

# **FUJITSU Software**

## **Interstage Application Server**

A decorative horizontal band with a red-to-dark-red gradient, featuring abstract, glowing white and red lines that swirl and intersect, creating a sense of motion and energy.

# Security System Guide

Windows/Solaris/Linux

B1WS-1088-03ENZ0(00)  
August 2014

# Preface

---

## Purpose of this Document

This manual provides information on how to set up and operate a secure Interstage system.

### Note

Throughout this manual Interstage Application Server is referred to as Interstage.

## Intended Readers

This document is intended for users installing and operating Interstage Application Server.

It is assumed that readers of this manual have a basic knowledge of the following:

- Authentication and access control
- The Internet
- XML
- SOAP and Web services
- SOAP security extension: Basic knowledge of electronic signatures (XML electronic signature and XML partial cipher).
- Basic knowledge of the OS used

## Structure of This Document

The structure of this manual is as follows:

### [Part 1 Security Risks and Measures](#)

#### [Chapter 1 Security Risks](#)

This chapter explains security risks.

#### [Chapter 2 Security Measures](#)

This chapter explains security measures.

### [Part 2 Authentication and Access Control](#)

#### [Chapter 3 Authentication and Access Control for the Interstage HTTP Server](#)

This chapter explains how to use the authentication and access control for the Interstage HTTP Server.

#### [Chapter 4 Access Control for the Interstage Directory Service](#)

This chapter describes the access control provided by the Interstage Directory Service.

#### [Chapter 5 Security Audit Trail Functions](#)

### [Part 3 Firewall and Proxy Server](#)

#### [Chapter 6 HTTP Tunneling](#)

This chapter explains how to use HTTP tunneling.

#### [Chapter 7 HTTP Tunneling of J2EE](#)

This chapter explains how to use HTTP tunneling with J2EE.

#### [Chapter 8 Linkage of the Proxy](#)

This chapter explains proxy linkage.

### [Part 4 Authentication and Encrypted Communications through Support for SSL](#)

#### [Chapter 9 Setting and Use of the Interstage Certificate Environment](#)

This chapter explains setting of the Interstage Certificate Environment ,and use of it.

## Chapter 10 Setting and Use of the Certificate/Key Management Environment Using the SMEE Command

This chapter explains how to configure and use the Certificate/Key Management Environment with the SMEE command.

## Chapter 11 How to Use SSL with Interstage HTTP Server

This chapter explains how to use SSL with the Interstage HTTP Server

## Chapter 12 How to Use SSL with the CORBA Service

This chapter explains how to use SSL with the CORBA Service.

## Chapter 13 How to Use SSL with J2EE

This chapter explains how to use SSL with J2EE.

## Chapter 14 Using SSL for Interstage Directory Service

This chapter explains SSL communication for the Interstage Directory Service.

## Appendix A Enhancing Security (Protecting Interstage Resources)

This appendix explains enhancing security in the internet environment.

## Appendix B Security Trends

This appendix describes security trends, implementations and recommendations for Application Server.










## Appendix C List of Certificates Integrated in Interstage

This appendix contains the list of certificates integrated with Interstage.

## Conventions

### Representation of Platform-specific Information

In the manuals of this product, there are parts containing content that relates to all products that run on the supported platform. In this case, an icon indicating the product platform has been added to these parts if the content varies according to the product. For this reason, refer only to the information that applies to your situation.

	Indicates that this product (32-bit) is running on Windows.
	Indicates that this product (64-bit) is running on Windows.
	Indicates that this product (32/64-bit) is running on Windows.
	Indicates that this product (32-bit) is running on Solaris.
	Indicates that this product (64-bit) is running on Solaris.
	Indicates that this product (32/64-bit) is running on Solaris.
	Indicates that this product (32-bit) is running on Linux.
	Indicates that this product (64-bit) is running on Linux.
	Indicates that this product (32/64-bit) is running on Linux.

## Abbreviations

Read occurrences of the following Components as their corresponding Service.

Service	Component
CORBA Service	ObjectDirector
Component Transaction Service	TransactionDirector

## Export Controls

Exportation/release of this document may require necessary procedures in accordance with the regulations of the Foreign Exchange and Foreign Trade Control Law of Japan and/or US export control laws.

## Trademarks

Trademarks of other companies are used in this documentation only to identify particular products or systems.

Product Trademarks/Registered Trademarks
Microsoft, Active Directory, ActiveX, Excel, Internet Explorer, MS-DOS, MSDN, Visual Basic, Visual C++, Visual Studio, Windows, Windows NT, Windows Server, Win32 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Other company and product names in this documentation are trademarks or registered trademarks of their respective owners.

## Copyrights

Copyright 2002-2014 FUJITSU LIMITED

April 2014 Third Edition
November 2012 First Edition

# Contents

---

Part 1 Security Risks and Measures.....	1
Chapter 1 Security Risks.....	3
1.1 Interstage Management Console.....	3
1.1.1 Resources to be Protected.....	3
1.1.1.1 Functions to be Protected.....	3
1.1.1.2 Resources to be Protected.....	3
1.1.2 Possible Security Risks to Resources.....	3
1.1.3 Countermeasures against Threats.....	3
1.1.3.1 Countermeasures against Decryption of User IDs and Passwords.....	4
1.1.3.2 Countermeasures against Exploitation of User IDs and Passwords.....	4
1.1.3.3 Countermeasures against Tampering of Data Recorded In Files.....	4
1.1.3.4 Countermeasures against Exploitation of Information Recorded in Files.....	4
1.1.3.5 Countermeasures against Damage to Files.....	4
1.2 J2EE Application.....	4
1.2.1 Resources to be Protected.....	4
1.2.1.1 Functions Used for Operation of J2EE Applications.....	5
1.2.1.2 Resources to be Protected.....	5
1.2.2 Possible Security Risks.....	5
1.2.3 Possible Countermeasures.....	6
1.2.3.1 Countermeasures against Decryption of Passwords.....	6
1.2.3.2 Countermeasures against Exploitation of Passwords.....	7
1.2.3.3 Countermeasures against Tampering of Data Recorded in Files.....	7
1.2.3.4 Countermeasures against Exploitation of Information Recorded in Files.....	7
1.2.3.5 Countermeasures against Damage to Data.....	7
1.2.3.6 Countermeasures against Damage to Files.....	7
1.3 Database Linkage Service.....	7
1.3.1 Resources to be Protected.....	7
1.3.1.1 Functions to be Protected.....	7
1.3.1.2 Resources to be Protected.....	8
1.3.2 Possible Threats to Resources.....	9
1.3.3 Countermeasures against Threats.....	10
1.3.3.1 Operations Confined to Specific Users.....	10
1.3.3.2 Periodic Backup.....	11
1.3.3.3 Use of the Security Function Provided by the Resource.....	12
1.4 OLTP Function.....	12
1.4.1 Resources to be Protected.....	12
1.4.1.1 Functions to be Protected.....	12
1.4.1.2 Resources to be Protected.....	13
1.4.2 Possible Threats to Resources.....	13
1.4.3 Countermeasures against Security Risks.....	14
1.4.3.1 Countermeasures against Decryption of Passwords.....	15
1.4.3.2 Countermeasures against Exploitation of Passwords.....	15
1.4.3.3 Countermeasures against Tampering of Data Recorded in the File.....	15
1.4.3.4 Countermeasures against Exploitation of Information Recorded in Files.....	15
1.4.3.5 Countermeasures against Damage to Data.....	15
1.4.3.6 Countermeasures against Damage to Files.....	15
1.5 Interstage Directory Service.....	15
1.5.1 Resources Requiring Security Protection.....	16
1.5.1.1 Interstage Directory Service Functions and Resources Requiring Protection.....	16
1.5.2 Potential Security Threats.....	16
1.5.3 Threats and Security Measures.....	17
1.5.3.1 Password Encryption.....	17
1.5.3.2 Communication Data Encryption.....	17
1.5.3.3 Periodic Change of Passwords.....	18

1.5.3.4 Operation by Limited Users.....	18
1.5.3.5 Access control settings.....	18
1.5.3.6 Periodic Data Backup.....	18
1.5.3.7 Setting Access Rights for Files.....	19
1.6 Interstage Single Sign-on.....	19
1.6.1 Configuration Model.....	19
1.6.2 Possible Threats.....	19
1.6.2.1 Threats when a business server or authentication server is located within a DMZ.....	19
1.6.2.2 Deleting, Rewriting, and Exposing Server Resources.....	21
1.6.2.3 Rewriting and Exposure of Communication Contents.....	21
1.6.2.4 User Spoofing.....	21
1.6.2.5 Authentication Server Spoofing.....	21
1.6.2.6 Threats resulting from leaving a terminal unattended.....	22
1.6.2.7 DoS Attack.....	22
1.6.2.8 Application Risk.....	22
1.6.2.9 Client Risk.....	22
1.6.2.10 Information Leakage Threat.....	22
1.6.3 Security Measures.....	22
1.6.3.1 Protecting the Authentication Infrastructure Setup File and Business System Setup File.....	22
1.6.3.2 Setting Access Permission for Operating Resources.....	22
1.6.3.3 Protecting Communication Contents.....	23
1.6.3.4 Countermeasures against Password Attacks.....	23
1.6.3.5 Confirming the Authentication Server.....	24
1.6.3.6 Managing authentication validity periods.....	24
1.6.3.7 Operating and Managing a Business Server.....	24
1.6.3.8 Application Programming.....	24
1.6.3.9 Applying Patches.....	25
1.6.3.10 Messages Displayed on the Web Browser.....	25
1.7 Multi Server Management .....	25
1.7.1 Configuration Model .....	25
1.7.2 Resources to be Protected .....	26
1.7.2.1 Functions to be Protected.....	26
1.7.2.2 Resources to be Protected.....	26
1.7.3 Possible Security Risks to Resources.....	27
1.7.4 Threat Prevention .....	27
1.7.4.1 Countermeasures against Decryption of User IDs and Passwords.....	27
1.7.4.2 Countermeasures against Exploitation of User IDs and Passwords.....	27
1.7.4.3 Countermeasures against Tampering of Data Recorded In Files.....	27
1.7.4.4 Countermeasures against Exploitation of Information Recorded in Files.....	28
1.7.4.5 Countermeasures against Damage to Files.....	28
1.8 Configuration Management Function.....	28
1.8.1 Configuration Management Function Usage Model.....	28
1.8.2 Resources to be Protected.....	29
1.8.2.1 Functions to be Protected.....	29
1.8.2.2 Resources to be Protected.....	29
1.8.3 Possible Security Risks to Resources.....	29
1.8.4 Threat Prevention.....	29
1.8.4.1 Countermeasures against Overwriting Information Recorded in Files.....	29
1.8.4.2 Countermeasures against Exploiting Information Recorded in Files.....	30
1.8.4.3 Countermeasures against File Corruption.....	30
Chapter 2 Security Measures.....	31
2.1 Common Security Measures.....	31
2.1.1 Notes on User Accounts.....	31
2.1.2 Backup.....	31
2.1.3 Notes on Interstage Installation Resources.....	31
2.2 Security Measures for Interstage Management Console.....	32

2.3 Security Measures for Operation of the Interstage HTTP Server.....	32
2.4 Security Measures for the Servlet Service.....	35
2.5 Security Measures for the EJB Service.....	36
2.5.1 Resources to be Protected.....	36
2.5.1.1 Resources to be Protected.....	36
2.5.2 Possible Threats to Resources.....	37
2.5.3 Countermeasures Against Threats.....	37
2.5.3.1 Confining Operation to Specific Users.....	37
2.5.3.2 Periodic Backup.....	38
2.5.3.3 SSL Encryption.....	38
2.6 Security Measures for Interstage JMS.....	38
2.7 Security Measures for CORBA Service.....	39
2.8 Security Measures for Portable-ORB.....	40
2.9 Security Measures for Event Service.....	41
2.10 Security Measures for IJServer Operation.....	42
2.11 Security Measures Concerning Operation of Interstage Directory Service.....	42
2.12 Measures for Multi Server Management.....	43
2.13 Measures for Configuration Manager.....	43
Part 2 Authentication and Access Control.....	44
Chapter 3 Authentication and Access Control for the Interstage HTTP Server.....	45
3.1 Types of Authentication.....	45
3.1.1 User Authentication (Basic Authentication).....	45
3.1.2 IP Access Control.....	46
3.1.3 Client Authentication.....	46
3.1.4 Online Collation.....	46
3.2 Setting the User Authentication.....	47
3.3 Setting the IP Access Control.....	49
3.4 Setting the Client Authentication.....	50
3.4.1 Set the Environment Definition File.....	51
3.5 Setting the Online Collation Function.....	53
3.5.1 Setting the Directory Server Environment.....	54
3.5.2 Setting the SSL Environment.....	56
3.5.3 Set the Environment Definition File.....	59
3.6 Relating Directives.....	67
3.6.1 Allow.....	68
3.6.2 AuthLDAPAttribute.....	68
3.6.3 AuthLDAPbasedn.....	69
3.6.4 AuthLDAPBindDN.....	69
3.6.5 AuthLDAPBindPassword.....	70
3.6.6 AuthLDAPCertPath.....	71
3.6.7 AuthLDAPEnabled.....	71
3.6.8 AuthLDAPHost.....	72
3.6.9 AuthLDAPPort.....	73
3.6.10 AuthLDAPSecure.....	73
3.6.11 AuthLDAPSecureVersion.....	74
3.6.12 AuthLDAPSslotPath.....	74
3.6.13 AuthLDAPTknLbl.....	75
3.6.14 AuthLDAPTknPwd.....	76
3.6.15 AuthName.....	76
3.6.16 AuthType.....	76
3.6.17 AuthUserFile.....	77
3.6.18 Deny.....	77
3.6.19 <Directory>.....	78
3.6.20 DirectoryIndex.....	78
3.6.21 Group.....	79
3.6.22 LoadModule.....	79

3.6.23 <Location>.....	80
3.6.24 Order.....	80
3.6.25 Redirect.....	81
3.6.26 Require.....	82
3.6.27 RewriteCond.....	82
3.6.28 RewriteEngine.....	84
3.6.29 RewriteRule.....	84
3.6.30 SSLCertExpand.....	87
3.6.31 SSLNotifyVers.....	88
3.6.32 User.....	88
<b>Chapter 4 Access Control for the Interstage Directory Service.....</b>	<b>90</b>
4.1 Designing Access Control.....	90
4.2 Defining Access Control Lists.....	91
4.2.1 File Format.....	91
4.2.2 Editing the Access Control List Definition File.....	92
4.2.3 Evaluation of Access Control List Definitions.....	97
4.3 Registering Access Control Lists.....	99
<b>Chapter 5 Security Audit Trail Functions.....</b>	<b>101</b>
5.1 Access Log.....	101
5.2 Login Log.....	106
5.3 Login Log Operations.....	111
5.4 Application Interface Details.....	112
<b>Part 3 Firewall and Proxy Server.....</b>	<b>114</b>
<b>Chapter 6 HTTP Tunneling.....</b>	<b>115</b>
6.1 HTTP Data Communication Using HTTP Tunneling.....	115
6.2 HTTP Tunneling Setup.....	116
6.2.1 Setting up the Web Server Environment.....	116
6.2.2 Setting up the Client Environment.....	118
6.2.3 Setting up HTTP Tunneling.....	119
6.2.4 Setting to be Made When an HTTP Proxy Server is to be Used.....	122
<b>Chapter 7 HTTP Tunneling of J2EE.....</b>	<b>123</b>
7.1 Use of HTTP Tunneling in J2EE Application Client.....	123
7.2 Method for Using HTTP Tunneling with IJServer (Contains Web Applications Only).....	123
7.3 Method for Using HTTP Tunneling with Java Applets.....	123
<b>Chapter 8 Linkage of the Proxy.....</b>	<b>125</b>
8.1 Linkage of the Proxy and Interstage Web Service.....	125
8.2 Linkage of the Proxy and Web Service Function of Java EE.....	125
<b>Part 4 Authentication and Encrypted Communications through Support for SSL.....</b>	<b>126</b>
<b>Chapter 9 Setting and Use of the Interstage Certificate Environment.....</b>	<b>128</b>
9.1 Certificates and Private Keys.....	128
9.2 Configuring Environments.....	130
9.2.1 Setting up Access Permissions in the Interstage Certificate Environment.....	130
9.3 Configuring the Interstage Certificate Environment with CSR.....	131
9.3.1 Configuring an Interstage Certificate Environment and Creating a Certificate Signing Request (CSR).....	132
9.3.2 Requesting Certificate Issuance.....	133
9.3.3 Registering Certificates and CRL.....	133
9.4 Configuring the Interstage Certificate Environment with PKCS#12.....	135
9.4.1 Configuring the Interstage Certificate Environment.....	135
9.4.2 Registering PKCS#12 Data, Certificates, and CRLs.....	135
9.5 Configuring Certificate Settings.....	137
9.5.1 Defining the Use of Certificates.....	137



9.5.2 Setting Up Various Service Environments.....	137
9.6 Certificate Management.....	138
<b>Chapter 10 Setting and Use of the Certificate/Key Management Environment Using the SMEE Command.....</b>	<b>140</b>
10.1 SSL Libraries Used with the Certificate/Key Management Environment.....	140
10.1.1 Types of SMEE Libraries.....	141
10.1.2 Certificate/Key Management Environment.....	141
10.2 Environment Setting for Certificate/Key Management Environment.....	144
10.2.1 Creating a Certificate/Key Management Environment.....	145
10.2.2 Creating a Private Key and Acquiring a Certificate.....	146
10.2.3 Registering the Certificate and CRL.....	147
10.3 Operating the Client Certificate.....	148
10.3.1 Obtaining the Client Certificate.....	148
10.3.2 Registering the Client Certificate.....	149
10.4 Resource Registration.....	149
10.5 Management of a Certificate/Key Management Environment.....	150
<b>Chapter 11 How to Use SSL with Interstage HTTP Server.....</b>	<b>152</b>
11.1 SSL for Interstage Certificate Environments.....	152
11.1.1 Creating the Interstage Certificate Environment.....	152
11.1.2 Setting the Interstage HTTP Server environment.....	152
11.2 SSL for Certificate/Key Management Environments Configured with the SMEE Commands.....	153
11.2.1 Creating the Certificate/Key Management Environments Configured with the SMEE Commands.....	154
11.2.2 Registering the User PIN.....	154
11.2.3 Setting the Interstage HTTP Server Environment.....	155
11.3 Relating Directives.....	159
11.3.1 Alias.....	160
11.3.2 CustomLog.....	160
11.3.3 DocumentRoot.....	162
11.3.4 ErrorLog.....	163
11.3.5 Group.....	164
11.3.6 Listen.....	164
11.3.7 LoadModule.....	165
11.3.8 LogFormat.....	165
11.3.9 ScriptAlias.....	168
11.3.10 ServerAdmin.....	169
11.3.11 ServerName.....	169
11.3.12 ServerRoot.....	170
11.3.13 SetEnvIf.....	171
11.3.14 SSLCertExpand.....	172
11.3.15 SSLCertExpire.....	172
11.3.16 SSLCertName.....	174
11.3.17 SSLCipherSuite.....	174
11.3.18 SSLCICACertName.....	176
11.3.19 SSEnvDir.....	177
11.3.20 SSExec.....	178
11.3.21 SSLHandshakeTimeout.....	178
11.3.22 SSSLIBMultiSession.....	179
11.3.23 SSLMaxSession.....	179
11.3.24 SSLNotifyVers.....	180
11.3.25 SSLSlotDir.....	180
11.3.26 SSLTokenLabel.....	181
11.3.27 SSLUserPINFile.....	181
11.3.28 SSLVerifyClient.....	182
11.3.29 SSLVersion.....	183
11.3.30 Timeout.....	184
11.3.31 User.....	184
11.3.32 <VirtualHost>.....	185

Chapter 12 How to Use SSL with the CORBA Service.....	186
12.1 SSL Linkage of the CORBA Service.....	186
12.2 CORBA Server Environment Setup.....	188
12.2.1 Specifying the Addition of SSL Information at Definition of Object Reference.....	188
12.3 SSL Environment Setup in Client.....	188
12.3.1 Defining a Private Key/Certificate in CORBA Service.....	189
12.3.2 Editing config File.....	189
12.4 Environment Setup for Event Service.....	189
Chapter 13 How to Use SSL with J2EE.....	191
13.1 Environment Setup for Servlet Service.....	191
13.2 Environment Setting for EJB Service.....	191
13.3 Environment Setting for Interstage JMS.....	192
13.4 Environment Setting for Interstage Web Service.....	192
Chapter 14 Using SSL for Interstage Directory Service.....	195
Appendix A Enhancing Security (Protecting Interstage Resources).....	196
A.1 Protecting Interstage Resources.....	196
A.2 Environment Setup for Interstage Resources Protection.....	197
A.2.1 CORBA Service.....	197
A.2.2 Component Transaction Service.....	201
A.2.2.1 Generating an Extended System.....	201
A.2.2.2 Generating an Interstage System Definition File.....	201
A.2.2.3 Registering the Interstage System Definition File.....	201
A.2.2.4 Initializing Interstage.....	202
A.2.2.5 Executing the Security-Enhancing Environment Setup Command.....	202
A.2.2.6 Notes.....	202
A.2.3 Database Linkage Service.....	205
A.2.4 EJB Service.....	206
A.2.4.1 Environment Construction Just After Installation.....	206
A.2.4.2 Environment Construction after Constructing an Environment for EJB Service Job Operation (Default System Only).....	206
A.2.4.3 Environment Construction after Constructing an Environment for EJB Job Operation (Multi-System).....	207
A.2.4.4 EJB Service Operation.....	207
A.2.4.5 Details of the ejbchangemode Command.....	208
A.2.4.6 Details of the Output Messages.....	210
A.2.5 Interstage JMS.....	212
A.2.5.1 Environment Construction.....	213
A.2.6 Interstage Management Console.....	213
A.2.6.1 Environment Construction.....	213
A.2.6.2 Details of the guiseemode Command.....	213
Appendix B Security Trends.....	215
Appendix C List of Certificates Integrated in Interstage.....	216

# Part 1 Security Risks and Measures

If the system security is violated, unauthorized access by malicious attackers can cause interference and unauthorized use of system operation as well as information leakage.

This part explains security threats to the system and measures that can be implemented to secure Interstage Application Server systems constructed in a network environment.

Target resources for protection (referred to as 'protection target resources') are broadly classified into the types shown in the table below. The range of responsibility for security differs depending on the resource type, therefore take the appropriate action described in this chapter if necessary.

Resource type	Meaning	Examples of protection target resources
System environment settings files System log files	These are environment settings files that affect operation of the product.  These files are provided with the product. The product administrator is responsible for the environment settings and the information output to the system log files.	<ul style="list-style-type: none"> <li>- Interstage-related definitions</li> <li>- Naming Service data files</li> <li>- Interstage HTTP Server environment definition files</li> <li>- OTS system information storage folders</li> <li>- Trace log storage folders</li> <li>- RMP properties files</li> <li>- CORBA Service log files</li> <li>- Component Transaction Service error log files</li> <li>- Transaction log files</li> <li>- Interstage HTTP Server log files</li> </ul>
Application environment settings files Application log files	These are environment settings files that affect operation of applications that run on this product.  These files are provided with the product. The applications administrator for this product is responsible for these environment settings and the information output to the application log files.	<ul style="list-style-type: none"> <li>- WorkUnit definitions</li> <li>- IIServer environment definition files</li> <li>- IIServer log files</li> <li>- CORBA WorkUnit output files</li> <li>- Implementation repository files</li> <li>- Naming Service data files</li> <li>- Resource definition storage repositories</li> <li>- Resource access information</li> <li>- XA linkage programs</li> <li>- OTS resource management programs</li> </ul>
WorkUnits' application processes	These are processes that run according to the settings defined in system environment settings files and the application environment settings files.  The system operator is responsible for security of applications deployed to the WorkUnit. Interstage Application Server manages security of the WorkUnit application process.	<ul style="list-style-type: none"> <li>- WorkUnit application processes</li> </ul>
Applications	These are application implementations.  The system operator is responsible for the application security.	<ul style="list-style-type: none"> <li>- EAR, WAR, JAR, and RAR files that are J2EE application deployment targets</li> </ul>

Resource type	Meaning	Examples of protection target resources
	The operating system is responsible for security of files created during application installation.	
Resources required to execute applications	<p>This includes data handled in applications, definition files and their content and logs for integrated products.</p> <p>The data, definition files and logs varies for each application implementation.</p> <p>IAS provides a management function for managing resources required to execute deployed applications.</p> <p>The system operator is responsible for environment settings and output generated by deployed applications.</p> <p>Examples of methods to manage these resources include OS file management and integrated product information management.</p>	<ul style="list-style-type: none"> <li>- The user ID and password used for authentication in J2EE applications</li> <li>- Data in the database</li> <li>- Logs in the database</li> <li>- Storage information for the repository used by J2EE applications and Interstage HTTP Server</li> <li>- Repository environment definition files used by J2EE applications and Interstage HTTP Server</li> <li>- Serialized files for J2EE application session recovery</li> </ul>

Chapter 1 Security Risks.....	3
Chapter 2 Security Measures.....	31

# Chapter 1 Security Risks

This chapter explains the resources to be protected (protection target resources), possible threats to the protection target resources, and measures to be taken against the individual threats. The chapter uses representative operation models of the Interstage Application Server to explain these.

## 1.1 Interstage Management Console

This section gives an overview of possible security risks in the general operating environment of the Interstage Management Console.

### 1.1.1 Resources to be Protected

This section describes the resources to be protected when the Interstage Management Console is used.

#### 1.1.1.1 Functions to be Protected

The following functions and procedures should be protected:

- User authentication
- Connection to Web server
- Interstage Management Console

#### 1.1.1.2 Resources to be Protected

The following resources should be secured in order to protect their corresponding function:

Table 1.1 Resources to be Protected

Function	Resource
User authentication	User ID and password used for authentication
Connection to Web server (when Interstage HTTP Server is used)	Definition file for Interstage HTTP Server

### 1.1.2 Possible Security Risks to Resources

The following describes possible security threats during operation of the Interstage Management Console.

Table 1.2 Possible Security Risks to Resources

Resource	Possible threat
User authentication	<ul style="list-style-type: none"><li>- Exploitation of user IDs and passwords</li><li>- Decryption of user IDs and passwords</li></ul>
Definition file for Interstage HTTP Server	<ul style="list-style-type: none"><li>- Tampering with data recorded in the file</li><li>- Exploitation of information recorded in files</li><li>- Damage to files</li></ul>

### 1.1.3 Countermeasures against Threats

The following table lists possible countermeasures against security risks.

Table 1.3 Countermeasures

Possible threat	Countermeasures
Decryption of User IDs and Passwords	<ul style="list-style-type: none"><li>- Constraint on the user ID and password</li></ul>

Possible threat	Countermeasures
Exploitation of user IDs and passwords	- Setting the expiration date of the user ID and password
Tampering of data recorded in the file	- Setting access permissions on the file storing the information - Periodic data backup
Exploitation of information recorded in files	- Setting access permissions on the file storing the information

### 1.1.3.1 Countermeasures against Decryption of User IDs and Passwords

In an environment open to the public like the Internet, user IDs or passwords may be decrypted on their transmission route. The Interstage Management Console implements encryption of user IDs and passwords, but it is still possible for them to be decrypted. To minimize this risk, set expiration dates on user IDs and passwords and change them periodically.

### 1.1.3.2 Countermeasures against Exploitation of User IDs and Passwords

In an environment open to limited users like an intranet, it is not likely that user IDs and passwords will be decrypted. Such an environment is often the management base of user ID and password information, and the information of user IDs and passwords is often saved in a file. If this file is accessible by unauthorized users, there is a high risk of exploitation of the user ID and password information. An effective countermeasure against this threat is to set appropriate access permissions to files storing user ID and password information.

### 1.1.3.3 Countermeasures against Tampering of Data Recorded In Files

To use the Interstage Management Console, the Interstage HTTP Server environment definition file is required. If the information in this file is illicitly tampered with, it may disable the Interstage Management Console, and cause various problems. An effective countermeasure against this threat is to set appropriate access permission on this file.

Periodic backups are also effective. For information about backups, refer to Maintenance (Resource Backup) in the Interstage Operator's Guide.

### 1.1.3.4 Countermeasures against Exploitation of Information Recorded in Files

There are files storing information necessary for operation of the Interstage Management Console. The contents of these files are also a part of resources, and it is important to prevent exploitation of them. To cope with the threat of exploitation of information, it is effective to set appropriate access permission on these files.

### 1.1.3.5 Countermeasures against Damage to Files

In the environment of the Interstage Management Console there are important files like the environment definition file. If information in these files is illicitly tampered with, it may disable the Interstage Management Console and cause various problems. An effective countermeasure against this threat is to set appropriate access permissions on these files.

Periodic backups are also effective. For information about backups, refer to Maintenance (Resource Backup) in the Operator's Guide.

## 1.2 J2EE Application

---

This section gives an overview of security risks in J2EE applications.

Generally, a J2EE application performs operations with client programs using various components. The client program of a J2EE application is sometimes executed as an independent Java program and sometimes via a Web browser. When it is executed via a Web browser, a Web server mediates the operation. The Web server is generally located in a Demilitarized Zone (DMZ) so that accesses to the Web browser and intranet area go through a firewall.

The deployment of JDK to a DMZ may cause security problems. If you are running a Servlet service in a DMZ, use JRE instead of JDK to run the Servlet service to avoid this problem.

### 1.2.1 Resources to be Protected

---

This section describes the resources to be protected when a general J2EE application is used.

### 1.2.1.1 Functions Used for Operation of J2EE Applications

The following functions require security for operation of a general J2EE application:

- User authentication
- Connection to Web server
- Invocation of Servlet and EJB
- Reading data from a database
- Writing data to a database
- Operating environment setup for Web Server
- Execution environment setup for Servlet and EJB
- Deployment of a J2EE application
- Recovery of session information

### 1.2.1.2 Resources to be Protected

The following table lists the resources that are used when the corresponding function available for a J2EE application is used. If high security is required, it is best to protect these resources.

Table 1.4 Resources to be Protected

Function	Resource to be protected
User authentication	Password used for authentication
Connection to Web server(When Interstage HTTP Server is used)	Log files for Interstage HTTP Server Access log Error log
Invocation of Servlet and EJB	IJServer log file Container log Container information log
Reading data from a database	Log in the database Data in the database
Writing data to a database	Log in the database Data in the database
Operating environment setup for Web Server(When Interstage HTTP Server is used)	Definition file for the Interstage HTTP Server
Execution environment setup for Servlet and EJB	IJServer environment definition file
Deployment of a J2EE application	ear, war, jar, and rar deployment files
Recovery of session information	Serialized file of the Session Recovery

### 1.2.2 Possible Security Risks

The following describes the possible security threats posed to resources to be protected during the operation of a J2EE application.

Table 1.5 Possible Security Risks

Resource to be protected	Possible threat
Password used for authentication	Decryption of passwords

Resource to be protected	Possible threat
	Exploitation of passwords
Log files for Interstage HTTP Server	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
IIServer log file	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
Log in the database	Tampering of data recorded Exploitation of information recorded Damage to data
Data in the database	Tampering of data recorded Exploitation of information recorded Damage to data
Definition file for the Interstage HTTP Server	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
IIServer environment definition file	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
ear, war, jar, and rar deployment files	Damage to files
Serialized file of the Session Recovery	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files

### 1.2.3 Possible Countermeasures

The following outlines possible countermeasures against security risks. For further details, refer to the descriptions for each component.

Table 1.6 Countermeasures

Possible threat	Countermeasures
Decryption of passwords	Encryption of passwords
Exploitation of passwords	Setting access permissions of the file storing the password information
Tampering of data recorded in the file	Setting access permissions on the file storing the information Periodic data backup
Exploitation of information recorded in files	Setting access permissions on the file storing the information
Damage to data	Periodic data backup
Damage to files	Setting access permissions on the file

#### 1.2.3.1 Countermeasures against Decryption of Passwords

In an environment open to the public like the Internet, passwords may be decrypted on their transmission route. You can minimize this risk by encrypting passwords. Using the https protocol via a Web browser is an example of this measure.



### 1.2.3.2 Countermeasures against Exploitation of Passwords

In an environment open to limited users like an intranet, it is not likely that passwords will be decrypted. Such an environment may be the management base of the passwords, and password information is often saved in a file. If this file is accessible by unauthorized users, there is a high risk of exploitation of the information in the file. An effective countermeasure against this threat is to set appropriate access permissions on this type of file.

### 1.2.3.3 Countermeasures against Tampering of Data Recorded in Files

There are environment definition files and other such files in the operating environment of a J2EE application. If the information in these files is illicitly tampered with, it may disable a J2EE application and cause various problems. An effective countermeasure against this threat is to set appropriate access permissions on these files. Periodic backups in preparation for tampering is also an effective measure.

### 1.2.3.4 Countermeasures against Exploitation of Information Recorded in Files

There are files storing information necessary for operation of a J2EE application. The contents of these files are also a part of resources, it is important to prevent their exploitation by setting appropriate access permissions.

### 1.2.3.5 Countermeasures against Damage to Data

There are some J2EE applications that use databases. For this type of application, the data stored in those databases should also be protected. In addition to the security function that the database itself has, periodic data backup is an effective countermeasure against damage to data.

### 1.2.3.6 Countermeasures against Damage to Files

There are required files in the operating environment of a J2EE application. If these files are damaged for some reason, the J2EE application cannot operate. An effective countermeasure against this threat is to set appropriate access permissions on these files.

## 1.3 Database Linkage Service

---

The Database Linkage Service can be used with the following products:

- Interstage Application Server Enterprise Edition
- Interstage Application Server Standard-J Edition

This section gives an outline of security risks in an operating mode where the database linkage service is used.

The database linkage function is required for the use of the distributed transaction function of a J2EE application or the global transaction function (global transaction linkage) of the OLTP function.

### 1.3.1 Resources to be Protected

---

This section describes the security risks when the database linkage service is used.

#### 1.3.1.1 Functions to be Protected

The following functions and procedures are to be protected:

- OTS system environment setup
- Registration and deletion of a resource definition file
- Creation and deletion of a program for XA linkage
- Creation and deletion of a resource control program for OTS
- OTS system operation
- Operation of the resource control program for OTS
- Operation of the resource control program for JTS
- Application operation

- Manipulation of transaction
- Resource access

### 1.3.1.2 Resources to be Protected

The following table lists the resources used when the database linkage service is used. If high security is required, it is desirable to protect these resources.

Table 1.7 Resources to be Protected

Function	Resource to be protected
OTS system environment setup	Folder storing the OTS system information Transaction log file Folder storing the trace log
Registration and deletion of a resource definition file	Repository storing the resource definitions
Creation and deletion of a program for XA linkage	Program for XA linkage
Creation and deletion of a resource control program for OTS	Resource control program
OTS system operation	Folder storing the OTS system information Transaction log file Folder storing the trace log
Operation of the resource control program for OTS	Repository storing the resource definitions Resource access information
Operation of the resource control program for JTS	Repository storing the resource definitions RMP property file Resource access information Folder storing the trace log
Application operation	Repository storing the resource definitions Resource access information Folder storing the trace log
Manipulation of transaction	Transaction log file Folder storing the trace log
Resource access	Resource access information Folder storing the trace log

The following describes the locations of the resources to be protected:

#### Windows32/64

- Folder storing the OTS system information  
Folder where the database linkage service is installed: \etc folder
- Transaction log file  
Transaction log file that was specified when the OTS system was created
- Folder storing the trace log  
Folder where the database linkage service is installed: \var folder

- Repository storing the resource definitions  
Folder where the database linkage service is installed: \etc\repository folder
- RMP property file  
Folder where the database linkage service is installed: \etc\RMP.properties file
- Resource access information  
Folder where the database linkage service is installed: \etc\repository folder

**Solaris32** **Linux32/64**

- Folder storing the OTS system information  
Folder where the database linkage service is installed: /etc folder
- Transaction log file  
Transaction log file that was specified when the OTS system was created
- Folder storing the trace log  
Folder where the database linkage service is installed: /var folder
- Repository storing the resource definitions  
Folder where the database linkage service is installed: /etc/repository folder
- RMP property file  
Folder where the database linkage service is installed: /etc/RMP.properties file
- Resource access information  
Folder where the database linkage service is installed: /etc/repository folder

### 1.3.2 Possible Threats to Resources **Windows32/64** **Solaris32** **Linux32/64**

The following describes the possible security risks to the database linkage service:

Table 1.8 Possible Security Risks

Resource to be protected	Possible threat
Folder storing the OTS system information	Tampering of information Exploitation of information Damage to data Damage to file
Transaction log file	Tampering of information Exploitation of information Damage to data Damage to file
Folder storing the trace log	Tampering of information Exploitation of information Damage to data Damage to file
Repository storing the resource definitions	Tampering of information Exploitation of information Damage to data

Resource to be protected	Possible threat
	Damage to file
RMP property file	Tampering of information Exploitation of information Damage to data Damage to file
Resource access information	Decryption of passwords Exploitation of passwords

### 1.3.3 Countermeasures against Threats Windows32/64 Solaris32 Linux32/64

For the database linkage service, the following are effective measures against security invasion.

- Operation confined to specified users
- Periodic backup
- Use of the security function provided by the resource

#### 1.3.3.1 Operations Confined to Specific Users

Operations confined to specific users can be effectively secured against the following threats:

- Tampering of information
- Exploitation of information
- Damage to data
- Damage to file
- Exploitation of passwords

Operations confined to specific users can be effectively secured by the following three procedures:

- [Restraint on Services](#)
- [Construction of Environment by Specific Users](#)
- [Changing Access Permissions of Protected Resources](#)

#### Restraint on Services

By restricting remotely accessible services (such as telnet and ftp) on nodes where Interstage is operating, you can prevent unauthorized accesses. This measure is effective against unauthorized accesses made through networks.

For details about how to restrict remotely accessible services, refer to the manual for each platform.

#### Construction of Environment by Specific Users

By restricting the operation of the entire system to specific users, you can prevent tampering of information. For the database linkage service, specific users shall be selected as described below for each platform.

Windows32/64

Administrator (Administrator user)

Solaris32 Linux32/64

root (Superuser)

Using only the authorization of the selected users, start construction of the environment and operation of the database linkage service. If the environment is already established, do the following according to the functions used:

- Creation of applications  
Create applications logged in as an authorized user.
- Creation of a resource control program  
Create resource control programs logged in as an authorized user.
- Operation of the application  
Activate applications logged in as an authorized user.

### Changing Access Permissions of Protected Resources

Change the access permissions of protected resources to prohibit access by users other than authorized users. To implement this measure, the aforementioned [Construction of Environment by Specific Users](#) must be done in advance. Perform this operation also logged in as an authorized user.

The following describes the procedure:

1. Stop the OTS system and resource control program.

`isstop -f`

2. Change the access permissions for the protected resources.

The target protected resources are the following five:

- Folder storing the OTS system information
- Transaction log file
- Folder storing the trace log
- Repository storing the resource definitions
- RMP property file

**Windows32/64**

Change the access permissions using [Property] of the protected resources. For the detailed procedure, refer to the manual of the OS.

**Solaris32 Linux32/64**

Change the access permissions using the 'chmod' command. For the detailed procedure, refer to the manual of the OS.

3. Start the OTS system and resource control program.

`isstart`

### 1.3.3.2 Periodic Backup

If you backup information periodically, you can restore the environment even if the information is tampered with. Periodic backup is an effective defense against the following threats:

- Tampering of information
- Damage to data
- Damage to file

There are two procedures for periodic backup:

- [Data Backup](#)
- [Data Restoration](#)

## Data Backup

Use the 'otsbackupsys' command to perform periodic backups. By executing this command periodically, you can save information before damage is done on a resource to be protected. For more information about this command, refer to the Reference Manual (Command Edition).

## Data Restoration

Restore the data when tampering or damage is detected in a resource to be protected. Use the 'otsrestoresys' command for restoration of data. Specify the desired file that is backed up, and restore it. For more information about this command, refer to the Reference Manual (Command Edition).

### 1.3.3.3 Use of the Security Function Provided by the Resource

When a password is transmitted in an environment open to the public like the Internet, the password may be read on the transmission path. You can minimize this risk by encrypting the password. The database linkage service guarantees consistency of transactions using the publicly available interface of each resource vendor.

- Decryption of passwords

For the details of the function, refer to the manual prepared by each resource vendor.

## 1.4 OLTP Function

---

The OLTP function can be used with the following products:

- Interstage Application Server Enterprise Edition
- Interstage Application Server Standard-J Edition

This section gives an overview of the threats posed by invasion of security in a general OLTP application.

Generally, an OLTP application performs operations with a CORBA client program. This client program is executed sometimes as an independent CORBA client program and sometimes as an applet in a Web browser. Although it is usual to place the CORBA client program in an intranet area, a Web server ("HTTP Tunneling") acts as an intermediary to enable it to run if it is placed in an Internet area. This Web server is generally located in the Demilitarized Zone (DMZ) so that accesses to Internet and intranet areas go through a firewall.

### 1.4.1 Resources to be Protected

---

This section describes the resources to be protected when a general OLTP application is used.

#### 1.4.1.1 Functions to be Protected

The following functions and procedures should be protected:

- User authentication
- Invocation of the CORBA application
- Invocation of the transaction application
- Access to Naming Service
- Access to Interface Repository
- Access to the load balance (\*1)
- Interstage environment setup
- Registration and deletion of the WorkUnit definition

\*1 This is not valid for Linux (64 bit).

### 1.4.1.2 Resources to be Protected

The following table lists the resources when an OLTP application is used. If high security is required, it is desirable to protect these resources.

Table 1.9 Resources to be Protected

Function	Resource to be protected
User authentication	Password used for authentication
Invocation of the CORBA application	Log file for CORBA service Implementation Repository file Output file for the CORBA WorkUnit Log file for standard output Log file for standard error output
Invocation of the transaction application	Error log file WorkUnit definition Output file for the transaction application Standard output file for the file transaction application Standard error output file for the transaction application
Access to Naming Service	Data file for Naming Service
Access to Interface Repository	Data file for Interface Repository
Access to the load balance (*1)	Naming Service for load balance
Interstage environment setup	Definitions related to Interstage Interstage system definition file Interstage operating environment file CORBA Service operating environment file Component Transaction Service environment definition file
Registration and deletion of the WorkUnit definition	WorkUnit definition

\*1 This is not valid for Linux (64 bit).

### 1.4.2 Possible Threats to Resources

The following describes the possible security threats posed to resources to be protected in operation of an OLTP application.

Table 1.10 Possible Security Threats

Resource to be protected	Possible threat
User account used for authentication	Decryption of passwords Exploitation of passwords
Log file for CORBA service	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
Implementation Repository file	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
Output file for the CORBA WorkUnit	Tampering of data recorded

Resource to be protected	Possible threat
	Exploitation of information recorded Damage to data
Error log file	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
WorkUnit definition	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
Output file for the transaction application	Tampering of data recorded Exploitation of information recorded Damage to data
Data file for Naming Service	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
Data file for Interface Repository	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
Naming Service for load balance (*1)	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
Definitions related to Interstage	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files
WorkUnit definition	Tampering of data recorded in the file Exploitation of information recorded in files Damage to files

\*1 This is not valid for Linux (64 bit).

### 1.4.3 Countermeasures against Security Risks

The following describes possible countermeasures against security risks to the resources.

Table 1.11 Countermeasures

Possible threat	Countermeasures
Decryption of Passwords	Encryption of passwords
Exploitation of passwords	Encryption of passwords Periodic password change
Tampering of data recorded in the file	Setting access permissions on the file storing the information Periodic data backup
Exploitation of information recorded in files	Setting access permissions on the file storing the information
Damage to data	Periodic data backup



Possible threat	Countermeasures
Damage to files	Setting access permission to the file

### 1.4.3.1 Countermeasures against Decryption of Passwords

In an environment open to the public like the Internet, passwords may be decrypted on their transmission route. You can minimize this risk by encrypting passwords.

### 1.4.3.2 Countermeasures against Exploitation of Passwords

In an environment open to the limited users like an intranet, it is not likely that passwords will be decrypted. Such an environment may be the management base of the passwords, and the information of passwords is often saved in a file. If this file is accessible by unauthorized users, there is a high risk of exploitation of the password information saved in the file. An effective countermeasure against this threat is to set appropriate access permissions on this type of file.

### 1.4.3.3 Countermeasures against Tampering of Data Recorded in the File

There are environment definition files and other such files in the operating environment of an OLTP application. If the information in this file is illicitly tampered with, it may disable an OLTP application and cause various problems. An effective countermeasure against this threat is to set appropriate access permissions on this file.

Periodic backup is also effective. For the information about backup, refer to Maintenance (Resource Backup) in the Interstage Operator's Guide.

### 1.4.3.4 Countermeasures against Exploitation of Information Recorded in Files

There are files storing information necessary for the operation of an OLTP application. The contents of these files are also a part of resources, and it is important to prevent exploitation of them. To minimize the risk of exploitation of information, it is effective to set appropriate access permissions on these files.

### 1.4.3.5 Countermeasures against Damage to Data

In the operating environment of an OLTP application, there are important files like the environment definition file. If information in these files is illicitly tampered with, it may disable an OLTP application and cause various problems. An effective countermeasure against this threat is to set appropriate access permissions on these files.

Periodic backup is also effective. For backup, refer to Maintenance (Resource Backup) in the Interstage Operator's Guide.

### 1.4.3.6 Countermeasures against Damage to Files

In the operating environment of an OLTP application, there are important files like the environment definition file. If information in these files is illicitly tampered with, it may disable an OLTP application and cause various problems. An effective countermeasure against this threat is to set appropriate access permission on these files.

#### Windows32/64

Operation must be done by authorized users (Administrator) having administrator privileges. Change the permissions of the file to be accessible only to authorized users.

For the detailed procedure, refer to the manual of the OS.

#### Solaris32/64 Linux32/64

Periodic backup is also effective. For backup, refer to Maintenance (Resource Backup) in the Interstage Operator's Guide.

## 1.5 Interstage Directory Service

This section describes security risks and measures relating to operation of Interstage Directory Service.

The Interstage Directory Service function can be used with the following products:

- Interstage Application Server Enterprise Edition

## 1.5.1 Resources Requiring Security Protection

This section explains the resources requiring security protection when Interstage Directory Service is used.

### 1.5.1.1 Interstage Directory Service Functions and Resources Requiring Protection

Interstage Directory Service returns a result in response to an authentication request from a client.

Interstage Directory Service has the following functions:

- User authentication function
- Password encryption function
- Entry search function
- Entry operating function
- Interstage Directory Service operation function
- Logging function
- Operating environment definition

The following table indicates the resources requiring security protection for each function:

Function	Resources requiring protection
User authentication function	Authentication information (passwords) of the registered users (entries) Authentication information (password) for the Interstage Directory Service administrator DN (identification information)
Password encryption function	Setting information for the user password encryption method
Entry search function	Passwords contained in search results
Entry operating function	Passwords contained in entries
Interstage Directory Service operation function	Interstage Directory Service
Logging function	Log related setup files Log data
Operating environment definition	Environment definition file

## 1.5.2 Potential Security Threats

The following indicates the potential security threats to the resources requiring Interstage Directory Service protection:

Resources requiring protection	Potential threats
Authentication information (passwords) of the registered users (entries) Authentication information (password) for the Interstage Directory Service administrator DN	Password decryption Password theft
Setting information for the user password encryption method	Illegal use of Interstage Directory Service
Passwords contained in search results	Password decryption Password theft

Resources requiring protection	Potential threats
Entries and passwords contained in entries	Unauthorized access Entry and password alteration Entry and password deletion
Log related setup files	Alteration of information contained in files File destruction
Log data	Alteration of information recorded in log data Log data destruction
Environment definition file	Alteration of information contained in files File destruction

### 1.5.3 Threats and Security Measures

In Interstage Directory Service, the following measures can be taken to guard resources from security violation:

Threats	Security Measures
Password decryption Password theft	Password encryption Communication data encryption Periodic change of passwords Access control settings
Illegal use of Interstage Directory Service Unauthorized access Entry and password alteration Entry and password deletion	Operation by limited users Access control settings
Alteration of information contained in files Alteration of information recorded in log data	Periodic data backup
File destruction Log data destruction	Setting access rights for files

#### 1.5.3.1 Password Encryption

When an entry search is requested from a client to Interstage Directory Service, the password included in an entry can be retrieved in the form of an encrypted password string by using a method other than the original encryption method for user password encryption. Password encryption is a good way of protecting against the threat of password decryption.

#### 1.5.3.2 Communication Data Encryption

When operation is requested from a client to Interstage Directory Service, DNs, authentication information (passwords), and other communication data are used without being encrypted in the initial settings. The same applies to communication between a master and slave when the replication function is used.

SSL communication is used for the encryption of communication data on a communication path. By using SSL communication, SSL encryption can be a good measure for countering against the threats of password decryption and theft even if communication eavesdropping occurs.

For details on SSL communication, refer to 'Method for Using SSL in Interstage Directory Service'.

### 1.5.3.3 Periodic Change of Passwords

It is possible that a password could be guessed or decoded by a malicious person (or computer) on the communication path. It is recommended that users observe the registration and operation rules for passwords used in user authentication.

A specific example of password registration rules:

- Use a password that is difficult to guess.
  - Use upper and lower case letters, special characters, and numeric characters together.
  - Avoid using personal information (names, nicknames, telephone numbers, date of birth, and so on).
  - Use eight or more characters for a password.
- Change passwords periodically. For example, change a password four times a year (every three months), and make sure that any new passwords are different from those used in the past.

### 1.5.3.4 Operation by Limited Users

As well as the threat of password decryption and theft, not remaining in place while logged in as the Interstage Directory Service Administrator DN to the Entry Administration Tool can result in unauthorized operation.

An example of unauthorized operation:

- The password for an entry is altered or deleted.

To cope with such a threat, it is recommended that operation rules to limit users are established and observed by users.

A specific example of operation rules to limit users:

- The location in which the Entry Administration Tool is used is a special location where access is controlled so that only permitted persons can enter and leave.
- When leaving their desks, users must log out or quit the Entry Administration Tool.
- When leaving their desks, users must enable the lockout function of their computer monitor screens.

### 1.5.3.5 Access control settings

To prevent a password containing entry data from being exposed or changed by an unauthorized user, access control can be set for specific entry data that limits operations for users.

For details on how to configure access control settings, refer to "Interstage Directory Service Access Control Settings".

This function can only be used when RDB is used for the repository database.

### 1.5.3.6 Periodic Data Backup

By performing data backup periodically, the environment can be restored even if information is altered through unauthorized access. Periodic backup provides good protection against the following threats:

- Destruction or deletion of Interstage Directory Service data
- Alteration of information recorded in files
- File destruction

Use the backup command (*irepbacksys*) or database (RDB) backup function to perform periodic backups. By periodically executing backup, information prior to the destruction of protection target resources can be saved, and a required generation can be restored even when resources are destroyed. For details about the backup method, refer to "Maintenance (Resource Backup)" - "Backing Up and Restoring Resources" in the Operator's Guide (Basic Edition).

### 1.5.3.7 Setting Access Rights for Files

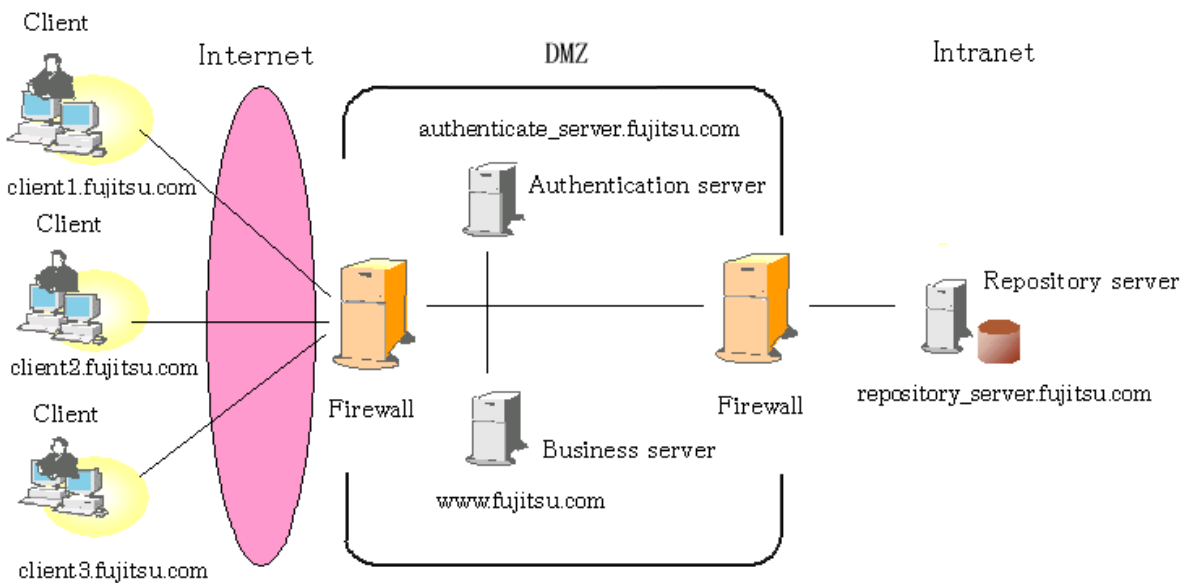
If program files, resource files, data or other files comprising Interstage Directory Service are destroyed or deleted, services may stop or a program may be unable to start in Interstage Directory Service. Setting appropriate access permission for files is an effective measure to protect against such threats. Avoid unnecessarily lowering the access permission levels that were set as initial settings.

## 1.6 Interstage Single Sign-on

This section explains the security threats for Interstage single sign-on and the countermeasures that can be taken.

### 1.6.1 Configuration Model

The figure below shows the basic configuration model for Interstage single sign-on.



#### Interstage Single Sign-on System

The Interstage Single Sign-on system consists of three types of servers: repository servers, authentication servers, and business servers. The user uses the system from the client Web browser.

Each server executes Web server programs. Programs that perform single sign-on run on the Web server programs. The authentication and repository servers verify users, and the business server authorizes the use of protection resources and provides various business services. More than one business server can be established.

If clients are to access the system from the Internet, it is possible to configure the system so that authentication and business servers are located within a DMZ. In such cases, always use the Interstage single sign-on system to perform session management. It will also be necessary to allocate the repository server in the intranet and protect it from being accessed directly from the Internet.

### 1.6.2 Possible Threats

This section explains the possible threats when using Interstage Single Sign-on.

#### 1.6.2.1 Threats when a business server or authentication server is located within a DMZ

When performing session management, it is possible to place the business server and/or the authentication server within a DMZ.

However, the risk of a server being hijacked increases when it is located in a DMZ. If a server is hijacked, there is a danger that communication data will be intercepted or falsified, or that a hijacker will masquerade as a bona fide user.

## Remark

In the unlikely event that a business server or authentication server has been hijacked, it will be necessary to update the encryption information (service ID) of all the servers making up the Interstage single sign-on system. For details on the service ID, refer to "Notes on Previous Versions" - "Service ID File" in the "Single Sign-on Operator's Guide".

The method used to update server encryption information (server ID) is explained below.

For more information about each command, refer to "Single Sign-on Operation Commands" in the Reference Manual (Command Edition).

### - Repository server

- If configured on a single repository server, or if configured with load balancing in the repository server (update system) and repository server (reference system)

1. Use the `ssoupsid` command to update the encryption information (service ID) of the repository server (or the repository server update system if more than one repository server is being used).
2. Restart the repository server. (\*1)
3. Download the authentication mechanism configuration file and send it to the authentication server, and the repository server (update system) if more than one repository server is in use.
4. Download the business system configuration file and distribute it to all business server administrators.

- If configured so that the number of repository server (update system) is increased, and the load is balanced:

1. Use the `ssoupsid` command to update the encryption information (service ID) of the repository server (update system) that is used to create a SSO repository which is operated in the master.
2. Restart the repository server. (\*1)
3. Perform the following in the machine that was used to update the encryption information (service ID)
  - Use the `ssobackup` command to export the repository server resource
  - Download the authentication infrastructure setup file, and then transfer it to the authentication server
  - Download the business system setup file, and then distribute it to the business server administrator
4. Use the `ssorestore` command to import the repository server resources that have been exported to all of the remaining repository server (update system) which are load-balancing.

### - Repository server (reference system)

If more than one repository server is in use, use the `ssoimpsv` command to update the encryption information (service ID) of the repository server (reference system) and restart the repository server (reference type) (\*1).

### - Authentication server

Use the `ssoimpac` command to update the encryption information (service ID) of the authentication server and restart the authentication server (\*1)(\*2).

### - Business server

Use the `ssoimpaz` command to update the encryption information (service ID) of the business server and restart the business server (\*1).

### - Java applications

If Java applications that use the JAAS provided by Interstage single sign-on are being used, use the `ssoimpaz` command to create a service ID file for the business server. After creating the service ID file, restart the Java application.

\*1 For details on how to restart each server and application, refer to "Operation and Maintenance" - "Stopping Single Sign-on", and "Operation and Maintenance" - "Starting Single Sign-on" in the "Single Sign-on Operator's Guide".

\*2 When Integrated Windows Authentication is used, Integrated Windows Authentication applications should also be restarted. For details on how to restart Integrated Windows Authentication applications, refer to "Operation and Maintenance" - "Stopping Single Sign-on" - "Stopping an Authentication Server", and "Operation and Maintenance" - "Starting Single Sign-on" - "Starting an Authentication Server" in the "Single Sign-on Operator's Guide".

If authentication or authorization does not proceed normally after the encryption information (service ID) has been updated, the update process may have failed. Check that all encryption information (service ID) is consistent and make any corrections that are needed.

#### **Checking the consistency of encryption information (service ID)**

- Examine the system log of each server where the encryption information (service ID) was updated to see if message sso00204 has been output.

If it has not, the encryption information (service ID) has not been updated. Perform the update procedure again and restart the server.

- Check that each server whose encryption information (service ID) has been updated or the relevant Java application was restarted after the update procedure.

Message sso00204 is output to the system log when the encryption information (service ID) is updated, so check that either a message indicating that the server was subsequently started appears in the system log, or that the relevant Java application was restarted.

If a restart has not been performed, restart the server or the Java application.

- Check that the "Service ID file consistency ID" in message sso00204 in the system logs of the repository server (reference system), authentication server and business server are the same as the "Service ID file consistency ID" in message sso00204 in the system log of the repository server (or update system if more than one repository server is in use).

If these Service ID file consistency IDs are different, update the encryption information (service ID) and restart the relevant servers.

### **1.6.2.2 Deleting, Rewriting, and Exposing Server Resources**

The repository server, authentication server, and business server contain important files to control the programs. The files include the authentication infrastructure setup file and business system setup file required for setting up each server, and the configuration file and service ID file created after setting up the servers. The possible threats to these resources are as follows:

- Deletion of resources, which disables system configuration and operation.
- Rewriting of resources, which causes results not intended by the administrator (e.g., disabled authentication or authorization).
- Exposure of resources, which causes user spoofing or system takeover.

### **1.6.2.3 Rewriting and Exposure of Communication Contents**

Important data items (e.g., user name, password, and authentication or authorization control information) are exchanged between the servers or between a Web browser (client) and a server. If these data items are rewritten, authentication or authorization may be controlled incorrectly. Interception of such data involves the risk of password leakage or spoofing.

Communication contents could be leaked by network interceptors, or by someone tapping into the information on the proxy server log or business server access log along the communication route.

### **1.6.2.4 User Spoofing**

Interstage Single Sign-on verifies users with one or both of two authentication methods: certificate authentication and password authentication using the user name and password.

Certificate authentication requires a security key paired with the certificate. Leakage of this key may cause spoofing. Similarly, password authentication requires the user name and password, leakage of which may cause spoofing. It is particularly dangerous to use a simple password because it can be guessed and tried by others relatively easily. The attacker may use a special program to make a dictionary or use the brute force attack method to decode.

### **1.6.2.5 Authentication Server Spoofing**

In password authentication, the authentication server asks the user to provide the user name and password. In practical terms, the Web browser prompts the user to enter the user name and password in the dialog box. The authentication request is usually issued when the user accesses the business server via a Web browser.

However, it is difficult to confirm that the Web browser requesting the user name and password is representing the proper authentication server. It is possible that an attacker posing as the authentication server could trick users into entering their names and passwords. Users could unknowingly give out their user names and passwords to a server prepared by the attacker.

### 1.6.2.6 Threats resulting from leaving a terminal unattended

If a user leaves his or her seat while services are being used, there is a danger that an attacker can use that user's Web browser, which has already been authenticated, to perform illegal activities. As long as the user's authentication remains valid, the attacker can masquerade as that user and access the business system.

### 1.6.2.7 DoS Attack

In a denial of services (DoS) attack, the attacker generates a large amount of accesses to the system to create heavier loads for the server. This leads to slower response resulting in deterioration of the service quality, or excludes regular users from using the services.

### 1.6.2.8 Application Risk

Interstage Single Sign-on stores important information in the Web browser cookie. The attacker could collect cookies for spoofing when the application operating on the business server is vulnerable, e.g., cross site scripting (XSS) or allocation of a malevolent application.

### 1.6.2.9 Client Risk

When an attacker takes advantage of Web browser defects and obtains cookie information, vulnerability may become apparent. This could pose a threat to Interstage Single Sign-on because the user uses a Web browser for the client.

### 1.6.2.10 Information Leakage Threat

Interstage Single Sign-on allows users to customize the messages displayed on the Web browser according to the user environment. The information in this message could provide an opportunity for attackers.

## 1.6.3 Security Measures

---

This section explains the action require to handle assumed threats.

### 1.6.3.1 Protecting the Authentication Infrastructure Setup File and Business System Setup File

The authentication infrastructure setup file and business system setup file are required for setting up a repository server, authentication server, and business server. Manage the files (and the password specified when downloading them) so that they cannot be leaked to a third party, and transfer them by safe means.

The downloaded authentication infrastructure setup file and business system setup file are encrypted using a password specified when downloading them. Exposure of the file contents may cause user spoofing or system takeover, so always delete these files once the server configuration is complete.

If it has been found that a business server or authentication server has been hijacked, update the encryption information (service ID) used in the Interstage single sign-on system and disable the encryption information (service ID) that has been used up to that point.

The method used to update the encryption information (service ID) is explained in "[1.6.2.1 Threats when a business server or authentication server is located within a DMZ](#)".

### 1.6.3.2 Setting Access Permission for Operating Resources

To protect operating resources on servers, appropriate access permissions must be established for the operating resources. Minimize the number of users or programs that can access the resources to protect them from deletion, rewriting, or exposure by an attacker.

Interstage Single Sign-on grants appropriate access permissions to operating resources. When changing the effective user of the Web server, also change the access permissions.

The administrator may delete operating resources by mistake, so periodically back up the operating resources.

To change the effective user of the Web server, see "Operation and Maintenance" in the Single Sign-on Operator's Guide. To back up operating resources, see the Operator's Guide.



### 1.6.3.3 Protecting Communication Contents

Encryption is an effective way of protecting communication contents from being rewritten or exposed. Use https as the protocol for the authentication and business servers and encrypt the communication contents. The SSL environment is required to operate https. The repository server need not use SSL communication because the Interstage Single Sign-on program encrypts the communication contents.

To set up environments for the authentication and business servers using https, see "Environment Setup (SSO Administrators)" and "Environment Setup (Business Server Administrators)" in the Single Sign-on Operator's Guide.

To operate the system more securely and prevent DoS attacks, install a firewall to protect the authentication and repository servers. For details, see "More Secure Use" in the Single Sign-on Operator's Guide.

### 1.6.3.4 Countermeasures against Password Attacks

The password used for authentication may be stolen and abused. Password theft includes brute force attack and dictionary attacks using hacking tools. To operate the system more securely, educate users using the items described below.

In a practical sense, add the operation requirements and security policy of the target system to determine the rules.

Interstage Single Sign-on consolidates the management of resource information using the Interstage Directory Service. The administrator DN authentication information (password) required for using the Interstage Directory Service must also be protected. Refer to "[1.5 Interstage Directory Service](#)" for details of the threats and countermeasures for the authentication information (password) of the Interstage Directory Service administrator DN.

#### Difficult-to-guess Password

Use a password that cannot be easily guessed by others or identified mechanically by some kind of tool.

A difficult-to-guess password should meet the following conditions:

- Cannot be guessed from personal information, e.g., name or birthday.
- Comprises the longest character string possible.
- Contains uppercase and lowercase letters, numbers, and symbols.
- Contains one complete word without modification.
- Is not a simple character string such as a repetition of the same character.

#### Password Management Method

The password must not be known to others. The following actions are very unwise:

- Disclosing the password to others.
- Leaving a note containing the password where others can see it.
- Storing the password in the Web browser.

#### Periodical Change of the Password

Even if the above two items are addressed, the password may be leaked. Periodically change the password to ensure secure operation.

##### Note

Interstage Single Sign-on does not provide a password change function. Educate users to change the password with appropriate frequency according to the system to be used.

If a password is guessed or stolen by others, stop all business servers and confirm whether the re-authentication interval that was set with either of the following operations has passed:

- Re-authentication interval for each user, set in ssoCredentialTTL of user information in the SSO repository.
- Standard re-authentication interval, configured in the Interstage Management Console, [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab > [Detailed Settings [Show]] > [Operation after Authentication] > [Re-authentication Interval].

After the re-authentication interval has passed, change the guessed or stolen password and restart all business servers.

### 1.6.3.5 Confirming the Authentication Server

It is necessary to advise users not to enter user names or passwords, by mistake, into the form authentication page or password authentication dialog represented by a false authentication server.

- Announce the correct authentication server host name (URL) to users.
- Have users access the business server via bookmarks set in their Web browsers or from links on reliable Web sites.
- When the requesting source in the basic authentication dialog could be faulty, make users cancel the dialog and confirm whether the URL displayed in the address display area of the Web browser matches that of the correct authentication server.
- If the requesting source of the form authentication page displayed by the Web browser is not clear, have the user confirm that the URL displayed in the address display area of the Web browser matches that of the correct authentication server.

### 1.6.3.6 Managing authentication validity periods

If a user leaves his or her seat for any length of time, an attacker can gain access to a business system through that user's authenticated Web browser. To prevent this, it is necessary to manage the period that a user's authentication remains valid (session).

- Instruct users to disable the session when they must leave their seat while services are being used.
- Design the system so that even if a user leaves his or her seat without disabling the session, the session is automatically disabled after a specified period of time.

For information about session management in Interstage single sign-on systems, refer to "Overview" in the Single Sign-on Operator's Guide.

### 1.6.3.7 Operating and Managing a Business Server

To prevent unauthorized access to the protection resources of the business server and control correct authentication or authorization, the business server must be operated and managed appropriately.

In particular, if the business server is not operated appropriately when it is integrated into Microsoft(R) Internet Information Services, access control for the protection resources may be lost. For details on how to operate business servers appropriately, refer to Setting up the First Business Server in "Environment Setup (Business Server Administrators)" of the "Single Sign-on Operator's Guide".

- Use https as the protocol of the business server and encrypt the communication contents with the Web browser.
- Do not operate an unnecessary Web service on another port of the same server.
- Create a service ID of the business server using FQDN of the business server.
- Before deploying an application such as CGI on the business server, verify that there is no security problem such as XSS.
- Minimize the number of users that can log in to the business server and record login actions.

### 1.6.3.8 Application Programming

Confirm that the application to be operated on the business server does not show vulnerability (such as buffer overflow or XSS) and is securely programmed.

This measure applies to web applications in general, and is not limited to Interstage Single Sign-on.

When using single sign-on JavaAPIs, the following threats are assumed. Take the appropriate action for each of these threats:

#### For Servlet Applications Using Single Sign-on JavaAPIs

Possible threat	Action
Application alteration	- Periodically change the password for the IJServer or IJServer cluster operation account to prevent it from being leaked or collected.
Application destruction	- Periodically back up data.
Leakage of credential information, user IDs, and passwords	- Use the Web server in SSL.

Possible threat	Action
	<ul style="list-style-type: none"> <li>- Minimize the number of access permissions to Web server access log files.</li> <li>- Use POST for the FORM method instead of GET</li> </ul>
Alteration or exposure of configuration files (login configuration file)	<ul style="list-style-type: none"> <li>- Minimize the number of access permissions to operating resources.</li> </ul>
Destruction of configuration files (login configuration file)	<ul style="list-style-type: none"> <li>- Periodically back up data.</li> </ul>

### 1.6.3.9 Applying Patches

Periodically check failure information regarding Web browsers and operating systems. If a new failure is detected, patches or workarounds are made available. Remind users to apply the latest security patches to their Web browsers. Similarly, apply the latest fix to the operating system of each server.

### 1.6.3.10 Messages Displayed on the Web Browser

When customizing messages to be displayed on users' Web browsers, use particular caution in regard to the contents.

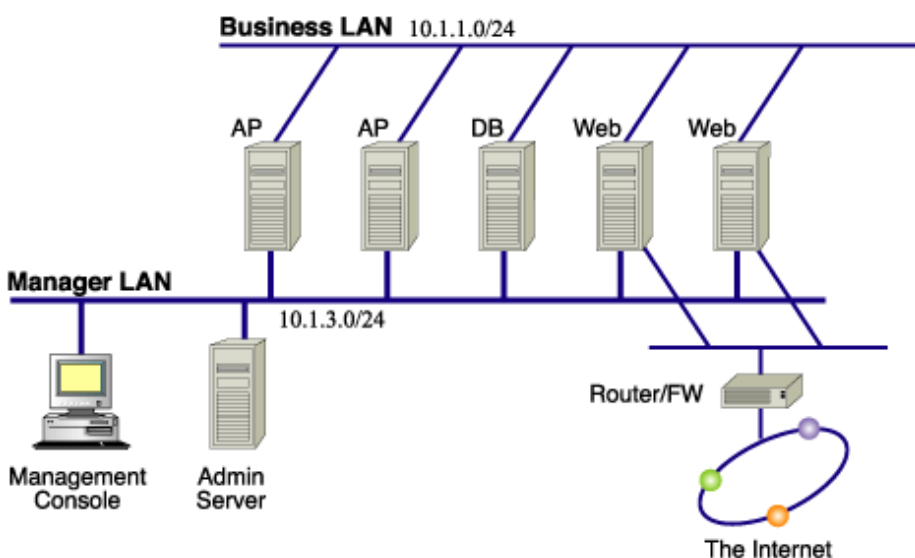
- Avoid including information that could be used as a stepping stone or clue to attacks.
- Before displaying telephone numbers, mail addresses, or URLs, verify that there will be no problem in publicizing such information.

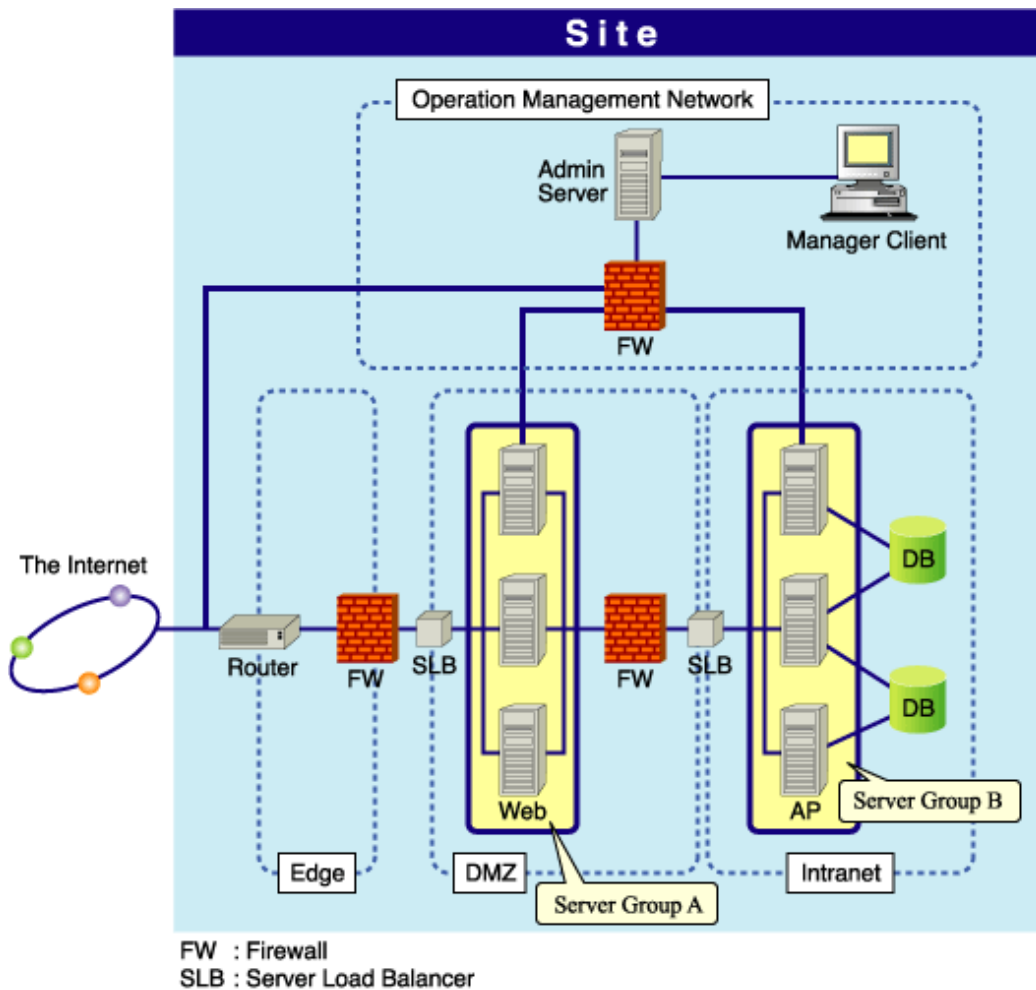
## 1.7 Multi Server Management Windows32/64 Solaris32 Linux32/64

This section describes how to deal with security threats using Multi Server Management.

### 1.7.1 Configuration Model Windows32/64 Solaris32 Linux32/64

When using Multi Server Management, the LAN for the flow of the actual business data and the LAN for the flow of operation management data between the Admin Server and Managed Server are usually separated. The former is called the "business LAN", and the latter the "management LAN". The following figure shows an overview of the business LAN and management LAN and a typical usage model for Multi Server Management.





### Multi Server Management Configuration Model

In a typical Multi Server Management configuration, one Admin Server manages one site. The site is configured using multiple servers, with servers that execute the same business applications grouped together. The Admin Server runs the servers in the site using the Interstage Management Console.

Apart from the fact that there is an Admin Server managing site operation (and that the business application is configured using multiple servers), there is no difference from the normal Interstage usage model. Refer to the operation model and Security Measures chapter for each Interstage function.

## 1.7.2 Resources to be Protected Windows32/64 Solaris32 Linux32/64

This section describes the resources to be protected when Multi Server Management is used.

### 1.7.2.1 Functions to be Protected

The following functions and procedures should be protected:

- Operations using the Interstage Management Console

### 1.7.2.2 Resources to be Protected

The following resources should be secured to protect the functions they provide:

Table 1.12 Resources to be Protected

Function	Resource
User authentication	User ID and password used for authentication
Connection to Web server (When Interstage HTTP Server is used)	Definition file for Interstage HTTP Server

### 1.7.3 Possible Security Risks to Resources

The following security threats may occur during operation of the Interstage Management Console.

Table 1.13 Possible Security Risks to Resources

Resource	Possible threat
User authentication	<ul style="list-style-type: none"> <li>- Exploitation of user IDs and passwords</li> <li>- Decryption of user IDs and passwords</li> </ul>
Definition file for Interstage HTTP Server	<ul style="list-style-type: none"> <li>- Tampering with data recorded in the file</li> <li>- Exploitation of information recorded in files</li> <li>- Damage to files</li> </ul>

### 1.7.4 Threat Prevention Windows32/64 Solaris32 Linux32/64

The following table lists countermeasures that can be taken against possible security risks.

Table 1.14 Threat Countermeasures

Possible threat	Countermeasures
Decryption of user IDs and passwords	<ul style="list-style-type: none"> <li>- User ID and password protection</li> </ul>
Exploitation of user IDs and passwords	<ul style="list-style-type: none"> <li>- Setting an expiration date for the user ID and password</li> </ul>
Tampering of data recorded in the file	<ul style="list-style-type: none"> <li>- Setting access permissions for the file storing the information</li> <li>- Periodic data backup</li> </ul>
Exploitation of information recorded in files	<ul style="list-style-type: none"> <li>- Setting access permissions for the file storing the information</li> </ul>

#### 1.7.4.1 Countermeasures against Decryption of User IDs and Passwords

In an environment open to the public like the Internet, user IDs or passwords may be decrypted on their transmission route. The Interstage Management Console implements encryption of user IDs and passwords, but it is still possible for them to be decrypted. To minimize this risk, set expiration dates for user IDs and passwords and change them periodically.

#### 1.7.4.2 Countermeasures against Exploitation of User IDs and Passwords

In an environment open to limited users like an intranet, it is not likely that user IDs and passwords will be decrypted. Such an environment is often the management base of user ID and password information, and user ID and password information is often saved in a file. If this file is accessible by unauthorized users, there is a high risk of exploitation of user ID and password information. An effective countermeasure against this threat is to set appropriate access permissions for files, storing user ID and password information.

#### 1.7.4.3 Countermeasures against Tampering of Data Recorded In Files

To use the Interstage Management Console, the Interstage HTTP Server environment definition file is required. If the information in this file is tampered with, it may disable the Interstage Management Console and cause various problems. An effective countermeasure against this threat is to set appropriate access permissions for this file. For Solaris or Linux systems, refer to Enhancing Security (Protecting Interstage Resources) in Appendix A.

Periodic backups are also effective. For backup information, refer to Maintenance (Resource Backup) in the Interstage Operator's Guide.

### 1.7.4.4 Countermeasures against Exploitation of Information Recorded in Files

The information required for operation of the Interstage Management Console is stored in files. The contents of these files are also resources, and it is important to prevent exploitation of them. An effective means of protecting these files is to set appropriate access permissions for them. For Solaris or Linux systems, refer to Enhancing Security (Protecting Interstage Resources) in Appendix A.

### 1.7.4.5 Countermeasures against Damage to Files

There are important files, such as the environment definition file, in the Interstage Management Console environment. If information in these files is tampered with, it may disable the Interstage Management Console and cause various problems. An effective countermeasure against this threat is to set appropriate access permissions for these files. For Solaris or Linux systems, refer to Enhancing Security (Protecting Interstage Resources) in Appendix A.

Periodic backups are also effective. For backup information, refer to Maintenance (Resource Backup) in the Operator's Guide.

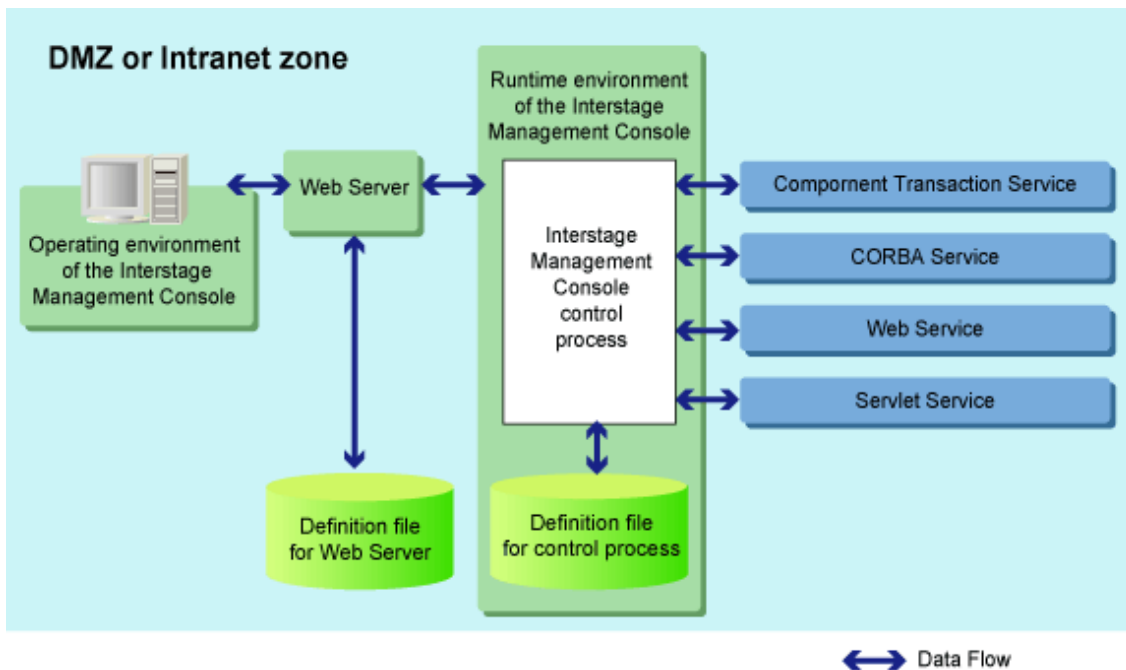
## 1.8 Configuration Management Function

This section describes how to deal with security threats using the Configuration Management function, and covers the following:

- 1.8.1 Configuration Management Function Usage Model
- 1.8.2 Resources to be Protected
- 1.8.3 Possible Security Risks to Resources
- 1.8.4 Threat Prevention

### 1.8.1 Configuration Management Function Usage Model

The following figure shows a typical usage model for the Configuration Management function.



#### Configuration Management Function Usage Model

The Configuration Management function stores operations in the Interstage Management Console internally. For this reason, users do not need to be aware of the configuration of the configuration management function. This chapter explains the settings information for the Environment Settings window in a repository that is available to the system administrator, and also explains security breach threats.

## 1.8.2 Resources to be Protected

---

This section explains the resources that should be protected for the repository that is managed by the Configuration Management function.

### 1.8.2.1 Functions to be Protected

The following functions and procedures should be protected:

- Operations using the Interstage Management Console

### 1.8.2.2 Resources to be Protected

The following resources are used in the Interstage Management Console. If advanced security measures are requested, it is advisable to protect these resources as part of that security.

Table 1.15 Resources to be Protected

Function	Resources that should be protected
Various operations using the Interstage Management Console	- Information stored in the repository

## 1.8.3 Possible Security Risks to Resources

---

Additional possible security threats to resources that should be protected against using the Configuration Management function are shown below.

Table 1.16 Possible Threats to Resources

Resources that should be protected	Additional possible threats
Information stored in the repository	<ul style="list-style-type: none"><li>- Overwriting the information that is recorded in files</li><li>- Exploiting the information that is recorded in files</li><li>- File corruption</li></ul>

## 1.8.4 Threat Prevention

---

The following table lists countermeasures that can be taken to prevent against security breaches using the Configuration Management function.

Table 1.17 Threat Countermeasures

Possible threat	Countermeasures
Overwriting the information that is recorded in files	<ul style="list-style-type: none"><li>- Implement access authority settings for the files in which information is saved</li><li>- Perform regular data backups</li></ul>
Exploiting the information that is recorded in files	<ul style="list-style-type: none"><li>- Implement access authority settings for the files in which information is saved</li></ul>
File corruption	<ul style="list-style-type: none"><li>- Implement access authority settings for the files</li></ul>

### 1.8.4.1 Countermeasures against Overwriting Information Recorded in Files

Various items of Interstage information are saved in the Configuration Management function repository in binary format. If the contents of these files are overwritten illegally, it might cause various problems, such as being unable to run Interstage. To effectively counter this type of threat, implement appropriate access authority settings for the files in which this information is saved. Regular data backups are also an effective preventative measure against files being overwritten illegally.

### 1.8.4.2 Countermeasures against Exploiting Information Recorded in Files

Various items of Interstage information are saved in the Configuration Management function repository in binary format. The descriptive content of these files is also a part of the resources, and it is important to prevent exploitation. To effectively counter this type of threat, implement appropriate access authority settings for the files in which this information is saved.

### 1.8.4.3 Countermeasures against File Corruption

In the Configuration Management function repository, there are files that determine the validity of information based on whether or not a file can be read. If these files are corrupted for some reason, registered information cannot be referenced. To effectively counter this type of threat, implement appropriate access authority settings for the files.



# Chapter 2 Security Measures

Generally, the services alone cannot completely protect resources from security attacks. Taking operational measures can also increase safety.

This chapter explains the security measures indicated in "Security Risks and Measures" separately for each service. To implement safe and firm operation against security violation, it is recommended to refer to and carry out the measures for the services used.

Security information on Fujitsu products is available from the following site. Keep checking the latest information.

<http://www.fujitsu.com/global/support/software/security/>

## 2.1 Common Security Measures

This section explains the following topics:

- [2.1.1 Notes on User Accounts](#)
- [2.1.2 Backup](#)
- [2.1.3 Notes on Interstage Installation Resources](#)

### 2.1.1 Notes on User Accounts

Windows32/64

To prevent termination of operation, alteration of resources, and leakage of information that may be done by end users, it is recommended not to register a user account that is not an authorized Administrator.

### 2.1.2 Backup

Periodic backup is recommended to minimize damage caused by external attacks, machine trouble, operation errors, and so on.

### 2.1.3 Notes on Interstage Installation Resources

Windows32/64

To prevent alteration of resources by end users, it is recommended not to set access permissions like "Everyone (full control)" that permit access from unspecified users to the folders and files under the Interstage installation.

The "issetfoldersecurity" command changes the permissions of the Interstage installation folder and subfolder. For details, refer to the Reference Manual (Command Edition).

Solaris32/64 Linux32/64

The user must select a security mode during Application Server install from:

- Secure mode (default)

If this mode is selected, Application Server operates under a stricter security environment. Interstage-related program execution permissions and file access permissions are granted only to members of the group nominated for secure mode.

- Compatibility mode

If this mode is selected, the product is installed with the same access permissions as in previous product versions.

The *issetsecuritymode* command can be used after the installation to set the security mode to secure mode or compatibility mode. For details on the *issetsecuritymode* command, refer to the Reference Manual (Command Edition).

If security mode is set to secure, the permission level required to run some commands is changed from general users to users that belong to the group nominated for secure mode. To allow a user other than root to execute these commands in secure mode, change the user's effective group to the group nominated for secure mode. The group to which a user belongs can be specified by one of the following methods:

- Specifying the effective group when the new user is created

Using the *useradd* command, the group that was specified in secure mode is specified as the owner group.

- Setting an effective group for existing users

Using the *newgrp* command, the effective group changes to the group that was specified in secure mode.

For details on how to change/check the effective group, refer to the OS documentation.

#### Note

The group nominated for secure mode cannot be deleted. Another group must be nominated for secure mode operation first.

## **2.2 Security Measures for Interstage Management Console**

---

This section explains the following topics:

- [Notes on User Accounts](#)
- [Notes on the Permissions of the Environment Definition File](#)
- [Notes on Communication Data](#)

### **Notes on User Accounts**

It is recommended to change passwords periodically to cope with possible problems like leakage of the Administrators group account information.

Permissions applied to general users can be set to restrict access to important functions such as starting and stopping Interstage from the Interstage Management Console. In Windows(R), a general user must be a member of the 'Administrators' group; in Solaris/Linux, a general user must have 'root' permission.

Also, to prevent operations occurring as a result of identity theft, the Web browser auto-complete function is disabled at the time of login.

### **Notes on the Permissions of the Environment Definition File**

To prevent alteration of resources and leakage of information by end users, it is recommended to set access permissions accordingly.

### **Notes on Communication Data**

It is recommended to use SSL encryption for server-client data.

## **2.3 Security Measures for Operation of the Interstage HTTP Server**

---

This section explains the following topics:

- [Notes When Making Access](#)
- [Notes on Communication Data](#)
- [Unauthorized Access to Resource Files](#)
- [Leakage of Password Information](#)
- [Server Information Leaks](#)
- [Threats of Denial of Service Attacks \(DoS\)](#)
- [Risk of Exploiting the HTTP TRACE Method](#)
- [Threat that the Account Name will be Discovered](#)

### **Notes When Making Access**

When an access is made from a Web browser to the Interstage HTTP server, there is a possible threat that an ill-intentioned person could make an unauthorized access to the Interstage HTTP Server by impersonating a user having proper access permission.

To prevent this, SSL encryption using SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0) client authentication is recommended. For information about SSL encryption, refer to the "How to Use SSL with Interstage HTTP Server" chapter.

### Notes on Communication Data

An ill-intentioned person could access communication data between the server and a user who has proper access permission.

SSL encryption is recommended in order to minimize this type of risk.

For information about SSL encryption, refer to the "How to Use SSL with Interstage HTTP Server" chapter.

### Unauthorized Access to Resource Files

Interstage HTTP Server has resource files listed below:

- Contents
- Environment definition file (httpd.conf)
- Access log file
- Error log file
- Trace log file
- Operation log file
- Maintenance log file
- CGI
- Environment definition file for each directory (.htaccess)

These files may be exposed to the threat of unauthorized access.

To protect these files, make these files inaccessible by end users. Making this file accessible only to users with administrator privileges is recommended (superuser for a Solaris/Linux system, and Administrator for Windows(R) system).

### Leakage of Password Information

The Interstage HTTP Server has a password file, which an ill-intentioned person may furtively look into.

The password data in the password file is encrypted; still, it is recommended that the administrator create the password file using the 'htpasswd' command to make it inaccessible by end users. For details on how to create the password file, refer to "Setting the User Authentication" in the "Authentication and Access Control for the Interstage HTTP Server" chapter.

### Server Information Leaks

If an ill-intentioned person obtains server information from the Server header field of the HTTP response header, there is a danger that they might use the OS/product information to attempt an illegal access.

To safeguard against this danger, it is recommended that the IHSServerHeader directive in the Interstage HTTP Server environment definition file (httpd.conf) is set to "Off", and that the Server header field of the HTTP response header is not sent.

```
IHSServerHeader Off
```

### Threats of Denial of Service Attacks (DoS)

An ill-intentioned person on the network could target a server and disable its services. To defend the server from Denial of Service attacks (DOS), it is recommended to use the following functions:

- User authentication:

For information about user authentication, refer to "User Authentication" in the "Authentication and Access Control for the Interstage HTTP Server" chapter.

- IP access control:

It is possible to permit access only to specific clients.

For information about IP access control, refer to "IP Access Control" in the "Authentication and Access Control for the Interstage HTTP Server" chapter.

- Use of SSL encryption:

High level of security can be retained, where client authentication is possible.

For information about SSL encryption, refer to the "How to Use SSL with Interstage HTTP Server" chapter.

- Limitations on the size of request message from client:

Set the maximum size of a request message to prevent a buffer overflow. The maximum size of the request message is set by the following directives of the environmental definition file (httpd.conf):

- LimitRequestBody
- LimitRequestFields
- LimitRequestFieldsize
- LimitRequestLine

## Risk of Exploiting the HTTP TRACE Method

Malicious users (or machines) on the network may read private information in HTTP request data or execute unwanted codes.

To prevent this risk, it is recommended that the TraceEnable directive in the Interstage HTTP Server environment definition file (httpd.conf) be set to "Off", and the HTTP TRACE method be disabled.

The TRACE method is the HTTP/1.1 method of receiving the data sent from the client side as response data. This method is used to diagnose the network environment. There is no problem in the Interstage HTTP Server operation if this method is disabled because it not usually used.

```
TraceEnable off
```

## Threat that the Account Name will be Discovered

**Solaris32/64** **Linux32/64**

There is always a risk that an account name on the Web server will be discovered on the network by a user (or machine) with malicious intent.

To counter this kind of threat, it is recommended that the settings in the Interstage HTTP Server environment settings file (httpd.conf) are made as shown below. These settings will disable requests to documents under the account user home directory.

```
LoadModule userdir_module "/opt/FJSVihs/modules/libexec/mod_userdir.so"
UserDir disabled
```

### Note

A hash mark (#) can be added to the start of the LoadModule and UserDir directives to make the line a comment.

To make a document under the account user home directory public, configure the following settings:

- Set the access authority in the home directory to be made public for access from the Web server.
- Disable the user directory settings for users that are not going to be made public.

An example of disabling the user directory settings for users that are not going to be made public is shown below.

### Example:

Making "user1" and "user2" documents under "user home directory/public\_html" public.

```
LoadModule userdir_module "/opt/FJSVihs/modules/mod_userdir.so"
UserDir public_html
UserDir disabled
UserDir enabled user1 user2
```

Making all documents, except for "user3" and "user4", under "user home directory/public\_html" public.

```
LoadModule userdir_module "/opt/FJSPihs/modules/mod_userdir.so"
UserDir public_html
UserDir disabled user3 user4
```

#### Notes:

If just "UserDir public\_html" is specified, when the "http://host name[:port number]/~user" request is received, the status code that is returned when the user name is specified as "user" depends on whether the user exists in the Solaris/Linux server. For this reason, the account name on the Web server might be discovered. These status codes are shown below.

- "user" does not exist:

The "404 Not Found" status code is returned.

- "user" exists:

The "403 Forbidden" status code is returned.

This status code is returned because, although "user" exists, access authority for access from the Web server for this user has not been set in the home directory. Specify users that can execute the Web server in the User directive.

#### Linux32/64

This problem occurs when the user home directory is created using the useradd command, and directory authority is only set for the owner, meaning that only that user has access permission.

## 2.4 Security Measures for the Servlet Service

---

This section explains the following topics:

- [Notes on the Use of Sessions](#)
- [Notes on Web Application Development](#)
- [Notes on Deployment of Web Applications](#)
- [Notes on the Root Directory of the Web Application](#)
- [Notes on Communication Data](#)
- [Notes on Session Recovery](#)

### Notes on the Use of Sessions

Session information is embedded in cookies or URL parameters.

When the Web server is connected to a Web browser via the Internet, the contents of communication are in danger of interception or alteration.

Therefore, SSL encryption is recommended.

### Notes on Web Application Development

For notes on web application development, refer to "Common Notes for Interstage" in the "Notes on Interstage Operation" chapter of the Product Notes.

### Notes on Deployment of Web Applications

#### Solaris32/64 Linux32/64

It is recommended to give write permissions only to users who execute the Servlet container to prevent alteration by end users.

### Notes on the Root Directory of the Web Application

If a directory open to the public on the Web server is the same as the root directory of the Web application, the body of the Web application including the class files and Jar files may be accessible through the Web browser.

To prevent this problem, it is recommended to make the directory made open by the Web server different from the root directory of the Web application.

### Notes on Communication Data

Possible threats to communication between the Web server connector and Servlet container are as follows:

- The Web server connector is impersonated to illegally access the Servlet container.
- Communication data is viewed by unauthorized person.
- Communication data is altered.

It is recommended to use SSL communication for protection from these threats. SSL version 3 (client authentication) is required for protection from impersonation.

Refer to "Environment Setup for Servlet Service" in the "How to Use SSL with J2EE" chapter for information on enabling SSL communication.

### Notes on Session Recovery

HTTP is used for communication between the Servlet container and the Session Registry Server.

The following security threats exist when this form of communication is used:

- Communication data is viewed by unauthorized person.
- Communication data is altered.

Communication between the Servlet container and Session Registry Server is contained within an intranet. Since security threats also exist within an intranet, use a secure network for the Servlet container and Session Registry Server.

## 2.5 Security Measures for the EJB Service

---

This section gives an outline of security risks when the EJB service is used.

EJB Service is required when the "EJB function" of J2EE applications is used.

### 2.5.1 Resources to be Protected

---

This section describes the resources to be protected when the EJB service is used.

#### 2.5.1.1 Resources to be Protected

The table below lists the resources that are used for EJB Service. When high security is required, protect these resources for security.

Table 2.1 Resources to be Protected

Function	Resource to be protected
EJB environment setup	Environment definition file of EJB Service
EJB application program operation	Environment definition file of EJB Service J2EE common directory

The following describes the locations of these resources. The directory structure of a Windows(R) system is taken for example.

- Environment definition file of EJB Service
  - All files under C:\Interstage\EJB\etc directory
  - All files under C:\Interstage\J2EE\etc directory
- J2EE common directory
  - All files under J2EE common directory

Solaris/Linux system is taken for example.

- Environment definition file of EJB Service  
All files under /opt/FJSVejb/etc directory  
All files under /opt/FJSVj2ee/etc directory
- J2EE common directory  
All files under J2EE common directory

## 2.5.2 Possible Threats to Resources

---

The following countermeasures can defend EJB Service against security invasion.

Table 2.2 Possible Threats to Resources

Resource to be protected	Threats
Environment definition file of EJB Service	Tampering of information Exploitation of information Damage to data Damage to files
J2EE common directory	Tampering of information Exploitation of information Damage to data Damage to files Exploitation of passwords

## 2.5.3 Countermeasures Against Threats

---

The following countermeasures can be used to minimize security risks for the EJB Service.

- Operation confined to authorized users
- Periodic backup
- Use of SSL encryption

### 2.5.3.1 Confining Operation to Specific Users

Confining operations to a limited set of users can be an effective defense against following threats:

- Tampering of information
- Exploitation of information
- Damage to data
- Damage to files
- Exploitation of passwords

Operation confined to specific users implements the following two procedures:

- Selection of the users
- Change of access permission to the protected resources

#### Selection of Specific Users

By fixing the operators of the entire system to a pre-specified set of users, you can prevent tampering of information.

## Change of Access Permission of the Protected Resources

Change the access permission of the resources to be protected.

### 2.5.3.2 Periodic Backup

Periodic backups make restoration of the environment possible when information is tampered with. Periodic backup is an effective defense against following threats:

- Tampering of information
- Damage to data
- Damage to files

Periodic backup implements the following two procedures:

- Backup of data
- Restoration of data

### Backup of Data

In preparation for tampering, back up the following resources periodically:

- Environment definition file of EJB Service
- J2EE common directory

If the above resources are backed up, the common J2EE resources and IIServer resources must be backed up. For detailed information about backup of the resources of EJB Service, refer to the "Maintenance (Resource Backup)" chapter of the Operator's Guide.

### Restoration of Data

If data has been damaged, restore the data.

### 2.5.3.3 SSL Encryption

The SSL encryption function is a function for data encryption using the SSL linkage of CORBA Service. Using the SSL linkage function, you can defend your system against the following threats:

- Exploitation of information
- Exploitation of passwords

For information about SSL encryption, refer to the "How to Use SSL with J2EE" chapter.

## 2.6 Security Measures for Interstage JMS

---

This section explains the following topic:

- [Unauthorized Access to Resource Files](#)

### Unauthorized Access to Resource Files

Interstage JMS Server has environment definition files as listed below:

- JNDI definition file (fjmsjndi.ser.\*) (\*1)
- JMS non-volatilization file (fjmsmng.ser.\*, fjmsdsubXXXX.ser, lock\XXXX) (\*1)
- Cluster environment definition file (fjmscluster.ser) (\*1)
- Console log (fjmsconsole.log)

\*1 For the locations where the files are stored, refer to "Backing Up and Restoring Resources", "Outline" in the "Maintenance (Resource Backup)" chapter of the Operator's Guide.



These files may be exposed to the threat of unauthorized access from an ill-intentioned person.

To protect these files from this threat, make these files inaccessible by end users. For this purpose, it is recommended to allow access only users having administrator authorization (superuser for a Solaris/Linux system, and Administrator for Windows(R) system).

Security measures must also be taken for Event Service. For information about Event Service, refer to "[2.9 Security Measures for Event Service](#)".

## 2.7 Security Measures for CORBA Service

---

This section explains the following topics:

- [Unauthorized Access to Resource Files](#)
- [Notes on Communication Data](#)
- [Notes on the Port Number used by CORBA Service](#)
- [Notes on Creation and Operation of Java Applets](#)

### Unauthorized Access to Resource Files

CORBA service has environment definition files as listed below:

- CORBA Service
  - CORBA Service environment definition information file (config) (\*1)
  - Host information definition file (inithost/initial\_hosts) (\*1)
  - Server default information file (boa.env) (\*1)
  - HTTP-IIOP gateway environment definition file (gwconfig) (\*2)
  - Implementation Repository file (impl.db)(\*1)
  - Initial Service file (init\_svc/initial\_services) (\*1)
  - Queue control information file (queue\_policy) (\*1) (\*3)
  - CORBA Service environment setup information file (odenvfile) (\*1)
- Naming Service
  - Naming Service registration information file (file under the CosNaming directory) (\*1)
  - Naming Service environment definition information file (nsconfig) (\*1)
- Load balance function (Provided only by the Interstage Application Server Enterprise Edition) (\*3)
  - Load balance function registration information file (file under the LBO directory) (\*1)
  - Load balance environment definition file (nslbo.conf) (\*1)
- Interface Repository
  - Interface Repository environment information file (irconfig, irpth) (\*1)
  - Interface Repository data file (irobf.qfl, irobf.qfp, irobftran) (\*1)

\*1 For the locations where the files and directories are stored, refer to "Backing Up and Restoring Resources", "Outline" in the "Maintenance (Resource Backup)" chapter of the Operator's Guide.

\*2 For the locations where the files are stored, refer to "gwconfig" in the "CORBA Service Environment Definition" appendix of the Tuning Guide.

\*3 This is not valid for Linux (64 bit).

These files may be exposed to the threat of unauthorized access from an ill-intentioned person.

To protect these files from this threat, make these files inaccessible by end users. For this purpose, it is recommended to allow access only by users having administrator authorization (superuser for a Solaris/Linux system, and Administrator for Windows(R) system).

### Notes on Communication Data

There is a possible threat that an ill-intentioned person furtively reads communication data between the server and a user who has proper access permission. Another threat is that the data is altered and transmitted as the right data.

It is recommended to use SSL encryption to encrypt data for retaining security.

For information about SSL encryption, refer to the "How to Use SSL with the CORBA Service" chapter.

### Notes on the Port Number used by CORBA Service

CORBA Service uses port number 8002.

When this product is used in a DMZ, suppress requests from outside the 8002 port should use a security measure such as a firewall.

### Notes on Creation and Operation of Java Applets

Be careful about the following points when creating and operating a Java applet that uses CORBA.

#### About Authorization Settings

If Java applets in operation are given more authorization than necessary, some malicious applets (including JavaScripts) may use it to cause some problems on client machines, such as damaged files, leakage of data in files, leakage of individual user's information, and so on.

When you use Java applets, set only the minimum authorization that is required. Do not set authorizations other than those described in the following manuals:

- The Distributed Application Development Guide (CORBA Service Edition) (provided with Interstage Application Server Enterprise Edition)
  - "Java Programming Guide" - "Execution of CORBA Applications" - "Client Setup (Pre-installed Java Clients)" - "Setting Permission for Java Libraries"
  - "Java Programming Guide" - "Execution of CORBA Applications" - "Client Setup (Portable-ORB)" - "Setting Permission for Java Libraries"
  - "Java Programming Guide" - "Digital Signatures in Applets" - "Digital Signature Procedures" - "policytool Command Setting (Supplements)"

#### About Errors and Exceptions

If information about an exception (stack trace) that occurs during operation of a Java applet is displayed on the screen (in a text field of the applet, on the Java console, etc.), internal information (internal structure) is leaked, which may be used by some malicious applets (including JavaScripts).

It is recommended not to display exception information (stack trace).

## 2.8 Security Measures for Portable-ORB

---

This section explains the following topics:

- [Unauthorized Access to Resource Files](#)
- [Notes on Communication Data](#)
- [Notes on Creation and Operation of Java Applet](#)

### Unauthorized Access to Resource Files

Portable-ORB service has environment definition files as listed below:

- Portable-ORB environment definition file (config) (\*1)
- Host information file (initial\_hosts) (\*1)

- Initial service file (initial\_services) (\*1)

\*1 For the locations where the files are stored, refer to "Backing Up and Restoring Resources", "Outline" in the "Maintenance (Resource Backup)" chapter of the Operator's Guide.

These files may be exposed to the threat of unauthorized access from an ill-intentioned person.

To protect these files from this threat, make these files inaccessible by end users. For this purpose, it is recommended to allow access only by users having administrator authorization (superuser for a Solaris/Linux system, and Administrator for Windows(R) system).

## Notes on Communication Data

There is a possible threat that an ill-intentioned person furtively reads communication data between the server and a user who has proper access permission. Another threat is that the data is altered and transmitted as the right data.

It is recommended to use SSL encryption to encrypt data for retaining security.

## Notes on Creation and Operation of Java Applet

Be careful about the following points when creating and operating a Java applet that uses Portable-ORB.

### About Authorization Settings

If Java applets in operation are given more authorization than necessary, some malicious applets (including JavaScript) may use it to cause problems on client machines, such as damaged files, leakage of data in files, leakage of individual user information, and so on.

When you use Java applets, set only the minimum authorization that is required. Do not set authorizations other than described in the following manuals:

- Distributed Application Development Guide (CORBA Service Edition) (provided with Interstage Application Server Enterprise Edition)
  - "Java Programming Guide" - "Execution of CORBA Applications" - "Client Setup (Pre-installed Java Clients)" - "Setting Permission for Java Libraries"
  - "Java Programming Guide" - "Execution of CORBA Applications" - "Client Setup (Portable-ORB)" - "Setting Permission for Java Libraries"
  - "Java Programming Guide" - "Digital Signatures in Applets" - "Digital Signature Procedures" - "policytool Command Setting (Supplements)"

### About Errors and Exceptions

If information about an exception (stack trace) that occurred during operation of a Java applet is displayed on the screen (in a text field of the applet, on the Java console, etc.), internal information (internal structure) is leaked, which may be used by some malicious applets (including JavaScript).

It is recommended not to display exception information (stack trace).

## 2.9 Security Measures for Event Service

---

This section explains the following topics:

- [Unauthorized Access to Resource Files](#)
- [Illegal Access to User Data Files](#)

### Unauthorized Access to Resource Files

Event service has environment definition files as listed below:

- Event Service configuration information (essystem.cfg) (\*1)
- Event channel operating environment (esgrpX.grp) (\*1)
- Event channel group management information (esmnggrp.db) (\*1)

- Unit definition file (file with the def extension) (\*1)
- Log file (ESLOG.log) (\*2)

\*1 For the locations where the files are stored, refer to "Backing Up and Restoring Resources", "Outline" in the "Maintenance (Resource Backup)" chapter of the Operator's Guide.

\*2 For the locations where the files are stored, refer to the "Messages Output by the Event Service" chapter of the Messages manual.

If a unit definition file is set during unit creation (when the 'esmunit' command is executed) for nonvolatile operation, the following directories are maintained:

- Directory to store the transaction file specified by "trandir."
- Directory to store the system (for unit control) file specified by "sysdir."
- Directory to store the event data file specified by "usedir."

These files and directories may be exposed to the threat of unauthorized access from an ill-intentioned person.

To protect these files and directories from this threat, make these files and directories inaccessible by end users. For this purpose, it is recommended to allow access only to users having administrator authorization (superuser for a Solaris/Linux system, and Administrator for Windows(R) system).

### Illegal Access to User Data Files

In the Event Service, files are created as user data files by executing the esgetchnlior command. Since EventChannel object references are stored in these files, there is a danger that an ill-intentioned person might attempt an illegal access. For this reason, take great care with how these files are handled.

## 2.10 Security Measures for IJServer Operation

---

IJServer is an operating environment for JEEE applications.

### Unauthorized Access to Resource Files

When IJServer is operated, the resource files for IJServer are stored in the ijserver directory under the J2EE common directory. These files may be subjected to unauthorized access by malicious persons or machines.

To protect these files from such threats, access to the files from general users can be inhibited. It is recommended to permit access only by users with administrator authority (administrator of the Windows(R) system).

### Notes on IJServer Execution

IJServer is an operating environment for J2EE applications and IJServer itself is executed as a process. Only users with administrator authority (administrators of the Windows(R) system) can execute IJServer. It is recommended to carefully select the users to whom administrator authority is assigned and periodically review this to improve safety.

## 2.11 Security Measures Concerning Operation of Interstage Directory Service

---

This is not valid for Standard-J Edition on Windows (64 bit).

This is not valid for Standard-J Edition on Linux (64 bit).

This section describes security measures relating to operation of the Interstage Directory Service.

### About Operation

Ensure the following to prevent incorrect operation:

- The Interstage Directory Service is operated by users who are well informed on the overall information system including the Interstage Directory Service, and who've received appropriate training.

- Interstage Directory Service is always correctly managed and operated according to the rules established in the manuals.

## Blocking External Access

Set up a firewall and routers appropriately, prevent the intrusion of unauthorized external packets and inhibit access to ports other than those specified.

## Restriction of Services

By restricting remotely accessible services (such as telnet and ftp) on nodes where Interstage is operating, you can prevent unauthorized accesses. This measure is effective against unauthorized accesses made through networks.

For details of how to restrict such remotely accessible services, refer to the manual for each platform.

## Notes on Accessing the Interstage Directory Service Server

When an LDAP client accesses the Interstage Directory Service server, there is a risk that an ill-intentioned person on the network may access the Interstage Directory Service server by impersonating a user having appropriate access permission. SSL encryption using SSL version 3 (client authentication) is recommended.

For SSL communication details, refer to the "Using SSL for Interstage Directory Service" chapter.

## 2.12 Measures for Multi Server Management Windows32/64 Solaris32 Linux32/64

---

This section explains the use of "roles" in Multi Server Management.

### Role Settings

When using Multi Server Management, it is important that the authority set for a user to log in to the Interstage Management Console is appropriate. This user authority is called a "role".

The executable operations vary according to the role authority. For further information and details about the role, refer to "Login Authentication for the Interstage Management Console" in the Operator's Guide.

## 2.13 Measures for Configuration Manager

---

This section explains the security measures for the Configuration Manager.

### Illegal Access to Resource Files

The Configuration Manager uses the following files.

- Business configuration management function repository (\*1)

\*1 This is the folder that is set in "Repository Environment Settings" of the Interstage Management Console [Configuration Management] tab.

It is possible that these files may be exposed to the threat of illegal access by a person (or machine) with malicious intent.

One measure to reduce this threat is to prevent access by general users. To achieve this, it is recommended that settings are made for these files so that only a user with administrator authority can access them (in Solaris/Linux systems, this is a super user, and in Windows(R) systems it is the Administrator).

# Part 2 Authentication and Access Control

---

Chapter 3 Authentication and Access Control for the Interstage HTTP Server.....	45
Chapter 4 Access Control for the Interstage Directory Service.....	90
Chapter 5 Security Audit Trail Functions.....	101

# Chapter 3 Authentication and Access Control for the Interstage HTTP Server

This chapter describes the authentication and access control that Interstage HTTP Server provides.

## 3.1 Types of Authentication

There are three types of authentication, as shown below.

- [3.1.1 User Authentication \(Basic Authentication\)](#)  
Authentication using a user name and password.
- [3.1.2 IP Access Control](#)  
Authentication using an IP address.
- [3.1.3 Client Authentication](#)  
Authentication using a client certificate (an SSL environment must have been set up).
- [3.1.4 Online Collation](#)  
User authentication using Directory Service.

Note

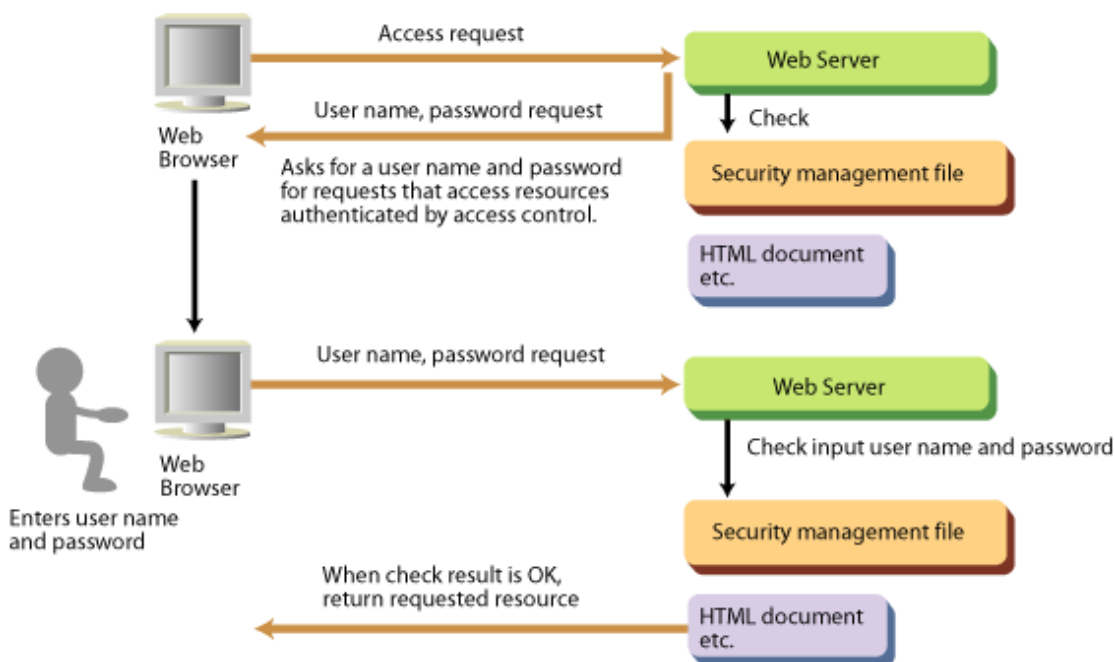
- User authentication and IP access control can be used independently or together.
- Online Collation cannot be used with User Authentication (Basic Authentication) using a password file.

### 3.1.1 User Authentication (Basic Authentication)

User authentication controls user names and passwords. User authentication has the function to limit access to the resource on the Web server for each user by controlling user names and passwords.

Web server determines whether or not to permit access to the resource from user names and passwords entered in the web browser.

The following figure shows the function of user authentication.



User Authentication

## Remarks

- In User Authentication, the user name and password sent over the network are not encrypted, and therefore might be easily deciphered. To avoid this, use SSL for communication between the client and server to encrypt the user name and password and achieve a secure communication.
- Web server User Authentication (Basic Authentication) information can be used in the Web application.

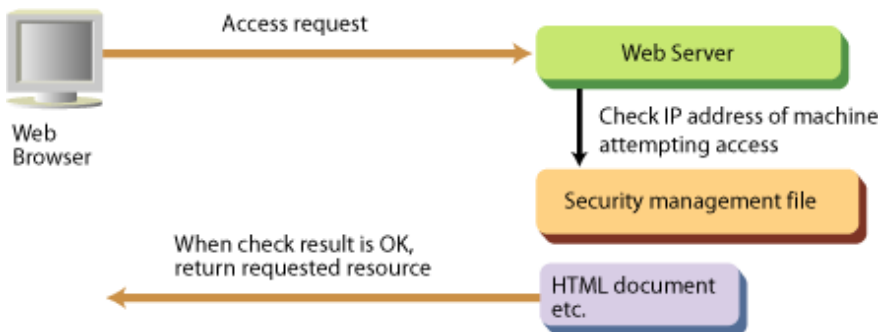
### 3.1.2 IP Access Control

---

IP access control limits accessing the resource on the Web server for each IP address of the equipment in the access source.

Web server determines whether or not to permit access to the resource from the IP address of the machine that is attempting access.

The following figure shows the function of IP access control.

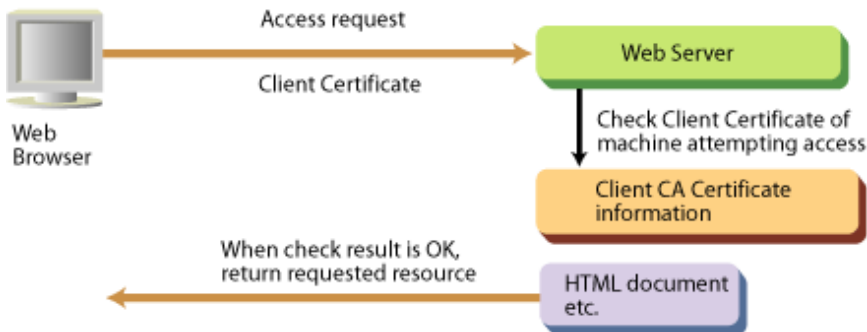


#### IP Access Control

### 3.1.3 Client Authentication

---

Client authentication restricts access to resources on the Web server to user possessing a client certificate. As a result, the identity of the client (Web browser) can be guaranteed. Figure 3-3 illustrates client authentication.



#### Client Authentication

#### Note

Use SSL protocol version SSL3.0 or SSL3.1 (TLS 1.0) for access restriction during client authentication.

### 3.1.4 Online Collation

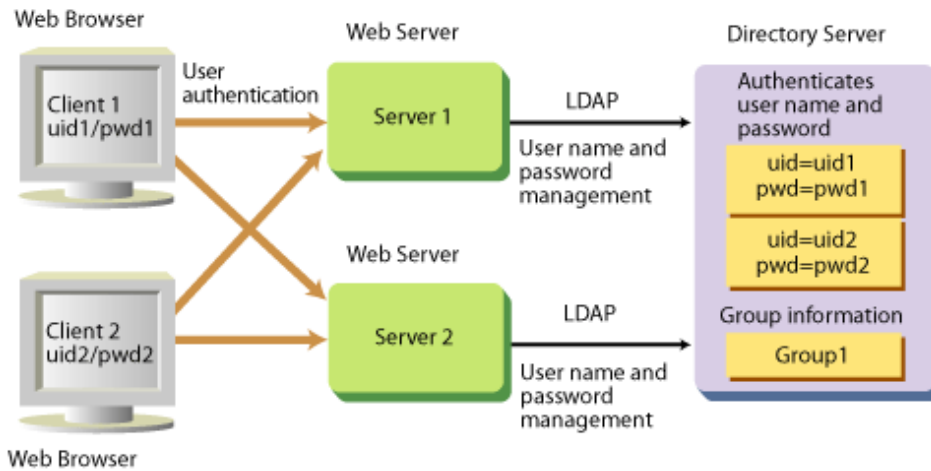
---

Online Collation is a user authentication feature that uses Directory Service. The user information (user name/password) used for authentication and group information are stored and managed on the directory server. When the user name and password are received from the Web browser (client), the Web server runs as a Directory Service client, communication is performed between the directory server and LDAP (Lightweight Directory Access Protocol), and the user information is collated online.



Using this feature, Directory Service user names and passwords are managed in batch, and common Web server user information can be used.

The following figure shows online collation.



### Online Collation

#### Note

Online Collation cannot be used with User Authentication (Basic Authentication) using a password file.

### Communication using SSL

SSL can be used for secure communication between the Web server and directory server. The SSL library and protocol version that are used are shown below.

Web server	SSL library	SSL protocol version
Interstage HTTP Server	SMEE3(SMEE 3.x or later)	2.0 or 3.0

#### Note

In SSL communication, only server authentication is supported.

## 3.2 Setting the User Authentication

User authentication is set according to the following procedures.

1. [Registering a User Password](#)
2. [Set the Environment Definition File](#)

#### Note

When the online collation function is in use user authentication cannot be used.

### Registering a User Password

Register a password for users to whom access permission is to be provided in the password file, by executing the htpasswd command after the command prompt.

Example [Windows32/64](#)

To create a new password file 'C:\Interstage\F3FMihs\servers\FJapache\conf\password.txt' and register a password for user 'user1':

```
C:\Interstage\bin\htpasswd -c C:\Interstage\F3FMihs\servers\FJapache\conf\password.txt user1
```

Example **Solaris32/64** **Linux32/64**

To create a new password file '/opt/FJSVihs/servers/FJapache/conf/password.txt' and register a password for user 'user1':

```
/opt/FJSVihs/bin/htpasswd -c /opt/FJSVihs/servers/FJapache/conf/password.txt user1
```

Notes

- To register subsequent users or to change a user password already registered, do not specify the htpasswd "-c" option.
- To delete a user, edit the password file by using a text editor.

The contents of the password file appear as follows when it is referenced using a text editor. To delete 'user2', delete the line containing 'user2' and save the file.

```
user1:$apr1$SR3.....$4aQAE2EU9NZTtbkxMEOa4/  
user2:$apr1$DS3.....$tEb4EYLhraAc1p2wIygTV/
```

- It is recommended that you change the access privileges for files created by this command:

**Windows32/64**

1. Start Windows Explorer.
2. Right-click the password file, then click [Properties].
3. In the [Properties] dialog box, click the [Security] tab.
4. Select "Deny" for [Full control] for all groups except SYSTEM and Administrators.

**Solaris32/64** **Linux32/64**

1. Login as superuser.
2. Change the file access privileges to "640".

```
chmod 640 <file>
```

3. Change the file owner to "root".

```
chown root <file>
```

4. Change the file group to "nobody" (the value set for the environment definition file (httpd.conf) Group directive).

```
chgrp nobody <file>
```

## Set the Environment Definition File

To allow the users whose password has been registered in the password file to access directories under a specified directory, use the following directives in the environment definition file (httpd.conf) of Interstage HTTP Server. By doing this, names and passwords of users who make access requests from Web browsers are checked and any access attempts from users whose names and passwords have not been registered in the password file are rejected.

Example **Windows32/64**

To allow the users whose names and passwords have been registered in the password file "C:\Interstage\F3FMihs\servers\FJapache\conf\password.txt" to access directories under a specified directory "C:\Interstage\F3FMihs\servers\FJapache\htdocs\users\name":

```
LoadModule auth_module "C:/Interstage/F3FMihs/modules/mod_auth.so"  
<Directory "C:/Interstage/F3FMihs/servers/FJapache/htdocs/users/name">  
  AuthUserFile "C:/Interstage/F3FMihs/servers/FJapache/conf/password.txt"  
  AuthName "Secret directory"  
  AuthType Basic  
  Require valid-user  
</Directory>
```

Example **Solaris32/64** **Linux32/64**

To allow the users whose names and passwords have been registered in the password file "/opt/FJSVihs/servers/FJapache/conf/password.txt" to access directories under a specified directory "/opt/FJSVihs/servers/FJapache/htdocs/users/name":

```
LoadModule auth_module "/opt/FJSVihs/modules/mod_auth.so"
<Directory "/opt/FJSVihs/servers/FJapache/htdocs/users/name">
  AuthUserFile "/opt/FJSVihs/servers/FJapache/conf/password.txt"
  AuthName "Secret directory"
  AuthType Basic
  Require valid-user
</Directory>
```

Note

When user authentication is set for the Servlet service application URL, the <Directory> section of the above example cannot be used. Use the <Location> section.

### 3.3 Setting the IP Access Control

For IP access control, you can allow only specified hosts to make access to directories under a specified directory using the following directives in the environment definition file (httpd.conf) of Interstage HTTP Server. By doing this, any access from Web browsers that are on unspecified hosts are rejected.

Example **Windows32/64**

To allow a specified host '192.168.1.1' to access directories under a specified directory "C:\Interstage\F3FMihs\servers\FJapache\htdocs\secret":

```
<Directory "C:/Interstage/F3FMihs/servers/FJapache/htdocs/secret">
  Order deny,allow
  Deny from all
  Allow from 192.168.1.1
</Directory>
```

Example **Solaris32/64** **Linux32/64**

To allow a specified host '192.168.1.1' to access directories under a specified directory "/opt/FJSVihs/servers/FJapache/htdocs/secret":

```
<Directory "/opt/FJSVihs/servers/FJapache/htdocs/secret">
  Order deny,allow
  Deny from all
  Allow from 192.168.1.1
</Directory>
```

Example **Windows32/64**

To allow a specified host '2001:db8::a00:20ff:fea7:ccea' to access directories under a specified directory "C:\Interstage\F3FMihs\servers\FJapache\htdocs\secret":

```
<Directory "C:/Interstage/F3FMihs/servers/FJapache/htdocs/secret">
  Order deny,allow
  Deny from all
  Allow from 2001:db8::a00:20ff:fea7:ccea
</Directory>
```

Example **Solaris32/64** **Linux32/64**

To allow a specified host '2001:db8::a00:20ff:fea7:ccea' to access directories under a specified directory "/opt/FJSVihs/servers/FJapache/htdocs/secret":

```
<Directory "/opt/FJSVihs/servers/FJapache/htdocs/secret">
  Order deny,allow
  Deny from all
```

```
    Allow from 2001:db8::a00:20ff:fea7:ccea
</Directory>
```

Example [Windows32/64](#)

To allow a specified domain 'allow-domain.com' to access directories under a specified directory "C:\Interstage\F3FMihs\servers\FJapache\htdocs\secret":

```
<Directory "C:/Interstage/F3FMihs/servers/FJapache/htdocs/secret">
    Order deny,allow
    Deny from all
    Allow from allow-domain.com
</Directory>
```

Example [Solaris32/64](#) [Linux32/64](#)

To allow a specified domain 'allow-domain.com' to access directories under a specified directory "/opt/FJSVihs/servers/FJapache/htdocs/secret":

```
<Directory "/opt/FJSVihs/servers/FJapache/htdocs/secret">
    Order deny,allow
    Deny from all
    Allow from allow-domain.com
</Directory>
```

Note

When IP access control is set for the Servlet service application URL, the <Directory> section of the above example cannot be used. Use the <Location> section.

## 3.4 Setting the Client Authentication

In Client Authentication (certificate authentication), an SSL environment is built and access control is performed using a client certificate sent from the client during SSL communication.

By setting authentication conditions for the client certificate attribute information in the Interstage HTTP Server environment definition file (httpd.conf), access control can also be performed using the client certificate condition settings.

The procedure for setting Client Authentication (certificate authentication) is shown below.

### Client Authentication (general certificate authentication)

1. Build the Interstage HTTP Server SSL environment.

For details, refer to the "[Chapter 11 How to Use SSL with Interstage HTTP Server](#)" chapter.

2. Set the environment definition file (httpd.conf).

Specify "with client authentication" in the file to use the certificate/key management environment SSL that was built using the SMEE command.

### Client Authentication (authentication using the certificate condition settings)

1. Build the Interstage HTTP Server SSL environment.

For details, refer to the "[Chapter 11 How to Use SSL with Interstage HTTP Server](#)" chapter.

To use certificate/key management environment SSL that was built using the SMEE command, specify "with client authentication" at the environment definition file (httpd.conf).

2. Set the environment definition file (httpd.conf).

For details on how to set the file (httpd.conf), refer below.

### 3.4.1 Set the Environment Definition File

In the Interstage HTTP Server environment definition file (httpd.conf), set the Client Authentication (authentication using the certificate condition settings) access control.

A sample of the file is displayed below:

```
SSLCertExpand on
SSLNotifyVers on

RewriteEngine On

RewriteCond %{ENV:EnvVarA} CondPatternA
RewriteCond %{ENV:EnvVarB} CondPatternB
RewriteRule .* - [L]

RewriteCond %{ENV:EnvVarC} CondPatternC
RewriteCond %{ENV:EnvVarD} CondPatternD
RewriteRule .* - [L]

RewriteRule .* - [F]
```

Note the following about the directives above:

- SSLCertExpand: Enables/disables the client certificate information environment variable settings. Specify "on" for this directive (if omitted, it will default to "on").
- SSLNotifyVers: Enables/disables the SSL-related environment variable settings. Specify "on" for this directive (if omitted, it will default to "on").
- RewriteEngine: Enables/disables the rewrite feature. Specify "On" for this directive.
- RewriteCond: Sets the authentication permissions conditions for the client certificate attribute information, and contains the condition pattern for the specified environment variable. It is possible to specify multiple RewriteCond directives before the RewriteRule directive (with the [L] flag) to set authentication permissions conditions that will be used together.

The environment variables that can be selected are listed below (note that they are used to control Web server behavior, not the operating system):

Environment variable	Client certificate item
SSL_CLIENT_CN	First and last name
SSL_CLIENT_C	Country
SSL_CLIENT_EMAIL	Mail address
SSL_CLIENT_O	Organization name
SSL_CLIENT_OU	Organizational unit name
SSL_CLIENT_T	Title
SSL_CLIENT_PHONE	Telephone number
SSL_CLIENT_ST	State/Prefecture
SSL_CLIENT_L	Street

For CondPattern, specify a regular expression that determines the environment variable value. To negate the pattern, prefix it with an exclamation mark (!). Strings containing spaces must be enclosed in double quotation marks ("").

- RewriteRule: If "[L]" is specified, this directive sets the access permissions according to the authentication permissions specified in RewriteCond. If "[F]" is specified, this directive sets the access denial to the client that sent the client certificate that did not match the authentication permissions conditions set above.

## Authentication Condition Settings for an Organization

### Example

Allowing access using a client certificate that matches one of the following conditions:

- Organization name is "organizationA", and organizational unit name is "organizationAunit1" or "organizationAunit2"
- Organization name is not "organizationB", or organizational unit name is neither "organizationBunit1" nor "organizationBunit2"
- Organization name is a string that starts with "organization" (no case sensitivity), and title is a string that contains "Manager"

#### Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMIhs/modules/mod_rewrite.so"

RewriteEngine On

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationA$
RewriteCond %{ENV:SSL_CLIENT_OU} ^organizationAunit1$|^organizationAunit2$
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationB$
RewriteCond %{ENV:SSL_CLIENT_OU} !(^organizationBunit1$|^organizationBunit2$)
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} "^organization.*" [NC]
RewriteCond %{ENV:SSL_CLIENT_T} .*Manager.*
RewriteRule .* - [L]

RewriteRule .* - [F]
```

#### Solaris32/64 Linux32/64

```
LoadModule rewrite_module "/opt/FJSVihs/modules/mod_rewrite.so"

RewriteEngine On

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationA$
RewriteCond %{ENV:SSL_CLIENT_OU} ^organizationAunit1$|^organizationAunit2$
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} ^organizationB$
RewriteCond %{ENV:SSL_CLIENT_OU} !(^organizationBunit1$|^organizationBunit2$)
RewriteRule .* - [L]

RewriteCond %{ENV:SSL_CLIENT_O} "^organization.*" [NC]
RewriteCond %{ENV:SSL_CLIENT_T} .*Manager.*
RewriteRule .* - [L]

RewriteRule .* - [F]
```

## Authentication Condition Settings for a Locale

### Example

Allowing access using a client certificate that matches one of the following conditions:

- Country "JP", Prefecture "Tokyo"/"Osaka"/"Kyoto"
- Country "US", State "California"/"New York"

#### Windows32/64

```
LoadModule rewrite_module "C:/Interstage/F3FMIhs/modules/mod_rewrite.so"

RewriteEngine On
```

```

RewriteCond %{ENV:SSL_CLIENT_C} ^JP$
RewriteCond %{ENV:SSL_CLIENT_ST} ^Tokyo$|^Osaka$|^Kyoto$
RewriteRule .* - [L,E=REMOTE_USER:JP-user]

RewriteCond %{ENV:SSL_CLIENT_C} ^US$
RewriteCond %{ENV:SSL_CLIENT_ST} "^California$|^New York$"
RewriteRule .* - [L,E=REMOTE_USER:US-user]

RewriteRule .* - [F]

```

**Solaris32/64 Linux32/64**

```

LoadModule rewrite_module "/opt/FJSVihs/modules/mod_rewrite.so"

RewriteEngine On

RewriteCond %{ENV:SSL_CLIENT_C} ^JP$
RewriteCond %{ENV:SSL_CLIENT_ST} ^Tokyo$|^Osaka$|^Kyoto$
RewriteRule .* - [L,E=REMOTE_USER:JP-user]

RewriteCond %{ENV:SSL_CLIENT_C} ^US$
RewriteCond %{ENV:SSL_CLIENT_ST} "^California$|^New York$"
RewriteRule .* - [L,E=REMOTE_USER:US-user]

RewriteRule .* - [F]

```

## Relating Directives

- LoadModule
- RewriteCond
- RewriteEngine
- RewriteRule
- SSLCertExpand
- SSLNotifyVers

## 3.5 Setting the Online Collation Function

Set the operation of the online collation function according to the following procedure.

In Interstage HTTP Server, the following directory servers are supported:

- Interstage Directory Service
 

Interstage Directory Service is the directory server provided in this product.
- Active Directory
 

Active Directory is the directory server provided by Microsoft(R).

### Notes

- To use the online collation function, the client API library (Interstage Directory Service SDK) is required in the same machine as the Interstage HTTP Server.

Online collation function operations can be performed:

- where SSL is not used between Interstage HTTP Server and Directory Server
- where SSL is used between Interstage HTTP Server and Directory Server

## Performing operations where SSL is not used between Interstage HTTP Server and Directory Server

1. Configure the Directory Server environment settings on the system in which Directory Server has been installed. Refer to "[3.5.1 Setting the Directory Server Environment](#)" for details of how to set the directory server environment.
2. Configure the environment definition file (httpd.conf) on the system in which Interstage HTTP Server has been installed. Refer to "[3.5.3 Set the Environment Definition File](#)" for details of how to set the Interstage HTTP Server environment definition file (httpd.conf).

## Performing operations where SSL is used between Interstage HTTP Server and Directory Server

1. Configure the Directory Server environment settings on the system in which Directory Server has been installed. Refer to "[3.5.1 Setting the Directory Server Environment](#)" for details of how to set the directory server environment.
2. Configure the SSL communication client environment on the system in which Interstage HTTP Server has been installed. Refer to "[3.5.2 Setting the SSL Environment](#)" for details of how to set the SSL environment.
3. Configure the environment definition file (httpd.conf) on the system in which Interstage HTTP Server has been installed. Refer to "[3.5.3 Set the Environment Definition File](#)" for details of how to set the Interstage HTTP Server environment definition file (httpd.conf).

The following sections provide procedures for operating the online collation function.

### 3.5.1 Setting the Directory Server Environment

---

To use the online collation function, the environment of the directory server must be set up.

#### Using Interstage Directory Service

##### (1) Preparing the Directory Server

Create the repository server to correspond with the environment setup of the directory server (Interstage Directory Service). If SSL is used for secure communication between the Interstage HTTP Server and the directory server, the SSL environment must also be configured in the Interstage Directory Service server environment.

For details on the directory server, refer to the Directory Service Operator's Guide.

##### (2) Creating Entries

On the directory server, use the Entry Management Tool to create the user information and group information entries.

##### Creating User Entry

Create the user entry with the following inetOrgPerson object class.

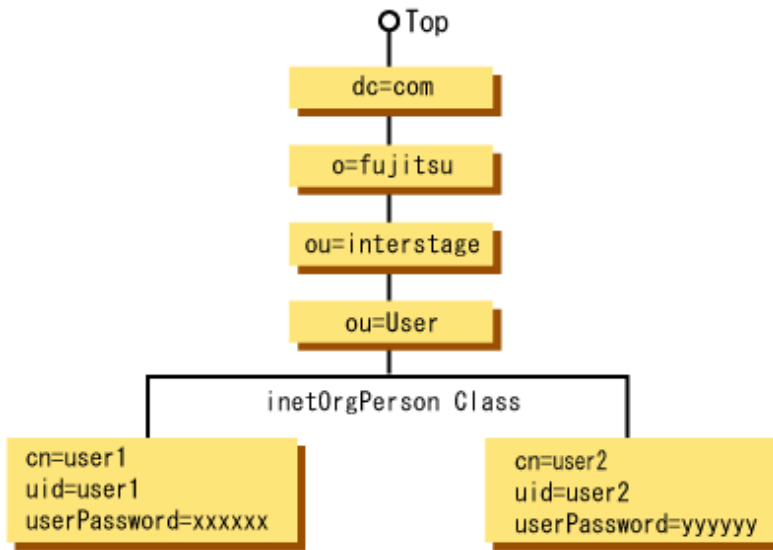
For the user entry, the following items must be set.

Table 3.1 User Entry Settings

Item	Description
cn attribute	Sets a user entry name.
uid attribute	Sets a user name for online collation.
userPassword attribute	Sets a password associated with the user name.



Example of User Entry Configuration



**Creating User Entry**

Creating Group Entry

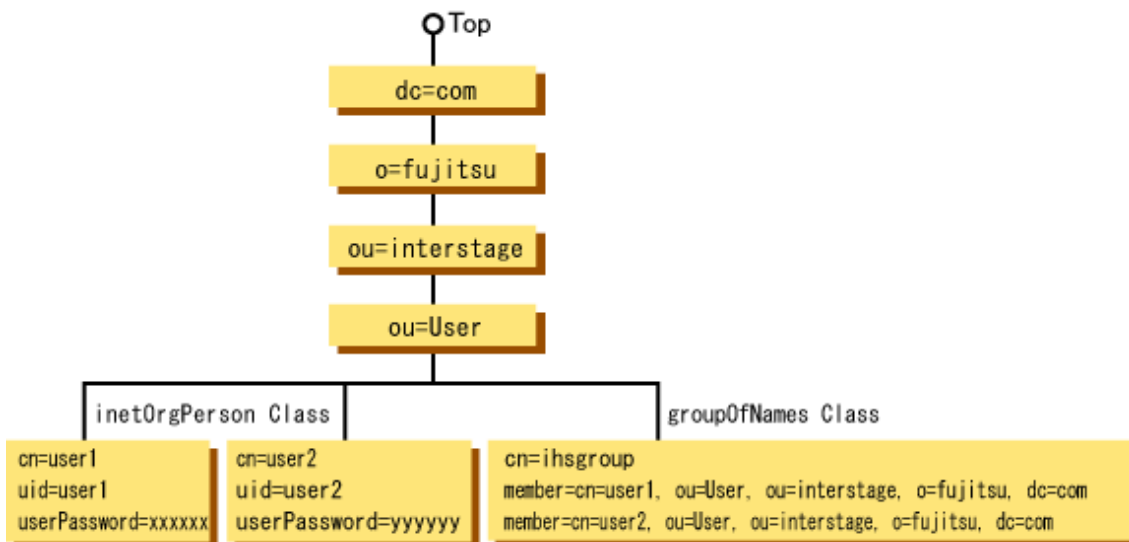
Create the group entry with the following groupOfNames object class.

For the group entry, the following items must be set.

Table 3.2 Group Entry Settings

Item	Description
cn attribute	Sets a name of a group to which the user performing online collation belongs.
member attribute	Sets a DN name of the user belonging to a group.

Example of Group Entry



**Group Entry Configuration**

**Using Active Directory**

Before configuring the Directory Server (Active Directory) environment settings, refer to the Windows(R) system manual.

To perform encrypted communication where SSL is used between Interstage HTTP Server and Directory Server, also configure the following SSL communication environment settings.

1. Create the Certificate Signing Request (CSR) that will make the request to the Certificate Authority (CA) to issue the certificate.
2. Make the request to the CA to issue the certificate.
3. In the SSL communication environment, register the CA certificate that was obtained from the CA, the site certificate, and the CRL.

## 3.5.2 Setting the SSL Environment

---

Using the online collation function, operations that use SSL can be configured between Interstage HTTP Server and Directory Server. To perform encrypted communication where SSL is used, configure the SSL client environment on the system in which Interstage HTTP Server has been installed.

The environments shown below can be used as SSL client environments. Configure one of the following SSL environments, depending on the operation.

- Interstage Certificate Environments
- Certificate/Key Management Environments Configured with the SMEE Commands

### Using Interstage Certificate Environment

Notes

**Windows32/64**

- Execute the SSL configuration command as a user that belongs to the Administrators group.

**Solaris32/64 Linux32/64**

- Execute the SSL configuration command as the superuser.
- Set the JDK or JRE installation path in the JAVA\_HOME environment variable, then execute the command.

#### (1) Create the owner group **Solaris32/64 Linux32/64**

Create an Interstage certificate environment owner group. Refer to "Setting up Access Permissions in the Interstage Certificate Environment" in the "Setting and Use of the Interstage Certificate Environment" chapter, for details of how to create the owner group.

#### (2) Create the Interstage Certificate Environment

Create the Interstage Certificate Environment type that is required for CA certificate and CRL management.

An example of the command execution is shown below.

Example **Windows32/64**

```
scsmakeenv -e
```

Example **Solaris32/64 Linux32/64**

Creating the Interstage Certificate Environment type to which access by users registered in the "iscertg" owner group that was created in step 1 above, is allowed.

```
scsmakeenv -e -g iscertg
```

#### (3) Obtain the CA certificate

Obtain the CA certificate from the CA that issued the site certificate registered in Directory Server. Follow the individual CA guidelines regarding how the CA certificate should be obtained.

#### (4) Obtain the CRL

Obtain the CRL from the CA that issued the site certificate registered in Directory Server. Follow the individual CA guidelines regarding how the CRL should be obtained.

## (5) Register the CA certificate

In Interstage Certificate Environment, register the CA certificate that was obtained in step 3 above. Register the CA certificate after the root CA certificate.

An example of the command execution is shown below.

Example **Windows32/64**

When the following certificates are registered:

- CA certificate : "C:\sslenv\CA.der"
- CA certificate nickname : "CA"

```
scsenter -n CA -f C:\sslenv\CA.der
```

Example **Solaris32/64** **Linux32/64**

When the following certificates are registered:

- CA certificate : "/sslenv/CA.der"
- CA certificate nickname : "CA"

```
scsenter -n CA -f /sslenv/CA.der
```

## (6) Register the CRL

In the Interstage certificate environment, register the CRL that was obtained in step 4 above.

An example of the command execution is shown below.

Example **Windows32/64**

Registering "C:\sslenv\CRL.der" as the CRL file

```
scsenter -c -f C:\sslenv\CRL.der
```

Example **Solaris32/64** **Linux32/64**

Registering "/sslenv/CRL.der" as the CRL file

```
scsenter -c -f /sslenv/CRL.der
```

## Using Certificate/Key Management Environments Configured with the SMEE Commands

Notes **Solaris32/64** **Linux32/64**

The required commands can only be executed by a non-superuser.

When configuring the environment definition file (httpd.conf), as in "[Setting 3: Operation Using SSL \(using a certificate/key Management Environment Configured with the SMEE Commands\)](#)" or "[Setting 6: Operation Using SSL \(using a certificate/key Management Environment Configured with the SMEE Commands\)](#)", specify this user as the User directive and the owner group that this user has been registered in as the Group directive.

### (1) Create the management directory

Create the directory that is required for CA certificate and CRL management.

An example of the command execution is shown below.

Example **Windows32/64**

```
mkdir C:\sslenv\slot
mkdir C:\sslenv\sslcert
mkdir C:\sslenv\sslcert\cert
mkdir C:\sslenv\sslcert\crl
```

Example [Solaris32/64](#) [Linux32/64](#)

```
mkdir /sslenv/slot
mkdir /sslenv/sslcert
mkdir /sslenv/sslcert/cert
mkdir /sslenv/sslcert/crl
```

## (2) Create/configure the private key management environment

Create the private key management environment that is required for private key management, then configure the environment settings.

An example of the command execution is shown below.

Example [Windows32/64](#)

```
makeslot -d C:\sslenv\slot
maketoken -d C:\sslenv\slot -s 1 -t token01
```

Example [Solaris32/64](#) [Linux32/64](#)

```
makeslot -d /sslenv/slot
maketoken -d /sslenv/slot -s 1 -t token01
```

## (3) Create the certificate/CRL management environment

Create the certificate/CRL management environment that is required for CA certificate and CRL management, then configure the environment settings.

An example of the command execution is shown below.

Example [Windows32/64](#)

```
cmmkenv C:\sslenv\sslcert -todir C:\sslenv\sslcert\cert,C:\sslenv\sslcert\crl
cmsetenv C:\sslenv\sslcert -sd C:\sslenv\slot -jc 1
```

Example [Solaris32/64](#) [Linux32/64](#)

```
cmmkenv /sslenv/sslcert -todir /sslenv/sslcert/cert,/sslenv/sslcert/crl
cmsetenv /sslenv/sslcert -sd /sslenv/slot -jc 1
```

## (4) Obtain the CA certificate

Obtain the CA certificate from the CA that issued the site certificate registered in Directory Server. Follow the individual CA guidelines regarding how the CA certificate should be obtained.

## (5) Obtain the CRL

Obtain the CRL from the CA that issued the site certificate registered in Directory Server. Follow the individual CA guidelines regarding how the CRL should be obtained.

## (6) Register the CA certificate

In Interstage Certificate Environment, register the CA certificate that was obtained in step 4 above. Register the CA certificate after the root CA certificate.

An example of the command execution is shown below.

Example [Windows32/64](#)

Registering "CA.der" as the CA certificate

```
cmntcert C:\sslenv\CA.der -ed C:\sslenv\sslcert -ca -nn CA
```

Example [Solaris32/64](#) [Linux32/64](#)

Registering "CA.der" as the CA certificate

```
cmntcert /sslenv/CA.der -ed /sslenv/sslcert -ca -nn CA
```

### (7) Register the CRL

In the certificate/CRL management environment, register the CRL that was obtained in step 5 above.

An example of the command execution is shown below.

Example **Windows32/64**

Registering "C:\sslenv\CRL.der" as the CRL file

```
cmentcrl C:\sslenv\CRL.der -ed C:\sslenv\sslcert
```

Example **Solaris32/64** **Linux32/64**

Registering "/sslenv/CRL.der" as the CRL file

```
cmentcrl /sslenv/CRL.der -ed /sslenv/sslcert
```

## 3.5.3 Set the Environment Definition File

Define the online collation function according to the mode of operation in the environment definition file (httpd.conf) for the Interstage HTTP Server.

The method for setting the environment definition file for Interstage HTTP Server (httpd.conf) varies depending on whether operation is set with SSL disabled or enabled between Interstage HTTP Server and the directory server. Set the file using the table below as a reference.

Table 3.3 Environment Definition File Settings

Directory Server	SSL environment used by Interstage HTTP Server	Refer to Setting Example
Interstage Directory Service	Operation without using SSL	Setting 1
	Operation using the SSL of the Interstage certificate environment (*1)	Setting 2
	Operation using the SSL of the certificate/key management environment configured with the SMEE command	Setting 3
Active Directory	Operation without using SSL	Setting 4
	Operation using the SSL of the Interstage certificate environment	Setting 5
	Operation using the SSL of the certificate/key management environment configured with the SMEE command	Setting 6

\*1 This also applies when SSL environments configured on the directory server are used.

### Note

- When the online collation function is set for the Servlet service application URL, the <Directory> section of the following example cannot be used. Use the <Location> section.
- Specify the same SSL protocol version as that on the directory server.

**Solaris32/64** **Linux32/64**

- When setting the LoadModule directive, ldap\_module must be set first, followed by auth\_ldap\_module.

An example of definition in the Interstage HTTP Server environment definition file (httpd.conf) for each case is shown below.

### Using Interstage Directory Service

Setting 1: Operation without Using SSL

Example **Windows32/64**

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '389'
- BindDN name used to access the directory server 'cn=manager,ou=interstage,o=fujitsu,dc=com'

- Name of the tree containing user information on the directory server 'ou=User,ou=interstage,o=fujitsu,dc=com'

```
LoadModule ldap_module "C:/Interstage/F3FMIhs/modules/util_ldap.so"
LoadModule auth_ldap_module "C:/Interstage/F3FMIhs/modules/mod_auth_ldap.so"

<Directory "C:/Interstage/F3FMIhs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN      cn=manager,ou=interstage,o=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled      on
  AuthName             "title"
  AuthType             Basic
  AuthLDAPHost         hostname
  AuthLDAPPort         389
  AuthLDAPbasedn       ou=User,ou=interstage,o=fujitsu,dc=com
  Require              valid-user
  AuthLDAPSecure       off
</Directory>
```

Example **Solaris32/64** **Linux32/64**

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '389'
- BindDN name used to access the directory server 'cn=manager,ou=interstage,o=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'ou=User,ou=interstage,o=fujitsu,dc=com'

```
LoadModule ldap_module "/opt/FJSVihs/modules/mod_ldap.so"
LoadModule auth_ldap_module "/opt/FJSVihs/modules/mod_auth_ldap.so"

<Directory "/opt/FJSVihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN      cn=manager,ou=interstage,o=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled      on
  AuthName             "title"
  AuthType             Basic
  AuthLDAPHost         hostname
  AuthLDAPPort         389
  AuthLDAPbasedn       ou=User,ou=interstage,o=fujitsu,dc=com
  Require              valid-user
  AuthLDAPSecure       off
</Directory>
```

Setting 2: Operation Using SSL (using the Interstage Certificate Environment or using SSL Configured on the Directory Server)

Example **Windows32/64**

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=manager,ou=interstage,o=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'ou=User,ou=interstage,o=fujitsu,dc=com'
- SSL protocol version 'SSL3.0'

```
LoadModule ldap_module "C:/Interstage/F3FMIhs/modules/util_ldap.so"
LoadModule auth_ldap_module "C:/Interstage/F3FMIhs/modules/mod_auth_ldap.so"

<Directory "C:/Interstage/F3FMIhs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN      cn=manager,ou=interstage,o=fujitsu,dc=com
  AuthLDAPBindPassword password
```

```

AuthLDAPEnabled      on
AuthName             "title"
AuthType             Basic
AuthLDAPHost         hostname
AuthLDAPPort         636
AuthLDAPbasedn       ou=User,ou=interstage,o=fujitsu,dc=com
Require              valid-user
AuthLDAPSecure       on
AuthLDAPSecureVersion 3
</Directory>

```

**Example** Solaris32/64 Linux32/64

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=manager,ou=interstage,o=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'ou=User,ou=interstage,o=fujitsu,dc=com'
- User who registered to owner groups of Interstage certificate environment 'nobody'
- Group to which the above user belongs: 'nobody'
- SSL protocol version 'SSL3.0'

```

LoadModule ldap_module "/opt/FJSVihs/modules/mod_ldap.so"
LoadModule auth_ldap_module "/opt/FJSVihs/modules/mod_auth_ldap.so"

User nobody
Group nobody

<Directory "/opt/FJSVihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN      cn=manager,ou=interstage,o=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled     on
  AuthName            "title"
  AuthType            Basic
  AuthLDAPHost        hostname
  AuthLDAPPort        636
  AuthLDAPbasedn      ou=User,ou=interstage,o=fujitsu,dc=com
  Require              valid-user
  AuthLDAPSecure      on
  AuthLDAPSecureVersion 3
</Directory>

```

**Setting 3: Operation Using SSL (using a certificate/key Management Environment Configured with the SMEE Commands)**

**Example** Windows32/64

Running the online collation function using the SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=manager,ou=interstage,o=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'ou=User,ou=interstage,o=fujitsu,dc=com'
- SSL protocol version 'SSL3.0'
- Slot information directory 'D:\sslenv\slot'
- Operation control directory 'D:\sslenv\sslcert'

- Token label 'token01'
- User PIN 'userpin'

```
LoadModule ldap_module "C:/Interstage/F3FMihs/modules/util_ldap.so"
LoadModule auth_ldap_module "C:/Interstage/F3FMihs/modules/mod_auth_ldap.so"

<Directory "C:/Interstage/F3FMihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN      cn=manager,ou=interstage,o=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled      on
  AuthName             "title"
  AuthType             Basic
  AuthLDAPHost         hostname
  AuthLDAPPort         636
  AuthLDAPbasedn       ou=User,ou=interstage,o=fujitsu,dc=com
  Require              valid-user
  AuthLDAPSecure       on
  AuthLDAPSecureVersion 3
  AuthLDAPSlotPath     "D:\sslenv\slot"
  AuthLDAPCertPath     "D:\sslenv\sslcert"
  AuthLDAPTknlbl       token01
  AuthLDAPTknpwd       userpin
</Directory>
```

**Example** Solaris32/64 Linux32/64

Running the online collation function using the SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=manager,ou=interstage,o=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'ou=User,ou=interstage,o=fujitsu,dc=com'
- SSL protocol version 'SSL3.0'
- Slot information directory '/home/slot'
- Operation control directory '/home/sslcert'
- Token label 'token01'
- User PIN 'userpin'
- User set up certificate and key management environment 'user1'
- Group to which the above user belongs: 'group1'

```
LoadModule ldap_module "/opt/FJSVihs/modules/mod_ldap.so"
LoadModule auth_ldap_module "/opt/FJSVihs/modules/mod_auth_ldap.so"

User user1
Group group1

<Directory "/opt/FJSVihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN      cn=manager,ou=interstage,o=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled      on
  AuthName             "title"
  AuthType             Basic
  AuthLDAPHost         hostname
  AuthLDAPPort         636
  AuthLDAPbasedn       ou=User,ou=interstage,o=fujitsu,dc=com
  Require              valid-user
  AuthLDAPSecure       on
```



```

AuthLDAPSecureVersion 3
AuthLDAPSlotPath      "/home/slot"
AuthLDAPCertPath      "/home/sslcert"
AuthLDAPTknLbl        token01
AuthLDAPTknPwd        userpin
</Directory>

```

## Using Active Directory

### Setting 4: Operation without Using SSL

#### Example Windows32/64

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '389'
- BindDN name used to access the directory server 'cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'cn=Users,dc=interstage,dc=fujitsu,dc=com'
- The directory server attribute name 'sAMAccountName' used as the user ID at the time of the authentication

```

LoadModule ldap_module "C:/Interstage/F3FMIhs/modules/util_ldap.so"
LoadModule auth_ldap_module "C:/Interstage/F3FMIhs/modules/mod_auth_ldap.so"

<Directory "C:/Interstage/F3FMIhs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled on
  AuthName "title"
  AuthType Basic
  AuthLDAPHost hostname
  AuthLDAPPort 389
  AuthLDAPbasedn cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPAttribute sAMAccountName
  Require valid-user
  AuthLDAPSecure off
</Directory>

```

#### Example Solaris32/64 Linux32/64

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '389'
- BindDN name used to access the directory server 'cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'cn=Users,dc=interstage,dc=fujitsu,dc=com'
- The directory server attribute name 'sAMAccountName' used as the user ID at the time of the authentication

```

LoadModule ldap_module "/opt/FJSVihs/modules/mod_ldap.so"
LoadModule auth_ldap_module "/opt/FJSVihs/modules/mod_auth_ldap.so"

<Directory "/opt/FJSVihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled on
  AuthName "title"
  AuthType Basic
  AuthLDAPHost hostname
  AuthLDAPPort 389
  AuthLDAPbasedn cn=Users,dc=interstage,dc=fujitsu,dc=com

```

```

AuthLDAPAttribute      sAMAccountName
Require                valid-user
AuthLDAPSecure        off
</Directory>

```

#### Setting 5: Operation Using SSL (using the Interstage Certificate Environment or using SSL Configured on the Directory Server)

##### Example Windows32/64

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'cn=Users,dc=interstage,dc=fujitsu,dc=com'
- The directory server attribute name 'sAMAccountName' used as the user ID at the time of the authentication
- SSL protocol version 'SSL3.0'

```

LoadModule ldap_module "C:/Interstage/F3FMIhs/modules/util_ldap.so"
LoadModule auth_ldap_module "C:/Interstage/F3FMIhs/modules/mod_auth_ldap.so"

<Directory "C:/Interstage/F3FMIhs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled on
  AuthName "title"
  AuthType Basic
  AuthLDAPHost hostname
  AuthLDAPPort 636
  AuthLDAPbasedn cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPAttribute sAMAccountName
  Require valid-user
  AuthLDAPSecure on
  AuthLDAPSecureVersion 3
</Directory>

```

##### Example Solaris32/64 Linux32/64

Running the online collation function without using SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'cn=Users,dc=interstage,dc=fujitsu,dc=com'
- The directory server attribute name 'sAMAccountName' used as the user ID at the time of the authentication
- SSL protocol version 'SSL3.0'
- User who registered to owner groups of Interstage certificate environment 'nobody'
- Group to which the above user belongs: 'nobody'

```

LoadModule ldap_module "/opt/FJSVihs/modules/mod_ldap.so"
LoadModule auth_ldap_module "/opt/FJSVihs/modules/mod_auth_ldap.so"

User nobody
Group nobody

<Directory "/opt/FJSVihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPBindPassword password

```

```

AuthLDAPEnabled      on
AuthName             "title"
AuthType             Basic
AuthLDAPHost         hostname
AuthLDAPPort         636
AuthLDAPbasedn       cn=Users,dc=interstage,dc=fujitsu,dc=com
AuthLDAPAttribute    sAMAccountName
Require              valid-user
AuthLDAPSecure       on
AuthLDAPSecureVersion 3
</Directory>

```

## Setting 6: Operation Using SSL (using a certificate/key Management Environment Configured with the SMEE Commands)

### Example [Windows32/64](#)

Running the online collation function using the SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com'
- Name of the tree containing user information on the directory server 'cn=Users,dc=interstage,dc=fujitsu,dc=com'
- The directory server attribute name 'sAMAccountName' used as the user ID at the time of the authentication
- SSL protocol version 'SSL3.0'
- Slot information directory 'D:\sslenv\slot'
- Operation control directory 'D:\sslenv\sslcert'
- Token label 'token01'
- User PIN 'userpin'

```

LoadModule ldap_module "C:/Interstage/F3FMihs/modules/util_ldap.so"
LoadModule auth_ldap_module "C:/Interstage/F3FMihs/modules/mod_auth_ldap.so"

<Directory "C:/Interstage/F3FMihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled      on
  AuthName             "title"
  AuthType             Basic
  AuthLDAPHost         hostname
  AuthLDAPPort         636
  AuthLDAPbasedn       cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPAttribute    sAMAccountName
  Require              valid-user
  AuthLDAPSecure       on
  AuthLDAPSecureVersion 3
  AuthLDAPSlotPath     "D:\sslenv\slot"
  AuthLDAPCertPath     "D:\sslenv\sslcert"
  AuthLDAPTknlbl       token01
  AuthLDAPTknpwd       userpin
</Directory>

```

### Example [Solaris32/64](#) [Linux32/64](#)

Running the online collation function using the SSL, under the following settings:

- Directory server 'hostname'
- Port number '636'
- BindDN name used to access the directory server 'cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com'

- Name of the tree containing user information on the directory server 'cn=Users,dc=interstage,dc=fujitsu,dc=com'
- The directory server attribute name 'sAMAccountName' used as the user ID at the time of the authentication
- SSL protocol version 'SSL3.0'
- Slot information directory '/sslenv/slot'
- Operation control directory '/sslenv/sslcert'
- Token label 'token01'
- User PIN 'userpin'
- User set up certificate and key management environment 'user1'
- Group to which the above user belongs: 'group1'

```

LoadModule ldap_module "/opt/FJSVihs/modules/mod_ldap.so"
LoadModule auth_ldap_module "/opt/FJSVihs/modules/mod_auth_ldap.so"

User user1
Group group1

<Directory "/opt/FJSVihs/servers/FJapache/htdocs/securityzone">
  AuthLDAPBindDN cn=administrator,cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPBindPassword password
  AuthLDAPEnabled on
  AuthName "title"
  AuthType Basic
  AuthLDAPHost hostname
  AuthLDAPPort 636
  AuthLDAPbasedn cn=Users,dc=interstage,dc=fujitsu,dc=com
  AuthLDAPAttribute sAMAccountName
  Require valid-user
  AuthLDAPSecure on
  AuthLDAPSecureVersion 3
  AuthLDAPSlotPath "/sslenv/slot"
  AuthLDAPCertPath "/sslenv/sslcert"
  AuthLDAPTknLbl token01
  AuthLDAPTknPwd userpin
</Directory>

```

## Relating Directives

- AuthLDAPAttribute
- AuthLDAPbasedn
- AuthLDAPBindDN
- AuthLDAPBindPassword
- AuthLDAPCertPath
- AuthLDAPEnabled
- AuthLDAPHost
- AuthLDAPPort
- AuthLDAPSecure
- AuthLDAPSecureVersion
- AuthLDAPSlotPath
- AuthLDAPTknLbl
- AuthLDAPTknPwd

- AuthName
- AuthType
- <Directory>
- Group
- LoadModule
- Require
- User

## 3.6 Relating Directives

---

The following directives are related to settings of the environment definition file to use the online collation function.

The description includes the following:

### Name

Directive name

### Synopsis

Directive format

### Description

Functional overview of the directive

### Context

Directive-set location indicated with one of the following keywords:

Global context

Setting used for action of the entire Web server

Virtual host

Setting which is available in the <VirtualHost> section and used for action of the virtual host

Directory

Setting which is available in the <Directory>, <Location>, and <Files> sections and used for action in response to a request for a specified directory, URL, or file

### Default Value

Value assumed when the directive is omitted. If a directive indicated with 'None' is omitted, the directive function is disabled.

### Initial value

Initial directive value

### Module

Name of the module that implements the directive function. A directive with no module name indication is included in the basic module.

### Note

Notes on the use of the directive

### Examples

Directive example (included only for a directive which requires complicated setting).

## 3.6.1 Allow

---

### Name

Allow

### Synopsis

Allow from host|network[/mask]env=environment-variable [host|network[/mask]env=environment-variable] ...

### Description

Specifies a host or network that is granted access to the directories.

Specifying 'all' for the host entry allows all hosts to access the directories.

Specifying the IP address of a host allows only that host to access the directories. The IPv6 address can also be specified in the IP address.

If the domain name is specified in the host, access is only allowed from the host that belongs to the specified domain.

Access is allowed when 'env=env-variable' is specified and the specified environment variable exists.

### Context

Directory

### Default Value

None

### Initial value

```
Allow from all
```

### Module

mod\_access

## 3.6.2 AuthLDAPAttribute

---

### Name

AuthLDAPAttribute

### Synopsis

AuthLDAPAttribute attribute name

### Description

Set the directory server attribute name to be used as the user name in the online collation function.

Attribute name

Use ASCII characters (1-byte characters: 0 to 9, A to Z, and a to z). Up to 256 bytes are allowed.

### Context

Directory

### Default Value

```
AuthLDAPAttribute uid
```

## Module

Windows32/64

mod\_auth\_ldap

util\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

## 3.6.3 AuthLDAPbasedn

---

### Name

AuthLDAPbasedn

### Synopsis

AuthLDAPbasedn BaseDN-name

### Description

Specifies the name of the tree that is storing information about users in the directory server using the DN name.

When information about the users is stored in multiple directories, specify the name of a high-order DN which is inclusive of all the user information storing directories. The directory specified in BaseDN is handled as the top directory from which a search is made for information about the users. The character string specified in BaseDN is transferred to the directory server as it is; specify it using the code used on the directory server.

BaseDN-name

Use ASCII characters (1-byte characters: 0 to 9, A to Z, and a to z). Up to 256 bytes are allowed.

### Context

Directory

### Default Value

None

## Module

Windows32/64

mod\_auth\_ldap

util\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

## 3.6.4 AuthLDAPBindDN

---

### Name

AuthLDAPBindDN

## Synopsis

AuthLDAPBindDN BindDN-name

## Description

Specifies the BindDN name used for access to the directory server. When making anonymous access, omit this directive.

BindDN-name

Use ASCII characters (1-byte characters: 0 to 9, A to Z, and a to z). Up to 256 bytes are allowed.

## Context

Directory

## Default Value

```
AuthLDAPBindDN anonymous
```

## Module

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

## 3.6.5 AuthLDAPBindPassword

---

### Name

AuthLDAPBindPassword

### Synopsis

AuthLDAPBindPassword BindPassword

### Description

When some BindDN name has been specified by the AuthLDAPBindDN directive, specify the password for the BindDN name. When making anonymous access, omit this directive.

BindPassword

Use ASCII characters (1-byte characters: 0 to 9, A to Z, and a to z). Up to 128 bytes are allowed.

### Context

Directory

### Default Value

None

### Module

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64



mod\_auth\_ldap

mod\_ldap

### 3.6.6 AuthLDAPCertPath

---

#### Name

AuthLDAPCertPath

#### Synopsis

AuthLDAPCertPath operation-control-directory-name

#### Description

Uses the absolute path to specify the operation control directory specified when the certificate/CRL control environment was created.

#### Context

Directory

#### Default Value

None

#### Module

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

### 3.6.7 AuthLDAPEnabled

---

#### Name

AuthLDAPEnabled

#### Synopsis

AuthLDAPEnabled on|off

#### Description

Specifies whether to apply LDAP authentication.

on

Applies LDAP authentication.

off

Does not apply LDAP authentication.

#### Context

Directory

## Default Value

```
AuthLDAPEnabled on
```

## Module

```
Windows32/64
```

```
mod_auth_ldap
```

```
Solaris32/64 Linux32/64
```

```
mod_auth_ldap
```

```
mod_ldap
```

## 3.6.8 AuthLDAPHost

---

### Name

```
AuthLDAPHost
```

### Synopsis

```
AuthLDAPHost Host-name
```

### Description

Specifies the host name including the domain name of a directory server or the IP address. The IPv6 address can also be specified in the IP address.

### Context

```
Directory
```

### Default Value

```
AuthLDAPHost localhost
```

## Module

```
Windows32/64
```

```
mod_auth_ldap
```

```
Solaris32/64 Linux32/64
```

```
mod_auth_ldap
```

```
mod_ldap
```

## Examples

Specifying "hostname" for the directory server host name

```
AuthLDAPHost hostname
```

Specifying "192.168.1.1" for the directory server IP address

```
AuthLDAPHost 192.168.1.1
```

Specifying "2001:db8::a00:20ff:fea7:ccea" for the directory server IPv6 address

```
AuthLDAPHost 2001:db8::a00:20ff:fea7:ccea
```

## 3.6.9 AuthLDAPPort

---

### Name

AuthLDAPPort

### Synopsis

AuthLDAPPort Port-number

### Description

Specifies the port number of the directory server.

### Context

Directory

### Default Value

For not using SSL:

```
AuthLDAPPort 389
```

For using SSL:

```
AuthLDAPPort 636
```

### Module

**Windows32/64**

mod\_auth\_ldap

**Solaris32/64 Linux32/64**

mod\_auth\_ldap

mod\_ldap

## 3.6.10 AuthLDAPSecure

---

### Name

AuthLDAPSecure

### Synopsis

AuthLDAPSecure on|off

### Description

Specifies whether to use SSL for the operation of the online collation function.

on

SSL is used.

off

SSL is not used.

### Context

Directory

## Default Value

```
AuthLDAPSecure off
```

## Module

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

## 3.6.11 AuthLDAPSecureVersion

---

### Name

AuthLDAPSecure

### Synopsis

AuthLDAPSecureVersion 2|3

### Description

Specify the SSL protocol version when SSL is used between the Interstage HTTP Server and the directory server.

If there is more than one SSL section in the environment definition file for the same directory server, specify the same version for all sections.

Set to one of the following values:

- 2  
Specify 2, when using 'SSL2.0' of the SSL protocol version
- 3  
Specify 3, when using 'SSL3.0' of the SSL protocol version.

### Context

Directory

### Default Value

```
AuthLDAPSecureVersion 3
```

## Module

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

## 3.6.12 AuthLDAPSlotPath

---

**Name**

AuthLDAPSlotPath

**Synopsis**

AuthLDAPSlotPath slot-information-directory-name

**Description**

Uses the absolute path to specify the slot information directory specified when the private-key control environment was created.

**Context**

Directory

**Default Value**

None

**Module**

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

### 3.6.13 AuthLDAPTknLbl

---

**Name**

AuthLDAPTknLbl

**Synopsis**

AuthLDAPTknLbl token-label

**Description**

Specifies the token label specified when the private-key was created.

**Context**

Directory

**Default Value**

None

**Module**

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

## 3.6.14 AuthLDAPTknPwd

---

### Name

AuthLDAPTknPwd

### Synopsis

AuthLDAPTknPwd user-PIN

### Description

Specifies the user PIN specified when the private-key was created.

### Context

Directory

### Default Value

None

### Module

Windows32/64

mod\_auth\_ldap

Solaris32/64 Linux32/64

mod\_auth\_ldap

mod\_ldap

## 3.6.15 AuthName

---

### Name

AuthName

### Synopsis

AuthName 'title'

### Description

Specifies the title displayed on the authentication screen in the ASCII alphanumeric characters (1 byte characters).

### Context

Directory

### Default value

None

## 3.6.16 AuthType

---

### Name

AuthType

## Synopsis

AuthType Basic|Digest

## Description

Specifies the type of authentication.

Basic

Sets basic authentication (the passwords are plain text).

Digest

Specifies digest authentication (the passwords are hash values).

## Context

Directory

## Default Value

None

## 3.6.17 AuthUserFile

---

### Name

AuthUserFile

### Synopsis

AuthUserFile file-name

### Description

Specifies the name of the password file used for user authentication.

### Context

Directory

### Default Value

None

### Module

mod\_auth

## 3.6.18 Deny

---

### Name

Deny

### Synopsis

Deny from host|network[/mask][env=environment-variable] [host|network[/mask][env=environment-variable] ...

### Description

Specifies a host or network that is denied access to the directories.

Specifying 'all' to the host entry denies access to all hosts.

Specifying the IP address of a host denies access to the directories for that host only. The IPv6 address can also be specified in the IP address.

If the domain name is specified in the host, access is only denied from the host that belongs to the specified domain.

Access is denied when 'env=env-variable' is specified and the specified environment variable exists.

### Context

Directory

### Default Value

None

### Module

mod\_access

## 3.6.19 <Directory>

---

### Name

<Directory>

### Synopsis

<Directory directory-path> ... </Directory>

### Description

Specifies the directory section only when a directive is used within the specific directory and sub-directories of that directory.

The directory name can be specified using a relative path, relative path from the directory specified in the DocumentRoot directive, wild card (? indicates a specific character, \* indicates a character string), and regular expressions.

Within the specified directory, all the directives allowed in the directory context can be used.

### Context

Global context, Virtual host

### Default Value

None

### Note

This section cannot be used for Servlet service applications. Use the <Location> section.

## 3.6.20 DirectoryIndex

---

### Name

DirectoryIndex

### Synopsis

DirectoryIndex file-name [file-name ...]

### Description

Sets the search target resource file name when the client specifies a forward slash (/) at the end of the URL and requests the directory index.



## Context

Global context, Virtual host, Directory

## Default Value

```
DirectoryIndex index.html
```

## Initial value

```
DirectoryIndex index.html index.html.var
```

## Module

mod\_dir

## Note

This directive setting will be disabled for access to the Servlet service application.

## 3.6.21 Group

---

### Name

Group

### Synopsis

**Solaris32/64** **Linux32/64**

Group groupID

### Description

Specifies the name of the group to use when a server process is executed.

For the group ID, the group name can be specified, or the group ID (numeric value) can be specified following a number sign (#).

### Context

Global context

### Default Value

```
Group nobody
```

### Initial Value

```
Group nobody
```

## 3.6.22 LoadModule

---

### Name

LoadModule

### Synopsis

LoadModule module ID file-name

## Description

Reads a plug-in module.

Specifies the name of the module structure defined in the plug-in module source file for the module ID. Specify the absolute path of the plug-in module file name.

## Context

Global context

## Default Value

None

## 3.6.23 <Location>

---

### Name

<Location>

### Synopsis

<Location *URL*>...</Location>

### Description

To use a directive only within the specific URL, only the URL section needs to be specified.

Specify the URL name in "/path" without including a scheme. Wildcards (? indicates a character, \* indicates a string), and regular expressions can be specified (to specify a regular expression, prefix the value with a tilde (~) followed by a space).

In the specified URL, all the directives allowed in the directory context can be used.

### Context

Global context, Virtual host

### Default Value

None

### Note

The forward slash (/) will not match any wildcards, so this must be specified explicitly.

## 3.6.24 Order

---

### Name

Order

### Synopsis

Order order

### Description

Specifies the order in which the Allow directive and the Deny directive are applied. Note that the Allow and Deny directives must be separated by a comma (,) with no space between them.

The directives are evaluated in the order below (set the conditions for access from the client):

- Deny,Allow

1. Allow access from hosts except those set in the Deny directive.
2. Allow access from hosts set in the Allow directive - this will overwrite the Deny directive setting.

If the Allow or Deny directives were not set (for example: <Directory> section or <Location> section), all access to the specified section will be allowed.

- Allow,Deny

1. Deny access from hosts except those set in the Allow directive.
2. Deny access from hosts set in the Deny directive - this will overwrite the Allow directive setting.

If the Allow or Deny directives were not set (for example: <Directory> section or <Location> section), all access to the specified section will be denied.

## Context

Directory

## Default Value

Order Deny,Allow
------------------

## Module

mod\_access

## 3.6.25 Redirect

---

### Name

Redirect

### Synopsis

Redirect [status] URL redirect-path

### Description

Sets the URL redirect destination - the full URL must be specified.

The valid status values are described below:

- permanent  
permanent redirect status (301) will be returned - specify this when the resource was moved permanently.
- temp  
temporary redirect status (302) will be returned - this is the default when the status is omitted.
- seeother  
"See Other" status (303) will be returned - specify this when the resource was moved temporarily.
- gone  
"Gone" status (410) will be returned - specify this when the resource was moved permanently and redirect-path is omitted.

### Context

Global context, Virtual host, Directory

## Default Value

None

## Module

mod\_alias

## Note

- This directive cannot be used for Servlet service applications - use <Location> instead.
- Do not specify just a forward slash (/) for the URL. If a forward slash (/) is specified for the URL and an identical Web server path is specified for the redirect-path, there will be a match with all requests, and an infinite number of redirections might occur.

## 3.6.26 Require

---

### Name

Require

### Synopsis

Require valid-user|user user-name|group group-name

### Description

Specifies the rule to be applied for user authentication.

**valid-user**

Authenticates all valid users.

When the online collation function is used, users registered with the directory server are allowed.

**user user-name**

Authenticates users specified by *user-name*.

When the online collation function is used, the uid attribute of the user is specified as the *user-name*.

Use a space as a delimiter between user and *user-name*.

**group group-name**

Authenticates groups specified by *group-name*.

When the online collation function is used, the DN of the group entry is specified as the *group-name*.

Use a space as a delimiter between group and *group-name*.

### Context

Directory

### Default Value

None

## 3.6.27 RewriteCond

---

### Name

RewriteCond

### Synopsis

RewriteCond TestString CondPattern [flag]

## Description

Sets the condition that will rewrite the URL. This directive can be set multiple times before the RewriteRule directive. If the test string value has satisfied the condition specified for CondPattern, the RewriteRule directive setting that follows will apply.

### - TestString

Specify the test string using the following variables:

#### - \$N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in the RewriteRule directive, URLPattern immediately before.

#### - %N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in the RewriteCond directive, CondPattern that satisfied the condition finally.

#### - %{server variable name}

Specify the server variable.

#### - %{ENV:environment variable name}

Specify the environment variable.

#### - %{HTTP:header name}

Specify a HTTP request header.

### - CondPattern

Specify a regular expression for the condition that will determine the test string value. To negate the pattern, prefix it with an exclamation mark (!).

### - flag (OPTIONAL)

Specify the flag that will control the condition decision. Separate multiple flags with a comma (,).

The valid values are described below:

#### - nocase (or, NC)

Specifies that case sensitivity is not be used.

#### - ornext (or, OR)

Specify this when multiple cases of this directive are specified for the OR condition. If this flag is not specified, then the AND condition will be used.

## Context

Global context, Virtual host, Directory

## Default Value

None

## Module

mod\_rewrite

## Note

- This directive will be enabled when the RewriteEngine directive is "On".
- Set this directive for each virtual host separately.

## 3.6.28 RewriteEngine

---

### Name

RewriteEngine

### Synopsis

RewriteEngine On|Off

### Description

Enables/disables the rewrite feature, which enables flexible rewriting of the URL (note that the URL rewrite conditions and rules are set in the RewriteCond and RewriteRule directives).

The valid values are described below:

- On
- Off

### Context

Global context, Virtual host, Directory

### Default Value

```
RewriteEngine Off
```

### Module

mod\_rewrite

### Note

Set this directive for each virtual host separately.

## 3.6.29 RewriteRule

---

### Name

RewriteRule

### Synopsis

RewriteRule URLPattern Substitution [flag]

### Description

Sets the rule for rewriting the URL.

By combining this with a rewrite-related directive such as the RewriteCond directive, flexible rewriting of the URL is possible.

- URLPattern

Specify the rewrite target URL, using a regular expression.

If a URL-encoded URL is specified, the rewrite target URL is the decoded URL.

- Substitution

Specify the URL that will be rewritten if the URL pattern is matched:

- \$N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in URLPattern.

- %N

Specify a number between 1 and 9 for N. This will be replaced by the string that corresponds to the regular expression grouping "parenthesis()" specified in the RewriteCond directive, CondPattern that satisfied the condition finally.

- %{server variable name}

Specify the server variable.

- %{ENV:environment variable name}

Specify the environment variable.

- %{HTTP:header name}

Specify an optional HTTP request header.

- -

The URL is not rewritten.

- flag (OPTIONAL)

Specify the flag enclosed in square brackets ([]). Separate multiple flags with a comma (,).

The valid values are described below:

- redirect[=status] (or, R[=status])

Executes external redirect in the URL that was rewritten.

The valid status types are described below (if [=status] is omitted, it will be redirected using status code "302" (Moved Temporarily)):

- permanent (or, 301)

Redirected using status code "301" (Moved Permanently).

- temp (or, 302)

Redirected using status code "302" (Moved Temporarily).

- seeother (or, 303)

Redirected using status code "303" (See Other).

- forbidden (or, F)

Returns status code "403" (Forbidden). Specify this as the condition that was set for the RewriteCond directive to forbid access to the Web server.

- gone (or, G)

Returns status code "410" (Gone). Specify this to notify the client of the fact that a page that does not exist was accessed.

- proxy (or, P)

If the rule is matched, the URL that was rewritten is assumed to be a proxy request and is used as a reverse proxy.

If this flag is specified, mod\_proxy, mod\_proxy\_connect and mod\_proxy\_http module must be set for the LoadModule directive.

- last (or, L)

If the rule is matched, URL rewrite processing is completed. Rules that follow will not be applied.

- next (or, N)

Restarts a series of rewrite processing rules starting from the first rule. A URL that has already been rewritten will be a target. To specify this flag, specify the completion condition appropriately so that rewrite processing will not be executed infinitely.

- chain (or, C)

If the rule is matched, the rules that follow will be applied. If the rule is not matched, none of the rules that follow will be applied.

- type=MIME type (or, T=MIME type)

If the rule is matched, the specified MIME type will be set for the Content-TypeURL header.

#### Note

The MIME type specified is invalid if a Servlet service application is accessed and a MIME type has been set for that application.

- nosubreq (or, NS)

The rule will not be applied for subrequests that occur in the Web server.

This is used when subrequests will occur for the file that was specified in the [DirectoryIndex](#) directive when the client (Web browser) specified a URL with a forward slash (/) at the end. However, the rule will not be applied for these subrequests.

- nocase (or, NC)

The rule will be applied without upper/lower case-sensitivity.

- qsappend (or, QSA)

If there is a query string (the string after the question mark (?) in the URL) in the URL before it is rewritten and Substitution, this appends an ampersand (&) and the query string that was specified in the URL before it was rewritten to the end of Substitution. If this flag is not specified, the query string will be overwritten by Substitution.

- noescape (or, NE)

URL escape at the time of the rewrite will be suppressed.

Normally, special characters such as the percentage sign (%) and semicolon (;) are escaped to a hexadecimal expression "%25" or "%3b". If this flag was specified, however, they will not be escaped.

- passthrough (or, PT)

Control will be passed to another module after the URL is rewritten.

Specify this when the [Alias](#) directive, [ScriptAlias](#) directive, and [Redirect](#) directive are used for the URL that was rewritten.

- skip=numeric (or, S=numeric)

If the rule is matched, application of the rules that follow will be skipped for the number of rules that was specified in the numeric.

- env=environment variable:value (or, E=environment variable:value)

If the rule is matched, the value for the environment variable that was specified will be set. \$N and %N can also be specified in the same way as Substitution for the value. For details on how to specify \$N and %N, refer to "Substitution" above.

## Context

Global context, Virtual host, Directory

## Default Value

None

## Module

mod\_rewrite

## Note

- This directive will be enabled when the setting is for the rewrite feature to be used (when "On" has been set for the RewriteEngine directive).
- To use this directive with a virtual host, set the directive for each virtual host separately. When this directive is set in the virtual host, the URL will be redirected internally if the host name of the URL that is to be rewritten and the address string that was specified in the <VirtualHost> section match. To redirect the URL externally, specify "redirect[=status] (or, R[=status])" in the flag setting.
- To specify a Servlet service application URL for Substitution, set external redirect or a reverse proxy. For details on how to set external redirect or the reverse proxy, refer to the examples below.



## Examples

The URLs that are rewritten according to each rule that was set in this directive when a request is received from the client (Web browser) are shown in the table below.

Settings content	Request from the client	URL after replacement (Note)
RewriteRule ^/somepath(.*) /otherpath\$1	GET /somepath/pathinfo	/otherpath/pathinfo (internal redirect)
RewriteRule ^/somepath(.*) /otherpath\$1 [R]	GET /somepath/pathinfo	http://thishost/otherpath/pathinfo (external redirect)
RewriteRule ^/somepath(.*) http://thishost/otherpath\$1	GET /somepath/pathinfo	/otherpath/pathinfo (internal redirect)
RewriteRule ^/somepath(.*) http://thishost/otherpath\$1 [R]	GET /somepath/pathinfo	http://thishost/otherpath/pathinfo (external redirect)
RewriteRule ^/somepath(.*) http://otherhost/otherpath\$1	GET /somepath/pathinfo	http://otherhost/otherpath/pathinfo (external redirect)
RewriteRule ^/somepath(.*) http://originhost/otherpath\$1 [P]	GET /somepath/pathinfo	http://originhost/otherpath/pathinfo (reverse proxy)
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1 [PT]	GET /test.cgi?abc	/cgi-bin/test.cgi?abc
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1 [PT,QSA]	GET /test.cgi?abc	/cgi-bin/test.cgi?abc
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1?xyz [PT]	GET /test.cgi?abc	/cgi-bin/test.cgi?xyz
RewriteRule ^/(.+\.cgi)\$ /cgi-bin/\$1?xyz [PT,QSA]	GET /test.cgi?abc	/cgi-bin/test.cgi?xyz&abc

Note: The meaning of each host name is as follows:

- thishost: The Web server in which the rules have been set
- otherhost: Other Web server
- originhost: Content generation host Web server when a proxy is used

## 3.6.30 SSLCertExpand

---

### Name

SSLCertExpand

### Synopsis

SSLCertExpand on|off

### Description

Specifies whether Client Authentication information will be set as an environment variable.

on

Client Authentication information is set as an environment variable.

off

Client Authentication information is not set as an environment variable.

## Context

Global context, Virtual host

## Default Value

For the main host:

```
SSLCertExpand on
```

For a virtual host:

```
SSLCertExpand <value set for this directive on the main host>
```

## Module

mod\_ihs\_ssl

## 3.6.31 SSLNotifyVers

---

### Name

SSLNotifyVers

### Synopsis

SSLNotifyVers on|off

### Description

Specifies whether an SSL-related environment variable will be set.

on

SSL-related information is set as an environment variable.

off

SSL-related information is not set as an environment variable. However, only the HTTPS environment variable will be set.

## Context

Global context, Virtual host

## Default Value

For the main host:

```
SSLNotifyVers on
```

For a virtual host:

```
SSLNotifyVers <value set for this directive on the main host>
```

## Module

mod\_ihs\_ssl

## 3.6.32 User

---

### Name

User

## Synopsis

**Solaris32/64** **Linux32/64**

User userID

## Description

Specifies the name of the user who executes the server process.

For the user ID, the user name can be specified, or the user ID (numeric value) can be specified following a number sign (#).

## Context

Global context

## Default Value

User nobody

## Initial Value

User nobody

# Chapter 4 Access Control for the Interstage Directory Service

This chapter describes the access control provided by the Interstage Directory Service.

## 4.1 Designing Access Control

Designing access control involves deciding *which access users* will be allowed to access *which access targets* with *what kind of access* when clients access the repository server.

For example, settings can be implemented to enable a certain employee ("A") to write (modify) her own telephone number; other employees to read her telephone number; and non-authenticated users (anonymous users) no access to her telephone number.

Access control should be designed at the same time as data to be registered in the repository (directory information trees) is designed.

The repository server evaluates access according to a combination of the following information:

- Entries or attributes that are subject to access control
- Users who are given access permission (or who are denied access)
- The access permission given to users

### Access Targets

Entries, subtrees or attributes can be specified as access targets. Design access control so that access to particular entries or subtrees, or particular attributes (such as passwords) is controlled.

In the example above, employee A's telephone number is the access target.

### Access Users

Either anonymous users or users (bind DNs) that are specified when a client accesses (binds to) the repository server can be specified as access users.

Access users can be classified into the following five types:

- Specific users
- Users that are registered in the repository as entries

In the example above, employee A is this kind of user when she accesses her own telephone number.

- Authenticated users
- Unauthenticated users (anonymous users)
- All users

The Administrator (administrator DN) is not subject to access control. The Administrator has full access permissions (authenticate, compare, search, read and write) to all entry information.

### Access Level

Six access levels can be specified, as follows:

- none

All access is denied to users with this access level.

- auth

Users with this access level are allowed to authenticate (bind to) the repository.

- compare

Users with this access level are allowed to perform comparison operations on an access target. Unlike users with the "search" access level, these users are only allowed to access the target to determine whether the comparison conditions are met ("true" or "false").

- search

Users with this access level are allowed to perform search operations on an access target. Users with "search" access permission will be notified if search conditions are met but will not be allowed to read entry information or attribute values.

- read

Users with "read" access permission are allowed to perform read operations on an access target. Users with "read" access permission are allowed to read information and attribute values for entries that meet the conditions specified in search operations.

- write

Users with "write" access permission are allowed to perform write operations on an access target. Specify this access level to allow users to add, delete or modify entries (by adding, deleting or modifying attributes) or change the name of entries.

## 4.2 Defining Access Control Lists

---

Access control settings are created by entering definition statements in an "access control list definition file" that defines access control.

Access control list definition files are edited using text editors. The Interstage Directory Service provides a sample access control list definition file so that new access control list definitions can be entered. Edit this file using a text editor.

The sample file can be found at the following location.

Windows32/64

```
C:\Interstage\IREP\sample\acl\acl.txt
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/sample/acl/acl.txt
```

### 4.2.1 File Format

---

The format of the access control list definition file is shown below. The access control list definition file is made up of "access" directives and associated arguments.

```
# Access control definition
#
# rootdn can always write!

access to attr=telephoneNumber
        by self write
        by users read

access to attr=userPassword
        by self write
        by users compare
        by * auth

access to *
        by self write
        by * read
```

Note:

- Comment lines

Lines that start with a "#" (hash) are ignored as comment lines.

- Blank lines

Blank lines separate access directives, but are ignored.

- "access" directives

"access" directive arguments are separated by spaces. To include a space in an argument, enclose the argument in double quotes (""). To include a double quote (") or a backslash (\) in an argument, place a backslash (\) in front of the character.

Lines that start with blanks are treated as continuations of the preceding line.

The first line must not start with a space. Make the first line a comment line or a definition statement.

- Multi-byte characters

To include multi-byte characters in comment lines or "access" directives, use UTF-8 for character encoding.

- Alphabetic characters are not case-sensitive.

- Specify a maximum of 1,024 bytes for the comment line and the "access" directive line, whether or not the lines are continuous.

## 4.2.2 Editing the Access Control List Definition File

---

Specify access targets, access users and access levels in the access control list definition file using "access" directives.

### Specification Format for "access" Directives

#### Syntax

```
access to <what>  
    by <who> <accesslevel>
```

Multiple "by" clauses can be specified.

#### Settings

Give access permission (specified by <accesslevel>) to at least one access user (specified by <who>) for one set of access targets of entries and attributes (specified by <what>).

Specify one "access" directive for each set of access targets. To define access control for multiple access targets, specify multiple "access" directives.

To define access control so that multiple users can access one set of access targets, specify multiple "by" clauses in a single "access" directive.

#### <what>

Specify the entries or attributes that are the access target.

#### <who>

Specify the access users who will be given permission to access the access target.

#### <accesslevel>

Specify the access level for these users.

#### Notes

Note the following points when defining access control list definition files. Refer to ["4.2.3 Evaluation of Access Control List Definitions"](#) for more information about how access control list definition files are evaluated.

- If the entries or attributes that are specified when a client accesses the repository do not match the access target (<what>) of any "access" directives, access to these entries and attributes will be denied.
- If the bind DN that is specified when a client accesses the repository does not match the access users (<who>) of any "access" directives, access to the repository server (and access to entries and attributes) will be denied.
- If multiple "access" directives have been specified in the access control list definition file, they will be evaluated in order from the beginning of the file, starting with the first "access" directive. Be very careful about the specification order of "access" directives, otherwise the resulting access definitions may not be as they were intended.

- All users accessing from clients are regarded as unauthenticated (anonymous) users until an authentication operation has been performed.

For the userPassword attribute, be sure to give unauthenticated (anonymous) users authentication ("auth") or bind permission. Refer to the notes in "Specifying Access Levels <accesslevel>" for more information.

## Specifying Access Targets <what>

For access targets (<what>), specify the entries or attributes that will be subject to access control. It is also possible to specify "all entries" or a combination of entries and attributes.

Note that the <what> access target can be omitted. In this case, the access target will be "all entries".

### Syntax

#### Specifying all entries

- \* (asterisk)

The access target will be "all entries" (including their attributes).

#### Specifying an entry

- dn.<scope>=<DN string>

For the DN string, specify the distinguished name identifier (DN) for the entry.

For the scope, specify one of the following:

- base:

The access target will be the entry that matches the specified DN string.

- one:

The access target will be all entries one level below the entry that matches the specified DN string.

The entry that matches the specified DN string will not be part of the access target.

- subtree:

The access target will be the entry that matches the specified DN string, all entries under that entry, and all entries in subtrees.

- children:

The access target will be all entries under the entry that matches the specified DN string and all entries in subtrees.

The entry that matches the specified DN string will not be part of the access target.

Suppose, for example, that the following entries have been registered in the repository.

- 1) ou=interstage,o=fujitsu,dc=com
- 2) ou=User,ou=interstage,o=fujitsu,dc=com
- 3) cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
- 4) ou=Other,ou=User,ou=interstage,o=fujitsu,dc=com
- 5) cn=OUser901,ou=Other,ou=User,ou=interstage,o=fujitsu,dc=com

In this case, if 'dn.base="ou=User,ou=interstage,o=fujitsu,dc=com"' has been specified, the access target will be 2).

If 'dn.one="ou=User,ou=interstage,o=fujitsu,dc=com"' has been specified, the access targets will be 3) and 4).

If 'dn.subtree="ou=User,ou=interstage,o=fujitsu,dc=com"' has been specified, the access targets will be 2), 3), 4) and 5).

If 'dn.children="ou=User,ou=interstage,o=fujitsu,dc=com"' has been specified, the access targets will be 3), 4) and 5).

- dn=<DN string>

The access target will be all entries that either include or match the specified DN string.

#### Specifying Attributes

- attr=<attribute list>

Attributes that match the specified attribute list will be used as the access target.

For attribute lists, specify either a single attribute name or multiple attribute names separated by commas (,).

### Specifying a Combination of Entries and Attributes

- dn=<DN string> attr=<attribute list>

Entries that match the specified DN string and attributes that match the specified attribute list will be used as the access target.

Separate entries (dn=<DN string>) and attributes (attr=<attribute list>) by a space.

### Note

- Do not insert spaces before or after the equals sign (=) that is used when specifying entries and attributes.
- Specify a maximum of 1,024 bytes for the access target <what>.
- If the entries or attributes that are specified when a client accesses the repository do not match the access target (<what>) of any "access" directives, access to these entries and attributes will be denied.

Use dn.<scope> and "\*" (asterisk) to control access for all users to entries and attributes in the repository.

### Settings Example

Creating definitions so that all users can read all entries

```
access to *
    by * read
```

Creating definitions so that all users can read the entry that matches the DN string "ou=UserX,o=fujitsu,dc=com", all entries under that entry, and all entries in subtrees.

```
access to dn.subtree="ou=UserX,o=fujitsu,dc=com"
    by * read
```

Creating definitions so that all users can read the entry that matches the DN string "cn=public,o=fujitsu,dc=com"

```
access to dn="cn=public,o=fujitsu,dc=com"
    by * read
```

Creating definitions so that users who have been registered as entries can write (modify) the values of their own "userPassword" and "homePhone" attributes

```
access to attr=userPassword,homePhone
    by self write
```

Creating definitions so that all users can read the value of the "mail" attribute for the entry that matches the DN string "cn=public,o=fujitsu,dc=com"

```
access to dn="cn=public,o=fujitsu,dc=com" attr=mail
    by * read
```

### Specifying Access Users <who>

For access users (<who>), specify the users (the bind DN specified when the client accesses the repository) who will be given access permission (specified by <accesslevel>). It is also possible to specify "all users".

Access users (<who>) can be specified using the six entry formats shown below. It is also possible to specify multiple "by" clauses in a single "access" directive, specifying different access levels (to the same access target) for each access user.

Note that the access user specification (<who>) cannot be omitted.

### Syntax

- \* (asterisk)

The specified access level will be applied to all users (all bind DNs).



- dn.<scope>=<DN string>

The specified access level will be applied to users whose bind DN matches the DN for the target range of entries specified by the scope.

The format for the scope is the same as for the dn.<scope> specification in "Specifying Access Targets <what>".

- dn=<DN string>

The specified access level will be applied to users whose bind DN matches the DN for entries that include or match the specified DN string.

- self

The specified access level will be applied to users whose bind DN matches the DN for a user that has been registered as an entry.

- users

The specified access level will be applied to authenticated (bound) users.

- anonymous

The specified access level will be applied to users that have not been authenticated (anonymous users) or users that have not been bound.

#### Note

- Specify a maximum of 1,024 bytes for the access users <who>.

- If the bind DN that is specified when a client accesses the repository does not match the access users (<who>) of any "access" directives, access to the repository server (and to entries and attributes) will be denied.

Use dn.<scope> and "\*" (asterisk) to control access for all users to entries and attributes in the repository.

#### Settings Example

Creating definitions so that all users can search all entries

```
access to *
  by * search
```

Creating definitions so that (1) users that have been registered as entries can read the value of their own "userPassword" attribute, (2) authenticated users can search the value of the "userPassword" attribute, and (3) all other users can authenticate (bind)

```
access to attr=userPassword
  by self read
  by users search
  by * auth
```

Creating definitions so that users whose bind DN matches the DN for the entry that matches the DN string "ou=UserX,o=fujitsu,dc=com", all entries under that entry, and all entries in subtrees can read the entry that matches the DN string "ou=UserX,o=fujitsu,dc=com", all entries under that entry, and all entries in subtrees

```
access to dn.subtree="ou=UserX,o=fujitsu,dc=com"
  by dn.subtree="ou=UserX,o=fujitsu,dc=com" read
```

#### Specifying Access Levels (<accesslevel>)

For the access level (<accesslevel>), specify the permissions that will be given to the access users (<who>) for the access target (<what>).

Access levels can be specified using the six entry formats shown below. One access level can be specified for each access user <who> ("by" clause). (Multiple access levels cannot be specified for a single access user.)

Note that the access level specification (<accesslevel>) cannot be omitted.

#### Syntax

- none

Prohibits all access.

- auth

Allows authentication operations (binding).

- compare

Allows comparison operations.

- search

Allows search operations (applying search filters). Reading search results is prohibited.

- read

Allows read operations (on search results).

- write

Allows write operations (adding, modifying, deleting or renaming entries).

Each of these access levels includes the privileges of lower access levels, as shown in the following table. For example, the "write" access level includes all other access levels. The "auth" access level is for allowing access to execute authentication operations without any other access permissions. This is to give minimal access permissions to critical resources such as passwords to users that have not been authenticated.

access level	Authentication operations (binding)	Comparison operations	Search operations	Read operations	Write operations
none	X	X	X	X	X
auth	O	X	X	X	X
compare	O	O	X	X	X
search	O	O	O	X	X
read	O	O	O	O	X
write	O	O	O	O	O

O: Allow

X: Prohibit

The access levels required when accessing the repository are as follows:

- Authentication (binding)

Authentication requires "auth" access permission to the "userPassword" attribute.

- Comparing

Comparing attributes requires "compare" access permission to the attribute to be compared.

- Searching

Searching requires "search" access permission to the attributes specified in the search filter and "read" access permission to the attributes and entries in the acquired search results.

- Adding entries

Adding an entry requires "write" access permission to the entry being added and to its parent entry .

- Deleting entries

Deleting an entry requires "write" access permission to the entry being deleted and to its parent entry.

- Modifying entries

Modifying entries requires "write" access permission to the entries and attributes being modified.

- Renaming identifiers

Changing relative distinguished name identifiers requires "write" access permission to the entry whose RDN (relative distinguished name) is being changed, and "write" access permission to the attribute that will become the new RDN. It also requires "write" access permission to the original RDN attribute.

#### Note

- All users that access the repository from clients are regarded as unauthenticated (anonymous) users until an authentication operation is performed. Only the administrator DN will be able to access the repository unless "auth" permission is given to "anonymous" users.

Be sure to give users that have not been authenticated (anonymous users) permission to bind (the "auth" access level) for the "userPassword" attribute.

```
access to attr=userPassword
    by self write
    by users compare
    by anonymous auth
```

- If the bind DN specified when clients access the repository does not match an access user (<who>) in the "by" clauses of any "access" directives, access to the access target (<what>) will be denied. This is because the "by" clause of all "access" directives ends with a silent "by \* none" clause.

#### Settings Example

Creating definitions so that users that have been registered as entries can write (modify) their own "telephoneNumber" attribute, and all other authenticated users can read their 'telephoneNumber" (and users that have not been authenticated cannot access this attribute)

```
access to attr=telephoneNumber
    by self write
    by users read
```

## 4.2.3 Evaluation of Access Control List Definitions

The question of whether to grant users (accessing from clients) access permission to entries or attributes is evaluated in the following order:

1. Evaluate the access target

The repository server compares the entries or attributes specified from the client with the access targets that have been specified in the access control list.

The repository server examines "access" directives in order (starting with the beginning of the access control list), looking for these entries or attributes. The repository server stops searching as soon as it finds the first access target in the access control list that matches the specified entries or attributes.

For example, if an access control list has been defined as shown below and there is a request to access the "telephoneNumber" attribute, the access target in line (1) matches the request, and so the "access" directive starting in line (3) is not examined.

```
access to attr=telephoneNumber    ... (1)
    by self write                  ... (2)
access to attr=telephoneNumber    ... (3)
    by users read                  ... (4)
```

2. Evaluate access users

Next, the repository server compares the access users in the "access" directive selected in Step 1 with the bind DN for the client that is requesting access, in the order in which "by" clauses appear. The repository server stops making comparisons as soon as the first access user that matches the bind DN for the client is found.

Using the access control list in Step 1, if there is an access request for the "telephoneNumber" attribute of an entry whose DN matches the bind DN of the client, the "by" clause in line (2) will match and the repository server will stop making comparisons. If there is an access request for the "telephoneNumber" attribute of another entry whose DN does not match the bind DN of the client, the "by" clause in line (2) will not match. Furthermore, because the evaluation ends at line (1), the access targets and access users in lines (3) and (4) will not be evaluated, and access will be denied.

### 3. Evaluate access levels

Finally, the repository server compares the access level provided by the access level for the access user selected in Step 2 with the access required for the operation that the client has requested. If this access level is greater than or equal to the actual access level required by the operation, access is granted. Otherwise, access is denied.

In this procedure, access will be denied if the entries or attributes in the access request do not match any access targets, or if the user requesting access does not match any access users.

The "by" clause of all "access" directives ends with a silent "by \* none", and all access control lists end with a silent "access to \* by \* none".

This means that the order in which "access" directives appear within access control list definition files is extremely important, because it determines the order in which "access" directives are evaluated.

If the access target for a particular "access" directive is more restrictive than the access target for another "access" directive, definitions should be made so that the more restrictive "access" directive appears earlier in the definition file. In the same way, if a particular access user is more restrictive than other access users, definitions should be made so that the user with more restrictive access appears earlier in the "access" directive.

#### Incorrect Definition Example 1

```
access to attr=telephoneNumber
    by users read      ...Evaluation stops here, so the next statement becomes meaningless.
    by self write
```

In this example, an attempt is made to create definitions so that users who have been registered as entries can modify the "telephoneNumber" attribute for their own entries. However, because the "self" access user is included under "users", the repository server stops evaluating at the "by users read" clause". As a result, users who have been registered as entries will be unable to update their own entries.

The intended definitions can be achieved by reversing the order of the "by" clauses, as shown in the correct example below.

#### Correct Definition Example 1

```
access to attr=telephoneNumber
    by self write
    by users read
```

#### Incorrect Definition Example 2

```
access to attr=mail by self write      ... Evaluation of the "mail" attribute stops here.
access to attr=mail by users read
access to attr=userPassword by self write  ...Evaluation of the "userPassword" attribute stops
here.
access to attr=userPassword by * auth
```

In this example, separate "access" directives to the same access target have been entered for different access users. Here, access control will not work as intended because evaluation stops at the first "access" directive for each access target.

The intended definitions can be achieved by specifying multiple "by" clauses for the same access target, as shown in the correct definition example below. This also makes the definitions easier to check.

#### Correct Definition Example 2

```
access to attr=mail
    by self write
    by users read
access to attr=userPassword
    by self write
    by * auth
```

## Note

Fujitsu recommends working on the specifications for access targets and access users so that the definitions for "access" directives are simple and minimal. If a large number of "access" directives are defined, operating performance may be affected when the repository starts or when access requests (operations) are issued from clients.

## Poor Definition Example

```
access to attr=mail
    by dn="cn=User001,ou=User,o=fujitsu,dc=com" write
    by dn="cn=User002,ou=User,o=fujitsu,dc=com" write
    by dn="cn=User003,ou=User,o=fujitsu,dc=com" write
    by users read
access to attr=userPassword
    by dn="cn=User001,ou=User,o=fujitsu,dc=com" write
    by dn="cn=User002,ou=User,o=fujitsu,dc=com" write
    by dn="cn=User003,ou=User,o=fujitsu,dc=com" write
    by * auth
```

In this example, definitions allowing users that have been registered as entries to modify the "mail" and "userPassword" attributes for their own entries have been made for each individual user.

In contrast, definitions can be made simply and with fewer lines by defining access users as "self", as shown in the good definition example below.

## Good Definition Example

```
access to attr=mail
    by self write
    by users read
access to attr=userPassword
    by self write
    by * auth
```

## 4.3 Registering Access Control Lists

Use the following procedure to register the access control list.

1. Stop the repository by selecting **System > Services > Repository** from the Interstage Management Console (if on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).
2. Display the current state of the access control list using the "-l" option of the access control list definition file registration/display command (*irepac*), and back up the existing access control list definition file using an arbitrary file name.
3. Register the new access control list definition file using the "-f" option of *irepac*.
4. Start the repository by selecting **System > Services > Repository** from the Interstage Management Console (if on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).
5. The backup file that was created in Step 2 poses a security risk, so be sure to delete this file after confirming that the repository runs correctly with the new access control list.

Refer to "irepac" under "Interstage Directory Server Commands" in the *Reference Manual (Command Edition)* for more information about the access control list definition file registration/display command.

Note that it is not possible to have an access control list with no settings at all. (If an empty file is specified with the "-f" option of *irepac*, the access control list will not be replaced with a list with no definitions.)

### Procedure for Restoring the Access Control List

The definitions in the access control list cannot be deleted or restored using *irepac*.

To restore the definitions in the access control list, perform the following procedure using the backup file that was created when the new access control list was registered.

1. Stop the repository by selecting **System > Services > Repository** from the Interstage Management Console (if on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).
2. Use the "-f" option of *irepac1* to reregister the backup file that was created when the new access control list was registered.
3. Start the repository by selecting **System > Services > Repository** from the Interstage Management Console (if on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).
4. The backup file that was created in Step 2 poses a security risk, so be sure to delete this file after confirming that the repository runs correctly with the restored access control list.

To restore the definitions in the access control list to the default state immediately after the repository was created, use the default access control list definition file (stored in the following location) with the same procedure as the "Procedure for Restoring the Access Control List".

**Windows32/64**

```
C:\Interstage\IREP\sample\acl\acl_init.txt
```

**Solaris32/64 Linux32/64**

```
/opt/FJSVirep/sample/acl/acl_init.txt
```

# Chapter 5 Security Audit Trail Functions

It is not possible to completely prevent unauthorized access to an online system. Even with comprehensive security measures in place, information can be leaked and data destroyed through illegal or unauthorized access. If such incidents occur, it is essential to trace the cause of the unauthorized access by performing audit log management. However, the process of outputting the required audit logs presents the following problems:

- To collect audit logs of unauthorized access, it is necessary to modify existing applications, which adds to development time.
- The size of an audit log increases with the scale of the business application, and logs can become too large for a limited number of internal auditors to handle.

Interstage Application Server provides the following security audit trail functions. These functions can use automatically output audit logs to track unauthorized access and illegal operations.

If Systemwalker Centric Manager V13 or later is installed, it is also possible to collect audit logs from distributed servers and manage them from a central location. This makes it easy to collect and analyze logs that originate from distributed servers.

- Access log

This log records the When, Where, Who, What and How of access to protected assets.

- Login log

This log records information about login requests to the Interstage JMX Service. It records when and where a request was issued and by whom, and the result of the request.

It is recommended that the security audit trail functions be used in conjunction with other security-related functions to guard against the unlikely event of a security breach.

## 5.1 Access Log

To prevent access to a system's protected assets, the security policies in the following table must be implemented. If these policies are not adhered to, unauthorized access may occur. Interstage Application Server uses audit logs to store information relating to when, where, who, what and how accesses take place. This means that any unauthorized access can be traced and investigated promptly.

	Security Policy
When	Specify the timeframes when access is permitted for each day of the week.
Where	Use network addresses and terminal numbers to restrict the PCs and terminals that can access a system.
Who	Issue IDs to those people permitted to use a system and use a password to verify the identity of users.
What	Restrict the information that can be accessed by particular IDs.
How	Restrict the operations (queries, updates, additions, deletions, etc.) that can be performed by particular IDs.

When Interstage and Symfoware are linked, Symfoware's audit log can be used to identify who intruded into which Web server to perform an unauthorized access.

Information relating to the time that services such as the Web Service and Servlet Service were accessed is output to audit logs automatically without having to modify applications. This means that if an unauthorized access to a business application is detected, the path of that access can be quickly identified. Audit logs that are collected at this time are referred to as access logs.

The following are explained in this section:

- Information Collected as Access Logs
- The request ID of the Web server
- Web Server Connection Information/IJServer Names Output to the Symfoware Audit Log
- How to Track Unauthorized Access
- Settings Method

## Information Collected as Access Logs

The following information is collected as an access log.

### Interstage single sign-on

When	- The date and time of the access
Where	- The IP address of the client that performed the access
Who	- User ID information
What	- What was accessed
How	- The processing result (additional information) - SessionID - The IP address of the repository server

### Interstage HTTP Server

When	- The date and time of access by a Web client
Where	- The IP address/host name of the Web client and proxy server. - The request ID of the Web server
Who	- Personal user information returned by the Web client - The user name sent from the Web client
What	- The content of the request issued by the Web client
How	- Code returned to the Web client - The amount of data sent to the Web client

### Interstage Directory Service

When	- The access date and time
Where	- IP address: Port number (host name)
Who	- The bind DN
What	- Protocol version - Search base - Search scope - Alias reference rules - Size limit - Time limit - Attribute acquisition method - Search filter - Compared DN - Updated DN - New RDN - Old DN deletion flag - Added DN - Deleted DN
How	- Request or response information



	<ul style="list-style-type: none"> <li>- The request or the result of a request</li> <li>- Error code</li> </ul>
--	--

**Note**

In Windows (64bit) and Linux (64bit), Interstage Directory Service can only be used with Interstage Application Server Enterprise Edition.

**Linking to Symfoware**

When linked to Symfoware, the following information will be collected in Symfoware's audit log. The name of the IJServer that accessed Symfoware will be set as the IJServer name.

- IP address (or host name) of the Web server
- The request ID of the Web server
- Web authentication user name
- IJServer name

**The request ID of the Web server**

Interstage HTTP Server assigns an identifier to a transmitted request and sends the identifier to the request destination. This identifier is referred to as a Web server request ID. The path of an unauthorized access can be easily traced by associating access logs that contain the same request ID.

Web server request IDs are guaranteed to be unique and are created as follows:

Alphanumeric characters (A to Z, a to z, 0 to 9, @, -) are used to encode 112 bits of data (comprising a 32-bit IP address, a 32-bit pid, a 32-bit timestamp and a 16-bit counter) into a 24-byte character string using the same method as MIME base 64 encoding.

**Note**

Request IDs are not sent if a Web server other than Interstage HTTP Server is used.

**Web Server Definitions**

To assign a request ID, add the following definition to the Interstage HTTP Server environment definition file (httpd.conf) and then restart the Web server.

**Windows32/64** (Default installation path)

```
LoadModule unique_id_module "C:/Interstage/F3FMihs/modules/mod_unique_id.so"
```

**Solaris32/64** **Linux32/64** (Default installation path)

```
LoadModule unique_id_module "/opt/FJSVihs/modules/mod_unique_id.so"
```

**Web Server Connection Information/IJServer Names Output to the Symfoware Audit Log**

In three-tier systems containing Web servers, application servers and database servers, applications on an application server generally use a single fixed user ID to connect to a database. (This is because while any number of non-specific users may log into a Web server, specific users tend to connect to a database.) For this reason, the connected user name output to the database audit log is not sufficient to determine who actually connected to the database.

Interstage Application Server can link to Symfoware and output Web server connection information to the Symfoware audit log automatically. The Web server connection information is output to the audit log together with database access information such as issued SQL statements, so the audit log is sufficient to identify who accessed a database. The IJServer name that accessed a database is also output, so it is possible to identify which IJServer manipulated data in the database.

**Information Collected when Interstage and Symfoware are Linked**

The following information is output when Interstage and Symfoware are linked.

Collected Information	Correspondence with Symfoware Audit Log
IP address (or host name) of the Web server	CLIENT_INF
The request ID of the Web server	
Web authentication user name	
IJServer name	MODULE_INF

Information is specified in **CLIENT\_INF** in the following format. The text in italics indicates variable information.

```
I=RequestID,u=UserID,h=HostName
```

RequestID	The request ID of the Web server
UserID	Web authentication user name
HostName	The IP address (or host name) of the Web server

#### Note

CLIENT\_INF can be up to 64 bytes long. If the length of UserID or HostName causes CLIENT\_INF to exceed 64 bytes, the h=HostName section will be output as a hyphen ("-"). If a hyphen is output, the username might also have been discarded. Check the Web server log for a user name or host name that matches the request ID.

To avoid information being lost, it is recommended that the user name be no longer than 20 bytes.

#### Sample output:

```
I=TzJ4HaqDyX8AABMMBcoAAAAw,u=peter,h=192.168.0.2
```

The above information is set automatically when an application executes getConnection with respect to a JDBC data source looked up using the J2EE JNDI function on an IJServer. Interstage automatically executes the following procedure routines provided by Symfoware to set the Web server connection information. When a request is issued to a connection obtained by getConnection, the audit log is output together with the Web server connection information.

- RDBII\_SYSTEM.RDBII\_CLIENT\_INF\_PROC[?]
- RDBII\_SYSTEM.RDBII\_MODULE\_INF\_PROC[?,?]

Nothing is specified for the MODULE\_INF action name (the second parameter in the above procedure), and the Web authentication user name is automatically output to the audit log only when the following functions are used to perform authentication:

- "User authentication (Basic authentication)" function for Web servers
- User authentication function for Web applications
- "Password authentication" function for single sign-on
- "Certificate authentication" function for single sign-on

If a J2EE application has its own user authentication function, the method described in "5.4 Application Interface Details" can be used to set the user ID. This means that information can be transmitted as the Web authentication user name in the Web server connection information using each protocol and information can be output to each audit log.

When accessing a database from an application such as a CORBA application, it is also possible to execute the procedure routine provided by Symfoware directly to set the Web server connection information. Note that if the procedure routine is executed after Web server connection information has already been set with the procedure routine, the existing information will be overwritten.

## How to Track Unauthorized Access

If unauthorized access to a database (Symfoware) has been confirmed, the following methods can be used to trace the access path.

### Tracking Web Servers and Web Clients

1. The "Web authentication user name" output to the Symfoware audit log can be used to identify the name of a user who performed an unauthorized access.

2. The "Web server IP address (or host name)" output to the Symfoware audit log can be used to identify the Web server accessed by an unauthorized user.
3. If the Web server has been identified using 2) above, the Web client that performed the unauthorized access can be identified from the Web server access log.

**Note**

If a Web client accesses a Web server via a proxy server, the Web client cannot be identified.

**Tracking Application Servers**

The following information is output to the Symfoware audit log. This information can be used to identify the application server accessed by an unauthorized user.

Symfoware Audit Log Item	Output Content
Process ID of application/RDB command	Process ID of the IJServer process
Host name/IP address of the machine that executed the application/RDB command	Host name or IP address of the machine that operated the IJServer
Module name	IJServer name

**Tracking the Path of an Unauthorized Access**

A Web server request ID is output by the application server to each audit log. This means that the request ID can be compared with each audit log to track how an unauthorized user accessed a database. This helps to quickly identify system weaknesses and implement appropriate security measures.

When audit logs are associated in this way, their contents can also be checked to determine whether or not the unauthorized user performed any other illegal acts.

**Interstage Single Sign-on Tracking**

According to the procedure shown below, it is possible to investigate the trail of a suspicious individual that was authenticated using Interstage Single Sign-on, from Sign-on until Sign-off.

1. Identify the "Web server request ID" that is output to the Symfoware audit log.
2. In the Interstage Single Sign-on business server access log, identify the record of the request in 1).
3. Identify the "Session ID" that is defined in the record in 2).
4. In the Interstage Single Sign-on authentication server and repository server access logs and the session management log, identify the record of the "Session ID" in 3).
5. From the record in 4), it is possible to track actions performed from the Sign-on operation until the Sign-off operation.
6. In the Interstage Single Sign-on business server access log, identify the record of the "Session ID" in 3).
7. From the record in 6), identify all the "Web server request IDs" that were accessed by the user.
8. Based on the "Web server request IDs" in 7), it is possible to track actions performed in the business system by suspicious individuals.

**Settings Method**

The following settings must be made if the Web server connection information/IJServer name are to be output to the Symfoware audit log:

- JDBC database definition settings

When defining the Symfoware JDBC database, configure the settings so the Web server connection information is output to the audit log.

- Symfoware audit log database setup

Set up the Symfoware audit log database, and configure the settings so the audit log is collected. For details, refer to the Symfoware manual.

For details on obtaining access logs for Interstage services, refer to the following manuals:

- Interstage Single Sign-on

Refer to the 'Messages Logged and Output in Single Sign-on' chapter of the Messages manual.

- Interstage HTTP Server

Refer to the "Interstage HTTP Server Operator's Guide".

- Interstage Directory Service

Refer to the "Directory Service Operator's Guide".

#### Note

In Windows (64bit) and Linux (64bit), Interstage Directory Service can only be used with Interstage Application Server Enterprise Edition.

## 5.2 Login Log

---

It is necessary to log into the Interstage Management Console before sending operation requests to the Interstage JMX Service. The Interstage JMX Service compares the user name and password entered into the Interstage Management Console login window against the user repository (operating system or Directory Service) to check whether they are correct before responding to the login request. If login is successful, the Interstage Management Console can then be used to send operation requests to the Interstage JMX Service.

Requests to log into the Interstage JMX Service can be divided into the following four types:

- Login using operating system authentication from the Interstage Management Console

When the operating system is selected as the user repository in the Interstage Management Console operation security settings, the user ID and password entered at the Interstage Management Console login window are referenced against the operating system by the Interstage JMX Service.

- Login using Directory Service authentication from the Interstage Management Console

When the Directory Service is selected as the user repository in the Interstage Management Console operation security settings, the user ID and password entered at the Interstage Management Console login window are referenced against the Directory Service by the Interstage JMX Service.

- Local authentication login using Interstage services

This login method is used when Interstage services linked to the Interstage JMX Service issue operation requests to the Interstage JMX Service.

- Logging into a managed server from a management server in a multiserver environment

When the multiserver management function is used, operation requests to a management server are issued to managed servers in the site. This login method is used when issuing operation requests from a management server to managed servers..

The login log can be used to check for unauthorized login requests because it contains the following information with respect to all login requests that use these four login types:

- The time at which a login request was issued
- Who issued a login request
- The result of a login request

The following are explained in this section:

- Log File Specifications
- Output Format
- Output Messages

### Log File Specifications

The login log is output to the following file (no settings are required for collecting this log; it is collected automatically):

#### Windows32/64

```
C:\Interstage\jmx\var\log\isjmxruntime\log\isjmxlogin.log
```

#### Solaris32/64 Linux32/64

```
/var/opt/FJSVisjmx/log/isjmxruntime\log\isjmxlogin.log
```

By default, the maximum size of the login log is 1 MB. This limit can be changed within the range 1 MB to 100 MB in the Interstage JMX Service environment definition file "isjmx.xml".

If the upper size limit is exceeded, the log file will be backed up under the following names. Only one backup generation is managed, with each new version replacing the previous one. If necessary, login log backups should be saved to a different location at regular intervals.

#### Windows32/64

```
C:\Interstage\jmx\var\log\isjmxruntime\log\isjmxlogin.log.old
```

#### Solaris32/64 Linux32/64

```
/var/opt/FJSVisjmx/log/isjmxruntime\log\isjmxlogin.log.old
```

## Output Format

The login log stores the execution result of each login request (success or failure) on a single line. The output format of the login log is as follows. Each item is delimited with a space character, facilitating analysis of logged information using Microsoft(R)Excel, for example.

```
<date and time> <host information> <message number>: <message text>
```

Item	Meaning
<date and time>	The date and time at which a login request was sent to the Interstage JMX Service This information is output in the format "YYYY/MM/DD hh:mm:ss.sss". The date and time are separated by a half-width space.
<host information>	Information about the host on which the login request to the Interstage JMX Service was issued
<message number>:<message text>	The message number and text indicating the execution result corresponding to the login request sent to the Interstage JMX Service

A sample login log output is shown below.

```
2006/08/02 15:14:19.329 127.0.0.1 1009:Local Authentication OK. Address=(127.0.0.1)
```

## Output Messages

The following messages are output:

- Message number 1000
- Message number 1001
- Message number 1002
- Message number 1003
- Message number 1004
- Message number 1005
- Message number 1006
- Message number 1007

- [Message number 1008](#)
- [Message number 1009](#)
- [Message number 1010](#)
- [Message number 1011](#)

For details on the meaning of these error codes, refer to [Error Code Meanings and Required Action](#).

**Message number 1000**

1000:Authentication OK. userDN=(%s)

Variable information

%s: User identifier

**Meaning**

Authentication by the Directory Service was successful.

**Message number 1001**

1001:Authentication NG. userDN=(%s) error code=(%x)

Variable information

%s: User identifier

%x: Error code

**Meaning**

Authentication by the Directory Service failed.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

**Message number 1002**

1002:Authentication ABORT. userDN=(%s1) error code=(%x) detail=(%s2)

Variable information

%s1: User identifier

%x: Error code

%s2: SSL-related error (Only when the error code is "0x0C")

**Meaning**

Authentication by the Directory Service was interrupted.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

**Message number 1003**

1003:Authentication OK. userName=(%s)

Variable information

%s: User name

**Meaning**

Authentication by the operating system was successful.

**Message number 1004**

1004:Authentication NG. userName=(%s) error code=(%x)

Variable information

%s: User name

%x: Error code

### Meaning

Authentication by the operating system failed.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

### Message number 1005

1005:Authentication ABORT. userName=(%s) error code=(%x)

#### Variable information

%s: User name

%x: Error code

### Meaning

Authentication by the operating system was interrupted.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

### Message number 1006

1006:Site Authentication OK. Address=(%s)

#### Variable information

%s: Management server host information

### Meaning

Authentication by the multiserver management function was successful.

### Message number 1007

1007:Site Authentication NG. Address=(%s) error code=(%x)

#### Variable information

%s: Management server host information

%x: Error code

### Meaning

Authentication by the multiserver management function failed.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

### Message number 1008

1008:Site Authentication ABORT. Address=(%s) error code=(%x)

#### Variable information

%s: Management server host information

%x: Error code

### Meaning

Authentication by the multiserver management function was interrupted.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

### Message number 1009

1009:Local Authentication OK. Address=(%s)

#### Variable information

%s: Local address

### Meaning

Local connection authentication was successful.

Note that this message is output after output of the 1001 or 1003 message. This message is output to the log when the tree is created in the navigation frame following logon. It does not represent an error state.

Message number 1010

1010:Local Authentication NG. Address=(%s) error code=(%x)

Variable information

%s: Local address

%x: Error code

Meaning

Local connection authentication failed.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

Message number 1011

1011:Local Authentication ABORT. Address=(%s) error code=(%x)

Variable information

%s: Local address

%x: Error code

Meaning

Local connection authentication was interrupted.

Refer to "[Error Code Meanings and Required Action](#)" for information about the error code.

Error Code Meanings and Required Action

Error code	Meaning and Required Action
0x00	Check the following and then log in again: <ul style="list-style-type: none"><li>- Check that the user name and password used to log in at the Interstage Management Console login window are correct.</li><li>- Check that the search base identifier specified in the Directory Service settings in the Interstage Management Console operation security settings is correct.</li><li>- Check that the user information registered with the Directory Service is correct.</li></ul>
0x01	Check the following and then log in again: <ul style="list-style-type: none"><li>- Check that the user name entered in the Interstage Management Console login window contains no invalid characters.</li><li>- Check that the search base identifier specified in the Directory Service settings in the Interstage Management Console operation security settings contains no invalid characters.</li></ul>
0x02	Check the following and then log in again: <ul style="list-style-type: none"><li>- Check that the administrator DN and password specified in the Directory Service settings in the Interstage Management Console operation security settings are correct.</li></ul>
0x03	Check the following and then log in again: <ul style="list-style-type: none"><li>- Check that the administrator DN specified in the Directory Service settings in the Interstage Management Console operation security settings contains no invalid characters.</li></ul>
0x04	Check the following and then log in again: <ul style="list-style-type: none"><li>- Check that a role has been assigned to the user authenticated by the Directory Service.</li></ul>
0x05	Check the following: <ul style="list-style-type: none"><li>- Check that the user name and password used to log in at the Interstage Management Console login window are correct. If the user name or password is not correct, log in using the correct one.</li><li>- A user specified when adding a server with the multiserver management function must have administrator privileges. Servers must also be added by a user who has administrator privileges.</li></ul>



Error code	Meaning and Required Action
0x06	Communication with the Directory Service failed. Check that the settings used to communicate with the Directory Service are correct. Also check that the Directory Service is running.
0x07	The Directory Service cannot be used. Check that the Directory Service is operating normally and then run the process again.
0x08	A password must be used when performing login authentication using the Directory Service. Check the following and then log in again:  - If a password has been specified for the user registered with the Directory Service, specify that password when logging in.  - If no password has been specified for the user registered with the Directory Service, specify a password then use that password when logging in.
0x09	The Directory Service host name or port specified in the Directory Service settings in the Interstage Management Console operation security settings is not correct. Check that the Directory Service host name and port are correct and perform the process again.
0x0A	Access is not from a management server belonging to the same site. Either the managed server site ID key or management server site ID key of the business grid base may be damaged, so restore the Interstage JMX Service resource files.
0x0B	A system error has occurred. Use the <i>iscollectinfo</i> command to collect information to help diagnose the problem then contact a Fujitsu SE.
0x0C	An SSL-related error has occurred. Error information relating to SSL will be output to "detail" in the following format:  - SSLerrortype=%s1 SSLerrorcode=%s2  %s1: SSLException error type  %s2: SSL error code  For details on the information output to "detail", refer to the messages in "Error Codes to be Reported from Interstage Directory Service" in the Messages manual.
0x0D	A system error has occurred. Use the <i>iscollectinfo</i> command to collect information to help diagnose the problem then contact a Fujitsu SE.
x0F	The Directory Service specified in the Directory Service settings in the Interstage Management Console operation security settings does not support simple authentication. Specify use of the Interstage Directory Service in the Directory Service settings in the Interstage Management Console operation security settings.

## 5.3 Login Log Operations

### If Writing to the Login Log Fails

If a problem such as an I/O error or insufficient disk space prevents information from being written to the login log or operation log, the following message will be output to the event log or system log and the operation request will continue to be processed.

- IS: WARNING: is20793: Failed to write the Interstage JMX Service login log file: DETAIL=%s1 INFO=%s2
- IS: WARNING: is20794: Failed to write the Interstage JMX Service operation log file: DETAIL=%s1 INFO=%s2

The login log that failed to be written will be recorded in the event log or system log, so the content of the log output will not be lost. The log will be output to the event log or system log each time the operation is performed, until the log write problem is resolved.

## Managing Login Log Generations

One generation of the login log backup will be maintained.

The message below will be output when the login log is backed up. When this message is output, the existing log backup file will be overwritten. Save copies of the log if it is necessary to retain the information.

- IS: INFO: is20795: The Interstage JMX Service login log was rolled over.

If for any reason the login log backup file fails to be created, the following warning message will be output and the operation process will continue. In such cases, log information will continue to be output to the same log file until the relevant backup can be created. The cause of the problem should therefore be eliminated as quickly as possible.

- IS: WARNING: is20791: Failed to roll over Interstage JMX Service login log file: DETAIL=%s

## Date Format Definition File used by Systemwalker Centric Managers Audit Log Management Function

The date format definition file is required by Systemwalker Centric Managers audit log management function for the logging of logins. The date format definition file used by the login logs is:

**Windows32/64**

```
C:\Interstage\jmx\etc\isjmxauditlog.fmt
```

**Solaris32/64** **Linux32/64**

```
/etc/opt/FJSVisjmx/isjmxauditlog.fmt
```

For details on the audit log management function and the date format definition file, refer to the Systemwalker Centric Manager User's Guide - Monitoring Function Edition.

## Identifying the Terminal used to Process Interstage Management Console Operations

For operations performed from the Interstage Management Console, the request is issued to the Interstage JMX Service by either of the following processes:

- The Interstage JServlet(OperationManagement) running on the same host
- The Interstage JMX Service on the Admin Server

If it is necessary to identify the terminal from which the Interstage Management Console operation requests were issued, you must refer to the time information in the login log and the access log of the Interstage HTTP Server (for the Interstage Management Console). By default, these logs are output to the directory shown below:

The time information recorded in the Interstage HTTP Server (for the Interstage Management Console) access log and the time information recorded in the Interstage JMX Service login log have different processing processes, therefore the time may not be the same.

**Windows32/64**

```
C:\Interstage\gui\trc\F3FMisgui.accesslog
```

**Solaris32/64** **Linux32/64**

```
/var/opt/FJSVisgui/trc/F3FMisgui.accesslog
```

For details on how to view the Interstage HTTP Server (for the Interstage Management Console) access log, refer to "[5.1 Access Log](#)".

## 5.4 Application Interface Details

### [Class name]

com.fujitsu.interstage.j2ee.security.AccessLog

### [Method name]

```
public static void setUserID(String id)
```

### Meaning

This method can be executed with a Web application or EJB application to set the user ID in the Web server connection information to be transmitted. If authentication is performed with a custom authentication function (and this method is used to set an authenticated user ID), the authenticated user ID can be sent via each protocol and the Web authentication user name can be set in the Symfoware audit log when Symfoware is accessed.

This method is valid for invoked threads that are currently running.

### [Usage]

Set the following classpath when compiling an application:

**Windows32/64**

```
C:\Interstage\J2EE\lib\isj2ee.jar
```

**Solaris32/64** **Linux32/64**

```
/opt/FJSVj2ee/lib/isj2ee.jar
```

# Part 3 Firewall and Proxy Server

---

---

Chapter 6 HTTP Tunneling.....	115
Chapter 7 HTTP Tunneling of J2EE.....	123
Chapter 8 Linkage of the Proxy.....	125

# Chapter 6 HTTP Tunneling

This chapter describes HTTP Tunneling.

Note

HTTP tunneling can be used with the following products running in the Windows(R) system, Solaris system, or Linux system:

- Interstage Application Server Enterprise Edition

## 6.1 HTTP Data Communication Using HTTP Tunneling

In HTTP tunneling, data communication using the HTTP protocol can be conducted by converting data communication with the IOP protocol used usually in CORBA applications into HTTP data. This is a useful function when you want to establish client-server linkage beyond the firewall.

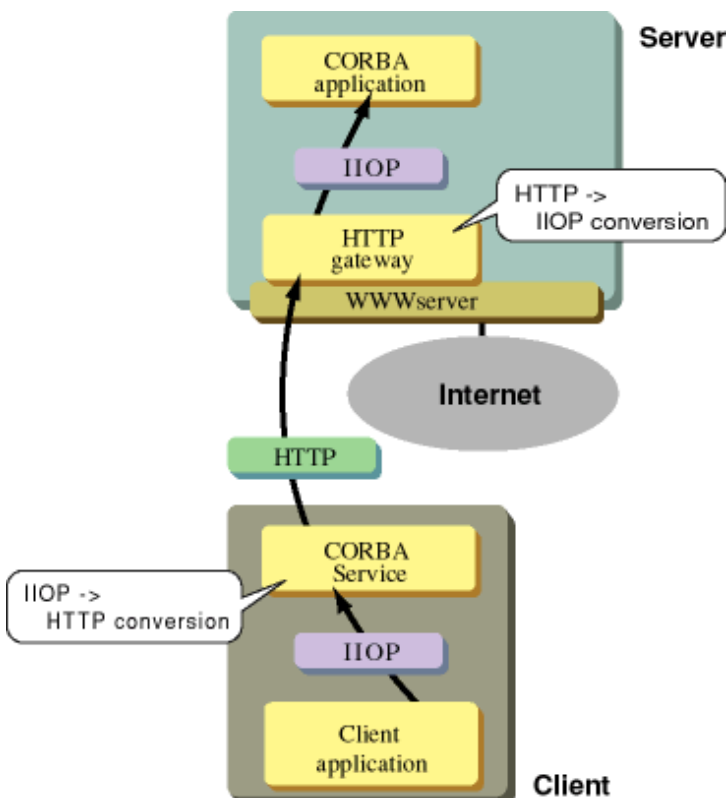
### HTTP Tunneling Mechanism

The following shows the HTTP tunneling mechanism:

On the client side, when HTTP tunneling is specified at start of the client application a request is sent as HTTP data during request sending from the client to the server.

On the server side, the following must be constructed: A Web server for receiving the HTTP data and HTTP gateway environment for converting HTTP data to IOP data. A request sent to the server is converted from HTTP to IOP data via the Web server and HTTP gateway environment. The server application (CORBA application) can receive the request as the IOP data.

The following figure shows a processing image of the HTTP tunneling.



### Processing Image of HTTP Tunneling

### Developing the CORBA Application

When HTTP tunneling is used by a CORBA application, the ordinary CORBA application can be used intact. The application need not be recreated (including re-linkage) to use the HTTP tunneling function.

## Constructing the HTTP Tunneling Environment (Constructing the HTTP Gateway Environment)

To perform data communication by the CORBA application through HTTP, the HTTP gateway environment must be constructed in the Web server.

The HTTP gateway environment enables the linkage to the following Web servers:

- Interstage HTTP Server

### Windows32/64

- Internet Information Services

For the HTTP gateway environment, refer to [6.2 HTTP Tunneling Setup](#).

## Operating HTTP Tunneling

To use HTTP tunneling, specify parameters for using the HTTP tunneling and for specifying the HTTP gateway at start of the client application.

This enables the CORBA application to perform data communication using HTTP between the client and server.

For more information about the start parameter, refer to [6.2 HTTP Tunneling Setup](#).

## 6.2 HTTP Tunneling Setup

---

This section describes the procedure for setting the environment when using the HTTP tunneling in the CORBA application linkage.

### Overview

This section describes the procedures for setting up the environment when HTTP tunneling is used.

Set up the environment for the Web server.

HTTP tunneling can be used by specifying the parameter when client applications are started.

See [6.2.1 Setting up the Web Server Environment](#) for details of setting up the Web server environment.

See [6.2.3 Setting up HTTP Tunneling](#) for details of the startup parameters.

#### Note

For HTTP tunneling, Interstage HTTP Server can be used as a Web server. In a Windows system, InfoProvider Pro and Microsoft Internet Information Services can be used. In a Solaris system, InfoProvider Pro can be used.

Refer to the following manual for details of the Web server functions, and terms related to operating procedures and commands.

### 6.2.1 Setting up the Web Server Environment

---

#### Establishing HTTP-IIOP Gateway

The HTTP-IIOP gateway must be established in the Web server when HTTP tunneling is used. The procedure is described below.

#### Notes

- Check the CORBA Service is operating on Web Server when the HTTP-IIOP gateway operates.

### Solaris32/64

- When using the HTTP tunneling function in the IPv6 environment, the following conditions must be met.
  - The Web server needs to be operated in IPv6.
  - In the IIOP\_hostname parameter in the config file, do not set an IPv6 format address or a host name that can be resolved in the IPv6 format.

#### (1) Using Interstage HTTP Server

Open the Interstage HTTP Server environment definition file using a text editor. Add the following definition to the last line:

```
LoadModule ODhttp_module <HTTP-IIOP gateway file> (*1)
<Location /od-httpgw>
    SetHandler odhttp-handler
    Order deny,allow
    Deny from all
    Allow from all
</Location>
```

For details on the Interstage HTTP Server environment definition file, refer to the "Interstage HTTP Server Operator's Guide".

\*1 HTTP-IIOP gateway file

#### Windows32/64

```
C:\Interstage\ODWIN\bin\httpgw\ODhttpAp.dll
```

#### Solaris32/64

```
/opt/FSUNod/lib/libOMhttpAp.so
```

#### Linux32/64

```
/opt/FJSVod/lib/libOMhttpAp.so
```

These are the file paths from default installation. Change them appropriately to correspond with the installation location specified.

#### Notes

##### Solaris32/64 Linux32/64

- When the Web server is Interstage HTTP Server, messages od40001 and od40002 are not output.

## (2) Using Internet Information Services

#### Windows32/64

Specify the C:\Interstage\ODWIN\bin\httpgw directory as the Internet Information Services virtual directory.

The procedure is as follows:

For IIS 5.0:

1. Select [Control Panel] > [Administrative Tools] > [Internet Services Manager] to start Internet Services Manager.
2. Click the icon for the local computer, and then select the target Web site.
3. Click [Operation] > [Create New] > [Virtual Directory].
4. On the virtual directory creation wizard, click [Next].
5. Enter an alias name (e.g., cgi-bin) in the Alias field, and then click [Next].
6. Specify Interstage-installation-folder\ODWIN\bin\httpgw in the Directory field, and then click [Next].
7. Check the "Execute ISAPI applications or CGIs" check box, and then click [Next].
8. Click [Finish].

For IIS 6.0:

1. Select [Control Panel] > [Administrative Tools] > [Internet Information Services (IIS) Manager] to start Internet Information Services (IIS) Manager.
2. Click the icon for the local computer, and then select the target Web site from Web Sites.
3. Click [Operation] > [Create New] > [Virtual Directory].
4. On the virtual directory creation wizard, click [Next].
5. Enter an alias name (e.g., cgi-bin) in the Alias field, and then click [Next].
6. Specify Interstage-installation-folder\ODWIN\bin\httpgw in the Path field, and then click [Next].

7. Check the "Execute ISAPI applications or CGIs" check box, and then click [Next].
8. Click [Finish].
9. Select Web Service Extensions.
10. Click [Operation] > [Add New Web Service Extension].
11. Enter an extension name in the Extension Name field.
12. Add Interstage-installation-folder\ODWIN\bin\httpgw\ODhttp.dll to Necessary Files.
13. Check the "Set extension status to permitted" check box.
14. Click [OK].

## Writing HTML

To use HTTP tunneling in a Java applet, the parameter must be shown in the param tab of the applet tab in the HTML file executed by the Java applet. For details of the parameter, refer to [6.2.3 Setting up HTTP Tunneling](#).

Following is an example of the HTML when a Java applet is used.

### (1) For Interstage HTTP Server

```
<applet code="Sample.class" width=280 height=300>
  <param name=ORB_FJ_HTTP value=yes>
  <param name=ORB_FJ_SSL value=yes>
  <param name=ORB_FJ_HTTPGW value=http://host.com/od-httpgw>
</applet>
```

### (2) For Internet Information Services

Windows32/64

```
<applet code="Sample.class" width=280 height=300>
  <param name=ORB_FJ_HTTP value=yes>
  <param name=ORB_FJ_SSL value=yes>
  <param name=ORB_FJ_HTTPGW value=http://host.com/cgi-bin/libODhttp.dll>
</applet>
```

## 6.2.2 Setting up the Client Environment

To perform encrypted communication that uses SSL in HTTP tunneling, the SSL environment settings must be configured in the client. The client SSL environment settings are explained below.

### For Pre-installed Client

To perform HTTP tunneling SSL communication in the client (pre-installed type), the SSL environment settings must be configured in the client. To configure the SSL environment for the client, use the same procedure that is used when performing SSL federation.

### For Portable-ORB

To use HTTP tunneling in the client (Portable-ORB), register the certificate in the Web browser environment. The Portable-ORB SSL environment settings are explained below.

To perform SSL communication using the site certificate issued by the CA, the certificate must be registered in the Web browser using the following methods:

- Make the CA certificate available to a Web server in which the SSL environment has not been set.
- Register the CA certificate the first time access is made from the Web browser.

When the certificate is registered in the Web browser, it is possible to use the services of the Web server in which the SSL environment has been set.

An example of the HTML for registering the CA certificate is shown below. When the following link is clicked, the CA certificate is downloaded from the Web server and registered in the Web browser.



```

<HTML>
<BODY>
<A HREF="cacert.der">CA certificate</A>
    . . .
    . . .
</BODY>
</HTML>

```

**Note**

- When SSL communication is performed in Portable-ORB version HTTP tunneling, there are browser and Java VM combinations that cannot be used. Supported browser and Java VM combinations are shown below.

Browser	Java VM	HTTPS(SSL)
Internet Explorer	JBK Plug-in	YES (see Note)
Internet Explorer	Java Plug-in	NO

Note: when a JBK Plug-in is used, the following must be defined in the JBK Plug-in settings file (jbkplugin.properties):

jbk.plugin.protocol.https=native

- The CA certificate data type is "application/x-x509-ca-cert". Check that there is an "application/x-x509-ca-cert" definition in the Web server environment definition file and also in the file in which the file extension relationship is specified (definition name:content-type). Check that the file extension of the certificate that was created is associated.
- The Web server that the CA certificate is downloaded from does not have to be the Web server that is used to perform SSL communication.
- If a CA certificate is updated because it has expired, for example, the old certificate must be deleted from the Web browser, and then the new certificate must be downloaded and re-registered.

**Obtaining the client certificate**

Client authentication is performed using SSL version 3.0, therefore the Web browser requires a client certificate (site certificate). This must be registered in the certificate/CRL management environment. Request a client certificate from the issuing CA.

**6.2.3 Setting up HTTP Tunneling**

In order to use HTTP tunneling, specify the parameters in the following table for the CORBA\_ORB\_init function called by a client application.

**Application other than Java applet**

Specify as a parameter when starting the application.

However, the application must be capable of passing the startup parameters to the CORBA\_ORB\_init function. The application presents no problem if it passes the main arguments to the CORBA\_ORB\_init function just as they are. Otherwise, the application logic must be modified so that the HTTP tunneling parameters are passed to the CORBA\_ORB\_init function.

**Java applet**

Use the <param> tag in the HTML file to specify the applet start time parameter.

**HTTP Tunneling Parameters**

Parameter Name	Meaning
-ORB_FJ_HTTP	Specifies whether HTTP tunneling is used - yes: HTTP tunneling is used (*1) The default, or if any value but yes is specified, is no tunneling.
-ORB_FJ_HTTPGW	Specifies the gateway that processes HTTP tunneling (*2)

Parameter Name	Meaning
	<p>(1) For Interstage HTTP Server</p> <p>[Format for using SSL communication]</p> <p>https://host-name/url-name</p> <p>[Format for not using SSL communication]</p> <p>http://host-name/url-name</p> <p>host-name:</p> <p>Specifies the Web server that downloads HTML.</p> <p>url-name:</p> <p>Specifies od-httpgw. For url-name, specify the URL of the Location directive.</p> <p>(2) For Internet Information Services <a href="#">Windows32/64</a></p> <p>[Format for using SSL communication]</p> <p>https://host-name/cgi-ID/gateway-name</p> <p>[Format for not using SSL communication]</p> <p>http://host-name/cgi-ID/gateway-name</p> <p>host-name:</p> <p>Specify the Web server that downloads the HTML</p> <p>cgi-ID:</p> <p>Specify the alias of the virtual directory.</p> <p>gateway-name:</p> <p>Specify Odhttp.dll (HTTP-IIOP gateway)</p>

\*1 If 'yes' is specified, the HTTP tunneling function is valid if the value of argc.argv posted by the parameter in CORBA\_ORB\_init() is specified.

\*2 The format of the host names that can be specified as arguments to be passed to "-ORB\_FJ\_HTTPGW" are shown below.

#### (1) For Interstage HTTP Server

```
http://host-name IPv4-address/URL-name
http://host-name IPv4-address:port-number/URL-name
https://host-name IPv4-address/URL-name
https://host-name IPv4-address:port-number/URL-name
```

#### (2) For Internet Information Services [Windows32/64](#)

```
http://host-name IPv4-address/cgi-identification-name/gateway-name
http://host-name IPv4-address:port-number/cgi-identification-name/gateway-name
http://[IPv6-address]/cgi-identification-name/gateway-name
http://[IPv6-address]:port-number/cgi-identification-name/gateway-name
https://host-name IPv4-address/cgi-identification-name/gateway-name
https://host-name IPv4-address:port-number/cgi-identification-name/gateway-name
```

When using an address in the IPv6 format, it needs to be enclosed by square brackets ("[" and "]").

### Application Other than the Java Applet

Specify the parameter in the following way when a client application (sample\_c) is started:

#### (1) For Interstage HTTP Server

```
sample_c -ORB_FJ_HTTP yes -ORB_FJ_SSL yes
         -ORB_FJ_HTTPGW http://host.com/od-httpgw
```

(2) For Internet Information Services **Windows32/64**

```
sample_c -ORB_FJ_HTTP yes -ORB_FJ_SSL yes
         -ORB_FJ_HTTPGW http://host.com/cgi-bm/Odhttp.dll
```

**Solaris32/64**

```
sample_c -ORB_FJ_HTTP yes
         -ORB_FJ_HTTPGW http://host.com/cgi-bm/libOMhttp.so
```

**Notes**

- In client applications, use CORBA\_ORB\_net\_disconnect() from the Fujitsu Extended Interface to disconnect the communication resource used. This is unnecessary when the Solaris or Linux system is used and the Web server is Interstage HTTP Server.
- When the Solaris or Linux system is used and the Web server is Interstage HTTP Server, no action is required because the connection with the server is released for each communication. Otherwise, client applications do not automatically disconnect the communication resource with the server at termination of the application. Thus, if the resource is not disconnected, the client application starts and stops repeatedly, the number of connections set in max\_IOP\_resp\_con in the config file is insufficient, and a COMM\_FAILURE exception will be posted.
- Client applications created with C, C++, Java, COBOL, or OOCOBOL can be used for HTTP tunneling. They cannot be used from the OLE-CORBA gateway.

**Java Applets**

The HTML used for Java applets is shown below.

When the parameters are written in HTML, do not specify the hyphens in the parameter names.

When Pre-installed type Java Library is Used

(1) For Interstage HTTP Server

```
<HTML>
<HEAD><!--demo.html-->
<TITLE>Java sample Applet </TITLE>
<BODY>
</HEAD>
<H1>Java sample Applet</H1>
<applet code="Sample.class" width=300 height=250>
<PARAM NAME=ORB_FJ_HTTP VALUE=yes>
<PARAM NAME=ORB_FJ_SSL VALUE=yes>
<PARAM NAME=ORB_FJ_HTTPGW VALUE=http://host.com/od-httpgw>
</applet><BR>
</BODY>
</HTML>
```

(2) For Internet Information Services **Windows32/64**

```
<HTML>
<HEAD><!--demo.html-->
<TITLE>Java sample Applet </TITLE>
</HEAD>
<BODY>
<HI>Java sample Applet</HI>
<applet code="Sample.class" width=300 height=250>
<PARAM NAME=ORB_FJ_HTTP VALUE=yes>
<PARAM NAME=ORB_FJ_SSL VALUE=yes>
<PARAM NAME=ORB_FJ_HTTPGW VALUE=http://host.com/cgi-bin/Odhttp.dll>
</applet><BR>
</BODY>
</HTML>
```

For an explanation of how to create HTML files when using Java applets, see the documents below.

- For Interstage Application Server Enterprise Edition:

Java Programming Guide in the Distributed Application Development Guide (CORBA Service Edition).

## 6.2.4 Setting to be Made When an HTTP Proxy Server is to be Used

---

When performing HTTP tunneling through an HTTP proxy server in the pre-installation type run-time (in an execution environment other than Portable-ORB), it is necessary to set the following in the config file of the CORBA server.

`http_proxy_use`: Specify whether to use HTTP tunneling (yes/no)

`http_proxy`: Specify the HTTP proxy server host name.

`http_proxy_port`: Specify the HTTP proxy server port number.

To enable the new setting of the config file, restart the CORBA service.

### Example

```
http_proxy_use = yes
http_proxy     = proxy.xxx.com
http_proxy_port = 8080
```

### Note

This specification is not required if Portable-ORB is used, because the proxy server specified in the Web browser is used.

## Chapter 7 HTTP Tunneling of J2EE

This chapter describes the HTTP Tunneling of J2EE.

HTTP tunneling for J2EE can be used with the following:

- J2EE application client
- IJServer (Web Applications Only)
- Java applet

HTTP tunneling for J2EE cannot be used with IJServer of any of the following types:

- Web Applications and EJB Applications run in same Java VM
- Web Applications and EJB Applications run in separate Java
- EJB Applications Only

Note

The HTTP Tunneling of J2EE can be used with the following:

- Interstage Application Server Enterprise Edition

### 7.1 Use of HTTP Tunneling in J2EE Application Client

To use HTTP tunneling with a J2EE application client, specify a gateway for processing HTTP tunneling using HTTPGW of the JNDI environment property. Refer to JNDI Service Provider Environment Setup in the J2EE User's Guide for details of the JNDI environment property.

An example of describing argument (-D) in the command line is shown below.

(1) For Interstage HTTP Server

```
java -DHTTPGW=http://host.com/od-httpgw SampleClient
```

(2) For Internet Information Services

```
java -DHTTPGW=http://host.com/cgi-bin/ODhttp.dll SampleClient
```

### 7.2 Method for Using HTTP Tunneling with IJServer (Contains Web Applications Only)

HTTP tunneling can be used with IJServer only when IJServer is 'Web Applications Only' type.

To use the HTTP tunneling function, set [HTTPGW] in the environment properties in the IJServer Java VM option or FJjndi.properties file.

For details about the values set for the [HTTPGW] in the environment properties and the settings contents, refer to 'J2EE application client' under 'JNDI Service Provider Environment Setup' in the JNDI chapter of the 'J2EE User's Guide'.

### 7.3 Method for Using HTTP Tunneling with Java Applets

When Java applets start, HTTP tunneling is specified with parameters of the <PARAM NAME> tags in HTML.

For information about the parameters to be specified, refer to "Setting up HTTP Tunneling" in "HTTP Tunneling".

An example is shown below.

(1) For Interstage HTTP Server. (The items in bold text are the settings for the <PARAM NAME> parameters.)

```
<applet code="Sample.class" width=300 height=250>  
<PARAM NAME=ORB_FJ_HTTP VALUE=yes>
```

```
<PARAM NAME=ORB_FJ_SSL VALUE=yes>  
<PARAM NAME=ORB_FJ_HTTPGW VALUE=https://host.com/od-httpgw>  
</applet>
```

(2) For Internet Information Services. (The items in bold text are the settings for the <PARAM NAME> parameters.)

**Windows32/64**

```
<applet code="Sample.class" width=300 height=250>  
<PARAM NAME=ORB_FJ_HTTP VALUE=yes>  
<PARAM NAME=ORB_FJ_SSL VALUE=yes>  
<PARAM NAME=ORB_FJ_HTTPGW VALUE=https://host.com/cgi-bin/Odhttp.dll>  
</applet>
```

## Chapter 8 Linkage of the Proxy

This chapter describes the linkage of the Proxy.

### 8.1 Linkage of the Proxy and Interstage Web Service

---

Interstage Web Service can be used with the following products:

- Interstage Application Server Enterprise Edition
- Interstage Application Server Standard-J Edition

In the Interstage Web service, linkage between Web services via a proxy is possible.

For details, refer to the 'Interstage Web Service Operation' chapter of the J2EE User's Guide.

If SSL is used on the Web service client, the default proxy port number is [80] (this is only effective if a host name has been set).

### 8.2 Linkage of the Proxy and Web Service Function of Java EE

---

In the Web Service function of Java EE, linkage between Web services via a proxy is possible.

For details, refer to the 'Developing Web Service Client Applications' - 'Using a Proxy' in the Java EE Operator's Guide.

# Part 4 Authentication and Encrypted Communications through Support for SSL

This part of the manual explains how to perform encryption communication using SSL.

Encryption and signature handling require environments for controlling certificates and private keys to be configured. Interstage uses three different environments described below for those purposes. Select an environment that is suitable for the services you use and your usage situation.

For this version, use of the Interstage certificate environment is recommended.

- Interstage certificate environment (recommended)

This environment can be shared by multiple services, and allows a unified control of certificates and private keys. You can access this environment using the Interstage Management Console.

For details on how to configure this environment, refer to the "[Chapter 9 Setting and Use of the Interstage Certificate Environment](#)" chapter.

Note: The following package is required for this environment:

Interstage Management Console

- Certificate/key management environment configured with the SMEE command

This environment needs to be configured separately for the respective services, using the SMEE command.

For details on how to configure this environment, refer to the "[Chapter 10 Setting and Use of the Certificate/Key Management Environment Using the SMEE Command](#)" chapter.

Note: The following components are necessary for this environment:

Secure communication service

**Solaris32**

FJSVsmee, FJSVslcr, and FSUNssl packages

**Solaris64**

FJSVsmee64 and FJSVslcr64 packages

**Linux32**

FJSVsmee and FJSVslcr packages

**Linux64**

FJSVsmee64 and FJSVslcr64 packages

- Keystore

The Java encryption packages JSSE (Java Secure Socket Extension) and JCE (Java Cryptography Extension) are used.

This environment needs to be configured separately for the respective services.

The following table shows the service that supports each environment.

## Services and Environments

Service name	Interstage certificate environment	Certificate/key management environment	Keystore
Interstage HTTP Server	Yes	Yes	No
CORBA Service (except for the client package)	Yes	Yes	No



Service name	Interstage certificate environment	Certificate/key management environment	Keystore
CORBA Service (for the client package)	No	Yes	No
Servlet Service	Yes	No	No
EJB Server/EJB Client	No	Yes	No
Interstage JMS (except for the client package)	(*1)	(*1)	No
Interstage JMS (for the client package)	(*2)	(*2)	No
Event Service	(*1)	(*1)	No
Interstage Directory Service server	Yes	No	No
Interstage Directory Service client	No	Yes	No
Interstage Single Sign-on	(*3)	(*3)	No

Yes: Supported

No: Not supported

\*1 Uses the environment configured in the CORBA Service (except for the client package).

\*2 Uses the environment configured in the CORBA Service (for the client package).

\*3 Uses the environment configured in Interstage HTTP Server to use SSL in the Interstage Single Sign-on repository server and authentication server.

**Note**

Whether the service can be used depends on the environment.

If SSL encrypted communication is to be performed in an environment configured with a version prior to V6.0, refer to the section on Authentication and Encrypted Communications through SSL Support in the previous version of the manual.

<a href="#">Chapter 9 Setting and Use of the Interstage Certificate Environment.....</a>	128
<a href="#">Chapter 10 Setting and Use of the Certificate/Key Management Environment Using the SMEE Command.....</a>	140
<a href="#">Chapter 11 How to Use SSL with Interstage HTTP Server.....</a>	152
<a href="#">Chapter 12 How to Use SSL with the CORBA Service.....</a>	186
<a href="#">Chapter 13 How to Use SSL with J2EE.....</a>	191
<a href="#">Chapter 14 Using SSL for Interstage Directory Service.....</a>	195

# Chapter 9 Setting and Use of the Interstage Certificate Environment

This chapter explains what is required for signature and encryption processing for SSL, and explains the required processing settings.

This chapter describes a case in which the Interstage certificate environment is used.

## Note

To use the Interstage certificate environment, you need to have the Interstage Management Console installed.

The Interstage certificate environment that is created here is typically used for the following services:

- Interstage HTTP Server
- CORBA Service (except client package)
- Servlet Service
- Interstage JMS

Note: To use SSL on Interstage JMS, use the environment configured in the CORBA Service.

- Event Service

Note: To use SSL on Event Service, use the environment configured in the CORBA Service.

- Interstage Directory Service
- Interstage Single Sign-on

## Note

- To use SSL in the Interstage Single Sign-on repository server and authentication server, use the environment configured in the Interstage HTTP Server.

When you use services other than those listed above or you have not installed the Interstage Management Console, refer to the relevant section of Part IV of this manual, "Authentication and Encrypted Communications through Support for SSL".

## 9.1 Certificates and Private Keys

This section explains certificates and private keys.

### What are the Certificates and the Private Keys?

The CA (Certification Authority) certificate, site certificate, and corresponding private key are required for signature and encryption processing such as for SSL communication. A certificate revocation list (CRL) is also used to check the validity of a certificate.

A certificate and CRL that conform to X.509 or RFC2459 and that use an RSA key can be used.

- CA certificate

Certificate of the CA itself.

A CA may issue a certificate to a subordinate CA, in which case the certificate of the CA itself and the certificate issued to the subordinate CA are both referred to as a CA certificate. The certificate issued to the subordinate CA is specifically referred to as an intermediate CA certificate.

- Site certificate

A site certificate is issued by a CA to certify the identity of a server, client, or service. It includes information on the user (server, client, or service) and information on the CA. The site certificate must always be used in combination with the CA certificate that issued the site certificate.

Certificates are assigned a validity period. Certificates can not be used after their validity period ends. It is necessary to update the key pair and obtain a new certificate before the validity period ends. Refer to "[Updating a Certificate \(Before Expiration\)](#)" for details.

- Private key corresponding to a site certificate

The private key forms a pair with the public key included in the site certificate.

#### Note

Losing or deleting a private-key means that the site certificate that it corresponds to is unable to be registered.

Therefore, be sure to keep a backup of private keys.

- Certificate revocation list (CRL)

The CA issues the CRL. The CRL contains a list of certificates revoked by the CA. Reasons a certificate may be revoked include theft of the private key; loss of user qualifications; and so on.

If the CRL is used with SSL communication, the validity of the certificate of the connected site or client is checked against it.

The CRL is issued regularly. It is often made public on Web servers and directory servers managed by the CA. The method used to publish the CRL depends on the method defined in the CA policy. Check the CA's policy information for details. The location to which the CRL should be published is sometimes included in the certificate.

PKCS#12 data may be used to deliver certificates and private keys or make a backup. PKCS#12 data includes a certificate, a private key corresponding to it, and a Certification Authority certificate, all of which are password-encrypted.

In the Interstage certificate environment, you can import (register) the following types of PKCS#12 data:

- PKCS#12 data exported (extracted) with the `scsexppfx` command from the Interstage certificate environment
- PKCS#12 data exported with the `cmmkpfx` command from a certificate/key management environment created with the SMEE command

In addition, you can import PKCS#12 data exported from the Interstage certificate environment into the following environments:

- Interstage certificate environment (by means of the `scsimppfx` command)
- Certificate/key management environment created with the SMEE command (by means of the `cmentpfx` command)

For details about the certificate/key management environment, refer to the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter.

## CA (Certification Authority)

The CA (Certification Authority) is required to obtain a certificate.

The Interstage Certificate Environment supports "Secure Site SSL Certificates" certificates and CRL issued by the VeriSign Inc. Certification Authority, "Secure Site with EV SSL Certificates" certificates and CRL issued by the VeriSign Inc. Certification Authority, "Cybertrust SureServer Certificate" and CRL issued by the Cybertrust, Inc. Certification Authority.

#### Note

Certificates issued by CAs (certification authorities) other than those listed above are considered to be granted if they satisfy the following:

- They comply with X.509 or RFC2459
- They use the RSA key and their key length is not more than 4,096 bits
- They use the following hash algorithm
  - MD5
  - SHA-1
  - SHA-256
  - SHA-384
  - SHA-512

However, the operations of such certificates with the Interstage Application Server as well as the acquisition process for them have not been assured. This means that they are not in the scope of official support.

## 9.2 Configuring Environments

---

The Interstage Certificate Environment is an environment in which certificates, private keys, and CRLs are managed. The Interstage Certificate Environment is configured and updated using commands and referenced using the Interstage Management Console. This section describes how to configure the Interstage certificate environment.

The resources of the Interstage Certificate Environment are placed in the following directory:

**Windows32/64**

```
C:\Interstage\etc\security
```

**Solaris32/64** **Linux32/64**

```
/etc/opt/FJSVisscs/security
```

You can configure the Interstage certificate environment in either of the following two ways, depending on how you obtain a certificate:

- Using a CSR (Certificate Signing Request)
- Using PKCS#12 data

These methods are described below.

### Using a CSR (Certificate Signing Request)

To ask VeriSign Inc. or another Certification Authority issuing certificates by means of a CSR to issue a certificate, or when a private Certification Authority is configured for a small-scale user using CSR, configure the environment using the following steps:

1. **Solaris32/64** **Linux32/64**

Create an Interstage certificate environment owner group.

Refer to "[9.2.1 Setting up Access Permissions in the Interstage Certificate Environment](#)".

2. Configure the Interstage certificate environment.

Refer to "[9.3 Configuring the Interstage Certificate Environment with CSR](#)".

3. Make the settings for use of the certificate.

Refer to "[9.5 Configuring Certificate Settings](#)".

### Using PKCS#12 Data

Use PKCS#12 data when a private Certification Authority is configured for a large-scale user and certificates are batch-issued. Configure the environment using the following steps:

1. **Solaris32/64** **Linux32/64** Create an Interstage certificate environment owner group.

Refer to "[9.2.1 Setting up Access Permissions in the Interstage Certificate Environment](#)".

2. Configure the Interstage certificate environment.

Refer to "[9.4 Configuring the Interstage Certificate Environment with PKCS#12](#)".

3. Make the settings for use of the certificate.

Refer to "[9.5 Configuring Certificate Settings](#)".

## 9.2.1 Setting up Access Permissions in the Interstage Certificate Environment

---

**Solaris32/64** **Linux32/64**

Before configuring the Interstage certificate environment, you need to create owner groups allowed to access the Interstage certificate environment.

The Interstage certificate environment is configured by a superuser and accessible to effective users who belong to a specific owner group.

Effective users are assigned depending on the service. Add effective users to owner groups by service.

Although you can create or modify an owner group using an OS tool, the steps below give an example of creating an owner group using the command line.

1. Create an Interstage certificate environment owner group.

The example below shows a command for creating a group named "iscertg".

```
groupadd iscertg
```

2. Execute the useradd or usermod command to register an effective user in the "iscertg" group.

The example below shows a command for adding "nobody" to "iscertg".

```
usermod -G iscertg nobody
```

For details about the commands, refer to the manual of the operating system you are using.

Specify the owner group you created with the -g option of the scsmakeenv command when configuring the Interstage certificate environment.

#### Note

- Execute the commands as a superuser.
- For effective users to be registered in the Interstage certificate environment, if SSL is used on Interstage HTTP Server, you need to set users who have been specified in the User directive of the Interstage HTTP Server environment definition file (httpd.conf). The initial user value specified in the User directive is "nobody."

#### Windows32/64

To give users without Administrators privileges access to the Interstage Certificate Environment, first create an Interstage Certificate Environment using the Administrators permission, then set the access permissions to allow appropriate users to access it.

This applies to the following:

- For CORBA Service, to allow users with a general permission to handle the SSL function.
- When integrating the business server that performs session management operations into Microsoft(R) Internet Information Services (IIS)

Select the Interstage Certificate Environment folder in Windows Explorer. Right-click and select "Properties". Click the "Security" tab. Select the relevant user or group. Select "Full control" permission. Click OK.

For details About the Interstage Certificate Environment folder, refer to "Configuring Environments" in the "Setting and Use of the Interstage Certificate Environment" chapter.

#### Note

If the [Security] tab is not displayed for the folder's properties on Microsoft(R) Windows(R) XP, take the following steps to display it:

1. Select [Start]-[Control Panel]-"Folder Options".
2. Click the [View] tab, remove the checkmark on "Use Simple File Sharing (Recommended)", and click "OK".

## 9.3 Configuring the Interstage Certificate Environment with CSR

This section describes how to configure the Interstage certificate environment using a CSR (Certificate Signing Request).

Create an Interstage certificate environment using the following steps:

1. [Configuring an Interstage Certificate Environment and Creating a Certificate Signing Request \(CSR\)](#)
2. [Requesting Certificate Issuance](#)
3. [Registering Certificates and CRL](#)

Note that you need to set up the environment to use the certificate after configuring the Interstage certificate environment. For more details refer to "9.5 Configuring Certificate Settings".

Refer to the Reference Manual (Command Edition) for details of the commands used later in this section.

Note

**Windows32/64**

- Execute commands as a user with Administrators authority.

**Solaris32/64 Linux32/64**

- Execute commands as a super user.
- Before execution, set the environment variable JAVA\_HOME to the installation path for JDK or JRE.

### 9.3.1 Configuring an Interstage Certificate Environment and Creating a Certificate Signing Request (CSR)

---

A certificate must be obtained to perform signature and encryption processing such as for SSL. For this purpose, it is necessary to create a certificate signing request (CSR) that is the data used to request the CA to issue a certificate. When a CSR is created, an Interstage Certificate Environment is also created if it does not exist. If an Interstage Certificate Environment already exists, that certificate environment is used.

Note

The nickname specified when the CSR is created must also be specified when the site certificate is registered.

Note that the list of nicknames specified in the CSR can be checked using the *scslist* command.

Additionally, new certificates cannot be registered using a nickname that is already registered in the Interstage certificate environment.

Creating a CSR generates a private key in the Interstage certificate environment. To protect the private key, make a temporary backup of the Interstage certificate environment after creating the CSR and keep it until you obtain the certificate. Refer to the Operator's Guide for details of the backup procedure.

When you make no backup, you need to again create the Interstage certificate environment and create and issue a CSR, if the Interstage certificate environment is damaged.

An example of creating a CSR is shown below:

**Windows32/64**

```
scsmakeenv -n SiteCert -f C:\my_folder\my_csr.txt -c
```

**Solaris32/64 Linux32/64**

```
scsmakeenv -n SiteCert -c -f /usr/home/my_dir/my_csr.txt -g iscrtg
```

Note

- The nickname specified for the -n option must be specified at registration of the site certificate. Be sure to remember the nickname.
- In an operating mode in which a service that runs as a client function obtains only server authentication, create a test certificate instead of CSR using the *scsmakeenv* command. Refer to the Reference Manual (Command Edition) for information on test certificate creation. After creating a test certificate, there is no need to perform the [9.3.2 Requesting Certificate Issuance](#) and [9.3.3 Registering Certificates and CRL](#) sections described below. Perform the sections "9.5.1 Defining the Use of Certificates", onwards.

The services listed below are concerned:

- Interstage Directory Service (if a standard database is used as the repository database and the Replication Connection Settings of the master in replication mode is set to use SSL)
- CORBA Service (client-sided setting when SSL linkage is in use, if client authentication is not to be performed)
- Servlet Service (SSL communication setting on the Web server connector side when Web server and WorkUnit are not on the same machine)

- Interstage HTTP Server (when SSL communication with a directory server on another system is set for the online access management function)

## 9.3.2 Requesting Certificate Issuance

---

Request the CA to issue a certificate, and obtain a certificate.

### Requesting Certificate Issuance

Send the CSR created with the `scsmakeenv` command to the CA to request certificate issuance. Follow the request procedure specified by the CA.

### Obtaining a Certificate

Obtain a certificate in binary data (DER) format or Base64 encoding data (PEM) format from the CA.

A certificate in PEM format is shown below:

```
-----BEGIN CERTIFICATE-----  
(Base-64-encoded certificate data is embedded.)  
-----END CERTIFICATE-----
```

Follow the acquisition procedure specified by the CA.

## 9.3.3 Registering Certificates and CRL

---

Register the certificates and CRL obtained from the CA in the Interstage Certificate Environment.

Register the CA certificate first.

#### Note

After registering the obtained certificates and CRL, be sure to make a backup of the Interstage Certificate Environment. Refer to the Operator's Guide for details of the backup procedure.

When you make no backup of the Interstage certificate environment, you need to again create the Interstage certificate environment and create a CSR and request certificate issuance, if the Interstage certificate environment is damaged.

### Registering the CA Certificate

Register the obtained CA certificate.

An example of registration is shown below.

**Windows32/64**

```
scsenter -n CA -f C:\my_folder\CA.der
```

**Solaris32/64 Linux32/64**

```
scsenter -n CA -f /usr/home/my_dir/CA.der
```

The CA certificate can be referenced by selecting [System] > [Security] > [Certificates] > [CA certificates] from the Interstage Management Console.

#### Note

- The CORBA Service requires all CORBA servers and clients that use SSL to register certificates from the same CA. Refer to the "How to Use SSL with the CORBA Service" chapter for information on how to register a certificate with the CORBA Service client package.

### Registering the Intermediate CA Certificate

Depending on the CA, intermediate CA certificates may be provided in addition to the CA and site certificates. In this case, register the intermediate CA certificates distributed by the CA before registering the site certificate.

The registration method is the same as for the CA certificate. For details, refer to ["Registering the CA Certificate"](#). For the intermediate CA certificate nickname, specify a name different to the CA or site certificate nickname.

## Registering a Site Certificate

Register the issued certificate as a site certificate.

An example of registration is shown below.

**Windows32/64**

```
scsenter -n SiteCert -f C:\my_folder\SiteCert.der -o
```

**Solaris32/64 Linux32/64**

```
scsenter -n SiteCert -f /usr/home/my_dir/SiteCert.der -o
```

The site certificate can be referenced by selecting [System] > [Security] > [Certificates] > [Site certificates] from the Interstage Management Console. Examine the validity period of the certificate to confirm the date when the certificate needs to be updated. Refer to ["Updating a Certificate \(Before Expiration\)"](#) for details.

### Note

For the -n option, specify the same nickname as that specified when creating a CSR.

## Registering the Certificate of Another Reliable Site

Register the certificate of another reliable site.

An example of registration is shown below.

**Windows32/64**

```
scsenter -n OtherSiteCert -f C:\my_folder\OtherSiteCert.der -e
```

**Solaris32/64 Linux32/64**

```
scsenter -n OtherSiteCert -f /usr/home/my_dir/OtherSiteCert.der -e
```

The certificate of another reliable site can be referenced by selecting [System] > [Security] > [Certificates] > [CA certificates] from the Interstage Management Console.

## Registering a CRL

There is no need to register the CRL unless it is used for revocation checks. If it is used for revocation checks, obtain and register the latest CRL regularly.

An example of registration is shown below.

**Windows32/64**

```
scsenter -c -f C:\my_folder\CRL.der
```

**Solaris32/64 Linux32/64**

```
scsenter -c -f /usr/home/my_dir/CRL.der
```

### Note

The Web Service client and Servlet Service (container) do not reference CRL to check for revocation.



## 9.4 Configuring the Interstage Certificate Environment with PKCS#12

---

This section describes how to configure the Interstage certificate environment using PKCS#12 data.

Create an Interstage certificate environment using the following steps:

1. [Configuring the Interstage Certificate Environment](#)
2. [Registering PKCS#12 Data, Certificates, and CRLs](#)

Note that you need to set up the environment to use the certificate after configuring the Interstage certificate environment. For details refer to "[9.5 Configuring Certificate Settings](#)".

Refer to the Reference Manual (Command Edition) for details of the commands used later in this section.

Note

**Windows32/64**

- Execute commands as a user with Administrators authority.

**Solaris32/64 Linux32/64**

- Execute commands as a super user.
- Before execution, set the environment variable JAVA\_HOME to the installation path for JDK or JRE.

### 9.4.1 Configuring the Interstage Certificate Environment

---

To set up signature handling and encryption, such as via SSL, you need to obtain a certificate and register it in the Interstage certificate environment.

This section gives an example of configuring the Interstage certificate environment.

**Windows32/64**

```
scsmakeenv -e
```

**Solaris32/64 Linux32/64**

```
scsmakeenv -e -g iscerty
```

Note

- For operation with server authentication on a service running as a client function, refer to and execute the scsmakeenv command to create a test certificate, not a CSR.

### 9.4.2 Registering PKCS#12 Data, Certificates, and CRLs

---

Register the PKCS#12 data, certificate, and CRL obtained from the Certification Authority in the Interstage certificate environment.

Note

Importing the PKCS#12 data registers the site certificate, private key corresponding to it, and the Certification Authority certificate in the Interstage certificate environment. Therefore, after importing PKCS#12 data, make a backup of the Interstage certificate environment. For details on how to make a backup, refer to the Operator's Guide.

If you do not make a backup, you need to recreate the Interstage certificate environment and import the PKCS#12 data, if the Interstage certificate environment is damaged.

#### Registering the CA Certificate

When a Certification Authority certificate is delivered separately from PKCS#12 data, first register the Certification Authority.

An example of registration is shown below.

Windows32/64

```
scsenter -n CA -f C:\my_folder\CA.der
```

Solaris32/64 Linux32/64

```
scsenter -n CA -f /usr/home/my_dir/CA.der
```

The CA certificate can be referenced by selecting [System] > [Security] > [Certificates] > [CA certificates] from the Interstage Management Console.

#### Note

- The CORBA Service requires all CORBA servers and clients that use SSL to register certificates from the same CA. Refer to the "How to Use SSL with the CORBA Service" chapter for information on how to register a certificate with the CORBA Service client package.
- All server and client systems that link to each other through communication using the Web service security function must register certificates of the same CA.

## Importing the PKCS#12 data

Import the site certificate and private key delivered using PKCS#12 data into the Interstage certificate environment.

An example of registration is shown below.

Windows32/64

```
scsimpfx -f C:\my_folder\MyCert.p12
```

Solaris32/64 Linux32/64

```
scsimpfx -f /usr/home/my_dir/MyCert.p12
```

The site certificate can be referenced by selecting [System] > [Security] > [Certificates] > [Site certificates] from the Interstage Management Console. Examine the validity period of the certificate to confirm the date when the certificate needs to be updated. Refer to "[Updating a Certificate \(Before Expiration\)](#)" for details..

## Registering the Certificate of Another Reliable Site

Register the certificate of another reliable site.

An example of registration is shown below.

Windows32/64

```
scsenter -n OtherSiteCert -f C:\my_folder\OtherSiteCert.der -e
```

Solaris32/64 Linux32/64

```
scsenter -n OtherSiteCert -f /usr/home/my_dir/OtherSiteCert.der -e
```

The certificate of another reliable site can be referenced by selecting [System] > [Security] > [Certificates] > [CA certificates] from the Interstage Management Console.

## Registering a CRL

There is no need to register the CRL unless it is used for revocation checks. If it is used for revocation checks, obtain and register the latest CRL regularly.

An example of registration is shown below.

Windows32/64

```
scsenter -c -f C:\my_folder\CRL.der
```

```
scsenter -c -f /usr/home/my_dir/CRL.der
```

**Note**

The Web Service client and Servlet Service (container) do not reference CRL to check for revocation.

## 9.5 Configuring Certificate Settings

---

After configuring the Interstage certificate environment, you need to make the settings for users of the certificate. This section describes how to do this.

1. [Defining the Use of Certificates](#)
2. [Setting Up Various Service Environments](#)

### 9.5.1 Defining the Use of Certificates

---

The certificates registered in the Interstage Certificate Environment can be referenced by selecting [System] > [Security] > [Certificates] > [CA certificates], or [System] > [Security] > [Certificates] > [Site certificates] from the Interstage Management Console.

Check whether the contents of the obtained certificates are correct. Also, examine the validity period of the certificate to confirm the date when the certificate needs to be updated. Refer to "[Updating a Certificate \(Before Expiration\)](#)" for details.

If SSL communication is to be used, an SSL definition must be created. Create an SSL definition by selecting [System] > [Security] > [SSL] > [Create a new SSL Configuration] tab from the Interstage Management Console.

Each certificate has a term of validity. Check this because system operation and functions may be stopped if the validity term of a certificate expires. It is necessary to obtain a new certificate before expiration. Refer to "[9.6 Certificate Management](#)" for more information.

### 9.5.2 Setting Up Various Service Environments

---

Environment setup (via the Interstage Management Console) is required for each service using SSL.

The option of Interstage Management Console window used for setting each service environment is shown below.

- Interstage HTTP Server

[System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Settings] tab > [Detailed Settings [Show]] > [SSL Settings].

To use SSL on the Virtual Host, you need to set up SSL on the following screens:

- When you create a new virtual host

[System] > [Services] > [Web Server] > [Web Server Name] > [Virtual Hosts] > [Create a new Virtual Host] tab > [Detailed Settings [Show]] > [SSL Settings].

- When you update the virtual host configuration setting

[System] > [Services] > [Web Server] > [Web Server Name] > [Virtual Hosts] > [(Virtual Host name)] > [Detailed Settings [Show]] > [SSL Settings].

- CORBA Service

[System] > [Environment setup] tab > [Detail setting] > [CORBA service detail setting] window.

To use SSL on a CORBA WorkUnit, you need to set up SSL on the CORBA WorkUnit setup screen. Access this screen as follows:

[System] > [WorkUnit] > [Select WorkUnit Name] > [Deploy] tab > [Detailed Settings [View]] > [Add SSL Info to Object Reference]

- Servlet Service

Refer to "Environment Setup for Servlet Service" in the "How to Use SSL with J2EE" chapter for environment setup details.

- Interstage JMS (\*1)

[System] > [Services] > [JMS] > [EventChannels] > [Create a New Configuration] tab > [Detail Setting [Show]] > [SSL Encryption].

- Interstage Directory Service

For the details of the environment setting, refer to the "Using SSL for Interstage Directory Service" chapter.

- Event Service

[System] > [Services] > [Event Service] > [EventChannels] > [Create a New Configuration] tab > [Detailed Settings [View]] > [SSL Encryption]

Note: To use SSL in Event Service, you need to set up the SSL environment for the CORBA Service.

\*1 If the Interstage JMS uses SSL, a CORBA Service SSL environment must be set up.

Refer to the Operator's Guide for information on starting the Interstage Management Console.

## 9.6 Certificate Management

After system operation begins, certificates, private keys, and CRLs must be correctly managed.

The commands shown in the following table are provided for certificate management:

Table 9.1 Certificate Management Commands

Command	Function
<i>scsmakeenv</i>	Configures or modifies the Interstage certificate environment. In addition, you can create a CSR or test certificate using this command
<i>scscenter</i>	Registers a certificate or CRL in the Interstage Certificate Environment
<i>scslistcrl</i>	Displays an overview of the CRL registered in the Interstage Certificate Environment
<i>scsdelete</i>	Deletes the site certificate with the corresponding private key, or the CA certificate from the Interstage Certificate Environment  Note: Performing a deletion may cause the system operation or restoration to be disturbed in some cases. Read through the section "Deleting a Certificate" described later and carefully make a deletion using this command.
<i>scsexppfx</i>	Exports (extracts) PKCS#12 data from the Interstage certificate environment
<i>scsimppfx</i>	Imports (registers) PKCS#12 data to the Interstage certificate environment
<i>scslist</i>	Lists the CSRs (Certificate Signing Requests) not associated with a site certificate and site and CA certificates registered in the Interstage certificate environment.

These commands can be used in the situations shown below.

For command syntax and usage details, refer to the Reference Manual (Command Edition).

### Note

To use the registered certificates, settings must be changed and applied using the Interstage Management Console.

### Updating a Certificate (Before Expiration)

If a certificate expires, operation and function may be stopped. Before expiration, a new certificate must be obtained and registered.

After a new certificate is obtained, the current certificate is usually switched to the new one. In this case, do not delete the old certificate; leave it as is.

To switch the certificate, repeat the procedure described in "9.2 Configuring Environments". At this time, the nickname used for the old certificate cannot be specified.

### Note

When the certificate is updated, the CSR will be created using the *scsmakeenv* command, however it will not be possible to specify the same nickname as the old certificate.

Depending on the operation policy of the CA, the CA certificate or intermediate CA certificate may be updated before the validity period of the certificate expires. In this case, check the site of each CA and obtain the new CA Certificate or intermediate CA certificate according

to the indicated procedure. After the CA Certificate or intermediate CA certificate has been registered using the `scscenter` command, register the new site certificate. At this time, any nickname that is not the same as the nickname of a certificate that has already been registered can be specified for the new CA certificate or intermediate CA certificate.

### **If a New Certificate and CRL are Obtained**

If a new certificate is issued or a new CRL is obtained due to an increase in certificate usage after system operation begins, use the `scscenter` command to register the certificate or CRL in the Interstage Certificate Environment.

### **Verifying Operation using a Test Site Certificate before System Operation Begins**

Before system operation begins or during application for a certificate, a test site certificate can be used to configure a system and verify operation.

Use the `scsmakeenv` command to create a test site certificate. The test site certificate is automatically registered in the Interstage Certificate Environment. There is no need to use the `scscenter` command to register the certificate.

#### **Note**

The test site certificate can be used for the following:

- Server authentication with Interstage HTTP Server
- CORBA Service with the client and server running on the same machine
- Interstage Directory Service using SSL on Replication Connection Settings in master of replication mode.

This certificate is for testing. Do not use it for actual operation.

To avoid a test certificate being mistakenly used for actual operation, it is recommended that the test certificate be deleted when testing is complete. It is also recommended that CA test certificates are similarly deleted.

### **Using the VeriSign Inc. Secure Site SSL Test Certificate**

Test CA Root is not included in the VeriSign Inc. root certificates registered using the `scsmakeenv` command. To use Secure Site SSL Test Certificate, obtain Test CA Root from VeriSign Inc. and then register it using the `scscenter` command. If Test CA Root is not registered, certificate verification fails, causing registration of Secure Site SSL Test Certificate to fail.

Since this a test certificate, do not use it for actual operation.

To avoid a test certificate being mistakenly used for actual operation, it is recommended that the test certificate be deleted when testing is complete. It is also recommended that CA test certificates similarly are deleted.

### **Deleting a Certificate**

A certificate that is no longer in use can be deleted.

Note that deleting a site certificate also deletes the corresponding private key. Losing a private-key permanently disables registration of the corresponding site certificate. If the CA certificate is deleted, the CA certificate and site certificate issued by the CA can no longer be used.

Use the `scsdelete` command carefully when deleting certificates.

Retaining certificates that have expired and can no longer be used does not cause any problems.

### **Making a PKCS#12 Data Backup and Restoring from this Backup**

You can make a PKCS#12 data backup of a site certificate, private key corresponding to it, and Certification Authority certificates required for verification of the site certificate. To do this, use the `scsexppfx` command. The PKCS#12 data backup made is password-encrypted to ensure the security of the private key.

You can restore from the PKCS#12 data backup using the `scsimppfx` command. In addition, you can use the `scsimppfx` command to transfer the backup data.

However, PKCS#12 data cannot include other reliable site certificates. For information on how to make a backup of the entire Interstage certificate environment, refer to the Operator's Guide.

# Chapter 10 Setting and Use of the Certificate/Key Management Environment Using the SMEE Command

This chapter describes the requirements for SSL communication and the required settings. It describes where to use a certificate/key management environment using the SMEE commands.

To use a certificate/key management environment, the following components must be installed.

## Solaris32

FJSVsmee, FJSVsclr, and FSUNssl packages

## Solaris64

FJSVsmee64 and FJSVsclr64 packages

## Linux32

FJSVsmee and FJSVsclr packages

## Linux64

FJSVsmee64 and FJSVsclr64 packages

You can configure and use a certificate/key management environment for each of the following services:

- Interstage HTTP Server
- CORBA Service
- Servlet Service
- Interstage JMS

Note: To use SSL with Interstage JMS, use the environment configured for the CORBA service.

- Event Service

Note: To use SSL with Event Service, use the environment configured for the CORBA service.

- Interstage Directory Service
- Interstage Single Sign-on

Note: To use SSL with Interstage Single Sign-on repository server and authentication server, use the environment configured for the Interstage HTTP Server.

To use services other than those mentioned above, refer to Part IV, Authentication and Encrypted Communications through Support for SSL, and read the related chapters.

## 10.1 SSL Libraries Used with the Certificate/Key Management Environment

---

This section explains the following topics:

- [10.1.1 Types of SMEE Libraries](#)
- [10.1.2 Certificate/Key Management Environment](#)
- [10.2 Environment Setting for Certificate/Key Management Environment](#)
- [10.3 Operating the Client Certificate](#)
- [10.4 Resource Registration](#)
- [10.5 Management of a Certificate/Key Management Environment](#)

## 10.1.1 Types of SMEE Libraries

---

With this version of Interstage Application Server, the following SSL libraries can be used (commands used for creating the environment vary according to the SMEE library to be used):

- SMEE3: SSL library of SMEE 3.x or later
  - Included in Interstage Application Server 4.0 or later.
  - UTF-8 certificates can be used.
  - To create and set up the key management environment, the *makeslot* and *maketoken* commands are used.
- SMEE2: SSL library of SMEE 2.2.x or earlier Windows32
  - Included in Interstage 1.0 and later, but not used in this version.
  - UTF-8 certificates cannot be used.
  - Unlike SMEE3, with SMEE2, the *mkslt* and *mktkn* commands are used to create and set up the key management environment.
  - Environments created using SMEE2 can be used with SMEE3. Refer to "[10.4 Resource Registration](#)" for information on how to migrate from an SMEE2 to a SMEE3 environment.

In this manual, the above libraries are referred to as SMEE2 and SMEE3.

## 10.1.2 Certificate/Key Management Environment

---

The following explains the certificate/key management environment, which is the operation environment when SSL (Secure Socket Layer) is used.

### Certificate and Private Key

To use SSL, the CA (Certification Authority) certificate, site certificate, and corresponding private key are required. A certificate revocation list (CRL) is also used to check the validity of a certificate.

A certificate and CRL that conform to X.509 or RFC2459 and that use an RSA key can be used.

- CA certificate

Certificate of the CA itself.

A CA may issue a certificate to a subordinate CA, in which case the certificate of the CA itself and the certificate issued to the subordinate CA are both referred to as a CA certificate. The certificate issued to the subordinate CA is specifically referred to as an intermediate CA certificate. A CA certificate that is issued by the CA to itself is also referred to as a root CA certificate.

- Site certificate

Certificate issued by the CA to certify the identity of a server or client.

This certificate contains information about the user (server, client, or service) and the CA and must always be used together with the certificate of the issuing CA.

Certificates are assigned a validity period. Certificates can not longer be used after their validity period ends. It is necessary to update the key pair and obtain a new certificate before the validity period ends. Refer to "[Updating a Certificate \(Before Expiration\)](#)" for details.

- Private key corresponding to a site certificate

This key is paired with a public key included in the site certificate.

#### Note

Losing a private key makes the site certificate that it corresponds to unusable. Be sure to make a back up of each private key.

- Certificate revocation list (CRL)

The CA issues the CRL. The CRL contains a list of certificates revoked by the CA. Reasons a certificate may be revoked include theft of the private key; loss of user qualifications; and so on.

If the CRL is used with SSL communication, the validity of the certificate of the connected site or client is checked against it.

The CRL is issued regularly. It is often made public on Web servers and directory servers managed by the CA. The method used to publish the CRL depends on the method defined in the CA policy. Check the CA's policy information for details. The location to which the CRL should be published is sometimes included in the certificate.

PKCS#12 data may be used to deliver certificates and private keys or make a backup. PKCS#12 data includes a certificate, a private key corresponding to it, and a Certification Authority certificate, all of which are password-encrypted.

In the Certificate/Key Management Environment, you can import (register) the following types of PKCS#12 data:

- PKCS#12 data exported (extracted) with the *scsexpfx* command from the Interstage certificate environment
- PKCS#12 data exported with the *cmmkpfx* command from a certificate/key management environment created with the SMEE command

In addition, you can import PKCS#12 data exported from the Certificate/Key Management Environment into the following environments:

- Interstage certificate environment (by means of the *scsimpfx* command)
- Certificate/key management environment created with the SMEE command (by means of the *cmentpfx* command)

## CA (Certification Authority)

The CA is required to create a certificate.

The Certificate/Key Management Environment supports certificates and CRLs issued by the following CAs:

- "Secure Site SSL Certificates" certificates issued by the VeriSign Inc.
- "Secure Site with EV SSL Certificates" certificates and CRL issued by the VeriSign Inc.
- "Cybertrust SureServer Certificate" and CRL issued by the Cybertrust, Inc.

### Note

Certificates issued by CAs (certification authorities) other than those listed above are considered to be granted if they satisfy the following:

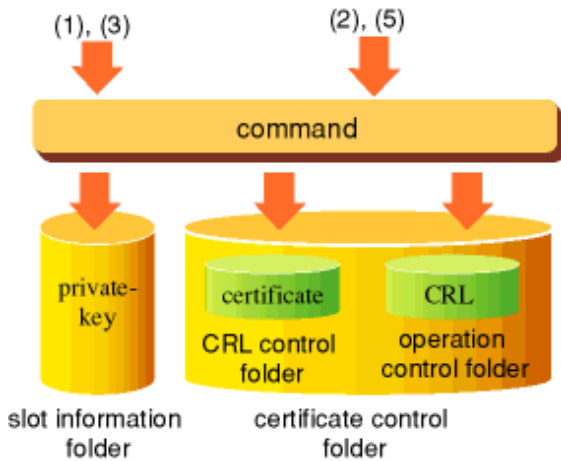
- They comply with X.509 or RFC2459
- They use the RSA key and their key length is not more than 4,096 bits
- They use the following hash algorithm
  - MD5
  - SHA-1
  - SHA-256
  - SHA-384
  - SHA-512

However, the operations of such certificates with the Interstage Application Server as well as the acquisition process for them have not been assured. This means that they are not in the scope of official support.

## Scheme of the Certificate/Key Management Environment

The certificate/key management environment is configured as shown in the following figure.





**Certificate/Key Management Environment Configuration**

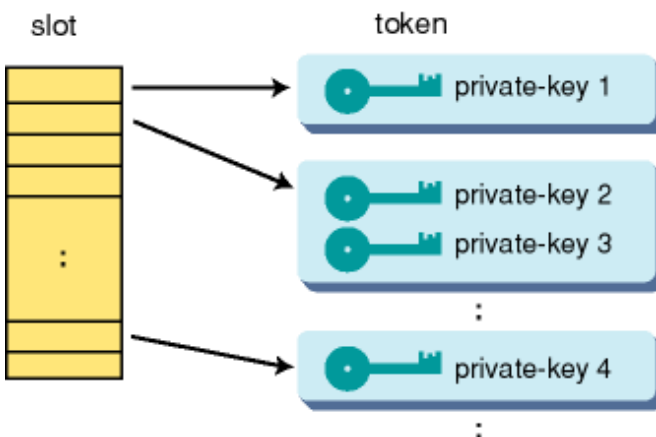
**Managing the Private Key**

In key management, private keys are handled using the concept of slot and token.

The slot is an abstraction of a physical slot in which an encryption device is installed. The token is an abstraction of a physical encryption device, to be installed in the slot.

One token is allocated to one slot, but multiple private keys can be registered in one token.

The following figure shows the relationships between slot, token, and private key.



**Relationship between Slot, Token and Private Key**

The slot password is needed for operations processing slot information, and the SO-PIN or user PIN is needed for operations processing token information. These passwords and PINs are set when the slot is generated or when the token is generated, respectively. The SO-PIN is set and is not used in normal operation.

The user PIN refers to the information required when accessing the private key in the token (when generating a private key using the *cmmakecsr* command or registering a private key using the *cmenterkey* command). Because a user PIN exists for each token, multiple pieces of private key information can be accessed with one user PIN if multiple private keys are registered in one token.

The following table lists the relationships between password and PIN with respect to slot and token.

Table 10.1 Relationships between Password and PIN

Type	Number of pieces	Major applications
Slot-password	1 for a slot	Generating a token
SO-PIN	1 for a token	-

Type	Number of pieces	Major applications
User PIN	1 for a token	Accessing a private key ( <i>cmmakecsr, cmenterkey</i> )

## 10.2 Environment Setting for Certificate/Key Management Environment

---

Set up the environment according to the following procedure:

1. Create a certificate/key management environment.
  - Create management directories.
  - Create and set up a key management environment.
  - Create a certificate/CRL management environment.
2. Create a private key and acquire a certificate.
  - Create a CSR (Certificate Signing Request) (create a private key at the same time.).
  - Make a request to issue a certificate.
  - Acquire a certificate.
3. Register the certificate and CRL.
  - Register the certificate of the CA.
  - Register the site certificate.
  - Register the CRL.

For details of each command used hereafter, refer to the "Reference Manual (Command Edition)".

The executable files for the SMEE commands are stored in the following directory:

To set up the SSL environment, use the following commands:

### Windows32/64

- Create and set up a key management environment command for SMEE3 (*makeslot, maketoken*):
  - Windows Server(R) x64 Edition  
Under %ProgramFiles%\SecurecryptoLibraryR64\Program\bin
  - Other than Windows(R) x64 Edition  
Under %ProgramFiles%\SecurecryptoLibraryR\Program\bin
- Others  
Under %CommonProgramFiles%\Fujitsu Shared\Fujitsu Shared\F3FSSMEE

### Solaris32 Linux32

- Create and set up a private key management environment command for SMEE3 (*makeslot, maketoken*):  
Under /opt/FJSVsclr/bin
- Others  
Under /opt/FJSVsme/bin

### Solaris64

- Create and set up a private key management environment command for SMEE3 (*makeslot, maketoken*):  
Under /opt/FJSVscl64/bin

- Others

Under /opt/FJVSme64/bin

**Linux64**

- Create and set up a private key management environment command for SMEE3 (*makeslot*, *maketoken*):

Under /opt/FJVSsclr64/bin

- Others

Under /opt/FJVSme64/bin

In the CORBA service, in order to execute with general user permission a CORBA application that uses the SSL linkage function, perform Steps 1 to 3 with the same user permission as the CORBA application user. If you set up an environment for certificate/key management using administrator permission, the environment will not be accessible with general user permission and this will prevent the SSL Link function from being used in the CORBA application.

If the certificate/key management environment is created with general user authority, the user who set up the environment has authority to access the environment and use the SSL linkage function. In this case, however, other general users do not have access authority for the environment. As a consequence, they cannot use SSL linkage.

To allow multiple general users to use the SSL linkage function, the certificate/key management environment access authority must be changed. Refer to "How to Use SSL with the CORBA Service" for details of access authority.

Note **Solaris32/64** **Linux32/64**

When you perform client attestation in Interstage HTTP Server, users other than super user authority need to operate Procedure 1 to 3 (since it is necessary to set up the process of a Web server by consideration on security except super user authority).

Moreover, this user and a group are set as the environmental definition file of Interstage HTTP Server. Refer to Environment Setting of the Interstage HTTP Server regarding environment setup of Interstage HTTP Server.

## 10.2.1 Creating a Certificate/Key Management Environment

Create a certificate/key management environment, which is the operation environment when using SSL.

### Creating Management Directories

Four directories are required for the certificate/key management environment. Create the four directories using the commands provided by the operating system.

Example

**Windows32/64**

```
mkdir d:\sslenv\slot          # Slot information directory
mkdir d:\sslenv\sslcert      # Operation management directory
mkdir d:\sslenv\sslcert\cert  # Certificate management directory
mkdir d:\sslenv\sslcert\crl   # CRL management directory
```

**Solaris32/64** **Linux32/64**

```
mkdir /export/home/slot      # Slot information directory
mkdir /export/home/sslcert   # Operation management directory
mkdir /export/home/sslcert/cert # Certificate management directory
mkdir /export/home/sslcert/crl # CRL management directory
```

### Creating and Setting Up a Key Management Environment

Create and set up the key management environment that is required for managing the private keys.

Example

**Windows32/64**

```
makeslot -d d:\sslnewenv\slot
maketoken -d d:\sslnewenv\slot -s 1 -t Token01
```

**Solaris32/64** **Linux32/64**

```
makeslot -d /export/home/slot
maketoken -d /export/home/slot -s 1 -t Token01
```

## Creating a Certificate Management Environment

Create and set up the certificate management environment required for managing certificates and CRL.

To use certificates of the CA supported in this product, register the root certificate (CA certificate) using the *cmsetenv* command.

### Example

**Windows32/64**

```
cmmkenv d:\sslenv\sslcert -todir d:\sslenv\sslcert\cert,d:\sslenv\sslcert\crl
cmsetenv d:\sslenv\sslcert -sd d:\sslenv\slot -jc 0 -rc C:\INTERSTAGE\IS_cert\contractcertlist
```

**Solaris32/64** **Linux32/64**

```
cmmkenv /export/home/sslcert -todir /export/home/sslcert/cert, /export/home/sslcert/crl
cmsetenv /export/home/sslcert -sd /export/home/slot -jc 0 -rc /etc/opt/FJSVisas/contractcertlist
```

### Note

Specify an installation certificate list file using the following path:

- For using Interstage HTTP server  
/etc/opt/FJSVihs/conf/contractcertlist

After completing the creation of the Certificate/key management environment, not all of the Certificate/key management environment directory names can be changed.

## 10.2.2 Creating a Private Key and Acquiring a Certificate

Make a request to issue a certificate to the CA and acquire it.

### Creating a CSR (At the Same Time Creating a Private Key)

Create a CSR to request the CA to issue a certificate.

Executing the following commands creates a private key at the same time.

### Note

To secure the private key, keep a backup of the certificate/key management environment file until the certificate is obtained.

If the certificate/key management environment is damaged without a backup, the private key will be lost and it will be necessary to create the certificate/key management environment and CSR again.

### Example

**Windows32/64**

```
cmmakecsr -ed d:\sslenv\sslcert -sd d:\sslenv\slot -f TEXT -c jp -cn
www.InterstageApplicationServer.com -o fujitsu -ou 4-1f -l "Shizuoka-shi" -s "Shizuoka-ken"
-kt RSA -kb 2048 -tl Token01 -of d:\sslenv\myCertRequest
ENTER TOKEN PASSWORD=> *1
```

**Solaris32/64** **Linux32/64**

```
cmmakecsr -ed /export/home/sslcert -sd /export/home/slot -f TEXT -c jp -cn
www.InterstageApplicationServer.com -o fujitsu -ou 4-1f -l "Shizuoka-shi" -s "Shizuoka-ken"
```

```
-kt RSA -kb 2048 -tl Token01 -of /export/home/myCertRequest
ENTER TOKEN PASSWORD=> *1
```

\*1 When these character strings appear on the screen, enter the user PIN. The entered characters are not echoed back.

## Making a Request to Issue a Certificate

Send a CSR to the CA to request the issuing of a site certificate.

How to make the request depends on the CA.

## Acquiring a Certificate

Acquire a certificate signed by the CA.

How to acquire a certificate depends on the CA.

## 10.2.3 Registering the Certificate and CRL

---

Register the obtained certificate and CRL in the certificate management environment.

After registering the certificate and CRL, make a backup of the certificate/key management environment. For details on how to make a backup, see the description of making a backup of data related to each service in Operator's Guide or "Resource Registration", "1.Search for Existing Resources (Private Key and Certificates)."

### Registering the CA Certificate

Register the acquired certificate of the CA in the certificate management environment.

Register all certificates issued by the CA that is used for the operation (site certificates and client certificates). Register the certificates of the CA supported in this product using the *cmsetenv* command.

Register the certificates starting with the root certificate.

Example

**Windows32/64**

The example below assumes the CA certificate is contained in d:\sslenv\ca-cert.der file.

```
cmcert d:\sslenv\ca-cert.der -ed d:\sslenv\sslcert -ca -nn CACert
```

**Solaris32/64** **Linux32/64**

The example below assumes the CA certificate is contained in /export/home/ca-cert.der file.

```
# cmcert /export/home/ca-cert.der -ed /export/home/sslcert -ca -nn CACert
```

Note

It is necessary to register the same issue office certificate with the CORBA Service by all the CORBA servers and CORBA clients that use SSL:

### Registering the Intermediate CA Certificate

Depending on the CA, an intermediate CA certificate may be provided in addition to the CA certificate and site certificate. Check with the CA to establish if an intermediate CA certificate will be provided. Register the intermediate CA certificate, if one is provided, before registering the site certificate.

The registration method is the same as for the CA certificate. For details, refer to "Registering the CA Certificate" above.

### Registering the Site Certificate

Register the site certificate issued by a CA in the certificate management environment.

Following registration, check the validity period of the certificate to determine when that certificate must be updated. The validity period can be checked using the *cmdspcert* command. Refer to the Reference Manual (Command Edition) for details on this command. Certificate update is explained in "[Updating a Certificate \(Before Expiration\)](#)".

## Example

**Windows32/64**

The example below assumes the site certificate is contained in d:\sslenv\my\_site\_cert.der file.

```
cmentcert d:\sslenv\my_site_cert.der -ed d:\sslenv\sslcert -own -nn MySiteCert
```

**Solaris32/64** **Linux32/64**

The example below assumes the site certificate is contained in /export/home/my\_site\_cert.der file.

```
# cmentcert /export/home/my_site_cert.der -ed /export/home/sslcert -own -nn  
MySiteCert
```

## Note

For the CORBA service, if you do not authenticate clients, you do not have to register site certificates on CORBA clients.

## Registering the CRL

There is no need to register the CRL unless it is used for revocation checks. If it is used for revocation checks, obtain and register the latest CRL regularly.

## Example

**Windows32/64**

The example below assumes the CRL is contained in d:\sslenv\crl.der file.

```
cmentcrl d:\sslenv\crl.der -ed d:\sslenv\sslcert
```

**Solaris32/64** **Linux32/64**

The example below assumes the CRL is contained in /entdir/crl.der file.

```
# cmentcrl /entdir/crl.der -ed /export/home/sslcert
```

## 10.3 Operating the Client Certificate

---

To perform client authentication using SSL version 3.0, the web browser needs the client certificate.

It is also required that the CA certificate that issued the client certificate be registered in the certificate/key management environment.

To perform client authentication, specify as follows in the SSL environment definition file:

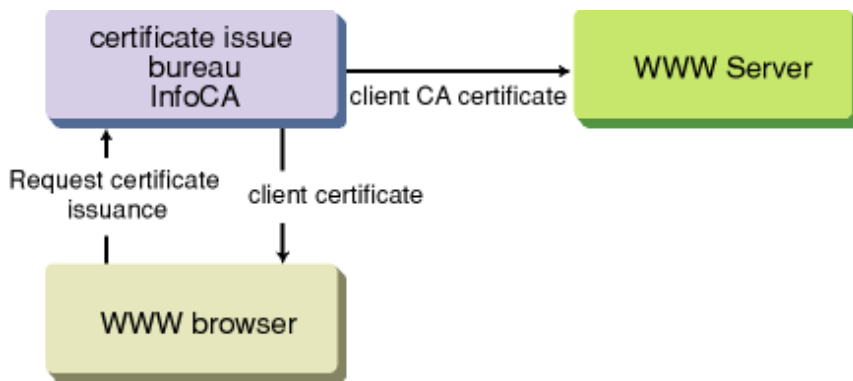
- Specify "3" or "2 3" for the SSL version (version).
- Specify "ON" for the verification method (clicertcheck) of the client certificate.

### 10.3.1 Obtaining the Client Certificate

---

To obtain a client certificate, ask the Certification Authority to issue the certificate.

Contact the relevant CA about the issue of the client certificate of the CA supported in this product., refer to the companies listed in the following figure.



### Issuance of Client Certificates

## 10.3.2 Registering the Client Certificate

Register the root certificate (CA certificate) of the CA supported in this product at the time of the certificate/CRL management environment setup.

Example

**Windows32/64**

```
cmsetenv d:\sslenv\sslcert -sd d:\sslenv\slot -jc 0 -rc
C:\INTERSTAGE\IS_cert\contractcertlist
```

**Solaris32/64** **Linux32/64**

```
cmsetenv /export/home/sslcert -sd /export/home/slot -jc 0 -rc
etc/opt/FJSVisas\contractcertlist
```

For command details, refer to the Reference Manual (Command Edition).

## 10.4 Resource Registration

When changing the SSL library to be used from SMEE2 to SMEE3, the existing certificate/key management environment can be used as it is.

However, to use the UTF-8 certificate, migration of the certificate/key management environment is required.

For the migration of the certificate/key management environment, create pfx data from existing resources and then register the pfx data in the new environment.

The following shows the procedure for migration:

1. Search for existing resources (private key and certificates).
2. Create a certificate/key management environment.
3. Register resources searched for in 1 in the environment created in 2.
4. Register the user PIN.

For command details, refer to the Reference Manual (Command Edition).

### 1. Search for Existing Resources (Private Key and Certificates).

Use the pfx data creation command to search for resources.

Example

**Windows32/64**

```
cmmkpfx d:\sslenv\my_site_pfx.pfx -ed d:\sslenv\sslcert -sn 1 -nn MySiteCert
```

## Solaris32/64

```
# cmmkpx /entdir/my_site_pfx.pfx -ed /export/home/sslcert -sn 1 -nn MySiteCert
```

Client CA certificates and CRL cannot be searched for by the pfx data creation command.

If a client CA certificate or CRL is needed, re-register using the ordinary method.

When creating the pfx data, specify the nickname of the "Site certificate". The pfx data creation command reads out the site certification, its private key, the Certification Authority of the site certificate (a complete setup to the root CA certificate), and creates the pfx data.

## 2. Create a Certificate/Key Management Environment.

Create a certificate/key management environment.

For details, refer to "10.2.1 Creating a Certificate/Key Management Environment".

## 3. Register Resources Searched For in 1. In the Environment Created in 2.

Use the pfx data registration command to register resources.

Example

## Windows32/64

The example below assumes the newly created Certificate/Key Management Environment is d:\sslnewenv\sslcert.

```
cmentpfx d:\sslenv\my_site_pfx.pfx -ed d:\sslnewenv\sslcert -sn 1 -nn  
MyNewSiteCert -entca
```

## Solaris32/64

The example below assumes the newly created Certificate/Key Management Environment is d:\sslnewenv\sslcert.

```
# cmentpfx /entdir/my_site_pfx.pfx -ed /export/home/new/sslcert -sn 1 -nn  
MyNewSiteCert -entca
```

When registering the pfx data, specify "-entca" because the CA certificate is contained in the pfx data. By doing this, the site certification, its private key, the Certification Authority of the site certificate (a complete set up to the root CA certificate) can be registered at the same time.

## 4. Register the User PIN.

Register the user PIN in the user PIN management file.

# 10.5 Management of a Certificate/Key Management Environment

Because each user certificate has an expiry date, re-acquisition and re-registration of certificates are needed.

The commands shown in the following table are therefore provided for managing certificates:

Table 10.2 Commands for Managing Certificates

Command	Description
cmlistcert	Displays a list of certificates registered with the certificate/key management environment.
cmdspcert	Displays contents of the specified certificate.
cmlistcrl	Displays a list of CRLs registered with the certificate/key management environment.
cmmrcert	Deletes certificates registered with the certificate/key management environment.

For information about the commands, refer to the Reference Manual (Command Edition).

## Updating a Certificate (Before Expiration)

If a certificate expires, operation and function may be stopped. Before expiration, a new certificate must be obtained and registered.



After a new certificate is obtained, the current certificate is usually switched to the new one. In this case, do not delete the old certificate; leave it as is.

To switch the certificate, repeat the procedure described in "[10.2.2 Creating a Private Key and Acquiring a Certificate](#)". At this time, the nickname used for the old certificate cannot be specified.

Depending on the operation policy of the CA, the CA certificate may be updated before the validity period of the certificate expires. In this case, check the site of each CA and obtain the new CA Certificate or intermediate CA certificate according to the indicated procedure. After the CA Certificate or intermediate CA certificate has been registered using the `-ca` option of the `cmntcert` command, register the new site certificate. At this time, any nickname that is not the same as the nickname of a certificate that has already been registered can be specified for the new CA certificate or intermediate CA certificate.

### **Using the VeriSign Inc. Secure Site SSL Test Certificate**

The VeriSign, Inc. root certificates that are registered using the `cmsetenv` command do not include "Secure Site SSL Test Certificate" root certificates. Therefore, to register a "Secure Site SSL Test Certificate", obtain a "Secure Site SSL Test Certificate" root certificate and the required intermediate CA certificate from VeriSign, Inc., then register them using the `cmntcert` command.

At this time, register the "Secure Site SSL Test Certificate" root certificate, required intermediate CA certificate, and "Secure Site SSL Test Certificate" in this order. If the "Secure Site SSL Test Certificate" root certificate and required intermediate CA certificate are not registered, the certificate verification will fail, therefore the registration of the "Secure Site SSL Test Certificate" will also fail.

Since this a test certificate, do not use it for actual operation.

To avoid a test certificate being mistakenly used for actual operation, it is recommended that the test certificate be deleted when testing is complete. It is also recommended that CA test certificates are similarly deleted.

# Chapter 11 How to Use SSL with Interstage HTTP Server

This chapter explains how to use the SSL for the Interstage HTTP Server.

The Interstage HTTP Server can use the following two environments for managing the certificates and private keys required for encryption and signature processing:

## SSL for Interstage Certificate Environments

To use Interstage Certificate Environment SSL communication, configure the environment settings shown below. For more information, refer to "[11.1 SSL for Interstage Certificate Environments](#)".

1. Create the Interstage Certificate environment
2. Set the Interstage HTTP Server environment.

## SSL for Certificate/Key Management Environments Configured with the SMEE Commands

To use SSL communication in the certificate/key management environment that is built using the SMEE command, configure the environment settings shown below. For more information, refer to "[11.2 SSL for Certificate/Key Management Environments Configured with the SMEE Commands](#)".

1. Create a certificate/key management environment.
2. Register the user PIN.
3. Set the Interstage HTTP Server environment.

## 11.1 SSL for Interstage Certificate Environments

This section explains the environment settings that are required in order to use Interstage Certificate Environment SSL communication.

1. Create the Interstage Certificate environment.
2. Set the Interstage HTTP Server environment.

### 11.1.1 Creating the Interstage Certificate Environment

Configure the Interstage certificate environment. Refer to the "Setting and Use of the Interstage Certificate Environment" chapter.

### 11.1.2 Setting the Interstage HTTP Server environment

Set an SSL environment of the Interstage HTTP Server using the Interstage management console.

SSL can be used to perform the following operations:

- Web server SSL definition

This is an SSL definition for the entire Web server.

- Virtual host SSL definitions

This is an SSL definition for each virtual host. Using this setting, communication that uses and does not use SSL can be operated at the same time.

The procedure used to configure the Interstage HTTP Server SSL environment using the Interstage Management Console is shown below.

#### Web Server SSL Definition

1. Start and then log in to the Interstage Management Console.
2. Use the following Interstage Management Console windows for these settings:

[System] > [Services] > [Web Server] > [Web Server name] > [Environment Settings] tab > [Detailed Settings] > [SSL]

- In [Enable SSL Encryption?], select "Yes".

- In [SSL Configuration], select the name of the SSL definition that will be used.

## Virtual Host SSL Definitions

1. Start and then log in to the Interstage Management Console.
2. Use the following Interstage Management Console windows for these settings:

To create a new virtual host:

[System] > [Services] > [Web Server] > [Web Server name] > [Virtual Hosts] > [Create a new Virtual Host] > [Detailed Settings] > [SSL]

- In [Enable SSL Encryption?], select "Yes".
- In [SSL Configuration], select the name of the SSL definition that will be used.

To configure the virtual host environment settings:

[System] > [Services] > [Web Server] > [Web Server name] > [Virtual Hosts] > [Virtual Host name] > [Detailed Settings] > [SSL]

- In [Enable SSL Encryption?], select "Yes".
- In [SSL Configuration], select the name of the SSL definition that will be used.

## Notes

The Site Certificate and CA Certificate both have a validity term, after which they will expire. If a Web server operation continues after this validity term has expired, the error message "ihs00504"/"ihs00505" is output and it will not be possible to perform Web server start/communication processing. Check the validity term of the certificate in the following Interstage Management Console windows and obtain and then register a new certificate before this validity term expires.

- [System] > [Security] > [Certificates] > [CA Certificate]
- [System] > [Security] > [Certificates] > [Site Certificate]

Note that, before the validity term of the Site Certificate and the CA Certificate expires, it is possible to specify that a warning message that notifies the number of days the certificate is still valid for ("ihs00536"/"ihs00537") be output at the required time.

An example of the Interstage HTTP Server environment definition file (httpd.conf) definitions is shown below.

Example: How to specify that the warning message ("ihs00536"/"ihs00537") that notifies the number of days the Site Certificate and CA Certificate are still valid for be output at the following times:

- Whenever the Web server is started, in a period that starts from 15 days before the certificate expires until the expiry date
- At 9:30 10 days before the validity term of the certificate expires (While the Web server is running.)
- At 9:30 3 days before the validity term of the certificate expires (While the Web server is running.)
- At 9:30 1 day before the validity term of the certificate expires (While the Web server is running.)

```
SSLCertExpire All 15 10,3,1:093000
```

## Relating Directives

- SSLCertExpire

# 11.2 SSL for Certificate/Key Management Environments Configured with the SMEE Commands

This section explains the environment settings that are required in order to use SSL communication in the certificate/key management environment that is built using the SMEE command.

1. Create a certificate/key management environment.
2. Register the user PIN.
3. Set the Interstage HTTP Server environment.

## 11.2.1 Creating the Certificate/Key Management Environments Configured with the SMEE Commands

---

Follow the procedure below to set an SSL environment:

1. Create a certificate/key management environment.

For details, refer to "Creating a Certificate/Key Management Environment" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter.

2. Create a secret key and acquire a certificate.

For details, refer to "Creating a Private Key and Acquiring a Certificate" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter.

3. Register the certificate and CRL.

For details, refer to "Registering the Certificate and CRL" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter.

4. Register the user PIN.

5. Set the Interstage HTTP Server environment definition file.

6. Register CA certificate on the Web browser.

For details, refer to "Operating the Client Certificate" in the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter.

Note

- **Solaris32/64** **Linux32/64**

When performing client authentication in the Solaris and Linux system, a user other than the super-user authority needs to execute Steps 1 to 3. (The user other than the super-user authority set the process of Web Server for consideration on security.)

In addition, specify the user or group in the Interstage HTTP Server environment definition file in step 5.

The following sections explain steps 4 and 5 for the Interstage HTTP Server.

## 11.2.2 Registering the User PIN

---

Register the user PIN in the user PIN management file.

By specifying the user PIN and user PIN management file in the *ihsregistupin* command, the user PIN is registered in the user PIN management file after encrypting it.

The following shows an example of registration.

Example **Windows32/64**

When the user PIN (dialog input) is encrypted and registered to the user PIN management file "d:\ssl\upinfile".

```
ihsregistupin -f d:\ssl\upinfile -d d:\sslenv\slot
```

Example **Solaris32/64** **Linux32/64**

When the user PIN (dialog input) is encrypted and registered to the user PIN management file "/home/ssl/upinfile".

```
ihsregistupin -f /home/ssl/upinfile -d /home/sslenv/slot
```

Note **Windows32/64**

We recommend changing the access privileges for the user PIN admin file:

1. Start Windows Explorer.
2. Right-click the user PIN admin file, then click [Properties].
3. In the [Properties] dialog box, click the [Security] tab.

4. Select "Deny" for [Allow Access] for all groups except SYSTEM and Administrators.

## 11.2.3 Setting the Interstage HTTP Server Environment

---

Make the SSL settings in the environment definition file (httpd.conf) of the Interstage HTTP Server.

SSL can be used to perform the following operations:

- Web server SSL definition

This is an SSL definition for the entire Web server. It is possible to configure SSL operations that use and do not use client authentication.

- Virtual host SSL definitions

This is an SSL definition for each virtual host. Using this setting, communication that uses and does not use SSL can be operated at the same time.

### Web Server SSL Definition

Example 

When operating SSL using the following settings:

- Port number "443"
- SSL protocol version "SSL3.0" OR "SSL3.1" (TLS 1.0)
- Verifies a client certificate.
- Slot information directory "d:\ssl\slotdir"
- Token label "secret\_key\_tok"
- User PIN file "d:\ssl\upinfile"
- Operation control directory "d:\ssl\envdir"
- Nickname of the site certificate "server\_cert"
- Nickname of the client CA certificate "client\_cert"

```
LoadModule ihs_ssl_module "C:/Interstage/F3FMIhs/modules/mod_ihs_ssl.so"

Listen 443
ServerAdmin webmaster@main.example.com
ServerName main.example.com

SSLExec          on
SSLVersion       3-3.1
SSLVerifyClient  require
SSLSlotDir       d:/ssl/slotdir
SSLTokenLabel    secret_key_tok
SSLUserPINFile   d:/ssl/upinfile
SSLEnvDir        d:/ssl/envdir
SSLCertName      server_cert
SSLClCACertName  client_cert
SSLCipherSuite   RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5:DES-CBC3-
MD5:RC4-MD5:RC2-MD5
```

Example  

When operating SSL using the following settings:

- Port number "443"
- SSL protocol version "SSL3.0" OR "SSL3.1" (TLS 1.0)
- Verifies a client certificate.

- Slot information directory "/home/ssl/slotdir"
- Token label "secret\_key\_tok"
- User PIN file "/home/ssl/upinfile"
- Operation control directory "/home/ssl/envdir"
- Nickname of the site certificate "server\_cert"
- Nickname of the client CA certificate "client\_cert"
- User of creating a certificate/key management environment "user1"
- Group of creating a certificate/key management environment "group1"

```

LoadModule ihs_ssl_module "/opt/FJSVihs/modules/mod_ihs_ssl.so"

Listen      443
ServerAdmin webmaster@main.example.com
ServerName  main.example.com

User user1
Group group1

SSLExec      on
SSLVersion   3-3.1
SSLVerifyClient require
SSLSlotDir   /home/ssl/slotdir
SSLTokenLabel secret_key_tok
SSLUserPINFile /home/ssl/upinfile
SSLEnvDir    /home/ssl/envdir
SSLCertName  server_cert
SSLClCACertName client_cert
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5:DES-CBC3-MD5:RC4-MD5:RC2-MD5

```

## Virtual Host SSL Definitions

Example [Windows32/64](#)

When operating SSL using the following settings:

- Virtual host not using SSL:  
Port number "80", Root directory open to the public "C:\www\public"
- Virtual host using SSL (without client authentication):  
Port number "443", Root directory open to the public "C:\www\secure1"
- Virtual host using SSL (with client authentication):  
Port number "8443", Root directory open to the public "C:\www\secure2"

```

LoadModule ihs_ssl_module "C:/Interstage/F3FMihs/modules/mod_ihs_ssl.so"

Listen 80
Listen 443
Listen 8443

SSLSlotDir    d:/ssl/slotdir
SSLTokenLabel secret_key_tok
SSLUserPINFile d:/ssl/upinfile

<VirtualHost 192.168.0.1:80>
  ServerName  main.example.com
  DocumentRoot C:/www/public

```

```

</VirtualHost>

<VirtualHost 192.168.0.1:443>
  ServerName      main.example.com
  DocumentRoot    C:/www/secure1
  SSLExec         on
  SSLVersion      2
  SSLEnvDir       d:/ssl/envdir
  SSLCertName     cert_for_purchase
  CustomLog       "|ihsrlog.exe -s logs/accesslog_secure1 1 5" ihs-analysis
  ErrorLog        "|ihsrlog.exe -s logs/errorlog_secure1 1 5"
</VirtualHost>

<VirtualHost 192.168.0.1:8443>
  ServerName      main.example.com
  DocumentRoot    C:/www/secure2
  SSLExec         on
  SSLVersion      3-3.1
  SSLVerifyClient require
  SSLEnvDir       d:/ssl/envdir
  SSLCertName     cert_for_manager
  SSLCACertName  CACert_InfoCA
  SSLCipherSuite  RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5:DES-CBC3-
MD5:RC4-MD5:RC2-MD5
  CustomLog       "|ihsrlog.exe -s logs/accesslog_secure2 1 5" ihs-analysis
  ErrorLog        "|ihsrlog.exe -s logs/errorlog_secure2 1 5"
</VirtualHost>

```

**Example** Solaris32/64 Linux32/64

When operating SSL using the following settings:

- Virtual host not using SSL:  
Port number "80", Root directory open to the public "/home/www/public"
- Virtual host using SSL (without client authentication):  
Port number "443", Root directory open to the public "/home/www/secure1"
- Virtual host using SSL (with client authentication):  
Port number "8443", Root directory open to the public "/home/www/secure2"
- User of creating a certificate/key management environment "user1"
- Group of creating a certificate/key management environment "group1"

```

LoadModule ihs_ssl_module "/opt/FJSVihs/modules/mod_ihs_ssl.so"

Listen 80
Listen 443
Listen 8443

User user1
Group group1

SSLSlotDir      /home/ssl/slotdir
SSLTokenLabel   secret_key_tok
SSLUserPINFile  /home/ssl/upinfile

<VirtualHost 192.168.0.1:80>
  ServerName      main.example.com
  DocumentRoot    /home/www/public
</VirtualHost>

<VirtualHost 192.168.0.1:443>

```

```

    ServerName      main.example.com
    DocumentRoot    /home/www/secure1
    SSLExec         on
    SSLVersion      2
    SSLEnvDir       /home/ssl/envdir
    SSLCertName     cert_for_purchase
    CustomLog       "|/opt/FJSVihs/bin/ihsrlog -s logs/accesslog_secure1 1 5" ihs-analysis
    ErrorLog        "|/opt/FJSVihs/bin/ihsrlog -s logs/errorlog_secure1 1 5"
</VirtualHost>

<VirtualHost 192.168.0.1:8443>
    ServerName      main.example.com
    DocumentRoot    /home/www/secure2
    SSLExec         on
    SSLVersion      3-3.1
    SSLVerifyClient require
    SSLEnvDir       /home/ssl/envdir
    SSLCertName     cert_for_manager
    SSLCACertName   CACert_InfoCA
    SSLCipherSuite  RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5:DES-CBC3-
MD5:RC4-MD5:RC2-MD5
    CustomLog       "|/opt/FJSVihs/bin/ihsrlog -s logs/accesslog_secure2 1 5" ihs-analysis
    ErrorLog        "|/opt/FJSVihs/bin/ihsrlog -s logs/errorlog_secure2 1 5"
</VirtualHost>

```

## Notes

The Site Certificate and CA Certificate both have a validity term, after which they will expire. If a Web server operation continues after this validity term has expired, the error message "ihs00504"/"ihs00505" is output and it is not possible to perform Web server start/communication processing. Check the validity term of the certificate using the `cmdspcert` command, and obtain and then register a new certificate before this validity term expires.

Note that, before the validity term of the Site Certificate and the CA Certificate expires, it is possible to specify that a warning message that notifies the number of days the certificate is still valid for ("ihs00536"/"ihs00537") be output at the required time.

An example of the Interstage HTTP Server environment definition file (`httpd.conf`) definitions is shown below.

Example: How to specify that the warning message ("ihs00536"/"ihs00537") that notifies the number of days the Site Certificate and CA Certificate are still valid for be output at the following times:

- Whenever the Web server is started, in a period that starts from 15 days before the certificate expires until the expiry date
- At 9:30 10 days before the validity term of the certificate expires (While the Web server is running)
- At 9:30 3 days before the validity term of the certificate expires (While the Web server is running)
- At 9:30 1 day before the validity term of the certificate expires (While the Web server is running)

```
SSLCertExpire All 15 10,3,1:093000
```

## Relating Directives

- CustomLog
- DocumentRoot
- ErrorLog
- Group
- Listen
- LoadModule
- ServerAdmin
- ServerName



- SSLCertExpire
- SSLCertName
- SSLCICACertName
- SSLCipherSuite
- SSLEnvDir
- SSLExec
- SSLSlotDir
- SSLTokenLabel
- SSLUserPINFile
- SSLVerifyClient
- SSLVersion
- User
- <VirtualHost>

## 11.3 Relating Directives

---

The following directives are related to the setup of the environment definition file needed to use SSL.

The description includes the following:

### Name

Directive name

### Synopsis

Directive format

### Description

Functional overview of the directive

### Context

Directive-set location indicated with one of the following keywords:

Global context

Setting used for action of the entire Web Server.

Virtual host

Setting which is available in the <VirtualHost> section and used for action of the virtual host.

Directory

Setting which is available in the <Directory>, <Location>, and <Files> sections and used for action in response to a request for a specified directory, URL, or file.

### Default value

Value assumed when the directive is omitted. If a directive indicated with "None" is omitted, the directive function is disabled.

### Initial value

Initial directive value

## Module

Name of the module that implements the directive function. A directive with no module name indication is included in the basic module.

## Note

Notes on the use of the directive

## Examples

Directive example (included only for a directive which requires complicated setting).

## 11.3.1 Alias

---

### Name

Alias

### Synopsis

Alias URL-path file-path|directory-path

### Description

Specifies a directory to be handled as a virtual directory. Documents provided can be stored in directories other than the directory specified with the DocumentRoot directive.

The URL path can consist of up to 224 alphanumeric characters or any of the following symbols:

+, -, ., /, \_.

The path must be unique. The same URL path as one specified in the ScriptAlias directive cannot be specified.

### Context

Global context, Virtual host

### Default value

none

### Module

mod\_alias

### Note

- If the name of the Servlet Service application Web application is "ROOT", this directive setting will be invalid.
- Servlet service applications cannot be specified in the URL path. If a Servlet Service application is specified in the URL path and this directive is set, the setting will be invalid.

**Solaris32/64** **Linux32/64**

- The mount point to the NFS server can be specified, as long as it is always accessible while the Web server is running. To guarantee that, before starting the Web server, make sure that the NFS server has started normally, and while the Web server is running, do not perform operations that make the NFS server inaccessible (such as powering off the NFS server).

## 11.3.2 CustomLog

---

### Name

CustomLog

## Synopsis

```
CustomLog "|ihsrlog-command-execution-statement"|log-file-name nickname [env=[!]environment-variable]
```

## Description

Creates access log files.

*ihsrlog-command-execution-statement*

Specifies the *ihsrlog* command execution statement.

*log-file-name*

Specifies the name of the file to which access log messages are to be output.

Specify the absolute path or the relative path from the ServerRoot directive to the log file. If the specified path does not begin with a slash "/", it is assumed to be the relative path from the ServerRoot directive. Specify the name of an already existing directory.

*nickname*

Specifies the nickname set in the LogFormat directive.

The initial value can be any of the following nicknames:

- common

Logs access in the Common Log Format.

- referer

Logs information about follow-up of the clients.

- agent

Logs information about the Web browsers used on the clients.

- combined

Logs all information obtained with the common, referer, and agent options.

- ihs-analysis

Logs information obtained using the Common nickname, and information about the request processing time and received requests.

env=[!]environment-variable

Specifies that an access log message be output if the specified environment variable is already set.

If "!" is specified at the beginning of the environment variable, no access log message is output when the specified environment variable is already set.

Use the SetEnvIf directive to specify the environment variable setting conditions.

## Context

Global context, Virtual host

## Default value

none

## Initial value

Windows32/64

```
CustomLog "|ihsrlog.exe -s logs/accesslog 1 5" ihs-analysis
```

Solaris32/64 Linux32/64

```
CustomLog "|/opt/FJJSVihs/bin/ihsrlog -s logs/accesslog 1 5" ihs-analysis
```

## Module

mod\_log\_config

## Note

- If this directive is set more than once, then all defined settings will be valid.
- If the [Update]/[Create] operation is performed in the following Interstage Management Console windows, "Directory where the log file is stored and Prefix for the log file name", which is set for the logfile executable statement of the `ihstrlog` command of this directive, will be enclosed in a backslash and double quotes (`\`). However, this has no impact whatsoever on operations.
  - [System] > [Services] > [Web Server] > [Web Server name] > [Environment Settings]
  - [System] > [Services] > [Web Server] > [Web Server name] > [Virtual Hosts] > [Virtual Host name] > [Detailed Settings]
  - [System] > [Services] > [Web Server] > [Web Server name] > [Virtual Hosts] > [Create a new Virtual Host]

**Solaris32/64** **Linux32/64**

- If the log file name is specified in this directive, error message `ihstr70009` is output when the file size set using the `ulimit` command (Bourne shell) or the `limit` command (C shell) is reached, and recording of the log fails.

**Solaris32/64**

- If this directive is added many times, there may be insufficient file descriptors, which are required in order to run the Web server. Refer to the Tuning Guide, and check whether there is a problem with the number of file descriptors.

## 11.3.3 DocumentRoot

---

### Name

DocumentRoot

### Synopsis

DocumentRoot directory-path

### Description

The directory that `httpd` provides the file is set.

Unless matched by a directive such as `Alias`, the server appends the path from the requested URL to the document root to generate the path for the document.

Be sure to set this directive.

### Context

Global context, Virtual host

### Default value

none

### Initial value

**Windows32/64**

```
DocumentRoot "C:/Interstage/F3FMihs/servers/(Web server name)/htdocs"
```

**Solaris32/64** **Linux32/64**

```
DocumentRoot "/opt/FJSVihs/servers/(Web server name)/htdocs"
```

## Note

- Do not put the slash (/) on the end of the directory specified for this directive.
- In the initial state, the sample content is stored in the directory that is specified in this directive. Depending on the Web server operation, either delete unnecessary sample content, or change the directory that is specified in this directive.

**Solaris32/64** **Linux32/64**

- The mount point to the NFS server can be specified, as long as it is always accessible while the Web server is running. To guarantee that, before starting the Web server, make sure that the NFS server has started normally, and while the Web server is running, do not perform operations that make the NFS server inaccessible (such as powering off the NFS server).

## Example

Accesses "/usr/web/index.html" when specifying "http://www.my.host.com/index.html" from a Web browser.

```
DocumentRoot "/usr/web"
```

## 11.3.4 ErrorLog

---

### Name

ErrorLog

### Synopsis

```
ErrorLog "ihsrlog-command-execution-statement"log-file-name
```

### Description

Creates error log files.

*ihsrlog* command execution statement

Specifies the *ihsrlog* command execution statement.

log-file-name

Specifies the name of the file to which error log messages are to be output. For the file name, specify the absolute path or the relative path from the ServerRoot directive. If the specified path does not begin with a slash "/", it is assumed to be the relative path from the ServerRoot directive. Specify the name of an already existing directory.

### Context

Global context, Virtual host

### Default value

**Windows32/64**

```
ErrorLog logs/error.log
```

**Solaris32/64** **Linux32/64**

```
ErrorLog logs/error_log
```

### Initial value

**Windows32/64**

```
ErrorLog "|ihsrlog.exe -s logs/errorlog 1 5"
```

**Solaris32/64** **Linux32/64**

```
ErrorLog "|/opt/FJSPihs/bin/ihsrlog -s logs/errorlog 1 5"
```

## Note

- If this directive is set more than once for both the main host and virtual host, then the settings last defined for each will be the valid ones.
- "syslog", which can be specified in Apache HTTP Server, cannot be used in this product.
- If the [Update]/[Create] operation is performed in the following Interstage Management Console windows, "Directory where the log file is stored and Prefix for the log file name", which is set for the logfile executable statement of the ihsrlog command of this directive, will be enclosed in a backslash and double quotes (\"). However, this has no impact whatsoever on operations.
  - [System] > [Services] > [Web Server] > [Web Server name] > [Environment Settings]
  - [System] > [Services] > [Web Server] > [Web Server name] > [Virtual Hosts] > [Virtual Host name] > [Detailed Settings]
  - [System] > [Services] > [Web Server] > [Web Server name] > [Virtual Hosts] > [Create a new Virtual Host]

**Solaris32/64** **Linux32/64**

- If the log file name is specified in this directive, error message ihs70009 is output when the file size set using the *ulimit* command (Bourne shell) or the *limit* command (C shell) is reached, and recording of the log fails.

## 11.3.5 Group

---

### Name

Group

### Synopsis

**Solaris32/64** **Linux32/64**

Group groupID

### Description

Specifies the name of the group to use when a server process is executed.

For the group ID, the group name can be specified, or the group ID (numeric value) can be specified following a number sign (#).

### Context

Global context

### Default value

nobody

### Initial value

```
Group nobody
```

## 11.3.6 Listen

---

### Name

Listen

### Synopsis

Listen [IP-address:]port

## Description

Specifies the port numbers or IP addresses of the multiple ports that receive the connection requests from clients. Normally, ports or addresses are specified in the Port directive, but in this directive, multiple port numbers as well as IP addresses can be specified. The port number can be within the range of 1 to 65535. In Solaris, the IPv6 address can be specified in square brackets ([ ]) in the IP address.

## Context

Global context

## Default value

None

## Initial value

```
Listen 80
```

## Note

- This directive must be set. If it is not, the Web server cannot be started.
- For port number, all the services on the system including applications must have different port numbers set. Note that, if a port number except 80 (HTTP) and 443 (HTTPS) is specified, there is a risk of a conflict with a well-known port between 1 and 1023.
- The same IP address and port number combination can only be set once in this directive.
- Use the IP address set in the operating system.
- For operations on operating systems where multiple IP addresses have been set, if the IP address is omitted then a request to connect to all the multiple IP addresses set in the operating system will be received. To receive requests to connect to a specific IP address only, the IP address must be specified.

**Windows32/64** **Linux32/64**

- IPv6 addresses cannot be specified in this directive. To run the server in an IPv6 environment, specify just the port number and not the IP address.

## 11.3.7 LoadModule

---

### Name

LoadModule

### Synopsis

LoadModule module ID filename

### Description

Reads a plug-in module. Specifies the name of the module structure defined in the plug-in module source file for module ID. The absolute path of the plug-in module file name is used.

### Context

Global context

### Default value

None

## 11.3.8 LogFormat

---

## Name

LogFormat

## Synopsis

LogFormat format [nickname]

## Description

Defines the customized log format.

The format parameters that can be specified as the format are shown below.

%A

The IP address of the Web Server that received the request

%b

The amount of data transferred to a client (in bytes)

Note: When SSL is communicated, the amount of the data transferred before doing the encryption processing is output.

%D

Duration (micro seconds) from the acceptance of a request to completion of processing

%{Foobar}e

Contents of the Foobar environment variable

%{UNIQUE\_ID}e

The unique ID assigned for each request

%h

The IP address/host name of systems such as the client or proxy server

%{Cookie}i

The value of the Cookie header when the Web Server received the request

%{Cookie2}i

The value of the Cookie2 header when the Web Server received the request

%{Foobar}i

Contents of a request header specified in Foobar

%{HOST}i

The value of the HOST header when the Web Server received the request

%{Referer}i

The value of the Referer header when the Web Server received the request

%{User-agent}i

The value of the User-agent header when the Web Server received the request

%l

Personal information of a user returned from a client

%{Cookie}n

The client IP address and unique ID set by the clickstream log of user activity on a site

%{Set-Cookie}o

The value of the Set-Cookie header when the Web Server responds the request



**%(Set-Cookie2)o**

The value of Set-Cookie2 header when the Web Server responds the request

**%p**

The port number of the Web server that received the request

**%P**

The process ID of the connection process that processed the request

**%r**

The first line of a request

**%s**

A status code for a request

**%S**

Duration (seconds.milliseconds) from acceptance of a request to completion of processing

**%t**

Time and date when a request was made

**%T**

Duration (seconds) from the acceptance of a request to completion of processing

**%u**

Name of a user sent from a client

Note: This is only output when the Interstage HTTP Server user authentication or online inquiry functionality is used.

**%U**

A path of the requested URL

**%X**

Connection status at the time the response was sent.

- X: Connection terminated abnormally before the response was sent.
- +: Connection was kept after the response was sent.
- -: Connection was closed after the response was sent.

For nickname, a nickname for the set format is specified.

## Context

Global context, Virtual host

## Default value

```
LogFormat "%h %l %u %t \"%r\" %>s %b" clf
```

## Initial value

```
LogFormat "%h %l %u %t \"%r\" %>s %b %A:%p %{Host}i %P %S %{UNIQUE_ID}e" ihs-analysis
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" \" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
```

## Module

mod\_log\_config

## Note

- If the information that was output for the specified format parameter is not available, or it cannot be output in the required format, a hyphen (-) is output.
- To specify "%1" in the format parameter, the IdentityCheck directive must be set as shown below, and the settings for collecting the "Identify user name" must be configured in the access log.

IdentityCheck On

- To specify "%{UNIQUE\_ID}e" in the format parameter, the LoadModule directive must be set as shown below to read the "unique\_id\_module" module.

**Windows32/64**

```
LoadModule unique_id_module "C:/Interstage/F3FMihs/modules/mod_unique_id.so"
```

**Solaris32/64** **Linux32/64**

```
LoadModule unique_id_module "/opt/FJSVihs/modules/mod_unique_id.so"
```

## 11.3.9 ScriptAlias

---

### Name

ScriptAlias

### Synopsis

ScriptAlias URL-path directory-path

### Description

ScriptAlias sets the directory for CGI execution. Specify a virtual directory name for the URL path, and specify the absolute path of the CGI execution directory for the directory path.

The URL path can consist of up to 224 alphanumeric characters or any of the following symbols:

+, -, ., \_, and /

The path must be unique. The same URL path as one specified in the Alias directive cannot be specified.

### Context

Global context, Virtual host

### Default value

none

### Initial value

**Windows32/64**

```
ScriptAlias /cgi-bin/ "C:/Interstage/F3FMihs/servers/(Web server name)/cgi-bin/"
```

**Solaris32/64** **Linux32/64**

none

### Module

mod\_alias

## Note

- If the name of the Servlet Service application Web application is "ROOT", this directive setting will be invalid.
- Servlet service applications cannot be specified in the URL path. If a Servlet Service application is specified in the URL path and this directive is set, the setting will be invalid.

**Solaris32/64** **Linux32/64**

- The mount point to the NFS server can be specified in the directory path, but it must always be possible to access the NFS server while the Web server is running. Make sure that the NFS server has started up normally before the Web server starts up. Also, do not perform operations that make it impossible to access the NFS server while the Web server is running (for example, powering off the NFS server).

## 11.3.10 ServerAdmin

---

### Name

ServerAdmin

### Synopsis

ServerAdmin *email-address*

### Description

Specifies the server administrator e-mail address the server puts in error messages sent to clients.

### Context

Global context, Virtual host

### Default value

none

### Note

This setting is invalid for Servlet service applications.

## 11.3.11 ServerName

---

### Name

ServerName

### Synopsis

ServerName *host*

### Description

Sets the host name or IP address of a server. The specified name is used to create a redirection URL.

If a namebase virtual host is used, the IP address cannot be specified for this directive that is set in the virtual host section. Specify the host name instead.

### Context

Global context, Virtual host

### Default value

none

## Initial value

```
ServerName (Host name)
```

## Note

The IPv6 address cannot be specified in this directive.

## 11.3.12 ServerRoot

---

### Name

ServerRoot

### Synopsis

ServerRoot directory-path

### Description

Sets the root directory path in which the server lives. Relative paths for setting files are based on the directory set in this directive. Normally, conf/ and logs/ are placed under this directory as subdirectories.

The settings for this directive for installation and creation of the Web server are shown below.

#### Windows32/64

(Default installation path)

```
C:\Interstage\F3FMihs\servers\  
(Web Server name)
```

#### Solaris32/64

(Default installation path)

```
/var/opt/FJSVihs/servers/  
(Web Server name)
```

#### Linux32/64

```
/var/opt/FJSVihs/servers/  
(Web Server name)
```

### Context

Global context

### Default value

None

### Initial value

#### Windows32/64

```
ServerRoot "C:/Interstage/F3FMihs/servers/  
(Web server name)"
```

#### Solaris32/64 Linux32/64

```
ServerRoot "/opt/FJSVihs/servers/  
(Web server name)"
```

## Note

This directive is set automatically during creation and installation of the Web server. For this reason, it should not be edited directly. If the value set for this directive is changed, Web server behavior cannot be guaranteed.

## 11.3.13 SetEnvIf

---

### Name

SetEnvIf

### Synopsis

SetEnvIf attribute attribute-value *environment-variable*[=value]

### Description

Set an environment variable when attributes in a request header from a client match with specified attribute values. The parameters are specified as shown below.

#### attribute

Specify one of the following values:

##### HTTP request header name

HTTP request header name, such as Host, User-Agent, Referer, Accept-Language

The HTTP request header name can be specified using a regular expression.

##### Remote\_Host

Host name of systems such as the client or proxy server

##### Remote\_Addr

IP address of systems such as the client or proxy server

##### Request\_Method

Method name

##### Request\_Protocol

Name and version of the protocol

##### Request\_URI

URL scheme and the portion following the host

##### Server\_Addr

IP address of the Web server that receives the request

#### attribute-value

Specify an attribute value. The attribute value can be specified using a regular expression.

#### environment-variable

This is specified in the following formats:

##### environment-variable name

The specified environment variable value is set to "1".

##### !environment-variable name

If the specified environment variable has already been set, that environment variable will be removed.

##### environment-variable name=value

The specified value is set in the specified environment variable.

## Context

Global context, Virtual host, Directory

## Default value

none

## Module

mod\_setenvif

## 11.3.14 SSLCertExpand

---

### Name

SSLCertExpand

### Synopsis

SSLCertExpand on|off

### Description

Specifies if the client certificate detailed item is set as the environment variable.

on

The client certificate detailed item is set as the environment variable.

off

The client certificate detailed item is not set as the environment variable.

### Context

Global context, Virtual host

### Default value

For the main host:

```
SSLCertExpand on
```

For a virtual host:

```
SSLCertExpand (The value set for this main host directive)
```

### Module

mod\_ihs\_ssl

## 11.3.15 SSLCertExpire

---

### Name

SSLCertExpire

### Synopsis

(1) When the Web server starts up, a warning message that notifies the number of days the certificate is still valid for is output

SSLCertExpire Startup day

(2) For the days/time specified while the Web server is running, a warning message that notifies the number of days the certificate is still valid for is output

SSLCertExpire Running days[,...][:time]

(3) When the Web server starts up, and for the days/time specified while the Web server is running, a warning message that notifies the number of days the certificate is still valid for is output

SSLCertExpire All day days[,...][:time]

(4) A warning message that notifies the number of days the certificate is still valid for is not output

SSLCertExpire None

## Description

Set whether a warning message is output before the validity term of the site certificate and CA certificate expires. Additionally, if the warning message is output, set the timing for the output.

## [Existence of output]

### Startup

A warning message that notifies the number of days the certificate is still valid for is output using the day condition.

### Running

A warning message that notifies the number of days the certificate is still valid for is output using the days (time) condition.

### All

A warning message that notifies the number of days the certificate is still valid for is output using the day and days (time) conditions.

### None

A warning message that notifies the number of days the certificate is still valid for is not output.

## [Timing for the output]

### day

When Startup/All are specified, specify how many days ahead of certificate expiry date a warning message is to be output in case Running/All are specified. The option must be specified as a number between 1 and 90 (unit: days). The timing for the output of the warning message is when the Web server starts up.

### days

When Running/All are specified, specify how many days ahead of certificate expiry date a warning message is to be output in case Running/All are specified. The option must be specified as a number between 1 and 90 (unit: days). More than one day of the week can be specified. In this case, separate each day of the week using a comma (.). A maximum of 90 days can be specified. The timing for the output of the warning message is the days and time specified for days/time while the Web server is running.

### time

When Running/All are specified, use the format shown below to specify the time at which the warning message is output. (If this is omitted, the format will be days and time left until the certificate's validity term expires.)

hhmmss (A numeric value between 000000 and 235959)

- hh: Hours (00-23)
- mm: Minutes (00-59)
- ss: seconds (00-59)

## [Warning message that is output]

The warning messages shown below are output according to the output timing specified above. For details on these messages, refer to "ihs00500 to ihs00599" in the "Messages Beginning with 'ihs'" chapter of the Messages manual.

- Warning message that notifies the number of days the site certificate is still valid for (ihs00536)

- Warning message that notifies the number of days the CA certificate is still valid for (ihs00537)

### Context

Global context

### Default value

```
SSLCertExpire All 14 90,60,30,14,7,6,5,4,3,2,1
```

### Module

mod\_ihs\_ssl

## 11.3.16 SSLCertName

---

### Name

SSLCertName

### Synopsis

SSLCertName *nickname*

### Description

Specifies the nickname of a site certificate registered in the certificate and CRL control environment, in up to 128 characters.

Only one SSLCertName directive can be defined for each host.

### Context

Global context, Virtual host

### Default value

none

### Module

mod\_ihs\_ssl

### Note

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.17 SSLCipherSuite

---

### Name

SSLCipherSuite

### Synopsis

SSLCipherSuite *encryption-method*

### Description

Specify the methods of encryption in descending order of priority. Use colons (:) as delimiters.

When the SSL protocol version "SSL2.0" is used (a value including 2 is specified in the SSLVersion directive), the following values can be specified.



Table 11.1 SSLVersion Directive Values if 2 or 2-3 is specified

Value	Explanation
RC4-MD5	SSL_TXT_RC4_128_WITH_MD5 (128 bit key)
RC2-MD5	SSL_TXT_RC2_128_CBC_WITH_MD5 (128 bit key)
DES-CBC3-MD5	SSL_TXT_DES_192_EDE3_CBC_WITH_MD5 (168 bit key)
DES-CBC-MD5	SSL_TXT_DES_64_CBC_WITH_MD5 (56 bit key)
EXP-RC4-MD5	SSL_TXT_RC4_128_EXPORT40_WITH_MD5 (40 bit key)
EXP-RC2-MD5	SSL_TXT_RC2_128_CBC_EXPORT40_WITH_MD5 (40 bit key)

When the SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0) is used (a value including 3 or 3.1 is specified in the SSLVersion directive), the following values can be specified.

Table 11.2 SSLVersion Directive Values if 3 or 2-3 is specified

Value	Explanation
RSA-RC4-MD5	SSL_TXT_RSA_WITH_RC4_128_MD5 (128 bit key)
RSA-RC4-SHA	SSL_TXT_RSA_WITH_RC4_128_SHA (128 bit key)
RSA-3DES-SHA	SSL_TXT_RSA_WITH_3DES_EDE_CBC_SHA (168 bit key)
RSA-DES-SHA	SSL_TXT_RSA_WITH_DES_CBC_SHA (56 bit key)
RSA-EXPORT-RC4-MD5	SSL_TXT_RSA_EXPORT_WITH_RC4_40_MD5 (40 bit key)
RSA-EXPORT-RC2-MD5	SSL_TXT_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (40 bit key)
RSA-AES-128-SHA	SSL_TXT_RSA_WITH_AES_128_CBC_SHA (128 bit key)
RSA-AES-256-SHA	SSL_TXT_RSA_WITH_AES_256_CBC_SHA (256 bit key)
RSA-SC2000-128-SHA	SSL_TXT_RSA_WITH_SC2000_128_CBC_SHA (128 bit key)
RSA-SC2000-256-SHA	SSL_TXT_RSA_WITH_SC2000_256_CBC_SHA (256 bit key)
RSA-NULL-MD5	SSL_TXT_RSA_WITH_NULL_MD5
RSA-NULL-SHA	SSL_TXT_RSA_WITH_NULL_SHA

If 2-3 or 2-3.1 is specified for the SSLVersion directive, at least one value must be specified for each version.

**Note**

The encryption types shown in the encryption method item ("SSL\_TXT\_XXX") supported by Interstage Application Server are:

- Public-key encryption method: RSA
- Private-key encryption method: DES, 3DES (triple DES), RC4, RC2, AES, SC2000 (NULL means no encryption.)
- Private-key processing mode: CBC, EDE (the numerical value shows the block length.)
- Hash key: SHA, MD5

**Context**

Global context, Virtual host

**Default value**

The following values are assumed according to the specified value for the SSLVersion directive. (In the following table, each encryption method is described on a new line for clarification.)

Table 11.3 Assumed Values of SSLVersion Directive if omitted

Value of the SSLVersion directive	Default value of this directive
2	DES-CBC3-MD5:

Value of the SSLVersion directive	Default value of this directive
	RC4-MD5: RC2-MD5: DES-CBC-MD5: EXP-RC2-MD5: EXP-RC4-MD5
3 3.1 3-3.1	RSA-SC2000-256-SHA: RSA-AES-256-SHA: RSA-SC2000-128-SHA: RSA-AES-128-SHA: RSA-3DES-SHA: RSA-RC4-MD5: RSA-RC4-SHA: RSA-DES-SHA: RSA-EXPORT-RC4-MD5: RSA-EXPORT-RC2-MD5
2-3 2-3.1	DES-CBC3-MD5: RC4-MD5: RC2-MD5: DES-CBC-MD5: EXP-RC2-MD5: EXP-RC4-MD5: RSA-SC2000-256-SHA: RSA-AES-256-SHA: RSA-SC2000-128-SHA: RSA-AES-128-SHA: RSA-3DES-SHA: RSA-RC4-MD5: RSA-RC4-SHA: RSA-DES-SHA: RSA-EXPORT-RC4-MD5: RSA-EXPORT-RC2-MD5

**Module**

mod\_ihs\_ssl

**Note**

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

**11.3.18 SSLCICACertName**

---

**Name**

SSLCICACertName

**Synopsis**

SSLCICACertName *nickname*

**Description**

Specifies the nickname of the CA certificate for confirming a client certificate, in up to 128 characters. This directive is used to select a specific certificate from client CA certificates registered in the operation control directory. The directive is enabled when SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0) is used.

Multiple SSLCICACertName directives can be defined for each host and each definition is enabled only for the corresponding host.

**Context**

Global context, Virtual host

**Default value**

The nicknames of all client CA certificates registered in the operation control directory are specified.

**Module**

mod\_ihs\_ssl

**Note**

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.19 SSLEnvDir

---

**Name**

SSLEnvDir

**Synopsis**

SSLEnvDir *operation-control-directory-name*

**Description**

Specifies the operation control directory used for SSL along with the absolute path.

Only one SSLEnvDir directive can be defined for each host.

**Context**

Global context, Virtual host

**Default value**

none

**Module**

mod\_ihs\_ssl

**Note**

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.20 SSLExec

---

### Name

SSLExec

### Synopsis

SSLExec [on|off]

### Description

Specifies whether SSL is used.

Only one SSLExec directive can be defined for each host.

on

SSL is used.

off

SSL is not used.

### Context

Global context, Virtual host

### Default value

SSLExec off
-------------

### Module

mod\_ihs\_ssl

### Note

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.21 SSLHandshakeTimeout

---

### Name

SSLHandshakeTimeout

### Synopsis

SSLHandshakeTimeout *seconds*

### Description

Sets the maximum wait time (in seconds) after a data packet is sent/received to/from the client in SSL connection establishment processing. A number from 0 to 65535 can be specified for the wait time. If the packet cannot be received even though the specified wait time is exceeded, the connection is closed. If "0" is specified, the wait time is unlimited.

Normally, this is set so that the time taken for SSL connection establishment processing can be tuned.

### Context

Global context

### Default value

Value set for the Timeout directive

**Module**

mod\_ihs\_ssl

## 11.3.22 SSLLIBMultiSession

---

**Name**

SSLLIBMultiSession

**Synopsis**

SSLLIBMultiSession concurrency

**Description**

Specifies the concurrency for the initial startup of the encrypted library. A number from 1 to 256 can be specified for the concurrency. If the value that is set is increased, communication processing for multiple connections immediately after startup becomes faster. If the value that is set is increased, however, note that the start processing time also increases.

**Context**

Global context

**Default value**

50

**Module**

mod\_ihs\_ssl

**Note**

The value that is set for this directive is extended automatically according to the number of requests, so in normal cases there is no need for it to be set.

## 11.3.23 SSLMaxSession

---

**Name**

SSLMaxSession

**Synopsis**

Number of SSLMaxSession requests

**Description**

Specifies the maximum number of requests used to retain SSL session information. A number from 0 to 65535 can be specified for the number of requests. Once SSL communication is performed, and SSL session information is retained on the server machine, it is possible to improve the request forwarding efficiency.

This directive is enabled if "SSL 3.0" or more is set for the SSL protocol version in the SSLVersion directive.

**Context**

Global context

**Default value**

SSLMaxSession 100
-------------------

## Module

mod\_ihs\_ssl

## Note

Approximately 4 kilobytes of virtual memory are used up for each increase of 1 in the value that is set for the number of requests. When tuning the application status, take care not to set a value that is too great.

## 11.3.24 SSLNotifyVers

---

### Name

SSLNotifyVers

### Synopsis

SSLNotifyVers on|off

### Description

Specifies whether an SSL-related environment variable is set.

on

SSL-related information is set as the environment variable.

off

SSL-related information is set as the environment variable. However, the HTTPS environment variable is set.

### Context

Global context, Virtual host

### Default value

For the main host:

```
SSLNotifyVers on
```

For a virtual host:

```
SSLNotifyVers (The value set for this main host directive)
```

## Module

mod\_ihs\_ssl

## 11.3.25 SSLSlotDir

---

### Name

SSLSlotDir

### Synopsis

SSLSlotDir *slot-information-directory*

### Description

Specifies the slot information directory for the private key control environment along with the absolute path.

Only one SSLSlotDir directive can be defined for the basic area of the environment definition file (httpd.conf).

**Context**

Global context

**Default value**

none

**Module**

mod\_ihs\_ssl

**Note**

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.26 SSLTokenLabel

---

**Name**

SSLTokenLabel

**Synopsis**

SSLTokenLabel *token-label*

**Description**

Specifies the token label of the token in which the private key of the server is registered, in up to 32 characters.

Only one SSLTokenLabel directive can be defined for the basic area of the environment definition file (httpd.conf).

**Context**

Global context

**Default value**

none

**Module**

mod\_ihs\_ssl

**Note**

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.27 SSLUserPINFile

---

**Name**

SSLUserPINFile

**Synopsis**

SSLUserPINFile *user-PIN-file-name*

**Description**

Specifies a user PIN file along with the absolute path.

Only one SSLUserPINFile directive can be defined for the basic area of the environment definition file (httpd.conf).

For information on creating a user PIN file, refer to "ihsregistupin" in the Reference Manual (Command Edition).

### Context

Global context

### Default value

none

### Module

mod\_ihs\_ssl

### Note

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.28 SSLVerifyClient

---

### Name

SSLVerifyClient

### Synopsis

SSLVerifyClient [none|optional|require]

### Description

Specifies the level of client certification when using SSL protocol version "SSL3.0" or "SSL3.1" (TLS 1.0).

Only one SSLVerifyClient directive can be defined for each host.

none

Does not verify a client certificate.

optional

Verifies a client certificate.

When a client does not provide the client certificate, the processing continues.

require

Verifies a client certificate.

When a client does not provide the client certificate, an error occurs.

When "2" is specified with the SSLVersion directive, this directive must be omitted or set to "none".

### Context

Global context, Virtual host

### Default value

One of the following values is specified according to the value specified with the SSLVersion directory.

Table 11.4 Assumed Values of SSLVersion Directive if omitted

Value of the SSLVersion directive	Default value of this directive
2	None
3	Optional
3.1	Optional



Value of the SSLVersion directive	Default value of this directive
2-3	Optional
2-3.1	Optional
3-3.1	Optional

## Module

mod\_ihs\_ssl

## Note

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.29 SSLVersion

---

### Name

SSLVersion

### Synopsis

SSLVersion 2|3|3.1|2-3|2-3.1|3-3.1

### Description

Specifies the version of SSL protocol to be used.

Only one SSLVersion directive can be defined for each host.

2

Uses SSL protocol version "SSL2.0".

3

Uses SSL protocol version "SSL3.0".

3.1

Uses SSL protocol version "SSL3.1" (TLS 1.0).

2-3

One of the following is the highest protocol version that can be used for communication by the client:

- SSL protocol version "SSL2.0"
- SSL protocol version "SSL3.0"

2-3.1

One of the following is the highest protocol version that can be used for communication by the client:

- SSL protocol version "SSL2.0"
- SSL protocol version "SSL3.0"
- SSL protocol version "SSL3.1" (TLS 1.0)

3-3.1

One of the following is the highest protocol version that can be used for communication by the client:

- SSL protocol version "SSL3.0"
- SSL protocol version "SSL3.1" (TLS 1.0)

## Context

Global context, Virtual host

## Default value

```
SSLVersion 3-3.1
```

## Module

mod\_ihs\_ssl

## Note

This directive cannot be specified if the SSLConfName directive is specified. If it is, the settings for this directive are invalid.

## 11.3.30 Timeout

---

### Name

Timeout

### Synopsis

Timeout *seconds*

### Description

Sets the maximum wait time (in seconds) after a data packet is sent/received to/from the client. A number from 0 to 65535 can be specified for the wait time. If the packet has not been received when the specified wait time is exceeded, the TCP connection is closed. If the network traffic increases causing the TCP connection to be frequently disconnected, increase the wait time to reduce the number of these disconnections.

#### Note

If the request does not arrive after the client TCP connection, the TCP connection will break when the time specified in this directive (in seconds) is reached.

### Context

Global context

### Default value

```
Timeout 300
```

### Initial value

```
Timeout 600
```

## 11.3.31 User

---

### Name

User

### Synopsis

**Solaris32/64** **Linux32/64**

User userID

## Description

Specifies the name of the user who executes the server process.

For the user ID, the user name can be specified, or the user ID (numeric value) can be specified following a number sign (#).

## Context

Global context

## Default value

```
User nobody
```

## Initial value

```
User nobody
```

## 11.3.32 <VirtualHost>

---

### Name

```
<VirtualHost>
```

### Synopsis

```
<VirtualHost> address[:port]> ... </VirtualHost>
```

### Description

Sets up a virtual host.

The following are specified for the address.

- The IP address of the virtual host
- A fully qualified domain name for the IP address of the virtual host.

When the address is not specified, a special name "< VirtualHost \_default\_>" can be specified.

The IPv6 address can also be specified in the IP address.

The port number that a virtual host uses is specified for the port. When all the port numbers are targeted, "\*" is specified.

### Context

Global context

### Default value

none

### Note

If "\*" is specified in the port number and the virtual host is set, the virtual host cannot be displayed, modified or deleted in the Interstage Management Console. Set the virtual host in the environment definition file (httpd.conf).

# Chapter 12 How to Use SSL with the CORBA Service

Client-server application linkage using the CORBA Service enables encrypted communication via SSL.

This chapter explains the SSL communication via the CORBA application.

In the CORBA service, the two environments listed below can be used to manage certificates and private keys required for encryption and signature processing.

- Interstage certificate environment
- Certificate/key management environment configured with the SMEE commands

Set either of the above environments according to the operation type. To use an Interstage certificate environment, refer to "Setting and Use of the Interstage Certificate Environment" Chapter to configure the Interstage certificate environment. Then, set an SSL environment in a CORBA service using the Interstage management console.

## Setting Access Permission

**Solaris32/64** **Linux32/64**

In an Interstage certificate environment, to run an application with permission of a common user (other than a system administrator (root)), the user must belong to an ownership group. Add the users running applications to the ownership group in the Interstage certificate environment. For more information, refer to Setting Up Access Permissions in the Interstage Certificate Environment in "Setting and Use of the Interstage Certificate Environment" Chapter.

In a certificate/key management environment configured with the SMEE commands, to run an application with permission of a common user (other than a system administrator (root)), execute the *odsetpath* command because common user access permission must be set in a private key/certificate.

**Windows32/64**

To enable a general user (a user without Administrators authority) to run an application in an Interstage certificate environment with general user authority, the access authority for the Interstage certificate environment must be changed. For details, refer to Setting up Access Permissions in the Interstage Certificate Environment in "Setting and Use of the Interstage Certificate Environment" Chapter.

To enable a general user (a user without Administrators authority) to run an application in a certificate/key management environment configured with the SMEE command access (assuming that user is not the one that actually configured the certificate/key management environment), the following needs to be completed:

- Executing user access authority must be added to the certificate/key management environment.

Use the following procedure to add executing user access authority to the certificate/key management environment:

Use Windows Explorer to select the certificate and key management environment folders. In the [Properties] menu, [Security] tab window, add access authority by adding users and groups. Set [Full Control] for the users and groups that are added.

### Note

If the [Security] tab is not displayed for the folder's properties on Microsoft(R) Windows(R) XP, perform the following steps to display it:

1. Select [Start]-[Control Panel]-"Folder Options".
2. Click the [View] tab, remove the checkmark on "Use Simple File Sharing (Recommended)", and click "OK".

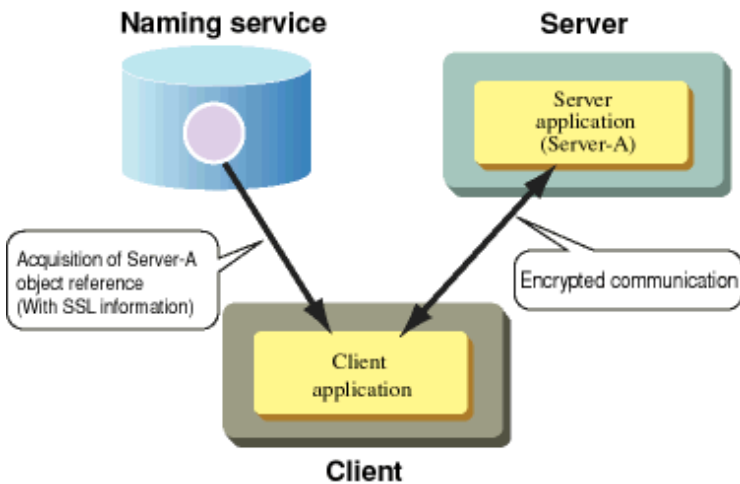
## 12.1 SSL Linkage of the CORBA Service

The SSL linkage function of the CORBA Service performs encrypted communication that is used for transferring data between CORBA applications by using SSL.

### Mechanism of the SSL Linkage Function

If encrypted communication is set for the object reference of the server application in CORBA application linkage, encrypted communication using SSL is conducted with any client linked to the object.

The following figure shows a processing image (when an object reference is generated statically) of the SSL linkage function.



### SSL Linkage Function

If SSL information is set for an object reference acquired by the client application, SSL encrypted communication is conducted to send and receive requests to the server application.

### Developing the CORBA Application

To perform SSL communication using the CORBA application linkage, the ordinary CORBA application can be used as is. It is only necessary to set SSL information when the CORBA application (server application) is registered. No application needs to be recreated (including re-linkage).

### Constructing SSL Linkage Environment

To perform encryption communication using SSL, the following processing must be done for the server and client: creating the certification management environment and registering the certificates.

To perform SSL communication during CORBA application operation, it is necessary to register the SSL environment in the CORBA Service and to set the SSL information for the CORBA application (server application) that performs SSL communication.

#### Acquiring and Registering Certificates (for both the Server and Client)

Create a private key/certificate management environment as an SSL environment, then register the CA certificate obtained from the certification authority and site certificate in the Interstage certificate environment. The same issuing office certificate must be registered for all servers and clients in which CORBA applications for SSL linkage were placed.

For an explanation of obtaining and registering certificates, refer to "Setting and Use of the Interstage Certificate Environment" Chapter and "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" Chapter.

#### Setting and Registering the SSL Environment with the CORBA Service (for both the Server and Client)

To use an Interstage certificate environment, set an SSL environment in a CORBA service using the Interstage management console.

To use a certificate/key management environment configured with the SMEE commands, first register an obtained certificate in the CORBA service using the *odset.SSL* command. Then, set the SSL linkage parameters in the operating environment file for the CORBA service (config) and incorporate SSL communication processing into the CORBA service.

#### Setting the SSL Information in the CORBA Application (Server Application Only)

To perform the SSL linkage using the CORBA application, the SSL information must be set in the object reference of the server application. To set the SSL information in the object reference, use the following method:

- Set the SSL information in the object reference at static generation of the object reference by the *OD\_or\_adm* command. (-s option)
- Specify the SSL information setting rule for the object reference generation during registration of the server application by the *OD\_impl\_inst* command. (ssl parameter)

The SSL information is set according to this rule during object reference generation (both static and dynamic generations).

## Operating the SSL Linkage

The application linkage that uses SSL can be performed by accessing the server application ( for the object reference). SSL information is to be added to this using the *OD\_or\_adm* and *OD\_impl\_inst* commands.

## SSL Linkage in the IPv6 Environment

The SSL linkage function cannot be used in the IPv6 environment.

# 12.2 CORBA Server Environment Setup

---

Configure an Interstage certificate environment, or configure a certificate/key management environment with the SMEE commands, according to the operation type. To use the Interstage certificate environment, set an SSL environment in the CORBA service using the Interstage management console.

## 12.2.1 Specifying the Addition of SSL Information at Definition of Object Reference

---

To perform SSL communication, execute both or either of the steps below to add SSL information to the object reference of the server application.

- Execute the *-s* option of the *OD\_or\_adm* command to define object reference with SSL information.
- Specify the *ssl* parameter in the definition file of the *OD\_impl\_inst* command, and select whether SSL information is to be added at definition of object reference.

For details on the relationships between the information specified by the *OD\_or\_adm* or *OD\_impl\_insts* Command and whether SSL communication is valid, refer to *OD\_impl\_inst*.

### Note

Once the SSL environment has been set in the CORBA service, the *OD\_or\_adm* command must be used to specify the host name (*-h* option) and port number (*-p* option) if the CORBA service is not restarted.

This port number must be the same as the SSL port number for the CORBA service that has been previously set.

# 12.3 SSL Environment Setup in Client

---

To use an Interstage certificate environment, set an SSL environment using the Interstage management console. The following is the procedure for setting an environment that enables CORBA clients to use SSL in a certificate/key management environment configured with the SMEE commands.

1. Create a certificate/key management environment.

For details, refer to Certificate and Private Keys in "Setting and Use of the Interstage Certificate Environment" Chapter.

2. Create a secret key and acquire a certificate.

For details, refer to What are the Certificates and the Private Keys in "Setting and Use of the Interstage Certificate Environment" Chapter.

3. Register the certificate and CRL.

For details, refer to Registering Certificates and CRL in "Setting and Use of the Interstage Certificate Environment" Chapter.

4. Define a private key/certificate in the CORBA Service.

5. Edit the config file.

The following sections explain the steps 4 and 5 for CORBA client.

### Note

To set up the SSL environment, use the following commands:

To use a parameter that is too long to enter at the command prompt, include the parameter in a batch file for execution.

Table 12.1 Client SSL Setup Commands

Command	Definition
C:\Interstage\ODWIN\bin\odsetSSL	Defines private key/certificate for CORBA Service.

## 12.3.1 Defining a Private Key/Certificate in CORBA Service

To perform SSL communication via CORBA application linkage, define a private key/certificate in the CORBA Service.

### Defining Private Key/Certificate

To define a private key/certificate in the CORBA Service, execute the odsetSSL command.

If the site certificate (client certificate) of the local host is used, specify the nickname of the site certificate. When the command is executed, input the user PIN set in the token.

#### Example

Define a private key/certificate in the CORBA Service.

```
odsetSSL -sd C:\slot -ed C:\sslcert -tl Token01 -nn Jiro
UserPIN:
Re-type UserPIN:
```

#### Note

Do not specify a nickname ("-nn Jiro" in the above example) in operation mode without using client certificates under SSL version 3.0.

### Security Attributes

For more information about the odsetSSL command, refer to *odsetSSL* in the Reference Manual (Command Edition).

The -verify option (specification of authentication when the client certificate is not present) need not be specified on the client side.

## 12.3.2 Editing config File

To embed SSL communication processing in the CORBA Service, specify "yes" in UNO\_IIOp\_ssl\_use of the config file.

When port number 4433 (initial value) for SSL communication is used by another program, specify an unused number in the range from 1024 to 65535 in UNO\_IIOp\_ssl\_port.

```
C:\Interstage\ODWIN\etc\config
UNO_IIOp_ssl_use = yes
UNO_IIOp_ssl_port = 4433
```

#### Note

To validate a new set value of the config file, reactivate the client application.

## 12.4 Environment Setup for Event Service

The Event Service can be used with the following products:

- Interstage Application Server Enterprise Edition
- Interstage Application Server Standard-J Edition.

For SSL communication in the Event Service, the SSL environment of the CORBA Service must be set up. For information about the SSL environment setup of the CORBA Service, refer [12.2 CORBA Server Environment Setup](#).

It is also necessary to set up SSL communication when setting up the Event Service environment for static generation and operation, or dynamic generation and operation. SSL communication in an event service is explained below:

## For Static Generation and Operation

To create an event channel by using the *esmchnl* command, set up SSL communication by specifying the *-ssl* option.

### Example

For SSL communication with an event channel named CHNL1 and created in the event channel group GROUP1:

```
esmchnl -g GROUP1 -c CHNL1 -ssl
```

## For Dynamic Generation and Operation (for Environment Setting using the Interstage Integration Command)

To set up the Interstage environment, add the following definition to the Interstage operating environment definition file, and set up SSL communication.

```
Event SSL=yes
```

## For Dynamic Generation and Operation (for Environment Setting using the Event Service Operation Command)

To set up an event service and an event factory using the *essetup* command, set up the SSL communication by specifying the *-ssl* option.

### Example

To perform SSL communication via the dynamically-generated event channel when the maximum number of processes is 5 and the total number of connected suppliers and consumers on the mixed models is 100:

```
esmchnl -g GROUP1 -c CHNL1 -ssl
```



# Chapter 13 How to Use SSL with J2EE

This chapter describes how to use SSL with J2EE.

## 13.1 Environment Setup for Servlet Service

This section explains how to operate the Interstage Management Console.

### Communication Encryption Using SSL between the Web Browser and Web Server

Set SSL with the Web server.

On the Interstage Management Console, select [Services] > [Web Server] > "Web Server name" > [Web Server Settings] tab > [Detailed Settings [Show]], then set the following at [SSL Settings].

- Select [Yes] for [Enable SSL Encryption?]
- Select the SSL configuration name to be used from [SSL Configuration]

When SSL is set, the Secure attribute is automatically added to the session management cookie.

When an SSL accelerator is used the Secure attribute is not automatically added to the session management cookie, so settings must be implemented to ensure the Secure attribute is always added to the session management cookie.

On the Interstage Management Console, click [WorkUnit] > "WorkUnit Name" > "Web Application Name" > [Application Settings]. In [Context Settings] > [Store session information in cookies?], select "Always add the Secure attribute to cookies".

### Communication Encryption Using SSL between the Web Server Connector and Servlet Container

Set the following on the Interstage Management Console:

- [Use SSL between Servlet Container and Connector?]
- [SSL Configuration to be used for the Servlet Container and Connector]

The setting method varies depending on the operating mode.

- When the Web server and Servlet container run on the same machine:

Select [WorkUnits] > Select "IIServer WorkUnit name" > [Settings] tab > [Web Server Connector Settings [Show]].

- When the Web server and Servlet container run on different machines

Set data for both the Web server connector and Servlet container:

- Setting for Web server connector

Select [Services] > [Web Server] > "Web Server name" > [Web Server Connector] > Select "IIServer WorkUnit name" > [Settings] tab > [Detailed Settings [Show]].

- Setting for Servlet container

Select [WorkUnits] > Select "IIServer WorkUnit name" > [Settings] tab > [Web Server Connector Settings [Show]].

## 13.2 Environment Setting for EJB Service

When using SSL linkage, use the Interstage Management Console to set encrypted communication using SSL.

This setup is the same as for an application using SSL in CORBA Service. For details, refer to the "How to Use SSL with the CORBA Service" chapter.

Steps specific to EJB Service are as follows:

### Set/Unset the Encrypted Communication Using the SSL Protocol

Use the Interstage Management Console to set and reset encrypted communication that uses SSL.

- Setting

Define the EJB container of the IJServer WorkUnit that uses SSL in the window of the Interstage Management Console as follows.

- From the Interstage Management Console, select [WorkUnit] > [IJServer name] > [Settings] > [EJB container settings [Show]].
- Specify "Yes" for [Use SSL for IIOP?].

- Unsetting

Define the EJB container of the IJServer WorkUnit that uses SSL in the window of the Interstage Management Console as follows.

- From the Interstage Management Console, select [WorkUnit] > [IJServer name] > [Settings] > [EJB container settings [Show]].
- Specify "No" for [Use SSL for IIOP?].

#### Note

SSL can only be used for IIOP communication when one of the following WorkUnit types applies.

- The Web application and EJB application run on different JavaVMs.
- Only an EJB application runs.

If the value for config (UNO\_IIOP\_ssl\_port) in the CORBA Service is changed after setting up SSL communication, the EJB application must be redeployed.

When HTTP tunneling is performed using SSL communication, the start parameter must be specified when the client application starts.

For more information, refer to the "HTTP Tunneling of J2EE" chapter.

HTTP tunneling can be used with the following products:

- Interstage Application Server Enterprise Edition

## 13.3 Environment Setting for Interstage JMS

---

Interstage JMS can be used with the following products.

- Interstage Application Server Enterprise Edition
- Interstage Application Server Standard-J Edition

If SSL is to be used for Interstage JMS, settings for signature and encryption processing must be implemented such as for SSL. Refer to the "Setting and Use of the Certificate/Key Management Environment Using the SMEE Command" chapter for details.

## 13.4 Environment Setting for Interstage Web Service

---

This section describes the method for using SSL in the Interstage Web service.

### Settings for using SSL for communication between Web service clients in the Web service

Set SSL with the Web server.

Refer to "Environment Setup for Servlet Service", "Communication Encryption Using SSL between the Web Browser and Web Server" in the "How to Use SSL with J2EE" chapter for details.

### Settings for using SSL for communication between Web services in Web service client applications

SSL can be used in the Web service call in Web service client applications.

SSL is used if the Web service endpoint URL starts with https://.

Certificate management and SSL definition can be performed easily by setting up the Interstage certificate environment to use SSL beforehand. For details on setting up/creating the Interstage certificate environment, refer to the "Setting and Use of the Interstage Certificate Environment" chapter of the Security System Guide.

## Notes

- If SSL communication is used without an Interstage certificate environment, the certificate and SSL definition are not targets of management, such as backup/restore, in this product, so manage them separately.
- The Interstage certificate environment is not provided in the client package.

The settings method for using SSL in Web service client applications is explained below.

## Environment variable settings

Set the following environment variables.

### CLASSPATH

To run an application on a server that is not IJServer, as well as the JAR required by the Web service client application, set the following JAR in CLASSPATH.

**Windows32/64**

```
C:\Interstage\lib\isadmin_scs.jar
```

**Solaris32/64** **Linux32/64**

```
/opt/FJSSVisscs/lib/isadmin_scs.jar
```

### LD\_LIBRARY\_PATH

To run an application on a server that is not IJServer, add the following path to the LD\_LIBRARY\_PATH environment variable.

**Windows32/64** **Solaris32/64**

```
Not required
```

**Linux32/64**

```
/opt/FJSSVisscs/lib
```

## Interstage certificate environment access authority settings **Solaris32/64** **Linux32/64**

The Web service client application must have authority to access the Interstage certificate environment. For details, refer to "Configuring Environments" in the "Setting and Use of the Interstage Certificate Environment" chapter of the Security System Guide.

## SSL settings

Configure the SSL settings in the Web service client application process unit.

If the Web service is called in a URL that starts with https:// without these settings being configured, Communication is performed according to the SSLSocket that is obtained using `javax.net.ssl.SSLSocketFactory.getDefault()`. URLConnection-specific settings and the specification of invalid implementations is not supported. For details on JSSE, refer to the JSSE documentation. Do not specify an implementation that is not supported.

### Process unit settings

Describe the following properties in the Web service settings file.

#### Key

```
com.fujitsu.interstage.isws.client.ssl.configname
```

#### Value

```
SSL definition names created in the Interstage certificate environment
```

For details on the Web service settings file, refer to "Web Service Settings File" in the "Interstage Web Service Operation" chapter of the J2EE User's Guide.

### Stub unit settings

Describe the following properties in the stub object.

**Key**

com.fujitsu.interstage.isws.client.ssl.configname

**Value**

SSL definition names created in the Interstage certificate environment

For details about the method used to specify the stub object, refer to "Settings Relating to HTTP Connections" in the "Developing Web Services" chapter of the J2EE User's Guide. If the stub unit settings are specified, they take priority over the system properties.

**Specified SSL definitions**

Encryption methods not supported by the JSSE provider are ignored, even if selected in the SSL definition. If an SSL definition not included in the encryption methods supported by the JSSE provider is specified, an exception occurs and the connection is not performed. For details on encryption methods supported by the JSSE provider, refer to the JDK/JRE documentation.

# Chapter 14 Using SSL for Interstage Directory Service

This is not valid for Standard-J Edition on Windows (64 bit).

This is not valid for Standard-J Edition on Linux (64 bit).

Interstage Directory Service supports encrypted communication using SSL.

This chapter explains SSL communication for the Interstage Directory Service.

## SSL Communication Targets

Interstage Directory Service supports SSL communication for the following communication paths:

Communication path	SSL communication target
Communication with command	Communication between the Interstage Directory Service and the following commands can be encrypted: ldapsearch command ldapmodify command ldapdelete command
Communication with application	Communication between the Interstage Directory Service and client applications can be encrypted.
Communication in replication operating mode	Communication between master and slave repositories in replication operation mode can be encrypted.

### Note

When the Entry Administration Tool and entry administration command (*irepmodifyent*) are used, SSL communication cannot be used for communication paths. Use them in a security-oriented environment by executing them on the same machine in the repository.

## Client Authentication

After client authentication is performed, only the SSL client that has presented a certificate issued by a specific CA is permitted to access the SSL server. This can prevent user spoofing.

## SSL linkage Environment Setup

To implement encrypted communication using SSL between an Interstage Directory Service client and server, the SSL environment must be registered in the client and SSL information must be set for the SSL communication server.

To implement SSL communication between the master and slave in replication operation mode using a standard database, the master and slave must both be set up in a certificate management environment and registered with a certificate.

For details on the setting up the environment, refer to the chapter 'Setting up the SSL Communication Environment' in the 'Directory Service Operator's Guide'.

# Appendix A Enhancing Security (Protecting Interstage Resources)

**Solaris32/64** **Linux32/64**

The information detailed here applies only to the Solaris and Linux systems.

In a computer system placed in an Internet environment, resources of the local system need to be protected from intrusion/attack from outside the organization.

This appendix explains, for a system constructed with Interstage and used in an Internet environment, how to prevent damage to Interstage resources by external attacks.

## A.1 Protecting Interstage Resources

To prevent damage to the Interstage resource file (such as overwriting or deleting it) by intruders from an external network or disabling the system operation, the system must be operated according to the following basic rules:

### Basic Rules for Preventing Resource Damage

To prevent resource damage, system operation needs to be performed according to the following basic rules:

- Limit the application operation authority during system operation to "specific users".
- The authority attribute of the resource file is restricted so that resources created during system operation cannot be rewritten by users other than "specific users".

Using this product, excluding part of functions, a system in accordance with the above rules can be constructed without special environment setup. However, some functions do not follow the above rules for reasons such as compatibility with older version products.

If the system operation is performed according to the above rules and part of the functions are used, the environment setup needs to be changed.

### Functions that require the Environment Setup

The following table lists functions (components) that require the environment setup so that a system to which basic rules for preventing resource damage are applied can be constructed.

Table A.1 Interstage Application Server Component Setup

Component	Package name	Environment setup item
CORBA Service	<b>Solaris32/64</b> FSUNod <b>Linux32/64</b> FJSVod	User setting in the application operation. Change of the authority attribute of generated resource files
Component Transaction Service	<b>Solaris32/64</b> FSUNtd FSUNextp <b>Linux32/64</b> FJSVtd FJSVextp	User settings in the application operation Change of the authority attribute of generated resource files
EJB Service	FJSVejb	User settings in the application operation Change of the authority attribute of generated resource files
Database Linkage Service	<b>Solaris32/64</b> FSUNots <b>Linux32/64</b> FJSVots	User settings in the application operation Change of the authority attribute of generated resource files

Component	Package name	Environment setup item
Interstage JMS	FJSVjms	User settings in the application operation Change of the authority attribute of generated resource files
Interstage Management Console	FJSVisgui	Change of the authority attribute of generated resource files

#### Notes

- To use the Database Linkage service, use "root" for specific users.
- When you use event service, please change the authority of an event service employment command using the *essecmode* command.

For details of the environment setup of each component, refer to [A.2 Environment Setup for Interstage Resources Protection](#).

## A.2 Environment Setup for Interstage Resources Protection

This section explains the environment setup for resource protection of each component.

### A.2.1 CORBA Service

Solaris32/64

#### Multi-System Operation

The file pathname described in this section is the pathname of the default system.

For a CORBA Service resource file in an extended system in multi-system operation, replace the pathname with an appropriate one in the following table.

Table A.2 CORBA Service Pathnames

File Type	Default System Pathname (*1)	Expended System Pathname
Environment definition file	/etc/opt/FSUNod/config	/var/opt/FJSVisas/system/system name/ FSUNod/etc/config
	/etc/opt/FSUNod/irconfig	/var/opt/FJSVisas/system/system name/ FSUNod/etc/irconfig
Database storage directory of the interface repository	/opt/FSUNtd/var/IRDB	/var/opt/FJSVisas/system/system name/FSUNod/ IRDB (default: setting to "IR path for DB file" in the Interstage operating environment definition)
	/opt/FSUNod/IRDB	(No extended system can be constructed by the <i>odadmin</i> command)
Dynamically generated file	Under /var/opt/FSUNod	Under /var/opt/FJSVisas/system/system name/ FSUNod/var
Operation log file	/var/opt/FSUNod/opelog/opelog	/var/opt/FJSVisas/system/system name/ FSUNod/var/opelog/opelog
	/var/opt/FSUNod/opelog/opelog.old	/var/opt/FJSVisas/system/system name/ FSUNod/var/opelog/opelog.old
	/etc/opt/FSUNod/.odopelog_locks	/var/opt/FJSVisas/system/system name/FSUNod/ etc/.odopelog_locks

\*1 The default system pathname is the default path in the installation/environment setup.

#### Environment Setup Item

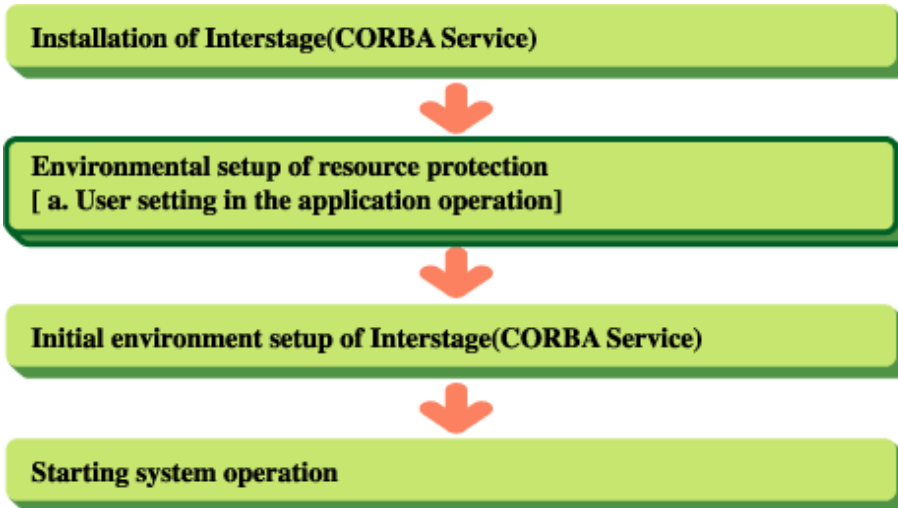
There are two items in the environment setup of the CORBA Service.

- a. User setting in the application operation
- b. Change of the authority attribute of generated resource files

If the initial environment setup of the Interstage (CORBA Service) has not been performed (just after installation), processing of A. is not needed.

The following explains details of the environment setup procedure:

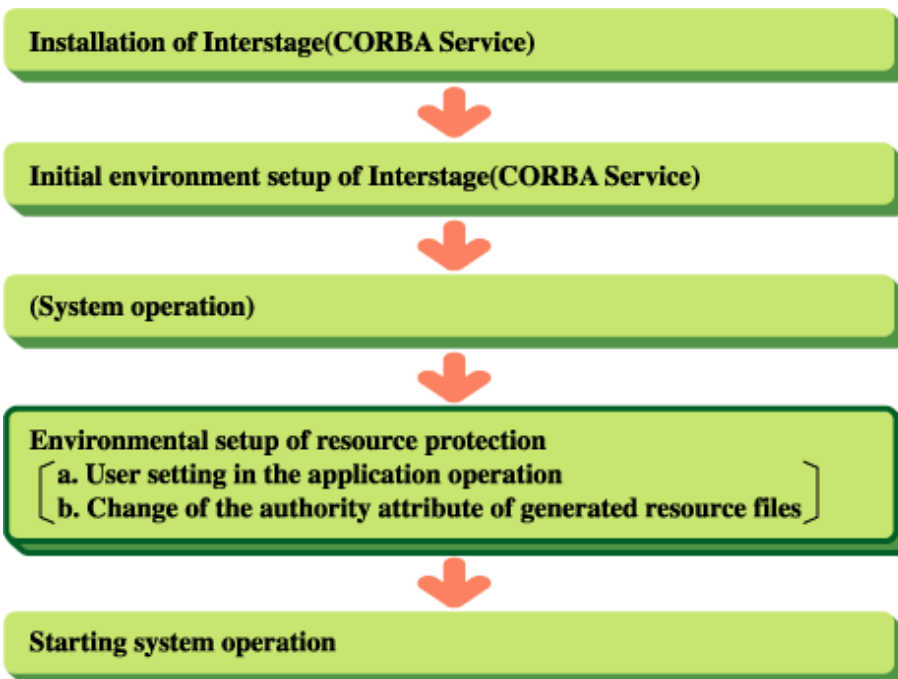
### Just After Installation



### Post-Installation CORBA Service Environment Setup

If the environment for resource protection is set just after installation of Interstage (CORBA Service: FSUNod/FJSVod package), carry out "A. User setting in the application operation" and then execute the *isinit* command (or *odadmin* command) for the initial environment setup of Interstage (CORBA Service).

### After the Interstage Initial Environment Setup



### Post-Initialization CORBA Service Environment Setup



If the environment for resource protection is set after the initial environment setup (execution of the *isinit* command or *odadmin* command, including subsequent system operation) of the Interstage CORBA Service, "A. User setting in the application operation" and "B. Change of the authority attribute of generated resource files" (see below) must be carried out.

## Setting the Environment

The following explains how to set the environment for resource protection.

### a. User Setting in the Application Operation

#### 1. Interstage stop

If Interstage is operating, stop it using the *isstop -f* command.

#### 2. Settings of the CORBA Service resource protection function and CORBA application operation user

Add the following description to the CORBA Service environment definition file (config):

```
iss_use = yes
iss_uid = user ID
iss_gid = group ID
```

#### Explanation

Set the user ID (owner) when a CORBA application is running to "user ID" ("iss\_uid"). Specify a user (hereafter "specific user") who has been registered with the system. Also, the actual group of "specific users" must be matched with that of the superuser who started up Interstage. "Group ID" ("iss\_gid") is optional.

#### 3. Settings of the resource protection function of the interface repository

Add the following description to the interface repository service environment definition file (irconfig):

```
iss_use = yes
```

#### 4. Changing the authority attribute for each operation log file

Change the authority attribute for each operation log file and storage directory.

For details, refer to "Changing the authority attribute for each operation log file", below.

#### 5. Perform the initial environment setup of Interstage (CORBA Service) or start Interstage (CORBA Service).

### b. Change of the Authority Attribute of Generated Resource Files

Change the authority attribute of files so that the access authority to the initial environment setup of the CORBA Service and directories/files generated dynamically during operation is restricted to the owner.

Restrict the access authority to files generated dynamically under /var/opt/FSUNod(Solaris) or /var/opt/FJSVod(Linux) to the owner.

#### 1. Change of the authority attribute of dynamically generated files

Change the authority attribute of files generated dynamically during operation of the CORBA Service. Make settings so that the owner becomes "specific user" and the write authority is restricted to the owner only.

```
#chown specific user dynamically generated file
#chmod 0644 dynamically generated file
```

#### Dynamically generated file

Target files dynamically generated are shown below.

```
Under /var/opt/FSUNod(Solaris) or /var/opt/FJSVod(Linux)
.log_pipe
.share
.named_pipe
Log
```

```
log.old
pid
```

## 2. Authority attribute change of the database storage directory of the interface repository

If an interface repository environment has been constructed by the initial environment setup (*isinit* or *odadmin* command) of the Interstage (CORBA Service) and the database administrator is other than root (default), the authority attribute of the database storage directory must be changed.

Set the owner of the database storage directory as the database administrator so that only the database administrator (owner) can hold the write authority.

```
#chmod 0755 database storage directory
#chown database administrator database storage directory
```

Use the database storage directory and database administrator specified when constructing (*isinit* or *odadmin* command) the interface repository in "database storage directory" and "database administrator".

Table A.3 Database Environment Setup Methods

	Initial Environment Setup Method	
	isinit command (Interstage operating environment definition file)	odadmin command (specified for executing the odadmin command)
Database storage directory	Setting to "IR path for DB file" <b>Solaris32/64</b> (default: /opt/FSUNtd/var/IRDB) <b>Linux32/64</b> (default: /opt/FJSVtd/var/IRDB)	Directory path <b>Solaris32/64</b> (default: /opt/FSUNod/IRDB) <b>Linux32/64</b> (default: /opt/FJSVod/IRDB)
Database administrator	Setting to "IR User Name" (default: root)	User name (default: root)

## 3. Changing the authority attribute for each operation log file

Change the authority attribute for each operation log file and storage directory. Set "specific users" for the owner, and configure the settings so that only the owner has write authority.

```
#chown specific user file
#chmod 0644 file
```

### **Solaris32/64**

(Default system)

/var/opt/FSUNod/opelog/opelog

/var/opt/FSUNod/opelog/opelog.old

/etc/opt/FSUNod/.odopelog\_locks

(Extended system)

/var/opt/FJSVisas/system/system name/FSUNod/var/opelog/opelog

/var/opt/FJSVisas/system/system name/FSUNod/var/opelog/opelog.old

/var/opt/FJSVisas/system/system name/FSUNod/etc/.odopelog\_locks

### **Linux32/64**

/var/opt/FJSVod/opelog/opelog

/var/opt/FJSVod/opelog/opelog.old

/etc/opt/FJSVod/.odopelog\_locks

```
#chown specific user Operation log storage directory
#chmod 0755 Operation log storage directory
```

#### Solaris32/64

(Default system)

/var/opt/FSUNod/opelog

(Extended system)

/var/opt/FJSVisas/system/system name/FSUNod/var/opelog

#### Linux32/64

/var/opt/FJSVod/opelog

## Effects on the User

- By the setting of the config file of the CORBA Service, execution of the application is limited to the specific users specified in `iss_uid` and other general users cannot execute the application. If a general user attempts to execute the application by mistake, ORB initialization (`ORB_init`) fails.
- If the database administrator of the interface repository is other than root (default) and "`iss_use=yes`" is set in the `irconfig` file, log information of the interface repository (database access function) is not collected even if the log information collection function is enabled ("`logging=yes`" in the `irconfig` file) (Log information of the cache server is collected).  
If "`iss_use=yes`" is set in the `irconfig` file, the `irlogdump` command (output/control of log information) must be executed with the administrator authority (root).

## A.2.2 Component Transaction Service

---

The Component Transaction Service can be used with the following products:

- Interstage Application Server Enterprise Edition

To operate the Component Transaction Service in a security-enhancing environment, the WorkUnit must be started by some specific user or superuser.

The command to set a specific user who is enabled to start the WorkUnit must be executed so that the Component Transaction Service can be started by this specific user or superuser. The specific user to be specified must be the same as the user of the user ID set to "`iss_uid`" in the CORBA Service operating environment file.

Make settings according to the procedure explained below.

In addition, when the multi-system function is being used, please carry out the procedure of security strengthening to all the systems on the server which performs security strengthening.

### A.2.2.1 Generating an Extended System

#### Solaris32/64

Use the `iscreatesys` command to create an extended system (required only for extending the system of the Enterprise Edition)

### A.2.2.2 Generating an Interstage System Definition File

Use the `isgendef` command to generate an Interstage system definition file.

For details on the generation of Interstage system definition file, refer to Generating an Interstage System Definition File in the Interstage Operator's Guide.

### A.2.2.3 Registering the Interstage System Definition File

Use the `isregistdef` command to register the Interstage system definition file.

For details on the registration of Interstage system definition file, refer to Registering the Interstage System Definition File in the Interstage Operator's Guide.

## A.2.2.4 Initializing Interstage

Use the *isinit* command to initialize Interstage.

For details on the initialization of Interstage, refer to Initializing Interstage in the Interstage Operator's Guide.

## A.2.2.5 Executing the Security-Enhancing Environment Setup Command

Execute the following command:

**Solaris32/64**

```
/opt/FSUNtd/bin/tdsecmode
```

**Linux32/64**

```
/opt/FJSVtd/bin/tdsecmode
```

The above command is valid once it is executed.

This command need not be re-executed even when Interstage is re-initialized.

By the *tdsecmode* command, following two can be specified as a strengthening level of security.

- level1

The security is enhanced as follows:

- The application operation authority during system operation is fixed to "specific user."
- The authority attribute of the resource file is restricted so that the resources (files and directories) generated during system operation will not be overwritten by a user other than the "specific user."

- level2

The authority attribute is restricted so that the IPC resources used by the packages related to the component transaction service will not be accessed by a user other than the "specific user" in addition to security strengthening of level1.

When applying by level2, the effective group of the "specific user" must be that of the super user that started Interstage.

Specify a level 2, in order to correspond to security strengthening environment.

For details on *tdsecmode*, refer to the Reference Manual (Command Edition).

In addition, a specific user can specify per system.

With the work up to here completed, the security-enhancing environment setup of the Component Transaction Service is completed.

### Note

Perform operation in the enhanced security environment in accordance with the following conditions:

- Commands that could be executed by only a superuser must be executed by a superuser.
- Commands that could be executed by a general user must be executed by a superuser or a specific user.
- If a command is executed by a specific user, specify the same effective group of the "specific user" as that of the super user that started Interstage.
- If a command that can be executed by a general user is executed by a user other than the specific user, an error may occur. In such a case, check whether the effective group of the "specific user" is the same as that of the super user that started Interstage.

## A.2.2.6 Notes

### 1. Notes when Executing the TD Compiler

The following explains work to be done when executing the TD compiler.

The TD compiler (*tdc* command) can be executed by only a specific user with the user ID set to "iss\_uid" in the CORBA Service operating environment file. If any other user attempts to execute the compiler, an access authority error of the TD compiler (*tdc* command) occurs.

If the following conditions are met, the following error message is output. Check the user ID:

## Conditions

1. Set a user ID other than that of the specific user specified in the enhanced security environment setting command (*tdsecmode* command) in "iss\_uid" in the config file of FSUNod.
2. Execute the TD compiler by the specific user specified in the enhanced security environment setting command.

## Output Message

UX:OD: error: IDL:CORBA/StExcep/UNKNOWN:1.0 occurred in the exception information of the od51401:IDLparser:CORBA\_ORB\_init function. The minor code is 0x464a0016. SYSTEM=xxxx) xxxx: variable information

## 2. Notes when AIM is Linked Solaris32/64

Be sure to register and delete a wrapper definition with the same user name.

If a wrapper definition is registered or deleted under the following conditions, the following event occurs:

### Conditions

- If a wrapper definition is registered to a superuser and then deleted by a specific user. or
- If a wrapper definition is registered to a specific user and then deleted by a general user. or
- If a wrapper definition is registered to a superuser and then deleted by a general user.

### Event

If the *delete* command (when *tdc -W* or *-delete* is specified) of a wrapper definition is executed, the following message is output:

UX:tdc: error: td32003: A system error occurred. error information (1003-81-13)

### Cause

Execution of the command failed because the wrapper definition registered by a superuser was attempted to delete by a specific user.

### Action

Re-execute the command by the user who registered the wrapper definition.

## 3. Notes when Registering/Updating WorkUnit Definitions

Be sure to register or update a WorkUnit definition by the user who starts the WorkUnit. The following event occurs if a WorkUnit definition registered or updated by a superuser is attempted to be started by a specific user.

### Event

If a WorkUnit start command (*isstartwu/tdstartwu* command) is executed, the following message is output to the console:

UX: extp errpr: EXTP2003: No access authority is granted to the parent directory or file: USER=%s1 FILE=%s2 SYSTEM=%s3  
(s1, s2, and s3 are variable strings)

### Cause

Execution of the command failed because the WorkUnit of the wrapper definition registered or updated by a superuser was attempted to started by a specific user.

### Action

Perform either of the following:

- Re-execute the command by a superuser.
- Delete the WorkUnit definition and then register it by a specific user before re-executing the command.

Moreover, carry out updating/deletion of a WorkUnit definition (at the time of execution of the *isaddwundef*, *tdadddef*, *isdelwundef*, and *tddeldef* commands) by the user who registered the WorkUnit definition.

## 4. Notes when an SMM Agent is Used

Be sure to execute a command (*isstartsmm*, *isstartsmma*, *isdisplaysmm*, *isaddtarget*, *isdeletetarget*, *isstopsmm*, *isstopsmma*) of the server machine status monitoring feature by a superuser.

Note that, if a command of the server machine status monitoring feature is executed by a user who is not a superuser, an access authority error occurs.

## 5. Notes when Linked to SystemWalker/OperationMGR

For WorkUnit operation from SystemWalker/OperationMGR, specify a specific user or superuser as a user who performs operations.

The strengthening level of security should be level2, and when operating by the specific user, specify the same effective group of the "specific user" that is a default setting at login as the effective group of the super user that started Interstage.

## 6. Notes when Interstage Operation API is Used

Execute applications that use any operation function (WorkUnit startup, WorkUnit stop, object closing, or object closure canceling) of the Interstage operation API with the authority of a specific user or superuser. In case the Interstage operation API is issued by the specific user, specify the same effective group of the user as that of the super user that started Interstage.

If this procedure is omitted, the following phenomena will occur when the Interstage operation API is executed:

[Initialization of Interstage operation API]

[API return value]

ISOP\_ESYSERR is reported as an execution result detailed value.

[Output message]

The following message is output in /var/log/messages:

UX : IS: ERROR: is20454:A system error occurred Error information(D 000ff:M 010b1:O 00004:F 10a:E -1)

[Execution of the information notification function or operation function of Interstage operation API]

[API return value]

ISOP\_ENOINIT is reported as a detailed execution result value.

(Because initialization of Interstage operation API environment will fail.)

[Output message]

No messages are output.

## 7. Notes when the Interstage Management Console is Used

To start the WorkUnit using Interstage Management Console, log in as a specific user for the startup.

If the Interstage Management Console is used to set up or start Interstage, execute the enhanced security environment setting command after setting up Interstage. Then start up Interstage using the Interstage Management Console.

If the Interstage Management Console is used to start a WorkUnit, log in to the system as a super user or specific user then perform operation.

An attempt to start up a WorkUnit by another user will cause the following error:

Case 1

If a WorkUnit is started by the super user and termination request is made by the specific user or another user, the following error message will be output:

UX:IS: error: is31057: This is not the user who started the work unit.

Case 2

If the WorkUnit definition registration is made by the specific user and the WorkUnit is started by a general user, the following error message will be output:

UX:IS: error: is31023: Work Unit unable to start : WU=Work Unit name

## 8. Notes on Command Execution

Commands that can be executed by a general user must be executed by a super user or a specific user. If a command is executed by the specific user, specify the same effective group of the user as that of the super user that started Interstage.

In case this procedure is omitted, the following phenomena will occur when a command is executed:

Table A.4 Execution Command Output

Execution command	Output message	
	Command reply message	/var/log/messages output message
When a WorkUnit is started by the <i>isstartwu</i> command:	UX : isstartwu: ERROR: is30153:A system resource shortage occurred	None
When a WorkUnit is stopped by the <i>isstopwu</i> command:	UX : isstopwu: ERROR: is30153:A system resource shortage occurred	None
When the <i>islistwudef</i> or <i>isinfwudef</i> command is executed:	UX : extp: ERROR: EXTP2003: Permission to access the file or parent directory is not granted:USER=%s1 FILE=%s2	UX : extp: ERROR: EXTP2003: Permission to access the file or parent directory is not granted: USER=%s1 FILE=%s2
When the <i>isresetretrycount</i> command is executed:	UX : isresetretrycount: ERROR : is31108: A memory shortage occurred: CODE='385'	UX : isresetretrycount: ERROR: is31108: A memory shortage occurred: CODE='385'
When the <i>islistwu</i> , <i>islistobj</i> or <i>isinfobj</i> command is executed:	UX : extp : ERROR: EXTP0690: A memory shortage occurred: CODE='UAPI 121 2'	UX : extp: ERROR: EXTP0690: A memory shortage occurred: CODE='UAPI 121 2'
When the <i>tdstartwu</i> , <i>tdstopwu</i> , <i>tdstandbywu</i> , <i>tdreleasewu</i> , <i>tdmodifyprocnum</i> or <i>tdmodifywu</i> command is executed:	UX : Command name: ERROR:td21002:An abnormality occurred in the command Reason code(50)	None
When the <i>tdlistwu</i> , <i>tdlstwu</i> , <i>tdlistobj</i> or <i>tdinfobj</i> command is executed:	UX : extp: ERROR: EXTP0690: A memory shortage occurred: CODE='UAPI 121 2' UX : Command name: ERROR:td24000:A memory shortage occurred	UX : extp: ERROR: EXTP0690: A memory shortage occurred: CODE='UAPI 121 2'
When the <i>tdstartsnap</i> , <i>tdstopsnap</i> , <i>tdlistwusnap</i> , <i>tdfreesnap</i> or <i>tdformsnap</i> command is executed:	UX : Command name: ERROR:td24501:A memory shortage occurred	None

Note

In the table, variable character strings in the message body are represented by %s1 and %s2. For details of the variable character string, refer to the Messages Manual.

**Solaris32/64**

For the output message of an extended system, a system name is added to the message text.

### A.2.3 Database Linkage Service

The Database Linkage Service can be used with the following products:

- Interstage Application Server Enterprise Edition
- Interstage Application Server Standard-J Edition

This section explains the case where resources are protected for operation of the Database Linkage Service.

1. Change to the root authority.

Change to the root authority because the subsequent processing requires the root authority.

2. By setup of CORBA service, set up so that a specific user may be set to root.
3. By setup of component transaction service, set up so that a specific user may be set to root.
4. If it is necessary, management to the resources protection shown below will be carried out.

The problem and solution about resources protection of Database Linkage Service (FSUNots package) in employment are explained.

## Problem

The resources (dumping file of OTS etc.) outputted to below by users other than root authority will be able to be destroyed.

Filename	User	Group	Perms
/var/opt/FSUNots	0	3	rwxrwxrwx

## Solution

The permission of the above-mentioned directory is changed by the *chmod* command.

```
chmod 755 /var/opt/FSUNots
```

## A.2.4 EJB Service

This section explains the case where resources are protected for operation of the EJB Service.

The following explains the required environment construction, how to operate the service, and security-enhancing command.

### A.2.4.1 Environment Construction Just After Installation

Construct an environment just after installation according to the following procedure:

1. Change to the Root Authority.

Change to the root authority because the subsequent processing requires the root authority.

2. Execute the Security-Enhancing Command.

Execute `/opt/FJSVejb/bin/ejbchangemode`. For details of the command, refer to Details of the `ejbchangemode` Command.

#### Example

```
> /opt/FJSVejb/bin/ejbchangemode
EJB package directory: /opt/FJSVejb
Temporary           : /tmp
Owner name          : root
Group name          : sys
Change mode         : Normal->Security
ejbchangemode:INFO:Terminated normally
>
```

### A.2.4.2 Environment Construction after Constructing an Environment for EJB Service Job Operation (Default System Only)

Construct an environment according to the following procedure after constructing an environment for EJB Service job operation:

1. Change to the Root Authority.

Change to the root authority because the subsequent processing requires the root authority.

2. Stop Interstage.

Use the *isstop* command to stop Interstage. When stopping it, be sure to specify the "-f" option.

3. Execute the Security-Enhancing Command.

Execute `/opt/FJSVejb/bin/ejbchangemode`. If an application storage folder has been changed, be sure to specify the PATH information of the application storage folder acquired by `ejbinfoapfolder` in an option argument. For details of the command, refer to Details of the *ejbchangemode* Command.

#### Example

```
> /opt/FJSVejb/bin/ejbchangemode
EJB package directory : /opt/FJSVejb
Temporary           : /tmp
```



```

Application folder      : /opt/FJSVj2ee/var/deployment/depoyed/ejbapp
Owner name             : root
Group name             : sys
Change mode            : Normal->Security
ejbchangemode:INFO:Terminated normally
>

```

### A.2.4.3 Environment Construction after Constructing an Environment for EJB Job Operation (Multi-System)

Construct an environment for the default system and extended system in according to the following procedure: It is not possible to construct a separate specific user environment for each system.

1. Acquire the System Information.

Use the *islistsys* command to acquire the system name.

#### Example

```

> islistsys
Default
system01
>

```

2. Change to the Root Authority.

Change to the root authority because the subsequent processing requires the root authority.

3. Stop Interstage.

Use the *isstop* command to stop Interstage in the default system and extended system. When stopping it, be sure to specify the "-f" option.

4. Execute the Security-Enhancing Command.

Execute */opt/FJSVejb/bin/ejbchangemode* each on the default system and extended system. If an application storage folder has been changed, be sure to specify the PATH information of the application storage folder acquired by *ejbinfoapfolder* in an option argument. Specify the system name in the "-M" option or environmental variable *IS\_SYSTEM*.

If the system name is specified both in the "-M" option or environmental variable *IS\_SYSTEM*, the system name specified in the "-M" option is enabled. If no system name is specified, the default system is assumed for operation.

For details of the command, refer to Details of the *ejbchangemode* Command.

#### Example of the extended system

```

> /opt/FJSVejb/bin/ejbchangemode -M system01
EJB package directory : /opt/FJSVejb
Temporary             : /tmp
System name           : system01
Application folder    : /var/opt/FJSVisas/system/system01/FJSVj2ee/var/deployment/depoyed/
ejbapp
Owner name            : root
Group name            : sys
Change mode           : Normal->Security
ejbchangemode: INFO: Terminated normally
>

```

### A.2.4.4 EJB Service Operation

Perform the job operation using the EJB Service according to the following procedure.

1. Change to the Root Authority.

Change to the root authority because the subsequent processing requires the root authority.

## 2. Set the File Mode Generating Mask.

Check the file mode generating mask. If "022" is not set, use the *umask* command to set "022".

### Note

The EJB Service generates files dynamically. Because files generated by Java depend on the file mode generating mask setting, settings must be made so that the write authority to "group" and "other" is not granted.

### Example

```
> umask
> 0          (022 is not set to the file mode generating mask)
> umask 022 (Set 022 to the file mode generating mask)
```

## 3. Start Interstage.

Use the *isstart* command to start Interstage.

## 4. Operate the EJB Service.

Use the EJB Service for job operation.

## Notes on EJB Service Operation

The following explains operations using the EJB Service.

- If the following error is output to the event log, the WorkUnit may have been started using a user ID without execution authority. Re-execute the command using a user ID with execution authority.

```
UX:extp: ERROR: EXTP4498: Some errors occurred: WU=EJB15WU USER=oracle SYSTEM=td001
```

```
UX:TD: ERROR: td11010: Work unit unable to start Reason code(ff)
```

- If the EJB package is uninstalled (pkgrm) while security is enhanced, files under /opt/FJSVejb are not deleted completely. Delete remaining files with the root authority.

### Example

```
> pkgrm FJSVejb
> rm -r /opt/FJSVejb
```

## A.2.4.5 Details of the *ejbchangemode* Command

The following explains details of the *ejbchangemode* command.

### Name *ejbchangemode*

Change the EJB Service operation to the specific user authority mode.

### Encoding format

```
ejbchangemode [-A <directory>|-T<directory>|-O<specific user ID>|-G<group>|-M<system name>]
```

### Description

Changes the EJB Service operation to the specific user authority mode to enhance security.

The following explains each of the *ejbchangemode* command arguments:

[-A]

If the application storage folder has not been changed, change the application storage folder so that it is prompted for operation of the specific user authority. If the specific user authority mode is changed just after installing the package, this option need not be specified.

<directory>

Specify an application storage folder. Specify a directory acquired by the *ejbinfoapfolder* command.

For details of the *ejbinfoapfolder* command, refer to the Reference Manual (Command Edition).

[-T]

Specify the directory to be used as a temporary work area by `ejbchangemode`. If this option is not specified, the default directory is used.

<directory>

Specify the directory to be used as a temporary work area by `ejbchangemode`.

[-O]

Specify the specific user ID for the EJB Service operation. If this option is not specified, the specific user name is made the root.

<owner>

Specify the specific user ID.

[-G]

Specify the group name for the EJB Service operation. If this option is not specified, `sys` is selected as the group name.

<group>

Specify a group.

[-M]

To perform operations on an extended system, specify the system name specified in the `iscreatesys` command. If this option is omitted, the default system name is used.

<sysname>

Specify a system name.

## Notes

Execute this command as a superuser while Interstage is stopped.

## Example

When the `ejbchangemode` command is executed, the following information is output:

1. Package directory whose specific user authority is to be changed
2. Directory used by the `ejbchangemode` command as a temporary work area
3. Specific user ID to be changed
4. Group ID to be changed
5. Information about the operation switching mode  
Normal->Security: switching from the normal operation mode to the specific user operation mode  
Security->Normal: switching from the specific user operation mode to the normal operation mode
6. Message indicating a normal end of the `ejbchangemode` command  
If "-A" is specified, information about the application storage folder is also displayed.  
If "-M" is specified, the system name is also displayed.

## Example

```
> /opt/FJSVejb/bin/ejbchangemode
EJB package directory: /opt/FJSVejb      ...1
Temporary              : /tmp            ...2
Owner name             : root            ...3
Group name             : sys             ...4
Change mode           : Normal->Security ...5
ejbchangemode:INFO:Terminated normally  ...6
>
```

## A.2.4.6 Details of the Output Messages

The following explains details of messages output by the *ejbchangemode* command.

### Message

ejbchangemode: INFO: Terminated normally

#### Meaning

The operation mode has been successfully switched to the specific user authority operation mode.

#### System action

Switched to the specific user authority operation mode.

### Message

ejbchangemode: ERROR: Specified invalid parameter: NAME=%s1

#### Variable information

%s1 = Option parameter passed as a command argument

#### Meaning

An invalid option parameter was specified.

#### System action

Stops switching to the specific user authority operation mode.

#### User action

Re-execute the command after specifying the correct option parameter.

### Message

ejbchangemode: ERROR: Not found EJB package directory: NAME=%s1

#### Variable information

%s1 = EJB Service directory

#### Meaning

No EJB Service directory is found.

#### System action

Stops switching to the specific user authority operation mode.

#### User action

Re-execute the command after installing the EJB Service.

### Message

ejbchangemode: ERROR: Not found EJB temporary directory:NAME=%s1

#### Variable information

%s1 = Temporary work area directory

#### Meaning

No temporary work area directory is found.

#### System action

Stops switching to the specific user authority operation mode.

#### User action

Take either of the following steps and then re-execute the command.

- Specify the temporary work area directory correctly.
- Do not specify the option "-T".

## Message

ejbchangemode: ERROR: Not found Application folder:NAME=%s1

### Variable information

%s1 = Application storage folder

### Meaning

No application storage folder is found.

### System action

Stops switching to the specific user authority operation mode.

### User action

Take either of the following steps and then re-execute the command.

- Specify the correct application storage folder. Execute the *ejbinfoapfolder* command during execution of the EJB Service and then specify the acquired PATH information.
- If no application storage folder is created, do not specify the option "-A".

## Message

ejbchangemode: ERROR: Specified invalid "-M" value: NAME=%s1

### Variable information

%s1 = System name specified in the option "-M"

### Meaning

An incorrect system name is specified.

### System action

Stops switching to the specific user authority operation mode.

### User action

Take either of the following steps and then re-execute the command.

- Specify the correct system name. Execute the *islistsys* command then specify the system name acquired from the displayed system list information.
- If no extended system is constructed, do not specify the option "-M".

## Message

ejbchangemode: ERROR: Not found directory: NAME=%s1

### Variable information

%s1 = Name of the directory in which switching to the specific user authority operation mode occurs

### Meaning

The following possibilities can be assumed:

- The EJB Service is not installed correctly.
- The extended system environment is not constructed correctly.

### System action

Stops switching to the specific user authority operation mode.

#### User action

Take either of the following steps and then re-execute the command.

- Install the EJB Service correctly.
- Construct the extended system environment correctly.

#### Message

ejbchangemode: ERROR: Specified invalid Environment "IS\_SYSTEM" value: NAME=%s1

#### Variable information

%s1 = System name specified in the environmental variable IS\_SYSTEM

#### Meaning

An incorrect system name is specified.

#### System action

Stops switching to the specific user authority operation mode.

#### User action

Take either of the following steps and then re-execute the command.

- Specify the correct system name. Execute the *islistsys* command and then specify the system name acquired from the system list information.
- If no extended system is constructed, do not specify the environmental variable "IS\_SYSTEM".

#### Message

ejbchangemode: ERROR: invalid EJB package directory: NAME=%s1

#### Variable information

%s1 = Name of the directory in which the EJB Service is installed

#### Meaning

The EJB Service is not installed correctly.

#### System action

Stops switching to the specific user authority operation mode.

#### User action

Re-execute the command after reinstalling the EJB Service.

#### Message

ejbchangemode: ERROR: Specified system name length exceeds limit

#### Meaning

The length of the specified system name exceeds the maximum value.

#### System action

Processing stops.

#### User action

Re-execute the command after specifying a system name that does not exceed the maximum number of bytes.

## A.2.5 Interstage JMS

---

The following explains the case where resources are protected in operation of Interstage JMS.

## A.2.5.1 Environment Construction

The following explains the required environment construction.

### Environment Construction for the Default System

Construct an environment for the default system according to the following procedure:

1. Stop all operating applications.
2. Change to the root authority.
3. Execute the security-enhancing command.

Execute `/opt/FJSVjms/bin/jmssetsecmode`.

Example

```
# /opt/FJSVjms/bin/jmssetsecmode secure -uid root -gid sys
```

### Environment Construction for an Extended System when the Multi-System Function is Used

Construct an environment for an extended system when the multi-system function is used after constructing an environment for the multiple systems according to the following procedure:

1. Stop all operating applications.
2. Change to the root authority.
3. Execute the security-enhancing command.

Execute `/opt/FJSVjms/bin/jmssetsecmode`.

Example

```
# /opt/FJSVjms/bin/jmssetsecmode secure -uid root -gid sys -M system1
```

### Notes

- By executing the security-enhancing command, execution of applications is limited to specific users and other users cannot execute the applications.
- If the security is enhanced together with other functions, the same specific user ID must be specified to construct an environment.

## A.2.6 Interstage Management Console

---

The following explains the case where resources are protected during operation of the Interstage Management Console.

Creation of the required environment and the security reinforcement command are explained.

### A.2.6.1 Environment Construction

The following explains environment construction immediately after installation.

1. Login in as a user with 'root' authority.  
'root' authority is required to execute the processing shown below.
2. Execute the security reinforcement command.

Execute the `/opt/FJSVisgui/bin/guiseemode` command.

```
# /opt/FJSVisgui/bin/guiseemode root
```

### A.2.6.2 Details of the `guiseemode` Command

The following explains details of the `guiseemode` command.

## Name `guisecmode`

Change the Interstage Management Console operation to the specific user authority mode.

## Encoding format

```
guisecmode ownername
```

## Description

This command enhances security for the operating environment of the Interstage Management Console.

The following explains each of the *guisecmode* command arguments:

`ownername`

Specify a specific user. To run the Interstage Management Console as a superuser only, specify the name of a superuser. A specific user can be specified in each system, but specify the directory that is used as the temporary work area in this case.

## Notes

- Only a superuser can execute this command.

## Example

Example of making the specific user 'user1':

```
guisecmode user1
```



# Appendix B Security Trends

This chapter describes security trends, implementations and recommendations for Application Server.

Since this information is release-specific, it may be subject to change.

## Encryption Algorithms

Due to ongoing research into encryption algorithm security and the availability of faster machines, encryption methods once considered secure can no longer be guaranteed. For this reason, the following algorithms should be avoided:

- MD5 algorithms
- RC2 encryption algorithms
- DES encryption algorithms

It is recommended that the following algorithms be changed to more robust algorithms where possible:

- RSAES-PKCS1-v1\_5 algorithms ("RSA encryption algorithms")
- SHA-1 algorithms
- 128-bit RC4 encryption algorithms
- 3-key Triple DES encryption algorithms

Consider the above encryption algorithms and those implemented by communication partner products before selecting appropriate encryption algorithms.

## SSL Protocol Version

The SSL2.0 protocol is known to have security problems. Switching to SSL3.0 and TLS1.0 has been recommended. However, to allow continued communication with third party products or Web browsers, some services are available to SSL2.0 communication.

Check the SSL protocol version that can be used in the service product and the service communication partners product. Ideally, this should be configured to prevent communication in SSL2.0.

## Certificate Reliability

Certificate reliability is guaranteed because it is issued by a CA you can trust. The CPS (Certification Practice Statement) is drawn up by the CA to detail operation policy and the responsibility range of the CA and to ensure reliability as a CA is maintained. The private key used for the certificate signature generally uses a tamper resistant device so that it cannot be stolen and is strictly managed. When the certificate is issued, reliability of the CA is also maintained by ongoing investigations such as identity checks on applicants.

In products and Web browsers that use certificates, trusted CAs certificates are incorporated. The VeriSign Inc. or Cybertrust, Inc. CA certificate is incorporated in Interstage Application Server.

Certificates generated for SSL encrypted communication with the Interstage Management Console and certificates generated using the *scsmakeenv* command for testing, however, are not issued based on rigorous CA applications. Certificate reliability and use responsibility is left to the judgement of the user or recipient of the certificate. It is recommended you use a certificate issued by a trusted CA.

It is recommended that you check the fingerprint of the CA certificate in advance and register the certificate in the Interstage certificate environment, certificate/key management environment, or Keystore before using it. If a CA certificate is forwarded to you during communication, check it and register it before using it in the manner described above.

If the reliability of the used certificate is low, the reliability of the encryption/signature that uses the certificate is also decreased. To operate the system securely, obtain a certificate from a trusted CA and use that certificate.

## Appendix C List of Certificates Integrated in Interstage

The certificates integrated in this version of Interstage are listed below. (\*1)

To register a certificate in a certificate environment, follow the procedure below:

- If the required certificate is in the list:

Register the certificates in the list.

- When using an Interstage certificate environment:

Use the *scsmakeenv* command with the *-c* option.

- When using a certificate/key management environment set up using an SMEE command:

Use the *cmsetenv* command with the *-rc* option.

For details on the *scsmakeenv* and *cmsetenv*, refer to the Reference Manual (Command Edition), section "SSL Commands" > "SSL Environment Setting Commands".

- If the required certificate is not in the list:

If a certificate not integrated in this version of Interstage is required, then check the CA site and obtain the CA or intermediate CA certificate, according to the advised procedure. After doing that, register the certificate:.

- When using an Interstage certificate environment:

Use the *scsenter* command.

- When using a certificate/key management environment set up using an SMEE command:

Use the *cmsetcert* command with the *-ca* option.

For details on the *scsenter* and *cmsetenv* commands, refer to the Reference Manual (Command Edition), section "SSL Commands" > "SSL Environment Setting Commands".

VeriSign, Inc.

Recipient	Expires
Class 3 Public Primary Certification Authority	2028/8/2 8:59:59
Verisign Class 3 Public Primary Certification Authority - G5	2036/7/17 8:59:59
Verisign Trust Network (Class 3 Public Primary Certification Authority - G2)	2028/8/2 8:59:59
VeriSign Class 3 Public Primary Certification Authority - G3	2036/7/17 8:59:59
VeriSign Universal Root Certification Authority	2037/12/2 8:59:59

Cybertrust, Inc.

Recipient	Expires
Baltimore CyberTrust Root	2025/5/13 8:59:00
GTE Cybertrust Global Root	2018/8/14 8:59:00