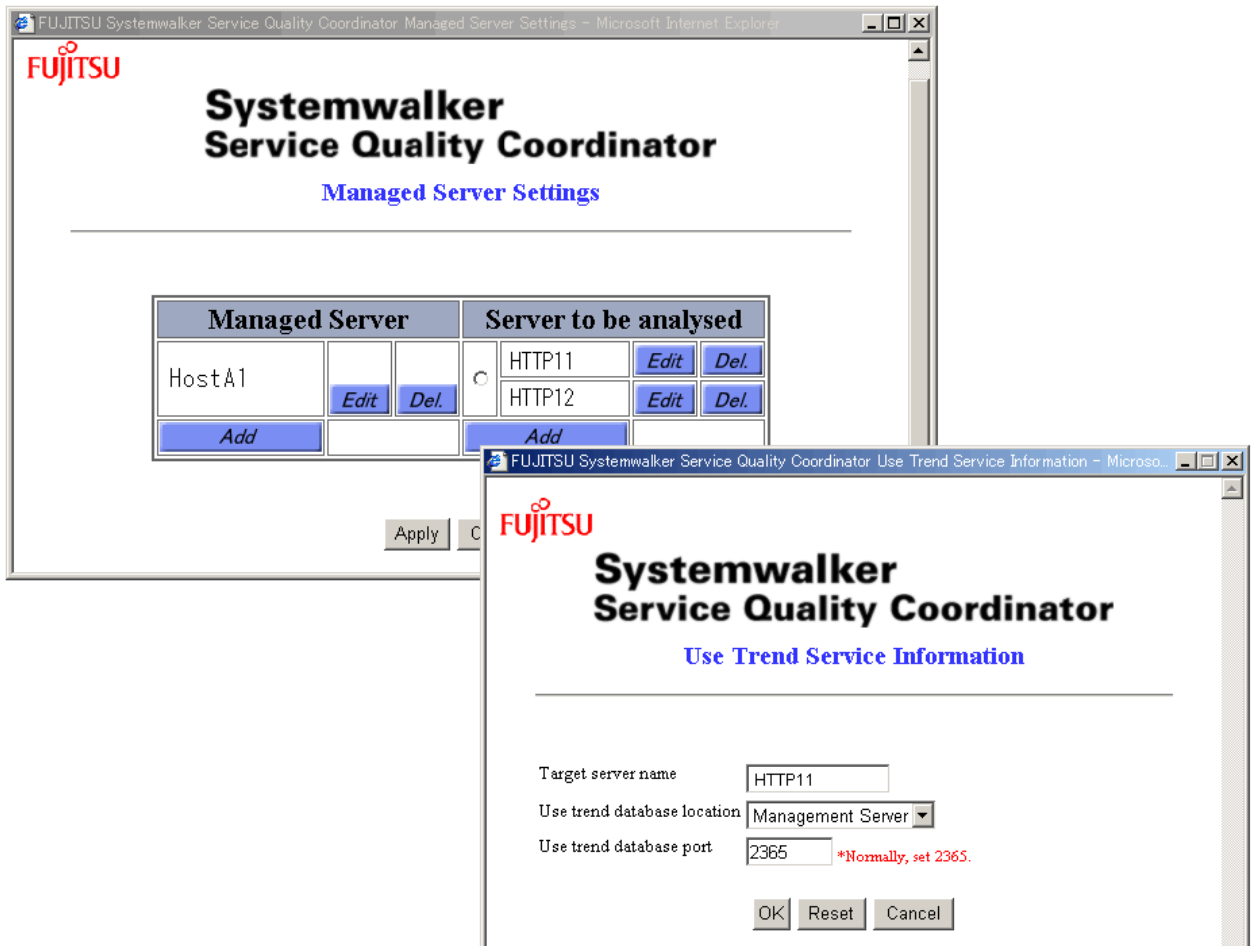


The following analysis target servers must be added here.

1. Use trend target server
 - Use trend 1 of Managed Server HostA1
 - Use trend 1' of Managed Server HostA2

Select the option button on the right side of the name of the Managed Server for which services are to be added, and click the [Add] button below the service field. The [Use Trend Service Information] window appears. Add all services.

How to register each analysis target server is explained as follows.



7.2.2.1 Registering a usage service

[Web Site Management] window->

[Environment Settings] window->

[Managed Server Settings] window->

Select the option button on the right side of the name of the Managed Server for which analysis target servers are to be added, and click the [Add] button below the analysis target server field. The following window displayed.






In the [Use Trend Service Information] window, set the Use Trend Service Information for the Managed Server.

Note

With the Managed Server selected on the [Managed Server Setting] window, if [Systemwalker Service Quality Coordinator Agent] check box is OFF when setting [Managed Server Information] window, analysis target server cannot be set.

The following explains the settings for an example of adding HostA1 use trend services.

Setting item	Examples of settings	Contents of settings
Target server name	HostA1	Specify the name of the server to be analyzed. The specified name must be unique among all use trend services regardless of the Managed Servers that add service.

Setting item	Examples of settings	Contents of settings
		 Point The specified name must match the character string specified for "Name" in the use trend database environment definition file that is used when the Trend Viewer is defined.
Use trend database location	Management server	Specify whether the use trend database for the use trend service is to be managed on the Managed Server or management server.
Use trend database port	2365	The use trend database port is usually 2365. Change this setting if this has been changed to any other port number. Otherwise, there is no need to change the default value (2365).  Note [Windows/Linux] The use trend database port is set up when SQC-A is installed. [Solaris] The use trend database port is not set up when SQC-A is installed.  See Refer to " 11.1.1.2 Start operation " for details on how to set up the use trend database port.

Similarly, add use trend services also for HostA2. Repeat the procedure explained in this section.

 **See**

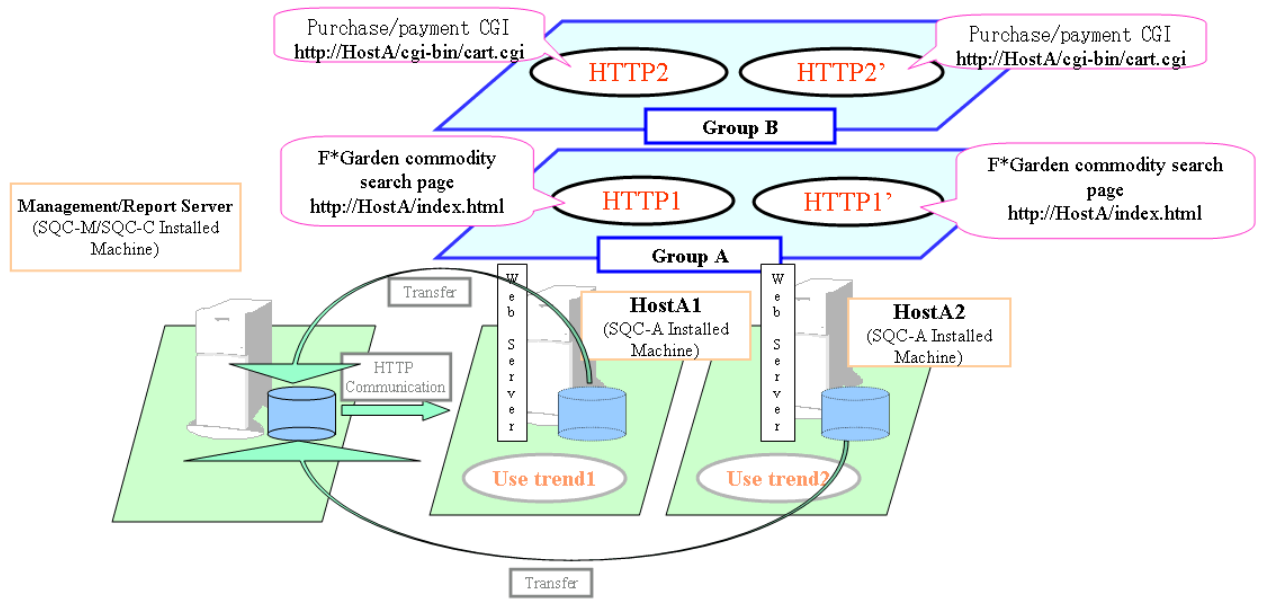
.....
See "[14.1.2.2 Usage service information window](#)" for details.
.....

7.3 Registering a Group

When multiple analysis target servers configure a virtual server or hosting, the multiple servers can be registered as a group.

When the group is registered, the analysis target servers can be managed together.

This section explains how to set with an example of grouping HostA1 and HostA2.

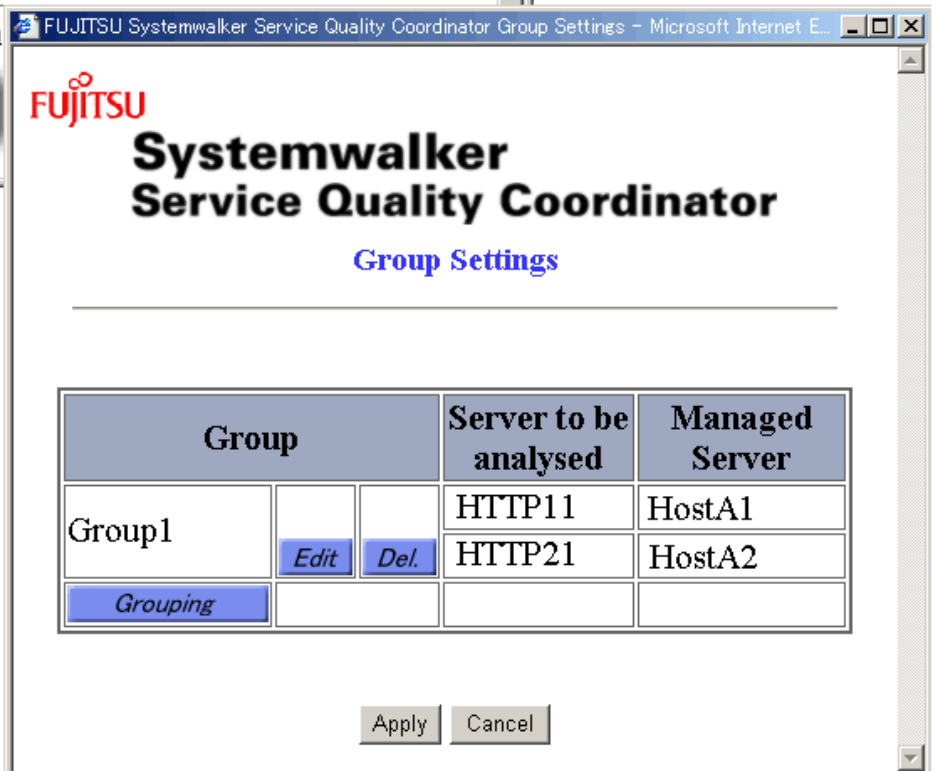


7.3.1 Group Information

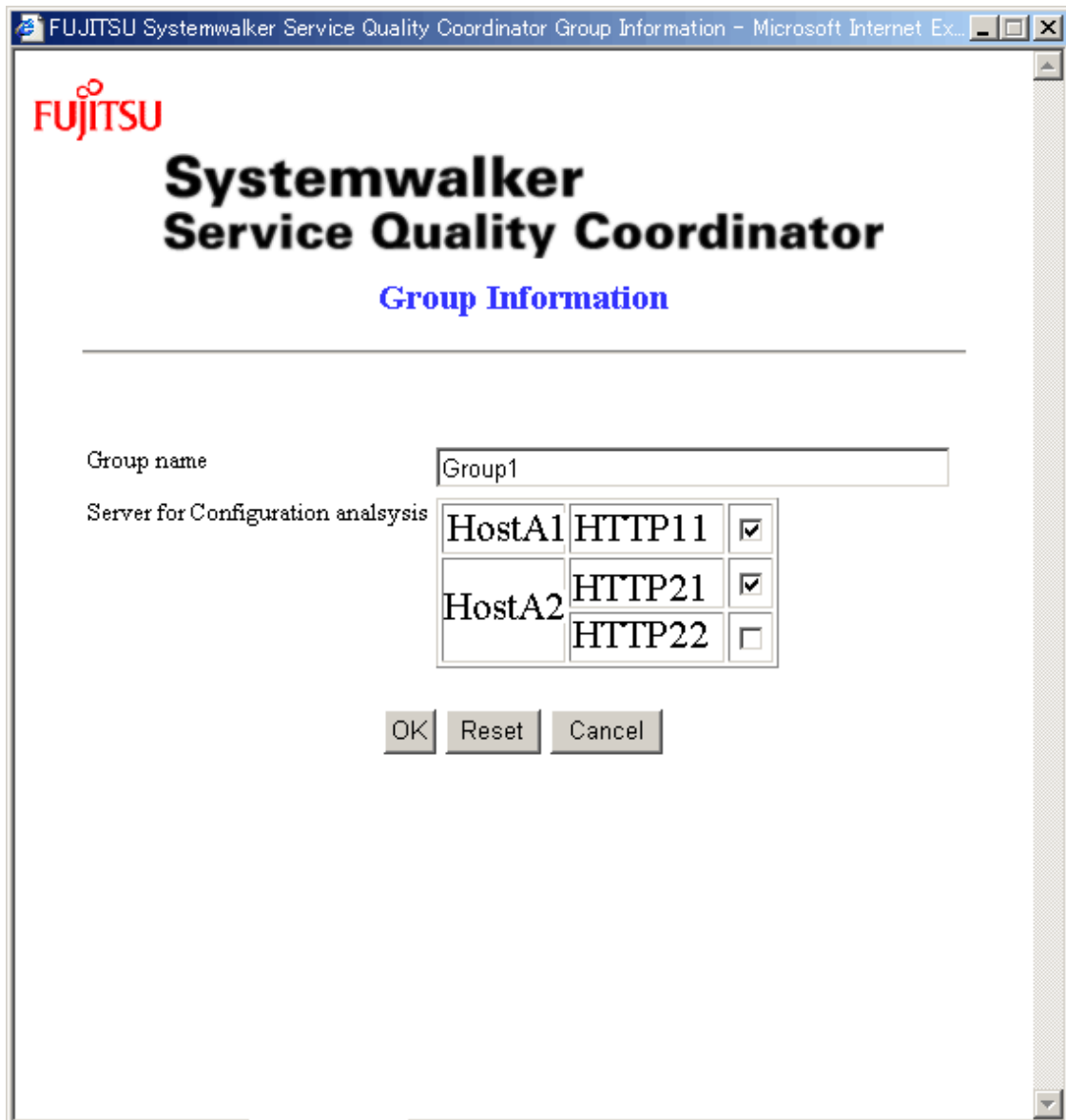
Open the [Group Settings] window following the following procedure.

Click the [Environment Settings] button on the [Web Site Management] window

->Click the [Grouping] button



Click the [Grouping] button below Server field. The following window appears.



The following explains the settings for the HTTP1_1/HTTP1_2 of the HostA1/HostA2.

Setting item	Examples of settings	Contents of settings
Group name	Group1	Specify the entry name for the group of servers. The specified name is used to indicate the group in each function window.
Component server	Select the HTTP1_1 of the HostA1, and the HTTP1_2 of the HostA2.	Check the checkboxes of the servers from the server list of the servers that composed the server group.

Also set the HTTP2 of the HostA1/HostA2. Similarly.



For the settings about the group, refer to "14.1.4 Group Settings window".

7.4 Registering a Report Server

Click the [Environment Settings] button on the [Web Site Management] window to open the Environment Settings page.

Click [Report Server] button to open [Report Server Settings] window.



The following explains the settings for adding a report server, using the system in "3.1 System Configuration" as an example.



Web Site Management Functionality uses the operation management client as the report server.

Setting item	Examples of settings	Contents of settings
Address	192.0.2.1	Specify the address of the report server. In the system used as an example, the management server and report server are installed on the same machine. So, specify the IP address of the management server.
Port	80	-

Chapter 8 Checking Operation

This chapter explains how to verify the following functions:

8.1 Displaying the Usage Analysis Window

This section explains how to display the usage analysis window.



It is required that the service of the usage DB reference engine be started in advance. Refer to "[11.1.2.2 Start operation](#)" for details.

To display the analysis window, do the following on the Web Site Management window of the Manager.

1. Click the [Trend Viewer] button on the [Web Site Management] window to display the [Trend Viewer-agent selection] page.



2. Choose the agent to be analyzed in [Trend Viewer-Agent selection] window and click the [OK] button.



3. The following window appears.

The screenshot shows the Fujitsu Trend Viewer interface. On the left, there are several dropdown menus for configuration: 'Analysis target server' (Web :HTTP11), 'Data type' (Summary), 'Analysis method', 'Analysis period' (Day: hour unit), and 'Unit' (Day: hour unit). Below these is a date selection list from 2004/02/26 to 2004/03/09, with 2004/03/05 selected. On the right, a table displays the report data for the period (Day: hour unit) 2004/ 3/ 5 0:00 - 23:59. The table has three columns: Item, Data, and Explanation.

Item	Data	Explanation
Session count (total)	13 times	Total number of visits on the server.
Request count (total)	27 times	Total number of URL requests on the server.
Traffic (total)	438 KB	Total amount of data sent from the server.
Hit count (total)	22 times	Total count of hit.
Client	0 times	Total hit count on the client.
Server	22 times	Total hit count on the server.
Error count (total)	5 times	Total number of errors.

 See

The Trend Viewer uses Java™ applet. For details on the Java™ applet, refer to "3.2 Environment Settings procedures".

8.2 Displaying a Report

This section explains how to display a report.

 Note

It is required that the service of the usage DB reference engine be started in advance. Refer to "11.1.2.2 Start operation" for details.

1. Click the [Trend Reporter] button on the [Web Site Management] window.



2. Click the [Generate] button on the [List of registered reports] page.



3. After all items on the left of [Registry of report] are set, click [TEST] button.

The screenshot shows a web browser window titled "FUJITSU Systemwalker Service Quality Coordinator Registry of report - Microsoft Internet Explorer". The page features the FUJITSU logo at the top left. Below the logo, there are several form fields and sections:

- Registered Report Name:** A text input field containing "HostA1HTTP1".
- Category:** A dropdown menu with "Analyzing Trend View(Summary)" selected.
- Report Type:** A dropdown menu with "Summary" selected.
- Report Object:** Radio buttons for "Service" (selected) and "Web Site". Below them, a text input field for "Service/Web Site :" contains "HostA1::HTTP1".
- Report Period:** A dropdown menu with "Today" selected.
- A large rectangular box with a border and a downward-pointing arrow above it, containing the text "It is not necessary to choose".
- Select Condition:** A dropdown menu with "None" selected. Below it, an equals sign "=" is followed by a text input field containing "It is not necessary to input".
- Two buttons: "Test" and "Register".

The browser's status bar at the bottom shows "Done" on the left and "Local intranet" on the right.

The following screen is displayed.

FUJITSU Systemwalker Service Quality Coordinator Registry of report - Microsoft Internet Explorer

2004 03 07 (Sun) 22:56:19

FUJITSU

Registered Report Name
HostA1HTTP1

Category
Analyzing Trend View(Summary)

Report Type
Summary

Report Object
 Service Web Site
 Service/Web Site : HostA1::HTTP11

Report Period
Today

▲
It is not necessary to choose
▼

Select Condition
None
= It is not necessary to input

Test
Register

[Trend View] Summary

Registered Report Name	HostA1HTTP1
Report Object	
Service/Web site	HostA1::HTTP11
Report Period	2004 03 05 (Fri)
Selecting item	None
Selecting key word	None

Summary in specified the term

Total Session count	Total Request count	Total Traffic volume	Total Hit count	Hit count (Client)	Hit count (Server)	Hit count (Remote)	Error count
13 times	27 times	437.53 KB	22 times	0 times	22 times	0 times	5 times

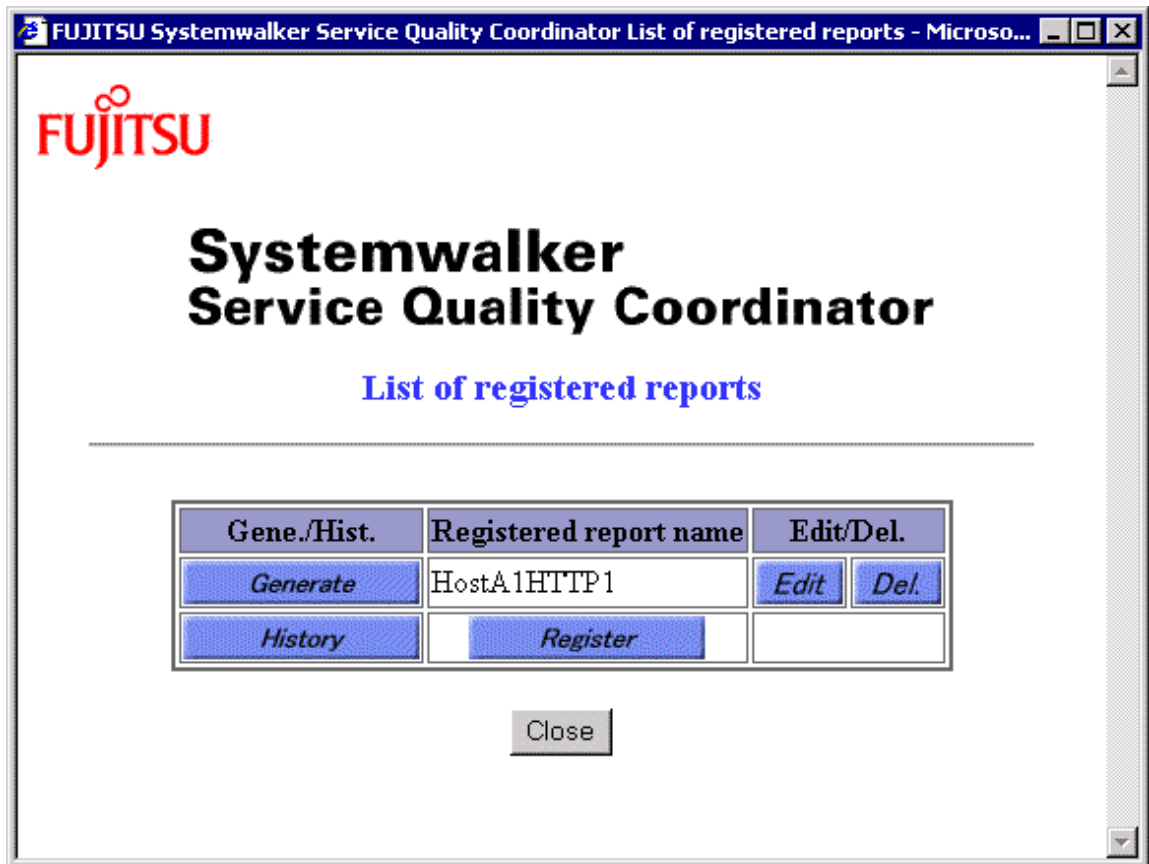
[Print the report](#) [Download data](#)

Done Local intranet

4. Make sure the report conditions are correct and click the [Register] button.

5. Click [Generate] button on the left of Registered report name that is registered the report conditions in [List of registered reports] screen.

In this case, hostA1HTTP1 is selected.



6. Make sure the registered report name is HostA1HTTP1. Click the [Generate] button.

FUJITSU

Registered Report Name
HostA1HTTP1

Category
Analyzing Trend View(Summary)

Report Type
Summary

Report Object
 Service Web Site
Service/Web Site :
HostA1::HTTP1

Report Period
Today

▲
It is not necessary to choose
▼


Select Condition
None
=
It is not necessary to input

Generate

Done Local intranet

- The report is displayed on the right of the screen.

FUJITSU Systemwalker Service Quality Coordinator Generate of report - Microsoft Internet Explorer 2004 03 07 (Sun) 22:56:19



Registered Report Name
HostA1HTTP1

Category
Analyzing Trend View(Summary)

Report Type
Summary

Report Object
 Service Web Site
 Service/Web Site : HostA1::HTTP11

Report Period
Today

▲
It is not necessary to choose
▼

Select Condition
None
= It is not necessary to input

[Trend View] Summary

Registered Report Name	HostA1HTTP1
Report Object	
Service/Web site	HostA1::HTTP11
Report Period	2004 03 05 (Fri)
Selecting item	None
Selecting key word	None

Summary in specified the term

Total Session count	Total Request count	Total Traffic volume	Total Hit count	Hit count (Client)	Hit count (Server)	Hit count (Remote)	Error count
13 times	27 times	437.53 KB	22 times	0 times	22 times	0 times	5 times

[Print the report](#) [Download data](#)

Done Local intranet

Part 3 Installation(Application)

Chapter 9 Web Marketing.....	71
Chapter 10 Monitoring for Tampering with Web Contents.....	102

Chapter 9 Web Marketing

This chapter explains how to operate Trend Viewer.

9.1 Determining an Analysis Method and Configuration

9.1.1 Overview of analysis type

Trend Viewer can be used as follows:

- Analysis by the use of trend analysis window
- Analysis by constant reporting

Analysis by the use trend analysis screen

Click the [Trend Viewer] button on the [Web Site Management] window to use this analysis. Analysis can be done interactively.

Use the analysis by the of use trend analysis screen when the detail of the Web site usage is needed to be analyzed.

Analysis by constant reporting

First click the [Trend Reporter] button on the [Web Site Management] window, then select a report type for use trend analysis to use this analysis. Because that frequently used report can be registered and the report can be printed, in case where periodical analysis as weekly report or monthly report is required, or int the case that the result should be saved this analysis by constant reporting is effective.

Analysis types

Trend Viewer displays analysis results of availability of the following two servers and one Web site group (analysis target server type):

- Web server
- Proxy server
- Web site group

Analysis results (analyzed data types) are classified into the eight types listed below. The Web server can display all of the eight types, and the Proxy server can display six types.

- Summary (total of each report of analysis target servers)
- Session report
- Request report
- Traffic report
- Cache report
- Error report
- Response report (Web server and Web site group)
- Page navigation report (Web server only)
- Number of actually visiting users report(Trend reporter of Web server only)

Trend Viewer uses various analysis methods (URL base and client base) to display editing results in a graph and list.

9.1.1.1 Traffic display

Traffic is displayed in kilobytes on each page that analyzes traffic status and displays other traffic (or total traffic and total of successful request traffic).

A value from one byte to less than 1,000 bytes is displayed as one kilobyte.

9.1.1.2 Response analysis page

Response analysis pages differ in the following points from other analysis pages.

Relation with SQC extended log collection

Response analysis analyzes data, based on the data that is stored in the SQC extended log file by collecting SQC extended logs. If SQC extended logs are not collected, execution of data analysis obtains no data analysis results.

Display data

A response analysis page displays the three values listed below. These values are displayed in descending order of average times (from lower response to higher response) in the table.

- Average (average response time in analysis period)
- Maximum (longest response time in analysis period (slow response))
- Minimum (shortest response time in analysis period (quick response))

The following table lists the display units and the number of digits.

Item	Explanation
Numeric value unit	Seconds
Number of digits	4 integer numbers and 2 decimal places (third decimal place rounded up)
Display range	0.01 to 3,599.99 seconds (less than 1 hour) (Less than 10 ms is displayed as 0.01 second.)
Value exceeding the display range	Displayed as 1 hour or longer

One hour (3600.00 seconds) or longer is displayed as "One hour or longer," but an actual value is used for the average value.

Graph display/switching

For graph display on the response analysis page in the use trend analysis window, the average, maximum, and minimum are put into graphs for only one line (one URL or client) that is selected from the table, unlike other analysis pages. By default, the graph for only the URL or client whose average time is Top1 (the top line in the table) is displayed. Use the mouse to select a line from the table to display the corresponding graph.

A name (URL or client name) that is selected from the table is displayed as a graph display target name under the analysis type name in the analysis information part (upper part of the graph) of the analysis page.



Note that this operation is the same as "Carrying out advanced analysis" in "11.2.6 Operation of analysis page" described later, but no drill down analysis is carried out for response analysis.

9.1.2 Analyzing cyclic transition

By specifying "Session report" and "Request report" as analyzed data types, you can analyze transitions in session and request reports in each period by various methods such as URL.

Analysis of transitions in each period enables the following kinds of questions to be answered:

- Which pages in which time zones are accessed a lot?
- Which pages are accessed most on weekends?
- How is the number of accesses affected by promotions such as advertising campaigns?

Because values and average values of previous terms can also be displayed during analysis, usage and transitions are easily compared and analyzed.

9.1.3 Analysis that identifies users

To analyze customer trends, you can perform analysis that identifies users.

Users can be identified in the following ways:

- Identifying users by user name authenticated on the Web server

If authentication is performed on the Web server, authorization user names can be used as a key for analysis.

The following is the procedure for analysis that identifies users by authentication of user name on the Web server.

1. Set the Web server log so that information about authorization user names is output to the Web server log.
2. In the usage DB environmental definition file of Systemwalker Service Quality Coordinator, add tokens (c-user) for the authorization user names of clients to the record format definition of the log file to be analyzed.
3. Select "Authorization user name base" as the analysis method on the analysis window before performing an analysis.

- Identifying users by IDs set in a cookie

If authentication is performed on the Web server using CGI, no information about authorized users is output to the Web server log. You can perform analysis that identifies users by setting user names authenticated by CGI in a cookie.

If authentication is not performed by CGI, you can perform analysis that identifies users by setting for Cookie an identifier that identifies the user on each page of the Web service.

The following is the procedure for performing analysis that identifies users with an ID set in a cookie.

1. Set user information in a cookie on each page of the Web service.
2. In the usage DB environmental definition file of Systemwalker Service Quality Coordinator, to the record format definition of the log file to be analyzed, add tokens (c-cookie) in a cookie.
3. Select "Access ID base" as the analysis method on the analysis window before doing the analysis.

- Identifying users by client host

When the Web server performs no authentication, such as that by the service that publishes information, and no information is set in a cookie, then users can be identified by the client host.

For the identification of users by client host, the ID address and host name of the client is used.

The following is the procedure for analysis that identifies users by client host.

1. Set the Web server log so that information about client hosts is output to the Web server log.
2. In the usage DB environmental definition file of Systemwalker Service Quality Coordinator, add tokens (c-host) for client hosts to the record format definition of the log file to be analyzed.
3. Select "Client host name base" or "Client IP address base" as the analysis method on the analysis window before doing the analysis.

Note

For analysis to identify users, content must be created such that authentication is performed or a cookie is set reliably when the Web service to be analyzed is used. If a page in the Web service is accessed directly without authentication or Cookie settings, then analysis that identifies users cannot be done.

Analysis that identifies users with an ID set in a cookie cannot be done if the user blocks cookies with a browser setting. In such a case, analysis that identifies users by client host can be used.

Note that in analysis in which users are identified by client host, different users are handled as the same client host in the following cases:

- IP addresses are allocated dynamically by DHCP (for example, ISP is used to connect).
- Access is via a proxy server (for example, corporate users connecting from behind a firewall).

9.1.4 Analysis using CSV output

This section explains analysis that uses CSV output of the Trend Viewer.

9.1.4.1 Analysis using the analysis window and analysis using CSV output

In Systemwalker Service Quality Coordinator, the following two methods can be used to analyze the usage of Web sites:

- Analysis using the analysis window
- Analysis using CSV output

In analysis that uses the analysis window, a browser can be used for analysis. The types of analysis that are available are the standard analysis methods provided by Systemwalker Service Quality Coordinator.

In analysis that uses CSV output, information from data in the usage DB of Systemwalker Service Quality Coordinator output to files in CSV format based on the data type is used to perform various types of analysis, such as analysis using added methods of analysis or analysis that includes other types of information.

For analysis that uses the analysis window, up to 300 lines of results are displayed. For analysis that uses CSV output, all cases can be analyzed.

9.1.5 Integrated analysis with data on the backbone system

This section describes the integrated analysis of information on the Web server and data on the backbone system.

9.1.5.1 Overview of integrated analysis with data on the backbone system

Systemwalker Service Quality Coordinator provides functions that, through the analysis of the Web site usage using the Web server log, are useful for doing business. The following types of analysis are made possible by integrated analysis of information output by Systemwalker Service Quality Coordinator and sales and customer data on the backbone system:

- Product purchase rates and purchased product trends of Web site users (sales data included in analysis)
- Behavior on the Web site of users who purchased products (sales data included in analysis)

- Usage of the Web site based on region, gender, and age (customer data included in analysis)

As shown in the above analysis examples, an analysis that is impossible with only Web server information becomes possible when data on the backbone system is integrated into the analysis. Integrated analysis makes Web sites more effective for business.

Systemwalker Service Quality Coordinator collects log data for a Web server and uses products such as the Symfoware e-Business Intelligence Suite, with advanced analysis functions that include data mining, for integrated analysis that uses data on the backbone system.

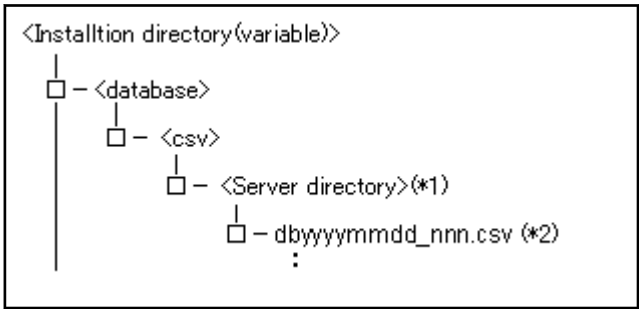
9.1.5.2 Method of integrated analysis with data on the backbone system

The following explains how to perform integrated analysis that uses data on the backbone system.

1. In the analysis target server definition block in the Usage DB environmental definition file, specify combined operation with both the Usage DB and CSV-format log file as the Usage DB operation type.

```
DatabaseMode = both
```

2. Log data for the Web server is output to the following directory as a CSV-format file by the Usage DB Registration Engine.



Note: < > indicates a directory.

(*1) The server directory is created with the name specified in Symbol of the Analysis Target Server Definition Block in the Usage DB environmental definition file.

(*2) Variables in the CSV-format log file name are listed below. Year/Month/Day is the date when the Usage DB is switched (created).

yyyy	Year (1980-)
mm	Month (01 - 12)
dd	Day (01 - 31)
nnn	Sequential number (001 - 099)

3. Enter the CSV-format log file output as shown above in the DB used by the analysis product (such as Symfoware e-Business Intelligence Suite) that performs integrated analysis with the data on the backbone system.

See "[15.2.6 Usage Log file](#)" for information about the format of CSV format log files.

4. The analysis product is used to do the analysis.

9.1.6 If you would like to analyze response

This section explains how to make analysis aiming at response when the customer accesses a page.

Analysis aiming at response enables the following information to be recognized and used for Web site operation.

- How long does it take for processing on the server system?

SQC extended log is used to analyze response.

9.1.6.1 SQC Extended Log Collectin

The SQC Extended Log Collection is used to collect and accumulate data not collected by the functions provided by the Web service (such as the Web server). Data accumulated by the SQC Extended Log Collection is called the "SQC extended log." The following SQC extended log can be collected and stored.

- [9.1.6.2 Response logs](#)
- [9.1.6.3 SQC extended log file](#)

9.1.6.2 Response logs

9.1.6.2.1 Outline

The response log is a log in which data on the response time of the CGI program collected in terms of the Web page user is accumulated.

The response time is a time interval required to receive a result from the CGI program after the Web page user executes a service that calls the CGI program.

For example, in the case of a Web page that executes searches, the response time is a time interval required to display a search result after the search is started.

Data is collected and accumulated in the response log by using the following three functions:

Data collection function1

Java™ applet (**ResLog1.class**) that runs on the Web browser. This function is called when the user references the Web pages and executes a service that calls the CGI program; and data is collected.

To run this function, refer to "[Editing WebPages](#)" in advance.

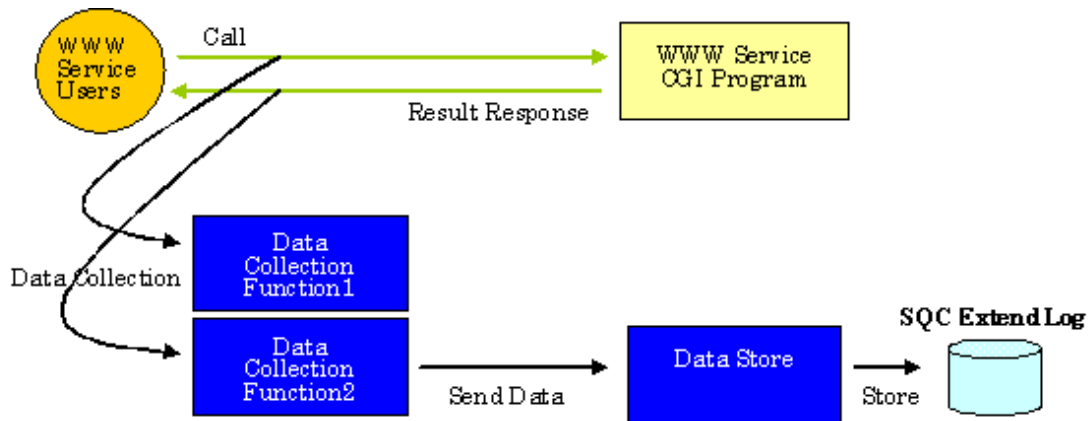
Data collection function2

Java™ applet (**ResLog2.class**) that runs on the Web browser. This function is called when the Web page user receives a result of a service that calls the CGI program. This applet collects data when a result is received and then sends the response time to the data accumulation function after calculating it together with data of the data collection function1.

To run this function, refer to "[Editing WebPages](#)" in advance.

Data accumulation function

CGI program (**reslog.cgi**) that runs on the Web server (installation machine). The data accumulation function is automatically started when data collection function2 is started. This function accumulates data sent from the data collection function2 in the SQC extended log file.



9.1.6.2.2 Making settings for log collection

This section explains how to make settings for response log collection.

Before making settings

It is necessary to register the CGI program (**reslog.cgi**) of the data accumulation function with the Web server in advance so that it can be executed. For details of the registration, refer to "[4.1 Settings for Web Server](#)".



See

.....
 Java™ applet is used by the data accumulation function (ResLog1.class, ResLog2.class). For details about Java™ applet, refer to "[3.2 Environment Settings procedures](#)".

Editing WebPages

Incorporate the Java™ applet for log collection into the HTML documents of each Web page that makes log collection. Both of the following two related Web pages must be edited:

- Web page that calls a service
 - Web page that calls the CGI program of a service
 - For example, a Web page that executes searches when a keyword is given.
- Web page that receives results
 - Web page that receives results (displays results) from the CGI program.
 - For example, a Web page that displays search results.

Editing Web pages that call a service

Incorporate the Java™ applet (ResLog1.class) of data collection function1 into the HTML document of the Web page that calls a service.

The following is a sample HTML document. URL in CODEBASE within the sample is described assuming that, like the setting example in "[4.1 Settings for Web Server](#)", the physical path of the directory www under the installation directory is registered as the alias "SQC".

In the following example, the Java™ applet (ResLog1.class) of the data collection function1 is called when the search button is clicked.

```

<!-- -->
<!-- Response log collection page Sample (Part 1) -->
<!-- -->
<HTML>
<HEAD>
<TITLE> Search service page (sample) </TITLE>
</HEAD>
<BODY BGCOLOR=WHITE>
<!-- ***** Systemwalker SQC (begin) ***** -->
<APPLET NAME="ResLog1" CODEBASE="/SQC/classes"
CODE="ResLog1.class" ARCHIVE="reslog.jar" WIDTH=1 HEIGHT=1>
</APPLET>
<!-- ***** Systemwalker SQC (end) ***** -->
<CENTER><FONT COLOR=GREEN> Search service page(sample) </FONT></CENTER>
<BR><BR>
<FONT SIZE=5 COLOR=BLUE> Search service </FONT>
<HR>
<FORM METHOD="post" ACTION="/cgi-bin/search.cgi">
Search key
<INPUT TYPE="text" NAME="key1" SIZE="25">
<BR><BR>
<INPUT TYPE="reset" VALUE="Reset">
<INPUT TYPE="submit" VALUE="Search" onClick="document.ResLog1.run()">
</FORM>
<HR>
<FONT COLOR=RED> Notes </FONT>
<P>
This site records and accumulates response reports of the search service. Results are used
exclusively to improve the search service. No violation of privacy is intended.
</P>
</BODY>
</HTML>

```

[Sample explanation]

Content	Explanation
Blue character	Description for incorporating data collection function1
Path to be specified in CODEBASE	URL of the storage directory of the Java™ class file of this product

The above sample is stored at the following storage location after installation.

[Windows]

```
Installation directory\sample\search_request_jp.html
```

[UNIX]

```
/opt/FJSVssqc/sample/search_request_jp.html
```

Editing the Web page that receives results

Incorporate the Java™ applet (ResLog2.class) into the HTML document of the Web page that receives displays results.

The following is a sample HTML document. URL in CODEBASE within the sample is described assuming that, like the setting example in "4.1 Settings for Web Server" the physical path of the directory www under the installation directory is registered as the alias "SQC".

```
<!-- -->
<!-- Response log collection page Sample (Part 2) -->
<!-- -->
<HTML>
<HEAD>
<TITLE> Search service page (sample) </TITLE>
</HEAD>
<BODY BGCOLOR=WHITE>
<!-- ***** Systemwalker SQC (begin) ***** -->
<APPLET CODEBASE="/SQC/classes"
CODE="ResLog2.class" ARCHIVE="reslog.jar" WIDTH=1 HEIGHT=1>
<PARAM NAME=url VALUE="/SQC/cgi-bin/reslog.cgi">
</APPLET>
<!-- ***** Systemwalker SQC (end) ***** -->
<CENTER><FONT COLOR=GREEN> Search service page (sample) </FONT></CENTER>
<BR><BR>
<FONT SIZE=5 COLOR=BLUE> Search service </FONT>
<HR>
<P>
Search result...
</P>
</BODY>
</HTML>
```

[Sample explanation]

[Windows]

Content	Explanation
Blue character	Description for incorporating data collection function2
Path to be specified in CODEBASE	URL corresponding to the following directory: Installation directory\www\classes
Path to be specified in VALUE	URL corresponding to the following file: Installation directory\www\cgi-bin\reslog.cgi

The above sample is stored at the following storage location after installation.

Installation directory\sample\search_result_jp.html

[UNIX]

Content	Explanation
Blue character	Description for incorporating data collection function2
Path to be specified in CODEBASE	URL corresponding to the following directory: /opt/FJSVswmag/www/classes
Path to be specified in VALUE	URL corresponding to the following file: /opt/FJSVswmag/www/cgi-bin/reslog.cgi

The above sample is stored at the following storage location after installation.

/opt/FJSVssqc/sample/search_result_jp.html
--

Notes on Web page editing

Use the identical string to specify URL in CODEBASE inside the APPLET tag of the Web page that calls a service and that in CODEBASE inside the APPLET tag of the Web page that receives (displays) results. Note that, if the URL is not identical, for example, if one URL is specified using a relative path and the other URL is specified using an absolute path, no response log can be collected.

Operation after settings

If a Web page with the settings for this log collection is used, log collection is carried out in the sequence show below:

	Target	Operation description
1	Web user:	References URL of the Web page using the Web browser.
2	Web user:	Executes a service (for example, a search service) that calls the CGI program.
3	Web user:	Receives a result from the CGI program.
4	Inside:	The response log is collected and accumulated.
5	Inside:	The log is registered with the Usage DB by the Usage DB Registration Engine.

	Target	Operation description
6	Analyzer:	An analysis can be carried out and results can be displayed on the analysis window. The URL based response analysis and client based response analysis are supported.

Note

If there is any error in the edited Web page, the response log cannot be collected. Before providing a Web page service, carry out tests to make sure that the response log is actually collected.

9.1.6.2.3 Stopping log collection

To stop the response log collection, delete (or comment out) the lines added to the HTML document of the Web page that start log collection. Delete such text from both the HTML page that calls a service and the HTML page that receives results.

To be deleted is the **blue text** in each HTML page as described in "9.1.6.2.2 Making settings for log collection". Once deleted, no response log is collected and accumulated even if this Web page is referenced and a service is called.

9.1.6.2.4 Log format

A response log with one line of text is accumulated in the SQC extended log file in response to one piece of data sent from data collection function2.

The format of one line is as follows. The field is delimited by one blank character.

1.Date 2.Type 3.Version 4.HostName 5.Path 6.Reserve 7.KeyData

No.	Field	Explanation														
1.	Date	<p>Time at the log is accumulated. This time is a local time on the installation machine. Its format is as follows and blue characters are variable: [dd/mon/yyyy:hh:mm:ss SHHMM]</p> <p>The meaning of each field is as follows:</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>dd</td> <td>Day (01 - 31)</td> </tr> <tr> <td>mon</td> <td>Month ("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec")</td> </tr> <tr> <td>yyyy</td> <td>Christian era (1970 -)</td> </tr> <tr> <td>hh</td> <td>Hour (00 - 23)</td> </tr> <tr> <td>mm</td> <td>Minutes (00 - 59)</td> </tr> <tr> <td>ss</td> <td>Seconds</td> </tr> </tbody> </table>	Field	Meaning	dd	Day (01 - 31)	mon	Month ("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec")	yyyy	Christian era (1970 -)	hh	Hour (00 - 23)	mm	Minutes (00 - 59)	ss	Seconds
Field	Meaning															
dd	Day (01 - 31)															
mon	Month ("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec")															
yyyy	Christian era (1970 -)															
hh	Hour (00 - 23)															
mm	Minutes (00 - 59)															
ss	Seconds															

No.	Field	Explanation	
		Field	Meaning
			(00 - 59)
		S	Flag of time difference with the Coordinated Universal Time (UTC) ("+","-")
		HH	Hour of time difference with the Coordinated Universal Time (UTC) (00 -)
		MM	Minutes of time difference with the Coordinated Universal Time (UTC) (00 -)
2.	Type	Data type (code that indicates the log type) The response log corresponds to "2".	
3.	Version	Version level of the log format. Currently only "1" for the response log.	
4.	HostName	(Web page user's) host name or IP address where the browser operates	
5.	Path	Path to the HTML document of the Web page	
6.	Reserve	Reserved Currently always "0"	
7.	KeyData	Response time (in milliseconds)	

For the file name, capacity estimation, and SQC extended log file switching, refer to ["9.1.6.3 SQC extended log file"](#).

9.1.6.3 SQC extended log file

This subsection explains the SQC extended log file.

The SQC extended log file is created automatically by the SQC extended log collection when the SQC extended logs are accumulated.

9.1.6.3.1 File name

Storage location

The SQC extended log file is stored under the following directory.

Directory for SQC extended log file

[Windows]

Variable file storage directory\extend-log\

[UNIX]

```
/var/opt/FJSVssqc/extend-log/
```

File name format

The SQC extended log file name has the following format. A new file name is created each time the SQC extended log file is switched. Characters shown in blue indicate variables.

logyyyyymmdd_nn

[Explanation of variable characters]

Symbol	Meaning
yyyy	Year created (1970 -)
mm	Month created (01 to 12)
dd	Day created (01 to 31)
nn	Serial number of the SQC extended log file among those log files created on the same day (01 to 99)

9.1.6.3.2 Capacity estimation

The formula for estimating the capacity per day is as follows. Characters shown in blue indicate variables.

$$(\text{Capacity per day}) = (50 + A + B) * C$$

Symbol	Meaning
A:	Average number of bytes of host name or IP address (of the Web page user) when the browser is operating
B:	Average number of bytes of path in HTML document of Web page
C:	Average number of access to HTML document of Web page per day

9.1.6.3.3 Switching the SQC extended log file

To simplify work such as backup of the SQC extended log file, the SQC Extended Log Collection periodically creates a new SQC extended log file (file name described in "9.1.6.3.1 File name": logyyyyymmdd_nn) to change the accumulation destination of the SQC extended log to a new log file. This is called "SQC extended log file switching."

SQC extended log file switching is performed in accordance with the settings in the Extended Log Environment Definition File "ExtendLogConfig".

For details on how to set the Extended Log Environment Definition File, refer to "9.1.6.4 Setting an extended log environment definition file".

9.1.6.4 Setting an extended log environment definition file

"Extended log environment definition file" is a file in which SQC extended log accumulation methods are defined. The extended log environment definition file needs to be set before the SQC extended log is collected.

This setting is required only when the SQC extended log is collected.

9.1.6.4.1 File storage location

The extended log environment definition file is a text file. Use a text editor such as Notepad to create and edit the file. The file path is given below.

[Windows]

```
Variable file storage directory\control\ExtendLogConfig
```

[UNIX]

```
/etc/opt/FJSVssqc/ExtendLogConfig
```

A sample of the extended environment definition file is prepared. Edit this sample to facilitate installation. This sample is stored in the following directory.

[Windows]

```
Installation directory\sample\ExtendLogConfig
```

[UNIX]

```
/opt/FJSVssqc/sample/ExtendLogConfig
```

The character code is as follows:

[Windows]

```
ASCII
```

[UNIX]

```
ASCII
```

9.1.6.4.2 Example of definition

A definition example of the extended log environment definition file is given below.

See "[15.2.2 Extended Log Environment Definition File](#)", in the online manual for details on setting the extended log environment definition file.

```
01/Jan/2001:00:00:00 +0900  
[Log]  
LogfileInterval = week(sun)  
01/Jan/2001:00:00:00 +0900
```

LogfileInterval is used to define extended log file switching units. The meaning of each option is listed below.

<Option>	<Meaning>
day	Daily

<Option>	<Meaning>
week(...)	Weekly
month(...)	Monthly

For "Week," use the following value to specify the start point for a week in parentheses.

<Option>	<Meaning>
sun	Sunday
mon	Monday
tue	Tuesday
wed	Wednesday
thu	Thursday
fri	Friday
sat	Saturday

For "month," use the following value to specify the start point for a month in parentheses. However, the last day of the month is specified if the start point is omitted.

<Option>	<Meaning>
Integer number from 1 to 31	Day of the month

 **Note**

Before providing the Web page service to collect the SQC extended log, execute a test to confirm that the SQC extended log is actually collected.

9.1.6.5 Setting a usage DB environment definition file

The Usage DB Environment Definition File defines the conditions for creating databases used to store various log data on the Web services. The file also defines the conditions for creating usage DBs.

Definitions in the use trend DB environment definition file are required to analyze response reports by using the collected SQC extended log.

Specify the analysis target log definition block for the SQC extended log in the use trend DB environment definition file.

For detail of the setting of a use trend database environment definition file, refer to "[15.2.1 Usage DB Environment Definition File](#)".

The following shows a definition example.

[Windows]

```
[Server]
Symbol = PUBLIC
<-- omission -->
```

```
[Log]
Symbol = WWW
<-- omission -->
[Log]
Symbol = Response
Name = ResponseLog
Path = "C:\SystemwalkerSQL\extend-log\log*"
Format = SQC-Extend
Region = +0900
```

[UNIX]

```
[Server]
Symbol = PUBLIC
<-- omission -->
[Log]
Symbol = WWW
<-- omission -->
[Log]
Symbol = Response
Name = ResponseLog
Path = "/var/opt/FJSVssqc/extend-log/log*"
Format = SQC-Extend
Region = +0900
```

Specify the following as the SQC extended log storage destination to be specified for Path.

[Windows]

```
Path = "variable file directory\extend-log\log*"
```

[UNIX]

```
Path = "/var/opt/FJSVssqc/extend-log/log*"
```

Specify "SQC-Extend" as the format.
Region uses a time difference from GMT (Greenwich Mean Time) to specify the region for the time.

9.1.6.6 Analysis using the usage analysis window

To analyze from the standpoint of response,specify the following in the usage analysis window.

Item	Contents specified
Analysis target server	Specify the server or group to be analyzed.
Analyzed data type	Response report
Analysis method	Specify one of the following: <ul style="list-style-type: none"> - URL base - Client host name base - Client IP address base
Analysis period	Specify the analysis target period and its unit.

9.1.6.7 Analyzing response using the management server

By combining the management server on which Manager is installed and the managed server on which Agent for Business is installed, you can analyze response reports on the managed server by using the management server.

The following explains how to analyze response reports on the managed server by using the management server.

Settings for the management server

Make the following settings on the management server:

1. Use "[7.2.2.1 Registering a usage service](#)" for the managed server setting in the environment settings to set the management location for the use trend DB in "Management Server."
2. Define the managed server in the analysis target server definition block in the use trend DB environment definition file.

Specify the following in the analysis target server definition block.

Item	Setting contents
Symbol	Specify the same symbol as that of the use trend DB environment definition file of the managed server.
Name	Specify the server name that is defined in the managed server setting window for environment settings.
DatabaseMode	db To register in the use trend database the log information that is transferred from the managed server and analyze it, specify that database.

Specify the following in the analysis target log definition block.

[Windows]

Item	Setting contents
Path	"<Variable file directory>\database\csv\<server directory>\e*.csv"
Format	SQC-ExtCSV Specify the CSV format extended log file as the recording format of the analysis target log file.

Item	Setting contents
Region	+0000 Specify no time difference as the region definition for the time data that is stored in the analysis target log file.

[UNIX]

Item	Setting contents
Path	"<Variable file directory>/database/csv/<server directory>/e*.csv"
Format	SQC-ExtCSV Specify the CSV format extended log file as the recording format of the analysis target log file.
Region	+0000 Specify no time difference as the region definition for the time data that is stored in the analysis target log file.

*1 The server directory is created with the name that is specified for Symbol in the analysis target server definition block in the use trend DB environment definition file.

The following shows a definition example.

[Windows]

<pre>[Server] Symbol = PUBLIC <-- omission --> DatabaseMode = db [Log] Symbol = WWW <-- omission --> [Log] Symbol = Response Name = ResponseLog Path = "C:\SystemwalkerSQC\database\csv\PUBLIC\e*.csv" Format = SQC-ExtCSV Region = +0000</pre>

[UNIX]

<pre>[Server] Symbol = PUBLIC <-- omission --> DatabaseMode = db [Log]</pre>
--

```
Symbol = WWW
<-- omission -->
[Log]
Symbol = Response
Name = ResponseLog
Path = "/var/opt/FJSVssqc/database/csv/PUBLIC/e*.csv"
Format = SQC-ExtCSV
Region = +0000
```

By making the setting above, Web server log information is transferred from the managed server to the management server and stored in the use trend DB of the management server.

Settings for the managed server

Make the following setting on the managed server.

1. Specify the operation that uses the CSV format log file as a use trend DB operation type in the analysis target server definition block in the use trend dB environment definition file.

```
DatabaseMode = csv
```

The following shows a definition example.

[Windows]

```
[Server]
Symbol = PUBLIC
<-- omission -->
DatabaseMode = csv
[Log]
Symbol = WWW
<-- omission -->
[Log]
Symbol = Response
Name = ResponseLog
Path = "C:\SystemwalkerSQC\extend-log\log*"
Format = SQC-Extend
Region = +0900
```

[UNIX]

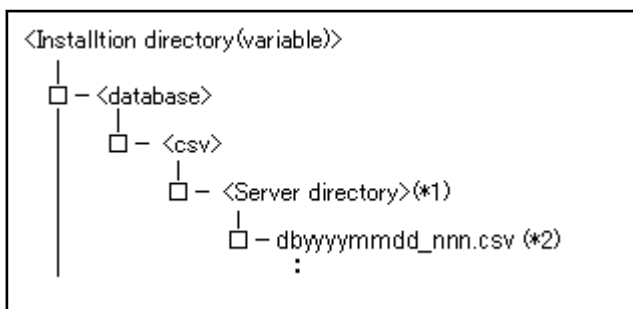
```
[Server]
Symbol = PUBLIC
```

```

<-- omission -->
DatabaseMode = csv
[Log]
Symbol = WWW
<-- omission -->
[Log]
Symbol = Response
Name = ResponseLog
Path = "/var/opt/FJSVssqc/extend-log/log*"
Format = SQC-Extend
Region = +0900

```

2. The use trend DB registration engine outputs the CSV format extended log file to the following directory.



* <> indicates a directory.

(*1) The server directory is created with the name that is specified for Symbol in the analysis target definition block in the use trend DB environment definition file.

(*2) The name variable (yyyyymmdd_nnn) for the CSV format extended log file is given below. The year, month, and date are when the use trend DB is switched (created).

yyyy	Year (1980 or later)
mm	Month (01 to 12)
dd	Date (01 to 31)
nnn	Serial No. (001 to 999)

When the setting above is made, a CSV format extended log file is created as a use trend DB for response report on the managed server, and log information is transferred between the managed server and the management server.

Analyzing the managed server

Trend Viewer of the management server is used to analyze the managed server log on the management server.

9.1.7 If you would like to analyze user types

This section explains how to make analysis focused on the types of users who access the Web sites.

Analysis focused on users enables the following information to be recognized and utilized for Web site operation.

- Which users often access membership sites?
- Which companies often access Web sites?

9.1.7.1 Specifying users

Systemwalker Service Quality Coordinator identifies users as follows:

- Identifying users by user name authenticated on the Web server

If authentication is performed on the Web server, authorization user names can be used as a key for analysis.

- Identifying users by IDs set in a cookie

If authentication is performed on the Web server using CGI, no information about authorized users is output to the Web server log. You can perform analysis that identifies users by setting user names authenticated by CGI in a cookie.

If authentication is not performed by CGI, you can perform analysis that identifies users by setting for Cookie an identifier that identifies the user on each page of the Web service.

- Identifying users by client host

When the Web server performs no authentication, such as that by the service that publishes information, and no information is set in a cookie, then users can be identified by the client host.

For the identification of users by client host, the IP address and host name of the client is used.



Note

For analysis to identify users, content must be created such that authentication is performed or a cookie is set reliably when the Web service to be analyzed is used. If a page in the Web service is accessed directly without authentication or Cookie settings, then analysis that identifies users cannot be done.

Analysis that identifies users with an ID set in a cookie cannot be done if the user blocks cookies with a browser setting. In such a case, analysis that identifies users by client host can be used.

Note that in analysis in which users are identified by client host, different users are handled as the same client host in the following cases:

- IP addresses are allocated dynamically by DHCP (for example, ISP is used to connect).
- Access is via a proxy server (for example, corporate users connecting from behind a firewall).

9.1.7.2 Environment settings

The following environment settings are required to analyze what kind of users visits the Web sites:

- Setting a Web server log output
- Setting a usage DB environment definition file

9.1.7.2.1 Setting a Web server log output

To analyze what kind of users visited to the Web server, the Web server must be set so that information about the users is output to the Web server log.

- Identifying users by user name authenticated on the Web server

Information about the user names that are authenticated by the Web server is output to the Web server log.

If the information is not output, set the Web server so that it is output to the Web server log.

- Identifying users by IDs set in a cookie

If authentication is performed on the Web server using CGI, and user names authenticated by CGI are set in a cookie, set the Web server so that the cookie information is output to the Web server log.

The following gives a setting example for the Web server.

[Windows]

- Microsoft(R) Internet Information Services 6.0

1. Chose from the [Start] menu as shown below to start Internet Service Manager.

[Start]

-> [Programs]

-> [Management tool]

-> [Internet Service Manager]



.....
If the environment is not as shown above, perform operation appropriately for the environment.
.....

2. Set extended log properties.

Point the mouse to the Web site for which extended log properties are to be set, then display the extended log property setting window.

Check the following and press the [Complete] button.

Cookie (cs(Cookie))

3. Save the Web server log.

If the information to be output to the log is changed in the extended log property setting window, the log output format is changed.



.....
Because the new log output format is defined for Systemwalker Service Quality Coordinator, it differs from the prechange log output format, causing an analysis error. Therefore, save and delete the prechange log.
.....

- Apache

[Windows]

1. Chose from the [Start] menu as shown below and open the configuration file.

[Start]

-> [Programs]

-> [Apache Web Server]

-> [Management]

-> [Edit Configuration]

Note

If the environment is not as shown above, perform operation appropriately for the environment.

2. Set the log output format.

Add the lines shown below to the log-related definition part.

The following gives an example when cookie information output definitions are added to the common format, a default log format.

```
#CustomLog logs/access.log common * Define this line as a comment.
```

```
CustomLog logs/access.log "%h %l %u %t \"%r\" %>s %b % {cookie}i"
```

See

Refer to the Apache manual for details.

3. Reflect the settings.

Save by overwriting and quit the editor. If the Apache HTTP server is active, shut down and reboot it.

[UNIX]

1. Use the editor to open the configuration file.
2. Set the log output format.

Add the lines shown below to the log-related definition part.

The following gives an example when cookie information output definitions are added to the common format, a default log format.

```
#CustomLog logs/access_log common * Define this line as a comment.
```

```
CustomLog logs/access_log "%h %l %u %t \"%r\" %>s %b % {cookie}i"
```

See

Refer to the Apache manual for details.

3. Reflect the settings.

Save by overwriting and quit the editor. If the Apache HTTP server is active, shut down and reboot it.

- Identifying users by client host

Normally, information about the client hosts is output to the Web server log.

If the information is not output, set the Web server so that it is output to the Web server log.

9.1.7.2.2 Setting a usage DB environment definition file

Set "Format" that is defined in the analysis target log definition block in the use trend DB environment definition file, based on the user identification method.

- Identifying users by user name authenticated on the Web server

Specify tokens (c-user) for Format, based on the Web server log output format.

- Identifying users by IDs set in a cookie

Specify tokens (c-cookie) for Format, based on the Web server log output format. When the tokens (c-cookie) are specified, define the cookie format according to the contents that are output as cookie information.

The following gives a definition example.

Output format of Web server log cookie information

"ID001;20020401" (ID001: user name)

```
[Server]
Symbol = PUBLIC
<-- omission -->
[Log]
Symbol = WWW
<-- omission -->
Format = "s-time{yyyy-mm-dd HH:MM:SS} c-host s-method s-url s-status s-bytes \"c-
cookie{id;*}\""
<-- omission -->
```

- Identifying users by client host

Specify tokens (c-host) for Format, based on the Web server log output format.

9.1.7.3 Analysis using the usage analysis window

Specify analysis methods in use trend analysis window, based on the user identification method.

- Identifying users by user name authenticated on the Web server

Specify "Authenticated user name base" as an analysis method in the use trend analysis window.

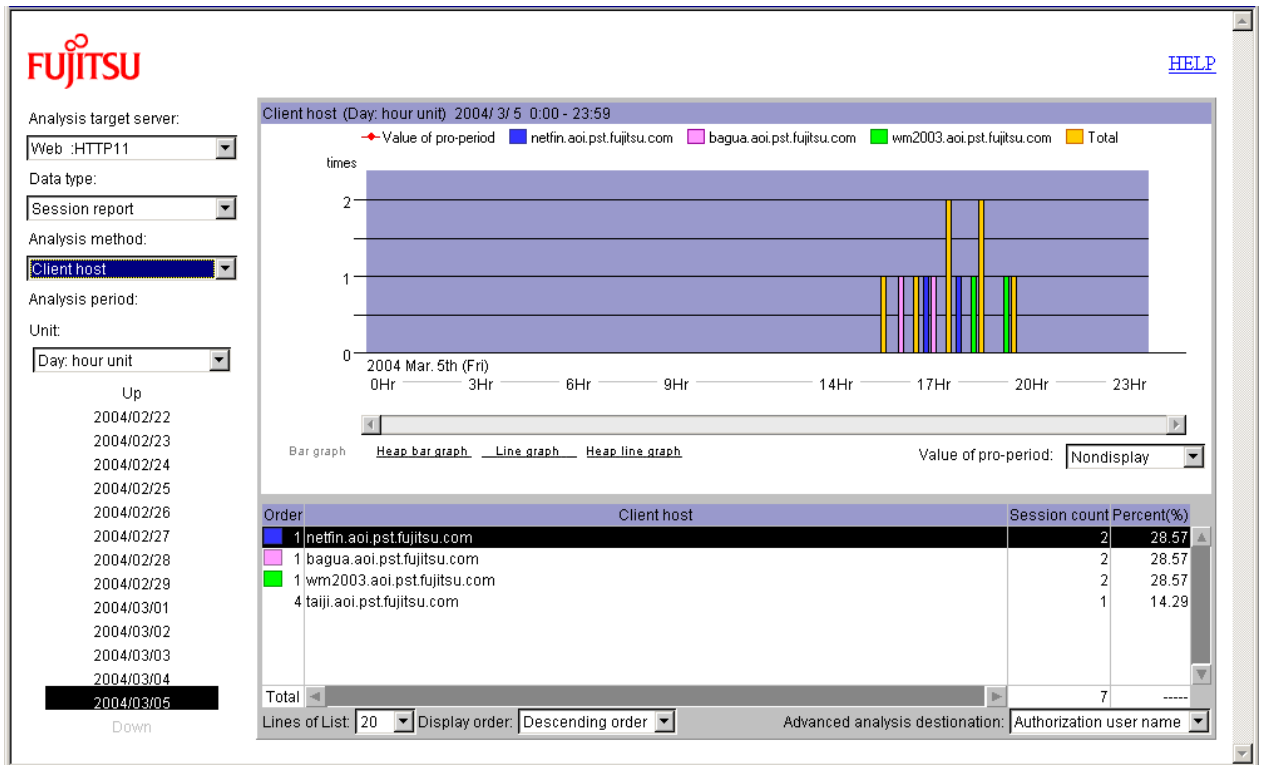
- Identifying users by IDs set in a cookie

Specify "Access ID base" as an analysis method in the use trend analysis window.

- Identifying users by client host

Specify "Client host name base" or "Client IP address base" as an analysis method in the use trend analysis window.

The following shows the window for analysis with users identified by client host.



9.1.8 If you would like to make analysis in subnetwork units

This section explains how to analyze the usage trend in a subnetwork unit (or a section unit). For example, which content is accessed by persons in which section, where the network is divided by section at the in-house Web site.

You can grasp the following information by analysis from the standpoint of the usage trend in the unit of subnetwork and utilize it for Web site operation.

- Which content is accessed by persons in which section?
- Analysis of accesses from two categories: one from in-house and the other from outside the company

9.1.8.1 Environment settings

The following environment setting is required to make analysis in subnetwork units.

- Setting for option definition file

9.1.8.1.1 Setting an option definition file

Each subnetwork to be analyzed is defined in the subnetwork-unit analysis definition block in the option definition file.



See

For information about the storage location of the Option Definition File refer to "15.2.3.1 File storage location".

The following gives an example where subnetworks are defined as listed below for analysis.

Subnetwork range	Subnetwork name
192.168.0.1 to 192.168.0.255	General affairs department
192.168.1.1 to 192.168.1.127	Sales department I
192.168.1.128 to 192.168.1.255	Sales department II
192.168.2.1 to 192.168.2.255	Manufacturing department
192.168.5.1 to 192.168.5.255	

In the above case, the definition of the subnetwork-unit analysis definition block in the option definition file is as follows:

```
[SubnetName]
192.168.0.1-192.168.0.255=General_affairs_department
192.168.1.1-192.168.1.127=Sales_department_I
192.168.1.128-192.168.1.255=Sales_department_II
192.168.2.1-192.168.2.255=Manufacturing_department
192.168.5.1-192.168.5.255=Manufacturing_department
```

 See

.....
 For the details about the setting, refer to "[15.2.3.3 File internal format \(analysis definition block for each subnetwork\)](#)".

9.1.8.2 Analysis using the usage analysis window

Open the use analysis screen as follows:

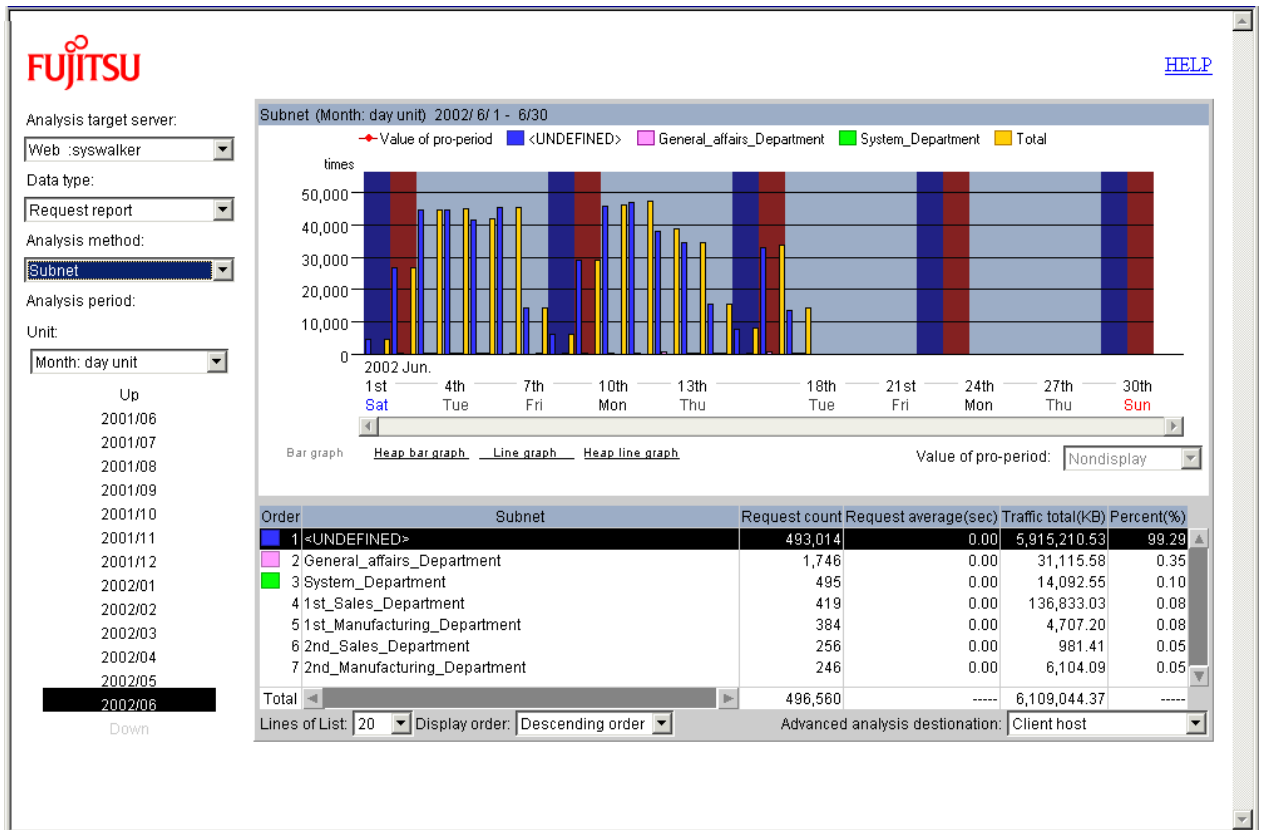
Click the [Trend Viewer] button on the [Web Site Management] window.

->Select the agent to be analyzed on the [Trend Viewer-Agent selection] window then click the [OK] button.

In the [use analysis] screen, analysis target server, analysis data type and analysis method can be selected. Here, select the "Subnet" as the analysis method.

The subnet definition block of the Option Definition File is effective in the [use analysis] screen as soon as it is defined.

The following shows the window for analysis on the subnetwork base.



Point

The information in the subnetwork-unit analysis definition block that is defined in the option definition file becomes valid from postdefinition analysis. This information enables subnetwork-unit analysis, including the information that has already been registered in the use trend DB.

9.1.9 If you would like to make analysis with specific subnetworks excluded

The use trend of the Web site for outside the company may be analyzed. In this case, however, because access from in-house for maintenance is also recorded in the Web server log, you would like to exclude such accesses to analyze the usage trend from the standpoint of general users.

This section explains how to analyze with specific internal subnetworks (IP address groups) excluded.

By analysis excluding accesses from the specific subnetworks, you can grasp the following information and utilize it for the Web site operation.

- How many times do general users access?
- Which content do general users often visit to?

9.1.9.1 Environment settings

The following environment setting is required to make analysis excluding specific subnetworks.

- Setting for option definition file

9.1.9.1.1 Setting an option definition file

Define the subnetworks that you want to exclude from the analysis targets in the specific subnetwork analysis exclusion definition block in the option definition file.



For information about the storage location of the Option Definition File refer to "[15.2.3.1 File storage location](#)".

The following gives an example of analysis excluding the following subnetworks.

Exclusion target subnetwork range
192.168.0.1 to 192.168.0.255
192.168.2.1 to 192.168.2.255

In the above case, the definition of the specific subnetwork analysis exclusion definition block in the option definition file is as follows:

```
[SubnetExcepted]
192.168.0.1-192.168.0.255
192.168.2.1-192.168.2.255
```



The contents that are specified in the specific subnetwork analysis exclusion definition block in the option definition file become valid when the use trend DB registration engine is started next.

Out of these contents, the information that has already been registered in the use trend DB does not become valid.



For details about the settings, refer to "[15.2.3.4 File internal format \(definition block with analysis of a specific subnetwork omitted\)](#)".

9.1.9.2 Analysis using the usage analysis window

The specification in the specific-subnetwork analysis exclusion definition block is processed by the usage DB register engine. So the analysis result before the definition is made remains the same as this function is not used.

Analysis using the use trend analysis window excludes access from the subnetworks that are specified in the specific subnetwork analysis exclusion definition block in the option definition file.



Out of the contents that are specified in the specific subnetwork analysis exclusion definition block in the option definition file, the information that has already been registered in the use trend DB does not become valid.

Therefore, if a period that extends to before the definition setting is selected, access from the subnetworks that are specified in the specific subnetwork analysis exclusion definition block is included for analysis.

9.1.10 If you would like to make analysis with specific URLs excluded

The use trend of a Web site may be analyzed. In this case, however, because access to the URL (content) for maintenance is also recorded in the Web server log, you would possibly like to exclude such access to analyze the use trend paying attention to the content for general users.

This section explains how to make analysis, excluding access to a specific URL.

Analysis excluding access to a specific URL enables the following information to be recognized and utilized for Web site operation.

- How much access to the content for general users, excluding access to the URL for maintenance is made?

9.1.10.1 Environment settings

The following environment setting is required to make analysis excluding access to a specific URL.

- Setting for option definition file

9.1.10.1.1 Setting an option definition file

Define the URL that you want to exclude from the specific URL analysis exclusion definition block in the option definition file.



See

For information about the storage location of the Option Definition File refer to "15.2.3.1 File storage location".

The following explains how to make analysis excluding access to the URL that Systemwalker Service Quality Coordinator uses on the managed server for processing.

URL to be excluded
/SQC/cgi-bin/dbtrans.cgi
/SQC/cgi-bin/wmAgtMibGet.cgi
/SQC/cgi-bin/wslmget.cgi

In the above case, the definition of the specific URL analysis exclusion definition block in the option definition file is as follows:

[URLExcepted]
/SQC/cgi-bin/dbtrans.cgi
/SQC/cgi-bin/wmAgtMibGet.cgi
/SQC/cgi-bin/wslmget.cgi

Note

The contents that are specified in the specific URL analysis exclusion definition block in the option definition file become valid when the use trend DB registration engine is started next.

Out of these contents, the information that has already been registered in the use trend DB does not become valid.

See

For details about the setting, refer to "15.2.3.5 File internal format (definition block with analysis of a specific URL omitted)".

9.1.10.2 Analysis using the usage analysis window

The contents that are specified in the specific URL analysis exclusion definition block in the option definition file are processed when the use trend DB registration engine is running. Therefore, analysis using the use trend analysis window becomes useless.

Analysis using the use trend analysis window excludes access to the URL that is specified in the specific URL analysis exclusion definition block in the option definition file.

Note

Out of the contents that are specified in the specific URL analysis exclusion definition block in the option definition file, the information that has already been registered in the use trend DB does not become valid.

Therefore, if a period that extends to before the definition setting is selected, access to the specific URL that is specified in the specific URL analysis exclusion definition block is included for analysis.

9.2 Notes

This section includes notes to assist you when using the analysis window.

9.2.1 Date and time

In the analysis window, the current date and time are determined based on the client machine date and time (including the year, month, and day).

For example, in the initial window immediately after starting the analysis window, the "Summary" window of the week: day unit including the current year, month, and day is displayed. "Current" in this case means the current date and time on the client machine.

9.2.2 Operation when moving to other URL

If the Web browser used to operate the analysis window is moved to another Web page (URL), the analysis window terminates.

If the Web browser returns to the analysis window Web page as a result of using Back or Next on the Web browser, the analysis window is restarted. In this case, settings and the standard mode in the Setup page do not store the former states, just as in the case where the analysis window is terminated and then restarted (Default values are set).

9.2.3 Extension name display

The display of the extension name depends on the final qualifier in the URL name. The following table lists the details:

Final qualifier of URL	Displayed extension name
If the URL name is a.html	html
If the URL name is a.gif	gif
If the URL name is a.GIF	GIF
If the URL name has no extension	<FILE>
If the URL name is a directory name	<DIRECTORY>
If the URL name is a domain name of the server	<HOMEDIRECTORY>
If the pathname cannot be obtained	<NOTHING>

9.2.4 Host name/IP address display when DNS conversion is not possible

If "SearchDNS=yes" is specified in the Usage DB Environment Definition File, host information (host name or IP address) for the client stored in the analysis target log is DNS-converted. If, however, the conversion fails for some reason, the display is as listed below:

Host information of the client stored in logs	DNS conversion	Displayed host name	Displayed IP address
IP address	Success	Host name	IP address
	Failure	IP address	IP address
Host name	Success	Host name	IP address
	Failure	Host name	Host name

9.2.5 Handling of the URL name to be analyzed

The URL name of the log file to be analyzed is analyzed faithfully. That is, uppercase and lowercase characters of the string contained in the URL name are distinguished and handled as different URL names.

9.2.6 Notes on selecting the URL based breakdown from the analysis method box

If you select the URL based breakdown from the analysis method box, only the URL names corresponding to the extensions specified in "RequestURLSuffix" of the Usage DB Environment Definition File are displayed.

9.2.7 Notes on selecting the URL extension based breakdown from the analysis method box

If you select the URL extension based breakdown from the analysis method box to execute advanced analysis based on URL, and the extension for advanced analysis is not specified in "RequestURLSuffix" of the Usage DB Environment Definition File, the extension excluded from analysis and "No data in this period" is displayed.

9.2.8 Notes on displaying analysis results of mass log data

If you select the year unit from the period unit box and display analysis results of mass log data, it may take some time before the analysis window is displayed.

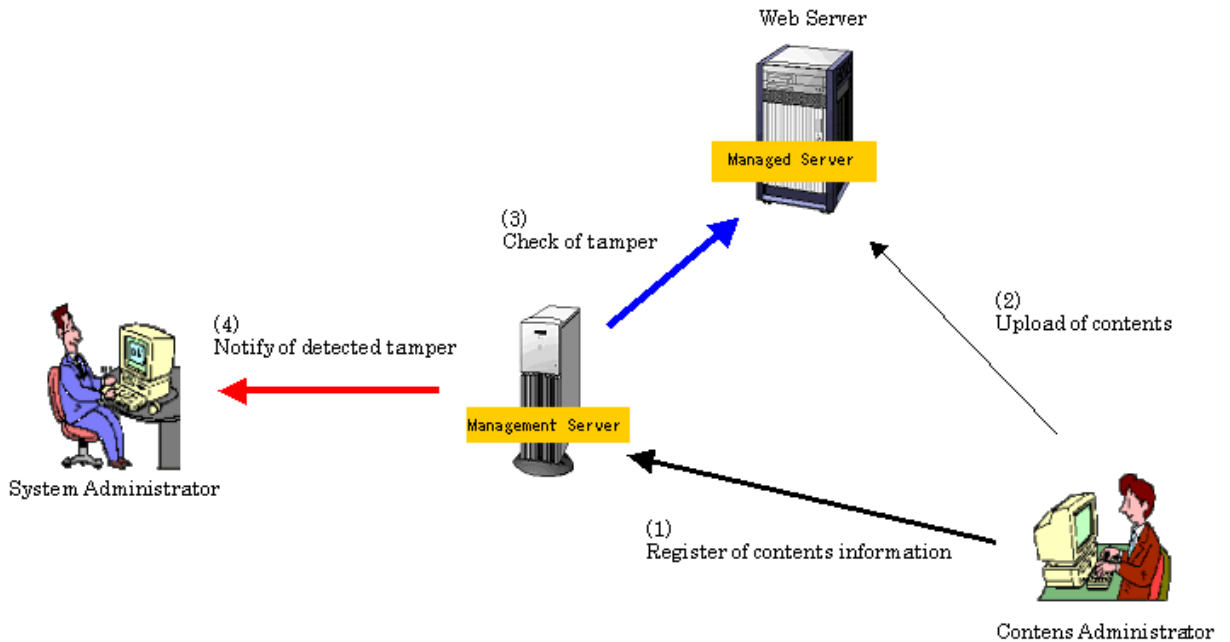
Chapter 10 Monitoring for Tampering with Web Contents

The system administrator can use the Contents Tampering Monitor to automatically monitor tampering with Web Contents (hereafter simply referred to as contents) and receive messages if tampering is detected.

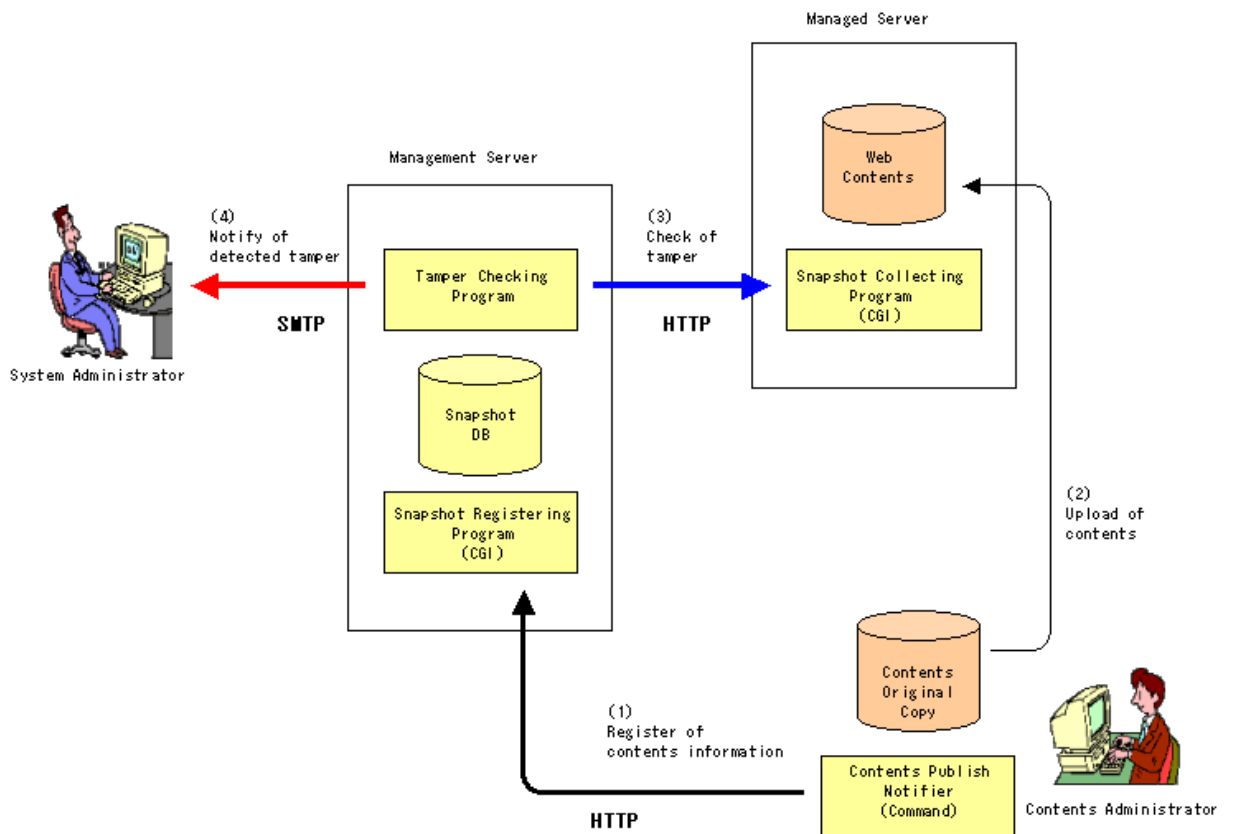
This chapter explains how to use the Contents Tampering Monitor.

10.1 Overview of Monitoring

The figure below shows an overview of tamper monitoring. The Contents Administrator registers content information for the Management Server ((1) in the figure) and then uploads the contents to the Web Server ((2) in the figure). The Contents Tampering Monitor, based on the registered content information, checks the contents on the Managed Server ((3) in the figure) and, if tampering is detected, notifies the System Administrator of the event through e-mail ((4) in the figure).



The figure below shows the internal operations of the Management Server, Managed Server and Contents Administrator's machine. The yellowish portions in the figure show the components of the Contents Tampering Monitor. The operation at (1) in the figure, which is caused when the Contents Administrator executes the Contents Publish Notifier, stores Contents Original Snapshot in the Snapshot DB. The operation at (3) in the figure, which is caused by periodical activation scheduled on the Management Server, compares the Web Contents (snapshot) and Contents Original Copy (snapshot in the Snapshot DB) for inspection. The operation at (4) in the figure is caused when tampering is detected in the operation at (3).



Note

The Snapshot Collecting Program (CGI) is a component installed together with Agent for Business. For this reason, Agent for Business must be installed on the Managed Server to be monitored.

Snapshots are generated based on the binary of the content, so if, for example, code conversion is performed using the operation in step 2 above, a discrepancy will arise between the registered binary for the content original and the binary for the public content, and tampering will be detected.

In order for tamper monitoring to operate correctly, take care during the operation in step 2 of the figure above to ensure that no discrepancy arises between the registered binary for the content original and the binary for the public content.

Point

"17.1.3 Tampering inspection program" are record and sent as follows:

- The operating status is recorded in the Contents Tampering Monitor. The record can be referenced through the "13.1.6 Action Statement window"
- Tamper detection is recorded in the [Send Log Path](#)
- A tamper detection message is recorded in the system log (event log under the Windows version or syslog under the Solaris version).
- A tamper detection message is sent to the [Alert E-mail Address](#) and [CC](#)

Point

- The Contents Tampering Monitor has a function that can correctly distinguish negligence from tampering even if the Contents Administrator forgets to perform the operation at (2) in the figure after the operation at (1). However, the function cannot distinguish operations correctly if they are performed in reverse order (operation (1) after operation (2)). Also, the function cannot distinguish correctly if operation negligence continues.
- The load on the Web Server is only snapshot collection for contents (minimum load).
- Because of a configuration for remote monitoring from the Management Server, even multiple Web Servers can be monitored in a batch.

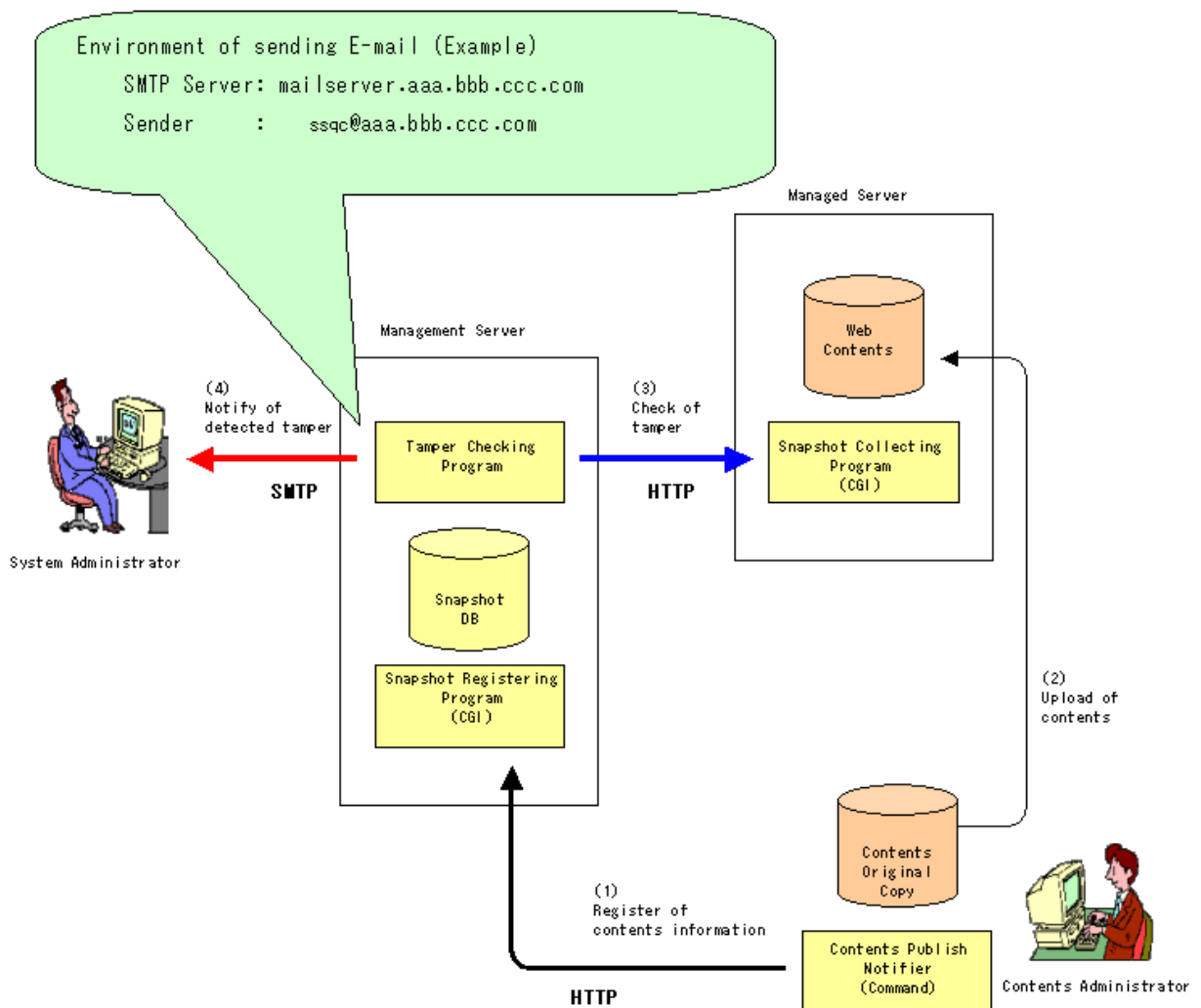
The following sections explain the tamper monitoring procedures based on the figure right above.

10.2 Environment Settings

Set up the environment as follows:

1. Set up the environment for sending tamper detection alert (e-mail).

This section explains how to set up the environment shown below as an example.



- 10.2.1 Setting the send environment for tampering detection reports

10.2.1 Setting the send environment for tampering detection reports

Open the Environment Properties window as follows:

[13.1 Viewing the Environment Settings Window](#) -> [13.1.1 Contents Tampering Monitor window \(menu window\)](#) -> [13.1.5 Environment Properties window](#)

To implement the case of the previous example, set data as shown below and click the [OK] button



Systemwalker Service Quality Coordinator Environment Properties - Microsoft Internet Ex...

FUJITSU

**Systemwalker
Service Quality Coordinator**
Environment Properties

SMTP server

Host Name

Sender E-mail Address

OK Reset Cancel

 See

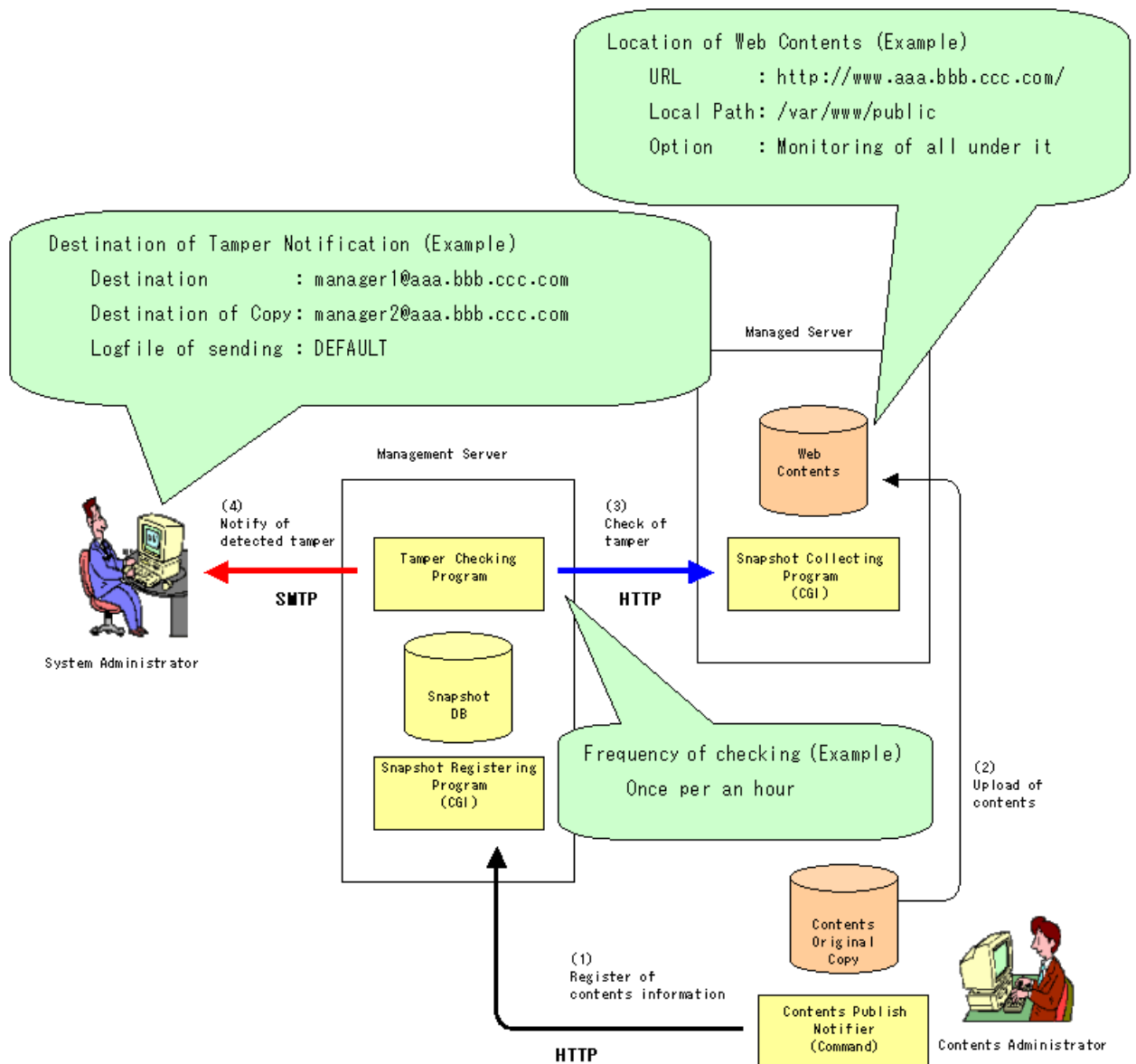
For details of the window, refer to "[13.1.5 Environment Properties window](#)."

10.3 Registering Monitoring Requirements

Register monitoring requirements as follows:

1. Specify the content publish location.
2. Specify the tamper checking frequency.
3. Specify the tamper detection notification destination.

This section explains how to register monitoring requirements for the following, as an example.



P Point

If there are two or more Contents Administrators, the monitoring requirements should be registered for each Contents Administrator. This enables each tamper detection alert to be sent to the right administrator.

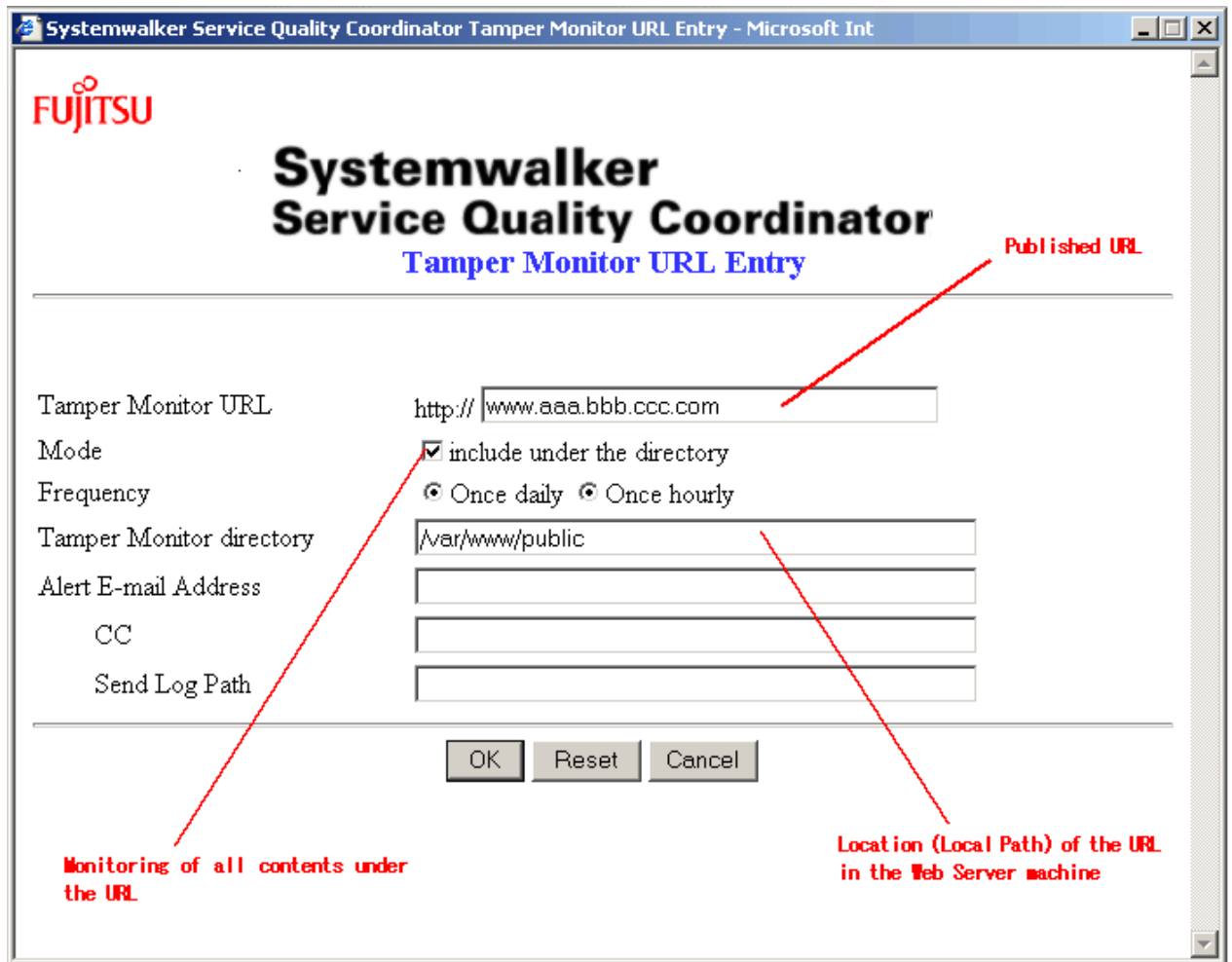
If monitoring requirements are registered by the level of importance of contents, the tamper checking frequency can be varied with the level of importance.

10.3.1 Specifying a content publish location

Open the Tamper Monitor URL Entry window as follows:

13.1 Viewing the Environment Settings Window -> 13.1.1 Contents Tampering Monitor window (menu window) -> 13.1.2 Tamper Monitor URL Entry window

To meet the previous example, set data as shown below:



See

Please refer to "13.1.2 Tamper Monitor URL Entry window" about the details of a screen.

Note

The behavior in step 3 of the figure in "10.3 Registering Monitoring Requirements" is performed on the managed server information (the URL for the agent) that matches the host information for the URL set up here.

The host information of the URL specified here should be the same as the host information of the agent URL specified in the managed server information.

- If a host name is set in the host component of the agent URL of the managed server, a host name should also be set in the host component of this URL.
- If an IP address is specified in the host component of the agent URL of the managed server, an IP address should also be set in the host component of this URL.

Note also that because only one IP address can be specified for a single managed server, in the case of a name-based virtual site, only one virtual site can be monitored using a single IP address.

Make sure that the host information for the URL set up here matches the host information for the URL of the agent in the managed server information. The part of the managed server information that needs to be checked has been circled in red in the screen shot below.

FUJITSU Systemwalker Service Quality Coordinator Managed Server Information - Microsoft I.

FUJITSU

Systemwalker Service Quality Coordinator

Managed Server Information

- Basic information

Server name

IP address

Subnet mask

Proxy Server

If the proxy server check box is selected, communication between the manager and agent is performed via the proxy server.
Specify the proxy server address and port below; otherwise, the default proxy server defined in the Management Server settings window is used.

Address

Port

- Attributes of Managed Server

Service Quality Coordinator Agent

Server where the Agent is installed.

Agent URL

**Example: "http://HOST[:PORT]/ALIAS/"*

OK Reset Cancel

10.3.2 Specifying an execution frequency for tampering inspection

To implement the case of the previous example, make an additional setting as shown below:

Systemwalker Service Quality Coordinator Tamper Monitor URL Entry - Microsoft Internet Explorer

FUJITSU

**Systemwalker
Service Quality Coordinator**
Tamper Monitor URL Entry

Tamper Monitor URL: http://

Mode: include under the directory

Frequency: Once daily Once hourly

Tamper Monitor directory:

Alert E-mail Address:

CC:

Send Log Path:

OK Reset Cancel

Checking once per an hour

 See

- Normally, it is enough to perform tamper checking once an hour. If needed, however, the tamper checking interval can be shortened. For more information about this, refer to "[13.3.1 If you would like to make tampering inspection with a shorter interval](#)".
- Tamper checking can also be performed at optional points. For more information about this, refer to "[13.3.2 If you would like to make tampering inspection at an optional time](#)".

10.3.3 Specifying a tampering detection reporting destination

To implement the case of the previous example, make additional settings as shown below:

Systemwalker Service Quality Coordinator Tamper Monitor URL Entry - Microsoft Internet Explorer

FUJITSU

Systemwalker Service Quality Coordinator

Tamper Monitor URL Entry

Tamper Monitor URL:

Mode: include under the directory

Frequency: Once daily Once hourly

Tamper Monitor directory:

Alert E-mail Address:

CC:

Send Log Path:

OK Reset Cancel

Destination of Tamper Notification

Destination of its copy

Logfile of sending (If no path is specified, a default path is selected.)

This ends basic settings. Click the [OK] button.

Point

The user can check the following to make sure that the settings are correct (when the data specified for "Tamper Monitor URL" indicates a directory):

1. Prepare dummy content.
2. Register dummy content information by referring to "[10.4.2 Notifying content publish \(contents administrator job\)](#)".
3. Upload the dummy content to the Web Server.
4. Perform tamper checking by referring to "[13.3.2 If you would like to make tampering inspection at an optional time](#)".
5. Delete the dummy content on the Web Server.
6. Perform tamper checking again by referring to "[13.3.2 If you would like to make tampering inspection at an optional time](#)".
7. Open the "[13.1.6 Action Statement window](#)" to check that the deletion of the dummy content was detected. If it was detected, the specification of the content publish location is correct.
8. Check that e-mail reached the tamper detection alert address. If e-mail indicating the deletion of the dummy content reached, the specification of the tamper detection alert notification destination is correct.

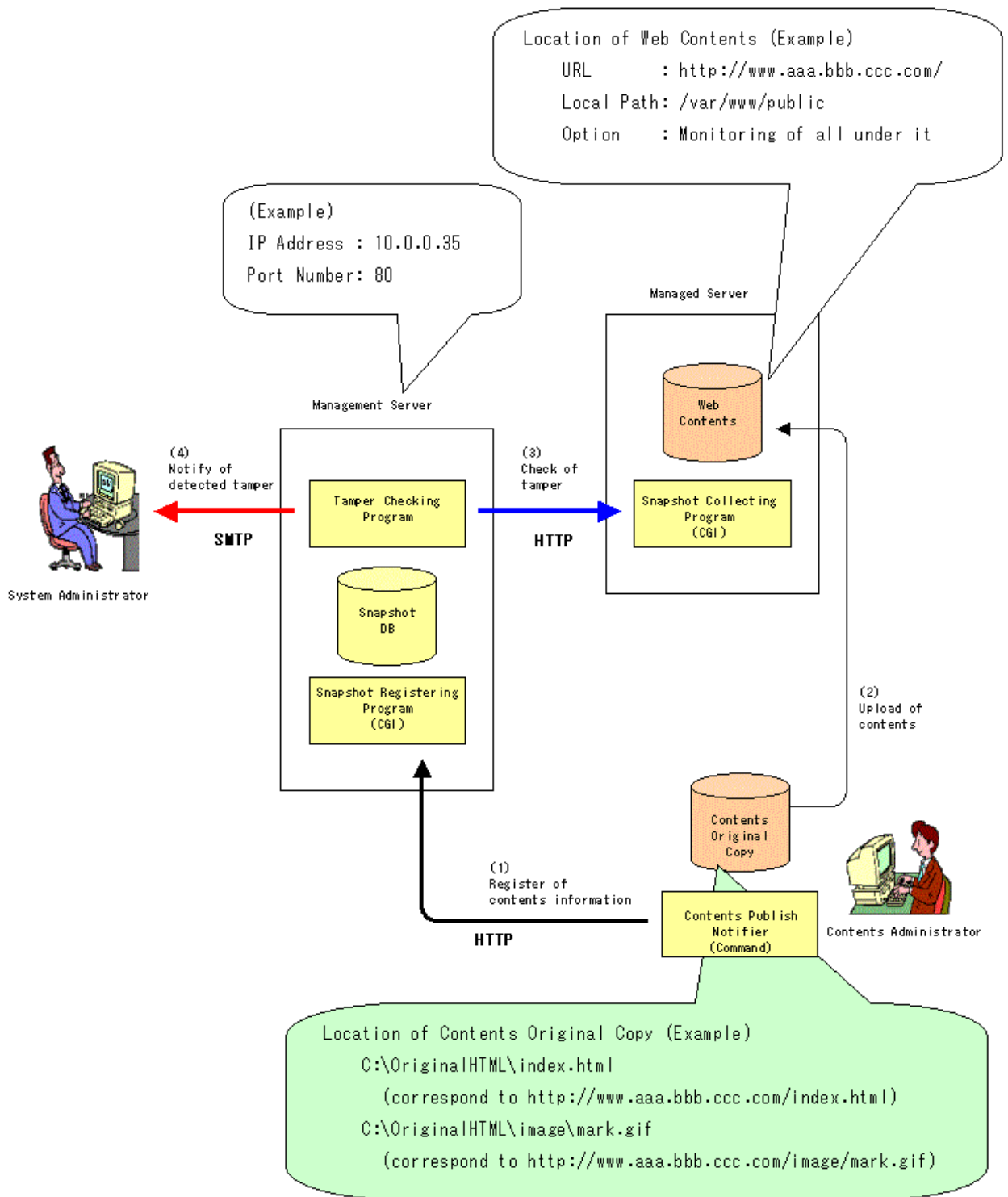
9. Delete the registration of the dummy content information by referring to "[10.4.2 Notifying content publish \(contents administrator job\)](#)".

10.4 Registering Contents

Register contents according to the following procedure:

1. Distribute a Contents Publish Notifier.
2. Notify contents publish (contents administrator job)

This section explains how to make settings for the following case as an example.



P Point

Contents that are possibly tampered are home pages and other frequently accessed pages. Narrowing the tamper checking targets to these contents can minimize the load on the Web Server and enables effective tamper monitoring.

10.4.1 Distributing a content publish notifier

Before the Contents Administrator registers contents information, the System Administrator must distribute a Contents Publish Notifier (MpupdtCntnts command) to the Contents Administrator. For the location of the notifier to be distributed, refer to "[18.1.1.1.1 MpupdtCntnts command location](#)".



For distribution, select the proper component for the platform used by the contents administrator.

10.4.2 Notifying content publish (contents administrator job)

Before registering contents information, the Contents Administrator must receive a Contents Publish Notifier (MpupdtCntnts command) from the System Administrator. The following explanation is based on the following work environment of the Contents Administrator.

- Platform: Windows
- MpupdtCntnts command storage directory: C:\Tool

To implement the case of the previous example, enter the command at the command prompt as shown below. For the MpupdtCntnts command specifications, refer to "[18.1.1.1.2 MpupdtCntnts command specifications](#)".

```
C:\> Tool\MpupdtCntnts -m 10.0.0.35 -p 80 -u http://www.aaa.bbb.ccc.com/index.html -f C:\OriginalHTML\index.html
Update complete
```

```
C:\> Tool\MpupdtCntnts -m 10.0.0.35 -p 80 -u http://www.aaa.bbb.ccc.com/image/mark.gif -f C:\OriginalHTML\image\mark.gif
Update complete
```



In the above example, the MpupdtCntnts command is entered for each piece of content. Contents can be registered in a batch if a content list file is created. For more information, refer to [18.1.1.1.2 MpupdtCntnts command specifications](#).

Part 4 User's Guide

Chapter 11 Analyzing Web Site Usage.....	115
Chapter 12 Evaluating the Usage.....	161
Chapter 13 Using the Contents Tampering Monitor.....	181

Chapter 11 Analyzing Web Site Usage

This chapter explains how to use the Web site's Trend Viewer.

11.1 Usage DB Engine

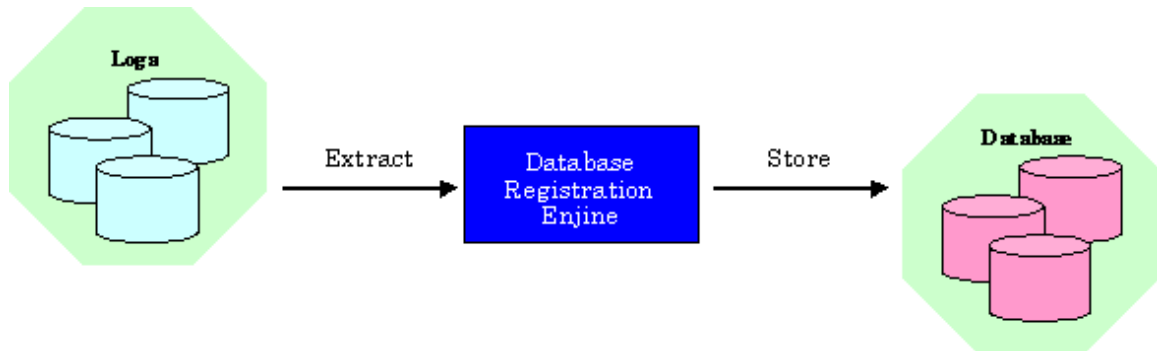
This section gives an outline of each Usage DB engine of Trend Viewer and briefly explains its operations.

11.1.1 Usage DB Registration Engine

11.1.1.1 Outline

The Usage DB Registration Engine registers with the Usage DB the logs related to the Web site and Proxy server running on the system on the installation machine.

The Usage DB Registration Engine references various logs periodically, to fetch differences between the old and new portions of data required for update, and stores them in the Usage DB.



11.1.1.2 Start operation

To carry out an analysis, the log data related to the Web service must be registered with the Usage DB in advance.

To support additions of various logs, a setting must be made such that the Usage DB register engine is started periodically to register additions of logs with the Usage DB one by one.

This setting is not done in the installation. So in order to use the Usage Analysis Function, start operation must be set. The method is explained as follows.

Starting the service

[Windows]

The Usage DB Registration Engine is a service (name: "Systemwalker SQC dbregsv") that is accessed using the Services dialog via Windows' Control Panel on the installation machine. The service is registered during installation, and operates at each starting time set then.

To carry out an analysis, this service must be started in advance in the following manner:

Log in with the account with Administrator authority and "Start" this service (name: "Systemwalker SQC dbregsv") in the Services dialog accessed from Windows' Control Panel.

[UNIX]

The Usage DB Registration Engine is operated at each starting time set during installation with the command (dbregmng command) started by the clock daemon (Solaris:cron/Linux:crond).

Registration with the clock daemon is the following procedure:

1. Login

Log in as a superuser.

2. The crontab file editing and reflection

Use the crontab command to register the startup definition of the Usage DB Registration Engine in the crontab file.

The following is an example of using the crontab command:

```
# crontab -e
```

If the above command is executed, the editor is started so that the crontab file can be edited. For example, add the following startup definition to start at the 15th minute of each hour.

```
# FJSVssqc
15 * * * * /opt/FJSVssqc/bin/dbregmng
```

Save the edited contents and terminate the editor. Changes are automatically reflected in the clock daemon.

11.1.1.3 Stop operation

Perform the following operation to stop the Usage DB Registration Engine.



If the Usage DB Registration Engine is stopped, data can no longer be registered with the Usage DB.

Stopping the service

[Windows]

To stop the Usage DB Registration Engine and to suspend the Web service analysis temporarily, stop the Usage DB Registration Engine in the following manner:

To stop the Usage DB registration service, log in with the account with the Administrator authority and then "Stop" this service (name: "Systemwalker SQC dbregsv") in the Services dialog accessed from Windows' Control Panel.



If the Startup type of the service is "Automatic" the service is automatically "started" when the installation machine is restarted.

If the service should remain stopped after restarting the installation machine, change the service's Startup type to "Manual".

[UNIX]

To stop the Usage DB Registration Engine and to suspend the Web service analysis temporarily, do the following procedure:

1. Login

Log in as a superuser.

2. The crontab file editing and reflection

Use the crontab command to disable (comment out) the startup definition of the Usage DB Registration Engine in the crontab file.

The following is an editing example:


```
# crontab -e
```

If the above command is executed, the editor is started so that the crontab file can be edited. For example, disable the startup definition as shown below:

```
# FJSVssqc  
#15 * * * * /opt/FJSVssqc/bin/dbregmng
```

Save the edited contents and terminate the editor. Changes are automatically reflected in the clock daemon.

11.1.1.4 Start up time

Usage DB register engine's start time is in 15 minutes each hour by default.

Do the following if the start time and the period between start should be changed.

[Windows]

1. Open the definition file by notepad or other text editor. The path is as follows:

```
<installation directory (variable)\control\Config
```

2. Edit the [DatabaseRegisterEngine] section.
For example, once a day, start at 12:00 can be defined as follows:

```
[DatabaseRegisterEngine]  
start = day(12:00)
```

Specify the start time in the "start". The following are the options.

<Option>	<Meaning>
hour(MM)	every hour
day(HH:MM)	every day

The token "MM" and "HH" is the start time, and can be specified with the following value:

<token>	<value>
HH	00-23 integer(hour)
MM	00-59 integer(minute)

3. Save the content and close the editor.
4. Restart the usage DB register engine service.
For the method to restart, refer to "11.1.1.3 Stop operation " and "11.1.1.2 Start operation".

[UNIX]

1. Login

Log in as a superuser.

2. The crontab file editing and reflection

Use the crontab command to register the startup definition of the Usage DB Registration Engine in the crontab file.

The following is an example of using the crontab command:

```
# crontab -e
```

If the above command is executed, the editor is started so that the crontab file can be edited. For example, add the following startup definition to start at once a day and 12:00.

```
# FJSVssqc  
00 12 * * * /opt/FJSVssqc/bin/dbregmng
```

Save the edited contents and terminate the editor. Changes are automatically reflected in the clock daemon.

11.1.1.5 URL extensions valid for analysis

Extensions that are valid for analysis in the Usage DB Registration Engine are those specified in RequestURLSuffix of "15.2.1.4 File internal format (analysis target server definition block)" in the Usage DB Environment Definition File. If nothing is defined, the Usage DB Registration Engine adopts the following default values:

- html
- htm
- shtml
- shtm
- stm
- cgi
- asp
- pl
- tcl
- sh

11.1.1.6 Space estimation in the Usage DB

The usage DB is created inside the server directory together with the information directories and management files.



.....
Server directory is created with the name specified to the Symbol of the analysis target server definition block in the Usage DB Environment Definition File.
.....

The estimation of the space for one server directory is as follows:

about 60% of the analysis target log size

Note

The space of the usage DB varies depending on the following conditions:

- URL length
- The number of contents
- The number of users
- The count of request
- Analysis contents (DNS search, Referer, User agent, etc)

The usage DB space may get 1.5 time larger depending on these conditions. Thus it is recommended that the estimation should be made periodically.

Besides, it is also recommended that the unnecessary (old) usage DB be backed up or removed periodically if the usage analysis function is used continuously.

See

For information about the backup, removal of the usage DB, refer to "[11.1.3 Usage DB backup and restore](#)".

11.1.1.7 Usage DB switching

The Usage DB Registration Engine creates a new Usage DB (dbyyyymmdd_nn, exyyyyymmdd_nn) periodically to back up the Usage DB. This is called "Usage DB switching".

The Usage DB switching is performed in accordance with the settings in the Usage DB Environment Definition File "DatabaseConfig." For details of the settings of the Usage DB Environment Definition File, refer to "[15.2.1 Usage DB Environment Definition File](#)".

11.1.1.8 Notes on use of Usage DB Registration Engine

When stopping the analysis target server

Stop the Usage DB Registration Engine. For information on the stop of the Usage DB Registration Engine, refer to "[11.1.1.3 Stop operation](#)".

When stopping the log collection on the analysis target server

Stop the Usage DB Registration Engine. For information on the stop of the Usage DB Registration Engine, refer to "[11.1.1.3 Stop operation](#)".

When changing the log format on the analysis target server

Since the Usage DB Registration Engine processes logs in accordance with the log format defined in the Usage DB Environment Definition File, processing may not be possible if logs in different formats are mixed.

To change the log format, separate the log files and then set the Usage DB Environment Definition File again.

Character code of the logs

In processing of analysis target log files, the Usage DB Registration Engine assumes that logs are stored with the character code and line feed code conforming to the operating system that is running. Their possible combinations are as follows:

[Windows]

Character code	Line feed code
ASCII	CR + LF

[UNIX]

Character code	Line feed code
ASCII	LF

Note that, if the combination is different from the above, correct processing cannot be performed. Especially, you must take care when handling network files on a remote host.

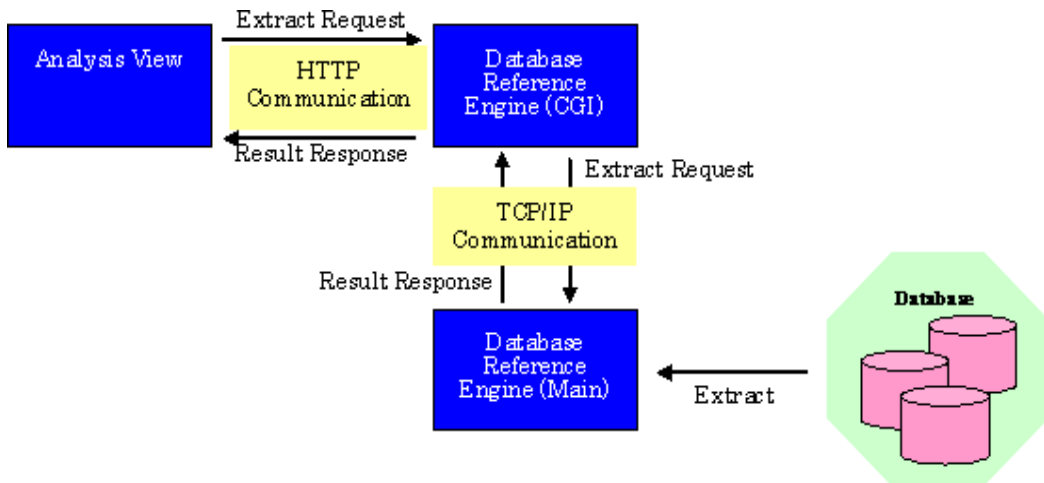
Handling logs that do not contain any line feed code

The Usage DB Registration Engine handles logs that do not contain any line feed as incomplete logs and excludes them from processing.

11.1.2 Usage DB Reference Engine

11.1.2.1 Outline

The Usage DB Reference Engine is positioned between the Analysis window and Usage DB, and provides an interface (using the HTTP communication via a Web server application) to extract data from the Usage DB for the Analysis window.



11.1.2.2 Start operation

To carry out an analysis on the Analysis window, a setting must be made such that the Usage DB Reference Engine is started in advance.

 Point

.....
In case of management server operation, do the start operation only on the management server. It is not necessary to do this setting on the managed server.
.....

Starting the service

[Windows]

The Usage DB Reference Engine, a service (name: "Systemwalker SQC dbrefsv") that can be operated in the Services dialog accessed via Windows' Control Panel on the installation machine, operates for each request to the Usage DB reference port. This service is registered during installation.

To carry out an analysis, this service must be started in advance in the following manner:

Log in with account with the Administrator authority and "Start" this service (name: "Systemwalker SQC dbrefsv") in the Services dialog accessed via Windows' Control Panel.

[Solaris]

The Usage DB Reference Engine is operated for each request to the Usage DB reference port set during installation with the command (dbref command) started by the Internet service daemon (inetd).

Register the Internet service daemon on the following server.

Operation method	Object server
Management server operation	Manager
Managed server operation	Agent

Point

Register the Internet service daemon on the server where the use trend database has been registered.

- Use a management server operation if the security of the agent is to be taken into account.
- For management server operations, it is unnecessary to register to the Internet service daemon on the agent.
- If the management server itself is a public server, or if managed server operations are being used, the dbref command can be registered with the Internet service daemon, but this involves a significant security risk.

Take additional measures (such as TCP wrappers) to ensure that security is maintained.

Make settings (with TCP Wrapper, etc) that dbref command can only be accessed from the local server

Use the following procedure to register the dbref command with the Internet service daemon, as it is not registered when SQC-A is installed.

Note

This procedure does not include settings for performing access control.

Access control setup methods are different depending on the application used to control access. Refer to the manual for the application being used.

1. Login
Log in as a superuser.
2. /etc/services or /etc/inet/services file editing

Use an editor to register the Usage DB registration port definition in the /etc/services or /etc/inet/services file. For example, in the case of 2365, add the following definition:

```
# FJSVssqc
dbref 2365/tcp
```

Refer to "[11.1.2.3 Usage DB reference port number](#)" for details on the port number for looking up the usage database.

3. /etc/inetd.conf or /etc/inet/inetd.conf file editing

Use an editor to edit the /etc/inetd.conf or /etc/inet/inetd.conf file.

If the network environment is the Internet, add the following definition:

```
# FJSVssqc
dbref stream tcp nowait nobody /opt/FJSVssqc/bin/dbref dbref -a
```

If the network environment is an Intranet, add the following definition:

```
# FJSVssqc
dbref stream tcp nowait nobody /opt/FJSVssqc/bin/dbref dbref
```

4. Reflection of changes

- At before Solaris 9 OS

The change is reflected in inetd by searching for process ID of inetd by using the ps command and the grep command, and using the kill command afterwards. The operation example is as follows.

```
# ps -A | grep inetd
process ID ...
# kill -HUP process ID
```

- When OS is Solaris 10 or later

The change is reflected by using the inetconv command. The operation example is as follows.

```
# inetconv
```

[Linux]

The Usage DB Reference Engine is operated for each request to the Usage DB reference port set during installation with the command (xinetd or dbref command) started by the Internet service daemon (inetd).

Registration with the Internet service daemon is carried out during installation. If, however, this engine has not been installed for some reason, register it by the following procedure:

- For xinetd

1. Login

Log in as a superuser.

2. /etc/services file editing

Use an editor to register the Usage DB registration port definition in the /etc/services file. For example, in the case of 2365, add the following definition:

```
# FJSVssqc
dbref 2365/tcp
```



See

Refer to "[11.1.2.3 Usage DB reference port number](#)" for details on the port number for looking up the usage database.

3. /etc/xinetd.d/dbref file creating

Use an editor to create a dbref file under /etc/xinetd.d.

If the network environment is the Internet, the contents of the dbref file are as follows. Set the IP address of the local host to xxx.xxx.xxx.xxx.

```
# FJSVssqc
service dbref
{
socket_type = stream
wait = no
user = nobody
server = /opt/FJSVssqc/bin/dbref
only_from = xxx.xxx.xxx.xxx 127.0.0.1
}
```

If the network environment is an Intranet, the contents of the dbref file are as follows.

```
# FJSVssqc
service dbref
{
socket_type = stream
wait = no
user = nobody
server = /opt/FJSVssqc/bin/dbref
}
```

4. Reflection of changes

Use the kill command so that changes are reflected in xinetd. The following is an operation example:

```
# kill -USR2 `cat /var/run/xinetd.pid`
```

- For inetd

1. Login

Log in as a superuser.

2. /etc/services file editing

Use an editor to register the Usage DB registration port definition in the /etc/services file. For example, in the case of 2365, add the following definition:

```
# FJSVssqc
dbref 2365/tcp
```



See

Refer to "[11.1.2.3 Usage DB reference port number](#)" for details on the port number for looking up the usage database.

3. /etc/inetd.conf file editing

Use an editor to edit the /etc/inetd.conf file.

If the network environment is the Internet, add the following definition:

```
# FJSVssqc
dbref stream tcp nowait nobody /usr/sbin/tcpd /opt/ FJSVssqc/bin/dbref
```

If the network environment is an Intranet, add the following definition:

```
# FJSVssqc
dbref stream tcp nowait nobody /opt/ FJSVssqc/bin/dbref dbref
```


4. /etc/hosts.allow, /etc/hosts.deny file editing (If the network environment is the Internet)

Use an editor to edit the /etc/hosts.allow file and then add the following definition to the head of the file. Set the IP address of the local host to xxx.xxx.xxx.xxx.

```
# FJSVssqc  
dbref : xxx.xxx.xxx.xxx 127.0.0.1
```

Use an editor to edit the /etc/hosts.deny file and then add the following definition to the head of the file. Set the IP address of the local host to xxx.xxx.xxx.xxx.

```
# FJSVssqc  
dbref : ALL EXCEPT xxx.xxx.xxx.xxx 127.0.0.1
```

5. Reflection of changes

Use the kill command so that changes are reflected in inetd. The following is an operation example:

```
# kill -HUP `cat /var/run/inetd.pid`
```

11.1.2.3 Usage DB reference port number

The default port number used for TCP/IP communication by the Usage DB Reference Engine is as follows:

Port number	2365
-------------	------

If this port number is being used by other application so it has been changed, use the changed port number.

11.1.2.4 Stop operation

Perform the following operation to stop the Usage DB Reference Engine.



If the Usage DB Reference Engine is stopped, the Usage DB is no longer referenced.

Stopping the service

[Windows]

To suspend the Usage DB and to stop the Usage DB Reference Engine temporarily, do the following procedure:

Log in to Windows with account with Administrator authority and then "Stop" this service (name: "Systemwalker SQC dbrefsv") using the Services dialog accessed via Windows' Control Panel.



If the startup type of the service is "Automatic" the service is automatically "started" when the installation machine is restarted.

If the service should remain stopped after restarting the installation machine, change the startup type to "Manual".

[Solaris]

To suspend the Usage DB and to stop the Usage DB Reference Engine temporarily, do the following procedure:

1. Login

Log in as a superuser.

2. /etc/services or /etc/inet/services file editing

Use an editor to disable (comment out) the Usage DB registration port definition in the /etc/services or /etc/inet/services file.

The following is an editing example:

```
# FJSVssqc
#dbref 2365/tcp
```

3. Edit of "/etc/inetd.conf" or "/etc/inet/inetd.conf" file

The edit example deletes the following parts.

```
# FJSVssqc
dbref stream tcp nowait nobody /opt/FJSVssqc/bin/dbref dbref -a
```

Or, the following parts are deleted.

```
# FJSVssqc
dbref stream tcp nowait nobody /opt/FJSVssqc/bin/dbref dbref
```

4. Reflection of change

- At before Solaris 9 OS

The change is reflected in inetd by searching for process ID of inetd by using the ps command and the grep command, and using the kill command afterwards. The operation example is as follows.

```
# ps -A | grep inetd
Process ID ...
# kill -HUP Process ID
```

- When OS is Solaris 10 or later

Inetd is stopped.

```
# svcadm disable -t inetd
```

The dbref service is deleted.

```
# svccfg delete -f dbref/tcp
```

"/var/svc/manifest/network/dbref-tcp.xml" is deleted.

```
# rm /var/svc/manifest/network/dbref-tcp.xml
```

Inetd.conf is reactivated.

```
# svcadm enable inetd
```

[Linux]

The use ..situation DB.. reference engine is started, and doesn't reside every time the use state is analyzed. The use state analysis function is not used, and when the reference engine is invalidated, use state DB is operated as follows.

- For xinetd

1. Login

Log in as a superuser.

2. /etc/services file editing

Use an editor to disable (comment out) the Usage DB registration port definition in the /etc/services file.

The following is an editing example:

```
# FJSVssqc  
#dbref 2365/tcp
```

3. Reflection of changes

Use the kill command so that changes are reflected in xinetd. The following is an editing example:

```
# kill -USR2 `cat /var/run/xinetd.pid`
```

- For inetd

1. Login

Log in as a superuser.

2. /etc/services file editing

Use an editor to disable (comment out) the Usage DB registration port definition in the /etc/services file.

The following is an editing example:

```
# FJSVssqc  
#dbref 2365/tcp
```

3. Reflection of changes

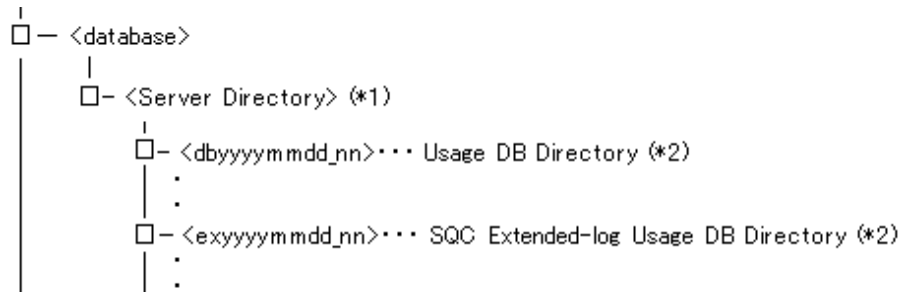
Use the kill command so that changes are reflected in inetd. The following is an editing example:

```
# kill -HUP `cat /var/run/inetd.pid`
```

11.1.3 Usage DB backup and restore

11.1.3.1 Backing up the Usage DB

The Usage DB is created in a variable file storage directory.



** <> is a directory.

(*1) The server directory is created with the name specified as 'Symbol' in of the Analysis Target Server Definition Block of the Usage DB Environment Definition file.

(*2) Variables in the directory name of the Usage DB are as follows. The year/month/day is the date on which the Usage DB is switched (created).

yyyy	Year (1980 -)
mm	Month (01 to 12)
dd	Day (01 to 31)
nn	Serial number (01 to 99)

When backing up the usage database, back up all of the files and directories in the server directory above.

Note

Make sure that the following processes are not running when the usage database is backed up.

[Windows]

dbregmng.exe
dbreg.exe

[UNIX]

dbregmng
dbreg

11.1.3.2 Restoring the Usage DB

When restoring the backed up Usage DB, restore it to the same directory as that used for backup.

- To restore the backed-up Usage DB in an old period

Restore the whole Usage DB directories (dbyyyymmdd_nn, exyyymmdd_nn) corresponding to the desired period.

In this case, do not restore the management files and the Usage DB Information Directories and the SQC Extend-log Usage DB Information Directories under the server directory. Note that if these files and directories are restored, analysis can be performed only for the analysis period the same when the back up was made.

- To restore the backed-up Usage DB because an error occurred in the current Usage DB

Restore all of the files in the backup server directory to the corresponding server directory.

Point

Before restoring the database, first back up the server directory on the server where the error occurred.

Then delete everything in the server directory on the server where the error occurred before restoring the database.

Note

Make sure that the following processes are not running when the usage database is restored.

[Windows]

dbregmng.exe
dbreg.exe

[UNIX]

dbregmng
dbreg

11.1.3.3 Deleting the Usage DB

If the old Usage DB becomes useless and should be deleted, delete the whole directory within the useless period (dbyyyymmdd_nn, exyyymmdd_nn).

Note

- The analysis for the period covered by the deleted usage DB will become unavailable. So it is recommended that you backup the Usage DB before you delete it. For information on backing up the Usage DB, refer to "[11.1.3.1 Backing up the Usage DB](#)".
- Do not delete any other files or directories. Usage DB may get damaged.

Note

Make sure that the following processes are not running when the usage database is deleted.

[Windows]

dbregmng.exe
dbreg.exe

[UNIX]

dbregmng
dbreg

11.2 Analysis Window

This section gives an outline of the usage analysis window.



For a details description of the operations of the usage analysis window, refer to the online help.

11.2.1 Outline

The analysis window is a graphical user interface (GUI) for the user and operates on the client machine.

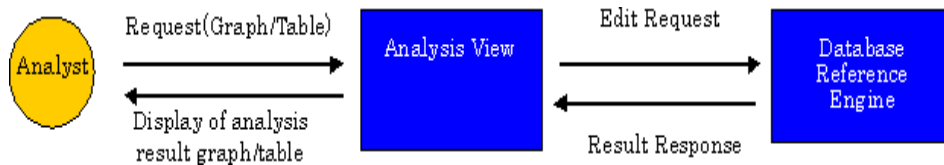
The analysis window is positioned between the user and the Usage DB Reference Engine. It presents data analysis results to the user from a variety of viewpoints, in graphical and tabular forms. The analysis window operates as a Web page (Java(TM) applet) on the user's Web browser.



For information about Java(TM) applet, refer to "3.2 Environment Settings procedures".

If any operation such as the analysis type or analysis method is specified on the analysis window, the Usage DB Reference Engine is instructed to collect data from the Usage DB in which analysis results are stored.

For information on operations of the analysis window, refer to "11.2.6 Operation of analysis page".



11.2.2 Start operation

The Usage Analysis Windows is a Web page (viewer.html) that can be started from the [Web Site Management] window following the operation described below:

1. Click the [Usage Analysis] button on the top page to display the agent selection page.
2. Select the agent to be analyzed and click the [OK] button.



Do not edit the source file for viewer.html.

11.2.2.1 Before startup

To use the analysis window, the following two Usage DB engines must be started in advance.

For information on operations for starting each engine, refer to "[4.2 Environment Settings for Usage Analysis](#)" (Managed Server), "[5.2 Environment Settings for Usage Analysis](#)" (Management Server) and "[11.1 Usage DB Engine](#)".

- Usage DB registration engine
- Usage DB reference engine

Point

To start the analysis window, this Web page (viewer.html) must be registered with the Web server in advance so that it can be referenced. For details of the registration, refer to "[4.1 Settings for Web Server](#)"(Managed Server) and "[5.1 Settings for Web Server](#)"(Management Server).

11.2.2.2 Start Operation

Do the following operation to start the Usage Analysis Window with the [Web Site Management] window.

1. Click the [Usage Analysis] button on the top page to display the agent selection page.
2. Select the agent to be analyzed and click the [OK] button.

The initial window following startup of the analysis window is the following analysis page:

Box	Status
Analysis target server	Server defined at the start of " 15.2.1 Usage DB Environment Definition File ".
Data type	Summary (overall statistical table)
Analysis method	None (For a summary, the analysis method cannot be selected)
Period unit	Day: hour unit including the current year/month/day ^(*)

Note

*1) For information about the current year/month/day, refer to "[11.2.7.1 Date and time](#)".

11.2.3 Stop operation

The analysis window can be closed by the following method:

- Close the Web browser that operates the analysis window.

11.2.4 Configuring the analysis window

The following explains a typical analysis window configuration, name (abbreviated name) of each part and contents. For details of the operations, refer to the following explanations and online help.

11.2.4.1 Analysis window features

After data is analyzed, an analysis page like the one below is displayed.

The initial window following startup is a summary window. No graph is displayed.

In this section, explanation is given with the analysis page by client host name of the request situation as a sample.



Description of the analysis window

1. Analysis target server box

- Select the server to be analyzed. If you select a server from the drop-down list, a data analysis is carried out and the "summary window" is displayed.

At this point, a drop-down list of the data type corresponding to the selected server type (Web server, Proxy server or Web Site group) is also provided in the data type box.

- The server name displayed in this box is the name specified in the Name operand of the "15.2.1 Usage DB Environment Definition File" of the "15.2.1.4 File internal format (analysis target server definition block)". Note that if the name is too long, the first part of the name is displayed.

2. Data type box

Select the type of analysis data required.

3. Analysis method box

From the drop-down list, select the required analysis method, to have data of the type selected in <2> analyzed from that point of view.

The content of the analysis page that is displayed depends on the selected analysis data type and analysis method. For further information, refer to "11.2.5 Analysis window options".

4. Period unit box

Select the period unit for analysis.

When you select the period unit for data analysis from the drop-down list, the display of "5. Period selection list" changes according to the selected unit.

Selecting the period unit for data analysis does not start data analysis.

5. Period selection list

- Select the interval for which data is to be analyzed.

6. Up and Down buttons

- To scroll the period list use these buttons:

Up - to view earlier periods, click this button at the top of the list

Down - to view later periods, click this button at the bottom of the list.

7. Analysis information

- The following information about the analysis results is displayed:

This part is intended for display only and no operation can be performed.

Information	Explanation
Analysis period	The period selected in the period selection list is displayed.
Extraction name/graph display target name	Only for the following analysis pages, the following contents are displayed below the analysis type name respectively: Advanced analysis page: Displays the extraction names. Response analysis page: Displays graph display target names. The extraction name is a name selected from a line of a table during advanced analysis. For details, refer to " Carrying out advanced analysis " in " 11.2.6.1 Performing data analysis ". The graph display target name is a URL name or client name displayed in a graph by selecting a line from a table. For details, refer to " 11.2.5.2 Response analysis page ".

8. The legend

- Color codes for the graph and their contents are displayed.

If a string for explaining the content is too long, it is displayed in abbreviated form at the top of the graph. For information on the correct content, refer to the table.

9. Numeric axis (vertical scale)

- The graph can be re-sized vertically by dragging on the top border with the mouse.

Operation	Result
Drag up	Enlarged (The graduation markings are enlarged)

Operation	Result
Drag down	Reduced (The graduation markings are reduced)
Double click	Scale automatically adjusted (reset to its initial size)

10. Time axis (horizontal scale)

- The graph can be re-sized horizontally by dragging on the right border with the mouse.

Operation	Result
Drag to the right	Enlarged (The graduation markings are enlarged)
Drag to the left	Reduced (The graduation markings are reduced)
Double click	Scale automatically adjusted (reset to its initial size)

11. Graph form

- Specify this to change the type of graph displayed.
Note that the graph forms available for selection depends on the analysis type.

12. Previous period value box

- The values for the previous period can be shown or hidden ('No display').
When you select from the drop-down list, values for the previous period are plotted as a line graph, depending on the selection.

13. Title line (Table header)

- Displays the title of each column of the table.

14. Data line

The total data of the analysis period is displayed in descending order in default.

In the order column (the leftmost column), the graph legend is displayed in addition to the numbers.

- For the following analysis page, a line selection can be made (by clicking a line) and the action is as listed below:

Analysis page	Action when a line selection is made
Analysis page in which an advanced analysis can be made	A line selection can be made (A line can be clicked). An advanced analysis is performed by selecting an advanced analysis destination box.
Analysis data type: response report	A line selection can be made (A line can be clicked). If a line selection is made, a graph of the selected line is displayed.

15. Traffic total field

- Displays the total of the accumulated data.

16. Advanced analysis destination box

- Select the analysis method for the advanced analysis destination.

If you click the advanced analysis destination box after clicking a 'Data line' and select a destination from the drop-down list, a data analysis (advanced analysis) is performed and a graph or table is displayed.

The advanced analysis destination box is displayed only on pages where advanced analyses can be performed.

17. Number of lines of the table

- Select here to modify the number of lines in the table of the analysis window.

18. Display Order

- Select here to modify the display order of the analysis window.

19. Help

20. Select here to display the online help in addition to the analysis window.

11.2.5 Analysis window options

In the analysis window, results of the availability of the following server types (analysis target server types) are displayed:

- Web server
- Proxy server
- Web site group

The following eight types of analysis results (analysis data types) are available. All eight types can be displayed on the Web server and six types can be displayed on the Proxy server.

- Summary (total of each status of the analysis target server)
- Session status
- Request status
- Traffic status
- Cache status
- Error status
- Response status (Web server and Web site group)
- Page navigation status (Web server only)

On the analysis window, results edited from a variety of analytical points of view (such as URL or client based) are displayed as graphs or tables for each analysis data type.

Regarding part of the analysis pages, supplementary remarks are provided in order.

- Traffic display
- Response analysis page

11.2.5.1 Traffic display

On each page that displays traffic status analysis and other traffic quantity (such as the total traffic quantity and total successful request traffic quantity), the traffic quantity is displayed in unit of kilobyte (KB).

Traffic quantity equal to or greater than 1 byte and less than 1,000 bytes is displayed as 1KB.

11.2.5.2 Response analysis page

The response analysis differs from other analysis pages as follows:

Relationship with SQC extended log collection

In response analysis, data is analyzed based on the data accumulated in the SQC extended log file by SQC extended log collection. If no SQC extended log collection is created, no data analysis result can be obtained even if an analysis of this data is performed.

Display data

The following values are displayed on the response analysis pages.

In tables, data is displayed in descending order of average time (descending order from the more delayed average response).

- Average (average response time in the analysis period)
- Maximum (longest [slowest] response time in the analysis period)
- Minimum (shortest [fastest] response time in the analysis period)

The following table lists the display unit and the number of digits:

Item	Meaning
Unit	Second
Number of digits	4-digit integer and two decimal places (Number rounded to second decimal place)
Range to be displayed	0.01s to 3,599.99s (less than one hour) (Less than 10ms is displayed as 0.01s)
If the display range is exceeded	Displayed as 1 hour or more

In the case of one hour (3600.00 seconds), "1 hour or more" is displayed but the actual value is used for the average value.

Graph display/switching

In contrast to other analysis pages, the response analysis pages provide for the average, maximum and minimum of one selected line (one URL or client) to be displayed as a graph. By default, the graph for only the URL or client whose average time is Top1 (first line in the table) is displayed. After selecting a line from a table, the graph can be switched to display details of the selected line.

In the analysis information section (above the graph) of the analysis page, the name (URL name or client name) selected from a table is displayed below the analysis type name as the graph display target name.



Note that this operation is the same as that in "Carrying out advanced analysis" in "11.2.6.1 Performing data analysis" described later, but no advanced analysis is carried out for response analysis.

11.2.6 Operation of analysis page

11.2.6.1 Performing data analysis

When data analysis is performed, the analysis page displayed (or updated) is that matching these selected values: "analysis target server type", "analysis data type", "analysis method" and "analysis period".

The following table lists the basic flow of data analysis (A down arrow indicates you continue to the next step. An up arrow indicates you can return to the previous step.):

Operation	Initial window
[1] Analysis window startup	Summary of the default analysis target server
[2] Analysis target server selection [Analysis target server box]	Summary
[3] Analysis data type selection [data type box]	Analysis method: head of the drop-down list
[4] Analysis method selection [Analysis method box]	Analysis period: Week: day unit including the current year/month/day
[5] Analysis period change [Period unit box and period selection list]	Analysis results selected in [3] and [4]
[6] Advanced analysis execution	Advanced analysis results

Data analysis is executed for all the operations shown in the table above.

Note that the flow of the operations shown in the table is an indicative procedure only. In practice, the procedure need not always be followed; some operations might be omitted or the order of operations might be interchanged.

However, selection of the analysis data type other than the summary in [3] is required for [4] Analysis method selection and an analysis page for which an advanced analysis can be carried out must be displayed for [6] Advanced analysis execution.

The following explains each of the above operations. For the "analysis window startup", refer to "11.2.2.2 Start Operation".

Analysis target server selection

The analysis target server can be selected from the "Analysis target server box". The server selected here must be defined in the Usage DB Environment Definition File in advance.

Analysis target server type

The analysis target server types are following three types:

- Web server
- Proxy server
- Web site group

By selecting an analysis target server, an analysis data type corresponding to that server type can be selected.

[Operation method]

1. In the analysis window, click "Analysis target server" and select a server from the drop-down list.
Data analysis is executed and the data analysis page is updated.

[Initial window]

The page displayed immediately after selecting the analysis target server has the following details:

Box	Status
Analysis target server	Selected server
Data type	Summary (overall statistical table)
Analysis method	None (For a summary, the analysis method box cannot be selected)
Period unit	Week: day unit including the current year/month/day ^(*)



Note

(*) For information about the current year/month/day, refer to "[11.2.7.1 Date and time](#)".

Analysis data type selection

Select the analysis data type from the following eight types (six types for the Proxy server).

- Summary (total of each status of the analysis target server)
- Session status
- Request status
- Traffic r status
- Cache status
- Error status
- Response status (for the Web server and the Web site group)
- Page navigation status (for the Web server)

The response status can be selected only if the type of the analysis target server is the Web server or the Web site group.

The page navigation status can be selected only if the type of the analysis target server is the Web server.

By selecting an analysis data type, drop-down lists of the analysis method box corresponding to the server type and analysis data type are provided.

[Operation method]

1. Click the "Data type box" and then select an analysis data type from the displayed drop-down list.
Data analysis is executed and the data analysis page is updated.

[Initial window]

The page displayed immediately after selecting the analysis target server has the following details:

Box	Status
Analysis target server	Selected server
Data type	Selected analysis data type
Analysis method	First analysis method in the drop-down list However, no analysis method for a summary (For a summary, the analysis method cannot be selected)
Period unit	Week: day unit including the current year/month/day (*1)

Note

(*1) For information about the current year/month/day, refer to "[11.2.7.1 Date and time](#)".

Selection of analysis viewpoint

list. This list includes all methods applicable to the selected "analysis target server type" and "analysis data type".

[Operation method]

1. Click the "Analysis method" box and then select the required analysis method.
A data analysis is carried out and the data analysis page is updated/displayed.

[Initial window]

The page displayed immediately after selecting the analysis method has the following details:

Box	Status
Analysis target server	Selected server
Data type	Selected analysis data type
Analysis method	Selected analysis method
Period unit	Same period unit/period as that of the previous analysis page

Note

- If no data analysis result is displayed:

If no data is output as a result of data analyses by a variety of operations, a "No data for this period" message is displayed.

For other messages, refer to "[17.2 Usage Analysis Function](#)".

Changing the analysis period

When the analysis period is changed, data analysis is performed so that editing results for a number of periods can be displayed. Also, as with the normal analysis page, the analysis period can be changed on the "Summary" window and advanced analysis page.

To change the analysis period, operate "the required period unit from the Unit box", then select "the required period from the Period selection list". When a period is selected from the period selection list, a data analysis is carried out and an analysis page of the edited results is displayed.

Carrying out advanced analysis

Advanced analysis is analysis focusing on a specific URL, clients or error numbers.

To perform an advanced analysis, you select a table line from the analysis page and then from the "Advanced analysis destination" box you select the analysis method of the advanced analysis destination. The advanced analysis is executed and the editing results extracted from the selected items are then displayed.

For example, if you select an arbitrary line from the table in the URL-based analysis page of the session status and select [Breakdown for each client host name] from the "Advanced analysis destination box" an analysis page for each client host name extracted using only the URL name of the line is displayed.

On this page, the total sessions for each client of the specific URLs is displayed.

Advanced analysis can be performed only for analysis pages listed on the "Pages where the advanced analysis can be carried out".

[Window display of the advanced analysis page]

In the analysis information section (above the graph), displayed after an advanced analysis is performed, the name selected from a table is displayed below the analysis type name as the extraction name.

For example, if an advanced analysis is performed from a URL based analysis page, the selected URL name is displayed there.

[Analysis page where the advanced analysis can be carried out]

On analysis pages where the advanced analysis can be performed, the table lines can be selected using the mouse.

On analysis pages of the response status, the lines of a table cannot be selected.

Line selection from a table in the response analysis is intended for graph display switching instead of the advanced analysis. For details, refer to "[11.2.5.2 Response analysis page](#)".

[Operation method]

1. Display an analysis page where the advanced analysis can be carried out.
2. Select a line to be subjected to advanced analysis (extracted) from the displayed table.
3. Click "Advanced analysis destination" and from the drop-down list select the required analysis method for the advanced analysis destination.

An advanced analysis (data analysis) is performed and the data analysis page is updated and displayed. The contents displayed are analysis results (analysis page) based on the line selected from the table.

[Initial window]

The window displayed immediately after the advanced analysis is performed has the following details:

Box	Status
Analysis target server	Selected server
Data type	Selected analysis data type
Analysis method	Analysis method selected from the "Advanced analysis destination box"
Extraction name	Item name selected from the table line
Period unit	Same period unit/period as that of the previous analysis page

Period unit box

The period box is displayed as "xx:yy" units. "xx" indicates the analysis period and "yy" indicates the unit (time axis unit) for plotting on graphs.

For example, if a data analysis is performed as "Week: day" unit, the result is:

Table: The total of results of one week.

Graph: Data for one week is plotted for each day.

Note that the "yy" unit does not apply to the pie chart and "Summary" window. Refer to "[Period unit for pie chart and summaries](#)" in the later section.

If the unit of analysis period is selected from the period unit box, the display of the period selection list changes so that a specific analysis period can be selected. No data analysis is executed when you select only the period unit.

Period selection list

In the period selection list, time intervals of the Unit selected on the analysis page are displayed. For example, a 'Week: day unit' setting results in 7-day Sunday-to-Saturday periods being displayed such as "2000/11/7 - 2000/11/13". When a period is selected from the list, a data analysis of the period is performed and the result analysis page is displayed. The analysis type is the same as that of the previous analysis page.

Period units that can be selected and the contents of period selection list when selected

Period unit	Displayed contents of the period selection list	Explanation of format
Year: half-year unit	yyyy	yyyy: year m: month (1 to 12) d: day (1 to 31)
Year: quarter unit	yyyy	
Year: month unit	yyyy	
Half-year: month unit	yyyy/1 - yyyy/6 yyyy/7 - yyyy/12	
Quarter: month unit	yyyy/1 - yyyy/3 : yyyy/10 - yyyy/12	
Month: day unit	yyyy/m	
Week: day unit	yyyy/m/d - yyyy/m/d (from Sunday to Saturday)	
Day: hour unit	yyyy/m/d	

[Operation method]

1. Click the "Unit" box and select the required unit from the drop-down list.

The period selection list is updated according to the unit selected.

(No data analysis is performed at this step.)

2. Select a specific period from the period selection list.

Data analysis is performed for the selected period and the analysis page is displayed.

(As other settings on the left side of the page have not been changed, the analysis type is the same as that of the analysis page previously displayed.)

[Period selection list paging]

If the required period is not currently displayed in the period selection list, the list can be scrolled to display the required period.

You scroll the list by clicking the Up button above the list or the Down button below the list.

Click the Up button to scroll to earlier dates. Click the Down button to scroll to later dates.

If the upper limit or lower limit of the display period of the period selection list is reached, each paging button becomes disabled (grayed), as follows:

- When the upper limit (any period including 1/1/1980) is displayed, the Up button becomes disabled.
- When the lower limit (any period including the current year/month/day) is displayed, the Down button becomes disabled.

[Future period]

No future period can be selected from the period selection list.

Since the current year/month/day is determined based on the client machine time, the client machine time must be correct so that the latest analysis results can be obtained.

For the client machine time, refer also to "[11.2.7.1 Date and time](#)".

Period unit for pie chart and summaries

On analysis pages where pie chart is displayed, the total of the selected period is displayed in graphical form.

Thus, editing results are the same for the period units shown below. In addition, a graph totaled for one year is displayed.

- Year: half-year unit
- Year: quarter unit
- Year: month unit

Displaying values for the previous period as graph

Values for the previous period are the comparison reference for graphical analysis. These values are not displayed by default.

By selecting the previous period value box, they can be displayed on the graphs. Previous-period values are always plotted as broken lines, regardless of the graph type.

Three modes are available for the display of pervious-period values depending on the display/calculation methods. The display mode can be selected for each analysis type. The selected display mode is stored for each analysis type while the analysis window is active.

On analysis pages that display a pie chart, previous-period values cannot be displayed.

[Display modes for previous-period values]

The following display types of previous-period values are available. They can be selected on all analysis pages, except for the "Summary" page and "Page Navigation Status" page.

Display mode for previous-period values	Graph display
Non-display	Previous-period values are not plotted. This is the default state.

Display mode for previous-period values	Graph display
Display	The total for each unit of one period prior to the analysis period is plotted as the previous-period value. For example, if the analysis period is "week: day unit", the total for Monday of last week is plotted for Monday.
Average value	The total for one period prior to the analysis period divided by the number of units is plotted as the previous-period value. For example, if the analysis period is "week: day unit", the value for the previous period is "total of the previous week/7".

[Operation method]

1. Click the "Value of pre-period" box.

2. Select the required display mode from the drop-down list.

The display of values for the previous period is updated according to the display mode selected.

If data for the previous period is unavailable, values for the previous period are not plotted.

[What is the previous period ?]

Current period unit	Previous period
Year: half-year unit	The previous year
Year: quarter unit	The previous year
Year: month unit	The previous year
Half-year: month unit	The previous period
First half	Second half of the previous year
Second half	First half of the same year
Quarter: month unit	The previous period
First quarter	Fourth quarter of the previous year
Second quarter	First quarter of the same year
Third quarter	Second quarter of the same year
Fourth quarter	Third quarter of the same year
Month: day unit	The previous month
Week: day unit	The previous week
Day: hour unit	The previous day

11.2.7 Notes

This section includes notes to assist you when using the analysis window.

11.2.7.1 Date and time

In the analysis window, the current date and time are determined based on the client machine date and time (including the year, month and day).

For example, in the initial window immediately after starting the analysis window, the "Summary" window of the week: day unit including the current year, month and day is displayed. "Current" in this case means the current date and time on the client machine.

No future period can be selected from the period selection list. Here "future" means any time after the client machine time.

Since no analysis period can be selected after the current client machine time, the latest editing results cannot be obtained if the client machine time is delayed. For this reason it is important to ensure that the client machine is always set to the correct date and time.

11.2.7.2 Operation when moving to other URL

If the Web browser used to operate the analysis window is moved to another Web page(URL), the analysis window terminates.

If the Web browser returns to the analysis window Web page as a result of using Back or Next on the Web browser, the analysis window is restarted. In this case, settings and the standard mode in the Setup page do not store the former states, just as in the case where the analysis window is terminated and then restarted (Default values are set).

11.2.7.3 Extension name display

The display of the extension name depends on the final qualifier in the URL name. The following table lists the details:

Final qualifier of URL	Displayed extension name
If the URL name is a.html	html
If the URL name is a.gif	gif
If the URL name is a.GIF	GIF
If the URL name has no extension	<FILE>
If the URL name is a directory name	<DIRECTORY>
If the URL name is a domain name of the server	<HOMEDIRECTORY>
If the pathname cannot be obtained	<NOTHING>

11.2.7.4 Host name/IP address display when DNS conversion is not possible

If "SearchDNS=yes" is specified in the Usage DB Environment Definition File, host information (host name or IP address) for the client stored in the analysis target log is DNS-converted. If, however, the conversion fails for some reason, the display is as listed below:

Host information of the client stored in logs	DNS conversion	Displayed host name	Displayed IP address
IP address	Success	Host name	IP address
	Failure	IP address	IP address
Host name	Success	Host name	IP address
	Failure	Host name	Host name

11.2.7.5 Handling of the URL name to be analyzed

The URL name of the log file to be analyzed is analyzed faithfully. That is, uppercase and lowercase characters of the string contained in the URL name are distinguished and handled as different URL names.

11.2.7.6 Notes on selecting the URL based breakdown from the analysis method box

If you select the URL based breakdown from the analysis method box, only the URL names corresponding to the extensions specified in "RequestURLSuffix" of the Usage DB Environment Definition File are displayed.

11.2.7.7 Notes on selecting the URL extension based breakdown from the analysis method box

If you select the URL extension based breakdown from the analysis method box to execute advanced analysis based on URL, and the extension for advanced analysis is not specified in "RequestURLSuffix" of the Usage DB Environment Definition File, the extension excluded from analysis and "No data in this period" is displayed.

11.2.7.8 Notes on displaying analysis results of mass log data

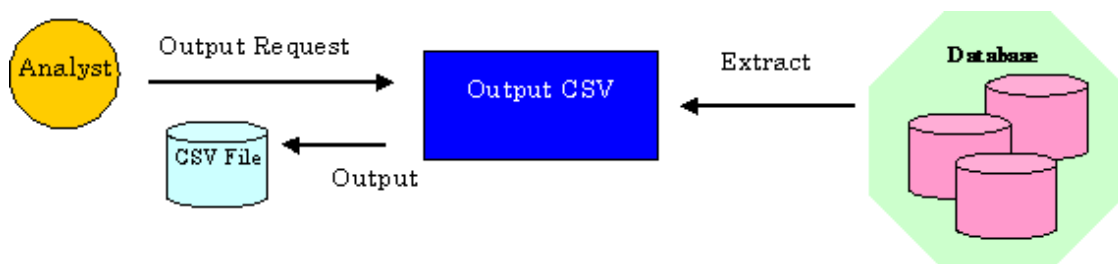
If you select the year unit from the period unit box and display analysis results of mass log data, it may take some time before the analysis window is displayed.

11.3 CSV Output

This section explains the CSV output of the Trend Viewer.

11.3.1 Outline

The CSV output is a command for outputting data from the Usage DB of the Trend Viewer to a file in the CSV format, depending on the data type.



11.3.2 Start operation

11.3.2.1 Startup

The CSV output is a command (dbprt command) that operates on the installation machine of Agent for Business. To start the CSV output, log in to the installation machine of Agent for Business and then execute the command in the following path:

[Windows]

```
Installation directory \bin\dbprt.exe
```

[UNIX]

```
/opt/FJSVssqc/bin/dbprt
```

11.4 SQC Extended Log Collection

The SQC Extended Log Collection is used to collect and accumulate data not collected by the functions provided by the Web service (such as the Web server). Data accumulated by the SQC Extended Log Collection is called the "SQC extended log". The following SQC extended log can be collected and accumulated.

11.4.1 Response log

11.4.1.1 Outline

The response log is a log in which data on the response time of the CGI program collected in terms of the Web page user is accumulated.

The response time is a time interval required to receive a result from the CGI program after the Web page user executes a service that calls the CGI program.

For example, in the case of a Web page that executes searches, the response time is a time interval required to display a search result after the search is started.

Data is collected and accumulated in the response log by using the following three functions:

Data collection function1

Java(TM) applet (**ResLog1.class**) that runs on the Web browser. This function is called when the user references the Web pages and executes a service that calls the CGI program; and data when the service is executed is collected.

To run this function, refer to "[Editing Web pages](#)" in advance.

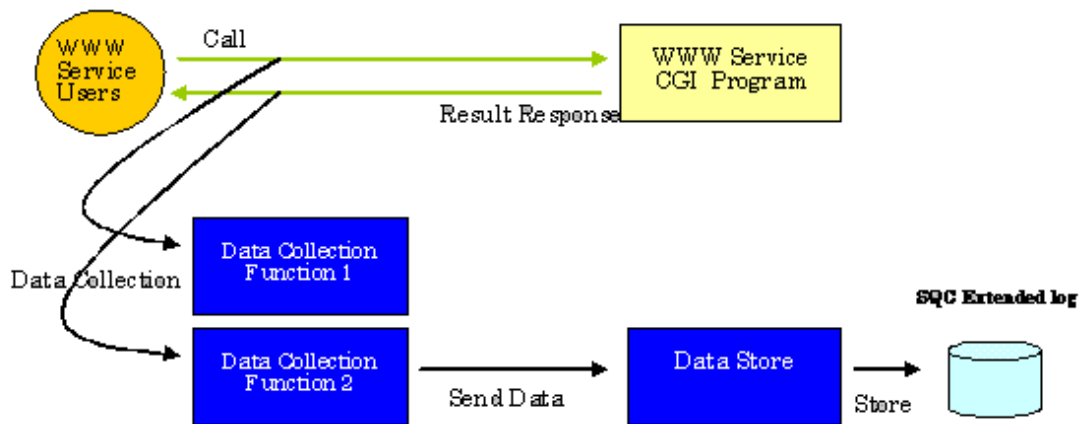
Data collection function2

Java(TM) applet (**ResLog2.class**) that runs on the Web browser. This function is called when the Web page user receives a result of a service that calls the CGI program. This applet collects data when a result is received and then sends the response time to the data accumulation function after calculating it together with data of the data collection function1.

To run this function, refer to "[Editing Web pages](#)" in advance.

Data accumulation function

CGI program (**reslog.cgi**) that runs on the Web server (installation machine). The data accumulation function is automatically started when data collection function2 is started. This function accumulates data sent from the data collection function2 in the SQC extended log file.



11.4.1.2 Making settings for log collection

This section explains how to make settings for response log collection.

Before making settings

It is necessary to register the CGI program (**reslog.cgi**) of the data accumulation function with the Web server in advance so that it can be executed. For details of the registration, refer to "[4.1 Settings for Web Server](#)".

Information

Java(TM) applet (ResLog1.class, ResLog2.class) is used by the data accumulation function. For information about the Java(TM) applet, refer to "[3.2 Environment Settings procedures](#)".

Editing Web pages

Incorporate the Java(TM) applet for log collection into the HTML documents of each Web page that makes log collection. Both of the following two related Web pages must be edited:

- Web page that calls a service
 - Web page that calls the CGI program of a service
 - For example, a Web page that executes searches when a keyword is given.
- Web page that receives results
 - Web page that receives results (displays results) from the CGI program.
 - For example, a Web page that displays search results.

Editing Web pages that call a service

Incorporate the Java(TM) applet (ResLog1.class) of data collection function1 into the HTML document of the Web page that calls a service.

The following is a sample HTML document. URL in CODEBASE within the sample is described assuming that, like the setting example in "[4.1 Settings for Web Server](#)" the physical path of the directory www under the installation directory is registered as the alias "SQLC".

In the following example, the Java(TM) applet (ResLog1.class) of the data collection function1 is called when the search button is clicked.

```

<!-- -->
<!-- Response log collection page Sample (Part 1) -->
<!-- -->
<HTML>
<HEAD>
<TITLE> Search service page (sample)</TITLE>
</HEAD>
<BODY BGCOLOR=WHITE>
<!-- ***** Systemwalker SQC (begin) ***** -->
<APPLET NAME="ResLog1" CODEBASE="/SQC/classes"
CODE="ResLog1.class" ARCHIVE="reslog.jar" WIDTH=1 HEIGHT=1>
</APPLET>
<!-- ***** Systemwalker SQC (end) ***** -->
<CENTER><FONT COLOR=GREEN> Search service page (sample) </FONT></CENTER>
<BR><BR>
<FONT SIZE=5 COLOR=BLUE> Search service </FONT>
<HR>
<FORM METHOD="post" ACTION="/cgi-bin/search.cgi">
Search key
<INPUT TYPE="text" NAME="key1" SIZE="25">
<BR><BR>
<INPUT TYPE="reset" VALUE="Reset">
<INPUT TYPE="submit" VALUE="Search" onClick="document.ResLog1.run()">
</FORM>
<HR>
<FONT COLOR=RED> Notes </FONT>
<P>
This site records and accumulates response reports of the search service. Results are used
exclusively to improve the search service. No violation of privacy is intended.
</P>
</BODY>
</HTML>

```

[Sample explanation]

Content	Explanation
Blue character	Description for incorporating data collection function1
Path to be specified in CODEBASE	URL of the storage directory of the Java(TM) class file of this product

The above sample is stored at the following storage location after installation.

[Windows]

```
Installation directory \sample\search_request_jp.html
```

[UNIX]

```
/opt/FJSVssqc/sample/search_request_jp.html
```

Editing the Web page that receives results

Incorporate the Java(TM) applet (ResLog2.class) into the HTML document of the Web page that receives (displays) results.

The following is a sample HTML document. URL in CODEBASE within the sample is described assuming that, like the setting example in "4.1 Settings for Web Server" the physical path of the directory www under the installation directory is registered as the alias "SQC".

```
<!-- -->
<!-- Response log collection page Sample (Part 2) -->
<!-- -->
<HTML>
<HEAD>
<TITLE> Search service page (sample) </TITLE>
</HEAD>
<BODY BGCOLOR=WHITE>
<!-- ***** Systemwalker SQC (begin) ***** -->
<APPLET CODEBASE="/SQC/classes"
CODE="ResLog2.class" ARCHIVE="reslog.jar" WIDTH=1 HEIGHT=1>
<PARAM NAME=url VALUE="/SQC/cgi-bin/reslog.cgi">
</APPLET>
<!-- ***** Systemwalker SQC (end) ***** -->
<CENTER><FONT COLOR=GREEN> Search service page (sample) </FONT></CENTER>
<BR><BR>
<FONT SIZE=5 COLOR=BLUE> Search service </FONT>
<HR>
<P>
Search result...
</P>
</BODY>
</HTML>
```

[Sample explanation]

[Windows]

Content	Explanation
Blue character	Description for incorporating data collection function2
Path to be specified in CODEBASE	URL corresponding to the following directory: Installation directory\www\classes
Path to be specified in VALUE	URL corresponding to the following file: Installation directory\www\cgi-bin\reslog.cgi

The above sample is stored at the following storage location after installation.

Installation directory\sample\search_result_jp.html

[UNIX]

Content	Explanation
Blue character	Description for incorporating data collection function2
Path to be specified in CODEBASE	URL corresponding to the following directory: /opt/FJSVswmag/www/classes
Path to be specified in VALUE	URL corresponding to the following file: /opt/FJSVswmag/www/cgi-bin/reslog.cgi

The above sample is stored at the following storage location after installation.

/opt/FJSVssqc/sample/search_result_jp.html

Notes on Web page editing

Use the identical string to specify URL in CODEBASE inside the APPLET tag of the Web page that calls a service and that in CODEBASE inside the APPLET tag of the Web page that receives (displays) results. Note that, if the URL is not identical, for example, if one URL is specified using a relative path and the other URL is specified using an absolute path, no response log can be collected.

Operation after settings

If a Web page with the settings for this log collection is used, log collection is carried out in the sequence as shown below:

Target	Operation description
[1]Web user:	References URL of the Web page using the Web browser.
[2]Web user:	Executes a service (for example, a search service) that calls the CGI program.
[3]Web user:	Receives a result from the CGI program.

Target	Operation description
[4]Inside:	The response log is collected and accumulated.
[5]Inside:	The log is registered with the Usage DB by the Usage DB Registration Engine.
[6]Analyzer:	An analysis can be carried out and results can be displayed on the analysis window. The URL based response analysis and client based response analysis are supported.

Note

If there is any error in the edited Web page, the response log cannot be collected. Before providing a Web page service, carry out tests to make sure that the response log is actually collected.

11.4.1.3 Stopping log collection

To stop the response log collection, delete the lines added to the HTML document of the Web page that start log collection. Delete such text from both the HTML page that calls a service and the HTML page that receives results.

To be deleted is the **blue text** in each HTML page as described in "[11.4.1.2 Making settings for log collection](#)" Once deleted, no response log is collected and accumulated even if this Web page is referenced and a service is called.

11.4.1.4 Log format

A response log with one line of text is accumulated in the SQC extended log file in response to one piece of data sent from data collection function2.

The format of one line is as follows. The field is delimited by one blank character.

1.Date 2.Type 3.Version 4.HostName 5.Path 6.Reserve 7.KeyData

No.	Field	Explanation								
1	Date	<p>Time at the log is accumulated. This time is a local time on the installation machine. Its format is as follows and blue characters are variable: [dd/mon/yyyy:hh:mm:ss SHHMM]</p> <p>The meaning of each field is as follows:</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>dd</td> <td>Day (01 - 31)</td> </tr> <tr> <td>mon</td> <td>Month ("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec")</td> </tr> <tr> <td>yy YY</td> <td>Christian era (1970 -)</td> </tr> </tbody> </table>	Field	Meaning	dd	Day (01 - 31)	mon	Month ("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec")	yy YY	Christian era (1970 -)
Field	Meaning									
dd	Day (01 - 31)									
mon	Month ("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec")									
yy YY	Christian era (1970 -)									

No.	Field	Explanation	
		hh	Hour (00 - 23)
		m m	Minutes (00 - 59)
		ss	Seconds (00 - 59)
		S	Flag of time difference with the Coordinated Universal Time (UTC) ("+","-")
		HH	Hour of time difference with the Coordinated Universal Time (UTC) (00 -)
		M M	Minutes of time difference with the Coordinated Universal Time (UTC) (00 -)
2.	Type	Data type (code that indicates the log type) The response log corresponds to "2".	
3.	Version	Version level of the log format. Currently only "1" for the response log.	
4.	HostName	(Web page user's) host name or IP address where the browser operates	
5.	Path	Path to the HTML document of the Web page	
6.	Reserve	Reserved Currently always "0"	
7.	KeyData	Response time (in milliseconds)	

For the file name, capacity estimation and SQC extended log file switching, refer to "[15.2.5 SQC extended log file](#)".

11.5 Navigation Guide for the Usage Analysis Window

This section explains how to analyze the usage of the Web site by using the Trend Viewer.

11.5.1 Analyzing changes in the number of Web site visitors

This section explains the method of analysis focusing on the transition of the number of visitors to the Web site.

By making analysis focusing on the transition of the number of visitors to the Web site, the following types of information can be obtained and used for effective operation of the Web site.

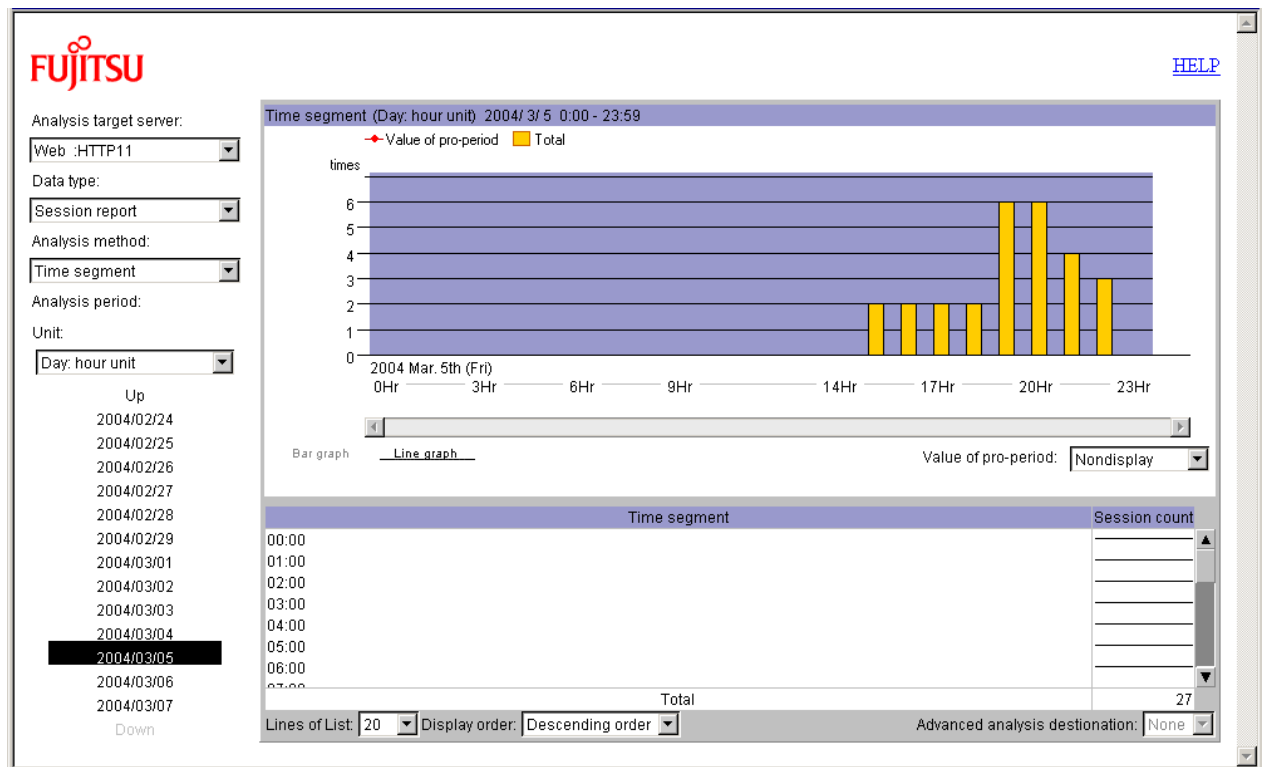
- Number of visitors
- Frequently accessed time zone

- Frequently accessed period, such as the beginning or end of the month

11.5.1.1 Analysis using the usage analysis window

To analyze with focusing on the transition of the number of visitors to the Web site, specify the following items in the usage analysis window:

Item	Specification
Analysis target server	Specify the server or the group to be analyzed.
Data type	Session status
Analysis method	Time segment
Analysis period	Specify the analysis period unit and period.
Unit	



If "Date: hour unit" is specified for the Analysis period, the transition of the number of sessions every hour on the specified date.

The number of sessions represents the number of persons who visits the site; the period from entering the site to exiting the site is counted as one session.

Note

If a user makes no access for a given period, the session is assumed ended. If the same user makes an access again, it is counted as another session.

Similarly, if the same user visits the site many times within a day, the individual visits are counted as separate sessions.

11.5.2 If you would like to make analysis in page units

This section explains the method of analysis focusing on the usage of each page that makes up the contents of the Web site, such as for checking which page is popular.

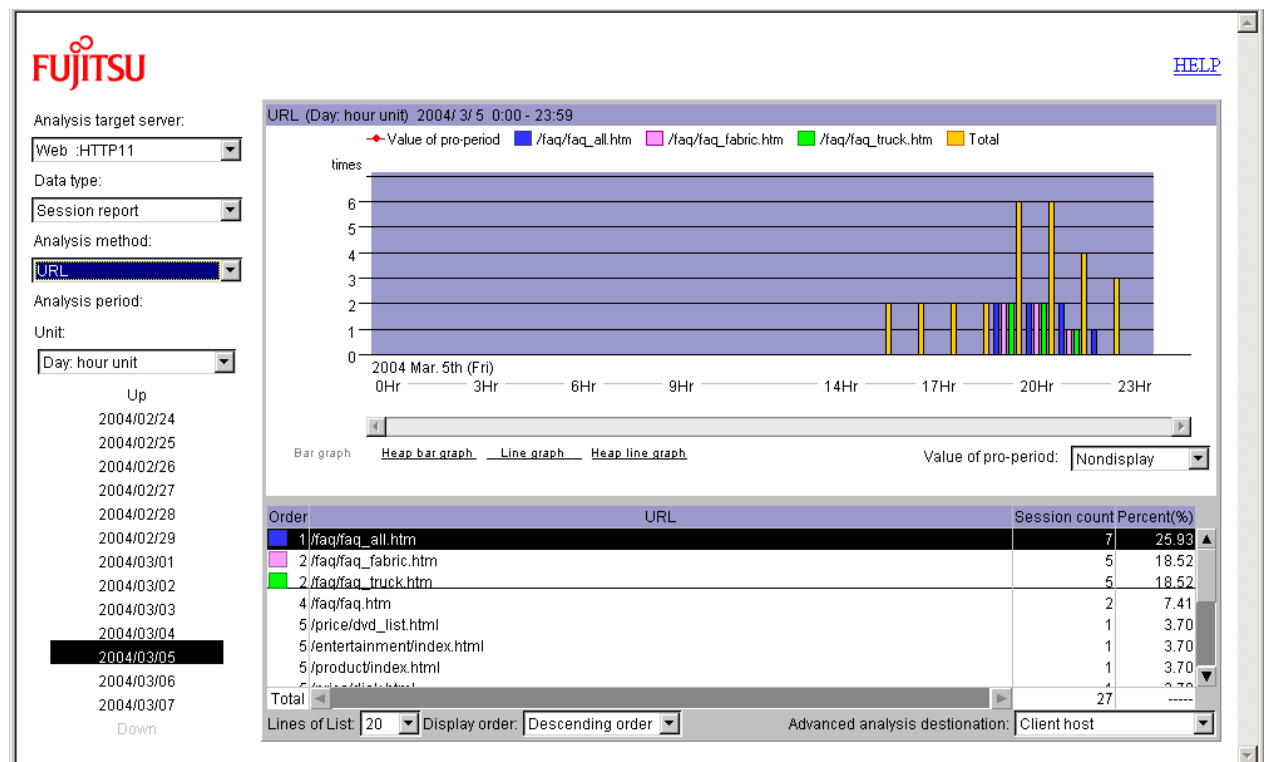
By making analysis focusing on the usage of each page, the following types of information can be obtained and used for effective operation of the Web site.

- Frequently used pages
- Usage of pages that the contents provider wants to be used
- Effective pages for information supply

11.5.2.1 Analysis using the usage analysis window

To analyze with focusing on the usage of each page, specify the following items in the usage analysis window:

Item	Specification
Analysis target server	Specify the server or the group to be analyzed.
Data type	Session status
Analysis method	URL
Analysis period	Specify the analysis period unit and period
Unit	



If "Date: hour unit" is specified for the analysis period, the usage of the URL (page unit) on the specified date is displayed.

The upper half of the analysis window graphs the session counts of three top ranking URLs and the total session count. The lower half shows the session counts for the specified number of URLs (20 URLs by default).

Point

Because "Session status" is specified for the analysis data type, usage analysis for each page is performed in units of sessions. In other words, even if the same user frequently accesses the same page within one session, the usage count is one. This analysis thus tells how many different users used the page.

"Request status" can also be specified for the analysis data type. In this case, if the same users frequently accesses the same page, the usage count is incremented each time the page is accessed. This analysis thus tells how many times the page was used.

Note

When URL is specified as the analysis method, the accesses to the URLs having the extensions specified with RequestURLSuffix in the analysis target server definition block in the Usage DB Environment Definition File are analyzed.

The default settings are as follows:

```
RequestURLSuffix = "html,htm,shtml,shtm,stm,cgi,asp,pl,tcl,sh"
```

11.5.3 Analyzing site navigation

An analysis of page navigation status of customers, such as status dealing with the sequence that a customer accesses the pages of the Web service and whether a customer reaches a desired page easily, provides useful information that can be used to, for example, review the configuration of content provided as the Web service.

11.5.3.1 Analyzing site navigation for an entire Web site

In a review of organization of the content on an entire Web site, site navigation analysis can reveal how the content of the Web service is being used.

In this type of analysis, a page navigation status on the most frequently used patterns on the Web site is displayed, providing reference material that can be used to focus on the organization of content on URL pages.

The following is an example of using site navigation analysis for an entire Web site.

1. Specify the following items on the analysis screen to perform the analysis.

Item	Specified content
Analysis data type	Page navigation status
Analysis method	Whole Web site

When the analysis is complete, a page navigation status on the most frequently used patterns for the Web site is displayed.

1. For a more detailed analysis of the page navigation status that focuses on a displayed URL page, specify the URL you want to analyze and then select "Next page" or "Previous page" as the drill-down destination.
2. For even greater detail, repeat the process of selecting the above URL and drilling down further.

11.5.3.2 Analyzing site navigation for a specific customer

Use site navigation analysis that focuses on a specific customer to analyze the sequence in which a particular customer using the Web service accesses the pages of the Web site.

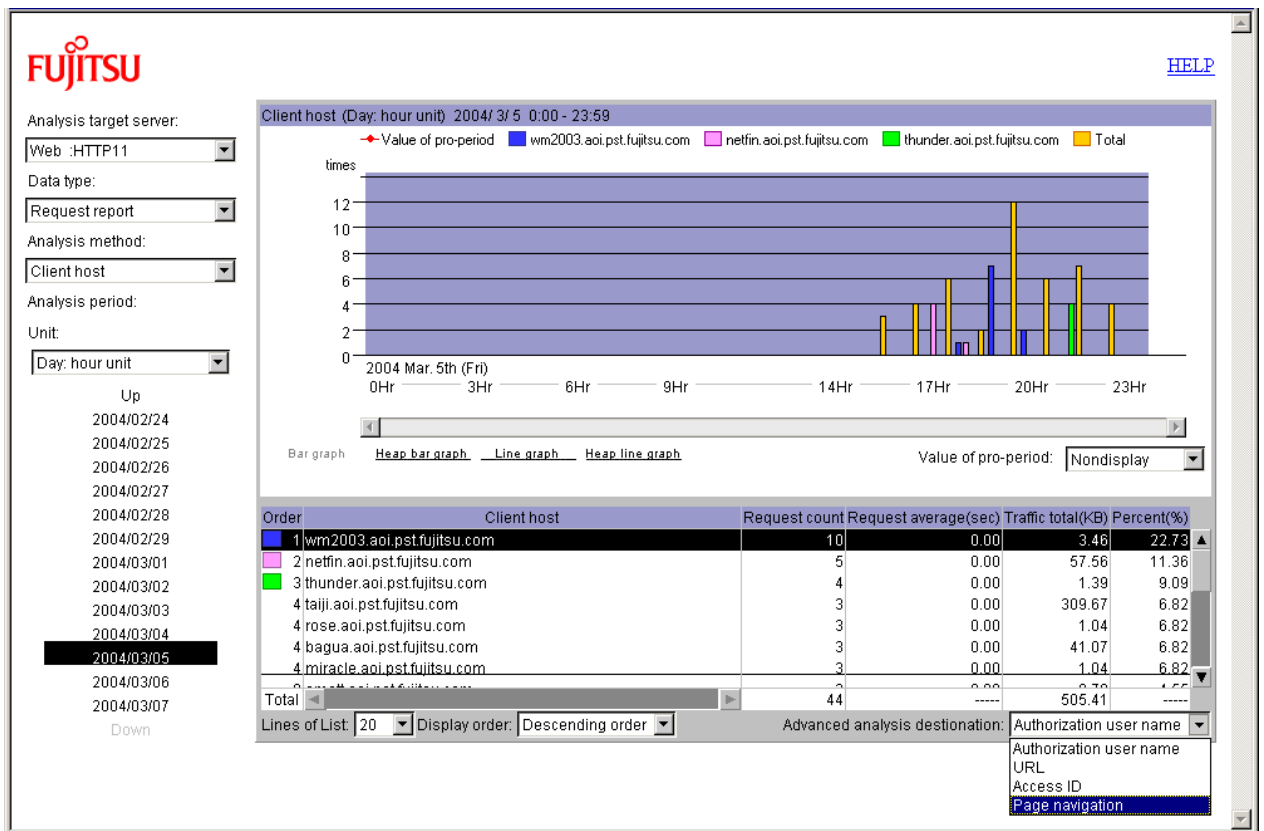
The following is an example of using site navigation analysis that focuses on a specific customer

1. Specify the following items on the analysis screen to perform the analysis.

Item	Specification
Analysis data type	Session status
	Request status
Analysis method	Client host name base
	Client IP address base
	Authorization user name base
	Access ID base

A list of customers that matches the specified analysis data type and analysis method is displayed.

2. Specify the customer on the displayed customer list that you want to analyze and then select "Page navigation" as the drill-down destination.



When the analysis is complete, a page navigation status on the most frequently used patterns for the customer is displayed.

FUJITSU [HELP](#)

Analysis target server: Web :HTTP11

Data type: Request report

Analysis method: Client host

Analysis period: Day: hour unit

Unit: Day: hour unit

Up

- 2004/02/24
- 2004/02/25
- 2004/02/26
- 2004/02/27
- 2004/02/28
- 2004/02/29
- 2004/03/01
- 2004/03/02
- 2004/03/03
- 2004/03/04
- 2004/03/05
- 2004/03/06
- 2004/03/07

Down

Page navigation (Day: hour unit) 2004/ 3/ 5 0:00 - 23:59 Client host: wm2003.aoi.pst.fujitsu.com

Order	URL	Request count	Percent(%)	Stay time (sec)
1	/faq/faq_truck.htm	2	25.00	240
2	/faq/faq_fabric.htm	1	12.50	120
3	/faq/faq_truck.htm	1	12.50	0
4	/faq/faq_all.htm	1	12.50	0
5	/faq/faq_fabric.htm	1	12.50	0
6	/faq/faq_truck.htm	1	12.50	0
7	/faq/faq_all.htm	1	12.50	0

Total

Lines of List: 20 Display order: Descending order Advanced analysis destination: Next page

1. For a more detailed analysis of the page navigation status that focuses on a displayed URL page, specify the URL you want to analyze and then select "Next page" or "Previous page" as the drill-down destination.

The screenshot displays the Fujitsu analysis tool interface. On the left, there are several dropdown menus for configuration: 'Analysis target server' (Web .HTTP11), 'Data type', 'Request report', 'Analysis method', 'Client host', 'Analysis period', and 'Unit' (Day: hour unit). A date selector shows dates from 2004/02/24 to 2004/03/07, with 2004/03/05 selected. The main area features a table titled 'Page navigation (Day: hour unit) 2004/ 3/ 5 0:00 - 23:59 Client host: wm2003.aoi.pst.fujitsu.com'. The table data is as follows:

Order	URL	Request count	Percent(%)	Stay time (sec)
1	/faq/faq_truck.htm	2	25.00	240
2	/faq/faq_fabric.htm	1	12.50	120
3	/faq/faq_truck.htm	1	12.50	0
4	/faq/faq_all.htm	1	12.50	0
5	/faq/faq_fabric.htm	1	12.50	0
6	/faq/faq_truck.htm	1	12.50	0
7	/faq/faq_all.htm	1	12.50	0

At the bottom of the table, there are controls for 'Lines of List' (set to 20), 'Display order' (set to Descending order), and 'Advanced analysis destination' (with options for Next page, Next page, and Forward page).

In case of session analysis, the page navigation of the most user's pattern is used as the basis. For example, if the most pattern is:

- A.html
- B.html
- C.html

In this case, if "B.html" is selected, and "Next page" is selected for advanced analysis, the result of next pages for users navigating from "A.html" to "B.html" is displayed in large amount order (the "C.html" is the most). But in case of request analysis, the result has nothing to do with the page navigation patterns to the selected URL. The page navigation pattern analysis from the selected URL is performed on all the page navigation patterns (within the specified period of time).

1. For even greater detail, repeat the process of selecting the above URL and drilling down further.

11.5.3.3 Analyzing site navigation for a specific URL

Use site navigation analysis that focuses on a specific URL to analyze the navigational sequences used to access a URL page that has been made public as Web site content and the origin of access to the URL page.

The following is an example of using site navigation analysis that focuses on a specific URL.

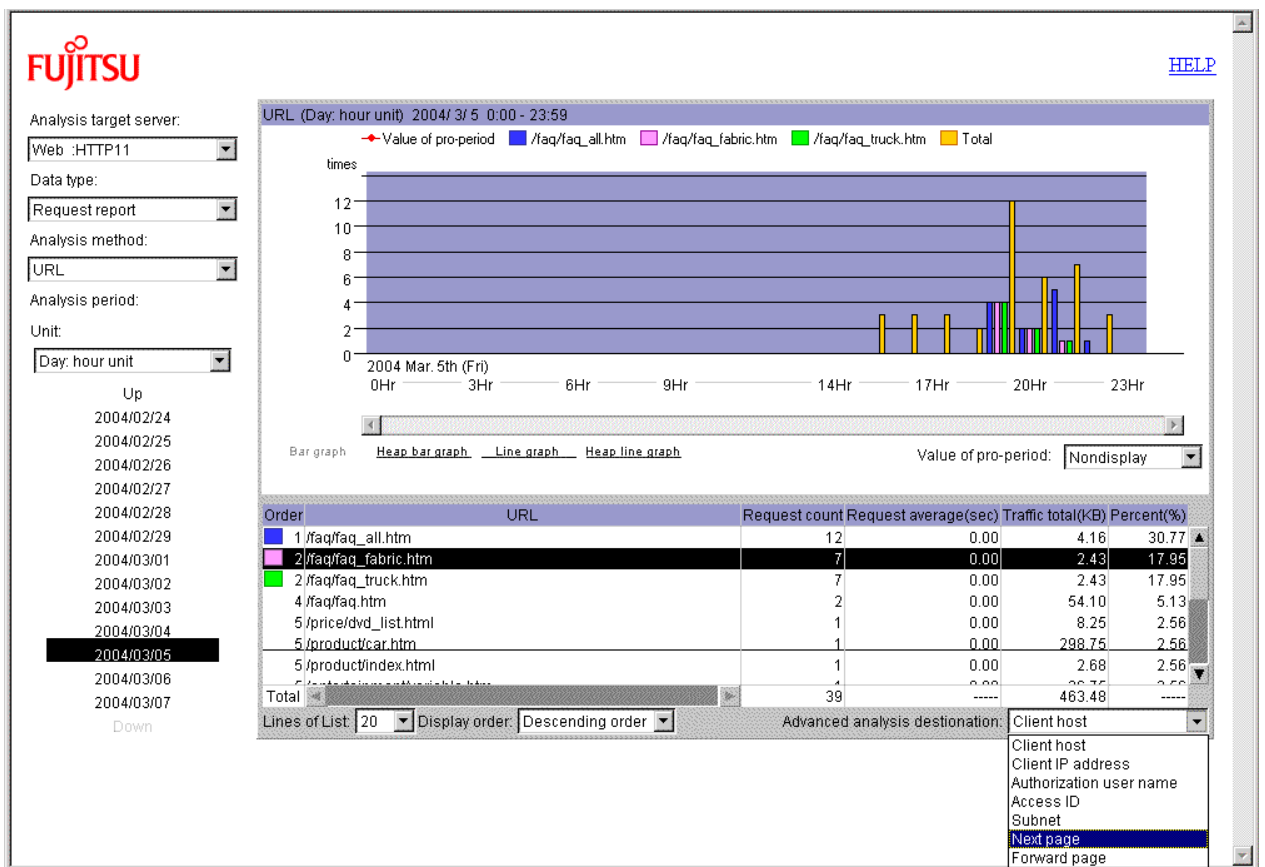
1. Specify the following items on the analysis screen to perform the analysis.

Item	Specification
Analysis data type	Session status

Item	Specification
	Request status
Analysis method	URL base EntryURL base ExitURL base

A list of URLs that matches the specified analysis data type and analysis method is displayed.

- In the displayed URL list, specify the URL you want to analyze and then select "Next page" or "Previous page" as the drill-down destination.



When the analysis is complete, a list of page navigation status (next page or previous page) for the specified URL is displayed.

In case of session analysis, selecting a URL from the result of session analysis for optional method URL or EntryURL leads to the analysis regarding the selected URL as the first URL when user visited the Web site. Similarly, selecting a URL from the result of the session analysis for optional method ExitURL leads to analysis regarding the selected URL as the last URL. But for request analysis, selecting a URL from the result of optional method URL leads to the analysis regarding the selected URL as just one URL while navigating the Web site.

1. Repeat the process of selecting the above URL and drilling down to obtain a more detailed analysis of the page navigation status.

 **Point**

.....

In case of session analysis, the selected URL is used as the destination from the URL selected in the previous advanced analysis. But in case of request analysis, it has nothing to do with the URL that selected for the previous advanced analysis. The analysis is made on all the navigation patterns (within the specified period of time) from the selected URL.

.....

Chapter 12 Evaluating the Usage

The Reporter can be used to evaluate the usage of the Web site.

If the conditions for creating reports to be referenced are registered in advance, the Reporter can be used to evaluate the usage as needed.

Reports created in the past can also be referenced.

This chapter explains how to use the Reporter.

12.1 Registered Report Window

This section provides a function overview of the registered report window and explains how to use the functions.

12.1.1 OutLine

For the Reporter, the conditions for generating reports (hereafter referred to as "the report conditions") must be registered before generating reports.

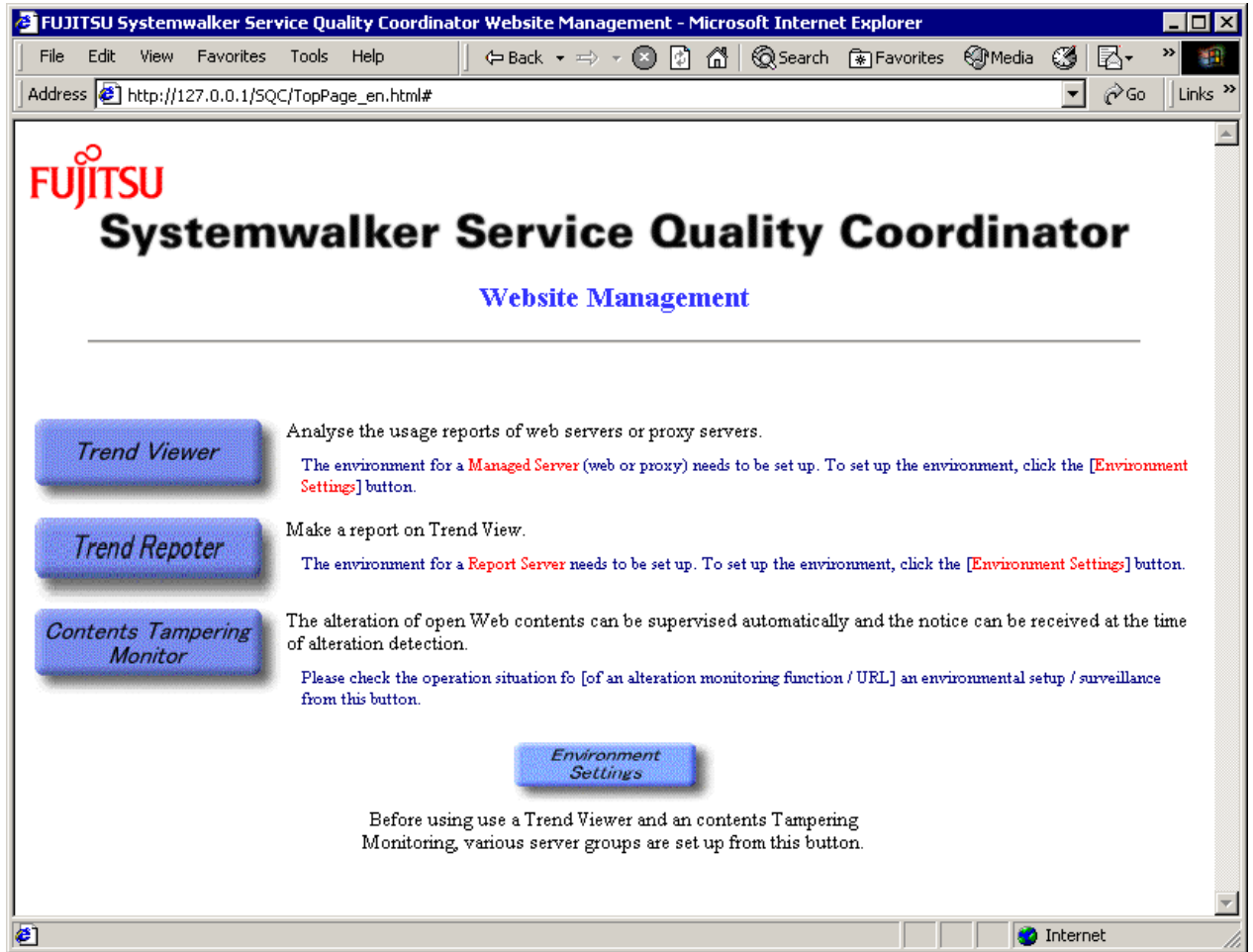
The List of registered reports window lists the report conditions already registered. The window is thus used for report management.

The following functions can be called from this window:

- Registering, editing or deleting the report conditions
- Generating a report according to the registered report conditions
- Referencing reports that were generated previously

12.1.2 Start operation

The registered report window is started by clicking the [Trend Report] button on the top page of the Web Site Management window.



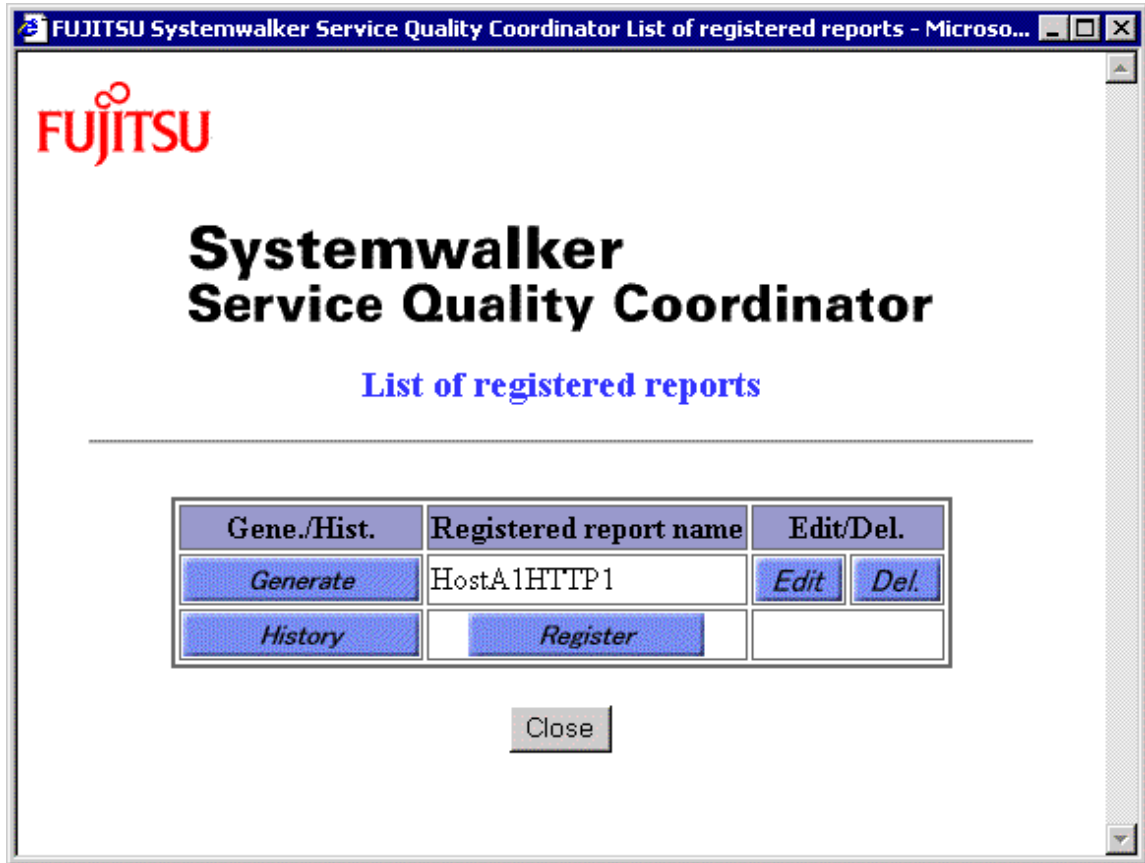
12.1.3 Quit operation

To quit the List of registered reports window, click the [Close] button on the bottom of the window.



12.1.4 Window configuration

This section shows the window configuration of the List of registered reports window and explains the components of the window.



Report table

The report table lists the report conditions already registered.

Each line of the report table corresponds to one set of report conditions and consists of a registered report name and operation buttons for the report conditions.

On the bottom line of the report table, the operation buttons for displaying the report history and registering new report conditions are provided.

Column		Description
Gene./Hist.	Generate	Clicking this button activates the Generate of report window and generates a report based on the report condition. Refer to " 12.3.2 Start operation " for the Generate of report window.
	History	Clicking this button activates the History of reports window displaying the reports that were generated previously. Refer to " 12.4.2 Start operation " for the History of reports window.
Registered report name		The report names registered in the report registration window are listed. Refer to " 12.2.4 Window configuration " of the Registry of report window. To register new report conditions, click the [Register] button on the bottom line. Refer to " 12.2.2 Start operation " for the Registry of report window.
Edit/Del.	Edit	Clicking this button displays the Registry of report window so that the registered report conditions can be edited. Refer to " 12.2.2 Start operation " for the Registry of report window.

Column		Description
	Del.	Clicking this button deletes the corresponding report conditions.

Buttons

Button	Function
Close	Closes the List of registered reports window.

12.2 Registry of report Window

This section provides a function overview of the Registry of report window and explains how to use the functions.

12.2.1 OutLine

The Registry of report window allows the user to:

- Set and register new report conditions.
- Edit and update the contents of the report conditions already registered.

12.2.2 Start operation

To open the Registry of report window:

- Click the [Register] button in the List of registered reports window.
- Click the [Edit] button for the target report conditions in the List of registered reports window.

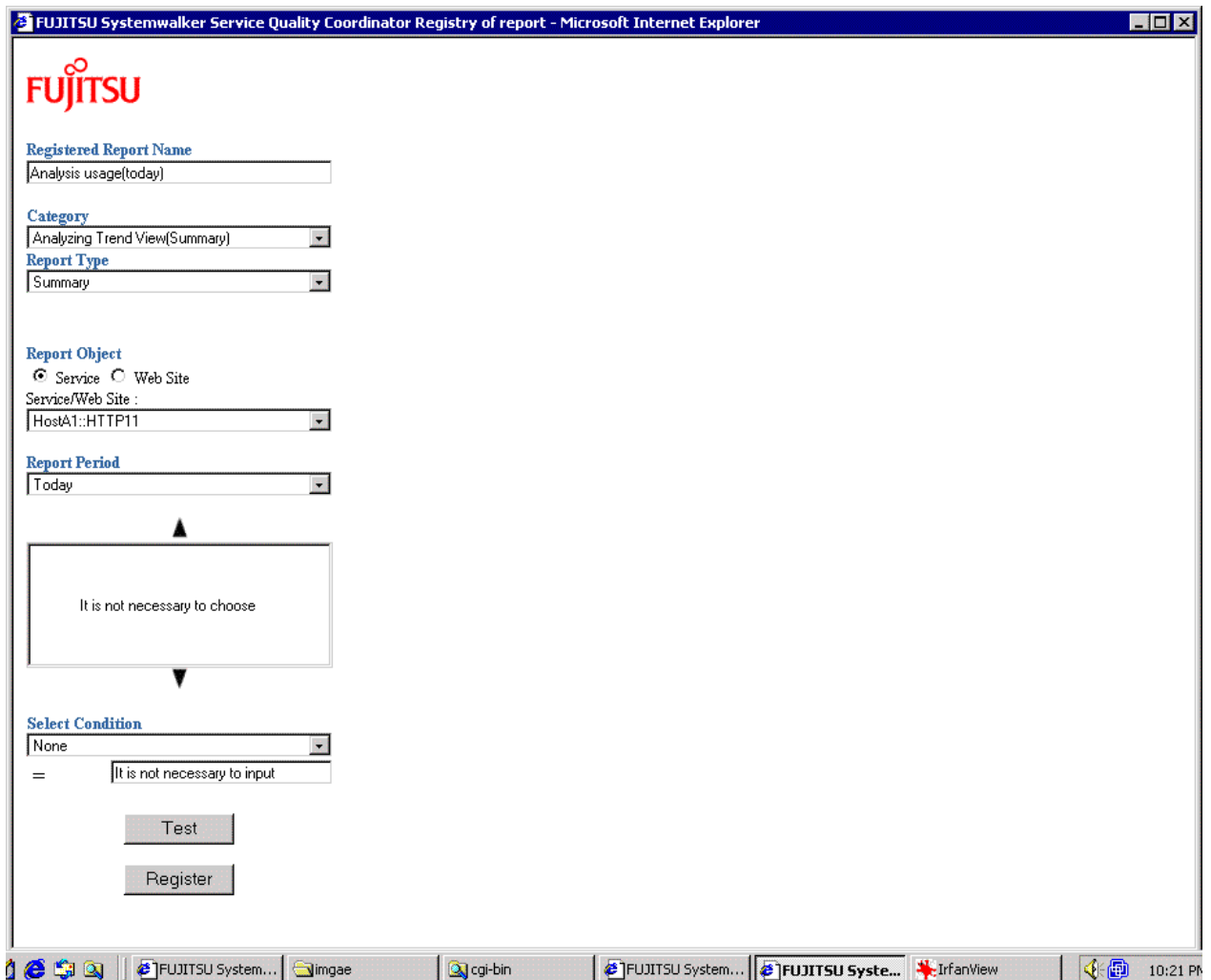


12.2.3 Quit operation

To quit the Registry of report window, close the Web browser that displays the window.

12.2.4 Window configuration

This section shows the configuration of the Registry of report window and explains the components of the window.



Report conditions

Setting item	Description
Registered Report Name	<p>Specify the name to be displayed in the report table in the List of registered reports window.</p> <p>Specify the name with up to 36 alphanumeric characters and/or symbols, excluding the following symbols:</p> <p>\$ " ' [] < > / ? ; : * \ & , . =</p>
Category	<p>Select the report category from the pull-down menu.</p> <p>The following categories can be selected. Refer to "12.5.1 Category and Report type" for details.</p> <ul style="list-style-type: none"> - Analyze usage (Summary) - Analyze usage (Session Report) - Analyze usage (Request Report) - Analyze usage (Traffic Report) - Analyze usage (Cache Report) - Analyze usage (Error Report) - Analyze usage (Response Report)

Setting item	Description
	<ul style="list-style-type: none"> - Analyze usage (Page Navigation Report) - Analyze usage (Actual Visit User Count)
Report Type	<p>Select the report type from the pull-down menu.</p> <p>The pull-down menu lists the report types corresponding to the selected category. Refer to "12.5.1 Category and Report type" for details.</p>
Generation conditions	<p>Set the conditions for generation reports.</p> <p>The settings for the generation conditions vary depending on the combination of the selected category and report type. Refer to "12.5.2 Other report parameters" for details.</p>

Point

.....

If the [Registry of report] window is started by clicking the [Edit] button on the [Registered Report] window, the content registered or edited last time is displayed.

.....

Buttons

Button	Function
Test	<p>Report according to the report condition is displayed on the right side of the window. This is for the checking of the report condition settings.</p> <p>Report is displayed but the history is not added by this operation.</p>
Register	<p>Register the report condition set.</p> <p>If you want to quit the registering, quit the Registry of Report window according to "12.2.3 Quit operation".</p>

12.3 Generate of report window

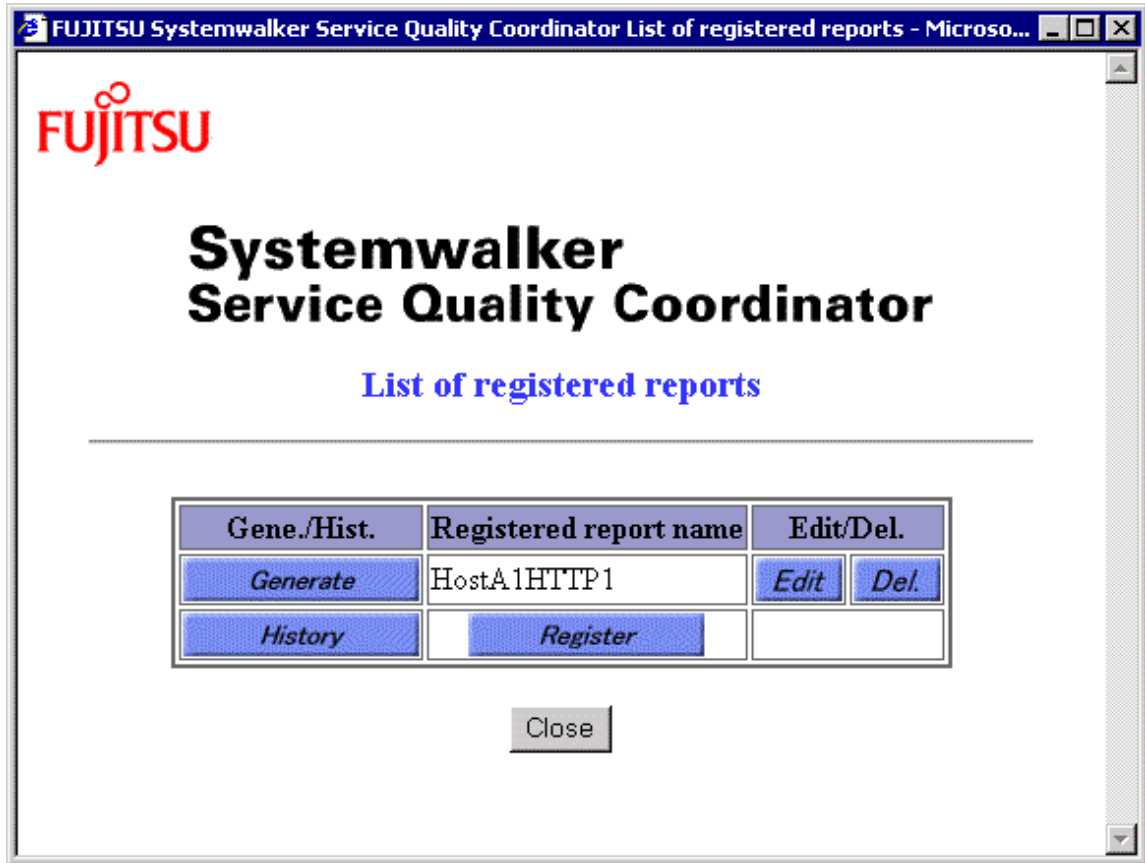
This section provides a function overview of the Generate of report window and explains how to use the functions.

12.3.1 OutLine

The Generate of report window is used to generate a report according to the report conditions that were registered previously.

12.3.2 Start operation

To open the Generate of report window, click the [Generate] button of the target report conditions in the List of registered reports window.

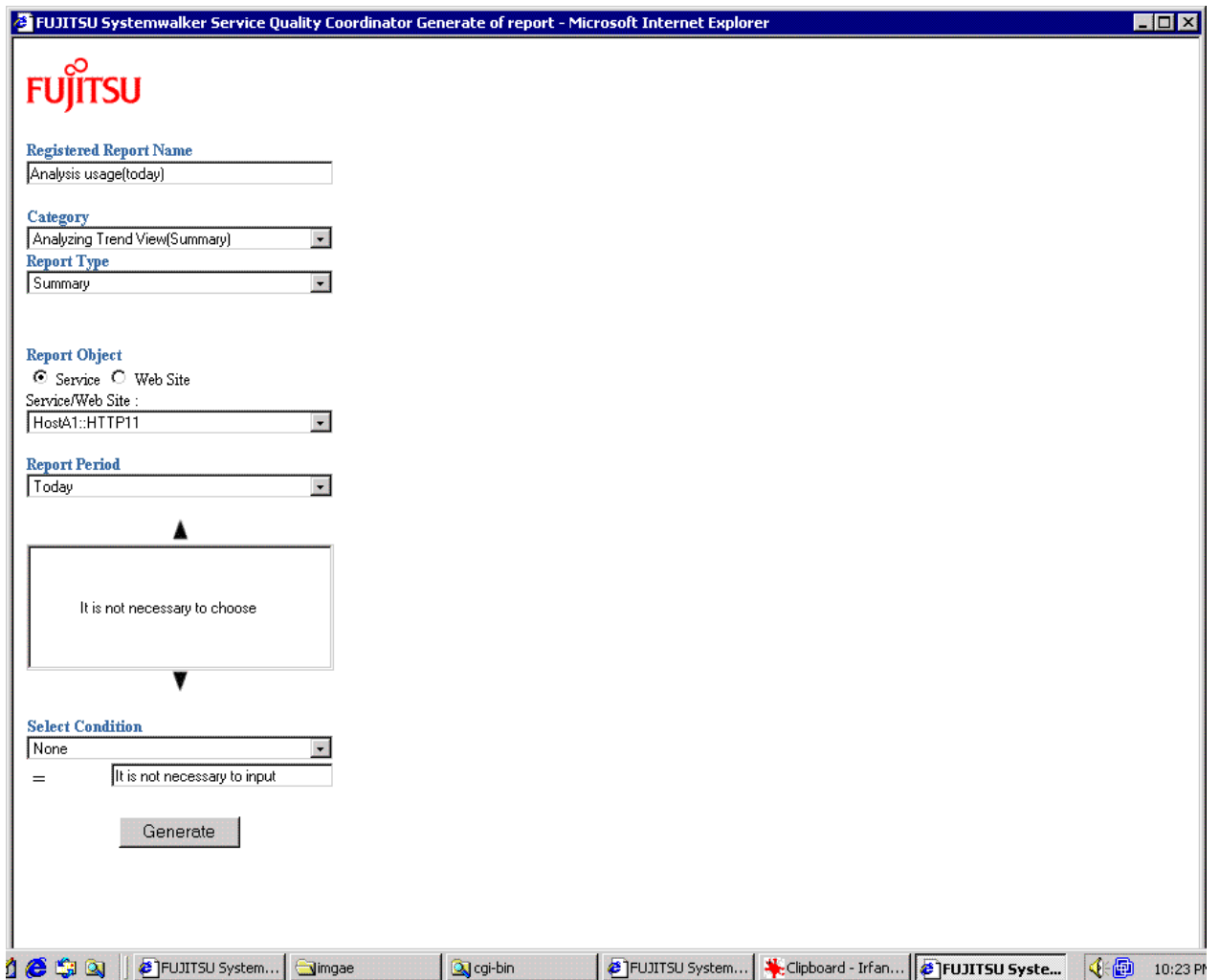


12.3.3 Quit operation

To quit the Generate of report window, close the Web browser that displays the window.

12.3.4 Window configuration

This section shows the configuration of the Generate of report window and explains the components of the window.



Report conditions

The report conditions that were set in the Registry of report window are displayed in the report condition setting items in the Generate of report window.

Of the setting items, the generation conditions can be changed in this window. The settings for the generation conditions vary depending on the combination of the selected category and report type. Refer to "[12.5.2 Other report parameters](#)" for details.

Note

The changes made to the generation conditions in this window are not reflected in the report conditions that were already registered.

Buttons

Button	Function
Generate	Generates a report according to the report conditions. The generated report is displayed on the right side of the window. For the contents of the generated report, refer to " 12.5.3 Report contents ".

12.4 History of Reports Window

This section provides a function overview of the History of Reports window and explains how to use the functions.

12.4.1 OutLine

The History of Reports window is used to display reports that were generated in the past.

12.4.2 Start operation

To open the History of Reports window, click the [History] button in the List of registered reports window.

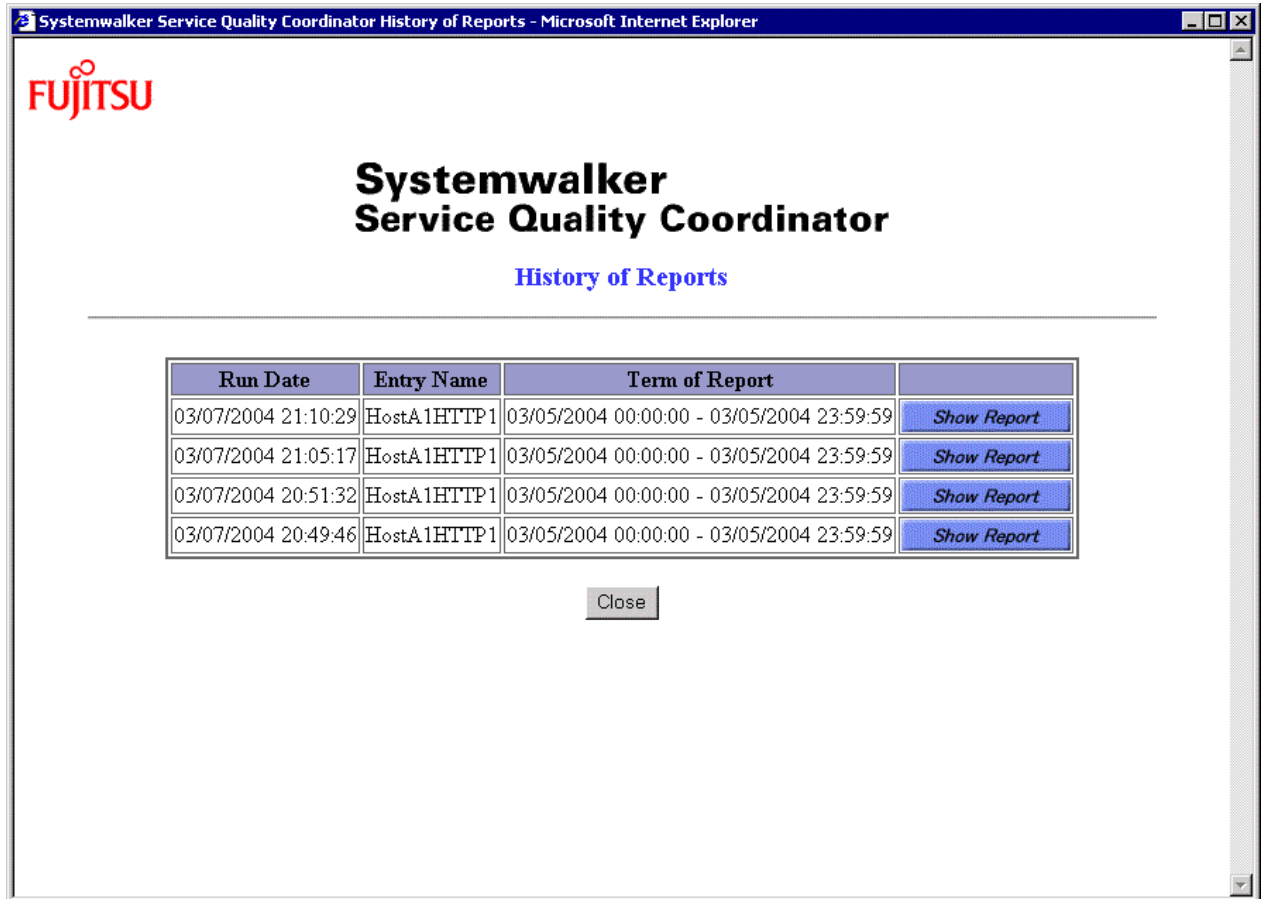


12.4.3 Quit operation

To quit the History of Reports window, click the [Close] button on the bottom of the window.

12.4.4 Window configuration

This section shows the configuration of the History of Reports window and explains the components of the window.




History table

The history table lists the reports that were generated in the past.

Each line of the history table is corresponding to an operation of the report generation.

The history table lists up to 50 reports in order of generation dates beginning from the latest generation date. Older reports than these latest 50 reports are automatically deleted from the oldest reports.

Column	Description
Run Date	The date and time when the report was generated is displayed.
Entry Name	The registered report name of a report that was generated is displayed.
Period of Report	<p>The period selected for generating a report is displayed.</p> <p> Point</p> <p>.....</p> <p>If a relative period of report such as "Yesterday" was selected for report generation, the actual period of report is displayed.</p> <p>.....</p>
Show Report button	<p>Clicking this button opens another window to display a report.</p> <p>For the format of the report displayed, refer to "12.5.3 Report contents".</p>

Buttons

Button	Function
Close	Closes the report history window.

12.5 Report paramters

This section explains the individual reports supported by the Reporter.

12.5.1 Category and Report type

The table below summarizes the categories and the corresponding report types supported by the Reporter.

No	Category	Report type	Outline
1	Analyze usage (Summary)	Summary	A summary of analysis results is output.
2	Analyze usage (Session Report)	Time Segment	Transition in each period is analyzed.
3		Client Host Name	Usage is analyzed for each host name that is obtained by DNS conversion of the client IP address.
4		Client IP Address	Usage is analyzed for each client IP address.
5		Authorization User Name	If authentication is performed on the WWW server or Proxy server, usage is analyzed for each authentication user name.
6		User Agent	Usage is analyzed for each agent that is used by the user who accesses the WWW server or Proxy server.
7		Referrer Host Name	The link that was used to reach the WWW server is reported for each referrer host name.
8		Referrer IP Address	The link that was used to reach the WWW server is reported for each referrer IP address.
9		Remote Host Name	In the Proxy server, usage is analyzed for each host name of the page that was accessed from inside the Proxy server. When the Proxy server is used in reverse operation mode, the WWW server to which a request was made from the outside is reported for each host name.
10		Remote IP Address	In the Proxy server, usage is analyzed for each IP address of the page that was accessed from inside the Proxy server. When the Proxy server is used in reverse operation mode, the WWW server to which a request was made from the outside is reported for each IP address.
11		URL	Usage is analyzed for each URL name that was accessed from clients.
12	Entry URL	Usage is analyzed for each entry URL of the URL that was accessed from clients.	

No	Category	Report type	Outline
13		Exit URL	Usage is analyzed for each exit URL of the URL that was accessed from clients.
14		Referrer URL	The link that was used to reach the WWW service is reported for each referrer URL.
15		Access ID	Usage is analyzed for each ID that was set in Cookie.
16		Directory	Usage is analyzed for each directory using the URL name accessed from clients.
17		Subnetwork	Usage is analyzed for each subnetwork that groups client IP addresses.
18	Analyze usage	Time Segment	Transition in each period is analyzed.
19	(Request Report)	Client Host Name	Usage is analyzed for each host name that is obtained by DNS conversion of the client IP address.
20		Client IP Address	Usage is analyzed for each client IP address.
21		Authorization User Name	If authentication is performed on the WWW server or Proxy server, usage is analyzed for each authentication user name.
22		Remote Host Name	In the Proxy server, usage is analyzed for each host name of the page that was accessed from inside the Proxy server. When the Proxy server is used in reverse operation mode, the WWW server to which a request was made from the outside is reported for each host name.
23		Remote IP Address	In the Proxy server, usage is analyzed for each IP address of the page that was accessed from inside the Proxy server. When the Proxy server is used in reverse operation mode, the WWW server to which a request was made from the outside is reported for each IP address.
24		URL	Usage is analyzed for each URL name that was accessed from clients.
25		URL Extension	Usage is analyzed for each extension (which extensions were frequently accessed).
26		Access ID	Usage is analyzed for each ID that was set in Cookie.
27		Directory	Usage is analyzed for each directory using the URL name accessed from clients as the key.
28		Subnetwork	Usage is analyzed for each subnetwork that groups client IP addresses.
29	Analyze usage	Time Segment	Transition in each period is analyzed.
30	(Traffic Report)	Client Host Name	Usage is analyzed for each host name that is obtained by DNS conversion of the client IP address.

No	Category	Report type	Outline
31		Client IP Address	Usage is analyzed for each client IP address.
32		Authorization User Name	If authentication is performed on the WWW server or Proxy server, usage is analyzed for each authentication user name.
33		Remote Host Name	In the Proxy server, usage is analyzed for each host name of the page that was accessed from inside the Proxy server. When the Proxy server is used in reverse operation mode, the WWW server to which a request was made from the outside is reported for each host name.
34		Remote IP Address	In the Proxy server, usage is analyzed for each IP address of the page that was accessed from inside the Proxy server. When the Proxy server is used in reverse operation mode, the WWW server to which a request was made from the outside is reported for each IP address.
35		URL	Usage is analyzed for each URL name that was accessed from clients.
36		URL Extension	Usage is analyzed for each extension (which extensions were frequently accessed).
37		Access ID	Usage is analyzed for each ID that was set in Cookie.
38		Subnetwork	Usage is analyzed for each subnet that groups client IP addresses.
39	Analyze usage (Cache Report)	Hit Location	Cache hits are analyzed for each hit location.
40	Analyze usage (Error Report)	Error Location	Errors are analyzed for each error location.
41		Server Error Code	Server errors are analyzed for each server error code.
42		Client Error Code	Client errors are analyzed for each client error code.
43		Remote Error Code	Remote errors are analyzed for each remote error code.
44	Analyze usage (Response Report)	URL	Usage is analyzed for each URL name that was accessed from clients.
45		Client Host Name	Usage is analyzed for each host name that is obtained by DNS conversion of the client IP address.
46		Client IP Address	Usage is analyzed for each client IP address.
47	Analyze usage (Page Navigation Report)	Entire Site	Page navigation (in which order the WWW service pages were accessed) is analyzed.
48	Analyze usage	Specified Server	The number of users who actually visited each client IP address per day is reported.

No	Category	Report type	Outline
	(Actual Visit User Count)		

12.5.2 Other report parameters

This section explains the generation conditions to be set in the Registry of report window. The section explains them separately for each category.

12.5.2.1 Common items

This section explains the items common to all categories.

Period of report

Select the period for generating a report.

Upper field

In the upper field, select the period type that represents the period for generating a report from the pull-down menu.

The following period types can be selected. "Today" is selected by default.

Period type	Description
Yesterday	A report for the day before the day on which report generation is executed is generated.
Today	A report for the day on which report generation is executed is generated.
(Select the day from the following)	When generating a report, select the report period from the list of days in the field below.
Last week	A report for the week before the week during which report generation is executed is generated.
This week	A report for the week during which report generation is executed is generated.
(Select the week from the following)	When generating a report, select the report period from the list of weeks in the field below.
Last month	A report for the month before the month in which report generation is executed is generated.
This month	A report for the month in which report generation is executed is generated.
(Select the month from the following)	When generating a report, select the report period from the list of months in the lower field.
(Select the year from the following)	When generating a report, select the report period from the list of years in the lower field.



Some items may not be selected depending on the combination of the selected category and report type.

Lower field

If "(Select the day from the following)" is selected in the upper field, select a specific day from the lower field. The lower field first lists seven days including today beginning from Sunday. To move the range of the days listed in the present field to the past or future, click the move button above or below the field.

If "(Select the week from the following)" is selected in the upper field, select a specific week from the lower field. The lower field first lists seven weeks including this week. To move the range of the weeks listed in the present field to the past or future, click the move button above or below the field.

If "(Select the month from the following)" is selected in the upper field, select a specific month from the lower field. The lower field first lists seven months including this month. To move the range of the months listed in the present field to the past or future, click the move button above or below the field.

If "(Select the year from the following)" is selected in the upper field, select a specific year from the lower field. The lower field first lists seven years including this year. To move the range of the years listed in the present field to the past or future, click the move button above or below the field.



The report period selected from the lower field in the Registry of report window is not reflected in the report conditions. Select the report period again from the lower field in the Generate of report window.

12.5.2.2 Report Object and Select Condition

This section explains the items specific to the following categories:

- Analyze usage (Summary)
- Analyze usage (Session Report)
- Analyze usage (Request Report)
- Analyze usage (Traffic Report)
- Analyze usage (Cache Report)
- Analyze usage (Error Report)
- Analyze usage (Response Report)
- Analyze usage (Page Navigation Report)
- Analyze usage (Actual Visit User Count)

Selecting the service or Web site

Select the object of the report generation by the option button.

Object	Description
Service	Selects the service as the object of the report generation. The service name corresponds to the analysis target server name on the [Use Trend Service Information] window.
Web site	Selects the Web site as the object of the report generation. The Web site includes the server group and service group.



For the managed server and Web site(group), refer to "[Chapter 7 Configuring the Operating Environment](#)".

Name of service, Web site

Select the report target from pulldown menu according to the selected service or Web site.



In the pulldown menu, some items that are not applicable to the selected Category, Reprot Type are also displayed. If those items are selected, Message indicating no data in the period is displayed.

Only the usage analysis services of the managed server in management operation can become the report target. In case of managed server operation, even if selected from the pulldown menu, the message indicating no data in the period is displayed.

Focusing conditions

When a report is generated, data that satisfy the condition specified by the focusing conditions is analyzed.

The focusing condition is specified in the following form:

- "Analysis method" = "Value"

Select the analysis method from the pull-down menu.

Specify by inputting the value directly that you want to focus about the specified analysis method.

The specification examples are as follows:

- When the analysis method is "client IP address":

Specify "198.51.100.1."

In this case, a report is generated about the accesses from the user whose client IP address is "198.51.100.1".

- When the analysis method is "URL":

Specify "/SQC/TopPage_en.html."

In this case, a report is generated about the accesses to URL "/SQC/TopPage_en.html."

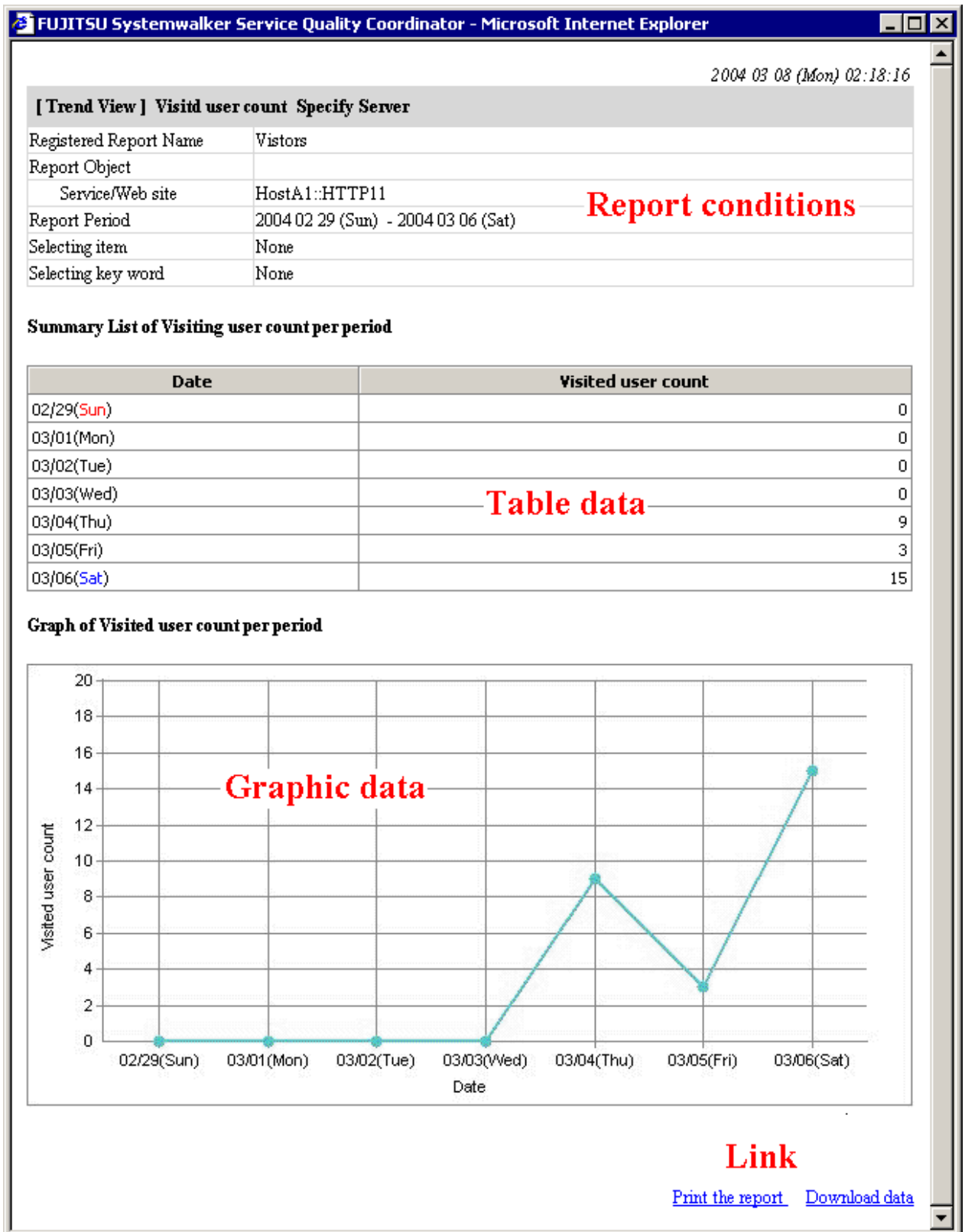


When you specify the focusing condition, a report is generated on the data exactly the same as the specified characters.

Wild card cannot be specified.

12.5.3 Report contents

This section explains the format of a report generated in the Generate of report window.



Report conditions

The contents of the report conditions set when generating a report in the Generate of report window are displayed.

Graphical data

Data collected and analyzed according to the report conditions is displayed in graphical format.

The displayed type of the graph and the number of graphs vary depending on the combination of the selected category and report type.

Table data

Data collected and analyzed according to the report conditions is displayed in a table form.

The displayed table items vary depending on the combination of the selected category and report type.

Link

Link	Description
Print report	Clicking this link to print the report.
Download data	Clicking this link to download the data used for report generation as a CSV file. If it does not work, right-click the link and select "Save to file" or "Save the link as" from the menu to download the data. For the CSV file format, refer to " 15.3.1 Report data file ".

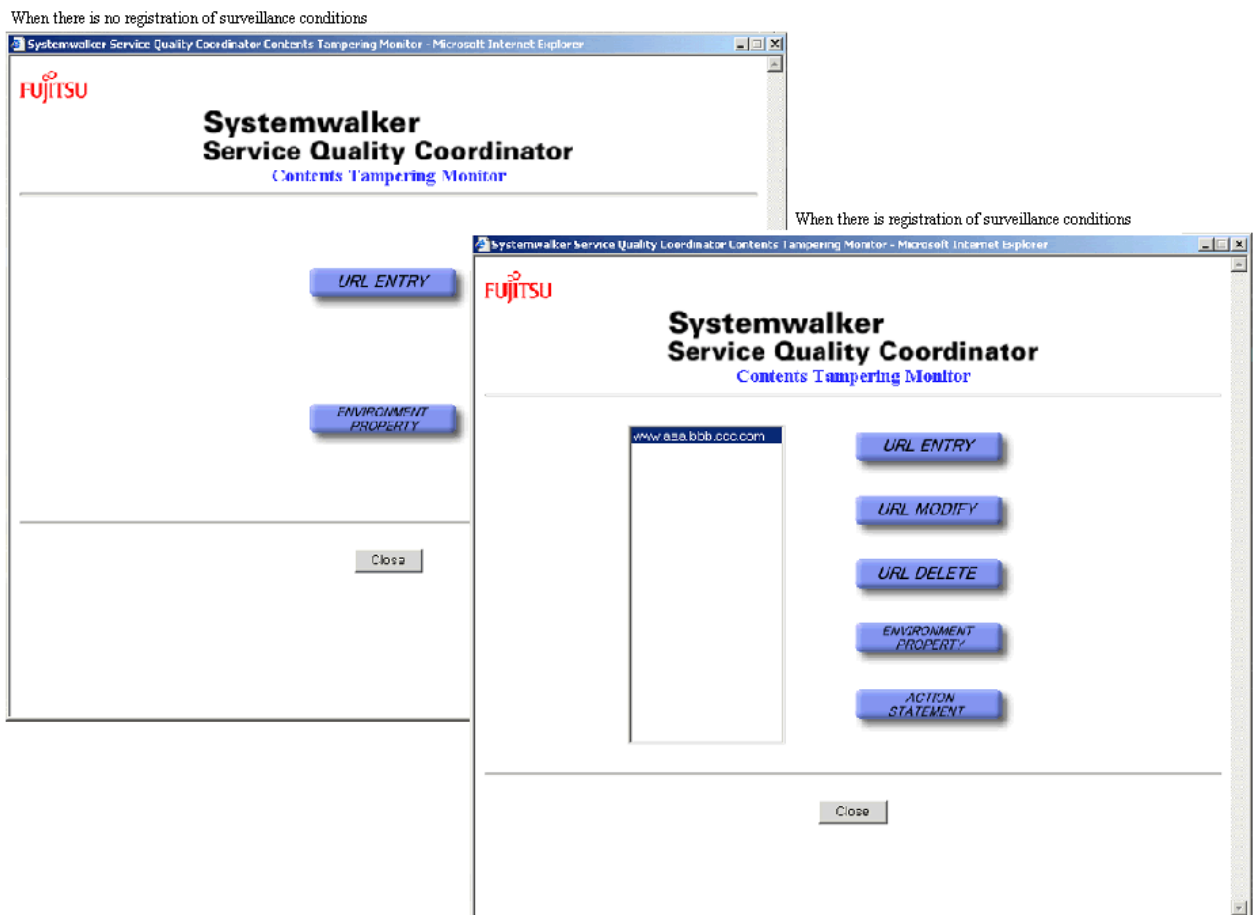
Chapter 13 Using the Contents Tampering Monitor

The system administrator can use the Contents Tampering Monitor to automatically monitor tampering with Web contents (hereafter referred to as contents) and receive messages if tampering is detected.

This chapter explains how to use the Contents Tampering Monitor.

13.1 Viewing the Environment Settings Window

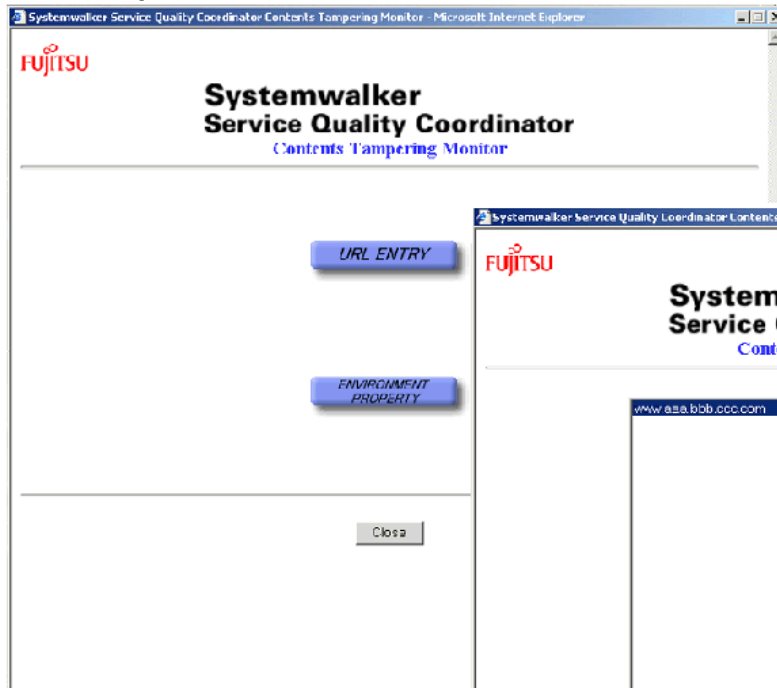
Environment Settings window for tamper monitoring can be opened from the Management Console window on the Management Server. Click the "Environment Settings" button in the Management Console window to display the Environment Settings window, and then click the "Contents Tampering Monitor" button.



13.1.1 Contents Tampering Monitor window (menu window)

The Contents Tampering Monitor window, which is a menu window for tamper monitoring, appears. The window configuration varies depending on whether monitoring conditions have been registered.

When there is no registration of surveillance conditions



When there is registration of surveillance conditions



[URL ENTRY] button

Displays the "[13.1.2 Tamper Monitor URL Entry window](#)".

Use this button when registering new monitoring conditions.

[URL MODIFY] button

Displays the "[13.1.3 Tamper Monitor URL Modify window](#)".

Use this button when modifying monitoring conditions already registered.

[URL DELETE] button

Displays the "[13.1.4 Confirm URL Delete window](#)".

Use this button when deleting monitoring conditions already registered.

[ENVIRONMENT PROPERTY] button

Displays the "[13.1.5 Environment Properties window](#)".

Use this button when defining the operating environment for the Contents Tampering Monitor.

[ACTION STATEMENT] button

Displays the "[13.1.6 Action Statement window](#)".

Use this button when checking the tamper checking status.

List

The URLs that represent the monitoring conditions already registered are listed.

When modifying or deleting monitoring conditions already registered, specify the URL that represents the target monitoring conditions.

13.1.2 Tamper Monitor URL Entry window

The Tamper Monitor URL Entry window is used to register monitoring conditions.

Systemwalker Service Quality Coordinator Tamper Monitor URL Entry - Microsoft Internet Explorer

FUJITSU

**Systemwalker
Service Quality Coordinator**
Tamper Monitor URL Entry

Tamper Monitor URL: http:// www.aaa.bbb.ccc.com

Mode: include under the directory

Frequency: Once daily Once hourly

Tamper Monitor directory: /var/www/public

Alert E-mail Address: manager1@aaa.bbb.ccc.com

CC: manager2@aaa.bbb.ccc.com

Send Log Path: C:\logs\mail.log

OK Reset Cancel

Tamper Monitor URL

Specify the URL of the content or the directory containing the content. If a directory is specified, the content right under the directory is to be monitored.

Specify the URL up to 1,023 characters excluding the following:

^ | [] { } < > () & \$ # " ' * , ?

Example 1: To specify content

http://www.fujitsu.com/index.html

Example 2: To specify a directory

http://www.fujitsu.com/



The URL specified here is used as to represent monitoring conditions in the Contents Tampering Monitor window, Action Statement window and the detection notification.

Mode

If this check box is selected when a directory is specified in [Tamper Monitor URL], all contents under the directory are to be monitored.

Frequency

Specify the frequency of tamper checking.

Tamper Monitor directory

Specify the absolute path of the file or directory on the Web server machine corresponding to the URL specified in [Tamper Monitor URL].

Specify the path up to 1,023 characters excluding the following:

`^|[]{} <>() & $ # " ' * , ?`

[Windows]

Example 1: To specify a file

`C:\www\index.html`

Example 2: To specify a directory

`C:\www`

[UNIX]

Example 1: To specify a file

`/var/www/index.html`

Example 2: To specify a directory

`/var/www`

Alert E-mail Address

Specify only one E-mail address to which a tamper detection notification is to be sent.

Specify the E-mail address up to 1,023 characters excluding the following:

`^|[]{} <>() & $ # " ' * , ?`

CC

Specify the E-mail address to which a copy of tamper detection notification is to be sent as needed. If two or more addresses are specified, delimit them with a semicolon(;).

Specify the E-mail address up to 1,023 characters excluding the following:

`^|[]{} <>() & $ # " ' * , ?`

Example: To specify two E-mail addresses

user1@fujitsu.com;user5@fujitsu.com

Send Log Path

If the send log file for tamper detection notification is to be changed from the default to another, specify the absolute path of the new file.

Specify the path up to 1,023 characters excluding the following:

^[] { } < > () & \$ # " ' * , ?

The default send log file is as follows:

[Windows]

Example:

<installation directory>\etc\seq\log\send.log

[UNIX]

Example:

/etc/opt/FJSVssqc/seq/log/send.log

Point

.....
The default send log file is renamed to send.log~ (past log is deleted) every time the amount of logged data exceeds a given level. The default log file thus contains only the recent log. To retain the past log, change the send log file from the default to another.
.....

13.1.3 Tamper Monitor URL Modify window

The Tamper Monitor URL Modify window is used to modify monitoring conditions already registered.

Systemwalker Service Quality Coordinator Tamper Monitor URL Modify - Microsoft Internet Explorer

FUJITSU

Systemwalker Service Quality Coordinator

Tamper Monitor URL Modify

Tamper Monitor URL: http:// www.aaa.bbb.ccc.com

Mode: include under directory

Frequency: Once daily Once hourly invalidity

Tamper Monitor directory:

Alert E-mail Address:

CC:

Send Log Path:

OK Reset Cancel

[Tamper Monitor URL]

The URL registered for monitoring is displayed.

[Mode]

Refer to [Mode](#) in the Tamper Monitor URL Entry window.

[Frequency]

Specify the frequency of tamper checking. If "invalidity" check box is selected, checking is stopped with the registered information left as is.

[Tamper Monitor directory]

Refer to [Tamper Monitor directory](#) in the Tamper Monitor URL Entry window.

[Alert E-mail Address]

Refer to [Alert E-mail Address](#) in the Tamper Monitor URL Entry window.

[CC]

Refer to [CC](#) in the Tamper Monitor URL Entry window.

[Send Log Path]

Refer to [Send Log Path](#) in the Tamper Monitor URL Entry window.

13.1.4 Confirm URL Delete window

The Confirm URL Delete window is used to delete monitoring conditions already registered.



13.1.5 Environment Properties window

The Environment Properties window is used to set the environment for sending tamper detection messages.



[Host Name]

Specify the host name of the SMTP server.

Specify the host name up to 1,023 characters excluding the following:

`^|[]{} <>() & $ # " ' * , ?`



Note

Be sure to use the default value (25) for the port number of the SMTP server

[Sender E-mail Address]

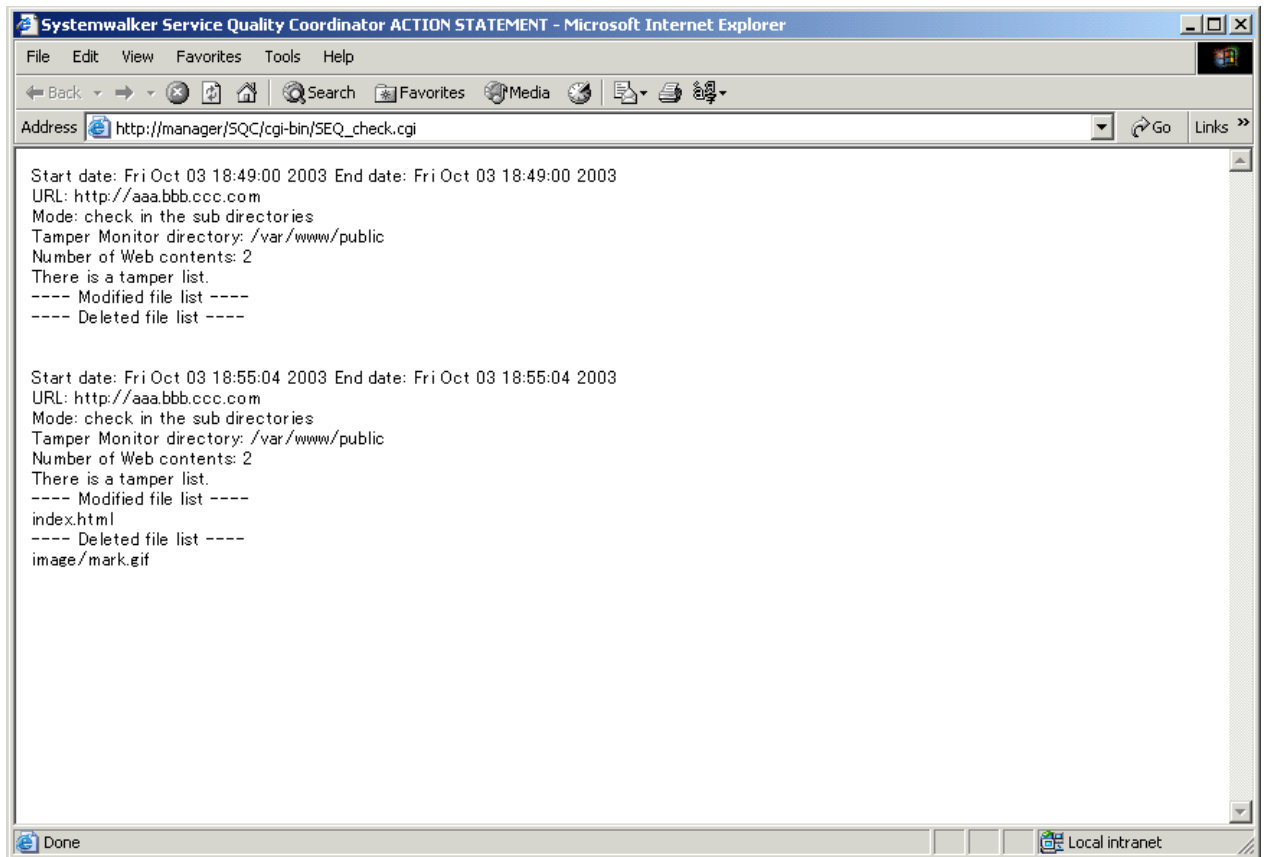
Specify the sender E-mail address to be included in tamper detection messages.

Specify the address up to 1,023 characters excluding the following:

`^|[]{} <>() & $ # " ' * , ?`

13.1.6 Action Statement window

The Action Statement window is used to check how tamper checking has been performed. This window displays the cumulative records of checking results in chronological order. The following example shows the results of tamper checking over one monitoring condition.



Start date

This is the date and time when tamper checking started.

End date

This is the date and time when tamper checking ended.

URL

This is [Tamper Monitor URL](#) registered as a monitoring condition.

Phase

If check for monitoring conditions was executed separately, a serial number is indicated.

Tamper checking is basically performed with a monitoring condition as a unit. However, if the number of contents included in the monitoring conditions exceeds a given level, the given level becomes a unit. The serial number is displayed. The phase is not displayed if the number of contents included in the monitoring conditions do not reach the given level.

Mode

This is [Mode](#) registered as a monitoring condition.

Tamper Monitor directory

This is [Tamper Monitor directory](#) registered as a monitoring condition.

Note

If [Tamper Monitor directory](#) is not found at Tamper checking, the following message is displayed and the below items are not displayed.

"Tamper Monitor directory is not found."

Number of Web contents

This is the total number of contents included in the monitoring conditions. If [Phase] is displayed, it is the number of contents to be checked with the check as a unit.

Modified file list

This is the list of the contents that might have been tampered (modified).

Deleted file list

This is the list of the contents that might have been tampered (deleted).

13.2 Tampering Detection Notice

Tamper detection notices are given by the following ways:

- E-mail notice
- Event message

An event message is the message outputted to the system log.

For the message contents, refer to "[17.1.3 Tampering inspection program](#)."

Note

If a tamper detection notice is given, confirm the contents on the Web server and take action properly.

13.2.1 E-mail notice

When the [Alert E-mail Address](#) had been set as a monitoring condition, if a tamper is detected, an E-mail is sent to the address. The following is an example of an E-mail notice.

```
From: ssqc@aaa.bbb.ccc.com
Subject: The notice of a contents tamper

URL: http://www.aaa.bbb.ccc.com (Phase 2)
Tamper Monitor directory: /var/www/public
Start date: Mon Apr 01 10:00:07 2002
End date: Mon Apr 01 10:00:21 2002
Number of tampered files: 2

Tampered file list

image/mark.gif code: 2
index.html code: 1

code:
  1: Web contents is modified.
  2: Web contents is deleted.
```

URL

This is [Tamper Monitor URL](#) registered as the monitoring conditions.

Phase

If check for monitoring conditions was executed separately, a serial number is indicated.
Tamper checking is basically performed with a monitoring condition as a unit. However, if the number of contents included in the monitoring conditions exceeds a given level, the given level becomes a unit. The serial number is displayed. The phase is not displayed if the number of contents included in the monitoring conditions do not reach the given level.

Start date

This is the date and time when tamper checking started.

End date

This is the date and time when tamper checking ended.

Tamper Monitor directory

This is [Tamper Monitor directory](#) registered as a monitoring condition



.....
If [Tamper Monitor directory](#) is not found at Tamper checking, message is displayed after End date and the below items are not displayed.

"Tamper Monitor directory is not found."
.....

Number of tampered files

The number of contents that might have been tampered.

code

This is the code that indicates the type of tamper. The meaning of the code is provided after the file list.

13.3 Customization

13.3.1 If you would like to make tampering inspection with a shorter interval

As the standard, the shortest frequency of tamper checking is once per hour. If the user wants to shorten the interval, customize the frequency of checking on the Management Server as follows:

1. Open the "[13.1.2 Tamper Monitor URL Entry window](#)" or "[13.1.3 Tamper Monitor URL Modify window](#)" and set the [Frequency] to [Once hourly].
2. Open the start control definition file dmcoll.ini using a text editor, and change the value of the polling parameter, which indicates the start interval in the section [SEQ], to the desired value.

The path of dmcoll.ini is as follows:

[Windows]

```
< variable file storage directory >\control\data\dmcoll.ini
```

[UNIX]

```
/etc/opt/FJSVssqc/data/dmcoll.ini
```

One of the following values (in minutes) can be specified for the polling parameter:

5, 10, 20, 30, 60

3. Restart the start control.

The restart procedure is as follows:

[Windows]

Open the service window on the control panel. Stop the next service and then restart it.

Systemwalker SQC sqcschdle

[UNIX]

Execute in the following order:

```
# /opt/FJSVssqc/bin/ssqsch stop
```

```
# /opt/FJSVssqc/bin/ssqsch start
```

1. Check the results in the "[13.1.6 Action Statement window](#)".

13.3.2 If you would like to make tampering inspection at an optional time

As a standard, the tamper checking is scheduled once a day or once per hour. However, the user can perform tamper checking when desired. Do the following on the Management Server:

1. Directly run the tamper checking program (tamper_detect.exe command).

The procedures to run the program are as follows:

[Windows]

```
C:> <installation directory>\bin\tamper_detect.exe
```

[UNIX]

```
# /opt/FJSVssqc/bin/tamper_detect.sh
```

2. Check the results in the "[13.1.6 Action Statement window](#)".

Part 5 References

Chapter 14 Setting the Web Site Management Window.....	195
Chapter 15 SQC file types.....	214
Chapter 16 Troubleshooting.....	259
Chapter 17 Messages.....	268
Chapter 18 Command Reference.....	278
Chapter 19 Environment Maintenance.....	286

Chapter 14 Setting the Web Site Management Window

The necessary settings for management server can be performed with the [Environment Settings] window, which is started from the [Web Site Management] window.

Specifying the following URL with a Web browser can start the [Web Site Management] window.

[Windows]

When the Management Server is a Windows version:

```
http://management server host name/SQC/default.htm
```

[UNIX]

When the Management Server is a Solaris or Linux version:

```
http://management server host name/SQC/index.html
```

Point

.....
If the Management Server is used in cluster operation mode, specify the virtual address (logical IP address or host name) for the host name of the Management Server.

Enterprise Edition provides the cluster operation function.
.....



Click the [Environment Settings] button to display the environment setting window.

14.1 Environment Settings Window


Settings for services and group of managed servers can be performed with the environment settings window.



This section explains how to make settings for servers and group settings for Managed Servers.



Explanation of buttons

The table below summarizes the usage of the buttons that can be selected from the Environment Settings window.

Button	Usage
Management Server	<p>Used to set information about the host in which the Management Server is installed and about the Default Proxy Server used in the environment managed by Systemwalker Service Quality Coordinator.</p> <p> Point</p> <p>.....</p> <p>Always make this setting before using each function.</p> <p>For the setting procedure, refer to "14.1.1 Management Server Settings window".</p> <p>.....</p>
Managed server	<p>Settings for management target servers and for those analysis target servers what should be registered to the managed servers (in order to use all sorts of functions) can be performed.</p> <p>Agent is installed on some Managed Servers and not installed on other Managed Servers.</p>


Button	Usage
	 Point Always make this setting after a server to be managed is added. For the setting procedure, refer to " 14.1.2 Managed server setting window ".
Group	Settings for grouping the analysis target servers that registered to the managed servers can be performed. For the setting procedure, refer to " 14.1.4 Group Settings window ".
Report Server	Used to sets information about the host in which a Report Server is installed, in the Report Server Settings window.  Point Always make this setting before using each function. For the setting procedure, refer to " 14.1.3 Report Server Settings window ".


14.1.1 Management Server Settings window

In the Management Server Settings window, set information on the host in which the Management Server is installed and on the Default Proxy Server used in the environment managed by Systemwalker Service Quality Coordinator.



Information setting items

Item	Requirement	Description
(Management Server) Address	You must set.	Specify the IP address or host name of the Management Server. When the Management Server runs in a cluster, specify a virtual address (logical IP address or logical host name) common to the active and standby systems. Set for each servers in case of doubled management server operation.  Note This item cannot be changed after a Managed Server is added. If the setting for this item needs to be changed, delete all managed servers.
(Management Server) Port	You do not have to set.	Specify the port number of the Web server that runs on the Management Server. This item need not be set if default port number 80 is used.

Item	Requirement	Description
		 Note This item cannot be changed after a Managed Server is added. If the setting for this item needs to be changed, delete all Managed Servers.
(Default Proxy Server) Address	You do not have to set.	If a Default Proxy Server is used in the environment managed by Systemwalker Service Quality Coordinator, specify the IP address or host name of the Default Proxy Server.
(Default Proxy Server) Port	You do not have to set.	If a Default Proxy Server is used in the environment managed by Systemwalker Service Quality Coordinator, specify the port number of the Default Proxy Server.

 **Point**

.....
Information on default proxy server is used only when the proxy server for the specific managed server is not specified.
.....

Window manipulation buttons

Button	Function
Apply	Applies the information specified for the items and closes the window.
Reset	Restores the item values to those with which the window opened.
Cancel	Closes the window without applying the information specified for the items.

14.1.2 Managed server setting window

In the Managed Server Settings window, set information on the server to be managed and on the services that are registered in the server to use each function.

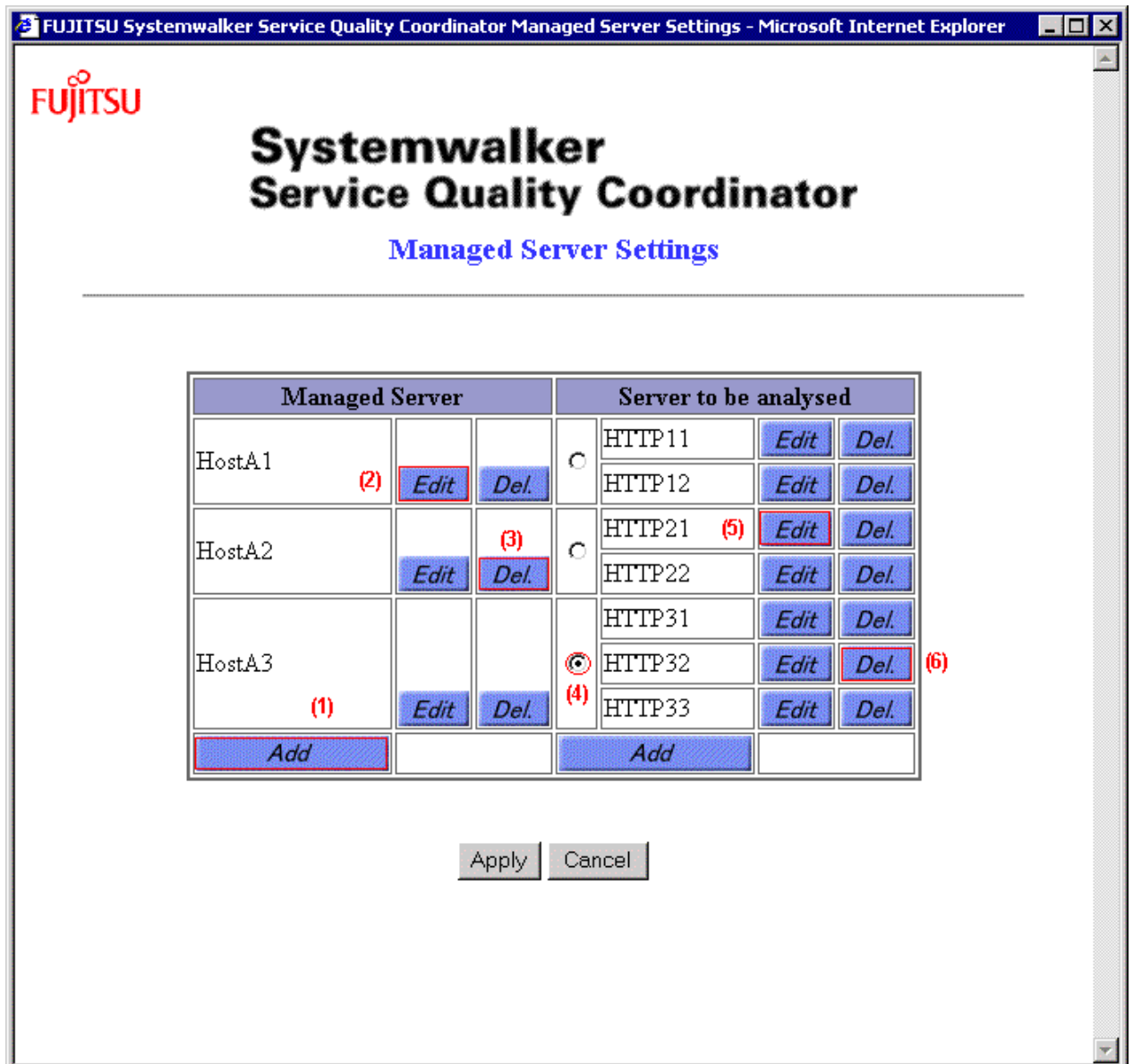


Table components

The table below summarizes the columns of the table displayed in the Managed Server Settings window.

Column	Description
Managed Server	The names of added Managed Servers are listed.
Target Server	Analysis target server names for usage analysis function added to the managed servers are displayed.

Operation for changing information

To change the information set for the managed server and target server, do as follows:

Processing	Operation	Number in figure
Adding a Managed Server	Click the [Add] button on the bottom of the Managed Server column. An empty 14.1.2.1 Managed Server Information window appears.	(1)
Editing Managed Server Information	Click the [Edit] button on the right side of the Managed Server to be edited. 14.1.2.1 Managed Server Information window having the current settings appears.	(2)
Deleting a Managed Server	Click the [Del.] button on the right side of the Managed Server to be deleted. The entry of the Managed Server disappears.	(3)
Adding a target server	Select the option button on the right side of the Managed Server for which a target server is to be added, and click the [Add] button on the bottom of the Target Server column. If the "Service Quality Coordinator Agent" check box for the Managed Server on which the target service is registered is cleared, "Use trend" is not displayed in the pull-down menu in the Service Type Select window.	(4)
Editing target server information	Click the [Edit] button on the right side of the service to be edited. 14.1.2.2 Usage service information window having the current settings appears.	(5)
Deleting a target server	Click the [Del.] button on the right side of the service to be deleted. The entry of the service disappears.	(6)

Window manipulation buttons

Button	Function
Apply	Applies the changes made in this window and in various information windows opened from this window, and closes the window.
Cancel	Closes the window without applying the changes made previously. If this button is clicked after a change is made, a prompt message appears asking whether to close the window without applying changes.

Note

To close this window, use the [Apply] or [Cancel] button.

If these buttons are not used, a temporary file remains in the work area on the Management Server.

Information

For information on how to delete the remaining temporary file, refer to "[14.1.5.1 Deleting unnecessary temporary files](#)".

14.1.2.1 Managed Server Information window

In the Managed Server Information window, set information on the servers that are managed by Systemwalker Service Quality Coordinator.

FUJITSU

Systemwalker Service Quality Coordinator

Managed Server Information

- Basic information

Server name

IP address

Subnet mask

Proxy Server

If the proxy server check box is selected, communication between the manager and agent is performed via the proxy server.
Specify the proxy server address and port below; otherwise, the default proxy server defined in the Management Server settings window is used.

Address

Port

- Attributes of Managed Server

Service Quality Coordinator Agent


Server where the Agent is installed.

Agent URL


**Example: "http://HOST[:PORT]/ALIAS/"*



Information setting items

Basic information

Item	Requirement	Description
Server name	You must set.	<p>Specify the Managed Server entry name.</p> <p>The server name must be unique among all managed servers.</p> <p>You cannot specify two or more character string that becomes same when if upper/lower characters are not distinguished.</p> <p>You cannot modify the server name of the existing managed server to the character string that becomes same when if upper/lower characters are not distinguished. If specified, registered in advance character-line is used.</p> <p>Specify the server name up to 64 alphanumeric characters and/or symbols, excluding the following:</p> <p>\$ \ " ' , : [] < > = &</p> <p>All of server name cannot be specified in number. One or more English letter must be included in the server name.</p> <p> Note</p> <p>.....</p> <p>If the name of a server that has been running is changed, past data can no longer be collected such as by the report display function.</p> <p>.....</p>
IP address	You must set.	Specify the IP address of the Managed Server.
Subnet mask	You must set.	Specify the subnet mask of the Managed Server.
Proxy Server	You do not have to set.	Select the check box if a Proxy Server is used for communication between the manager and agent.
(Proxy Server) Address	You do not have to set.	<p>Specify the address of the Proxy Server that is used specifically for this managed server.</p> <p>If the address is not specified, the default Proxy Server address in the Management Server Settings window is used.</p>
(Proxy Server) Port	You do not have to set.	<p>Specify the port of the Proxy Server that is used specifically for this Managed Server.</p> <p>If the port is not specified, the Default Proxy Server port in the Management Server Settings window is used.</p>

Attributes of managed server

Item	Requirement	Description
Service Quality Coordinator agent	You do not have to set.	<p>Select the check box if Systemwalker Service Quality Coordinator is installed.</p> <p> Point</p> <p>.....</p> <p>If this check box is not selected, the lower two settings are disabled.</p> <p>.....</p>

Item	Requirement	Description
Agent URL	You do not have to set.	<p>Specify the alias URL for the Web server that has been set in the environment settings for the managed server. Use the following format for this setting:</p> <p>"http://host[:port]/alias/"</p> <p>For the "host" part, set either the IP address or the host name (including the domain). Also, if the Web server on the managed server is using a port number other than the well-known port (80), the "port" specification must be made as well.</p> <p> See</p> <p>.....</p> <p>Refer to "4.1 Settings for Web Server", for details on the Web server settings for the managed server.</p> <p>.....</p> <p> Note</p> <p>.....</p> <p>This item cannot be changed if analysis target server is added. If it needs to be changed, delete all use trend services.</p> <p>.....</p>

Window manipulation buttons

Button	Function
OK	Ends specifying data for items and closes the window.
Reset	Restores the item values to those with which the window opened.
Cancel	Closes the window without applying the information specified for the items.

14.1.2.2 Usage service information window

In the Use Trend Service Information window, set information on each Web log subjected to the Trend Viewer.



Information Setting Item

Item	Requirement	Description
Target server name	You must set.	<p>Specify the name of the server to be analyzed.</p> <p>The analysis target server name must be unique throughout the use trend services regardless of the Managed Server for which a service is added.</p> <p>You cannot specify two or more character string that becomes same when if upper/lower characters are not distinguished as the analysis target server.</p> <p>If specified, it is recognized as used. You cannot modify the analysis target server name of the existing service to the character string that becomes same when if upper/lower characters are not distinguished.</p> <p>If specified, the registered in advance is used.</p>

Item	Requirement	Description
		<p>Specify the server name up to 20 alphanumeric characters and/or symbols, excluding the following: \$ \ ' , : [] < > = & All of analysis target server name cannot be specified in number.</p> <p>One or more English letter must be included in the analysis target server name.</p> <p>The specified name must match the character string specified for "Name" in the use trend database environment definition file that is used when the Trend Viewer is defined.</p> <p>For details of the use trend DB environment definition file, refer to "15.2.1 Usage DB Environment Definition File".</p>
Use trend database location	You must set.	<p>Specify whether the use trend DB for the use trend service is to be managed on the Managed Server or Management Server.</p> <p>If the service is entered in a group, select Management Server.</p> <p>This item cannot be changed after the service is entered in a group.</p> <p>If the item needs to be changed, exclude the service from the group.</p> <p>For information on the use trend DB management location, refer to "2.1.1 Locating methods of the analysis data".</p> <p>This item must match the "DatabaseMode" item in the use trend DB environment definition file on the Managed Server.</p> <p>For details of the use trend DB environment definition file, refer to "15.2.1 Usage DB Environment Definition File".</p>
Use trend database port	You must set.	<p>The use trend database port is usually 2365. Change this setting if this has been changed to any other port number. Otherwise, there is no need to change the default value (2365).</p> <p>[Windows/Linux]</p> <p>The use trend database port is set up when SQC-A is installed.</p> <p>[Solaris]</p> <p>The use trend database port is not set up when SQC-A is installed.</p> <p>Refer to "11.1.2.2 Start operation" for details on how to set up the use trend database port.</p> <p>This item is shared between all use trend services on the managed server. If there are multiple services, any changes made to one will be applied to all the others.</p>

Window manipulation buttons

Button	Function
OK	Ends specifying data for items and closes the window.
Reset	Restores the item values to those with which the window opened.
Cancel	Closes the window without applying the information specified for the items.

14.1.3 Report Server Settings window

In the Report Server Settings window, set information on the host in which the Report Server is installed.



FUJITSU
Systemwalker
Service Quality Coordinator
Report Server Settings

Report Server

Address

Port

Information setting items

Item	Requirement	Description
(Report Server) Address	You must set.	Specify the IP address or host name of the Report Server.
(Report Server) Port	You do not have to set.	Specify the port number of the Web server running on the Report Server. No specification is needed if default port number 80 is used.

Window manipulation buttons

Button	Action
Apply	Applies the information specified for the items and closes the window.
Reset	Restores the item values to those with which the window opened.
Cancel	Closes the window without applying the information specified for the items.

14.1.4 Group Settings window

Settings for grouping the analysis target servers registered to the managed servers can be performed with the Group Settings window.

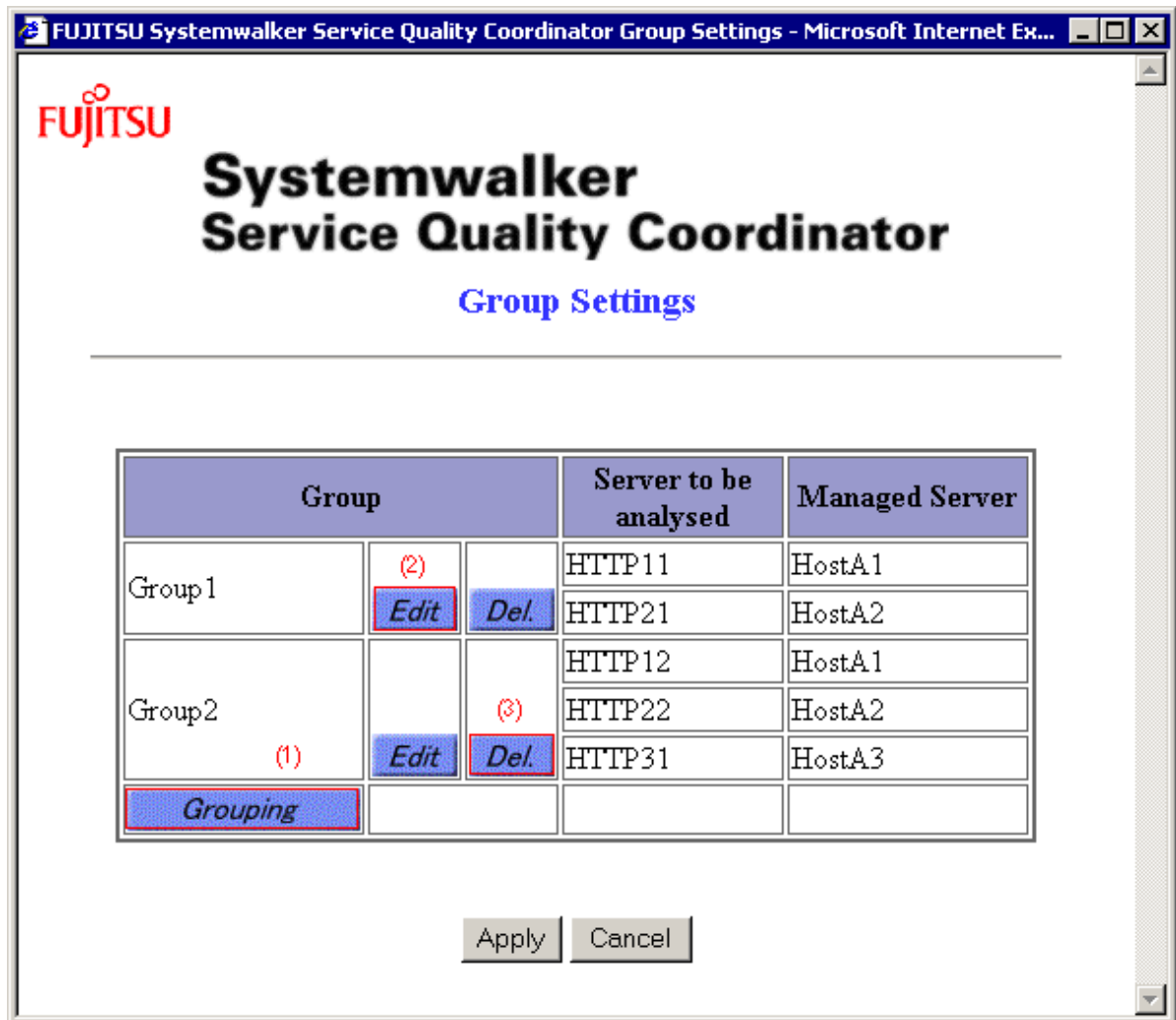


Table components

The table below summarizes the columns of the table displayed in the Group Settings window.

Column	Description
Group	The names of added groups are listed.
Target Server	Analysis target server names for the usage analysis services that configuration the group are displayed.

Column	Description
Managed Server	Server names of the managed servers that the usage analysis services are added are displayed.

Operation for changing information

To change group information, do as follows:

Processing	Operation	Number in figure
Adding a group	Click the [Grouping] button on the bottom of the Group column. An empty 14.1.4.1 Group Information window .	(1)
Editing group information	Click the [Edit] button on the right side of the group to be edited. 14.1.4.1 Group Information window having the current settings appears.	(2)
Deleting a group	Click the [Del.] button on the right side of the group to be deleted. The entry of the group disappears.	(3)

Window manipulation buttons

Button	Function
Apply	Applies the changes made in this window and in various information windows opened from this window, and closes the window.
Cancel	Closes the window without applying the changes made previously If this button is clicked after a change is made, a prompt message appears asking whether to close the window without applying changes.

Note

Clicking the [Apply] or [Cancel] button to close this window.

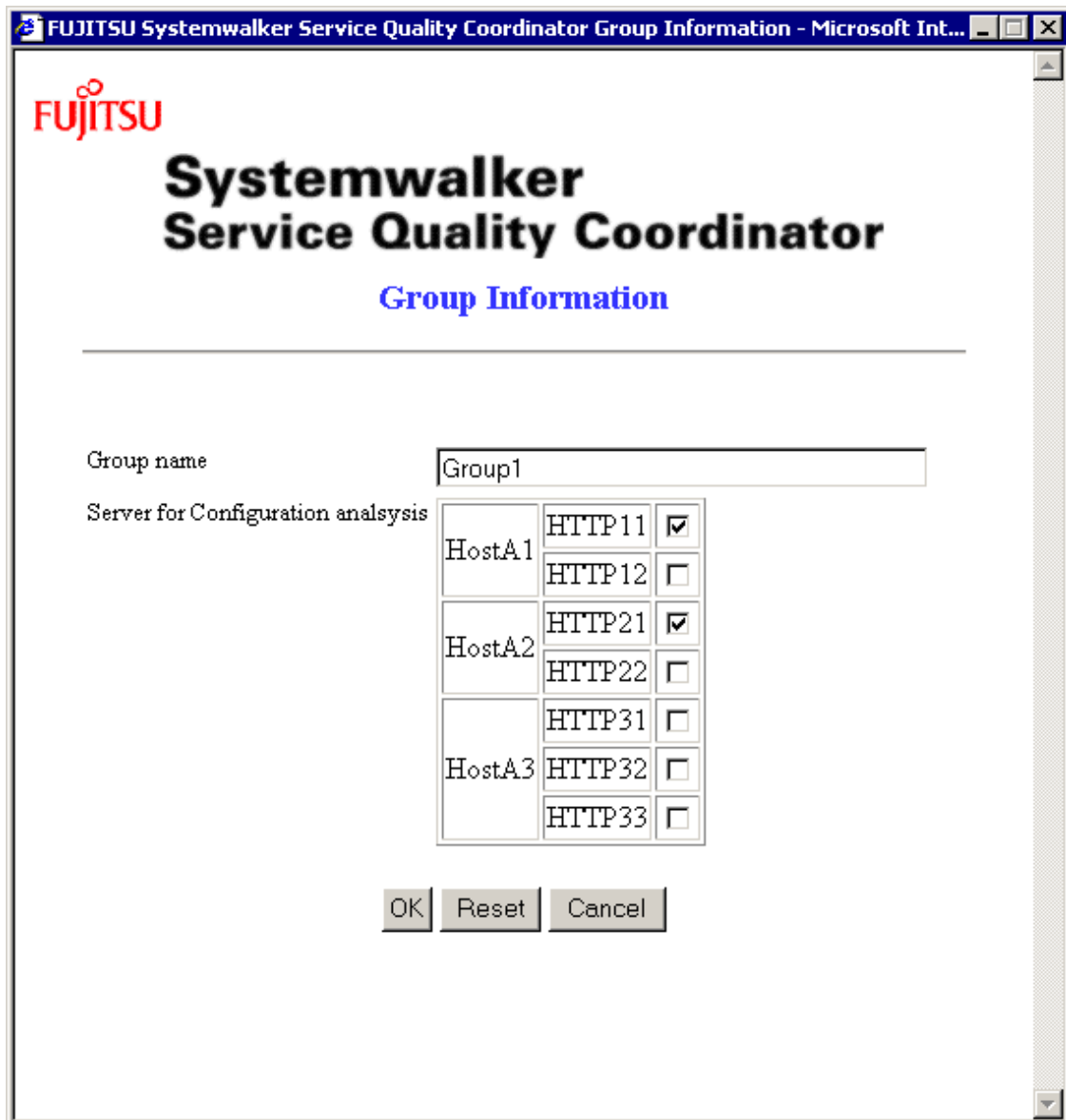
If these buttons are not used, a temporary file remains in the work area on the Management Server.

See

For information on how to delete the remaining temporary file, refer to "[14.1.5.1 Deleting unnecessary temporary files](#)".


14.1.4.1 Group Information window

In the Group Information window, set information on a group and the Target Servers that form the group.



Information setting items

Item	Requirement	Description
Group name	You must set.	<p>Specify the group entry name.</p> <p>The group name must be unique among all groups.</p> <p>You cannot specify two or more character string that becomes same when if upper/lower characters are not distinguished.</p> <p>If specified, it is recognized as used. You cannot modify the group name of the existing group to the character string that becomes same if upper/lower characters are not distinguished.</p> <p>If specified, the character string registered in advance is used.</p> <p>Specify the group name up to 64 alphanumeric characters and/or symbols, excluding the following: \$ \ " ' , : [] < > = &</p> <p>All of group name cannot be specified in number.</p>

Item	Requirement	Description
		One or more English letter must be included in the group name.
Target Server	You do not have to set.	<p>Specify the Target Servers that constitute the group. Select these servers by selecting the corresponding check boxes from the Target Server list. Only those that the Usage DB storage locations are set to management server are displayed.</p> <p> Point</p> <p>.....</p> <p>No Target Server can belong to more than one server group.</p> <p>If an existing Target Server is not found in the server list, it is probable that the server already belongs to another server group.</p> <p>.....</p>

Window manipulation buttons

Button	Action
OK	Ends specifying data for items and closes the window.
Reset	Restores the item values to those with which the window opened.
Cancel	Closes the window without applying the information specified for the items.

14.1.5 Notes

This section provides notes on the environment settings windows.

14.1.5.1 Deleting unnecessary temporary files

If the Managed Server Settings window or Group Settings window is closed using a method other than clicking the [Apply] or [Cancel] button, an unnecessary temporary file remains on the Management Server.

Leaving temporary files on the Management Server does not make any problem for Website Management operation. However, if too many temporary files are accumulated such that the disk space is pressed, they should be deleted.

Note

.....

Before deleting temporary files, ensure that all of the Managed Server Settings window, Server Group Settings window and Service Group Settings window are closed.

.....

- Path

[Windows]

Variable file storage directory \temp\

[UNIX]

/var/opt/FJSVssqc/temp/

- **Temporary file name**

EnvSetPolTempNNN -N.ini

HttpBodyTempNNN - N.ini (directory)

Chapter 15 SQC file types


15.1 List of SQC file types

This table lists the SQC file types used to control the SQC environment and to transfer usage data.

File name	File location		
	Management Server		Management Server
Usage DB Environment Definition File	Present	Present	None
Extended Log Environment Definition File	None	Present	None
Option Definition File	Present	Present	None
CSV File	Present	Present	None
SQC Extended Log File	Present	Present	None
CSV Format Log File	Present	Present	None
Start up Environment Definition File	Present	Present	None

15.2 SQC Definition Files

This section explains the environment settings to be made before using the Trend Viewer for a Web site.

Item	Need for operation
Setting of Usage DB Environment Definition File	Required. The file must be set before operation begins.
URL registration (in the Web server)	Required. URL must be registered before operation begins.
Setting of Extended Log Environment Definition File	Optional. The file must be set before operation if SQC extended log is to be collected.
Setting of Option Definition File	Optional. The file must be set before operation begins if the following types of analysis are performed: Subnetwork-specific analysis Specific-subnetwork exclusion definition Specific-URL exclusion definition
Setting of Start up Environment Definition File	Optional. Change it in case you want to change the start up time of the usage DB registry engine.  See For details on changing the start up time, refer to " 11.1.1.4 Start up time ".

Note

- The extended log environment file is defined to the managed server that collects SQC extended log.
- Option definition file is defined to the server that manages Usage DB.
 - When the managed server is operated (Usage analysis is executed on the managed server), the file is defined to the managed server.
 - When the management server is operated (the log information on the managed server is transferred to the managed server and Usage analysis is executed on the management server), the file is defined to the management server.

15.2.1 Usage DB Environment Definition File

The Usage DB Environment Definition File defines the conditions for creating databases used to store various log data on the Web services. The file also defines the conditions for creating usage DBs.

Analysis window data and CSV output data are all supplied from the usage DB.

15.2.1.1 File storage location

The Usage DB Environment Definition File is a text file. Use a text editor such as Notepad to create and edit the file.

[Windows]

```
<variable_file_directory>\control\DatabaseConfig
```

[UNIX]

```
/etc/opt/FJSVssqc/DatabaseConfig
```

A sample Usage DB Environment Definition File is stored in the folder shown below during installation. The user can edit the sample file to create a Usage DB Environment Definition File.

[Windows]

```
<install_directory>\sample\DatabaseConfig
```

[UNIX]

```
/opt/FJSVssqc/sample/DatabaseConfig
```

Character codes of the text are as follows:

[Windows]

```
ASCII
```

[UNIX]

```
ASCII
```

15.2.1.2 File internal configuration

In the Usage DB Environment Definition File, time stamps are provided on the first and last lines for validity checking, and the definitions for the server(s) to be analyzed are provided between the time stamps.

Up to 20 definitions can be provided for the server(s) to be analyzed.

The definition for one analysis target server consists of the following definition blocks:

- Analysis target server definition block * 1
- Analysis target log definition block * 1 or 2

The whole file structure is shown below:

Time stamp
Analysis target server definition block
Analysis target log definition block
Analysis target log definition block
:
Analysis target server definition block
Analysis target log definition block
:
Time stamp

Note

- The analysis target server definition is a definition made for a server to be analyzed.
If two or more servers are to be analyzed, the corresponding number of definitions should be provided.
- The analysis target log definition is a definition about the log for the server defined by the analysis target server definition.
One or two analysis target log definitions can be made for one analysis target server definition.
If two log definitions are provided, the following restrictions apply to their combination:

Analysis target log definition 1	Analysis target log definition 2	Validity	Remarks
Web server or Proxy server log	SQC extended log	Valid	None
Web server or Proxy server log	Web server or Proxy server log	Not valid	If two Web server or Proxy server log definitions are provided, separate the analysis target server definition for each of the log definitions. In this case, analysis target log definition 1 is valid.
SQC extended log	SQC extended log	Not valid	If two SQC extended log definitions are provided,

Analysis target log definition 1	Analysis target log definition 2	Validity	Remarks
			separate the analysis target server definition for each of the log definitions. In this case, analysis target log definition 1 is valid.

15.2.1.3 File internal format (basic)

The coding format of the Usage DB Environment Definition File is shown below:

Line coding format	Description
[xxxxxxxxxx]	Indicates the beginning of a definition block as well as the end of the previous definition block
xxxx = xxxxxxxxxxxx	Indicates parameters in a definition block. ' ' means OR, i.e., the parameter on either side can be specified.
none	A null line is treated as a comment.
# xxxxxxxxxxxx	A line beginning with '#' is treated as a comment.

15.2.1.4 File internal format (analysis target server definition block)

In the Usage DB Environment Definition File, an analysis target server definition block should be provided in the following format:

Format

<pre> [Server] Symbol = server-symbol Name = server-name Type = web proxy Domain = domain-name DatabaseInterval = day week(sun mon tue wed thu fri sat) month(1-31) SearchDNS = yes no RequestURLSuffix = "suffix-list" DatabaseMode = db csv both DefaultURLPage = "default-url" </pre>
--

Explanation

[Server]

Indicates the beginning of an analysis target server definition block.

Symbol

Defines the symbol of the analysis target server.

For server-symbol, specify a symbol with up to 10 alphanumeric characters (a to z, A to Z, and 0 to 9) beginning with an alphabetic character (a to z or A to Z).

This symbol is used as the directory name when a directory corresponding to the analysis target server is created under the usage DB storage directory.

Name

Defines the name of the analysis target server.

For server-name, specify the server name with up to 20 characters.

The specified name is displayed in the analysis target server box in the analysis window and used as the keyword for selecting the analysis target server. If the specified name is too long to be accommodated in the analysis target server box, the portion that is able to accommodate from the beginning is displayed. If multiple analysis target servers are specified, specify their names so that they can be distinguished by the leading parts of the names.

Type

Defines the type of the analysis target server.

The meanings of the options are as follows:

Option	Meaning
web	Web server
proxy	Proxy server

Domain

Defines the domain name of the analysis target server.

For domain-name, specify the domain name (including a subdomain name). For instance, when the fully qualified domain name (FQDN) is host.xxx.yyyy.zzzz, specify xxx.yyyy.zzzz.

In the analysis window, detailed data by the host name can be displayed. The host name refers to the FQDN. The domain name specified here is used for conversion to FQDN if the host name in the analysis target server log is recorded only with the name in the domain.

DatabaseInterval

Defines the changeover unit for the usage DB corresponding to the analysis target server.

The meanings of the options are as follows:

Option	Meaning
day	Daily
week(...)	Weekly
month(...)	Monthly

If week is specified, specify also one of the following values to indicate the start day of the week in parentheses:

Option	Meaning
sun	Sunday
mon	Monday
tue	Tuesday
wed	Wednesday
thu	Thursday
fri	Friday
sat	Saturday

If month is specified, specify also one of the following values to indicate the start day of the month. If the specified day does not exist, the last day of the month is used.

Option	Meaning
1 to 31	Day of the month

The default is shown below. If the default is to be used, the line itself can be omitted.

DatabaseInterval = week(sun)



Refer to "[11.1.1.7 Usage DB switching](#)" for details of usage DB changeover.

SearchDNS

Defines whether to perform DNS search.

In the analysis window, detailed data by the host name and by the IP address can be displayed. However, only one of them is recorded in the analysis target server log. This parameter specifies whether to perform DNS search to retrieve the other. The meanings of the options are as follows:

Option	Meaning
yes	Perform DNS search.
no	Do not perform DNS search.

The default is shown below. If the default is to be used, the line itself can be omitted.

SearchDNS = yes



If SearchDNS = no is specified, the usage DB registration engine does not perform DNS search and performs analysis based on the record in the analysis target log file. This affects the display in the analysis window as follows:

- When the client names in the analysis target log file are recorded with their IP addresses

When one of the following items is specified in the analysis method box or advanced analysis box, data for the corresponding FQDN is analyzed and displayed:

- For each client host name
- For each referrer host name
- For each remote host name

- When the client names in the analysis target log file are recorded with their host names

When one of the following items is specified in the analysis method box or advanced analysis box, data for the corresponding FQDN is analyzed and displayed:

- For each client IP address
- For each referrer IP address
- For each remote IP address



RequestURLSuffix

Defines URLs subject to request analysis.

To check clients' interests, it is important that request analysis is performed from the viewpoint of client's will. Requests generated by clients' will tend to be targeted to URLs having specific extensions such as html. For suffix-list, specify the URL extensions corresponding to clients' will by separating them with a comma (.). Up to 40 URL extensions can be specified.

The default is shown below. If the default is to be used, the line itself can be omitted.

RequestURLSuffix = "html,htm,shtml,shtm,stm,cgi,asp,pl,tcl,sh"



The user can drill down according to URL by selecting detail by URL extension in the analysis method box. In this case, if the extension for drilldown is not specified for RequestURLSuffix in the Usage DB Environment Definition File, the extension is treated as excluded for analysis. "No data is available for this period" is displayed.



DatabaseMode

Defines the usage DB operation mode.

This definition can be specified only on a managed server (Agent for Business). It is ignored if specified on the Management Server (Manager). The meanings of the options are as follows:

Option	Meaning
db	Only the usage DB is used. Specify this option if analysis is performed on the managed server.
csv	Only the Usage Log file is used. The CSV format file is transferred to the Management Server and stored in the usage DB of the Management Server. Specify this option if analysis is performed on the Management Server.

Option	Meaning
both	Both the usage DB and CS format log file are used. A Usage Log file is created as well as a usage DB.

The default is shown below. If the default is to be used, the line itself can be omitted.

DatabaseMode = db

Note

If DatabaseMode = csv is specified, log data for the analysis server is transferred to the Management Server and therefore analysis cannot be performed on the managed server.

DefaultURLPage

Defines the URL file that is automatically added if the path information file name is omitted in the analysis target log.

When a Web site is accessed, the file name may be omitted in the URL specification such as http://www.fujitsu.com/. If so, the Web server can access the Web content by automatically adding the default file name.

By default the Trend Viewer performs analysis separately when an access is made with the file name specified and when an access is made with the file name omitted. If this parameter is defined, the defined file name is automatically added even when an access is made with the file name omitted, thereby enabling the same analysis to be performed as when an access is made with the file name specified.

For default-url, specify the file name to be automatically added if the file name is omitted in the URL specification. Observe the following specification rules:

- The file name must not exceed 255 characters (bytes).
- The file name must be enclosed in double quotation marks.
- Alphanumeric characters excluding blanks and the following characters can be used for the file name:

" # % , < > \

- Only one file name can be specified.

This parameter has no default definition and is valid only when it is specified.

Example

A sample definition is as shown below:

<pre>[Server] Symbol = PUBLIC Name = OpenServer Type = web Domain = xxxx.yyyy.zzzz DatabaseInterval = week(sun) SearchDNS = yes</pre>

```
RequestURLSuffix = "html,htm,shtml,shtm,stm,cgi,asp,pl,tcl,sh"  
DatabaseMode = db  
DefaultURLPage = "index.html"
```

15.2.1.5 File internal format (log definition block to be analyzed)

In the Usage DB Environment Definition File, an analysis target log definition block should be provided in the following format:

Format

```
[Log]  
Symbol = log-symbol  
Name = log-name  
Path = log-path  
Format = format-symbol | "format"  
Region = diff-time
```

Explanation

[Log]

Indicates the beginning of an analysis target log definition block.

Symbol

Defines the symbol of the analysis target log.

For log-symbol, specify a symbol with up to 10 alphanumeric characters (a to z, A to Z, and 0 to 9) beginning with an alphabetic character (a to z or A to Z).

Name

Defines the name of the analysis target log.

For server-name, specify the log name with up to 20 characters.

Path

Defines the path of the analysis target log file.

For log-path, specify the absolute path of the file. If multiple log files are created under the same directory, use the wildcard (*: any characters numbering 0 or more) to specify all of these files. If the path contains any blanks, enclose the entire path within double quotation marks("").

Format

Defines the record format in the analysis target log file.

Specify format-symbol or "format" for the record format.

If format-symbol is used, specify a symbol corresponding to a fixed format. For symbols that can be specified, refer to [Kind and meaning of symbol](#) later in this section.

If "format" is used, specify tokens corresponding to data along with the delimiters by placing them in a line. If the record format in the analysis target log file does not correspond to any fixed format, use "[Kind and meaning of token](#)" for specification.

To perform analysis of the managed server log on the Management Server, specify SQC-CSV using format-symbol as the record format of the relevant managed server on the Management Server side.

Point

The usage DB registration engine treats all characters, which do not match the token string specified for "format", as delimiters. Note that any misspelled token is treated as a delimiter.

The usage DB registration engine reads logs from the analysis target log file and processes only those logs whose record formats match the formats specified here, and then stores them in the usage DB. Log records whose record format does not match any format specified here are not processed.

Thus, logs in the specified record format need to be output to the log file to be analyzed. To draw attention to any possible error in the record formats specified here, the usage DB registration engine stops processing if a given number of records whose record format does not match the format specified here are found from the start of the log file.

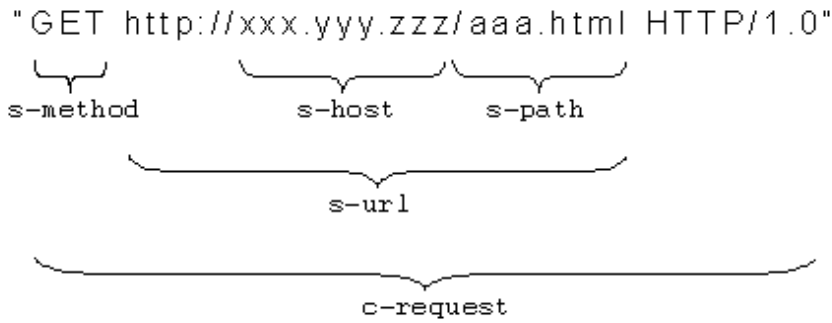
The token types and their meanings are as follows:

Kind and meaning of token

Token	Meaning
c-host	Host name of IP address of the client
c-user	Authentication user name of the client
s-time{time-format}	Time the server completed request processing
c-request (*1)	First request sent from the client to the server
s-method (*1)	Method requested by the client to the server (part of c-request)
s-url (*1)	URL requested by the client to the server (part of -request)
s-host (*1)	Host name of IP address requested by the client to the server (part of s-url)
s-path (*1)	File path requested by the client to the server (part of s-url)
s-status	Status code sent from the server to the client
r-status	Status code sent from the remote server to the server
s-bytes	Number of bytes transferred from the server to the client
r-bytes	Number of bytes transferred from the remote server to the server
l-url	Content of the Refer request header sent from the client to the server
c-agent	Content of the User-Agent request header sent from the client to the server
s-elapsed{elapsed-format}	Time required by the server for request processing
c-cookie{cookie-format}	Content of Cookie sent from the client to the server
*	Variable element other than the above
\	Escape character (To specify "\", add escape characters like "\\.")

Point

(*1) The following shows the relationships among c-request, s-method, s-url, s-host, and s-path:



.....

In time-format, place the tokens corresponding to the time format along with the delimiters in a line. The following table lists the meanings of time-format tokens:

Token	Meaning
yyyy	Year (1980 to 2038)
yy	Year (00 to 99)
mm	Month (01 to 12)
mon	Month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec)
month	Month (January, February, March, April, May, June, July, August, September, October, November, December)
dd	Day (01 to 31)
HH	Hour (00 to 23)
MM	Minute (00 to 59)
SS	Second (00 to 59)
seconds	Total seconds

In elapse-format, describe the token indicating the unit of the elapsed time. The token is one of the following:

Token	Meaning
s	Seconds
ms	Milliseconds

In cookie-format, place tokens corresponding to the cookie format along with the delimiters in a line. The following table lists the meanings of the cookie-format tokens:

Token	Meaning
id	Access ID defined in Cookie
*	Variable elements other than the above

Note

If the record format "format" is defined by listing the tokens, make sure that the following required tokens have been specified. Note that the analysis cannot be performed if these required tokens are not specified.

Required tokens
s-time
c-host
s-url (or c-request, s-path)
s-status
s-bytes

For Microsoft Internet Information Services, the default log file format does not contain log information corresponding to the "s-bytes" required token (the number of bytes transferred from the server to the client). Make sure this information is defined in the log file format before performing analysis. (The equivalent for Microsoft Internet Information Services is "sc-bytes".)

Point

If the record format is defined using "format", make sure the required tokens are included.

Analysis to be conducted	Require token
For each authentication user	c-user
For each referrer	l-url
For each browser	c-agent
Request processing time on the server	s-elapse
Error and cache data on the remote server as well in proxy server analysis	r-status

The following table lists the types of symbols (when web is defined in the analysis target server definition) for the Web server and their meanings:

Kind and meaning of symbol

Symbol	Corresponding log
	"format" content
Common	Common Logfile Format of W3C. This format corresponds to the following log formats: <ul style="list-style-type: none">- Common log format of W3C httpd (CERN httpd)- Common log format of Apache httpd- Common log format of Microsoft Internet Information Services (NCSA Common log format)- Common log format of Netscape Enterprise Server

Symbol	Corresponding log
	"format" content
	- Common log format of Fujitsu InfoProvider Proand so on "c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes"
Common +R+U	The Refer request header and User-Agent request header contents are added to Common. This format can be adapted to the following formats or their customized formats: - Custom log format of Apache httpd - W3C Extended log format of Microsoft Internet Information Services (W3C extended log format) - Flexible log format and Custom log format of Netscape Enterprise Server - Extended log format of Fujitsu InfoProvider Proand so on "c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes \"l-url\" \"c-agent\""
Microsoft -MS	Microsoft Internet Information Server's specific format. This format corresponds to the following log format: - Microsoft Log Format of Microsoft Internet Information Server 3.0 and 4.0 (*1) *1 Microsoft Internet Information Services 5.0 has a different format to V3.0 and V4.0. Here, specify the format directly by placing tokens. "c-host, c-user, s-time{yy/mm/dd, HH:MM:SS}, *, *, *, *, *, s-bytes, s-status, *, s-method, s-path, *"
SQC-Extend	SQC extended log format * Symbol specification only
SQC-CSV	Usage Log file of SQC To analyze a log of the managed server on the Management Server, specify SQC-CSV for the relevant managed server. * Symbol specification only
SQC-ExtCSV	CSV format extended log file of SQC To analyze a response log of the managed server on the Management Server, specify SQC-ExtCSV for the relevant managed server. * Symbol specification only

Note

When specifying the record format using a symbol, compare the content of the "format" corresponding to this symbol with a log that has actually been taken and make sure that the formats match before making the specification. Take particular care with formats that have date sections, as this may vary depending on the system.

The following table lists the types of symbols (when proxy is defined in the analysis target server definition) for the Proxy server and their meanings:

Symbol	Corresponding log
	"format" content
Common	"Common Logfile Format" of W3C. This format corresponds to the following log formats:

Symbol	Corresponding log
	"format" content
	<ul style="list-style-type: none"> - Common log format, Extended log format, and Extended2 log format of Netscape Proxy Server - Common log format of Squid - Common log format of DeleGate - Common log format of Apache httpd - Common log format of W3C httpd (CERN httpd) - Common log format of Fujitsu InfoProxy ... and so on <pre>"c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes"</pre>
Common+R+U	<p>The Refer request header and User-Agent request header contents are added to Common. This format can be adapted to the following formats or their customized formats:</p> <ul style="list-style-type: none"> - Flexible log format and Custom log format of Netscape Proxy Server - Custom log format of DeleGate - Custom log format of Apache httpd <pre>"c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes \"%l-url\" \"c-agent\""</pre>
Common+Ts	<p>The processing time (seconds) is added to Common. This format can be adapted to the following formats or their customized formats:</p> <ul style="list-style-type: none"> - Flexible log format and Custom log format of Netscape Proxy Server - Custom log format of DeleGate - Custom log format of Apache httpd <pre>"c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes s-elapsed{s}"</pre>
Common+Tms	<p>The processing time (milliseconds) is added to Common. This format can be adapted to the following formats or their customized formats:</p> <ul style="list-style-type: none"> - Flexible log format and Custom log format of Netscape Proxy Server - Custom log format of DeleGate - Custom log format of Apache httpd <pre>"c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes s-elapsed{ms}"</pre>
Netscape-Extend	<p>Netscape Proxy Server's specific format. This format corresponds to the following log formats:</p> <p>Extended log format and Extended2 log format of Netscape Proxy Server</p> <pre>"c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes r-status r-bytes * * * * * s-elapsed{s}"</pre>
Squid-Native11	<p>Squid's specific format. This format corresponds to the following log format:</p> <ul style="list-style-type: none"> - Native log format of Squid (Version 1.1 format) <pre>"s-time{seconds} s-elapsed{ms} c-host */s-status s-bytes s-method s-url * */* *"</pre>
Microsoft-Native	<p>Microsoft Proxy Server's specific format. This format corresponds to the following log format:</p>

Symbol	Corresponding log
	"format" content
	<ul style="list-style-type: none"> - WebProxy log format of Microsoft Proxy Server <p>"c-host, c-user, c-agent, *, time{yy/mm/dd, HH:MM:SS}, *, *, *, *, *, *, *, s-elapsed{ms}, s-bytes, r-bytes, *, *, s-method, s-url, *, *, s-status, *"</p>
DeleGate-Default	<p>DeleGate's specific format. This format corresponds to the following log format:</p> <ul style="list-style-type: none"> - Default log format of HTTP of DeleGate <p>"c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes :*"</p>
InfoProxy-Extend	<p>Fujitsu InfoProxy's specific format. This format corresponds to the following log format:</p> <ul style="list-style-type: none"> - Extended log format of Fujitsu InfoProxy <p>"c-host * c-user [s-time{dd/mon/yyyy:HH:MM:SS} *] \"c-request\" s-status s-bytes s-elapsed{ms} r-status r-bytes * * * * * * * * * *"</p>
SQC-CSV	<p>Usage Log file of SQC</p> <p>To analyze a log of the managed server on the Management Server, specify SQC-CSV for the relevant managed server.</p> <p>* Symbol specification only</p>

 Note

When specifying the record format using a symbol, compare the content of the "format" corresponding to this symbol with a log that has actually been taken and make sure that the formats match before making the specification. Take particular care with formats that have date sections, as this may vary depending on the system.

When the log record format is specified using a symbol for "format", the analysis methods that can be used are as follows:

No	Symbol value	Analysis type
1	Common	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - Entry URL - Exit URL - URL extension
2	Common +R+U	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - User agent - Referrer host name

No	Symbol value	Analysis type
		<ul style="list-style-type: none"> - Referrer IP address - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - Entry URL - Exit URL - Referrer URL - URL extension
3	Microsoft-MS	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - Entry URL - Exit URL - URL extension
4	Common+Ts	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - URL extension <p data-bbox="475 1467 1204 1585">Note: In "Request report", "Traffic report", and "Cache report", the elapsed time indicating the processing capability of the Web server or Proxy server to be analyzed is in seconds. The elapsed time is displayed on each analysis window.</p>
5	Common+Tms	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - URL extension <p data-bbox="475 1951 1204 2007">Note: In "Request report", "Traffic report", and "Cache report", the elapsed time indicating the processing capability of the Web server or Proxy server</p>

No	Symbol value	Analysis type
		to be analyzed is in milliseconds. The elapsed time is displayed on each analysis window.
6	Netscape-Extend	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - URL extension <p>Note: In "Request report", "Traffic report", and "Cache report", the elapsed time indicating the processing capability of the Web server or Proxy server to be analyzed is in milliseconds. The elapsed time is displayed on each analysis window.</p>
7	Squid-Native11	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - URL extension <p>Note: In "Request report", "Traffic report", and "Cache report", the elapsed time indicating the processing capability of the Web server or Proxy server to be analyzed is in milliseconds. The elapsed time is displayed on each analysis window.</p>
8	Microsoft-Native	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - URL extension <p>Note: In "Request report", "Traffic report", and "Cache report", the elapsed time indicating the processing capability of the Web server or Proxy server to be analyzed is in milliseconds. The elapsed time is displayed on each analysis window.</p>
9	DeleGate-Default	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only)

No	Symbol value	Analysis type
		<ul style="list-style-type: none"> - URL - URL extension
10	InfoProxy-Extend	<ul style="list-style-type: none"> - Client host name - Client IP address - Authentication user name - Remote host name (Proxy server only) - Remote IP address (Proxy server only) - URL - URL extension <p>Note: In "Request report", "Traffic report", and "Cache report", the elapsed time indicating the processing capability of the Web server or Proxy server to be analyzed is in milliseconds. The elapsed time is displayed on each analysis window.</p>
11	SQC-Extend	<ul style="list-style-type: none"> - URL - Client host name - Client IP address

Region

Defines a region for the time data recorded in the analysis target log file.

For diff-time, specify the region time using the time difference with GMT (Greenwich Mean Time). The specification format is shown below:

Format	Explanation
[+ -]HHMM	+: Fast
M	-: Slow
	HH: Hour (00 to 23)
	MM: Minute (00 to 59)

Note

Regions of time data recorded in the log depend on the type of the Web server or Proxy server to be analyzed.

It is necessary to check which format of time data is collected. For information about the format of collected time data, refer to the manual of each server.

Example

Sample definitions are shown below:

[Windows]

```
[Log]
Symbol = WWW
Name = WebServerLog
# W3C Extended log file format
# Option: Date, time, client IP address, method, URI Stem, Http status, and number of transmitted
bytes
Path = "C:\WINNT\system32\LogFiles\W3SVC1\ex*.log"
Format = "s-time{yyyy-mm-dd HH:MM:SS} c-host s-method s-url s-status s-bytes"
Region = +0000
```

[UNIX]

```
[Log]
Symbol = WWW
Name = WebServerLog
Path = /usr/local/apache/logs/access_log
Format = Common
Region = +0900
```

15.2.2 Extended Log Environment Definition File

The Extended Log Environment Definition File is a file that defines how to accumulate the SQC extended logs.

To collect the SQC extended logs, an Extended Log Environment Definition File must be set in advance. If no SQC extended log is to be collected, there is no need to set this file.

15.2.2.1 File storage location

The Extended Log Environment Definition File is a text file. To create or edit the file, use a text editor such as Notepad. The path of this file is shown below:

[Windows]

```
<variable_file_directory>\control\ExtendLogConfig
```

[UNIX]

```
/etc/opt/FJSVssqc/ExtendLogConfig
```

A sample Extended Log Environment Definition File is stored in the folder shown below during installation. The user can edit the sample file to create an Extended Log Environment Definition File.

[Windows]

```
<install_directory>\sample\ExtendLogConfig
```

[UNIX]

```
/opt/FJSVssqc/sample/ExtendLogConfig
```

Character codes are as follows:

[Windows]

ASCII

[UNIX]

ASCII

15.2.2.2 File internal configuration

The time stamp for the validity check is written on the first line and last line of the Extended Log Environment Definition File and the definitions of extended logs are written between these lines.

The definition of an extended log is a group (called a definition block in this document) of the following definitions.

- Extended log definition block * 1

The overall image within the file is as follows:

Time stamp
Extended log definition block
Time stamp

15.2.2.3 File internal format (basic)

The format of the Extended Log Environment Definition File is shown below:

Basic

Line format	Meaning
[xxxxxxxxxx]	Indicates the beginning of a definition block as well as the end of the previous definition block
xxxx = xxxxxxxxxx	Indicates parameters in a definition block. ' ' means OR, i.e., the parameter on either side can be specified.
none	A null line is treated as a comment.
# xxxxxxxxxxxx	A line beginning with '#' is treated as a comment.

15.2.2.4 File internal format (extended log definition block)

In the Extended Log Environment Definition File, the extended log definition block should be written in the following format:

Format

[Log]

```
LogfileInterval = day | week(sun|mon|tue|wed|thu|fri|sat) | month(1-31)
```

Explanation

[Log]

Indicates the start of an extended log definition block.
If there is no information within the block, the line itself can be omitted.

LogfileInterval

Defines the switching unit of the extended log files. The table below lists the options and their meanings:

Options	Meaning
day	Daily
week(...)	Weekly
month(...)	Monthly

For week, specify the start day of the week in the parentheses using the values listed below:

Option	Meaning
sun	Sunday
mon	Monday
tue	Tuesday
wed	Wednesday
thu	Thursday
fri	Friday
sat	Saturday

For month, specify the start day of the month in the parentheses using the values listed below. If the specified day does not exist in that month, the last day of the month is used.

Option	Meaning
1 to 31	Day of the month

The default is shown below. If the default is to be used, the line itself can be omitted.

```
LogfileInterval = week(sun)
```



.....
For details of SQC extended log switching, refer to "[15.2.5.3 Switching a SQC extended log file over to another](#)".
.....



Before providing the Web page service that collects the SQC extended logs, test the service to ensure the SQC extended logs are actually collected.

15.2.3 Option Definition File

The Option Definition File contains an environment definition file that the Trend Viewer uses for the following analyses:

- Subnetwork-specific analysis
- Specific-subnetwork exclusion analysis
- Specific-URL access exclusion analysis

15.2.3.1 File storage location

The Option Definition File is a text file. To create or edit the file, use a text editor such as Notepad. The path of this file is shown below:

[Windows]

```
<variable_file_directory>\control\OptionConfig
```

[UNIX]

```
/etc/opt/FJSVssqc/OptionConfig
```

A sample Option Definition File is stored in the folder shown below during installation. The user can edit the sample file to create an Option Definition File.

[Windows]

```
<install_directory>\sample\OptionConfig
```

[UNIX]

```
/opt/FJSVssqc/sample/OptionConfig
```

Character codes are as follows:

[Windows]

```
ASCII
```

[UNIX]

```
ASCII
```

15.2.3.2 File internal configuration

The Option Definition File consists of the following definition blocks:

- Subnetwork-specific analysis definition block (one block)
- Specific-subnetwork analysis exclusion definition block (one block)
- Specific-URL analysis exclusion definition block (one block)

The overall image within the file is as follows:

Subnetwork-specific analysis definition block
Specific-subnetwork analysis exclusion definition block
Specific-URL analysis exclusion definition block

The coding format of Option Definition File is shown below:

Line coding format	Description
[xxxxxxxxxx]	Indicates the beginning of a definition block as well as the end of the previous definition block
xxxx = xxxxxxxxxx	Indicates parameters in a definition block.
none	A null line is treated as a comment.
# xxxxxxxxxxx	A line beginning with '#' is treated as a comment.

15.2.3.3 File internal format (analysis definition block for each subnetwork)

The user may want to use the Trend Viewer to perform analysis for each subnetwork that is a group of IP addresses. If so, the user can define the name of the subnetwork to be analyzed in the subnetwork-specific analysis definition block.

The format of the subnetwork-specific analysis definition block is shown below:

Format

[SubnetName]

subnet-region=subnet-name

Explanation

[SubnetName]

Indicates the beginning of a subnetwork-specific analysis definition block.

subnet-region

Specifies the subnetwork range for which a subnetwork name is defined.

Specify the subnetwork range using the following format:

Format	Meaning
i.i.i-j.j.j	Area from i.i.i to j.j.j
i.i.i	Area from i.i.i to i.i.255
i.i.*	Area from i.i.0 to i.i.255
i.i.*	Area from i.i.0.0 to i.i.255.255
i.*	Area from i.0.0.0 to i.255.255.255
*	Area from 0.0.0.0 to 255.255.255.255

In the above table, i and j each indicate an integer from 0 to 255 and an asterisk (*) indicates the wildcard character. Only one wildcard character can be specified within one definition.

subnet-name

Specifies the subnetwork name corresponding to the subnetwork range.

When specifying the subnetwork name, observe the following:

- The length of the subnetwork name must not exceed 200 bytes.
- The following types of characters can be used for the subnetwork name:
 - Alphanumeric characters
 - Underscore (_)

Note

When defining a subnetwork-specific analysis definition block, note the following:

- If two or more definitions are provided for the same subnetwork, the definition provided later is effective.
- Uppercase and lowercase letters are distinguished.
- You can specify the same subnetwork name for the different subnetworks.

Example

Sample definitions are shown below:

- Sample definition 1 (with no duplicated definition)

```
[SubnetName]
10.20.125.0-10.20.125.127= SubnetExample
192.168.*=Subnet_Example
```

- "10.20.125.0 to 10.20.125.127" is defined as "SubnetExample."
 - "192.168.0.0 to 192.168.255.255" is defined as "Subnet_Example"
- Sample definition 2 (with a duplicated definition: a narrower range is defined later)

```
[SubnetName]
10.*=SQC
10.20.30.*=SQC_Agent
10.20.30.0-10.20.30.127=SQC_Manager
```

- "0.0.0.0 to 9.255.255.255" are not defined as subnetworks.
 - "10.0.0.0 to 10.20.29.255" are defined as SQC.
 - "10.20.30.0 to 10.20.30.127" are defined as SQC_Manager.
 - "10.20.30.128 to 10.20.30.255" are defined as SQC_Agent.
 - "10.20.31.0 to 10.255.255.255" are defined as SQC.
 - "11.0.0.0 to 255.255.255.255" are not defined as subnetworks.
- Sample definition 3 (with a duplicated definition: a wider range is defined later)

```
[SubnetName]
10.20.30.*=SQC_Manager
10.20.30.128-10.20.30.255=SQC_Agent
10.*=SQC
```

- "0.0.0.0 to 9.255.255.255" are not defined as subnetworks.
- "10.0.0.0 to 10.255.255.255" are defined as SQC.
- "11.0.0.0 to 255.255.255.255" are not defined as subnetworks.

15.2.3.4 File internal format (definition block with analysis of a specific subnetwork omitted)

The user may want to use the Trend Viewer to perform analysis excluding a specific subnetwork, which is a group of IP addresses, such as a management department network on the Web site. If so, the user can define the subnetworks to be excluded from analysis in the specific-subnetwork analysis exclusion definition block.

The format of the specific-subnetwork analysis exclusion definition block is shown below:

Format

```
[SubnetExcepted]
subnet-region
```

Explanation

subnet-region

Specifies the subnetwork range to be excluded from analysis.

Specify the subnetwork range using the following format:

Format	Meaning
i.i.i-j.j.j	Area from i.i.i to j.j.j
i.i.i	Area from i.i.i to i.i.255
i.i.*	Area from i.i.0 to i.i.255
i.i.*	Area from i.i.0.0 to i.i.255.255
i.*	Area from i.0.0.0 to i.255.255.255
*	Area from 0.0.0.0 to 255.255.255.255

In the above table, i and j each indicate an integer from 0 to 255 and an asterisk (*) indicates the wildcard character.

Note

When defining a specific-subnetwork analysis exclusion definition block, note the following:

- Only one wildcard character can be specified within one definition.

Example

A sample definition is shown below:

```
[SubnetExcepted]
10.25.125.1-10.25.125.127
192.168.*
```

15.2.3.5 File internal format (definition block with analysis of a specific URL omitted)

The user may want to use the Trend Viewer to perform analysis excluding a specific URL such as management content on the Web site. If so, the user can define the URLs to be excluded from analysis in the specific-URL analysis exclusion definition block.

The format of the specific-URL analysis exclusion definition block is shown below:

Format

```
[URLExcepted]
url-name
```

Explanation

url-name

Specifies the path (excluding the server name) of the Web content to be excluded from analysis

When specifying the path, observe the following:

- The length of the path must not exceed 1,023 characters.
- The following symbols cannot be used for the path:

^[[]{}<>()&\$#" '*,?

Note

Notes when defining the definition block with analysis of a specific URL omitted are shown below.

- If the path ends with a slash (/), any record with a path ending with a slash that appears in the Web server log is excluded from analysis.

Example

A sample definition is shown below:

- The sample definition shown below excludes the following URLs:
 - http://www.fujitsu.com/SSQC
 - http://www.fujitsu.com/SQC/viewer.html
 - http://www.fujitsu.com/SQC/html/swwm03/swwm0168.html
 - http://www.fujitsu.com/cgi-bin/program.cgi

```
[URLExcepted]
/SSQC
/SQC/viewer.html
/SQC/html/swwm03/swwm0168.html
/cgi-bin/program.cgi
```

15.2.4 Usage DB Output file

This section describes the format of the CSV file created by the dbprt command as a means of exporting data from the SQC Usage database.

15.2.4.1 Usage DB Output file format

This section explains the format of the comma separated value (CSV) file that is created after execution of the dbprt command.

The CSV file is a text file. The text character code depends on the platform used.

[Windows]

Character code
ASCII

UNIX]

Character code
ASCII

Data is separated with a comma (,) and output to the file. The file consists of the following lines:

Title line
Data line
Data line
:
:
Data line

The following table lists explanations of each line:

Line	Explanation													
Title	The field name (item name) of each field is output to only the first line as the title line. Each field is delimited by a comma (,).													
Data	<p>On the second and subsequent lines, multiple data lines are output as results of editing. On each data line, one piece of data edited each hour is output. Data is displayed in ascending order of date/time (chronological order).²</p> <p>Each field is separated by a comma (,). The date field and time field are placed in this order and then fields depending on the data type are placed.</p> <p>The format of the date field is as follows:</p> <table border="1"> <thead> <tr> <th>Form</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td rowspan="3">yyyy/mm/dd</td> <td>yyy y</td> <td>Christian era(1980)</td> </tr> <tr> <td>mm</td> <td>Month(01 to 12)</td> </tr> <tr> <td>dd</td> <td>Day(01 to 31)</td> </tr> </tbody> </table> <p>The format of the time field is as follows:</p> <table border="1"> <thead> <tr> <th>Form</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>h</td> <td>Hour(00 to 23)</td> </tr> </tbody> </table>	Form	Explanation	yyyy/mm/dd	yyy y	Christian era(1980)	mm	Month(01 to 12)	dd	Day(01 to 31)	Form	Explanation	h	Hour(00 to 23)
Form	Explanation													
yyyy/mm/dd	yyy y	Christian era(1980)												
	mm	Month(01 to 12)												
	dd	Day(01 to 31)												
Form	Explanation													
h	Hour(00 to 23)													

Format for each data type

The following table lists details of the title line and data line for each data type. Although the format description in this table extends over multiple lines, the actual output is one line.

Data type	File output format
session (session information)	Title line (1st line) date, hour, c-host, c-ip, authuser, r-host, r-ip, url, entry-request, exit-request, session, c-acsid

Data type	File output format	
	Data line (2nd and subsequent lines)	yyyy/mm/dd,h,"c-host","c-ip","authuser","r-host","r-ip","url",entry-request,exit-request,session,"c-acsid"
request (request information)	Title line (1st line)	date,hour,c-host,c-ip,authuser,r-host,r-ip,url,s-traffic,e-traffic,e-request,c-hit,s-hit,r-hit,c-acsid
	Data line (2nd and subsequent lines)	yyyy/mm/dd,h,"c-host","c-ip","authuser","r-host","r-ip","url",s-traffic,e-traffic,e-request,c-hit,s-hit,r-hit,"c-acsid" Remarks: The total request count is the sum of e-request, c-hit, s-hit, and r-hit.
error (error information)	Title line (1st line)	date,hour,c-host,c-ip,authuser,r-host,r-ip,url,s-error-code,r-error-code,e-request,c-acsid
	Data line (2nd and subsequent lines)	yyyy/mm/dd,h,"c-host","c-ip","authuser","r-host","r-ip","url","s-error-code","r-error-code",error-num,"c-acsid"
agent (agent information)	Title line (1st line)	date,hour,c-host,c-ip,url,agent,session
	Data line (2nd and subsequent lines)	yyyy/mm/dd,h,"c-host","c-ip","url","agent",session
link (referrer information)	Title line (1st line)	date,hour,l-host,l-ip,l-url,r-host,r-ip,r-url,url,session
	Data line (2nd and subsequent lines)	yyyy/mm/dd,h,"l-host","l-ip","l-url","r-host","r-ip","r-url","url",session
response (response information)	Title line (1st line)	date,hour,c-host,c-ip,url,avr-response,max-response,min-response
	Data line (2nd and subsequent lines)	yyyy/mm/dd,h,"c-host","c-ip","url",avr-response,max-response,min-response

Explanation of fields on the 2nd and subsequent lines for each data type

Field	Meaning
yyyy/mm/dd	Date field
h	Time field
"agent"	Agent name
"authuser"	Authentication user name. If no data is available, "-" is output.

Field	Meaning
"c-host"	Client host name. If no data is available, "-" is output.
"c-ip"	Client IP address. If no data is available, "-" is output.
"c-acsid"	Access ID set by Cookie
"url"	URL of the Web page
"l-host"	Referrer host name
"l-ip"	Referrer IP address
"l-url"	Referrer URL
"r-host"	Remote host name
"r-ip"	Remote IP address
"r-url"	Remote URL
"s-error-code"	Code for error that occurred on the server. If no data is available, "-" is output.
"r-error-code"	Code for error that occurred on the remote server. If no data is available, "-" is output.
session	Session count
c-hit	Hit count on the client
s-hit	Hit count on the server
r-hit	Hit count on the remote server
entry-request	Entry request count
exit-request	Exit request count
s-traffic	Successful request traffic
e-request	Failed request count
e-traffic	Failed request traffic
error-num	Error count
avr-response	Average response time (in milliseconds)
max-response	Maximum response time (in milliseconds)
min-response	Minimum response time (in milliseconds)

15.2.4.2 Capacity estimation

This section provides an example of capacity estimation under the conditions shown below. Refer to this example when you estimate the capacity by applying each CSV-output data type and periods.

Conditions

Data type	Visit information
Size per line	About 150 bytes (depending on the length of the client name and URL)
Access count	About 10,000/day

Approximate maximum size per day

About 150 bytes * about 10,000 = about 1.5 MB (/day)

Actually, the same visitor (client) may often visit the same URL more than once within the same one hour. In such cases, the data of this kind is summarized on one line, and therefore actual size becomes smaller than the above size if the total access count is the same.

15.2.5 SQC extended log file

This subsection explains the SQC extended log file.

The SQC extended log file is created automatically by the SQC Extended Log Collection when the SQC extended logs are accumulated.

15.2.5.1 File name

Storage location

The SQC extended log file is stored in the following directory.

[Windows]

```
<variable_file_directory>\extend-log\
```

[UNIX]

```
/var/opt/FJSVssqc/extend-log/
```

File name format

The SQC extended log file name has the following format. A new file name is created each time the SQC extended log file is switched. The characters shown in blue indicate variables.

logyyyyymmdd_nn

[Explanation of variable characters]

Symbol	Meaning
yyyy	Year of creation date (1970 to n)
mm	Month of creation date (01 to 12)
dd	Day of creation date (01 to 31)
nn	Serial number of the SQC extended log file among those log files created on the same day (01 to 99)

15.2.5.2 Capacity estimation

The formula for estimating the capacity per day is as follows. The characters shown in blue indicate variables.

(Capacity per day) = (50 + A + B) * C

Symbol	Meaning
A	Average number of bytes of the client field
B	Average number of bytes of the document field
C	Average access count to the document per day

15.2.5.3 Switching a SQC extended log file over to another

To simplify work such as backup of the SQC extended log file, the SQC Extended Log Collection periodically creates a new SQC extended log file (file name logyyymmdd_nn as described in 15.2.5.1) to change the accumulation destination of the SQC extended log to the new log file. This operation is referred to as "SQC extended log file switching."

SQC extended log file switching is performed in accordance with the settings in the Extended Log Environment Definition File "ExtendLogConfig".

For details on how to set the Extended Log Environment Definition File, refer to "[15.2.2 Extended Log Environment Definition File](#)".

15.2.6 Usage Log file

This section describes the CSV log files created by the Usage DB Registration Engine on the Managed Server as a means of transferring usage data to the Management Server..

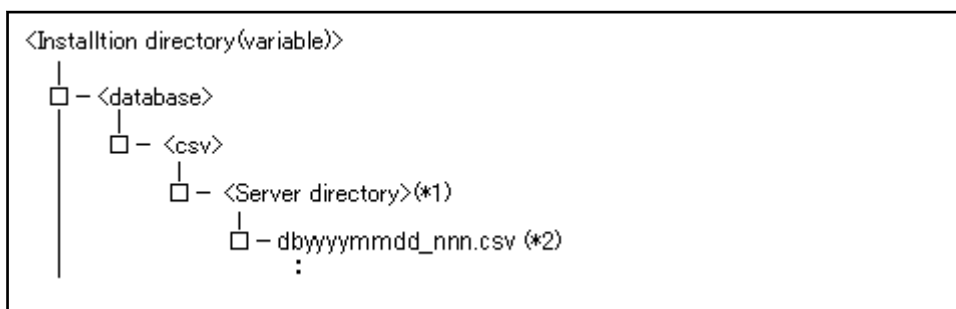
15.2.6.1 Usage Log file format

This section explains the format of the CSV format log file.

CSV format log files are used for Web server and proxy server logging. In addition, CSV format extended log files are used for analysis of response reports.

Storage location and file name

CSV format log files are stored in the following directory:



* <> indicates a directory.

*1 The server directory is assigned the name specified by Symbol in the analysis target server definition block of the Usage DB Environment Definition File.

*2 The variable (yyymmdd_nnn) in the CSV format log file name is shown below. The date means the date on which the usage DB was switched (created).

yyyy	Year (1980 and after)
mm	Month (01 to 12)
dd	Day (01 to 31)
nnn	Serial number (001 to 999)

When response report analysis is performed, a CSV format extended log file for response report analysis is created with the following file name under the server directory shown above. The variable (yyymmdd_nn) in the name of the CSV format extended log file is the same as that in the CSV format log file name.

eyyyymmdd_nnn.csv

In addition, an index file is created with the following file name under the server directory. This is to improve the efficiency of access to the CSV format file when the CSV format log file is transferred from the managed server to the Management Server. The index file is a special file for the Usage DB Registration Engine. Do not use the index file.

dbyyyymmdd.index

eyyyymmdd.index

File format

The CSV format log file and CSV format extended log file are text files. The character codes used for the texts vary depending on the platform.

[Windows]

Character code
ASCII

[UNIX]

Character code
ASCII

Data in the file is separated by a comma (.). The file consists of the following lines.

Title line
Data line
Data line
:
:
Data line

The following table explains each line.

Line	Explanation
Title	The field name (item name) of each field is output to only the first line as the title line. Each field is delimited by a comma (,).
Data	Data lines are output on the second and subsequent lines. One valid record in the Web server log is output as one data line. Data is output in ascending order (old to new) of date and time. Each field is separated with a comma (,). A hyphen (-) is output in fields for which there is no applicable data.

Format of each line

The following table lists details of the title line and data line for each data type. Although the format description in this table extends over multiple lines, the actual output is one line.

CSV format log file

Line	File output format
Title line (first line)	server,s-date,s-time,c-host,c-ip,s-method,s-protocol,s-host,s-ip,s-path,s-status,r-status,s-byte,r-byte,l-url,c-agent,s-elaps,c-cookie-id,c-user
data line (from the second line)	"server","yyyy/mm/dd","hh:mm:ss","c-host","c-ip","s-method","s-protocol","s-host","s-ip","s-path","s-status","r-status","s-byte","r-byte","l-url","c-agent","s-elaps","c-cookie-id","c-user"

CSV format extended log file

Line	File output format
Title line (first line)	server,s-date,s-time,c-host,s-url,c-response
Data line (from second line)	"server","yyyy/mm/dd","hh:mm:ss","c-host","c-ip","s-url","c-response"

Explanation of data line fields (second and subsequent lines)

CSV format log file

Field	Meaning
"server"	Web server name
"yyyy/mm/dd"	Date on which the server completes processing of a request

Field	Meaning										
	<table border="1"> <thead> <tr> <th>Form</th> <th colspan="2">Explanation</th> </tr> </thead> <tbody> <tr> <td rowspan="3">yyyy/mm/dd</td> <td>yyyy</td> <td>Christian era (1980 .)</td> </tr> <tr> <td>mm</td> <td>Month (01 - 12)</td> </tr> <tr> <td>dd</td> <td>Day (01 - 31)</td> </tr> </tbody> </table>	Form	Explanation		yyyy/mm/dd	yyyy	Christian era (1980 .)	mm	Month (01 - 12)	dd	Day (01 - 31)
Form	Explanation										
yyyy/mm/dd	yyyy	Christian era (1980 .)									
	mm	Month (01 - 12)									
	dd	Day (01 - 31)									
"hh:mm:ss"	Time at which the server completes processing of a request <table border="1"> <thead> <tr> <th>Form</th> <th colspan="2">Explanation</th> </tr> </thead> <tbody> <tr> <td rowspan="3">hh:mm:ss</td> <td>hh</td> <td>hour (00~23)</td> </tr> <tr> <td>mm</td> <td>minute (00~59)</td> </tr> <tr> <td>ss</td> <td>second (00~59)</td> </tr> </tbody> </table>	Form	Explanation		hh:mm:ss	hh	hour (00~23)	mm	minute (00~59)	ss	second (00~59)
Form	Explanation										
hh:mm:ss	hh	hour (00~23)									
	mm	minute (00~59)									
	ss	second (00~59)									
"c-host"	Client host name										
"c-ip"	Client IP address										
"s-method"	Method the client requests from the server										
"s-protocol"	Protocol the client requests from the server										
"s-host"	Host name the client requests from the server										
"s-ip"	IP address the client requests from the server										
"s-path"	File path the client requests from the server										
"s-status"	Status code sent to the client by the server										
"r-status"	Status code sent to the server by the remote server										
"s-byte"	Number of bytes sent by the server to the client										
"r-byte"	Number of bytes sent by the remote server to the server										
"l-url"	Referrer URL										
"c-agent"	Content of the User-Agent request header sent by the client to the server										
"s-elaps"	Time period required by the server for request processing (in milliseconds)										
"c-cookie-id"	Access ID defined for a cookie										
"c-user"	Client authentication user name										

CSV format log file

Field	Meaning										
"server"	Web server name										
"yyyy/mm/dd"	Date on which the server completes processing of a request <table border="1"> <thead> <tr> <th>Form</th> <th colspan="2">Explanation</th> </tr> </thead> <tbody> <tr> <td rowspan="3">yyyy/mm/dd</td> <td>yyyy</td> <td>Christian era (1980 .)</td> </tr> <tr> <td>mm</td> <td>Month (01 - 12)</td> </tr> <tr> <td>dd</td> <td>Day (01 - 31)</td> </tr> </tbody> </table>	Form	Explanation		yyyy/mm/dd	yyyy	Christian era (1980 .)	mm	Month (01 - 12)	dd	Day (01 - 31)
Form	Explanation										
yyyy/mm/dd	yyyy	Christian era (1980 .)									
	mm	Month (01 - 12)									
	dd	Day (01 - 31)									
"hh:mm:ss"	Time at which the server completes processing of a request										

Field	Meaning												
	<table border="1"> <thead> <tr> <th>Form</th> <th colspan="2">Explanation</th> </tr> </thead> <tbody> <tr> <td>hh:mm:ss</td> <td>hh</td> <td>hour (00~23)</td> </tr> <tr> <td></td> <td>mm</td> <td>minute (00~59)</td> </tr> <tr> <td></td> <td>ss</td> <td>second (00~59)</td> </tr> </tbody> </table>	Form	Explanation		hh:mm:ss	hh	hour (00~23)		mm	minute (00~59)		ss	second (00~59)
Form	Explanation												
hh:mm:ss	hh	hour (00~23)											
	mm	minute (00~59)											
	ss	second (00~59)											
"c-host"	Client host name												
"s-url"	Path of the HTML document that the client requested of the server												
"c-response"	Response time in milliseconds												

15.2.6.2 Capacity estimation

An example for calculating an approximate capacity under the following conditions is shown below. Refer to the example to estimate the capacity considering the period in which the CSV-format log file is output.

Conditions

Data type	Visit information
Size per line	About 250 bytes (depending on the length of the client name and URL)
Access count	About 10,000/day

Approximate maximum size per day

About 250 bytes * about 10,000 = about 2.5 MB (/day)

15.2.6.3 Deleting a Usage Log file

The Usage Log file is created when log data of the Managed Server is transferred to the Management Server and analyzed on the same Server. The file is no longer needed after it is transferred to the Management Server and stored in the usage DB.

This section explains how to delete the Usage Log file that is no longer needed after it is stored in the usage DB on the Management Server. Before deleting the Usage Log file, make a backup copy of the file as needed in preparation for problems such as destruction of the usage DB.

Usage Log file that can be deleted

Usage Log file that can be deleted

The Usage Log files that were transferred to the Management Server and stored in the usage DB can be deleted.

Furthermore, the Usage Log files stored in the usage DB of the Usage Log files on the Managed Server and the Management Server can be deleted.

The files to be deleted are as follows:

dbyyyymmdd_nnn.csv
 eyyyymmdd_nnn.csv
 dbyyyymmdd.index

eyyyymmdd.index

Note

"dbyyyymmdd.index" and "eyyyymmdd.index" are stored on the managed server only.

The storage locations for the files to be deleted are as follows:

[Windows]

<variable_file_directory>\database\csv\ <i>Server directory</i> \
<variable_file_directory>\database\csv\ <i>Server directory</i> \Server_Csv_Backup\
<variable_file_directory>\database\csv\ <i>Server directory</i> \Extend_Csv_Backup\

[UNIX]

/var/opt/FJSVssqc/database/csv/ <i>Server directory</i> /
/var/opt/FJSVssqc/database/csv/ <i>Server directory</i> /Server_Csv_Backup/
/var/opt/FJSVssqc/database/csv/ <i>Server directory</i> /Extend_Csv_Backup/

Note

"*Server directory*" is the name specified by "Symbol" in the analysis target server definition block in the usage database environment definition file.

Conditions for deleting CSV format log files

Delete only the CSV format log files that meet the following conditions.

- Management server side

Use a text editor to open the log files stored in the following directory. If there are no errors in any of the analysis target servers, delete those files that are stored in the directory for storing CSV format log files and whose dates are more than three days (server actual operating day) old counting back from the date of the latest file.

Note

Do not delete any files if there are errors.

[Windows]

<variable_file_directory>\log\dbreg.log

[UNIX]

/var/opt/FJSVssqc/log/dbreg.log

- Managed server side

Check the files that have been transferred within the directory for storing CSV format log files, and delete those files whose dates are more than three days (server actual operating day) old counting back from the date of the latest file.



Refer to "[Storage location and file name](#)" in "[15.2.6.1 Usage Log file format](#)" for information on how to read the dates for CSV format log files.



Make sure that the following processes are not running when CSV format log files are deleted.

[Windows]

dbregmng.exe
dbreg.exe

[UNIX]

dbregmng
dbreg

Automatically deleting an unnecessary Usage Log file

The user may want to automatically delete the Usage Log file that has already been transferred to the Management Server and stored in the usage DB.

To automatically delete an unnecessary Usage Log file, create a batch file (or shell script) used for deletion and run it using the scheduler function.

For the scheduler function, you can use the OS standard function as shown below or introduce and use the product with the scheduler function such as Systemwalker Operation Manager.

- OS standard scheduler function

[Windows]

AT command

[UNIX]

cron command

15.3 Report data file

15.3.1 Report data file

The Service Level Reporter can be used to download the data used for creating reports as a CSV file.



Refer to "[12.5.3 Report contents](#)" for the download procedure.

The following explains the format of the CSV files.

15.3.1.1 Report data file format

This explains the format of the CSV files which are downloadable from reports.

Summary

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"summary"
4 to 5	Internal control information
6	Total number of sessions
7	Internal control information
8	Total number of requests
9	Internal control information
10	Total traffic (byte)
11	Internal control information
12	Number of hits
13	Internal control information
14	Number of hits (client)
15	Internal control information
16	Number of hits (server)
17	Internal control information
18	Number of hits (remote)
19	Internal control information
20	Number of errors

Session report (by time segment)

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"session"
4 to 5	Internal control information
6	Period
7	Internal control information
8	Number of sessions (count)

Session report (by other report type)

- Summary data

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"session"
4 to 5	Internal control information
6	Value corresponding to the report type (such as a client host name)
7	Internal control information
8	Number of sessions (count)
9	Internal control information
10	Percentage (%)

- Transition data

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"session"
4 to 7	Internal control information
8	Number of sessions (count)
9	Internal control information
10	Percentage (%)

* Records for periods are output for each time segment.

Request report (by time segment)

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"request"
4 to 5	Internal control information
6	Period
7	Internal control information
8	Number of requests (count)
9	Internal control information
10	Request average (milliseconds)
11	Internal control information
12	Total traffic (byte)

Request report (by other report type)

- Summary data

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"request"
4 to 5	Internal control information
6	Value corresponding to the report type (such as a client host name)
7	Internal control information
8	Number of requests (count)
9	Internal control information
10	Request average (milliseconds)
11	Internal control information
12	Total traffic (byte)
13	Internal control information
14	Percentage (%)

- Transition data

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"request"
4 to 7	Internal control information
8	Number of requests (count)
9	Internal control information
10	Request average (milliseconds)
11	Internal control information
12	Total traffic (byte)
13	Internal control information
14	Percentage (%)

* Records for periods are output for each time segment.

Traffic report (by time segment)

Column position	Content
1	Time (UTC base)
2	Internal control information

Column position	Content
3	"traffic"
4 to 5	Internal control information
6	Period
7	Internal control information
8	Total traffic (byte)
9	Internal control information
10	Number of requests (count)
11	Internal control information
12	Request average (milliseconds)

Traffic report (by other report type)

- Summary data

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"traffic"
4 to 5	Internal control information
6	Value corresponding to the report type (such as a client host name)
7	Internal control information
8	Total traffic (byte)
9	Internal control information
10	Number of requests (count)
11	Internal control information
12	Request average (milliseconds)
13	Internal control information
14	Percentage (%)

- Transition data

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"traffic"
4 to 7	Internal control information
8	Total traffic (byte)
9	Internal control information

Column position	Content
10	Number of requests (count)
11	Internal control information
12	Request average (milliseconds)
13	Internal control information
14	Percentage (%)

* Records for periods are output for each time segment.

Cache report

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"cache"
4 to 5	Internal control information
6	Occurrence location
7	Internal control information
8	Number of hits (count)
9	Internal control information
10	Number of successful requests (count)
11	Internal control information
12	Total successful traffic (byte)
13	Internal control information
14	Successful request average (milliseconds)
15	Internal control information
16	Percentage (%)

Error report (by error location)

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"error"
4 to 5	Internal control information
6	Occurrence location
7	Internal control information
8	Number of errors (count)
9	Internal control information
10	Percentage (%)

Error report (by error record)

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"error"
4 to 5	Internal control information
6	Error code
7	Internal control information
8	Number of errors (count)
9	Internal control information
10	Percentage (%)

Response report

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"response"
4 to 5	Internal control information
6	Value corresponding to the report type (such as URL)
7	Internal control information
8	Average response time (milliseconds)
9	Internal control information
10	Maximum response time (milliseconds)
11	Internal control information
12	Minimum response time (milliseconds)

Page navigation report

Column position	Content
1	Time (UTC base)
2	Internal control information
3	"pagenavi"
4 to 5	Internal control information
6	URL
7	Internal control information
8	Number of requests (count)
9	Internal control information
10	Staying time (seconds)
11	Internal control information
12	Percentage (%)

* Records are output for each URL in descending order of frequently accessed paths.

Number of actually visiting users

Column position	Content
1	Date (local time base)
2	Time (local time base)
3	Client host name
4	Client IP address
5	Authentication user name
6	Remote host name
7	Remote IP address
8	URL
9	Entry request count
10	Exit request count
11	Number of sessions (count)
12	Access ID

Chapter 16 Troubleshooting

This section explains how to respond to problems.

16.1 Usage Analysis

This section explains how to troubleshoot when Trend Viewer does not function normally.

Check the following item sequentially referring to "[Set confirmation](#)".

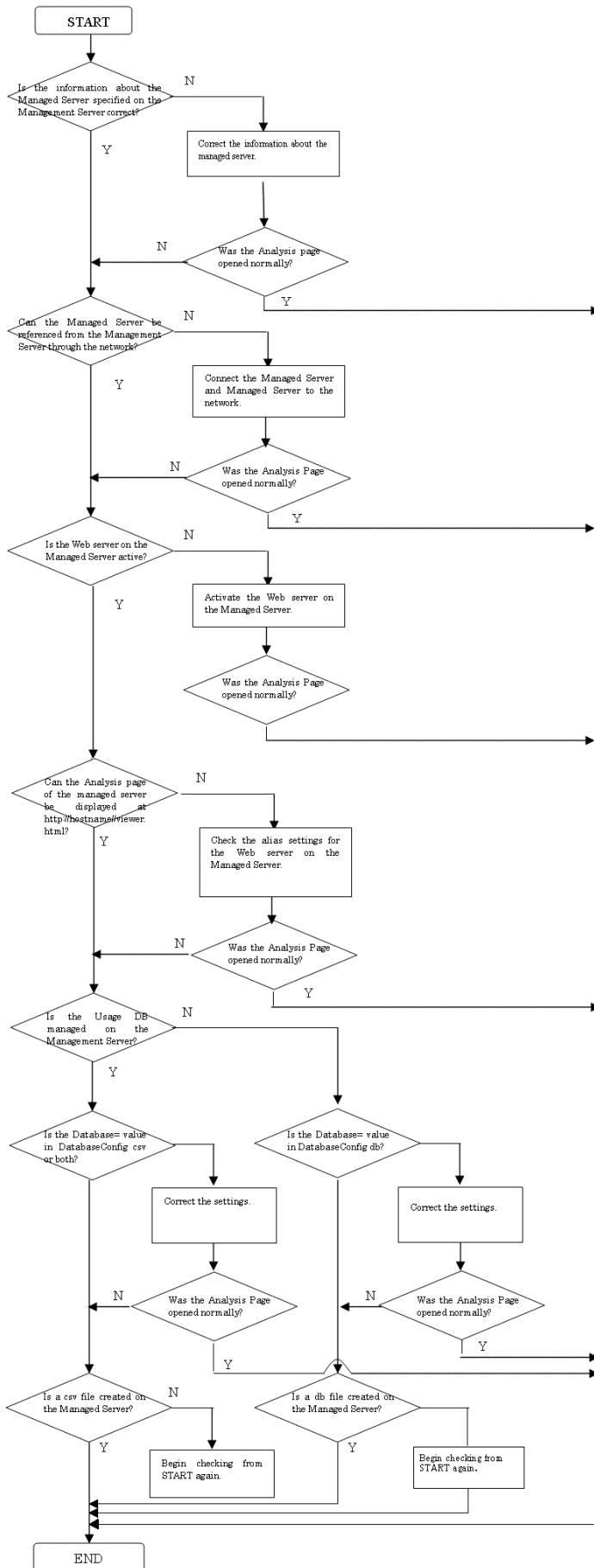
1. Check the environment settings.
2. Take action according to the present situation.
 1. "The server does not respond. A connection timeout occurred" is displayed.
 2. The DB registration engine causes an application error during operation.
 3. Error message "404 File not found" is displayed in the analysis window.
 4. An error message is displayed in the analysis window.

The confirmation procedure is shown as the flowchart as follows.

Check the setting according to this flowchart and take action.

For details of each type of processing, refer to the tables that follow the figure.

Figure 16.1 Figure: Flow chart of Usage Analysis



Set confirmation

Classification	Check item	Corrective action
Environment settings	Check and correct the settings by referring to " 11.2.2 Start operation ".	-
"The server does not respond. A connection timeout occurred" is displayed.	Check whether the managed server definition is correct.	Check the setting window to see whether information on the target server is defined correctly. Also, refer to " 4.2 Environment Settings for Usage Analysis " to check whether the current settings are correct.
-	Can the managed server be referenced from the Management Server through the network?	Make settings so that the managed server can be referenced from the Management Server through the network.
-	Check whether the Agent for Business Web server is active.	If the Agent for Business Web server is not active, activate the Web server and check that any page on the server can be displayed.
-	Can specifying the URL open the Agent for Business usage analysis window? http://(hostname)/SQC/viewer.html (hostname) : managed server host name or IP address	Check whether the setting of the Web server alias on the managed server is correct.
-	Check whether the usage DB has been created. <pre> < Installation directory > ├── <database> │ ├── <csv> │ │ └── < Server directory > (*1) │ │ └── dbyyyyymmdd_nnn.csv (*2) │ │ ⋮ </pre> <p>(*1) The server directory is created with the name specified by Symbol in the analysis target server definition block in the usage DB environment setting file.</p> <p>(*2) The variables in the directory name in the usage DB are as follows. The date means the date on which the usage DB was switched (created).</p>	If the usage DB has not been created, the environment must be set so that a usage DB is created. Refer to " 4.2 Environment Settings for Usage Analysis " and check whether the current environment settings are correct.
The DB registration engine causes an application error during operation.	Check whether a file with extension .LOCK exists under the following directory: <installation directory (variable)>\database	Make a backup copy of the file with the .LOCK extension, delete the file, and then restart the service.
-	Check whether the database contains an error.	If the database contains an error, refer to " 4.2 Environment Settings for Usage Analysis " and correct the settings, then delete the database file.

Classification	Check item	Corrective action
		A new database will be automatically recreated according to the routine schedule.
Error message "404 File not found" is displayed in the analysis window.	Check whether the URL required for display in the analysis window is registered.	Refer to " 4.1 Settings for Web Server " and check the URL registration status.
An error message is displayed in the analysis window.	-	Refer to " 17.2.3 Analysis window " and take proper action.

16.2 Report Display

This section explains how to troubleshoot when the report function does not function normally.

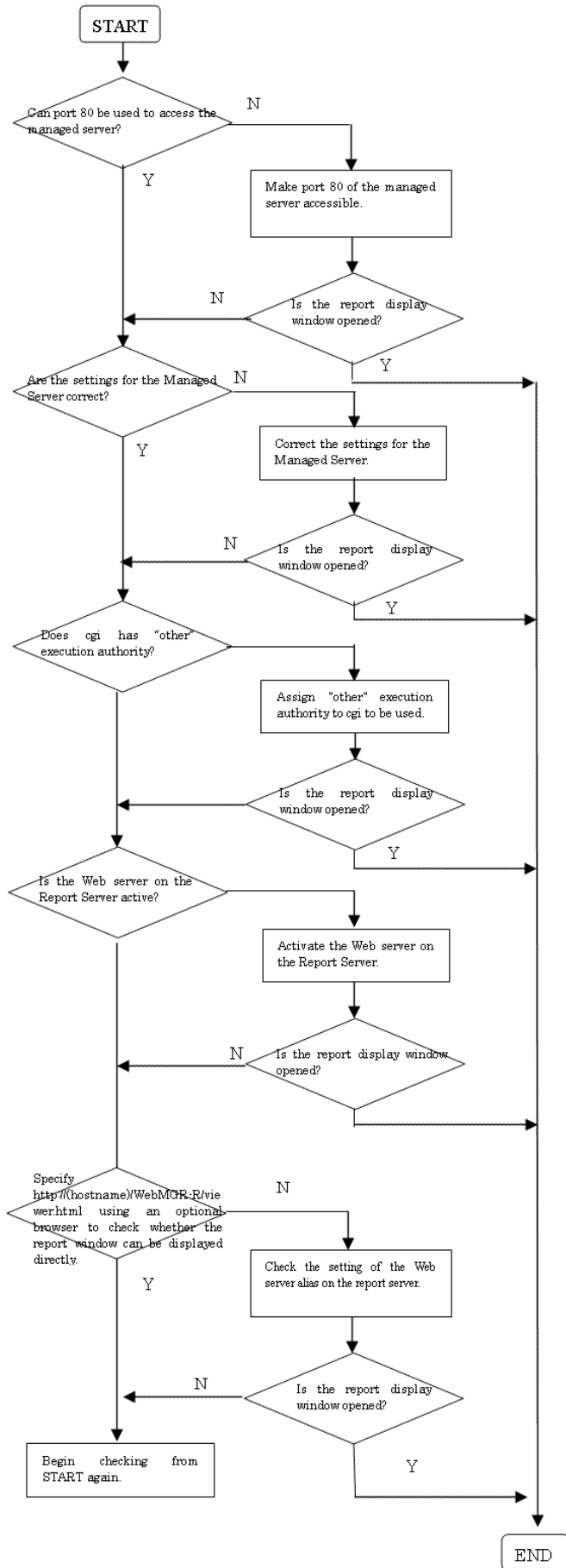
Check the following items in order:

The confirmation procedure is shown as the flowchart as follows.

Check the setting according to this flowchart and take action.

For details of each type of processing, refer to the table that follows the figure.

Figure 16.2 Figure: Flow chart of Report Display



 Note

Web Site Management Functionality uses the operation management client as the report server.

Classification	Check item	Corrective action
Environment settings	Does the following file permit an access from "other" to obtain performance information? /var/opt/FJSVssqc/database/csv /opt/FJSVssqc/exa/etc/ MpTrfExaAgt.ini	Assign the file at the left access authority for "other"
-	Check that Manager can access Agent for Business using http port 80.	Set the http port to 80.
-	Are the settings for the managed server correct?	Refer to " 7.2 Registering a Managed Server " and check whether the settings for the managed server are correct.
The report window cannot be displayed.	Are the settings for the report server correct?	Check whether the report server IP address displayed at Management Server in the Environment Setting window is correct.
-	Is the Web server on the report server active?	Activate the Web server on the report server and check that any window of the Web server can be displayed.
-	Can the report window be opened directly by specifying the following URL from an arbitrary browser? http://(hostname)/SSQC/console.html (hostname): report server host name or IP address.	Refer to " 5.1.1.1 Setting virtual directories " and check the Web server alias setting on the report server.
-	Can the report server be referenced from the Management Server through the network?	Correct the network settings so that the report server can be referenced from the Management Server through the network.
-	Check the properties of the virtual directory.	Set an account having administrator authority as an account used for anonymous access. Follow the procedure below: 1.Select virtual directory name SQC from the setting window of Microsoft(R) Internet Information Services. 2.Set directory security using the properties window of the above virtual directory as follows:

Classification	Check item	Corrective action
		2-1. Select the "anonymous access" check box. 2-2. Specify the user having administrator authority as an account used for anonymous access.
Error message "Error: ExtendCopy()" is displayed.	If report generation is performed continuously using the report function while the version of Microsoft(R) Internet Information Server is 4.0, the following occurs: -Microsoft(R) Internet Explorer "Error: ExtendCopy()" is displayed.	Add the following registry entry and then restart IIS. HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet \Services\Inetinfo\Parameters Value name: DisableMemoryCache Data type: DWORD Value: 1

 **Note**

Web Site Management Functionality uses the operation management client as the report server.

16.3 Contents Tampering Monitor

This section explains how to troubleshoot when tamper monitoring does not function normally.

Check the following items in order:

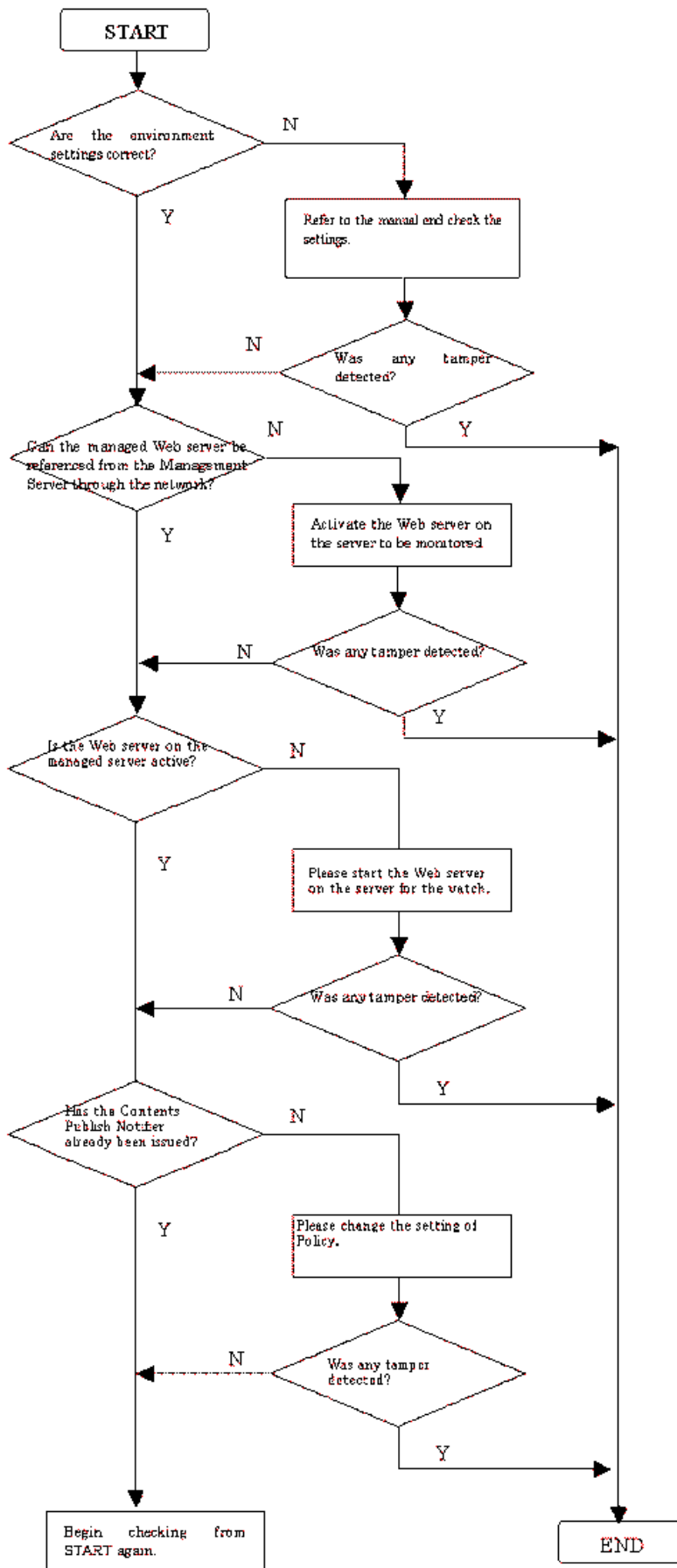
1. Check the environment settings.
2. Take action according to the present situation.
 1. Tampering is not detected (reported).

The confirmation procedure is shown as the flowchart as follows.

Check the setting according to this flowchart and take action.

For details of each type of processing, refer to the table that follows the figure.

Figure 16.3 [Figure : Flow chart of Tamper Monitoring]



Classification	Check item	Corrective action
Environment settings	Check that Agent for Business can be accessed from Manager using http port 80.	Set the http port to 80.
-	Are the settings for the managed server correct?	Refer to " 7.2 Registering a Managed Server " and check whether the settings for the managed server are correct.
-	Is the Web server on the managed server active?	Activate the Web server on the managed server.
Tampering is not detected (reported).	Are the environment settings correct?	Refer to " 10.2 Environment Settings " and check the settings.
-	Has the Contents Publish Notifier already been issued?	Refer to " 10.4.2 Notifying content publish (contents administrator job) " and issue the Contents Publish Notifier.

Chapter 17 Messages

The following explains the messages.

17.1 Contents Tampering Monitor messages

The following explains error messages and their meaning.

17.1.1 Contents Tampering Monitor - settings windows

The following table lists the message texts, the meaning of message texts, and the corrective actions when the settings window of the Contents Tampering Monitor is used.

Message text	Meaning	Action
An error occurred. Failed to open a file	The file could not be opened.	Contact an SE.
An error occurred. Failed to read a file	The file could not be read.	Contact an SE.
An error occurred. File data format invalid	The format of data in the file is invalid.	Contact an SE.
An error occurred. Failed to write to a file	Writing data to the file failed.	Contact an SE.
An error occurred. Failed to allocate an installation directory	The installation directory could not be allocated.	Contact an SE.
An error occurred. Failed to apply the lock	Lock application failed.	Retry later. If the same symptom recurs, contact an SE.
An error occurred. Failed to reserve memory	Memory could not be reserved.	Increase the memory capacity.

17.1.2 Content publish notifier

For messages output by the content publish notifier, the following table lists the message text, its meaning, and corrective action.

Message text	Meaning	Action
Update complete	Normal termination	None
insufficient number of parameters	Parameters are missing.	Specify correct parameters and retry.
URL is not entered	The specified content publish URL is not included in any monitoring conditions registered. Alternatively, the snapshot DB is destroyed.	Check the specified content publish URL. Check also whether it is included in the monitoring conditions registered. If the specified content publish URL is normal and is included in the

Message text	Meaning	Action
		monitoring conditions registered, contact an SE.
URL is too long	The specified URL exceeds the buffer length.	Check the specified content publish URL.
Can not open the file	The content list file could not be opened.	Check the content list file.
Can not read the file	The content list file could not be read.	Check the content list file.
Invalid file data format	The format of data in the content list file is invalid.	Check the content list file.
Can not write data to the file	Writing data to <content list file>.lst or <content list file>.err failed.	Check write authority for the directory containing the content list file. Alternatively, check the disk capacity.
Socket open error	The socket for connection to the Management Server could not be opened.	Retry later.
Socket connect error	An attempt to set up a connection to the Management Server failed.	Check the specified IP address and port number.
Socket connect : Not Found "%1"	The specified IP address is not found. %1: IP address	Check the specified IP address.
Socket send error	Request transmission to the Management Server failed.	Retry later.
CGI error (number = %1)	An error occurred in the snapshot registration program (CGI) on the Management Server. %1: Error code	Contact an SE

17.1.3 Tampering inspection program

The following table shows the message text, its meaning, and corrective action for the message output by the tampering inspection program.

Identifier (Event ID)	Message text	Meaning and action
031001001e (5010)	Web contents have been tampered. (Object: %1, Phase: %2, Files: %3) %1: Tamper Monitor URL %2: Phase of tamper checking %3: Number of tampered files	Tampering detection message For names of tampered files, check " 13.1.6 Action Statement window " or " Send Log Path ".
031001002e (5010)	Tamper Monitor Directory has been deleted. (Object: %1) %1: Tamper Monitor URL	Tampering detection message

Identifier (Event ID)	Message text	Meaning and action
		For Tamper Monitor Directoly, check " 13.1.6 Action Statement window " or " Send Log Path ".

17.2 Usage Analysis Function

The following explains message text, its meaning, and action to be taken.

17.2.1 Usage DB Registration Engine

ID	Message text	Meaning and action
012001024w	"No file, the database environment definition file."	Check whether the usage database environment definition file exists. If this message is output even though the usage database environment definition file exists, back up the database that produced the error and all of the files in the "log" directory under the installation directory (variable), and then contact an SE.
101002200e	"Cannot get memory."	Memory is insufficient.
102001001e	"Cannot read a internal file, '%s'. (%s', error:%.2u)"	Internal error. Back up files in the log directory under the installation directory (variable), and then contact an SE.
102001002e	"Cannot write a internal file, '%s'. (%s', error:%.2u)"	Internal error. Back up files in the log directory under the installation directory (variable), and then contact an SE.
102001101e	"Cannot get memory."	Memory is insufficient.
102002001e	"Cannot read a log file, '%s'. (%s'"	An operation (the value in parentheses is a keyword indicating the operation) related to the log file failed. Check the log file path and the log-recording format defined in the Usage DB Environment Definition File.
102002002e	"Cannot read a log file, '%s'. (%s', errno:%.2u)"	An operation (the value in parentheses is a keyword indicating the operation) related to the log file failed. Check the log file path and the log-recording format defined in the Usage DB Environment Definition File.
102002101e	"Cannot get memory."	Memory is insufficient.
102003101e	"Cannot get memory."	Memory is insufficient.
102004001e	"Cannot read a log file, '%s'. (%s'"	An operation (the value in parentheses is a keyword indicating the operation) related to the log file failed.

ID	Message text	Meaning and action
		Check the log file path and the log-recording format defined in the Usage DB Environment Definition File.
102004002e	"Cannot read a log file, '%s'. (%s', errno:%.2u)"	An operation (the value in parentheses is a keyword indicating the operation) related to the log file failed. Check the log file path and the log-recording format defined in the Usage DB Environment Definition File.
102005001e	"Cannot read a log file, '%s'. (%s)"	An operation (the value in parentheses is a keyword indicating the operation) related to the log file failed. Check the log file path and the log-recording format defined in the Usage DB Environment Definition File.
102005002e	"Cannot read a log file, '%s'. (%s', errno:%.2u)"	An operation (the value in parentheses is a keyword indicating the operation) related to the log file failed. Check the log file path and the log-recording format defined in the Usage DB Environment Definition File.
102005021e	"Invalid path, '%s'."	Check the log file defined in the Usage DB Environment Definition File.
102005022e	"Cannot read a directory, '%s'. (%s', errno:%.2u)"	Check the log file defined in the Usage DB Environment Definition File.
102005023w	"Invalid log form detected in a log file '%s', continuously."	A log read from the log file does not match the log format defined in the Usage DB Environment Definition File. Check the definition of the log format in the Usage DB Environment Definition File.
102005101e	"Cannot get memory."	Memory is insufficient.
103001003e	"[server=%s][log= %s]Database register engine stopped, because an error occurred."	Error message. Because an error occurred during analysis of analysis server log symbol: sss and analysis target log symbol: nnn of the Usage DB Environment Definition File, the Usage DB Registration Engine stopped. Search for related messages before this message and take the required action.
103001004w	"[server=%s][log= %s]Database recovery started."	Warning message. Because an error occurred during database registration of analysis server log symbol: sss and analysis target log symbol: nnn of the Usage DB Environment Definition File, recovery of the Usage DB Registration Engine was started.
103001005w	"[server=%s][log= %s]Database recovery succeed."	Warning message. Recovery of the database of analysis server log symbol: sss and analysis target log symbol: nnn of the Usage DB Environment Definition File was completed normally.

ID	Message text	Meaning and action
103001006e	"[server=%s][log=%s]Database recovery error."	Recovery of the database was not completed. Recovery of the database of analysis server log symbol: sss and analysis target log symbol: nnn of Usage DB Environment Definition File failed. Back up files in the log directory under the installation directory (variable) and in the database that failed, then contact an SE
103001007e	"[server=%s][log=%s]Database was abnormal."	Error message. If this message is output frequently, back up files in the log directory under the installation directory (variable) and in the database that failed, then contact an SE.
103001100e	"No database environment definition file."	Check whether the Usage DB Environment Definition File exists. If this message is output even when this file exists, back up files in the log directory under the installation directory (variable) and in the database that failed, then contact an SE.
103001303e	"Invalid parameter. ""	In correct parameter. If this message is output frequently, back up files in the log directory under the installation directory (variable) and in the database that failed, then contact an SE.
103003100e	"No log file for analysis."	Check whether the path specified in the Usage DB Environment Definition File is correct.
103019100e	"The database serial number exceeded was over limit."	Since the database count that can be managed by the agent was reached, analysis can no longer be conducted using this database name. Specify another database name.
1030nn200e	"Cannot get memory."	Memory is insufficient.
105001101e	"Database register engine stopped, because an error occurred."	Because an error preventing the continuation of operation occurred, the Usage DB Registration Engine stopped. Search for related messages before this message and take the required action. If no related messages are found, back up files in the log directory under the installation directory (variable), then contact an SE.
402001008e	"Cannot get memory."	Memory is insufficient.

17.2.2 Usage DB Reference Engine

ID	Message text	Meaning and action
201001001e	"Cannot get memory."	Memory is insufficient.
201001002e	"Cannot get a path."	The environment of the product cannot be accessed. If this condition continues, the environment of the product may be damaged. Reinstall the product.
201001004e	"Cannot close a file. (errno=%2u)"	Internal error. Back up files in the log directory under the installation directory (variable), then contact an SE.

ID	Message text	Meaning and action
201002001e	"Cannot locate a record. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201002002e	"Cannot read data in a file. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201002004e	"Cannot get memory."	Memory is insufficient.
201003001e	"Cannot get memory."	Memory is insufficient.
201003002e	"Cannot open a file. (path='%s', errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201003003e	"Cannot locate a record. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201003004e	"Cannot read data in a file. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201004003e	"Cannot locate a record. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201004004e	"Cannot read data in a file. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201004005e	"Invalid contents in record."	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201005003e	"Cannot locate a record. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201005004e	"Cannot read data in a file. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201005005e	"Invalid contents in record."	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201006002e	"Cannot open a file. (path='%s', errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201006003e	"Internal error."	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201006004e	"Cannot read data in a file. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201007003e	"Can not locate a record. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.

ID	Message text	Meaning and action
201008003e	"Cannot read data in a file. (errno=% .2u)"	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
201008004e	"Invalid contents in record."	Internal error. Back up files in the log directory under the variable file storage directory, and then contact an SE.
202001001e	"Cannot get memory."	Memory is insufficient.
202001101e	"Database reference engine stopped, because an error occurred."	Because an error preventing the continuation of operation occurred, the Usage DB Reference Engine stopped. Search for related messages before this message and take the required action. If no related messages are found, back up files in the log directory under the installation directory (variable), then contact an SE.
202002002e	"Cannot get memory."	Memory is insufficient.
202004002e	"Cannot get memory."	Memory is insufficient.
202006004e	"Cannot get memory."	Memory is insufficient.
202013003e	"Cannot get memory."	Memory is insufficient.
202016003e	"Cannot get memory."	Memory is insufficient.
202030006e	"Cannot get memory."	Memory is insufficient.
202033001e	"Cannot get memory."	Memory is insufficient.
202035001e	"Cannot get memory."	Memory is insufficient.
202036001e	"Cannot get memory."	Memory is insufficient.

17.2.3 Analysis window

Error messages to be displayed in the analysis window are displayed on the analysis pages.

Messages displayed on the analysis pages

If any of the error messages is displayed, analysis results on the analysis pages (such as graphs and tables) are not displayed.

Error message	Meaning and action
There is no data in this period.	<p>[Meaning]</p> <p>There is no data that satisfies the analysis conditions (analysis type and analysis term) in the database.</p> <p>[Cause]</p> <p>The following circumstances are likely:</p> <ul style="list-style-type: none"> - There are no accesses to the server to be analyzed. - Although the server was accessed, no accesses were registered by the Usage DB Registration Engine. <p>[Action]</p> <p>Check the log of the server to be analyzed and the startup status of the Usage DB Registration Engine.</p>

Error message	Meaning and action
<p>Connection timeout from server.</p> <p>Please make analysis period short, or try again after a while.</p>	<p>[Meaning]</p> <p>Analysis was done, but a time-out occurred during communication with the Usage DB Reference Engine.</p> <p>[Cause]</p> <p>The following circumstances are likely:</p> <ul style="list-style-type: none"> - Because the server load was high, processing of the Usage DB Reference Engine was not completed. - Because the load of the Usage DB Reference Engine was high, processing was not completed. <p>[Action]</p> <p>Reduce the analysis time or retry after waiting a while.</p>
<p>Data not displayed.</p> <p>Analysis data is not correct.</p>	<p>[Meaning]</p> <p>Analysis was done, but a data error was detected during communication with the Usage DB Reference Engine.</p> <p>[Cause]</p> <p>The following circumstances are likely:</p> <ul style="list-style-type: none"> - The database is damaged. <p>[Action]</p> <p>Check for errors in the Usage DB Registration Engine.</p>
<p>No response from server</p> <p>Connection timed out</p>	<p>[Meaning]</p> <p>Analysis was done, but a time-out occurred in the connection to the Usage DB Reference Engine.</p> <p>[Cause]</p> <p>The following circumstances are likely:</p> <ul style="list-style-type: none"> - The CGI of the Usage DB Reference Engine could not be accessed. - The main unit of the Usage DB Reference Engine was not started. <p>[Action]</p> <p>Check the settings of the virtual directories and the active status of services of the Usage DB Registration Engine.</p>

17.2.4 CSV output command

ID	Message text	Meaning and action
204001001w	"Operands are necessary."	An operand is needed. Check the command specification.
204001002w	"Invalid option or operand."	An option or operand is incorrect. Check the command specification.
204001003e	"This CSV file %s already exist."	An existing file was specified as the output file. Specify as the output file a new file or an existing file with the overwrite-disabled option

ID	Message text	Meaning and action
204001005e	"The server for which you input the symbol does not exist."	The specified server symbol is not defined in the Usage DB Environment Definition File. Check the definition in the Usage DB Environment Definition File.
204001009i	"Data is nothing in this period."	Information message
204001010i	"Output to %s."	Information message
204001016e	"Can not write a CSV file."	I/O error occurred during writing to the output file.
204001017e	"The database environment definition file does not exist."	Because no Usage DB Environment Definition File has been created, no database is available.
204001019e	"%s has not been analyzed yet."	The log of the specified server has not been analyzed.
204001020e	"Can not get the current working directory."	The current working directory cannot be accessed. Check the permissions for the current directory.
204001021e	"Can not delete a file."	An empty output file could not be deleted.

17.2.5 Common messages

ID	Message text	Meaning and action
011001021e	"Cannot read the start parameter definition file. (%s)"	The startup parameter definition file, which is an internal file, could not be read. If this state continues, the environment of the product may be damaged. Reinstall the product.
011001023e	"Cannot read the start parameter definition file. (line=%u)"	Specific lines of the startup parameter definition file, which is an internal file, could not be read. If this state continues, the environment of the product may be damaged. Reinstall the product.
012001021e	"Cannot read the database environment definition file. (%s)"	The Usage DB Environment Definition File could not be read. If this state continues, the environment of the product may be damaged. Reinstall the product.
012001023e	"Cannot read the database environment definition file. (line=%u)"	Specific lines of the Usage DB Environment Definition File could not be read. Check the lines whose line numbers are displayed.
012001024w	"No file, the database environment definition file."	No Usage DB Environment Definition File has been created. Create a DB environment definition file.
013001021e	"Cannot read the extended log environment definition file. (%s)"	The Extended Log Environment Definition File could not be read. If this state continues, the environment of the product may be damaged. Reinstall the product.

ID	Message text	Meaning and action
013001023e	"Cannot read the extended log environment definition file. (line=%u)"	Specific lines of the Extended Log Environment Definition File could not be read. Check the lines whose line numbers are displayed.
014001021e	"Cannot read the option definition file. (%s)"	The Option Definition File could not be read. If this state continues, the environment of the product may be damaged. Reinstall the product.
014001023e	"Cannot read the option definition file. (line = %u)"	Specific lines of the Extended Log Environment Definition File could not be read. Check the lines whose line numbers are displayed.
014001024e	"No file, the option definition file."	No Option definition file has been created. Create an option definition file.
021001101i	"Service started."	Service start report
021001103i	"Service stopped."	Service stop report
021001104e	"Service stopped, because an error occurred."	Because an error that makes continuation of the service impossible occurred, the service stopped. Search for related messages before this message and take the required action. If no related messages are found, back up files in the log directory under the installation directory (variable), then contact an SE.
022001013e	"Cannot get memory."	Memory is insufficient.
023001001e	"Cannot get memory."	Memory is insufficient.
023001101e	"Cannot use the port %u, because it is used by another application."	The Usage DB reference port is being used by another application. To change the port number, uninstall the product, and then reinstall it.
023003001e	"Cannot get memory."	Memory is insufficient.
401001001e	"Cannot get memory."	Memory is insufficient.
401001003e	"Invalid parameter is found in policy file.(path='%s' rec='%s')"	In the definition of the information for servers that are not Management Servers, the type of Usage DB is specified incorrectly.
401001004e	"The server only defined in policy.ini.(server='%s')"	The group definition information and the definition in the Usage DB Environment Definition File do not match. Check the definition of the displayed server.

Chapter 18 Command Reference

This explains the commands.

18.1 Contents Tampering Monitor

18.1.1 Contents Tampering Monitor

18.1.1.1 Content publish notifier

The content publish notifier is provided as the MpupdtCntnts command.

18.1.1.1.1 MpupdtCntnts command location

The MpupdtCntnts commands for each execution environment are stored at the following locations on this product's DVD-ROM:

Execution environment : Windows

```
<DVD-ROM>\tools\seq\windows\MpupdtCntnts.exe
```

Execution environment : Solaris

```
<DVD-ROM>\tools\seq\solaris\MpupdtCntnts
```

Execution environment : Linux

```
<DVD-ROM>\tools\seq\linux\MpupdtCntnts
```



Note

Use the proper command for the platform used. Using an improper command will result in operation failure.

18.1.1.1.2 MpupdtCntnts command specifications

Format

```
MpupdtCntnts -m <IP address> -p <port number> -u <content publish URL> [-f <content original file>] [-d]
```

```
MpupdtCntnts -m <IP address> -p <port number> -l <content list file>
```

Function

This command notifies (for registration or deletion) the Contents Tampering Monitor on the Management Server of content information.

Options

-d

Deletes content information.

-m <IP address>

Specifies the IP address of the Management Server in dot format.

-p <port number>

Specifies the port number of the Management Server in decimal notation.

*This port number is the same as that used for connection to the Management Console. It is normally 80.

-u <content publish URL>

Specifies the URL of the noticen target content on the Web server.

The URL can be specified with up to 1,023 ASCII characters. Leading http:// can be omitted.

*The -u option is disabled if the -l option is specified.

-f <content original file>

Specifies the absolute path of the original file of the notice target content.

The path can be specified with up to 1,023 ASCII characters.

*If this option is omitted, information is collected from the URL on the Web server and registered as the data of the content original copy.

*The -f option is disabled if the -l option is specified.

-l <content list file>

Specifies the absolute path of the file that contains the list of the notification target contents.

The path can be specified with up to 1,023 characters.



.....
In the content list file, one or more pairs of content publish URL (corresponding to the -u option) and content original file (corresponding to the -f option) can be defined. The content list file can thus be used to notify multiple sets of content information in a batch.

For information on the file format, refer to "[18.1.1.1.3 Content list file format](#)".

.....
When the -l option is specified, the following two files are created in the same directory as the content list file:

- <content list file name>.lst

If a notice error occurs, the line on which an error occurred in the content list file is output as is. If no notice error occurs, the file is empty.

- <content list file name>.err

If a notice error occurs, refer to the contents of both files by associating the corresponding line numbers and check for error causes.

The file with extension .lst is useful for re-notifying only the content where an error occurred.



The -u and -f options are disabled if the -l option is specified.

End status

0

Normal end

>0

Abnormal end

Output message

Refer to "[17.1.2 Content publish notifier](#)".

Examples

[Windows]

Example 1: To register content information from URL on the Web server

```
C:\> MpupdtCntnts -m 10.0.0.1 -p 80 -u http://www.aaa.bbb.ccc.com/index.html
```

Example 2: To register content information by specifying the content

```
C:\> MpupdtCntnts -m 10.0.0.1 -p 80 -u http://www.aaa.bbb.ccc.com/index.html -f C:\OriginalHTML\index.html
```

Example 3: To delete content information

```
C:\> MpupdtCntnts -m 10.0.0.1 -p 80 -u http://www.aaa.bbb.ccc.com/index.html -d
```

Example 4: To register content information in a batch using a content list

```
C:\> MpupdtCntnts -m 10.0.0.1 -p 80 -l C:\OriginalHTML\LIST
```

[UNIX]

Example 1: To register content information from URL on the Web server

```
$ MpupdtCntnts -m 10.0.0.1 -p 80 -u http://www.aaa.bbb.ccc.com/index.html
```

Example 2: To register content information by specifying the content original copy

```
$ MpupdtCntnts -m 10.0.0.1 -p 80 -u http://www.aaa.bbb.ccc.com/index.html -f /var/  
OriginalHTML/index.html
```

Example 3: To delete content information

```
$ MpupdtCntnts -m 10.0.0.1 -p 80 -u http://www.aaa.bbb.ccc.com/index.html -d
```

Example 4: To register content information in a batch using a content list file

```
$ MpupdtCntnts -m 10.0.0.1 -p 80 -l /var/OriginalHTML/LIST
```

18.1.1.1.3 Content list file format

The content list file is a text format file in which notice information for one piece of content is written on one line.

Line format

```
<operation>,<content original file>,<content publish URL>
```

Field

<operation>

Specifies one of the following types of operation for content:

a:Register

d>Delete

I:Ignore



.....
This operation is useful if it is used as follows: Prepare a list that covers all pieces of content to be noticed and change only the operation field properly when new notice or update notice is needed.
.....

<content original file>

Specifies the absolute path of the original file of the content to be noticed.

The path can be specified with up to 1,023 ASCII characters.

<contents publish URL>

Specifies the URL of the notice target content on the Web server.

The URL can be specified with up to 1,023 ASCII characters. Leading http:// can be omitted.

If this option is omitted, information is collected from the URL on the Web server and registered as the data of the content original copy.

Examples

[Windows]

Example 1: To register content information from URL on the Web server

```
a,,http://www.aaa.bbb.ccc.com/index.html
```

```
a,,http://www.aaa.bbb.ccc.com/image/mark.gif
```

Example 2: To register content information by specifying the content original copy

```
a,C:\OriginalHTML\index.html,http://www.aaa.bbb.ccc.com/index.html
```

```
a,C:\OriginalHTML\image\mark.gif,http://www.aaa.bbb.ccc.com/image/mark.gif
```

[UNIX]

Example 1: To register content information from URL on the Web server

```
a,,http://www.aaa.bbb.ccc.com/index.html
```

```
a,,http://www.aaa.bbb.ccc.com/image/mark.gif
```

Example 2: To register content information by specifying the content original copy

```
a,/var/OriginalHTML/index.html,http://www.aaa.bbb.ccc.com/index.html
```

```
a,/var/OriginalHTML/image\mark.gif,http://www.aaa.bbb.ccc.com/image/mark.gif
```

18.2 Usage Analysis Function

18.2.1 Trend Viewer

The Trend Viewer can output Usage DB data to a file in CSV format depending on the data type when the dbprt command is used.

The following explains how to use the dbprt commands.

18.2.1.1 dbprt

Format

Windows]

```
dbprt [/f]/[h] target server start day end day data type output file
```

UNIX]

```
dbprt [-f][-h] target server start day end day data type output file
```

Function

The CSV output fetches data from the Usage DB to output it in the CSV format.

Options

Windows]

Options	Meaning
/f	<p>Suppresses the overwrite confirmation of the output file.</p> <ul style="list-style-type: none"> - If /f is specified, overwrite is forcibly executed even if the file exists. - If /f is not specified, execution is canceled if the file exists.
/h	Displays the command help. For details, refer to " Command help ".

UNIX]

Options	Meaning
-f	<p>Suppresses the overwrite confirmation of the output file.</p> <ul style="list-style-type: none"> - If -f is specified, overwrite is forcibly executed even if the file exists. - If -f is not specified, execution is canceled if the file exists.
-h	Displays the command help. For details, refer to " Command help ".

Operands

Operands	Meaning										
Target server	Specify the symbol of the analysis target server set in the Usage DB Environment Definition File. (For information on the Usage DB Environment Definition File, refer to " 15.2.1 Usage DB Environment Definition File ".)										
Start day	<p>Specify the start day of the extraction period. Its format is as follows:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Form</th> <th colspan="2">Explanation</th> </tr> </thead> <tbody> <tr> <td rowspan="3">yyyymmdd</td> <td>yyy</td> <td>Christian era (1980 ·)</td> </tr> <tr> <td>mm</td> <td>Month (01 · 12)</td> </tr> <tr> <td>dd</td> <td>Day (01 · 31)</td> </tr> </tbody> </table>	Form	Explanation		yyyymmdd	yyy	Christian era (1980 ·)	mm	Month (01 · 12)	dd	Day (01 · 31)
Form	Explanation										
yyyymmdd	yyy	Christian era (1980 ·)									
	mm	Month (01 · 12)									
	dd	Day (01 · 31)									
End day	Specify the end day of the extraction period. Its format is the same as that of the start day.										
Data type	Specify the type of data to be extracted. Specify either of the following data types:										

Operands	Meaning														
	<table border="1"> <thead> <tr> <th>Data Type</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>session</td> <td>Session information</td> </tr> <tr> <td>request</td> <td>Request information</td> </tr> <tr> <td>error</td> <td>Error information</td> </tr> <tr> <td>agent</td> <td>Agent information</td> </tr> <tr> <td>link</td> <td>Link information</td> </tr> <tr> <td>response</td> <td>Response information</td> </tr> </tbody> </table>	Data Type	Explanation	session	Session information	request	Request information	error	Error information	agent	Agent information	link	Link information	response	Response information
Data Type	Explanation														
session	Session information														
request	Request information														
error	Error information														
agent	Agent information														
link	Link information														
response	Response information														
Output file	Specify the path of the file in which extracted data is stored. If the path string contains any blank character, specify the path by enclosing it in double quotation marks.														

Termination status

The return value and display message when the command finishes are as listed below:

End state	Return value	Display message
Normal end	0	The output file name was output.
Abnormal end	Greater than 0	Error message

If the command ends normally, the file displayed in the output file name is created.

If the command ends abnormally, an error message is displayed and no file is created.

An error message corresponding to each error is displayed. For details, refer to "[17.2 Usage Analysis Function](#)".

Execution Example

An execution example of the command is as follows. In this example, session information of January 2001 of the analysis target server whose symbol is "PUBLIC" is output to a file whose name is "session-2001-01.csv".

Windows]

```
C:\temp> "C:\Program Files\SystemwalkerSQC\bin\dbprt" PUBLIC 20010101 20010131 session
session-2001-01.csv
C:\Program Files\SystemwalkerSQC\bin\dbprt: Output to session-2001-01.csv
C:\temp>
```

UNIX]

```
# /opt/FJSVssqc/bin/dbprt PUBLIC 20010101 20010131 session session-2001-01.csv
/opt/FJSVssqc/bin/dbprt:Output to session-2001-01.csv
#
```


Command help

When using the dbprt command, help messages are output in the following cases:

- When an incorrect operand is specified
- When a required operand is not specified
- "/h" is specified in the operand.

Contents of a help message are as follows:

Windows]

dbprt outputs data in WWW Service Analyze Function Database to a file formed CSV according to a data kind.

dbprt [/f]/[h] server start-date end-date data-kind output-file

/f Not confirm to overwrite the output file.

/h Display help message.

server A symbol of the server in database environment definition file.

start-date Start date of an output period. Form like 20010101.

end-date End date of an output period. Form like 20010131.

data-kind A kind of output data.

output-file A file name to store the data.

Using dbprt, it required to be started the Database Register Engine in advance.

UNIX]

dbprt outputs data in WWW Service Analyze Function Database to a file formed CSV according to a data kind.

dbprt [-f][-h] server start-date end-date data-kind output-file

-f Not confirm to overwrite the output file.

-h Display help message.

server A symbol of the server in database environment definition file.

start-date Start date of an output period. Form like 20010101.

end-date End date of an output period. Form like 20010131.

data-kind A kind of output data.

output-file A file name to store the data.

Using dbprt, it required to be started the Database Register Engine in advance.

Chapter 19 Environment Maintenance

This chapter describes the maintenance of the definitions for operation and of databases.

19.1 Management Server Resources

19.1.1 Database

19.1.1.1 Usage DB

For information about backing up and restoring a usage database, see "[11.1.3 Usage DB backup and restore](#)".

19.2 Managed Server Resources

19.2.1 Database

19.2.1.1 Usage DB

For information about backing up and restoring a usage database, see "[11.1.3 Usage DB backup and restore](#)".