Interstage Application Server

V7.0

Smart Repository Operator's Guide

Trademarks

Trademarks of other companies are used in this operator’s guide only to identify particular products or systems:

Product	Trademark/Registered Trademark
Microsoft, Visual Basic, Visual C++, Windows, Windows NT, Internet Information Server, and Internet Explorer	Registered trademarks of Microsoft Corporation in the U.S.A. and other countries
Sun, Solaris, Java, and other trademarks containing Java	Trademarks of Sun Microsystems, Inc., in the U.S.A. and other countries
Linux	Registered trademark of Linus Torvalds in the U.S.A. and other countries
Red Hat, RPM and all Red Hat-based trademarks and logos	Trademarks or registered trademarks of Red Hat, Inc. in the U.S.A and other countries
UNIX	Registered trademark of the Open Group in the United States and other countries
Netscape, Netscape FastTrack Server, Netscape Enterprise Server, and Netscape Navigator	Registered trademarks of Netscape Communications Corporation in the U.S.A. and other countries
CORBA, Object Management Group, OMG, OMG IDL, IIOP, Object Request Broker, and ORB	Trademarks or registered trademarks of Object Management Group, Inc., in the U.S.A. and other countries
Interstage and ObjectDirector	Registered trademarks of Fujitsu Limited

This document contains technology relating to strategic products controlled by export control laws of the producing and/ or exporting countries. This document or a portion thereof should not be exported (or re-exported) without authorization from the appropriate government authorities in accordance with such laws.

Fujitsu Limited

First Edition (March 2005)
The contents of this manual may be revised without prior notice.

Interstage Application Server Plus
Interstage Application Server Enterprise Edition

Preface

Purpose of this Document

The purpose of this document is to explain the setup and operation of Smart Repository.

Who Should Read this Document?

This document is intended for the users of Smart Repository.

It is assumed that readers have a basic understanding of the following:

- The relevant operating system
- The Internet
- SSL
- LDAP and X.500
- C
- Java
- Java application development using JNDI

Organization of this Document

This Operator’s Guide is document is organized as follows.

- *Chapter 1 - Overview*

  This chapter explains the concepts such as the system configuration of Smart Repository, and the basics of the directory service. It also provides a functional overview.

- *Chapter 2 - Environment Setup*

  This chapter explains the environment setup for Smart Repository.

- *Chapter 3 - Entry Management*

  This chapter explains the management of entries in Smart Repository.

- *Chapter 4 - Operation and Maintenance*

  This chapter explains the operation and maintenance of Smart Repository.

- *Chapter 5 - Creating an Application (JNDI)*

  This chapter describes how to create an application (JNDI) using Smart Repository.

- *Appendix A - Manipulating a Repository in a Cluster Environment*

  Appendix A details the procedure for operating a repository in a cluster environment.

- *Appendix B - Error Codes*

  Appendix B describes the error codes of Smart Repository.

- *Appendix C – Smart Repository Object Classes*

  Appendix C describes the object classes handled by Smart Repository.

- *Appendix D - Smart Repository Attributes*

  Appendix D lists the attributes handled by Smart Repository.

- *Appendix E* - Search Filter

  Appendix E explains the search filters handled by Smart Repository.

Table of Contents

Chapter 1 Overview

Chapter 2 Environment Setup

Chapter 4 Operation and Maintenance

Appendix C Smart Repository Object Classes

Appendix D Smart Repository Attributes

Chapter 1

Overview

This chapter provides an overview of Smart Repository and its functions.

- Smart Repository
- Basic Knowledge of Directory Services and LDAP
- Features and Configuration of Smart Repository
- Major Functions of Smart Repository

Smart Repository

To deal with rapidly changing market environments, corporate users are integrating their information systems with Web services based on Internet technologies. To realize this goal, two elements are required: high-level security to authenticate and manage users, and reduced development and operation costs.

Smart Repository provides a directory service based on the Lightweight Directory Access Protocol (LDAP) that reduces operation, management, and development costs by enabling centralized control of resources instead of conventional distributed control.

Considerations for Integrating Web Services

It is natural, when building a corporate information system, to want to utilize existing resources (including systems and data) to reduce development costs and time. An integrated Web service based on Internet technologies is indispensable for corporate information systems as it lends itself to utilizing these resources.

However, the following issues must be considered before integrating a Web service:

- Integrated management, including the integration of departmental systems.
- Support for diversified users.
- Security.
- Increased operation and management costs.

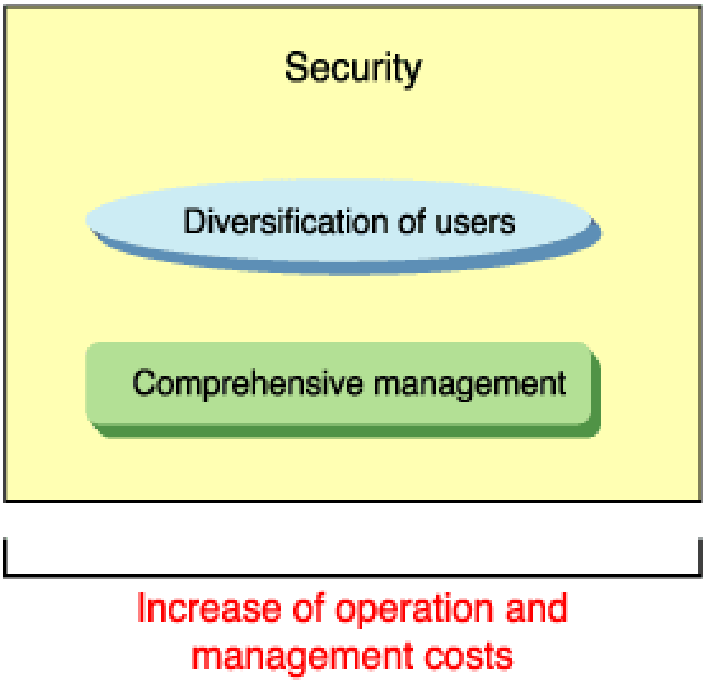


Figure 1-1 Problems of a Conventional System

Integrated management, including the integration of departmental systems

Under a Web service, numerous departmental systems are also integrated. However, various systems (for example, the personnel information system or business management system) are used by different people, all with differing levels of system access depending on their departments and positions.

Furthermore, in response to the rapidly changing market, the number of required information systems will increase, with users increasing accordingly.

System integration is ineffectual if users continue to be managed system by system.

Support for diversified users

The business environment of a company is drastically changing. This is evident in the shift from the traditional department-and-section system to a project team system, and the diversification of employment types to include loaned staff, part-time, contract, and temporary employees.

Additionally, companies increasingly disclose information to their customers via the Internet.

New information systems differ from traditional ones in that the types and levels of system users are fragmented. Managing fragmented users is, therefore, a major challenge of implementing a new information system.

Security

Security of information, including in-house and customer information is a high business priority. Businesses cannot over-emphasize the importance of providing adequate security for all of their data.

However, ensuring security for diversified users with varying access levels has become almost impossible through conventional solutions.

Increase of Operation and Management Costs

Offering convenience to an increasing number of diversified users, while also ensuring their security entails high development costs. Operation and management have also become major concerns in terms of both human resources and costs.

Advantages of Introducing Smart Repository

A directory service can help solve the problems mentioned above. Directory services provide the location and information for resources (such as Web servers, Web services, and user information) that are distributed over a system.

This type of integrated resource management will free individual systems from performing their own resource management.

Smart Repository provides a directory service based on the Lightweight Directory Access Protocol (LDAP), which is becoming increasingly recognized as a global standard.

Smart Repository offers features including operations on the Interstage Management Console; simplified entry administration; high reliability through replication, backup/restore, and access logs; automatic encoding of passwords; and security through SSL communications.

Using these features, Smart Repository can centrally control the resources of all integrated systems and customize settings for diversified users. User access permissions can therefore be carefully managed.

Automatic encoding of passwords provides thorough security.

When used in combination with the Interstage Single Sign-on, Smart Repository allows users to access Web servers and Web services to which they have permission using only one User ID and password. This maintains security and offers convenience.

These features will significantly reduce the system development and operation management costs.

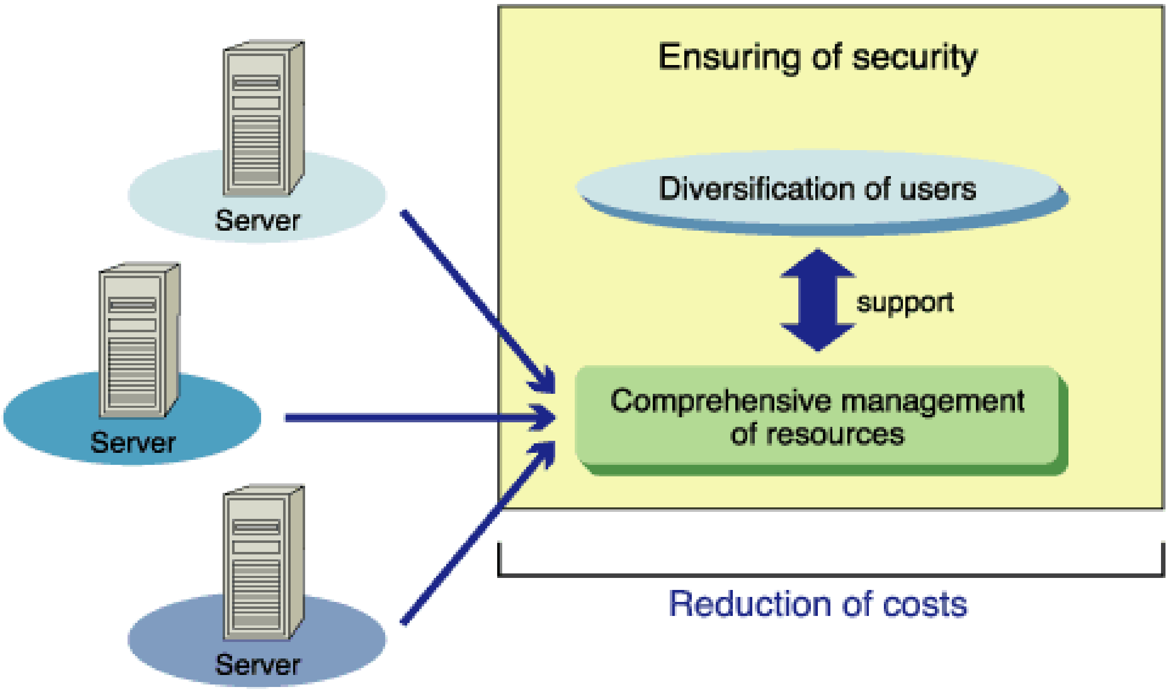


Figure 1-2 Benefits of Integrated Resource Management with Directory Services

Operating Modes

Smart Repository offers the following operation modes, depending on the particular objectives and considerations of your system (such as the system scale and the ensuring of high reliability).

Furthermore, each server can be operated in hot standby mode depending on the cluster.

Standalone Mode

In standalone mode, information is managed on one server.

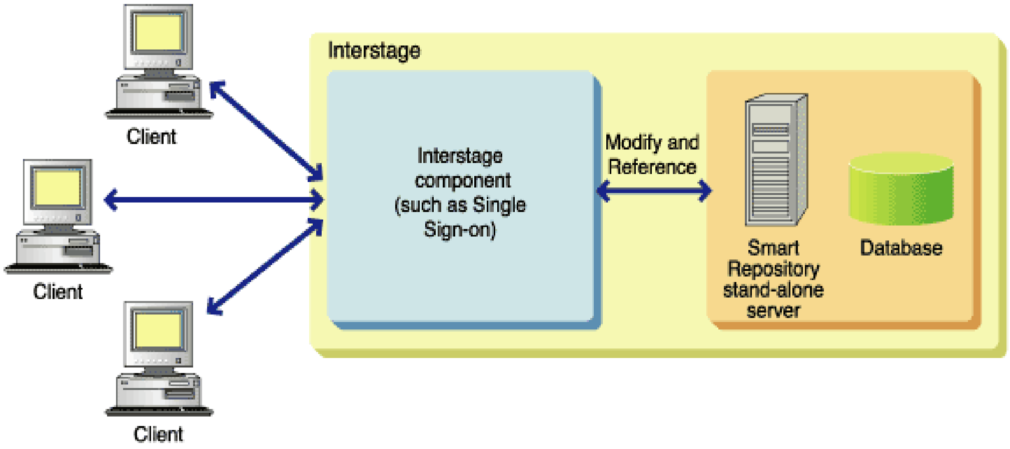

Client
Client
Client
Interstage
Interstage component (such as Single Sign-on)
Modify and Reference
Smart Repository stand-alone server
Database

Figure 1-3 Smart Repository Standalone Mode

Master/Slave (replication) mode

In this mode, one server acts as the master server and multiple slave servers replicate data from it. This mode not only alleviates the load concentration on the master but also enables the construction of a high-reliability system.

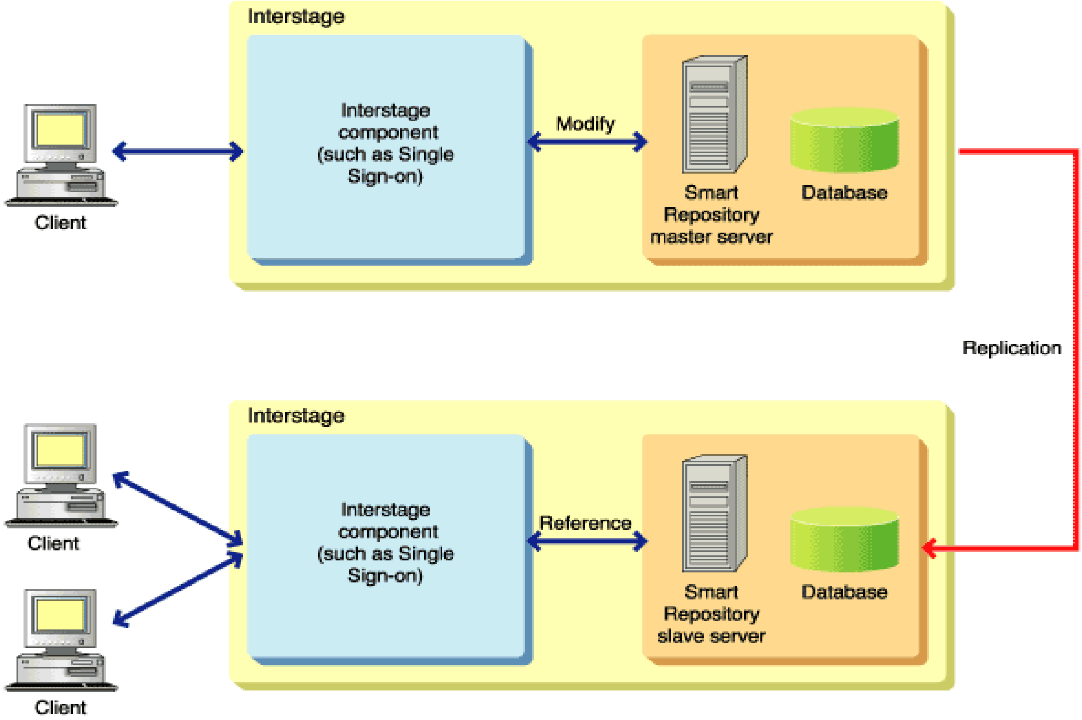

Interstage
Client
Interstage component (such as Single Sign-on)
Modify
Smart Repository master server
Database
Replication
Interstage
Client
Client
Interstage component (such as Single Sign-on)
Reference
Smart Repository slave server
Database

Figure 1-4 Smart Repository Replication Mode

Hot Standby Mode

In this mode, two servers are used: an operational server (operation control server) as well as a server standing by in case of an emergency (standby server). The servers share a disk and the data stored on it. If the operation control server fails (for example due to a hardware failure), its functions will be inherited by the standby server, from which the disk will be accessed. In this mode, based on the cluster service function, the system can continue operating without suspending the entire business operations.

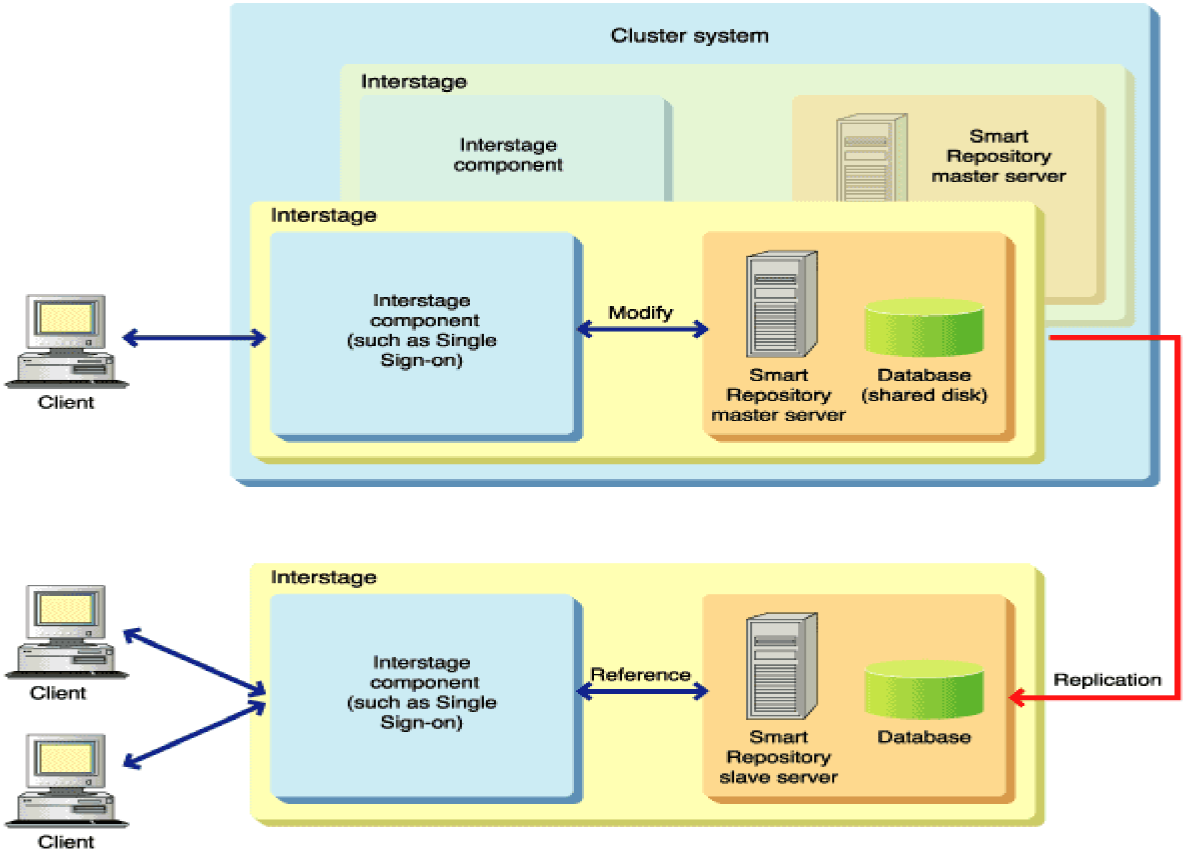

Cluster system
Interstage
Interstage component
Smart Repository master server
Interstage
Interstage component (such as Single Sign-on)
Modify
Smart Repository master server
Database (shared disk)
Client
Interstage
Client
Client
Interstage component (such as Single Sign-on)
Reference
Smart Repository slave server
Database
Replication
Client

Figure 1-5 Smart Repository Hot Standby Mode

Basic Knowledge of Directory Services and LDAP

This section provides basic information on the directory services required to use Smart Repository.

Directory Services

A directory service is used to efficiently navigate and manage access to information. Directory services associate physical (real) resources including systems, devices, and equipment with virtual namespaces managed by the directory service. This allows users to search for and reference necessary information and access systems, devices, and equipment using the location information provided.

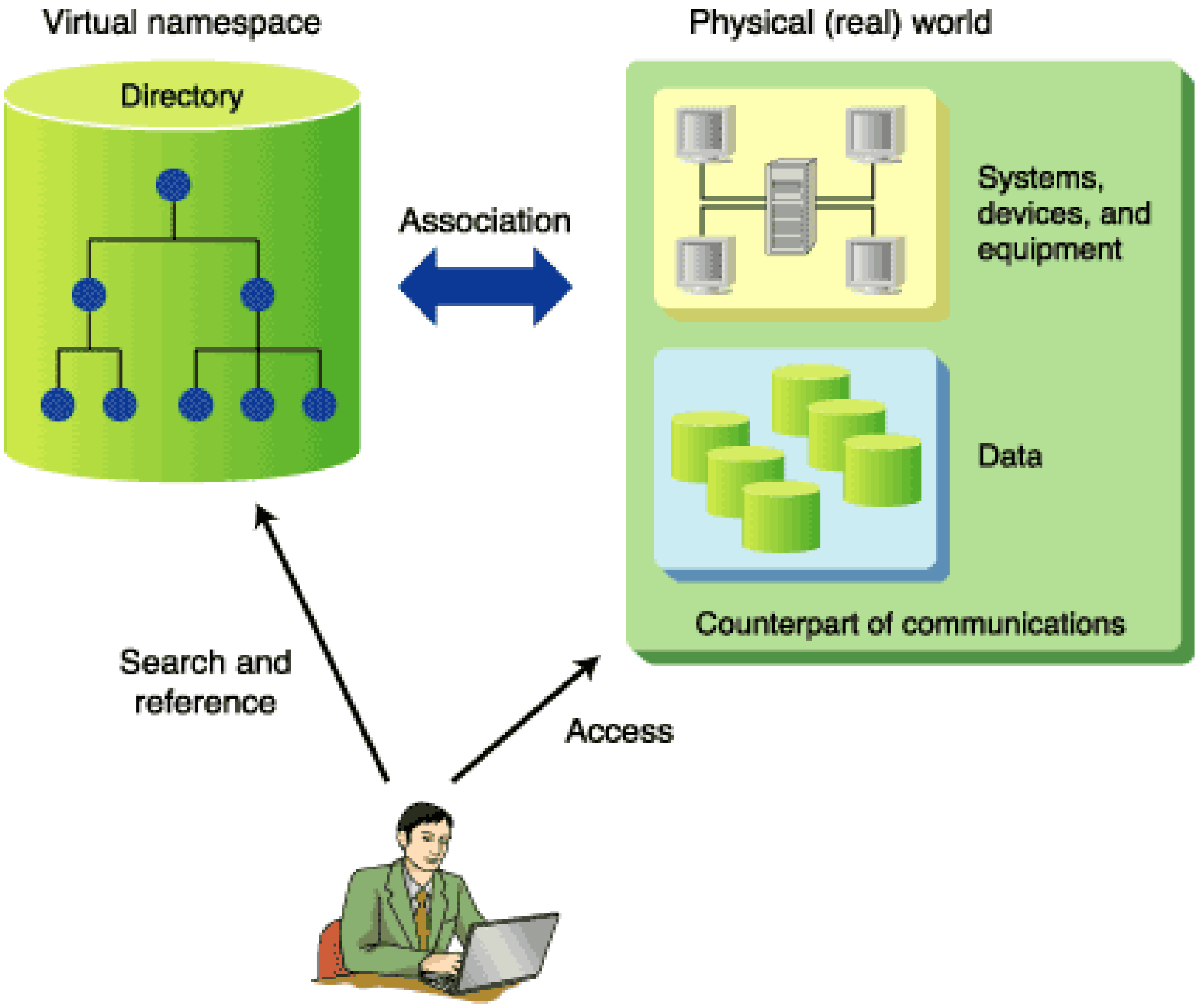


Figure 1-6 Directory Services

In Smart Repository, each system that manages the directory service information is called a 'repository.'

LDAP

A directory service was standardized and defined by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) in the 'X.500' specification.

Although X.500 is a highly versatile protocol, software developed based upon it tends to be large-scaled and thus has a higher development cost. The Lightweight Directory Access Protocol (LDAP) is a subset of essential X.500 functions that can be easily used in Internet technologies.

LDAP is an Internet-standard directory access protocol that runs on TCP/IP, which allows an LDAP client such as a browser to directly search for and reference data using a directory service.

LDAP Data Model

For ease of understanding, LDAP may be thought of as a hierarchical database.

In LDAP, a unit of information such as a person or organization is called an entry.

Entries are managed in a hierarchical fashion (in a tree).

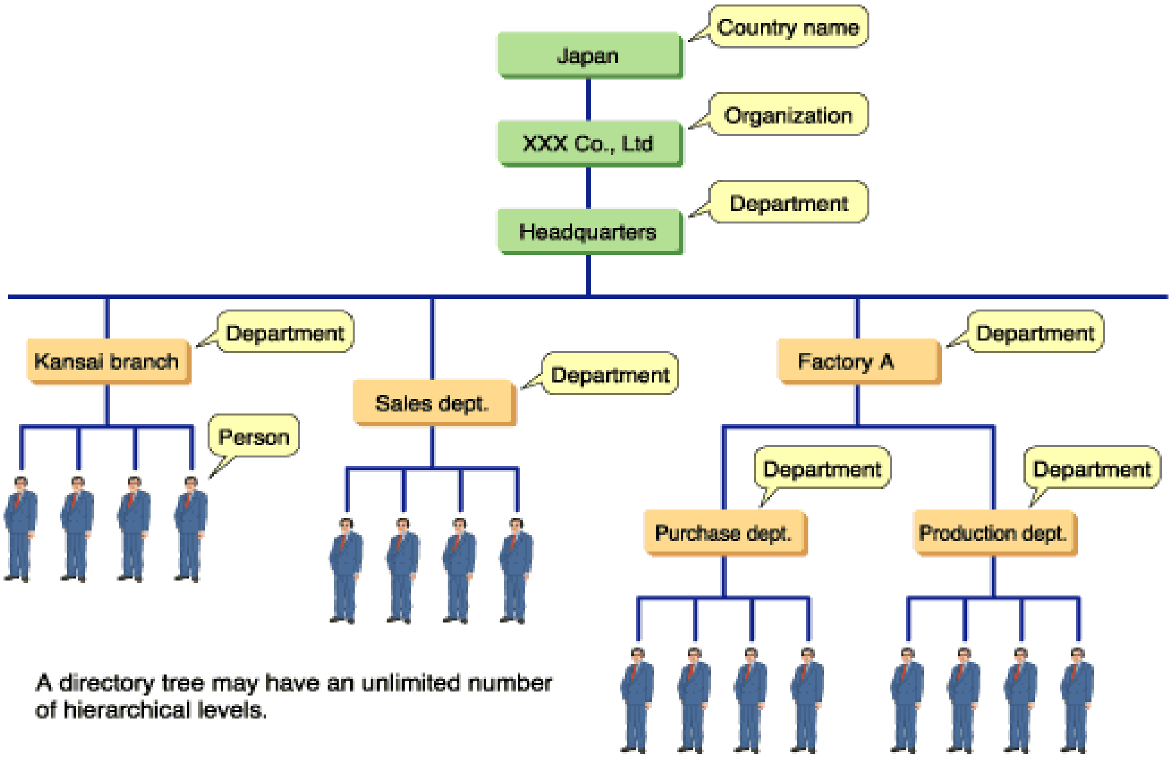


Figure 1-7 Hierarchical Directory Tree

The hierarchical structure of entries is called a 'Directory Information Tree (DIT).' A database storing a DIT is called a 'Directory Information Base (DIB).'

Entries are classified into the following types depending on their position in a DIT:

Root entry

An entry located at the top (root) of a DIT. A root entry, unique to a directory server, is a special entry with a different attribute value for each directory server.

Upper entry

An entry located above a particular entry.

Lower entry

An entry located below a particular entry.

Leaf entry

An entry without a lower entry.

Sub tree

A part of a DIT consisting of a particular entry and its lower entries.

Object and Object Class

In an entry, an 'object' is characterized by an 'object class' indicating an attribute of the information.

Entries are classified according to object classes. The following describes an object and an object class.

Attribute Type and Attribute Value

An object has an 'attribute type' representing its detailed item name and an 'attribute value' representing the actual value (content) of the item.

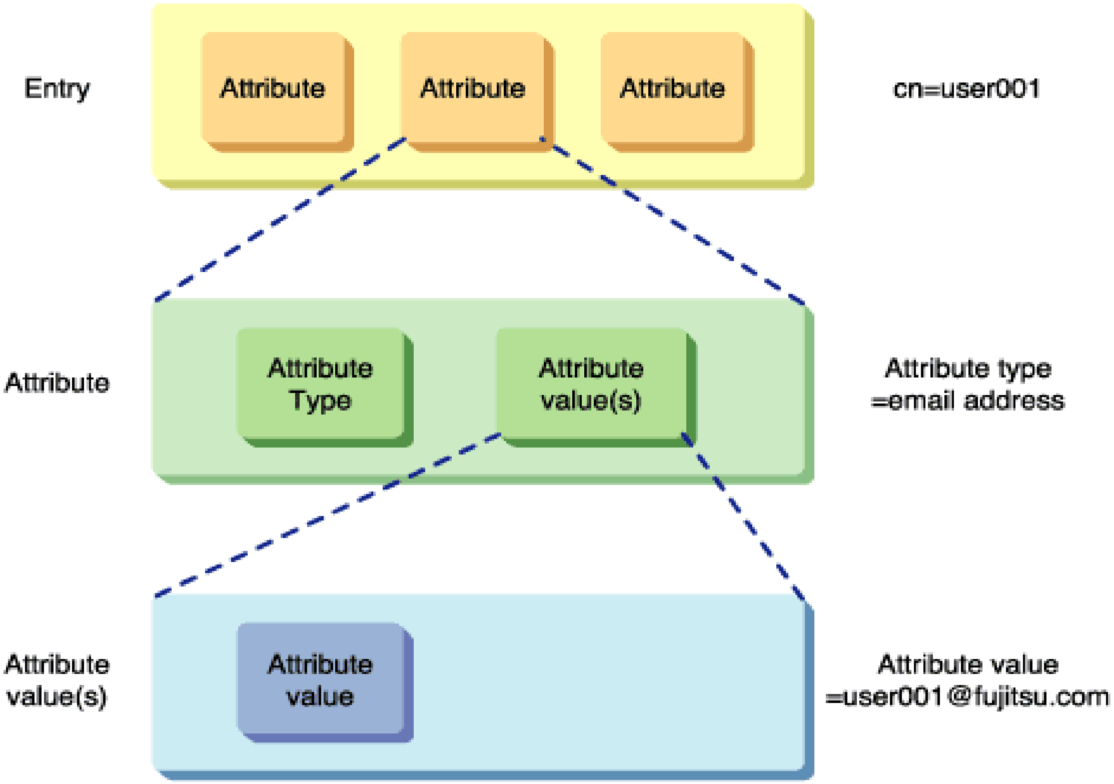


Figure 1-8 Attribute Types and Values

Distinguished Names of Entries

Entries have distinguished names, which consist of RDNs and DNs.

RDN (Relative distinguished name)

A name used to identify an entry's immediately lower entry. An RDN must be unique in its sibling relationship.

```
Example: "o=fujitsu"
```

DN (Distinguished name)

A name defined as a string of RDNs of the entry and its upper entries, representing an object. A DN must be unique in a DIT.

```
Example: "cn=user001,o=fujitsu,c=jp"
```

Smart Repository also has a special DN called an Administrator DN, which is used to manage a repository.

Schema

A set of definitions of data types (DIT structure, object class, and attribute) to be stored in a directory is called a 'schema'.

Basic Services of LDAP

Smart Repository supports LDAP V3 as an access protocol for use between a server and a client. LDAP V3 allows a user or a client to reference and modify the information in a directory.

The following lists the services provided by the directory. For more information, refer to Chapter 6 - 'Creating an Application (JNDI).'

- Bind

  To access a directory, you need to enter your DN and password information for authentication. However, no particular authentication is required to access a directory as anonymous (an anonymous user). In this case, the directory server will see you as an anonymous user.

- Unbind

  To close the connection to the directory server, you need to perform the unbind operation.

- Search

  To view information stored on the directory server, you can use the search operation.

- Compare

  The server will compare a password or other item with the information stored on it to check whether it is correct. Unlike search, no actual information will be displayed. This function can also distinguish entries that do not have a specified attribute value or attribute type.

- Add

  The add operation adds information to the directory server.

- Delete

  The delete operation deletes information stored on the directory server.

- Modify

  The modify operation modifies information stored on the directory server.

- ModifyDN and ModifyRDN

  When modifying a distinguished name, specify whether you want to delete the attribute values of the DN, new RDN, and old RDN of the entry being modified. To move an entry (and a sub tree), specify the DN of a new immediately upper entry.

- Abandon

  To stop searching for information on the directory server, perform the abandon operation.

Features and Configuration of Smart Repository

This section describes the features and configuration of Smart Repository.

Features of Smart Repository

Smart Repository has the following features.

- When Smart Repository is accessed using the API (for Java), the information needed by an application on the Application Server is easily stored in or searched from Smart Repository.
- The commands irepmodifyent, irepaddrole, ldapmodify, ldapsearch, and ldapdelete and the Entry Administration Tool are provided to facilitate search, add, delete, and modify operations in Smart Repository.
- The Interstage Management Console facilitates the construction of a repository.

Configuration of Smart Repository

This section describes the component configuration of Smart Repository.

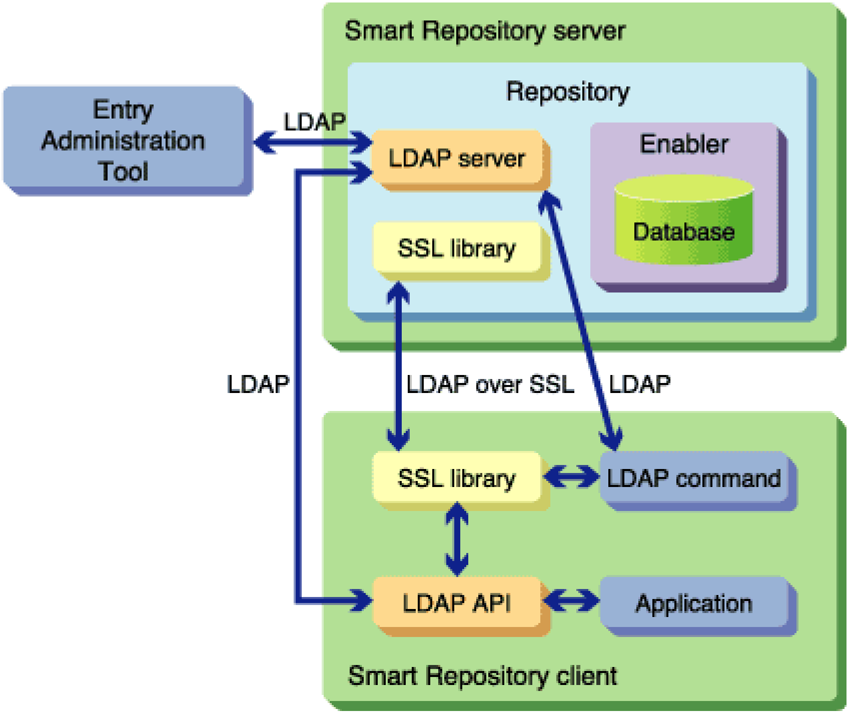


Figure 1-9 Smart Repository Component Configuration

Smart Repository Server

A Smart Repository server consists of the LDAP server and the Enabler.

LDAP server

A program that searches and stores information when it receives a request from an application through the LDAP API.

Enabler

A database that stores information. Fujitsu Enabler is used.

Smart Repository Client

A Smart Repository client consists of the LDAP-API and LDAP commands.

LDAP API (Java)

A library running on the Application Server to allow an LDAP application to access the Smart Repository server. The LDAP-API is available for Java.

LDAP commands

Commands that facilitate operations involving information on the Smart Repository server (search, add, delete, and modify).

Entry Administration Tool

A GUI-based tool that facilitates operations involving information on the Smart Repository server (search, add, delete, and modify).

Major Functions of Smart Repository

Smart Repository provides the following functions:

- Authentication
- Automatic encoding
- SSL communication
- Entry administration
- Replication
- Backup/restore
- Access log

Authentication

The Authentication function checks that only authorized users access Smart Repository. It therefore protects resources stored in Smart Repository from unauthorized access.

Before gaining access, users are required to enter their user entry information (user DN and password) stored in the database of Smart Repository.

Although the stored user passwords have been encrypted using the user password encryption method, users specify a plain text password for authentication.

Automatic Encoding

Smart Repository can store user authentication information for various applications. At this time, the password (userPassword attribute) can be encrypted as the entry information of the user. The encryption principle (user password encryption method) is specified when setting up the Smart Repository environment.

For information on how to specify a user password encryption method, refer to 'Managing the Repository Service' in Chapter 8 - 'Services' in the Operator's Guide.

User Password Encryption Method

In Smart Repository, a password (userPassword attribute) can be encrypted using the methods shown in Table 1-1. The passwords are then stored in the Smart Repository database.

Although if the user password encoding mothod that has been specified when the Smart Repository environment configuring is different to the user password encryption method of userPassword attribute which has been stored in the repository, the authentication process is distinguished in repository automatically.

Note

- Only a userPassword attribute can be encrypted.
- If a password registered in Smart Repository needs to be searched by its original, plain text format, select the Original encryption method.

Table 1-1 Password Encryption Methods

Encryption method	Description
Original encryption method	This method encrypts a password using the original encryption method, encodes it in Base64 format, and then stores it in the database. When a client program of Smart Repository submits the password, the password is decrypted into plain text.
MD5 method	This method encrypts a password using the irreversible MD5 encryption algorithm. The password is first converted into a 24-byte password, encoded in Base64 format, and prefixed with the ID characters '{MD5}' (to indicate that it has been encrypted using the MD5 method). It is then stored in the database. Using the MD5 method, the password specified by the client program of Smart Repository is encrypted to the same encryption password every time. If the password is submitted to the Smart Repository client program, the identification 'MD5' is added to the encrypted password.
SMD5 method	This method encrypts a password using the irreversible MD5 encryption algorithm. The password is first converted into a 28-byte password, encoded in Base64 format, and prefixed with the ID '{SMD5}' (to indicate that it has been encrypted using the SMD5 method). It is then stored in the database. If the password is submitted by a client program of Smart Repository, a different encrypted password will be generated using this method.
SHA method	This method encrypts a password using the irreversible SHA-1 encryption algorithm. The password is first converted into a 28-byte password, encoded in Base64 format, and prefixed with the ID '{SHA}' (to indicate that it has been encrypted using the SHA method). It is then stored in the database. If the same password is submitted by a client program of Smart Repository, the same encrypted password will be generated using this method.
SSHA method	This method encrypts a password using the irreversible SHA-1 encryption algorithm. The password is first converted into a 32-byte password, encoded in Base64 format, and prefixed with the ID '{SSHA}' (to indicate that it has been encrypted using the SSHA method). It is then stored in the database. If the same password is submitted by a client program of Smart Repository, a different encrypted password will be generated in this method.

Encryption method	Description
Crypt method Solaris OE Linux	This method encrypts a password using the irreversible Crypt encryption algorithm. The password is first converted into a 13-byte password, encoded it in Base64 format, and prefixed with the ID '{CRYPT}' (to indicate that it has been encrypted using the Crypt method). It is then stored in the database. Using this method, only the first eight characters of a password will be used to generate the encrypted password. Any characters after the first eight are ignored.
Plaintext	This method does not encrypt a password but stores it in plain text in the database. When a password is submitted by a client program of Smart Repository, a plain text password will be returned to the client.

SSL Communication

Data transmitted over a network may be stolen by a third party. SSL can be used to encrypt data before it is transmitted over a network to prevent eavesdropping and ensure safe communications.

SSL communications use the server authentication method in which a client that is about to communicate with Smart Repository will first check whether Smart Repository has a correct identity and then encrypt data before transmitting it.

Target of SSL Communications

Table 1-2 shows the communication paths used by Smart Repository for SSL communications.

Table 1-2 Communication Paths

Communication path	Target of SSL communications
Communications with a command	Encrypted communications may be performed between one of the following commands and a repository: - ldapsearch command - ldapmodify command - ldapdelete command
Communications with an application	Encrypted communications may be performed between a client application and a repository.
Communications in replication mode	Encrypted communications may be performed between a repository (master) and another repository (slave) in replication mode.

Note

When you use the Entry Administration Tool or an entry administration command (irepmodifyent), SSL communications cannot be performed on the communication path. Therefore, run the Entry Administration Tool or entry administration command in a sufficiently secure environment; for example, on the same computer as the repository.

For security measures, refer to 'Security Measures' in the Security System Guide.

Entry Administration

In Smart Repository, the following features are available to add an entry to the database or modify an existing entry.

- Commands
- Entry Administration Tool
- SDK

Furthermore, the commands and SDK allow you to specify special characters in a DN. The commands, Entry Administration Tool, and SDK allow you to specify character strings in both a DN and an attribute value.

Note

When an entry is modified, Smart Repository does not check the schema.

Therefore, incorrectly modifying an entry (for example deleting a required attribute in the entry, or incorrectly adding an attribute to an object class) causes conflict between items of information in the repository. Be careful when modifying an entry.

Operating an Entry

Commands

Manipulate the entry information of the repository using commands.

You can specify Japanese characters (Shift JIS and EUC) for these commands. You can also manipulate binary data (such as jpegPhotos) in an entry.

The following four commands are available:

- irepmodifyent
- ldapmodify
- ldapsearch
- ldapdelete

Of the above commands, ldapmodify, ldapsearch, and ldapdelete support the use of the SSL function, which secures communications.

For information on using the commands, refer to Chapter 15 - 'Smart Repository Operation Commands' in the Reference Manual (Command Edition).

Command Functions

The following describes the use of the commands:

Table 1-3 Command Descriptions

Command function	Description
Adding entry information	Add entry information to the repository using the irepmodifyent or ldapmodify command.
Modifying entry information	Modify entry information in the repository using the irepmodifyent or ldapmodify command.
Deleting entry information	Delete entries from the repository using the ldapdelete, irepmodifyent, or ldapmodify command.
Searching for entry information	Search for entries in the repository using the ldapsearch command.

For more information on the command functions, refer to 'Using the Command to Manage Entries' in Chapter 3, Entry Management.

Entry Administration Tool

The Entry Administration Tool is a GUI used to manage entries registered in the repository.

The Entry Administration Tool allows you to manipulate entries as described in Table 1-4:

Table 1-4 Entry Administration Tool

Manipulation of entries	Description
Adding an entry	To add an entry, bring up the window for adding an entry. Enter values to register an entry in the connected repository.
Modifying an entry	To modify an entry, bring up the window for modifying an entry. Enter values to modify an entry in the connected repository.
Deleting an entry	Select the entry that you want to delete and thus delete an entry from the connected repository.
Search	Search for an entry in the connected repository. Enter the required search conditions and start searching from the specified search start position. Entries extracted in the search will then be displayed. You can also modify, delete, or rename the extracted entries.
Rename	Select an entry in the connected repository and rename the entry.
Move	Move an entry in the connected repository.
Copy	Copy an entry in the connected repository.
Display mode	Change the mode in which data is displayed in the list view.
Display options	Set options of the display of the administration tool.

SDK

The SDK allows you to develop an LDAP application that accesses a Smart Repository server on an Application Server. The application may be developed in Java. For more information, refer to Chapter 6 - 'Creating an Application (JNDI).'

Entry Search

Entry search is performed as follows:

1. Narrow down information by specifying a search range.
2. For the attribute value of each entry in the search range, specify filtering criteria to extract the items that match the criteria.

The following describes search ranges and filters:

Search Range

Three levels of search are provided:

Search Range	Description
Base object search	Searches specified entry itself.
One level search	Searches the layer one level under that of specified entry.
Sub tree search	Searches the specified entry and all the layers under its layer.

Filter

The following five filters can be specified:

Filter	Description
Equal	Extracts items with an attribute value equal to the specified value.
Substring	Extracts items when the attribute value contains the specified substring. Forward matching, backward matching, arbitrary part matching, or any combination of these can be used in the substring.
Greater	Extracts items with an attribute value greater than the specified value.
Less	Extracts items with an attribute value less than the specified value.
Present	Extracts items with an attribute value.

In addition, by combining some of the above filters, more detailed filtering criteria can be specified. The following table contains the logical operations that are used to combine filters:

Logical Operation	Description
AND	Combine multiple filters with the logical product (AND) operation. Valid if all the criteria are true.
OR	Combine multiple filters with the logical add (OR) operation. Valid if any of the criteria is true.

Specifying a Special Character in a DN

To specify a special character in a command, SDK, or DN, it is necessary to either include a backslash (\) before the special character as an escape character or enclose the special character in double quotes (").

The following lists the special characters for which an escape character is needed.

- "," (Comma)
- "+" (Plus)
- """ (Double quote)
- "<" (Less than)
- ">" (Greater than)
- ";" (Semicolon)
- "#" (Hash) (only when it is specified as the first character of the DN)
- "/" (Slash) (only for JNDI)

Note

No escape character is required when you specify any other special character than shown above.

Example: Specifying a special character

Table 1-5 Special Characters

Example	Explanation
o="Fujitsu , Inc.", c=jp	The value of o, including a comma, must be enclosed in double quotes (").
o=\"Fujitsu\", c=jp	The value of o must be enclosed in double quotes ("). However, each double quote must have a backslash (\), before it as an escape character.
cn="user001 + sn=Fujitsu"	The two elements of the RDN need a plus sign between them as a connecting symbol
cn="user001 + Fujitsu"	The RDN, including a plus sign (+), must be enclosed in double quotes (").

Example

Examples of a DN containing special characters that require the escape treatment:

```
cn=a\b,o=Fujitsu, Inc.,c=jp
```

For a Command

For a command, it is necessary to apply the escape treatment to special characters, and enclose the attribute values that include the special characters with double quotes (").

```
cn="a\\b",o="Fujitsu\, Inc.",c=jp
```

For (JNDI)

Care needs to be taken for JNDI.

The backslash (\) functions as a special character in LDAP, JNDI, and the Java language Some examples of its use are shown below:

Suppose that a cn attribute containing \ is specified.

```
a\b
```

According to a rule of LDAP, it is necessary to apply the escape treatment to the backslash (\).

```
cn=a\\b
```

According to the JNDI specification, it is necessary to apply the escape treatment to each backslash (\) for the specification of this name.

```
cn=a\\\\b
```

According to the Java language specification, it is necessary to apply the escape treatment to each backslash (\) in order to specify this name as a literal.

```
String name1 = "cn=a\\\\\\\\b";
```

A comma (,) and double quote ("),need to be treated in the following ways, respectively:

```
String name2 = "cn=a\\\\,b";
String name3 = "cn=a\\\\\"b";
```

The specification of the first example in JNDI is as follows:

```
String name = "cn=a\\\\\\\\b,o=Fujitsu\\\\, Inc.,c=jp";
```

Replication

If information in the Smart Repository database is managed on one computer, database performance may deteriorate when it becomes large-scaled and the number of accesses increases.

The replication function provides load balancing in a large-scale configuration. This function allows the database of a server to be duplicated to another server.

Using the replication function, any entry modification made in Smart Repository (master), including adding, modifying, and deleting entries, will be reflected in another Smart Repository (slave).

Backup/Restore

In case of hardware and software faults, you can perform backup and restore the resources required to operate Smart Repository.

If the event of a fault, you can restore the environment from resources that you previously backed up, minimizing down time.

Access Log

The access log function collects Smart Repository. This function allows you to check whether any unauthorized access has occurred.

For more information, refer to 'Logs' In Chapter 4 - 'Operation and Maintenance.'

Chapter 2

Environment Setup

This chapter explains the environment setup required to use Smart Repository.

The environment for Smart Repository is set up using the Interstage Management Console.

Environment definitions such as the following can be set:

- General settings of the repository (such as public directory and Administrator DN)
- Detailed settings of the repository (such as database settings, access log settings, and replication settings)

To operate the Interstage Management Console, use the following window after starting the Interstage Management Console and logging in.

- To create a repository or define a replication environment:

  Select the [Create a New Repository] tab on the [Repository: View Status] window on the [System] > [Service] > [Repository]

- To reference or modify the simple or detailed settings of the repository:

  Select the Repository option on the Service menu, and then choose the repository name from the list in the [Repository: View Status] window on the [System] > [Service] > [Repository].

To operate the Interstage Management Console on Admin Server, use the following window.

- To create a repository or define a replication environment:

  Select the [Create a New Repository] tab on the [Repository: View Status] window on the [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]

- To reference or modify the simple or detailed settings of the repository:

  Select the Repository option on the Service menu, and then choose the repository name from the list in the [Repository: View Status] window on the [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository].

For information on the startup of the Interstage Management Console, see Chapter 2 - "Configuring the Interstage Management Console" in the Operator's Guide. For information on window operations of the Interstage Management Console, see Chapter 8 - "Services" in the Operator's Guide.

Flow of the Environment Setup

The environment setup for Smart Repository can roughly be divided into the following four parts:

- Design of a repository (data and tree design and operating mode decision)
- SSL communication environment setup (required only if SSL communication is used)
- Creation of a repository
- Registration of user information

Application development is common to both the stand alone mode and replication mode, however for operation in replication mode, environment setup for the slave server is needed.

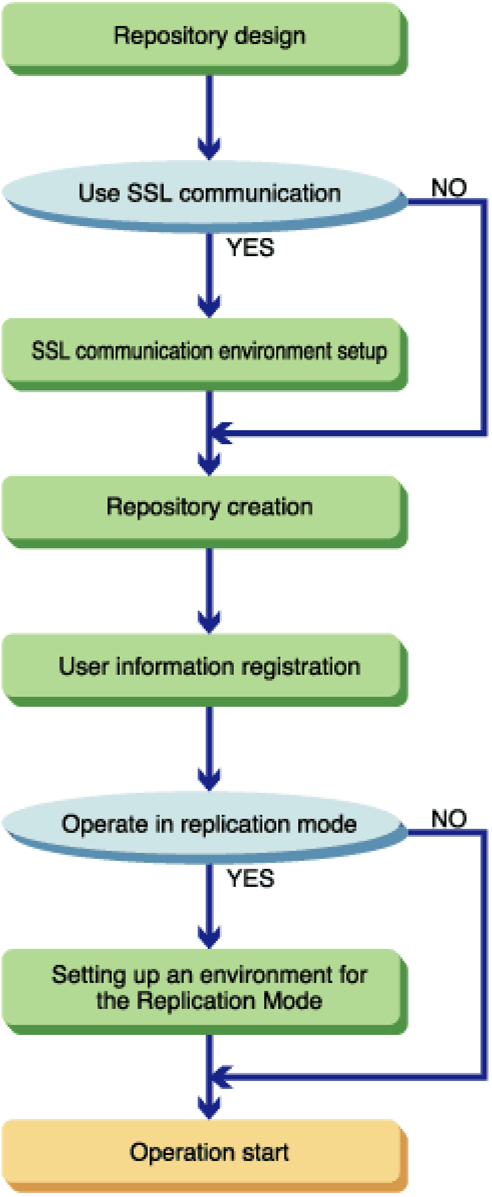

Repository design
Use SSL communication
NO
YES
SSL communication environment setup
Repository creation
User information registration
Operate in replication mode
NO
YES
Setting up an environment for the Replication Mode
Operation start

Figure 2-1 Environment Setup Flow

Table 2-1 lists the required environment setup for each operating mode:

Table 2-1 Environment Setup for Operating Modes

	Standalone mode without using SSL communication	**Standalone mode using SSL communication**	**Replication mode without using SSL communication**	**Replication mode using SSL communication**
Designing a repository	Designing a repository	Designing a repository	Designing a repository	Designing a repository
Setting up an environment for SSL communication		Setting up an environment for SSL communication		Setting up an environment for SSL communication
Creating a repository	Creating a repository	Creating a repository	Creating a repository (master server)	Creating a repository (master server)
Registering user information	Registering user information	Registering user information	Registering user information	Registering user information
Setting up an environment for the Replication Mode			Setting up an environment for the Replication Mode	Setting up an environment for the Replication Mode

To change Smart Repository in standalone mode to the replication mode, see Setting Up an Environment for the Replication Mode.

To add a slave server to Smart Repository in replication mode, see Setting Up an Environment for the Replication Mode.

To delete a slave server from Smart Repository in replication mode, see Procedure for Deleting a Slave Server during Replication Operation.

Designing a Repository

Design a repository before installing Smart Repository.

- Data design

  The following information is stored in the repository: user information such as the user name, password, and E-mail address and information about the organization to which the user belongs.

  Decide which data is to be stored.

- Tree design

  After deciding the data (entries) to be stored in the repository, define the hierarchical structure between entries and entry names.

- Operating mode design

  Smart Repository provides two operating modes: standalone mode in which information is managed by one computer and replication (master/server) mode in which one computer is designated as the master server (modification system) and multiple slave servers (reference systems) are arranged to replicate data from the master server.

  Decide also whether to use SSL communication.

Designing Data

Decide on the data to be stored in the repository.

The repository is generally used for information searching (similar to a telephone directory) and management of users of the Web server.

Since the repository is suitable for reference (information search), do not store the following types of data in the repository:

- Data that is frequently modified (overwritten)
- Large data, such as image and audio data
- Data with a large number of attributes per unit of data (entry)

By considering not only the current data needs, but also the data that may be needed in the future, the required database capacity and future expansion requirements can be estimated more easily.

Designing a Tree

Decide the structure of the directory information tree such as the hierarchical structure between entries and entry names.

Consider the following three points:

- Entry name

  Each entry name in the repository must be unique. Use one or more attribute values for the entry name. The cn attribute (name), for example, is generally employed as the user entry, but if there are two or more users with the same name, it will not be unique. In that case, use the uid (user ID) attribute or employeeNumber (employee number) attribute.

  Note

  A DN identical to the "Administrator DN" cannot be used as an entry name.

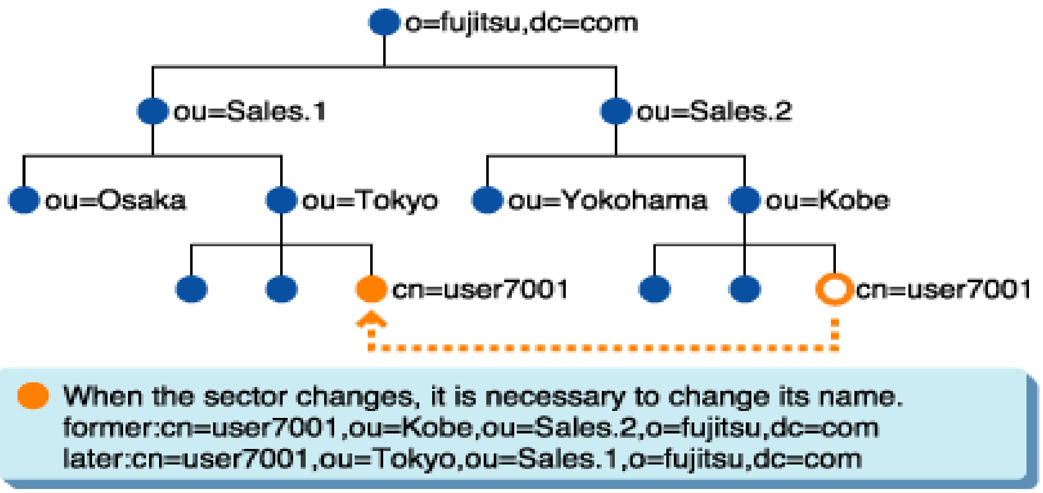
- Tree root (public directory)

  Entry at the top (root) of a tree. This entry is specific to the repository and all other entries are stored under this entry. Any attribute can be used as the root entry name, but it is recommended to use the domain name (dc(domainComponent)), organization (o(organization)), and country (c(country)).

- Relationship between entries

  Make the hierarchical structure of a tree as shallow and flat as possible. This is because any name change should be avoided. Do not use an organization name or department name of a company at a branch point, because organization names may be changed. Name changes can be avoided if entries are divided into "user information," "service," and so on.

  Figure 2-2 below. illustrates the complications of changing names within complex hierarchies.



● When the sector changes, it is necessary to change its name.
former:cn=user7001,ou=Kobe,ou=Sales.2,o=fujitsu,dc=com
later:cn=user7001,ou=Tokyo,ou=Sales.1,o=fujitsu,dc=com

Figure 2-2 Change Sector Details in a Complex Tree

In Figure 2-3, since the tree is of a flat structure, changing the sector details does not involve a complex name change.

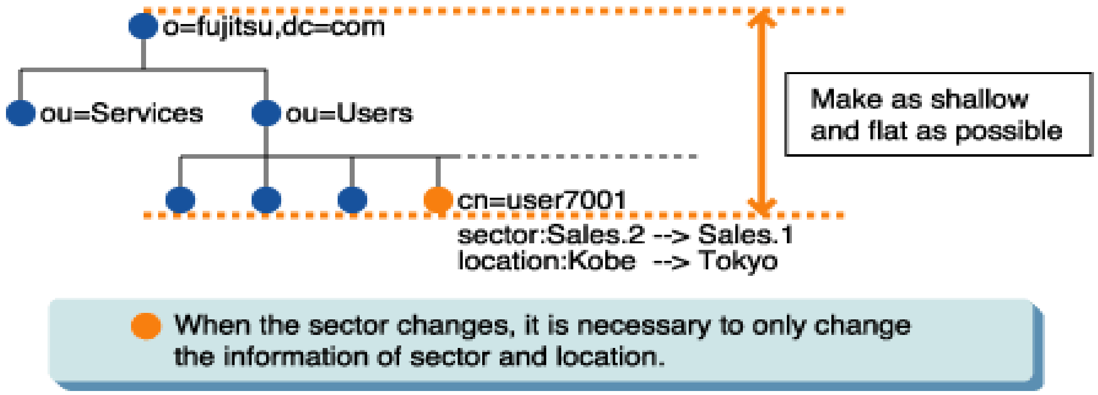

o=fujitsu,dc=com
ou=Services
ou=Users
cn=user7001
sector:Sales.2 --> Sales.1
location:Kobe --> Tokyo
Make as shallow and flat as possible
When the sector changes, it is necessary to only change the information of sector and location.

Figure 2-3 Change Sector Details in a Flat Tree

Choosing the Operating Mode

System Configuration Decision

The operating mode in which one server is used to manage information in the Smart Repository database is called the standalone mode.

As a standalone system grows, so does the number of system accesses. As a result of this, performance may suffer. The replication function is provided to balance the load in large-scale configurations. Using replication, copies of the server database are created on separate servers with client requests divided between them.

To install the replication mode, it is necessary to set up both the master server that can perform updates of information (such as addition, modification, and deletion) and slave servers that maintain copies.

When using a cluster environment for replication operation, see Appendix A: "Manipulating a Repository in a Cluster Environment."

Smart Repository Environment Setup Sheet for Replication Operation

A Smart Repository environment setup sheet (Excel file) is available to assist the configuration of the Interstage Management Console during the replication operation setup. This file is stored in "ApplicationServer\tuning" in Manual CD.

If Microsoft(R) Excel 97 or a later version has been installed, design a replication operation using the file "SR_repli.xls." For details on how to use it, see the explanation within that file.

Conditions for Using the Smart Repository Environment Setup Sheet

The Smart Repository environment setup sheet is a file that can be used if Microsoft(R) Excel 97 or later has been installed.

Since the setup sheet uses macros, before using it, enable the macros by setting the security level of Microsoft(R) Excel. For details on how to set the security level, see the Microsoft(R) Excel Help. Consult the security Administrator before changing the security level.

The following procedure describes how to set the security level to use the sheet in Microsoft(R) Excel 2002.

1. Start Microsoft(R) Excel 2002 and select [Macros] and then [Security] from the Tools menu.
2. The Security window will display. Select the radio button [Medium] on the [Security level] tab.
3. Click the [OK] button.
4. Shut down Microsoft(R) Excel and then restart it.
5. Select [Open] from the File menu, browse to the Smart Repository environment setup sheet, and select it.
6. If the Enable Macros dialog box displays, click the [Enable macros] button to enable the macros.
7. Restore the macro security level to its original level as required.

Note

- Replication mode cannot be set up using multiple repositories on the same machine.
- Set up multiple slave repositories with the same master repository on the same machine is unsupported.
- Configure the master machine and the slave machine with same platform.
- Build master machine and slave machine using the same version.

Decision Whether to Use SSL Communication

Under the initial setup, when clients request processing from Smart Repository, the distinguished name (DN), password, and other communication data are used without encryption. This also applies to communication between the master server and slave servers when replication is used.

SSL communication is used to encrypt data sent in the transmission lines. SSL encryption protects data from the threats of decryption and eavesdropping, even if the communication lines are monitored.

If client authentication is used, access to the SSL server is permitted only to those SSL clients who present a certificate issued by a specific CA, preventing access of clients who disguise themselves.

If the number of clients is large and access to Smart Repository is frequent, it is recommended to reduce the server load by using the SSL accelerator to ensure response performance.

An SSL communication environment needs to be set up before creating a repository.

Setting up an Environment for SSL Communication

An SSL communication environment needs to be set up to enable encrypted communication between the client and server in both standalone and replication operations.

To conduct SSL communication between the master server and slave server in replication operation, set up an SSL environment on the master server and configure the relevant SSL information on the slave servers involved in SSL communication. Under replication, it is possible to conduct SSL communication either between client and server or between master server and slave server, or both.

Note

Install the Application Server as the management target server for construction of the SSL communication environment in the Admin Server. For details of the Admin Server and Managed Server, refer to Chapter 5 - "Site" in the Operator's Guide. For details about installing the Application Server, refer to "Installation Information".

Setup of an SSL Communication Environment (Between Client and Server)

Smart Repository is intended to allow SSL communication for the following clients:

- Smart Repository LDAP command (ldapsearch, ldapmodify, and ldapdelete commands)
- User applications that access the Smart Repository server

Set up an SSL communication environment according to the following procedure:

- Server
  1. Setup of an Interstage certificate environment ((1) to (5) in the following figure)
  2. Implementation settings to use the certificate ((6) in the following figure)

The following flow diagram illustrates how to set up an SSL communication environment for the server.

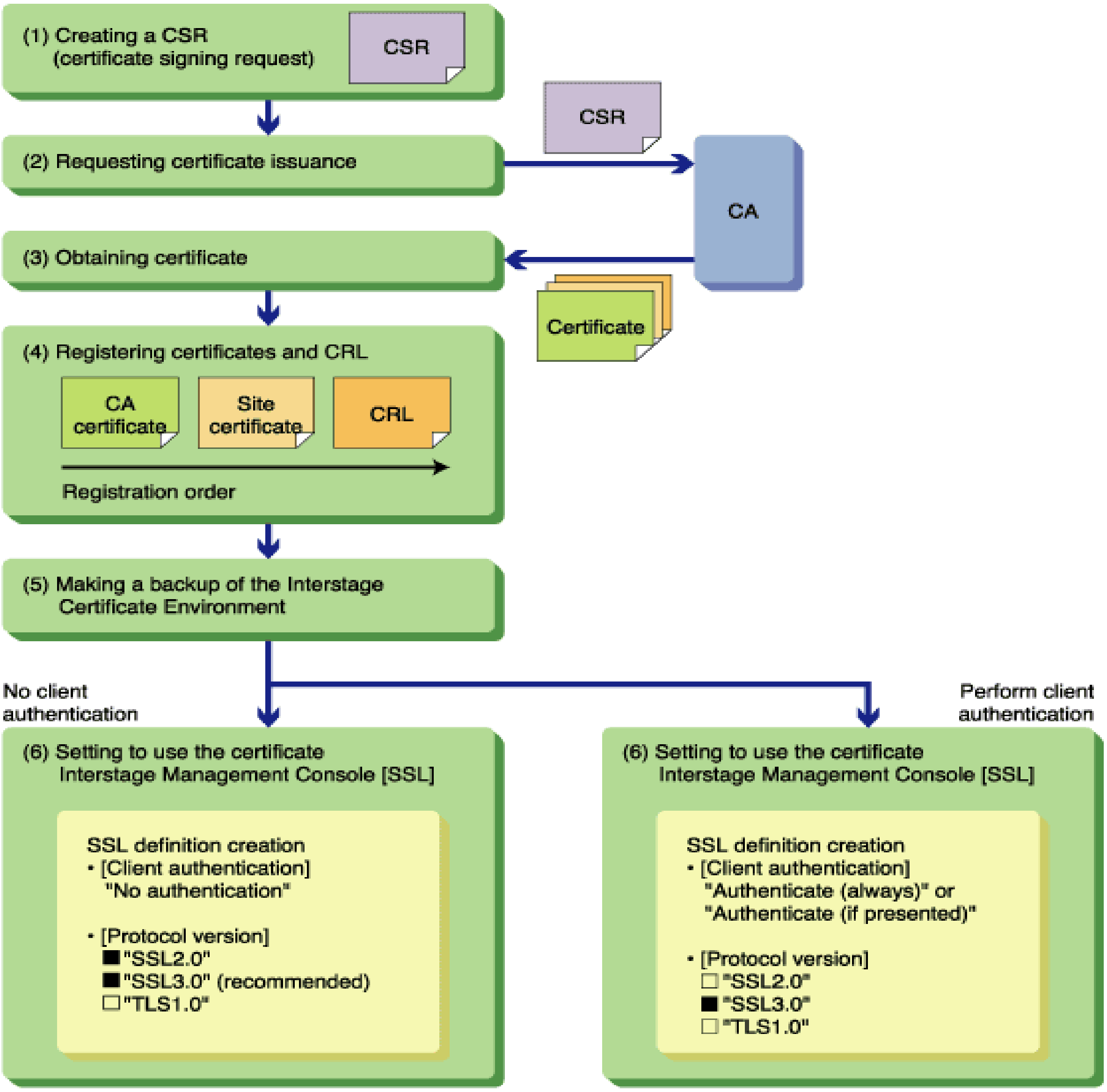

(1) Creating a CSR
(certificate signing request)
CSR
CSR
(2) Requesting certificate issuance
CA
(3) Obtaining certificate
Certificate
(4) Registering certificates and CRL
CA certificate
Site certificate
CRL
Registration order
(5) Making a backup of the Interstage Certificate Environment
No client authentication
Perform client authentication
(6) Setting to use the certificate
Interstage Management Console [SSL]
SSL definition creation
• [Client authentication]
"No authentication"
• [Protocol version]
■"SSL2.0"
■"SSL3.0" (recommended)
□"TLS1.0"
(6) Setting to use the certificate
Interstage Management Console [SSL]
SSL definition creation
• [Client authentication]
"Authenticate (always)" or
"Authenticate (if presented)"
• [Protocol version]
□"SSL2.0"
■"SSL3.0"
□"TLS1.0"

Figure 2-4 Server Communication Environment Setup

- Client
  1. Creation of a certificate/key management environment ((1) in the following figure)
  2. Creation of a private key and acquisition of a certificate ((2) to (4) in the following figure)
  3. Registration of the certificate and CRL ((5) to (6) in the following figure)
  4. Setting of the SSL environment definition file ((7) in the following figure)
  5. Encryption of the user PIN ((8) in the following figure)

Figure 2-5 illustrates the set up of an SSL communication environment for the client.

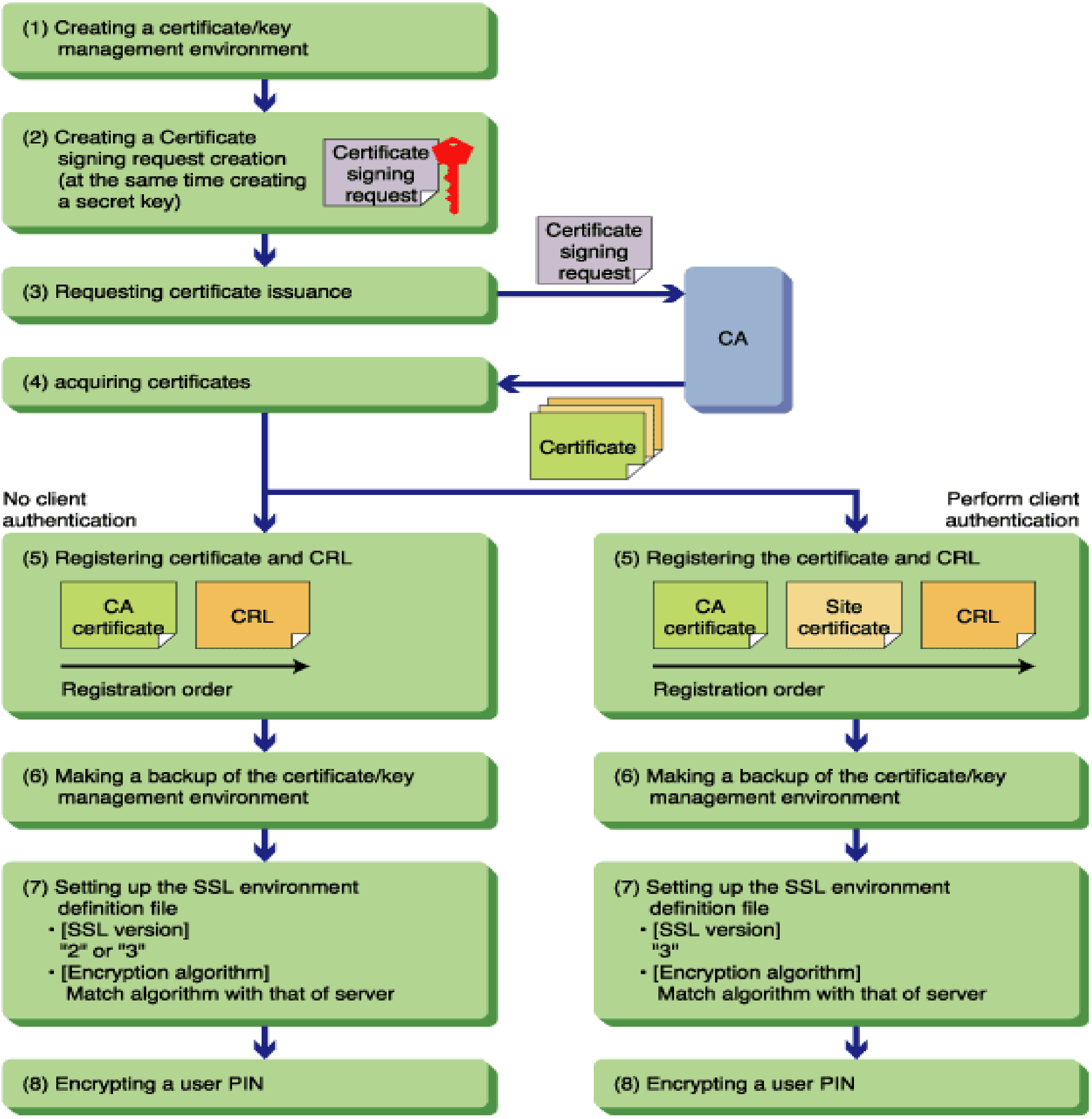

(1) Creating a certificate/key management environment
(2) Creating a Certificate signing request creation (at the same time creating a secret key)
Certificate signing request
(3) Requesting certificate issuance
Certificate signing request
CA
(4) acquiring certificates
Certificate
No client authentication
Perform client authentication
(5) Registering certificate and CRL
CA certificate
CRL
Registration order
(5) Registering the certificate and CRL
CA certificate
Site certificate
CRL
Registration order
(6) Making a backup of the certificate/key management environment
(6) Making a backup of the certificate/key management environment
(7) Setting up the SSL environment definition file
• [SSL version] "2" or "3"
• [Encryption algorithm] Match algorithm with that of server
(7) Setting up the SSL environment definition file
• [SSL version] "3"
• [Encryption algorithm] Match algorithm with that of server
(8) Encrypting a user PIN
(8) Encrypting a user PIN

Figure 2-5 Client Communication Environment Setup

Conducting Encrypted Communication Using SSL in Replication Operation

To conduct encrypted communication using SSL in replication operation, set up an SSL environment on the master server and configure the relevant SSL information on the slave server involved in the SSL communication.

Note

Do not modify the used SSL configuration or its content during replication. Modifying the SSL configuration during replication may prevent successful operation.

Procedure for Setting up an SSL Communication Environment for the Slave Server

Note

- Do not specify a test certificate in the SSL configuration used by the repository of the slave server.

Set up an SSL communication environment for the slave server according to the following procedure:

1. Setup of an Interstage certificate environment
2. Implementation of settings to use the certificates

For more details, see the procedure for "Server" described in Setting up an Environment for SSL Communication.

Procedure for Setting up an SSL Communication Environment for the Master Server

Performing No Client Authentication

Note

- It is necessary to use the same CA certificate and CRL as those obtained when setting up an SSL communication environment for the slave server.

Set up an SSL communication environment for the master server according to the following procedure:

1. Setup of an Interstage certificate environment ((1) and (2) in the following figure)
   - Create a site certificate for testing.
   - Nickname of the site certificate for testing: testCert
   - Name: repository.fujitsu.com
   - Organization unit name: Interstage
   - Organization name: Fujitsu Ltd.
   - City name: Yokohama
   - Prefectural name: Kanagawa
   - Country code: jp

```
scsmakeenv -n testCert
Password:   (*1)

Input X.500 distinguished names.
What is your first and last name?
[Unknown]:repository.fujitsu.com   (*2)
What is the name of your organizational unit?
[Unknown]:Interstage   (*2)
What is the name of your organization?
[Unknown]:Fujitsu Ltd.   (*2)
What is the name of your City or Locality?
[Unknown]:Yokohama   (*2)
What is the name of your State or Province?
[Unknown]:Kanagawa   (*2)
What is the two-letter country code for this unit?
[Un]:jp   (*2)
Is <CN=SiteName.domain, OU=Interstage, O=Fujitsu Ltd., L=Yokohama,
ST=Kanagawa, C=jp> correct?
[no]:yes   (*3)
SCS: INFO: scs0102: Self-sign certificate was issued
```

*1. Enter the password. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*2. For the content to be entered, see the "Reference Manual (Command Edition)."

*3. If the displayed content is correct, enter "yes." To re-try the input, enter "no."

4. Setting to use the certificates ((3) in the following figure)

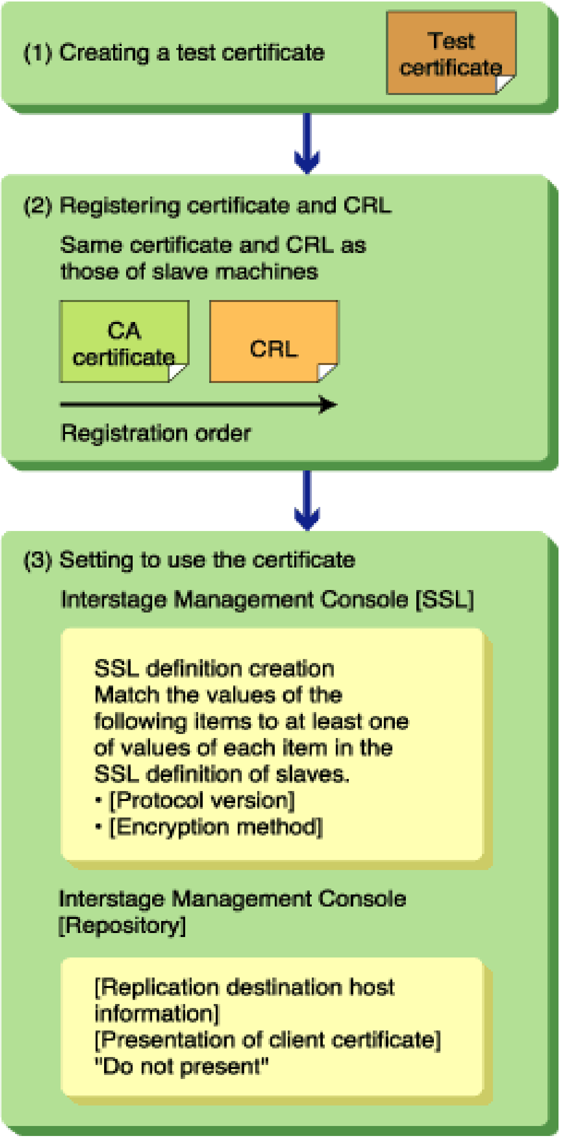
   Certificates registered in the Interstage certificate environment can be referenced by selecting [System] > [Security] > [Certificate] > [CA Certificate] or [System] > [Security] > [Certificate] > [Site certificate] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificates] or [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [Site Certificates]) on the Interstage Management Console.

   Check whether the content of the acquired certificate is correct.

   An SSL configuration needs to be created to conduct SSL communication. Create an SSL configuration on the [Create New] tab after selecting [System] > [Security] > [SSL] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [SSL]) on the Interstage Management Console.

   It is necessary for [Protocol version] and [Encryption method] to match at least one definition in the SSL configuration used by the repository of the slave server respectively.

The following flow diagram illustrates the procedure for setting up an SSL communication environment when no client authentication is performed.



(1) Creating a test certificate
Test certificate
(2) Registering certificate and CRL
CA certificate
CRL
Registration order
(3) Setting to use the certificate

Same certificate and CRL as those of slave machines

Interstage Management Console [SSL]

SSL definition creation
Match the values of the following items to at least one of values of each item in the SSL definition of slaves.
- [Protocol version]
- [Encryption method]

Interstage Management Console [Repository]

[Replication destination host information]
[Presentation of client certificate] "Do not present"

Figure 2-6 SSL: Communication Environment without Authentication

Performing Client Authentication

Note

- It is necessary to use the same CA certificate and CRL as those obtained when setting up an SSL communication environment for the slave server.
- If the setting of [Client authentication] of [Environment settings] in the SSL configuration used by the repository of the slave server is "Authenticate (Always authenticate a client certificate)," do not specify a certificate for testing in the SSL configuration used for replication.

Set up an SSL communication environment for the master server according to the following procedure:

1. Setup of an Interstage certificate environment ((1) to (5) in the following figure)

   The detailed procedure up to this point is the same as the Server procedure described in Setting up an Environment for SSL Communication.

2. Setting to use the certificate ((6) in the following figure)

   Certificates registered in the Interstage certificate environment can be referenced by selecting [System] > [Security] > [Certificate] > [CA Certificate] or [System] > [Security] > [Certificates] > [Site Certificates] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificates] or [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [Site Certificates]) on the Interstage Management Console.

   Check whether the content of the acquired certificate is correct.

   An SSL configuration needs to be created to conduct SSL communication. Create an SSL configuration on the [Create a New Repository] tab after selecting [System] > [Security] > [SSL] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [SSL]) on the Interstage Management Console.

   Select "SSL3.0" for [Protocol version]. It is necessary for [Encryption] to match at least one definition in the SSL configuration used by the repository of the slave server.

The following flow diagram illustrates the procedure for setting up an SSL communication environment when client authentication is performed.

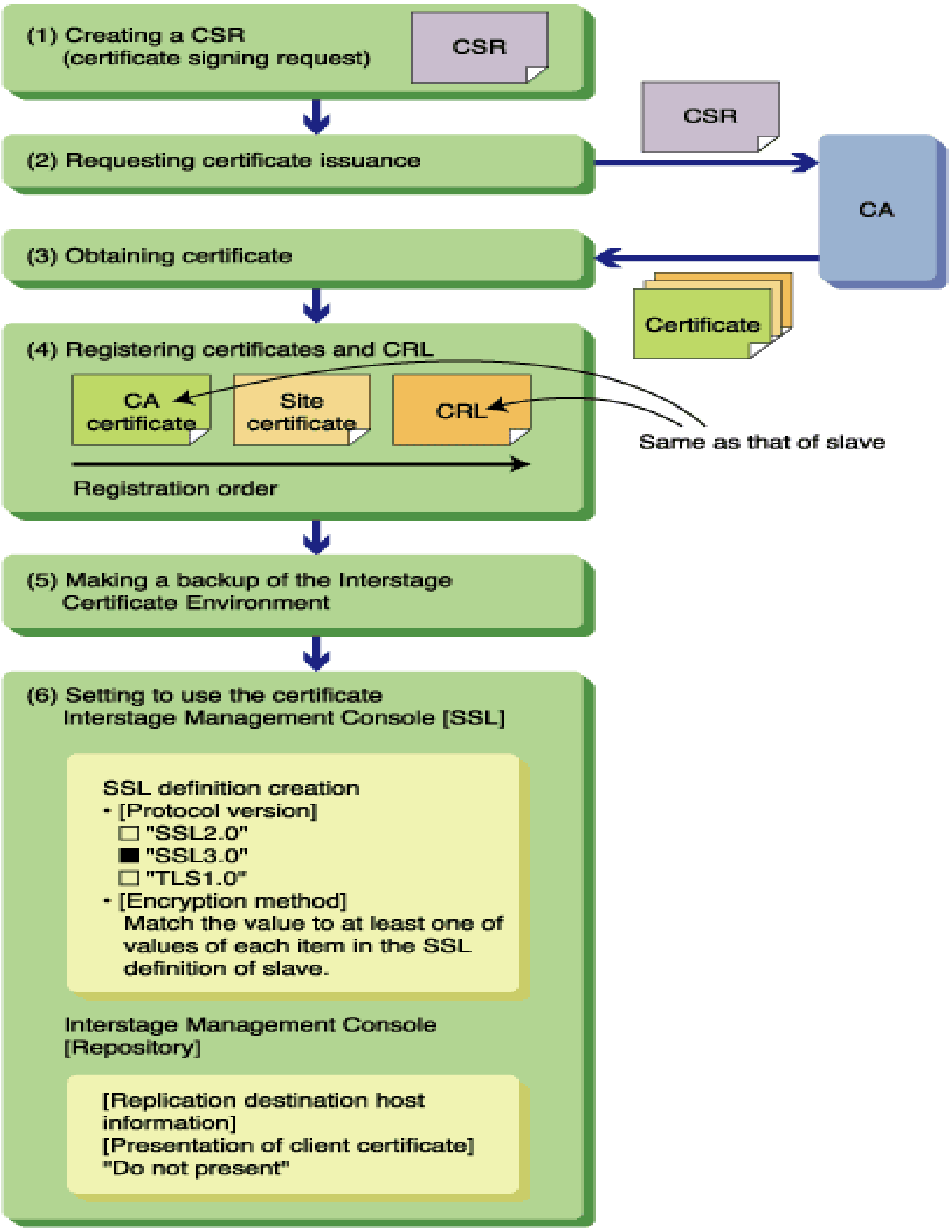

(1) Creating a CSR
(certificate signing request)
CSR
CSR
(2) Requesting certificate issuance
CA
(3) Obtaining certificate
Certificate
(4) Registering certificates and CRL
CA certificate
Site certificate
CRL
Same as that of slave
Registration order
(5) Making a backup of the Interstage Certificate Environment
(6) Setting to use the certificate
Interstage Management Console [SSL]
SSL definition creation
• [Protocol version]
□ "SSL2.0"
■ "SSL3.0"
□ "TLS1.0"
• [Encryption method]
Match the value to at least one of values of each item in the SSL definition of slave.
Interstage Management Console [Repository]
[Replication destination host information]
[Presentation of client certificate]
"Do not present"

Figure 2-7 SSL Communication with Client Authentication

The following explains the case where the CA of certificates used by the client and server are the same. For an explanation of the case in which the client and server use different CA certificates, and for further details on encrypted communication using SSL, see the "Security System Guide."

Setting up an Interstage Certificate Environment (Server)

Set up an Interstage certificate environment on a server of Smart Repository.

The following explains how to set up an Interstage certificate environment using CSR (certificate signing request).

Setting up an Interstage certificate environment entails the following steps:

1. Setup of an Interstage certificate environment and creation of CSR (certificate signing request)
2. Request to issue a certificate
3. Registration of the certificate and CRL (certificate revocation list)

After setting up an Interstage certificate environment, configure the environment to use the certificate. For more details, see Setting to Use the Certificates (Server).

For details of each command to be used in the following procedure, see the Reference Manual (Command Edition).

Note

Windows

Execute the commands as a user with the Administrator authority.

Solaris OE Linux

Execute the commands as a superuser.

Set the installation path of JDK or JRE to the environment variable JAVA_HOME for command execution.

Setup of an Interstage Certificate Environment and Creation of CSR (Certificate Signing Request)

To perform signing and encryption such as SSL, a certificate is necessary. For this purpose, create a CSR (certificate signing request), which is data used to request a certificate from CA (VeriSign Inc., or another Certification Authority).

If no Interstage certificate environment exists at this point, an Interstage certificate environment is created at the same time. If an Interstage certificate environment exists, that environment is used.

Note

No test certificate can be used in the following cases. Create a CSR instead of a test certificate.

- Smart Repository server in standalone mode.
- Slave server in replication mode.
- Master server when performing client authentication in replication mode.

An example of creating a CSR is shown below:

Windows

Nickname of the site certificate: SiteCert

Request output destination file name: C:\sslenv\my_csr.txt

Name: repository.fujitsu.com

Organization unit name: Interstage

Organization name: Fujitsu Ltd.

City name: Yokohama

Prefectural name: Kanagawa

Country code: jp

```
scsmakeenv –n SiteCert –f C:\sslenv\my_csr.txt –c
New Password:   (*1)
Retype:   (*1)

Input X.500 distinguished names.
What is your first and last name?
[Unknown]:repository.fujitsu.com   (*2)
What is the name of your organizational unit?
[Unknown]:Interstage   (*2)
What is the name of your organization?
[Unknown]:Fujitsu Ltd.   (*2)
What is the name of your City or Locality?
[Unknown]:Yokohama   (*2)
What is the name of your State or Province?
[Unknown]:Kanagawa   (*2)
What is the two-letter country code for this unit?
[Un]:jp   (*2)
Is <CN=repository.fujitsu.com, OU=Interstage, O=Fujitsu Ltd., L=Yokohama,
ST=Kanagawa, C=jp> correct?
[no]:yes   (*3)
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
SCS: INFO: scs0101: CSR was issued <C:\sslenv\my_csr.txt>
```

Solaris OE Linux

Nickname of the site certificate: SiteCert

Request output destination file name: /sslenv/my_csr.txt

Name: repository.fujitsu.com

Organization unit name: Interstage

Organization name: Fujitsu Ltd.

City name: Yokohama

Prefectural name: Kanagawa

Country code: jp

```
# scsmakeenv –n SiteCert –c –f /sslenv/my_csr.txt
New Password:   (*1)
Retype:   (*1)

Input X.500 distinguished names.
What is your first and last name?
[Unknown]:repository.fujitsu.com   (*2)
What is the name of your organizational unit?
[Unknown]:Interstage   (*2)
What is the name of your organization?
[Unknown]:Fujitsu Ltd.   (*2)
What is the name of your City or Locality?
[Unknown]:Yokohama   (*2)
What is the name of your State or Province?
[Unknown]:Kanagawa   (*2)
What is the two-letter country code for this unit?
[Un]:jp   (*2)
Is <CN=repository.fujitsu.com, OU=Interstage, O=Fujitsu Ltd., L=Yokohama,
ST=Kanagawa, C=jp> correct?
[no]:yes   (*3)
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
UX: SCS: INFO: scs0101: CSR was issued </sslenv/my_csr.txt>
```

*1. Enter the password. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*2. For the content to be entered, see the "Reference Manual (Command Edition)."

*3. If the displayed content is correct, enter "yes." To retry the input, enter "no."

Note

- Specify the nickname specified in the -n option when registering a site certificate. Do not forget it.
- If CSR is created, a private key is created in the Interstage certificate environment. To protect the private key, back up the Interstage certificate environment until a certificate is obtained. For details of the backup method, see the Operator's Guide.

  If the Interstage certificate environment is damaged and no backup is available, make another request for an Interstage certificate environment (CSR creation) and the issue of a certificate.

Request to Issue a Certificate

Make a request to issue a certificate to the CA and obtain it.

If the scsmakeenv command is executed normally, a request is output to the file that stores the CSR (certificate signing request). This file is specified in the "-f" option of the scsmakeenv command. Send the file to the CA to request the issue of a certificate. Follow the request creation procedure of each CA.

Registration of a Certificate and CRL (Certificate Revocation List)

Register the certificates and CRL obtained from the CA in the Interstage certificate environment.

Register the certificates starting with the certificate of the CA.

Registration of a Certificate of CA

Register the obtained certificate of CA.

The following shows some examples of registration:

Windows

CA certificate: C:\sslenv\CA.der

Nickname of the CA certificate: CA

```
scsenter -n CA -f C:\sslenv\CA.der
Password:   (*1)
Certificate was added to keystore
SCS: INFO: scs0104: Certificate was imported
```

Solaris OE Linux

CA certificate: /sslenv/CA.der

Nickname of the CA certificate: CA

```
# scsenter -n CA -f /sslenv/CA.der
Password:   (*1)
certificate was added to keystore
UX: SCS: INFO: scs0104: Certificate was imported
```

*1. Enter the password. The entered string will not be echoed back.

Registration of a Site Certificate

Register the issued certificate as a site certificate.

The following shows some examples of registration:

Windows

Site certificate: C:\sslenv\SiteCert.der

Nickname of the site certificate: SiteCert

```
scsenter -n SiteCert -f C:\sslenv\SiteCert.der –o
Password:   (*1)
Certificate reply was installed in keystore
SCS: INFO: scs0104: Certificate was imported
```

Solaris OE Linux

Site certificate: /sslenv/SiteCert.der

Nickname of the site certificate: SiteCert

```
# scsenter -n SiteCert -f /sslenv/SiteCert.der –o
Password:   (*1)
Certificate reply was installed in keystore
UX: SCS: INFO: scs0104: Certificate was imported
```

*1. Enter the password. The entered string will not be echoed back.

Registration of CRL

Register the obtained CRL.

The following shows some examples of registration:

Windows

CRL C:\sslenv\CRL.der

```
scsenter -c -f C:\sslenv\CRL.der
Password:   (*1)
SCS: INFO: scs0105: CRL was imported
```

Solaris OE Linux

CRL /sslenv/CRL.der

```
# scsenter -c -f /sslenv/CRL.der
Password:   (*1)
UX: SCS: INFO: scs0105: CRL was imported
```

*1. Enter the password. The entered string will not be echoed back.

Backup of an Interstage Certificate Environment

After registering the obtained certificates and CRL, be sure to back up the Interstage certificate environment. For the backup method, see the Operator's Guide.

If the Interstage certificate environment is damaged and no backup is available, make another request for an Interstage certificate environment (CSR creation) and the issue of a certificate.

The following shows some examples of registration:

Windows

```
mkdir X:\Backup\scs
xcopy /E C:\Interstage\etc\security X:\Backup\scs   (*1)
```

Solaris OE Linux

```
# mkdir /backup/scs
# cp -rp /etc/opt/FJSVisscs/security /backup/scs   (*1)
```

*1. It is recommended to save to removable media.

Setting to Use the Certificates (Server)

Make the setting on a server of Smart Repository.

After setting up an Interstage certificate environment, some set up is required to enable use of the certificates. The required setup procedure is described in the following sections.

Setting to Use the Certificates

Certificates registered in the Interstage certificate environment can be viewed by selecting [System] > [Security] > [Certificate] > [CA Certificate] or [System] > [Security] > [Certificate] > [Site certificate] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificates] or [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [Site Certificates]) on the Interstage Management Console.

Check whether the content of the obtained certificate is correct.

An SSL configuration needs to be created to conduct SSL communication. To create an SSL configuration, select the [Create New] tab from [System] > [Security] > [SSL] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [SSL]) on the Interstage Management Console.

Select a site certificate rather than a test certificate.

When no client authentication needs to be performed, select "Do not authenticate" in [Client authentication]. In [Protocol version], select both "SSL 2.0" and "SSL 3.0" (recommended) or either of them.

To perform client authentication, select "Authenticate (Always authenticate a client certificate)" or "Authenticate (Authenticate if a client certificate is presented)" in [Client authentication]. In [Protocol version], select both "SSL 3.0."

Creating a Certificate and Key Management Environment (Client)

Implement the required settings on a client of Smart Repository.

Create a certificate and key management environment, which is an operation environment for SSL.

Perform the following procedures as a user who executes the Smart Repository client.

Use the SMEE command to build the Certificate/Key management environment of the Smart Repository client. For details about each of the commands shown on this page, refer to "SSL Environment Setting Commands" in the "Reference Manual -Command Edition".

Windows

SMEE commands are stored in the following directories.

- Create/Setup command of SMEE3 private key management environment (makeslot, macktoken)

  system drive :\Program Files\SecurecryptoLibraryR\Program\bin

- Excluding the above.

  system drive :\Program Files\Common Files\Fujitsu Shared\F3FSSMEE

Creation of a Management Directory

Create the directories needed to manage the certificates and private keys.

The following shows some examples of creating directories:

Windows

```
mkdir D:\sslenv\slot   (*1)
mkdir D:\sslenv\sslcert   (*2)
mkdir D:\sslenv\sslcert\cert   (*3)
mkdir D:\sslenv\sslcert\crl   (*4)
```

Solaris OE Linux

```
$ mkdir /sslenv/slot   (*1)
$ mkdir /sslenv/sslcert   (*2)
$ mkdir /sslenv/sslcert/cert   (*3)
$ mkdir /sslenv/sslcert/crl   (*4)
```

*1. Slot information directory

*2. Operation control directory

*3. Certificate management directory

*4. CRL management directory

Creation and Setting of a Private Key Management Environment

Create and set a private key management environment required to manage the private keys.

The following shows some examples of creating a private key management environment:

Windows

```
makeslot -d D:\sslenv\slot
New Slot-password:   (*1)
Retype:   (*1)
makeslot: Succeeded. New Slot-ID is 1.   (*2)
maketoken -d D:\sslenv\slot -s 1 -t Token01   (*2)
Slot-password:   (*1)
New SO-PIN for Token01:   (*3)
Retype:   (*3)
New User-PIN for Token01:   (*4)
Retype:   (*4)
```

Solaris OE Linux

```
$ makeslot –d /sslenv/slot
New Slot-password:   (*1)
Retype:   (*1)
makeslot: Succeeded. New Slot-ID is 1.   (*2)
$ maketoken -d /sslenv/slot -s 1 -t Token01   (*2)
Slot-password:   (*1)
New SO-PIN for Token01:   (*3)
Retype:   (*3)
New User-PIN for Token01:   (*4)
Retype:   (*4)
```

*1. Enter the slot password. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*2. As a result of executing the makeslot command, the slot ID of the generated slot is returned. Specify this value in the -s option of the maketoken command.

*3. Enter SO-PIN. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*4. Enter user PIN. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

Creation of a Certificate and CRL Management Environment

Create and set a certificate and CRL management environment to manage the certificates and CRL.

To use a certificate of VeriSign Inc. or another Certification Authority, register the CA Certificate of the root CA of VeriSign Inc. or another Certification Authority.

The following shows an example of creating a certificate and CRL management environment using a Certificate (Integration Certificate List File "contractcertlist"):

Windows

```
cmmkenv D:\sslenv\sslcert -todir
D:\sslenv\sslcert\cert,D:\sslenv\sslcert\crl
cmsetenv D:\sslenv\sslcert -sd D:\sslenv\slot -jc 1 -rc
C:\Interstage\IS_cert\contractcertlist
```

Solaris OE Linux

```
# cmmkenv /sslenv/sslcert -todir /sslenv/sslcert/cert,/ sslenv/sslcert/crl
# cmsetenv /sslenv/sslcert -sd /sslenv/slot -jc 1 -rc
/etc/opt/FJSVisas/contractcertlist
```

Creating a Private Key and Acquiring a Certificate (Client)

Create a private key and acquire a certificate on a client of Smart Repository.

Make a request to issue a certificate to CA (certification authority) and obtain it.

Creation of a Certificate Signing Request (Concurrent Creation of a Private Key)

Create a certificate signing request to make a request to CA to issue a certificate.

If the following command is executed, a private key is created at the same time.

The following shows some examples of creating a certificate signing request:

Windows

```
cmmakecsr -ed D:\sslenv\sslcert -sd D:\sslenv\slot -f TEXT -c jp -cn
"repository.fujitsu.com" -o "Fujitsu Ltd." -ou "Interstage" -l "Yokohama" -s
"Kanagawa" -kt RSA -tl Token01 -of D:\sslenv\myCertRequest
ENTER TOKEN PASSWORD=>   (*1)
```

Solaris OE Linux

```
$ cmmakecsr -ed /sslenv/sslcert -sd /sslenv/slot -f TEXT -c jp -cn
"repository.fujitsu.com" -o "Fujitsu Ltd." -ou "Interstage" -l "Yokohama" -s
"Kanagawa" -kt RSA -tl Token01 -of /sslenv/myCertRequest
ENTER TOKEN PASSWORD=>   (*1)
```

*1. Enter the user PIN. The entered characters will not be echoed back.

Request to Issue a Certificate

Send a certificate signing request to the CA to make a request for a site certificate.

Follow the procedure of each CA for making a request.

Acquisition of a Certificate

Obtain a certificate signed by the CA.

Follow the procedure of each CA for obtaining a signed certificate.

Registering a Certificate and CRL (Client)

Register a certificate and CRL with a client of Smart Repository.

Register a certificate and CRL in a certificate and CRL management environment.

Registration of a CA Certificate

Register the obtained CA certificates in the certificate and CRL management environment.

Register the certificates starting with the CA certificate of the root CA.

Note

Certificates of the same CA must be registered with the Smart Repository server and Smart Repository client that use SSL.

The following shows some examples of registration:

CA Certificate: CA.der

Windows

```
cmentcert D:\sslenv\CA.der -ed D:\sslenv\sslcert -ca -nn CA
normal end certid = IG6GwPx4gjZEZ2NptohObuWHU9A=   (*1)
```

Solaris OE Linux

```
$ cmentcert /sslenv/CA.der -ed /sslenv/sslcert -ca -nn CA
normal end certid = qpD2dla7zA5xUEeDoLNgtb4c5WE=   (*1)
```

*1. The value of certid may be different each time the command is executed.

Note

- The client verifies the site certificate registered with the client. Register the CA certificates used by the client to verify the site certificates with the client.
- All CA certificates registered with the client become the reliable CA certificates when conducting SSL communication between client and server. Since the site certificates are specified in the SSL configuration used by the server repository, register the CA certificates needed to verify a specified site certificate with the client.

Registration of a Site Certificate

Register a site certificate in a certificate and CRL management environment.

Perform the registration only if client authentication is required.

If no client authentication is needed, there is no need to register a site certificate.

Note

No certificate for testing can be used.

The following shows some examples of registration:

Site certificate: user-cert.der

Windows

```
cmentcert D:\sslenv\user-cert.der -ed D:\sslenv\sslcert -own -nn user-cert
normal end certid = 4aCjpxEud6++drEiLbyx4XPCQ2U=   (*1)
```

Solaris OE Linux

```
$ cmentcert /sslenv/user-cert.der -ed /sslenv/sslcert -own -nn user-cert
normal end certid = HhMYCOMdh+gzxHToSyoOyEogdac=   (*1)
```

*1. The value of certid may be different each time the command is executed.

Registration of CRL

Register the obtained CRL in a certificate and CRL management environment.

The following shows some examples of registration:

Windows

```
cmentcrl D:\sslenv\CRL.der -ed D:\sslenv\sslcert
normal end CrlID = bAAqy9Qgh8bw2CUG18m3IuEc2mM=   (*1)
```

Solaris OE Linux

```
# cmentcrl /sslenv/CRL.der -ed /sslenv/sslcert
normal end CrlID = WLw6q/bNZ7qsQ+8hRjVOJzinmJY=   (*1)
```

*1. The value of CrlID may be different each time the command is executed.

Backup of the Certificate/CRL/Private Key Management Environment

Back up the certificate/CRL/private key management environment.

The following shows some examples:

Windows

```
mkdir X:\Backup\irepcli
xcopy /E D:\sslenv\slot X:\Backup\irepcli   (*1)
xcopy /E D:\sslenv\sslcert X:\Backup\irepcli   (*1)
```

Solaris OE Linux

```
$ mkdir /backup/irepcli
$ cp -rp /sslenv/slot /backup/irepcli   (*1)
$ cp -rp /sslenv/sslcert /backup/irepcli   (*1)
```

*1. It is recommended to save to removable media.

Setting an SSL Environment Definition File (Client)

Store information about the SSL environment on the Smart Repository client.

For user applications using JNDI or the Smart Repository LDAP command (ldapsearch, ldapmodify, and ldapdelete commands), store the information in the SSL environment definition file.

For the Smart Repository LDAP command, specify the SSL environment definition file using the -Z option.

Smart Repository provides some samples of the SSL environment definition file. Copy the file and then customize it for the environment.

Windows

```
C:\Interstage\IREP\sample\conf\sslconfig.cfg
```

Solaris OE Linux

```
/opt/FJSVirep/sample/conf/sslconfig.cfg
```

Description Format

In the file, describe the definition of each item in a separate line.

The description format is shown below.

```
Definition name = Value
```

Do not enter blanks before or after '='.

Value refers to the characters enclosed by '=' and the new line character. Blank characters and the tab are also valid for Value.

A line starting with ‘#' is considered a comment.

Note Windows

If a blank character is contained in a directory name or file name, specify the name in the 8.3 format (i.e. "file name.extension" in which the file name consists of up to eight characters and the extension can be up to three characters).

A file name in the 8.3 format can be checked by adding the "/X" option to the DIR command.

List of Definition Items

Table 2-2 lists the items in the SSL environment definition file.

Table 2-2 SSL Environment Definition Items

Definition item	Definition name	Required or Optional setting
SSL version	ssl_version	Required
Encryption algorithm	crypt	Optional
Slot information directory	slot_path	Required
Token label	tkn_lbl	Required
User PIN	tkn_pwd	Required
Operation control directory	cert_path	Required
User certificate nickname	user_cert_name	*1 (see below)
Certificate verification method	ssl_verify	Required
Timer value	ssl_timer	Optional

*1. If omitted, a user certificate registered in the certificate management environment is assumed.

SSL Version (ssl_version)

Explanation

Describe the version of the SSL protocol to be used:

Setup value	Explanation
2	Use the SSL version 2.0 only.
3	Use the SSL version 3.0 only.

Abbreviation Value

This definition item cannot be abbreviated.

Example

```
ssl_version=3
```

Encryption Algorithm (crypt)

Explanation

Select the encryption methods to be used for SSL from the following table and then describe them separated by ':' in order of priority.

Configure the same settings as those of the SSL configuration used by the Smart Repository server, which is the communication party.

If '2' is specified as the SSL version (ssl_version), the following values can be used:

Setup value	Explanation
DES-CBC3-MD5	168bit triple DES encryption, MD5 MAC
RC4-MD5	128bit RC4 encryption, MD5 MAC
RC2-MD5	128bit RC2 encryption, MD5 MAC
DES-CBC-MD5	56bit DES encryption, MD5 MAC
EXP-RC4-MD5	40bit RC4 encryption, MD5 MAC
EXP-RC2-MD5	40bit RC encryption, MD5 MAC

If '3' is specified as the SSL version (ssl_version), the following values can be used:

Setup value	Explanation
RSA-3DES-SHA	168bit triple DES encryption, SHA-1 MAC
RSA-RC4-SHA	128bit RC4 encryption, SHA-1 MAC
RSA-RC4-MD5	128bit RC4 encryption, MD5 MAC
RSA-DES-SHA	56bit DES encryption, SHA-1 MAC

RSA-EXPORT-RC4-MD5	40bit RC4 encryption, MD5 MAC
RSA-EXPORT-RC2-MD5	40bit RC2 encryption, MD5 MAC
RSA-NULL-SHA	No encryption, SHA-1 MAC
RSA-NULL-MD5	No encryption, MD5 MAC

The following types of encryption represented in the encryption method ("SSL_TXT_XXX") are supported by the Interstage Application Server:

– Public key encryption method: RSA

– Private key encryption method: DES, 3DES (triple DES), RC4, RC2 (NULL indicates no encryption)

– Private key processing mode: CBC, EDE (numeric value: block length)

– Hash key: SHA, MD5

MAC is a message authentication code.

Abbreviation Value

The default value depends on the specified SSL version (ssl_version). In the following explanation, each encryption method is on a new line.

– If the SSL version '2' is specified:

DES-CBC3-MD5:

DES-CBC-MD5:

RC4-MD5:

RC2-MD5:

EXP-RC4-MD5:

EXP-RC2-MD5

– If the SSL version '3' is specified:

RSA-3DES-SHA:

RSA-DES-SHA:

RSA-RC4-MD5:

RSA-RC4-SHA:

RSA-EXPORT-RC4-MD5:

RSA-EXPORT-RC2-MD5:

RSA-NULL-MD5:

RSA-NULL-SHA

Example

```
crypt=RSA-3DES-SHA:RSA-DES-SHA:RSA-RC4-MD5:RSA-RC4-SHA:RSA-EXPORT-RC4-
MD5:RSA-EXPORT-RC2-MD5:RSA-NULL-MD5:RSA-NULL-SHA
```

Slot Information Directory (slot_path)

Explanation

Describe the slot information directory created in "Creating a Certificate and Key Management Environment (Client)" using the full specification.

Abbreviation Value

This definition item cannot be abbreviated.

Example

Windows

```
slot_path=D:\sslenv\slot
```

Solaris OE Linux

```
slot_path=/sslenv/slot
```

Token Label (tkn_lbl)

Explanation

Specify the token label specified in "Creation and Setting of a Private Key Management Environment."

Abbreviation Value

This definition item cannot be abbreviated.

Example

```
tkn_lbl=Token01
```

User PIN (tkn_pwd)

Explanation

Enter the user PIN specified in "Creation and Setting of a Private Key Management Environment."

After entering the user PIN, the irepencupin command needs to be used for encryption.

For details on encryption of the user PIN, refer to Encrypting the User PIN (Client). For information about how to use the irepencupin command, see "Smart Repository operation command" in the Reference Manual (Command Edition)."

Abbreviation Value

This definition item cannot be abbreviated.

Example

```
tkn_pwd=Token111
```

Operation Control Directory (cert_path)

Explanation

Describe the operation control directory created in "Creating a Certificate and Key Management Environment (Client)" using the full pathname.

Abbreviation Value

This definition item cannot be abbreviated.

Example

Windows

```
cert_path=D:\sslenv\sslcert
```

Solaris OE Linux

```
cert_path=/sslenv/sslcert
```

User Certificate Nickname (user_cert_name)

Explanation

Specify the nickname of the user certificate specified in "Registering a Certificate and CRL (Client) ".

Abbreviation Value

All nicknames of the user certificate registered in the certificate management environment are assumed.

Example

```
user_cert_name=user-cert
```

Certificate Verification Method (ssl_verify)

Explanation

Specify the verification method of certificates. The following verification methods can be specified:

Setup value	Certificate verification method
0	No verification
1	Verify certificates used by the Smart Repository client.
2	Verify certificates used by the Smart Repository client and those sent by the Smart Repository server.

Abbreviation Value

This definition item cannot be abbreviated.

Example

```
ssl_verify=2
```

Timer Value (ssl_timer)

Explanation

Specify the wait time for connecting the server and client or sending/receiving data in seconds. Specify a value equal to or greater than 1.

Abbreviation Value

3600

Example

```
ssl_timer=300
```

Examples of SSL Definition File Settings

Windows

```
#
# ==== SSL environment file ====
#
# ----------------------------
# SSL protocol version
# ssl_version=2 | 3
# ----------------------------
ssl_version=3


# ----------------------------
# Slot directory
# slot_path=directory path
# ----------------------------
```

```
slot_path=D:\sslenv\slot


# ------------------------------
# Token label
# tkn_lbl=token label
# ------------------------------
tkn_lbl=Token01


# ------------------------------
# User PIN
# tkn_pwd=user pin
# ------------------------------
tkn_pwd=xxxxxxxx   (*1)


# ------------------------------
# Certificate directory
# cert_path=directory path
# ------------------------------
cert_path=D:\sslenv\sslcert


# ------------------------------
# User certificate nickname
# user_cert_name=nickname
# ------------------------------
#user_cert_name=user-cert   (*2)


# ------------------------------
# Verify mode
# ssl_verify=0 | 1 | 2
# ------------------------------
ssl_verify=2


# ------------------------------
# Timer
# ssl_timer=time(sec)
# ------------------------------
ssl_timer=300
```

*1. Specify the user PIN specified in "Creation and setting of a private key management environment."

*2. To enable all site certificates registered in the certificate and key management environment, place "#" at the start of the lines.

Solaris OE Linux

```
#
# ==== SSL environment file ====
#
# ------------------------------
# SSL protocol version
# ssl_version=2 | 3
# -----------------------------
ssl_version=3


# -----------------------------
# Slot directory
# slot_path=directory path
# -----------------------------
slot_path=/sslenv/slot


# -----------------------------
# Token label
# tkn_lbl=token label
# -----------------------------
tkn_lbl=Token01


# -----------------------------
# User PIN
# tkn_pwd=user pin
# -----------------------------
tkn_pwd=xxxxxxxx   (*1)


# -----------------------------
# Certificate directory
# cert_path=directory path
# -----------------------------
cert_path=/sslenv/sslcert


# -----------------------------
# User certificate nickname
# user_cert_name=nickname
# -----------------------------
#user_cert_name=user-cert   (*2)


# -----------------------------
# Verify mode
# ssl_verify=0 | 1 | 2
# -----------------------------
ssl_verify=2


# -----------------------------
# Timer
# ssl_timer=time(sec)
# -----------------------------
ssl_timer=300
```

*1. Specify the user PIN specified in "Creation and setting of a private key management environment."

*2. To enable all site certificates registered in the certificate and key management environment, place "#" at the start of the lines.

Encrypting the User PIN (Client)

The user PIN described in the SSL environment definition file needs to be encrypted.

By specifying the SSL environment definition file in the irepencupin command, the user PIN described in the file will be encrypted. For information about how to use the irepencupin command, see "Smart Repository operation command" in the Reference Manual (Command Edition)."

The following shows some execution examples:

Windows

```
irepencupin -f D:\conf\sslconfig.cfg
```

Solaris OE Linux

```
# irepencupin –f /conf/sslconfig.cfg
```

Note

Solaris OE

If the command is executed successfully, a backup file (SSL environment definition file name.backup) will be created in the same directory. If no backup file will be needed, delete it.

Creating a Repository

This section explains how to create a repository.

The repository of the slave server in master-slave (replication) mode can be created by restoring on the slave server a repository created on the master server through backup of the repository. For the procedure for creating a repository, refer to Setting Up an Environment for the Replication Mode.

In standalone mode, the Interstage Management Console of the machine that sets up the standalone server is used to create a repository. In master-slave mode, the Interstage Management Console of the machine that sets up the master server is used. For information on how to operate the Interstage Management Console, see Chapter 8 - "Services" in the Operator's Guide.

Note

Creating a repository takes several minutes. This includes the time needed to create database information used inside the repository. The time required for creation varies a little depending on the machine performance.

1. Select [System] > [Service] > [Repository] > [Create a New Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository] > [Create a New Repository]).
2. Click the [Create] button after specifying the following details for each item:

   Simple Settings

- Repository name

  Specify the repository name that identifies each repository. This item can be specified only when creating a new repository. Once the repository has been created, the name cannot be changed.

- Administrator DN

  Specify the DN (distinguished name) for the administrator who will manage the created repository in the DN format. This item can be specified only when creating a new repository. Once the repository has been created, the value cannot be changed.

- Administrator DN password

  Specify the password of the administrator who will manage the created repository.

- Administrator DN password (re-entry)

  Re-enter the password of the administrator who will manage the created repository.

- Public Directory

  Specify the top entry to make the repository public in the DN (distinguished name) format. The public directory can be specified only when creating a new repository. Once the repository is created, the value cannot be changed.

- Create default tree?

  Specify whether to create a default tree. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- Port number

  Specify the port number to use for non-SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- Enable SSL encryption?

  Specify whether to conduct SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- SSL Port number

  Specify the port number to use for SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- SSL configuration

  Decide on the SSL configuration to be used for SSL communication.

[Detailed Settings] Database Settings

- User password encryption method

  Specify the encryption method to use when storing the user password attributes. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- Database Storage Directory

  Specify the database storage directory using the full pathname. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

For other items, there is normally no need to change the initial values. Change them if required.

For character definitions, including the number of characters and the range that can be specified for each item, see Setting Items of the Interstage Management Console

Once the repository has been created, it is added to the [Repository: View Status] window (open this window by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).

Windows

The created repository will also be added to the Windows(R) service under the following name:

Interstage Smart Repository (repository name)

```
Interstage Smart Repository (repository name)
```

3. Start the created repository from the [Repository: View Status] window.

Registering User Information

When registering user information with the created repository, the following three registration methods can be selected, depending on the amount of user information to register and the operating method:

- Using the CSV file

  This method is suitable when user information is controlled in one place (for example, in a personnel database).

  Large amounts of user information are added to the repository using a CSV file, which is extracted from the source of the information (in this example, the personnel database). When information needs to be updated, for example to accommodate personnel changes and new recruits, a CSV file extracting only the new information is used to update the repository.

- Using the LDIF file

  An LDIF file is created to add all entries to the repository together.

- Using the Entry Administration Tool

  Use the Entry Administration Tool for managing entries during both development and directory setup tests performed by the system administrator.

Importing User Information Using the CSV File

The following diagram shows the procedure for adding entries using the CSV file:

1. Extract CSV format data from the database of user information.
2. Set the mapping rules (conversion rules).
3. Execute the import command.

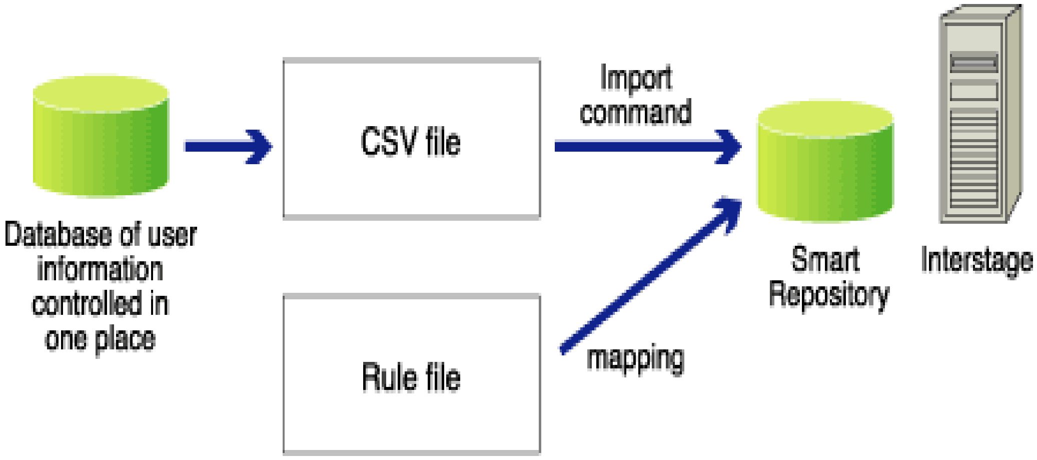


Figure 2-8 Add Entries using the CSV File

Extracting CSV Format Data from the Database of User Information Controlled in One Place

Use the database functions to extract data in the CSV format from the database of user information. If data on the database is binary, such as certificates, convert it into text (Base64) format.

For details of the CSV format, see, "Using the CSV File" in Chapter 3 - Entry Management.

Setting the Mapping Rules (Conversion Rules)

To register CSV format data with the repository, it is necessary to associate the CSV format data information and repository information. Mapping rules are provided to associate both types of information. For details on how to set the mapping rules, see "CSV and Rule Files" In Chapter 3 – Entry Management.

Executing the Import Command

Execute the irepmodifyent command. Entry data will then be added according to the mapping rules.

For details of the irepmodifyent command, see the Reference Manual (Command Edition).

Importing User Information Using the LDIF File

The sample LDIF file provided by Smart Repository contains user information. Entries can easily be added to the repository by specifying the information to be registered or changed in the sample LDIF file and executing the ldapmodify command.

For details of the LDIF file, see "Using the CSV file" in Chapter 3 - Entry Management. For details of the ldapmodify command, see the Reference Manual (Command Edition).

Example:

Specify the Administrator DN and Administrator DN password set when the repository was created from the [Create a New Repository] tab (after selecting [System] > [Service] > [Repository] (If on the Admin Server, create it from [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) in the Interstage Management Console. In the following example, 389 is specified as the repository port number, "cn=manager,ou=interstage,o=fujitsu,dc=com" as the Administrator DN, and "admin" as the Administrator DN password.

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

Administrator DN password: admin

Windows

LDIF file: C:\Interstage\IREP\sample\ldif\addldif.txt

```
C:\Interstage\ID\Dir\sdk\C\bin\ldapmodify –p 389 –D
"cn=manager,ou=interstage,o=fujitsu,dc=com" –w admin –a –f
C:\Interstage\IREP\sample\ldif\addldif.txt
```

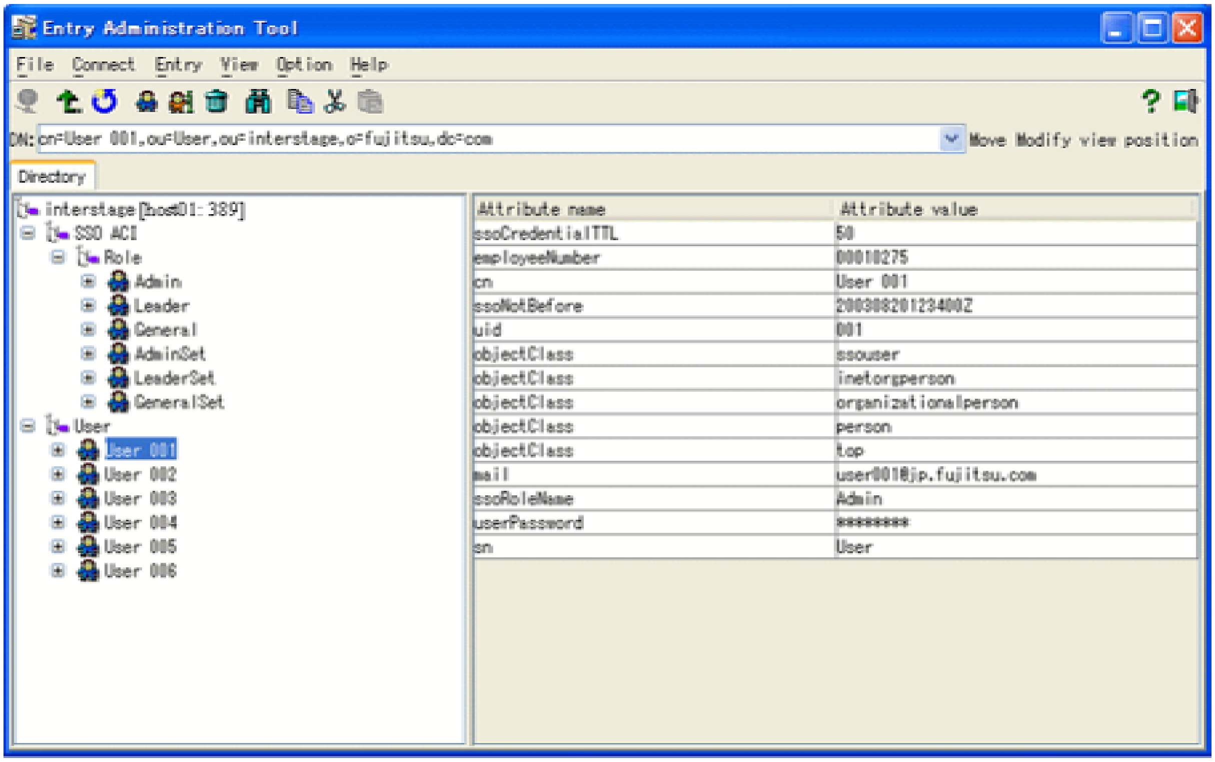
Solaris OE Linux

LDIF file: /opt/FJSVirep/sample/ldif/addldif.txt

```
/opt/FJSVidsdk/C/bin/ldapmodify -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -w admin -a -f
/opt/FJSVirep/sample/ldif/addldif.txt
```

Importing User Information Using the Entry Administration Tool

Using the Entry Administration Tool, registered entries in the repository can be added, modified, deleted, and retrieved through a GUI.



DN: cn=User 001,ou=User,ou=interstage,o=fujitsu,dc=com

Attribute name	Attribute value
ssoCredentialTTL	50
employeeNumber	00010275
cn	User 001
ssoNotBefore	20030820123400Z
uid	001
objectClass	ssouser
objectClass	inetorgperson
objectClass	organizationalperson
objectClass	person
objectClass	top
mail	user001@jp.fujitsu.com
ssoRoleName	Admin
userPassword	********
sn	User

Note

If an external file is specified as a binary attribute value and only the content of the external file is stored, the file name is not stored. This means, that if an entry containing a binary attribute is selected, only the data size of the binary file stored in the repository is displayed in the attribute value field of the binary attribute.

Startup method

Windows

Select [Programs] - [Interstage] - [Smart Repository] - [Entry Administration Tool] from the [Start] menu.

Solaris OE Linux

```
irepeditent
```

For further details of how to use the Entry Administration Tool, see the Entry Administration Tool Help.

Setting Up an Environment for the Replication Mode

To set up a new system in replication mode, or to change from standalone mode to replication mode, configure a new environment according to the following procedure.

The following flow diagram illustrates the procedure for setting up a new system in replication mode.

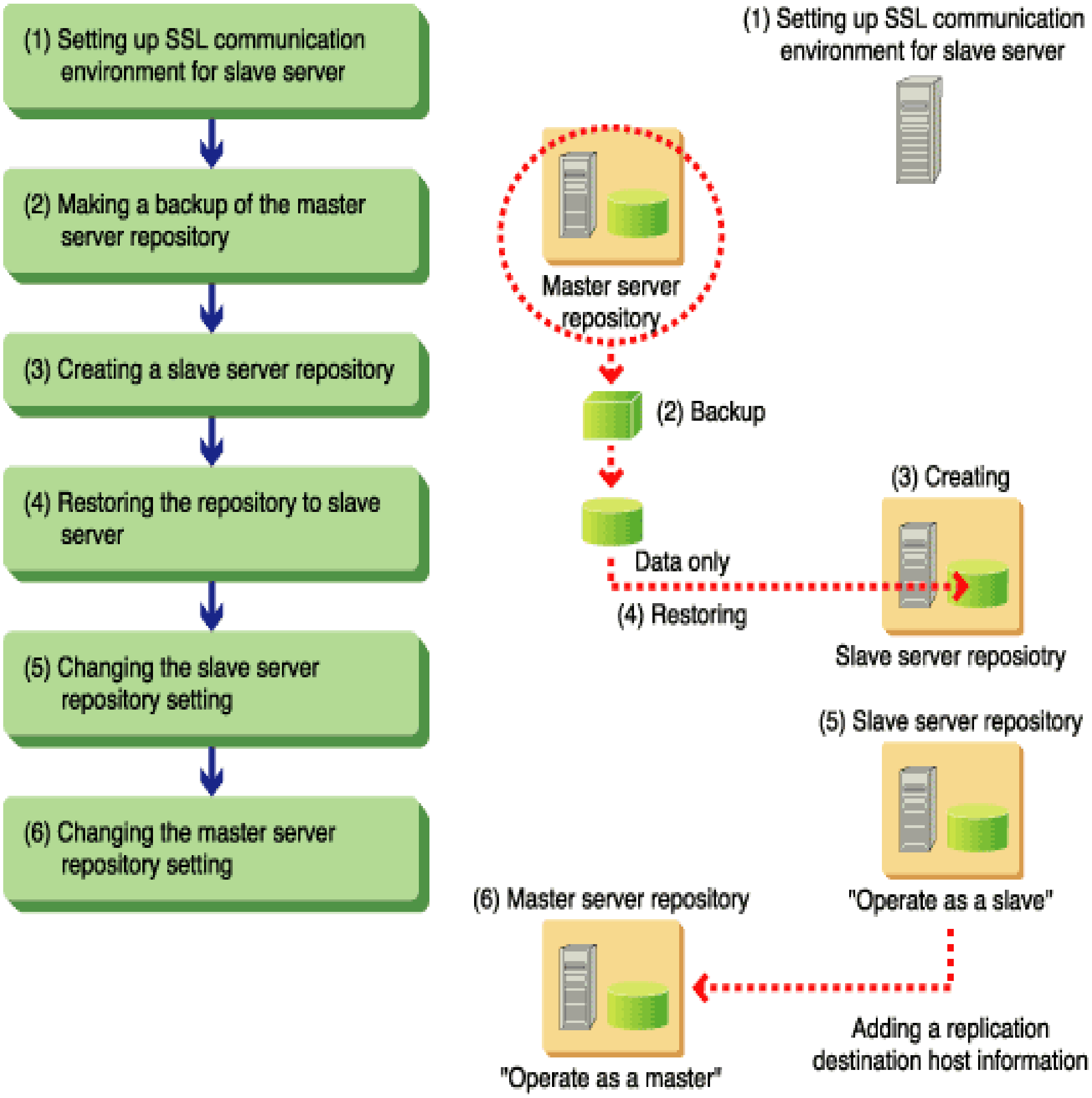

(1) Setting up SSL communication environment for slave server
(2) Making a backup of the master server repository
(3) Creating a slave server repository
(4) Restoring the repository to slave server
(5) Changing the slave server repository setting
(6) Changing the master server repository setting
(1) Setting up SSL communication environment for slave server
Master server repository
(2) Backup
(3) Creating
Data only
(4) Restoring
Slave server reposiotry
(5) Slave server repository
"Operate as a slave"
(6) Master server repository
"Operate as a master"
Adding a replication destination host information

Figure 2-9 Add a Slave in Replication Mode

The Master server repository is the repository created by "Creating a Repository". If the repository for the master server is not created, create it by referencing the details in "Flow of the Environment Setup".

Note

- Data is reflected in the slave server only after replication connection settings are added to the master server.
- During replication installation, do not add, modify, or delete entries not related to the installation.
- Replication mode cannot be set up in multiple repositories on the same machine.
- Set up multiple slave servers with the same master repository on the same machine is unsupported.

When using a cluster environment for replication operation, see Appendix A: "Manipulating a Repository in a Cluster Environment."

Setting up an SSL Communication Environment for the Slave Server

To conduct encrypted communication using SSL in replication mode, set up an SSL environment for the master server and configure SSL information on the slave servers that will be communicating with SSL.

Configuring an SSL communication environment for the slave servers entails the following steps:

1. Interstage certificate environment setup
2. Implementing settings to use the certificates

For the detailed procedure, see the Server procedure described in Setting up an Environment for SSL Communication.

Backing up the Master Server Repository

To create a repository of the slave server, it is necessary to back up repository data of the master server and restore it on the slave server machine.

The following explains how to back up repository data of the master server.

1. Select [Repository] from the [System] > [Service] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) on the Interstage Management Console of the master server machine.
2. Select the check box of the repository intended for master operation on the [Repository: View Status] window and then click the [Stop] button to stop the repository.
3. On the master server, execute the irepbacksys command with the -dataonly option. This will back up the repository data of the master server to a file. The command should be executed with Administrator authority.

   For details of the irepbacksys command, see the "Backup Commands" in the Reference Manual (Command Edition).

   Windows

   Backup destination directory: X:\Backup\irep\rep001_back

   Repository name: rep001

```
irepbacksys -d X:\Backup\irep\rep001_back –R rep001 -dataonly
IREP: INFO: irep11000: Backup has completed. X:\Backup\irep\rep001_back
[rep001]
```

Solaris OE Linux

Backup file name (excluding the extension): /backup/irep/rep001_back

Repository name: rep001

For the backup file name, specify the name of the file (excluding the extension) in which repository data is backed up.

```
# irepbacksys –f /backup/irep/rep001_back -R rep001 –dataonly
UX:IREP: INFO: irep11000: Backup has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

Creating a Repository for the Slave Server

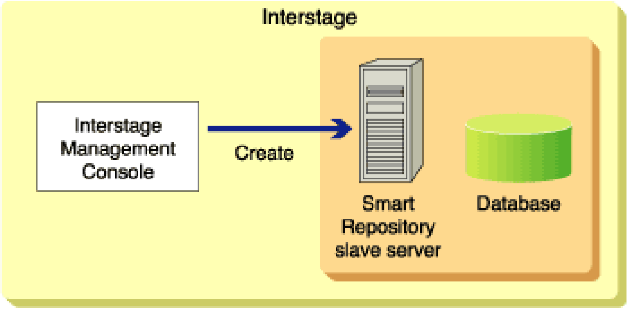


Figure 2-10 Use Interstage Management Console to Create a Repository

The following procedure describes how to create a repository on the slave server using the Interstage Management Console.

Note

Several minutes are needed to create a repository. This includes the time needed to create database information used inside the repository. The total time required varies a little depending on the machine performance.

1. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]). Then select the [Create a New Repository] tab.
2. Click the [Create] button after completing the details for each item shown below. Details shown in bold must be configured in the same way as the repository of the master server.

[General Settings]

- Repository Name

  Specify the same repository name as that of the master server. This must be configured during repository setup. After the repository is created, the name cannot be changed.

- Administrator DN

  Specify the DN (distinguished name) for the administrator who will manage the created repository in the DN format. This must be configured during repository setup. After creating a repository, the value cannot be changed.

  Administrator DN password Specify the password of the administrator who will manage the repository.

- Administrator DN password (re-entry)

  Re-enter the password of the administrator who will manage the created repository.

- Public Directory

  Configure with the same value as the master server. This must be configured during repository setup. After the repository is created, the value cannot be changed.

- Create default tree?

  Configure with the same value as the master server. This must be configured during repository setup. After the repository is created, the value cannot be changed.

- Port number

  Specify the port number to use for non-SSL communication. This must be configured during repository setup. After the repository is created, the value cannot be changed.

- Enable SSL encryption?

  Specify whether SSL communication will be used. This must be configured during repository setup. After the repository is created, the value cannot be changed.

- SSL port number

  Specify the port number to use for SSL communication. This must be configured during repository setup. After the repository is created, the value cannot be changed.

- SSL configuration

  Define the SSL configuration to be used for SSL communication.

[Detailed Settings] Database Settings

- User password encryption method

  Specify the same encryption method as that of the master server. This must be configured during repository setup. After the repository is created, the value cannot be changed.

- Database Storage Directory

  Specify the same storage directory as that of the master server. This must be configured during repository setup. After the repository is created, the value cannot be changed.

For other items, there is normally no need to change the initial values; however, change them if it is required.

For character definitions, such as the number of characters and the range that can be specified for each item, see Setting Items of the Interstage Management Console.

After the repository has been created, it will be added to the [Repository: Status] window. Open the window by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

Windows

The created repository will also be added to the Windows(R) service under the following name:

```
Interstage Smart Repository (repository name)
```

To check the master server settings, use the Interstage Management Console on the master server. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and then select the repository created for the master server from the [Repository: View Status] window. Select [General Settings] or [Detailed Settings (display)] to view them.

3. Start the created repository from the [Repository: View Status] window.

Restoring the Repository to the Slave Server

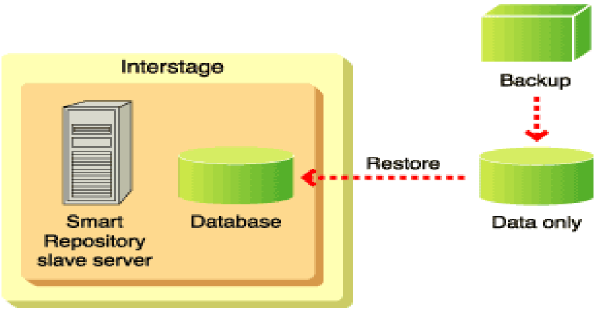


Figure 2-11 Restore Data to the Slave Server Repository

The backups of the master server repository data can be restored to the machine of the slave server.

The following procedure describes how to restore repository data.

1. Transfer the backup directory (backup file, if on Solaris OE or Linux) (created in the procedure above, "Backing up the Master Server Repository") to the machine of the slave server. Ensure that, during transfer, the data is not intercepted by unauthorized parties. After copying the file, make sure that it is deleted.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) in the Interstage Management Console on the slave server.
3. Check the status of the slave repository from the [Repository: View Status] window. If it does not display as stopped, check its check box and then click the [Stop] button to stop the repository.

4. On the slave server machine, execute the ireprestsys command with the -dataonly option. This will restore the backup directory (backup file, if on Solaris OE or Linux) data. Specify the backed-up repository name in the command.

   A confirmation message displays, requesting to overwrite the database. To replace it and continue restoring the data, enter 'y' or 'Y'. To stop the data restoration, enter 'n' or 'N'. If any other key is typed, the following message will display, awaiting user input: "Data already exists in database store. (C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)

   Are you sure of deleting data in database store? (y/n):"

   For details of the ireprestsys command, see the Reference Manual (Command Edition).

   Windows

   Backup destination directory: X:\Backup\irep\rep001_back

   Repository name: rep001

   Database storage directory: C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 –dataonly
Data already exists in database store.
(C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)
Are you sure of deleting data in database store? (y/n):y
IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back
[rep001]
```

   Solaris OE

   Backup destination directory: /backup/irep/rep001_back.tar.Z

   Repository name: rep001

   Database storage directory: /var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data

```
#ireprestsys -f /backup/irep/rep001_back.tar.Z –R rep001 –dataonly
Data already exists in database store.
(/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z[rep001]
```

Linux

Backup destination directory: /backup/irep/rep001_back.tar.Z

Repository name: rep001

Database storage directory: /var/opt/FJSVena/DStores/FJSVirep/rep001/data

```
#ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 –dataonly
Data already exists in database store.
(/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z[rep001]
```

Changing the Repository Settings of the Slave Server

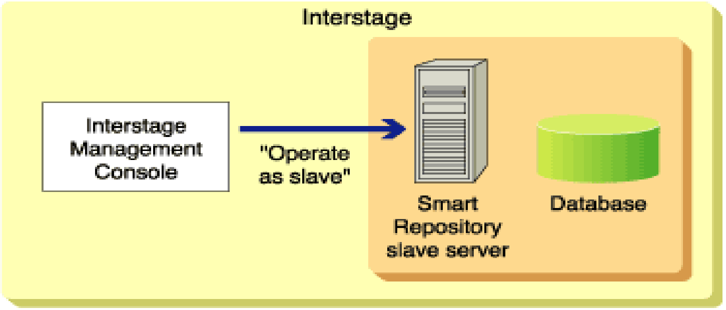


Figure 2-12 Change Repository Settings of the Slave Server

Change the repository settings of the slave server to have it operate in replication mode. The following procedure describes how to change the settings using the Interstage Management Console on the slave server.

1. Click [System] > [Service] > [Repository] (If on the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and then select the slave repository in the [Repository: View Status] window.
2. Click [Detailed Settings (View)] and then under [Replication Settings], select "Slave" as the [Operation mode].
3. Select the host name of the master server machine in the newly-displayed [Slave operation settings].
4. Click the [Apply] button.
5. Check the check box of the changed repository, and then click the [Start] button to start the repository.

Changing the Repository Settings of the Master Server

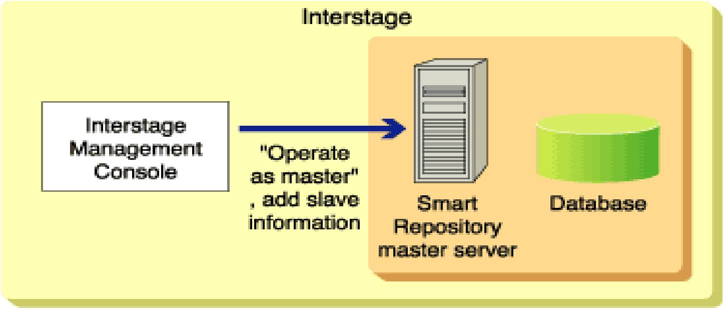

Interstage
Interstage Management Console
"Operate as master" , add slave information
Smart Repository master server
Database

Figure 2-13 Configure the Master Server with Slave Information

Configure the master server repository with information about the newly-added slave server repository. The following procedure describes how to configure the master server using the Interstage Management Console on the master server machine.

1. Click [System] > [Service] > [Repository] (If on the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and then select the master repository in the [Repository: View Status] window.
2. Click [Detailed Settings (View)]. If the [Operation mode] under [Replication Settings] is "Master," proceed to Step 3. If the setting is not "Master," select this option. [List of replication destination hosts will then display.
3. Click the [Add] button, and configure the information about the slave server machine for each item in [Replication destination host list]. Click the [Apply] button. If using SSL communication for replication operation, select "Yes" for [Present client certificate?], and the value of [SSL configuration] defined in the master server's SSL communication environment setup].

Note

– If "No" is selected in [Present client certificate?] while site certificates are registered, no SSL configuration will be needed. However, all site certificates will automatically be sent from the master server to the slave server. For security, it is recommended that select "Yes".

– Some slave server environment settings must match those configured in the master server repository. If one of these settings does not match, the application will continue operating and no error will display. However, since it may cause an error during operation, ensure that all settings are correct before applying the changes.

  [Create default tree?]

– Several seconds to several minutes are needed to change the repository settings. This includes the time needed to confirm the connection to the replication destination. The total time varies a little depending on the use of SSL, network environment, and machine performance.

4. Check the check box of the changed repository and then click the [Start] button to start the repository.

Procedure for Deleting a Slave Server during Replication Operation

The following figure illustrates the procedure for deleting a slave server during replication operation.

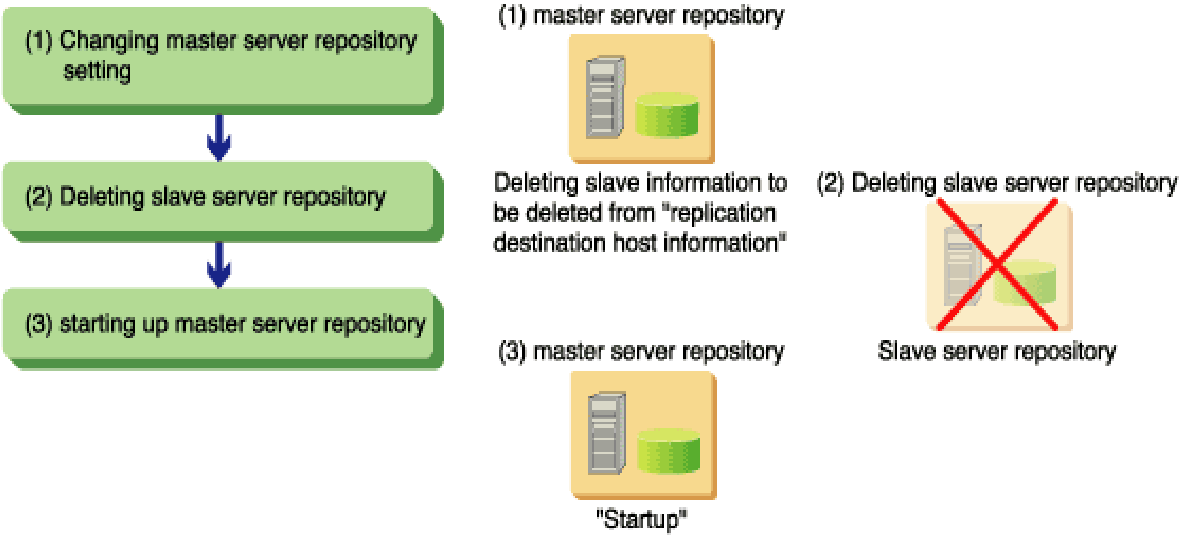

(1) Changing master server repository setting
(2) Deleting slave server repository
(3) starting up master server repository
(1) master server repository
Deleting slave information to be deleted from "replication destination host information"
(2) Deleting slave server repository
Slave server repository
(3) master server repository
"Startup"

Figure 2-14 Delete a Slave Server in Replication Mode

Changing the Repository Settings of the Master Server

This procedure involves deleting information about the slave server repository from the master server repository.

1. Stop the repository during the master operation. This is performed by using the Interstage Management Console connected to the machine of the master server.
2. Click [Detailed Settings [display]] on the [Environment settings] window of the stopped repository.
3. Select the slave repository to be deleted from [Replication destination host list]
4. Click the [Delete] button.

Deleting the Repository of the Slave Server

The repository of the slave server will be deleted.

1. Stop the repository in slave operation using the Interstage Management Console connected to the machine of the slave server.
2. Delete the stopped repository in slave operation.

Starting up the Repository of the Master Server

Use the instruction shown below to start the repository of the master server.

Start the repository in master operation using the Interstage Management Console connected to the machine of the master server.

Setting Items of the Interstage Management Console

This section describes the items to be set for the Interstage Management Console.

General Settings

- Repository Name
- Administrator DN
- Administrator DN password
- Public Directory
- Create default tree?
- Port number
- Enable SSL encryption?
- SSL port number
- SSL configuration
- Connection idle timeout

Database Settings

- Maximum number of searchable entries
- Cache Size
- Search Timeout
- User password encryption method
- Database Storage Directory

Access Log Settings

- Output Access Log?
- Output level
- Access log storage directory
- Rotation type
- Size
- Number of access log files

Replication Settings

- Operation mode

Slave Operation Settings

- Master host name

Master Operation Definition (Replication Connection Settings)

- Host name
- Port number
- Enable SSL encryption?
- Present client certificate?
- SSL configuration
- DN for connection
- Password for the connection.

Note

Do not directly edit the files created when setting up an environment for Smart Repository. If files are directly edited, operational problems may occur.

General Settings

Repository Name

Specify the repository name that identifies each repository, using a string of up to eight characters.

Allowable characters include alphanumeric characters and the underline (_). The first character must always be an alphabetical character. If an alphabetical upper-case character is specified, it will be converted into an alphabetical lower-case character. The initial value is "repnnn" (nnn are numeric characters 001, 002, 003 ...).

The repository name can be specified only during repository setup.

To enable replication, the [Repository name] value for the master and slave must be identical.

In Smart Repository, information is stored in Fujitsu Enabler. The following products of Interstage use Enabler.

- Interstage Apworks
- Interstage Contentbiz
- Interstage Portalworks

If any of these products and Smart Repository are both installed on the same server, the data store name and the repository name of Fujitsu Enabler used in these products must be different.

Administrator DN

Specify the DN (distinguished name) for the administrator who will manage the repository created in the DN format. The DN is a string of up to 512 bytes. The string specified in [Public Directory] will be added to the specified Administrator DN.

"cn", “ou", “o", “c", “l", and “dc" can be specified as an attribute of RDN (relative distinguished name) which constitutes the DN (distinguished name) format.

Alphanumeric characters, the minus sign (-), the period (.), and the underline (_) can be specified as an attribute value of RDN (relative distinguished name) which constitutes the DN (distinguished name) format.

Insert the equal sign (=) between the specified attribute name and attribute value of the RDN (relative distinguished name) which constitutes DN (distinguished name) format.

If multiple RDN (relative distinguished name) are specified, separate them with a comma (,). For example, "cn=manager" and "cn=manager, ou=managergroup" can be specified. The initial value is "cn=manager", it can only be modified when the repository is first created.

Note

It is not possible to specify multiple attributes for the RDN (relative distinguished name) of the Administrator DN (Multi-AVA cannot be used). For example, multiple attributes cannot be specified using the plus sign (+) for example, “cn=User001+sn=fujitsu".

Administrator DN Password

Use a string of up to 128 bytes to specify the password for the administrator to manage the created repository. . Allowable characters include alphanumeric characters, the comma (,), the plus sign (+), the equals sign (=), the minus sign (-), the period (.), and the underline (_). No initial value is provided.

Public Directory

Use a string of up to 512 bytes to specify the top entry that makes the repository public in the DN (distinguished name) format.

"cn", “ou", “o", “c", “l", and “dc" can be specified as an attribute of the RDN (relative distinguished name), which constitutes DN (distinguished name) format.

Alphanumeric characters, the minus sign (-), the period (.), and the underline (_) can also be specified as an attribute value of the RDN (relative distinguished name) which composes DN (distinguished name) format.

Specify equal sign (=) between the attribute name and the attribute value of RDN (relative distinguished name) which composes DN (distinguished name) format is specified.

If multiple RDN (relative distinguished name) are specified, separate them with a comma (,). For example,"ou=interstage,o=fujitsu,dc=com" and "c=jp" can be specified. The initial values are "ou=interstage,o=fujitsu,dc=com."

The public directory can only be modified when the repository is first created..

To enable replication, the value in [Public directory] must be the same for both master and slave.

Note

It is not possible to specify multiple attributes for the RDN (relative distinguished name) of the public directory (Multi-AVA cannot be used). For example, multiple attributes cannot be specified by using plus sign (+) like “ou=fujitsu+st=tokyo".

Create Default Tree?

Specify whether to create a default tree. Create the default tree structure which can be used for each common service. The initial value is Create.

- Yes (set by default)

  A default tree will be created under the top directory specified in [Public Directory].

- No

  Only the top directory specified in [Public Directory] will be created. No default tree will be created.

If create the tree is selected, a default tree structure that can be used commonly with the following services will be created:

- Single sign-on repository server
- Online inquiry function of the Interstage HTTP Server
- Security function of the J2EE applications
- User management on the LDAP of Interstage Portalworks

The default tree is constructed from the initial value of "ou=interstage,o=fujitsu,dc=com". It is specified in the public directory and when "Yes" is selected it will display as shown below. If the initial value of [Public Directory] is changed, "ou=interstage,o=fujitsu,dc=com" will be replaced by the new directory.

Tree to be created (DN format)	**Application**
ou=User,ou=interstage,o=fujitsu,dc=com	User information storage tree for each service
ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Access control information storage tree for single sign-on
ou=Resource,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Protected resource storage tree for single sign-on
ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Role definition storage tree for single sign-on

To enable replication, the value in [Create default tree?] must be the same for both the master and slave.

This item can be specified only when during repository setup.

Port Number

Specify the port number (between 1 and 65535) used for non-SSL communication.   The initial value is 389.

It is a good idea to specify the port number after designing the port numbers to be used by each service on the server.

The port number can be specified only during repository setup.

Note

There is a higher risk of services attempting to use the same ports if a port number other than the initial value is used. This is particularly relevant for port numbers between 1 and 1023 which are commonly-used.

Enable SSL encryption?

Specify whether to use SSL communication. If it is specified, the client-server authentication and encrypted communication of SSL will be used as the communication protocol between each service connected to the repository. This makes it possible to protect information and avoid threats such as tapping, falsification, and impersonation.

- Yes

  SSL communication is performed. The port number specified in [SSL port number] and the SSL configuration specified in [SSL configuration] will be used for communication.

- No (Default setting)

  SSL communication is not performed.

Only the [SSL Port number] and [SSL configuration] need to be specified if SSL communication is used.

Enable SSL encryption? can be defined only during repository setup.

Note

Since the normal (non-SSL) port will be set up even if "Yes" is specified in [Enable SSL encryption?], protection by the firewall will be needed.

SSL Port Number

Specify the port number (between 1 and 65535) used for SSL communication.

Specify the port number after designing the port numbers used by each service on the server. The initial value is "636."

Specify this item only if SSL communication is being used. The SSL port number can be specified only when creating a new repository.

Note

There is a higher risk of services attempting to use the same ports if a port number other than the initial value is used. This is particularly relevant for port numbers between 1 and 1023 which are commonly-used.

SSL Configuration

To conduct SSL communication, create and specify a SSL configuration to be used for SSL communication. No SSL configuration is provided by default.

Connection Idle Time

Specify the period after which connection to the client is disconnected. Values can be between 0 and 3600 seconds. The initial time is "900" seconds.

If "0" is specified, the connection idle time will be unlimited.

Database Settings

Maximum number of searchable entries

Specify the maximum number of entries to be returned after performing a search (between 0 and 10000). The maximum number is unlimited if a search is performed by an Administrator DN. The initial value is "500"

If "0" is specified, the maximum number of entries returned is unlimited.

Cache Size

Specify the cache size when performing a search. Values can be between 100 and 65535 pages. One page corresponds to 4KB. The initial time is "1000" pages.

Search Timeout

Specify the timeout period when performing a search (between 0 and 3600 seconds). The timeout period is unlimited if the search is performed by an Administrator DN. The initial time is "3600" seconds.

Point

Operation when the maximum number of searchable entries and search timeout are specified.

The maximum number of searchable entries and the search timeout can be defined on the Smart Repository server and the client respectively.

The client refers to the ldapsearch command, Entry Administration Tool, and user applications that access the Smart Repository server.

Table 2-3 shows the relationship between the Smart Repository server and client designations.

Table 2-3 Smart Repository Server and Client Designations

DN accessed from the client (bound DN)	Client specified value	Relationship between server specified value and client specified value	Operation
Administrator DN	Present	Client < Server	Client specified value is valid
	Present	Client >= Server	Client specified value is valid
	None	-	Unlimited
	0	-	Unlimited
Others	Present	Client < Server	Client specified value is valid
	Present	Client >= Server	Server specified value is valid
	None	-	Server specified value is valid
	0	-	Server specified value is valid

The following shows how to specify the maximum number of searchable entries and search timeout on the client:

- ldapsearch command

  -l option (search time limit) and -z option (search size limit) of "ldapsearch" in Reference Manual (Command Edition).

- Entry Administration Tool

  "Entry Administration Tool" > "Operate Entry" > "Search Entry/Attribute" > "Specify search option" in the Entry Administration Tool Help

User Password Encryption Method

Specify the encryption method used when storing user password attributes. The initial value is "SHA."

- SHA

  The password is encrypted by the irreversible SHA-1 encryption algorithm. The password is encrypted before being returned to the client..

- Individual encryption

  The password is encrypted by an individual encryption method. The password is encrypted before being returned to the client.

- MD5

  The password is encrypted by the irreversible MD5 encryption algorithm. The password is encrypted before being returned to the client..

- SMD5

  The password is encrypted by the irreversible MD5 encryption algorithm. The password is encrypted before being returned to the client.

  In contrast to the MD5 method, a different (encrypted) password is generated each time the same password is submitted by the client.

- SSHA

  The password is encrypted by the irreversible SHA-1 encryption algorithm. The password is encrypted before being returned to the client.

  In contrast to the SHA method, a different (encrypted) password is generated each time the same password is submitted by the client.

- Crypt Solaris OE Linux

  The password is encrypted by the irreversible Crypt encryption algorithm. The password is encrypted before being returned to the client.

- No encryption

  The password is not encrypted. When it is returned to the client, the password is not encrypted.

For the functions of each encryption method, see "User password encryption method" In Chapter 1 – Overview.

The user password encryption method can be specified only during system setup.

To enable replication, [User password encryption method] for the master slave must by identical.

Database Storage Directory

Enter the storage directory of the database using the full specification.

The actual storage directory of the database is defined by appending "/repository_name/data" (or for Windows(R) “\repository_name\data") to the specified storage directory.

Table 2-4 lists the valid directory lengths and characters.

Table 2-4 Valid Database Storage Directory Characters

	Windows	Solaris OE	Linux
Length	Up to 192 bytes	Up to 242 bytes	Up to 242 bytes
Valid characters	- En-size alphanumeric character - Dollar sign ($) - Ampersand (&) - Single quotation mark (') - Plus sign (+) - Minus sign (-) - Period (.) - Equals sign (=) - at sign (@) - Underline (_) - Back quotation mark (`) - Tilde (~) - Square bracket ([]) - Brace ({}) - Space ( ) - Colon (:) - Slash (/) - Backslash (\)	- En-size alphanumeric character - Slash (/) - Minus sign (-) - Underline (_) - Tilde (~)	- En-size alphanumeric character - Slash (/) - Minus sign (-) - Underline (_) - Tilde (~)

The multi-byte code system cannot be used. In Windows®, the colon (:) can be used only when specifying a drive character and the backslash (\) can be used only to separate directories. When specifying a drive, include "\" for example, "C:\"

The initial values are as follows:

Windows

```
"C:\Interstage\Enabler\EnablerDStores\IREP" (default installation path)
```

Solaris OE

```
"/var/opt/FJSVena/EnablerDStores/FJSVirep"
```

Linux

```
"/var/opt/FJSVena/DStores/FJSVirep"
```

Always specify this item. This item can be specified only for new creation.

To enable replication, [Database storage directory] for the master and the slave must by identical.

Note

- Set the database storage directory after ensuring that sufficient disk space is available.
- Note the Permissions settings when any database storage directory other than the initial value is set.

Windows

When specifying a database storage directory other than the default, give the "Administrators" group full control access to all directories within the directory.

Solaris OE Linux

When specifying a database storage directory other than the default, set the owner of all directories within the storage directory to "oms" and permit "read," "write," and "execute" to the owner.

The following shows an example of setting permissions on the storage directory (the database storage directory is assumed to be "/data/user"):

1. If no storage directory is created, create a database storage directory. By specifying the -p argument, a non-existent parent directory can also be created.

   ```
   mkdir -p /data/user
   ```

2. Set the permissions of "read," "write," and "execute" to the directory. By specifying the -R argument, the permissions can be set recursively through the sub-directories.

   ```
   chmod -R 700 /data
   ```

3. Set "oms" to the directory as its owner. By specifying the -R argument, the owner can be set recursively through the sub-directories.

```
chown -R oms /data
```

Access Log Settings

Output Access Log?

Specify whether to output the access log.

- Yes (default value)

  Outputs the access log.

- No

  The access log will not be output.

If the access log is unnecessary, there is no need to set values for [Output types], [Access log storage directory], [Rotation type], [Size], and [Number of access log files to maintain].

Output types

Specify the output content of the access log. If output the access log has been selected, at least one output level must be specified. "Client requests" and "Server errors" are set by default.

- Client requests (default value)

  Outputs request information from the client.

- Server errors

  Outputs error responses of the server. (default value)

- Normal Server responses

  Outputs normal responses of the server.

- Server search result of DN

  Outputs search result responses of the server.

Access log storage Directory

Enter the access log storage directory of the access log using the full specification.

The actual access log storage directory of the access log is a directory defined by appending "/repository_name/log" (for Windows(R),“\repository_name\log") to the specified access log storage directory.

Table 2-5 lists the valid directory lengths and characters.

Table 2-5 Valid Access Log Storage Directory Characters

	Windows	Solaris OE	Linux
Length	Up to 192 bytes	Up to 960 bytes	Up to 960 bytes
Valid character	- En-size alphanumeric character - Dollar sign ($) - Ampersand (&) - Single quotation mark (') - Plus sign (+) - Minus sign (-) - Period (.) - Equals sign (=) - at sign (@) - Underline (_) - Back quotation mark (`) - Tilde (~) - Square bracket ([]) - Brace ({}) - Space ( ) - Colon (:) - Slash (/) - Backslash (\)	- En-size alphanumeric character - Slash (/) - Minus sign (-) - Underline (_) - Tilde (~)	- En-size alphanumeric character - Slash (/) - Minus sign (-) - Underline (_) - Tilde (~)

The multi-byte code system cannot be used. In Windows®, the colon (:) can be used only when specifying a drive character and the backslash (\) can be used only to separate directories. When specifying a drive, include "\" for example, "C:\"

The initial values are as follows:

Windows

```
"C:\Interstage\IREP\var" (default installation path)
```

Solaris OE Linux

```
"/var/opt/FJSVirep"
```

Always specify this item.

Note

- Set the access log storage directory after ensuring that sufficient disk space is available.
- Note the Permissions settings when any access log storage directory other than the initial value is set.

Windows

When specifying an access log storage directory other than the default, give the "Administrators" group full control access to all directories within the access log storage directory.

Rotation Type

Specify how to split the access log. If the log reaches the maximum size, the number of files set in [Number of access log files to maintain] will be saved. "Size" is set by default.

- Size

  Rotation in file size
- Daily

  Rotation in days
- Monthly

  Rotation in months

Size

Specify the maximum size of the access log between 1 and 1024 MB. If the log reaches this size, the number of files set in [Number of access log files to maintain] will be saved. The initial value is "5" MB.

Number of access log files to maintain

Specify the number of access log files between 1 and 99. If this number is exceeded, the access logs will be deleted in order of date. The initial value is "2."

Replication Settings

Operation mode

Specify the operating mode with regards to replication. The operating mode must be specified for each host. "Stand-alone" is set by default.

- Stand-alone

  Operated on a stand-alone basis. No replication operation is performed.
- Slave

  Operated as a slave.

- Master

  Operated as the master.

Note

Once the operating mode is set to "Slave" or "Master," it cannot be changed to another mode.

Slave Operation Settings

Master host name

Specify the host name of the master using a string of up to 106 bytes. Only host names that can be address-resolved are valid. Allowable characters include en-size alphanumeric characters, the minus sign (-), the period (.), and the underline (_). No initial value is provided.

When performing a cluster operation, specify the host names of the operation and standby nodes separated by a comma (,) in a string of up to 106 bytes. For example, "cluster01, cluster02." The same host name cannot be specified as both the operation node and standby node.

This item can be specified only when "Slave" is specified in [Operation mode].

Note

If the network environment of the server machine is changed while the Interstage Management Console is active, set the environment after restarting the Interstage Management Console. If JDK1.3 or JRE1.3 is used as the execution environment of the Interstage Management Console, be sure to restart. It is recommended to restart the Interstage Management Console also when JDK1.4 or JRE1.4 is used. If the Interstage Management Console is not restarted, network address resolution may temporarily fail.

For details of restarting the Interstage Management Console, see "Configuring the Interstage Management Console" in the Operator's Guide.

Master Operation Definition (Replication Connection Settings)

Host name

Specify the host name of the slave specified in advance using a string of up to 106 bytes. Only host names that can be address-resolved are valid. Characters that can be used include en-size alphanumeric characters, the minus sign (-), the period (.), and the underline (_). No initial value is provided.

When performing a cluster operation of the slave, specify the logical host name in the cluster environment.

The host name can be specified only when adding [Replication connection settings].

Note

If the network environment of the server machine is changed while the Interstage Management Console is active, set the environment after restarting the Interstage Management Console. If JDK1.3 or JRE1.3 is used as the execution environment of the Interstage Management Console, be sure to restart. It is recommended to also restart the Interstage Management Console when JDK1.4 or JRE1.4 is used. If the Interstage Management Console is not restarted, network address resolution may temporarily fail.

For details of restarting the Interstage Management Console, see "Configuring the Interstage Management Console" in the Operator's Guide.

Port number

Specify the port number for replication of the slave between 1 and 65535. The initial value is "389."

The port number can be specified only when adding [Replication Connection Settings].

Enable SSL encryption?

Specify whether SSL will be used with the port number specified for replication of the slave. "No" is set by default.

Enable SSL encryption? can be specified only when adding [Replication Connection Settings].

- Yes

  SSL communication performed. Specify whether to present the client certificate in [Present client certificate?].

- No

  SSL communication is not performed.

If SSL communication is not going to be used, there is no need to specify [SSL configuration] and [Present client certificate?].

To use SSL communication with the port number specified in for replication of the slave, "Yes" must always be specified.

Present client certificate?

When using the SSL communication with the port number specified for replication of the slave, select to present the client certificate?. "No" is set by default.

- Yes

  A client certificate needs to be presented when conducting SSL communication. Specify the client certificate to be presented in [SSL configuration].

- No

  No client certificate needs to be presented when conducting SSL communication.

If "No" is selected, the contents of [SSL configuration] will be invalidated.

If "Authenticate (Always authenticate a client certificate)" is specified in [Client authentication] of the environment settings of the SSL configuration specified for the slave, "Yes" must always be specified.

This setting must be specified if "Yes" is selected in [Enable SSL encryption?] when adding [Replication Connection Settings].

Note

> If any client certificate is installed in the Interstage certificate environment, the client certificate will be presented even if "No" is selected.

SSL configuration

To conduct SSL communication that presents the client certificate, create an SSL configuration in which the client certificate is specified and then specify the created SSL configuration.

If "Authenticate (Always authenticate a client certificate)" is specified in [Client authentication] of the environment settings of the SSL configuration specified for the slave, the SSL configuration must always be specified.

This setting must be specified if "Yes" is specified in [Enable SSL encryption?] when adding [Replication Connection Settings] and "Yes" is specified in [Present client certificate].

DN for the connection

Specify, in a string of up to 512 bytes, the "Administrator DN (distinguished name)" for connecting to the slave. The public directory will be added to the specified DN (distinguished name) for connection.

"cn", "ou", "o", "c", "l", and "dc" can be specified as an attribute of the RDN (relative distinguished name), which uses DN (distinguished name) format.

Alphanumeric characters, the minus sign (-), the period (.), and the underline (_) can also be specified for an attribute value of the RDN (relative distinguished name) which comprises the DN (distinguished name) format.

Insert the equal sign (=) between the specified attribute name and attribute value of the RDN (relative distinguished name), which composes DN (distinguished name) format.

If multiple RDN (relative distinguished name) are specified, separate them with a comma (,). For example, "cn=manager" and "cn=manager, ou=managergroup". The initial value is "cn=manager",

[DN for the connection] can be specified only when adding "Replication Connection Settings".

Note

> It is not possible to specify multiple attributes for the RDN (relative distinguished name) of the DN for connection (Multi-AVA cannot be used). For example, multiple attributes cannot be specified by using the plus sign (+) like “cn=User001+sn=fujitsu".

Password for the connection

Specify (using a string of up to 128 bytes) the password of the "DN (distinguished name) for manager" for the slave as a password for connecting to the slave. Valid characters include alphanumeric characters, the comma (,), the plus sign (+), the equals sign (=), the minus sign (-), the period (.), and the underline (_). No initial value is provided.

Chapter 3

Entry Management

This chapter explains how to manage entries;

The following three methods can be used to manage entries:

- Use the command
- Use the Entry Administration Tool
- Use SDK.

Table 3-1 lists the access restrictions to entries that are set in Smart repository. However, 'Administrator DN' access is not restricted.

O: Operable, X: Not operable, -: Not applicable

Table 3-1 Smart Repository Access Restrictions

Attributes, entries	Access type	Authenticated user	Anonymous user
Personal userPassword attribute	Modify	O	-
	Reference	O	-
	Search	O	-
	Compare	O	-
Others' userPassword attribute	Modify	X	X
	Reference	X	X
	Search	X	X
	Compare	O	X
Personal entries	Modify	O	-
	Reference	O	-
	Search	O	-
	Compare	O	-
Other attributes and entries	Modify	X	X
	Reference	O	O
	Search	O	O
	Compare	O	O

Note

- No schema check is performed when entries are modified in Smart Repository.

  This means that if inappropriate entry modifications (such as deleting a required attribute in an entry or adding an attribute to the Object Class that must not be added) are performed, information in the repository will be contradictory. Sufficient care must therefore be taken when modifying entries.

- Entries of the repository in slave operation cannot be added, modified, or deleted.

Schemata that can be used in Smart Repository

Information about entries that need to be added or modified in a repository must comply with a schema. If an add/modify request does not obey the schema, an error is returned from the repository.

Table 3-2 shows the elements of the LDAP schema.

In Smart Repository, 'Object class definition,' 'Attribute type definition,' 'Attribute syntax definition,' and 'Matching rule definition' can be used.

Table 3-2 Elements of the LDAP Schema

Element	Explanation
Object class definition	Defines the class type, base class, and attributes that an entry can hold.
Attribute type definition	Defines the type of data that an attribute can hold. The attribute type is defined by element, such as the name, attribute syntax, and matching rule.
Attribute syntax definition (syntax)	Defines the characters that can be used for an attribute value and attribute value type.
Matching rule definition (matching rule)	Defines the attribute matching rules that are used to compare and search.
Name format definition	Defines the attributes that can be used for RDN. This element cannot be used by Smart Repository.
DIT structure rule definition	Defines the entry placement restrictions. This element cannot be used by Smart Repository.
DIT content rule definition	Defines the combination of object classes. This element cannot be used by Smart Repository.

The following explains the object class definition and attribute type definition. Details about the attribute syntax definition and matching rule definition is explained in 'Attribute type definition.'

Note

In Smart Repository, the standard schema defined by RFC is used. No extension function of schema is provided.

For information about the schema definitions that can be used in Smart Repository, see Appendix C - List of Object Classes and Appendix D - List of Attributes.

Object Class Definition

An object class definition consists of the following elements:

- Object class OID
- Object class name
- Base class
- Object class type
- Required attributes
- Optional attributes.

Object Class OID

Object identifier, OID (Object IDentifier), to identify each object class.

OID is assigned not only to each object class, but also to each element in LDAP. This is an ISO standard.

Object Class Name

Name of the object class to be defined.

Base Class

This is a definition of an object class on which another object class is based. If defining some object class, it may be defined based on the definition of another object class. The object class on which a new definition is based is called the base class.

A derived class inherits the required attributes and optional attributes from the base class.

Object Class Type

An object class can be divided into one of the following categories, abstract type (ABSTRACT), structural type (STRUCTURAL), or auxiliary type (AUXILIARY). These categories are explained in Table 3-3.

Table 3-3 Object Class Types

Type	Explanation
Abstract type (ABSTRACT)	An object class provided to define other object classes. Top is a typical example of this type of object class. An entry that belongs to an abstract object class only cannot exist.
Structural type (STRUCTURAL)	An object class from which an entry can be created. An entry must always belong to one of the structural object classes.
Auxiliary type (AUXILIARY)	An object class that cannot create an entry alone and can create one only in combination with another structural object class. An entry that belongs to an auxiliary object class only cannot exist.

Required Attributes

Attributes of an object class that must be registered when using the class.

Optional Attributes

Attributes (not required) of an object class that are used as additional information when using this class.

For information about the object class definition that can be used in Smart Repository, see 'List of Object Classes.'

Attribute Type Definition

An attribute type definition consists of the following elements:

- Attribute type OID
- Attribute type name
- Base attribute type
- Matching rules
  - Matching rules of equality
  - Matching rules of ordering
  - Matching rules of substring matching
- Attribute syntax
- Single flag

Attribute Type OID

OID to identify the attribute type.

Attribute Type Name

Name of the defined attribute.

Base Attribute Type

Attribute on which another attribute is based. The attribute syntax and matching rules are inherited from the base attribute type. However, in contrast to the object classes, there are also some cases where an attribute type does not inherit from another attribute type.

Matching Rules

Matching rules describe the conditions checked when comparing attributes. If the matching rules are not specified, comparisons between attributes cannot be made to match them.

Matching Rules of Equality

Matching rules based on values being equal are applied for searches and other operations.

Table 3-4 Matching Rules of Equality

Name	Explanation
objectIdentifierMatch	OID
distinguishedNameMatch	DN
caseIgnoreMatch	Case-insensitive, space ignored
caseExactMatch	Case-sensitive, space ignored
numericStringMatch	Numeric string
booleanMatch	True/false
octetStringMatch	Optional octet string
uniqueMemberMatch	Name with an optional UID
caseExactIA5Match	Case-sensitive, space ignored
caseIgnoreIA5Match	Case-insensitive, space ignored

Matching Rules of Ordering

Matching rules based on inequality are applied for searches and other operations.

Table 3-5 Matching Rules of Ordering

Name	Explanation
caseIgnoreOrderingingMatch	Case-insensitive, space ignored
caseExactOrderingingMatch	Case-sensitive, space ignored
numericStringOrderingingMatch	Numeric string

Matching Rules of Substring Matching

Matching rules are applied for searches or comparisons with a partial string.

Table 3-6 Substring Matching

Name	Explanation
caseIgnoreSubstringsMatch	Case-insensitive, space ignored
caseExactSubstringsMatch	Case-sensitive, space ignored
numericStringSubstringsMatch	Numeric string

Attribute Syntax

Format of the attribute values:

Table 3-7 Attribute Values Syntax

Syntax	Allowable Value
Audio	Sound data can be used.
Binary	Binary data can be used.
Bit String	Bit strings can be used. Example: '0101111101'B
Boolean	Either TRUE or FALSE can be used. Example: TRUE
Certificate	Certificate data can be used.
Certificate List	Certificate list data can be used.
Certificate Pair	Certificate pair data can be used.
Country String	2-character strings listed in ISO 3166 can be used.
Directory String	Usable within the range handled by UTF-8. In terms of characters, this corresponds to being within the Unicode range.
DN	DN can be used. Example: cn=User001,o=fujitsu,dc=com
Enhanced Guide	Used by the X.500 client for creating a search filter Example: person#(sn)#oneLevel
Facsimile Telephone Number	Strings similar to those of Printable String can be used.
Fax	Octet strings including Group3 FAX images can be used.
Generalized Time	The local time (YYYYMMDDhhmmss.pZ format) or the international standard time (YYYYMMDDhhmmss.p format) can be used.
IA5 String	The CCITT International Alphabet No.5 (equivalent to ASCII) can be used.
INTEGER	Numeric characters can be used. Example: 1321
JPEG	JPEG data can be used.
Numeric String	Numeric characters (0 to 9) and space can be used. Example: 1997
Octet String	Byte strings (Each byte is any value between 0x00 and 0xFF) can be used.
OID	OID can be used. Example: 1.2.3.4
Other Mailbox	Electronic mailbox data other than X.400 and RFC822 can be

Syntax	**Allowable Value**
Audio	Sound data can be used.
Binary	Binary data can be used.
Bit String	Bit strings can be used. Example: '0101111101'B
Boolean	Either TRUE or FALSE can be used. Example: TRUE
Certificate	Certificate data can be used.
Certificate List	Certificate list data can be used.
Certificate Pair	Certificate pair data can be used.
Country String	2-character strings listed in ISO 3166 can be used.
	used. The format is as follows: mailbox-type '$' mailbox mail-type is the type of mail and mailbox is a mail address Example: user001@interstage.fujitsu.com

Postal Address	Usable within the range (Unicode) handled by Directory String
	*1: Using alphanumeric characters only results in the following format. Up to six dstring can be combined.
	postal-address = dstring *('$' dstring)
	dstring = 30 alphanumeric characters

Presentation Address	The format described by RFC1278 can be used.
Printable String	Alphanumeric characters and the following symbols can be used: - Space - ''' (Single quotation mark) - '(' (left bracket) - ')' (right bracket) - '+' (plus sign) - ',' (comma) - '-' (Minus sign) - '.' (period) - '/' (slash) - ':' (colon) - '=' (equals sign) - '?' (question mark) -

Syntax	Allowable Value
Audio	Sound data can be used.
Binary	Binary data can be used.
Bit String	Bit strings can be used. Example: '0101111101'B
Boolean	Either TRUE or FALSE can be used. Example: TRUE
Certificate	Certificate data can be used.
Certificate List	Certificate list data can be used.
Certificate Pair	Certificate pair data can be used.
Country String	2-character strings listed in ISO 3166 can be used.
Protocol Information	Protocol information of each network address can be used.
Telephone Number	Characters similar to those of Printable String can be used. *1: Using '-' (Minus sign) and space results in the following examples: If searched with telephoneNumber=0123* 012-345-6789 0123456789 Both hit.

Teletex Terminal Identifier	Identifiers of the Teletex terminals can be used. The format is as follows:
	teletex-id = ttx-term 0*('$' ttx-param)
	ttx-term = printable string
	ttx-param = ttx-key ':' ttx-value
	ttx-key = 'graphic' / 'control' / 'misc' / 'page' / 'private'
	ttx-value = octet string
	The first printable string is the first part of the Teletex terminal identifier to be encrypted. 0 or more octet string is the subsequent part of the Teletex terminal identifier.

Telex Number	The Teletex numbers can be used. The format is as follows: actual-number '$' country '$' answerback actual-number syntactically represents the number part of the Teletex number that is to be encrypted. Country is the country code of Teletex and answerback is the return code for the Teletex terminal.
UTC Time	The local time (YYMMDDhhmmssZ format) or the international standard time (YYMMDDhhmmss format) can be used.

Single Flag

The single flag indicates whether one or multiple attribute values can be set.

For example, the telephone number may use multiple attributes, but using multiple attributes for an employee number could cause problems. In such a case, set the single flag to True.

For the attribute type definition, attribute syntax definition, and matching rule definition that can be used in Smart Repository, see 'List of Attributes.'

Using the Command to Manage Entries

This section explains how to manage entries by command.

Entry information can be fetched into a file from the database in Smart Repository. This operation is called exporting. At this point, the file is stored in the LDIF.

It is also possible to register a large amount of entries in the database in Smart Repository using the CSV or LDIF files. This operation is called importing.

When the CSV file is used, the irepmodifyent command is used for importing.

When the LDIF file is used, the ldapmodify command is used for importing and the ldapsearch command is used for exporting.

Importing using the CSV File

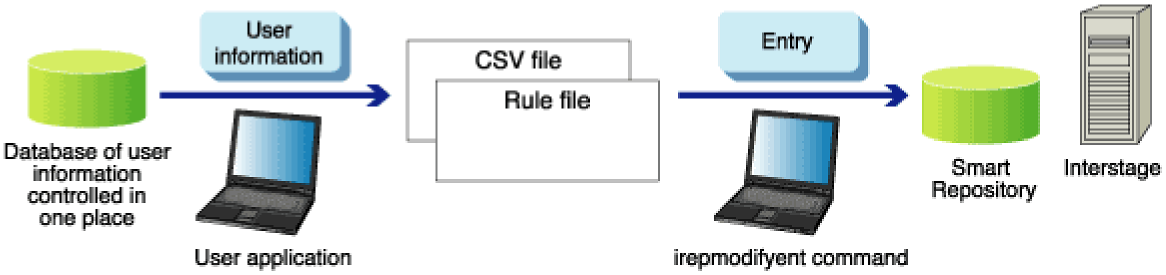


Figure 3-1 Import Flow using CSV File

Importing and Exporting using the LDIF File

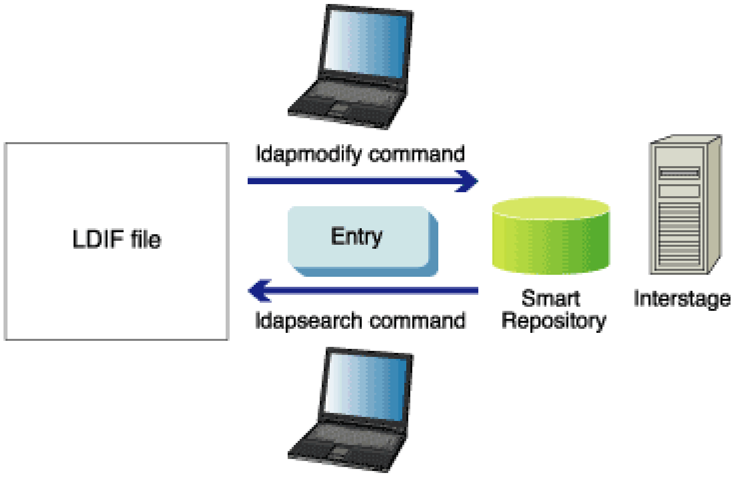


Figure 3-2 Import and Export using the LDIF file

Using the CSV File

Once information has been fetched from source data managed in an external database and saved in a CSV file, the data in the CSV file can be used to perform addition, modification and deletion of entries to the database of Smart Repository.

In the CSV file, information required to add, delete, or modify one entry is described in one line. A comma is used as the delimiter for each record (item). Double quotation marks (") should enclose values that include commas.

It is necessary to define the meaning of each item in the CSV file and operations on entries in an XML rule file. To import user information using the CSV file, the rule file must also be specified in the irepmodifyent command.

Some sample files are placed in the following locations.

Windows

```
C:\Interstage\IREP\sample\csv\
```

Solaris OE Linux

```
/opt/FJSVirep/sample/csv/
```

- CSV file sample to add an entry: add.csv
- CSV file sample to delete an entry: del.csv
- CSV file sample to modify an entry: mod.csv
- Rule file sample: rule.xml

The repository setting used by the sample files is as follows:

Repository host name	**hostname**
Administrator DN password	admin
Others	Use the initial value.

Using the LDIF File

LDIF (LDAP Data Interchange Format) is a standard format used to describe directory entries in the text format and is defined by RFC2849. LDIF is used to add entries to the repository and to change entry information in the repository.

The following types of LDIF are available:

1. Standard format to describe entry information.

   Use this format to save time if a large number of entries needs to be added to the repository

2. Modification format to describe modification information of entries.

   Use this format to change entry information in the repository.

Some LDIF file samples or file samples that can perform the same operations as those of the above CSV file samples are placed in the following locations. Use these files to check processing results.

Windows

```
C:\Interstage\IREP\sample\ldif\
```

Solaris OE Linux

```
/opt/FJSVirep/sample/ldif/
```

- LDIF file sample to add an entry: addldif.txt
- LDIF file sample to delete an entry: delldif.txt
- LDIF file sample to modify an entry: modldif.txt
- LDIF file sample to change the entry name: nameldif.txt

CSV and Rule Files

The following section explains the formats that are used for the CSV and rule files.

CSV File

Entry information to be imported is defined as follows only for the 0th item (The item count starts with '0'). Operations on the repository can be specified.

If any value other than the specified values (including the case in which nothing is described) is described for the 0th item, the line is considered to be a comment line.

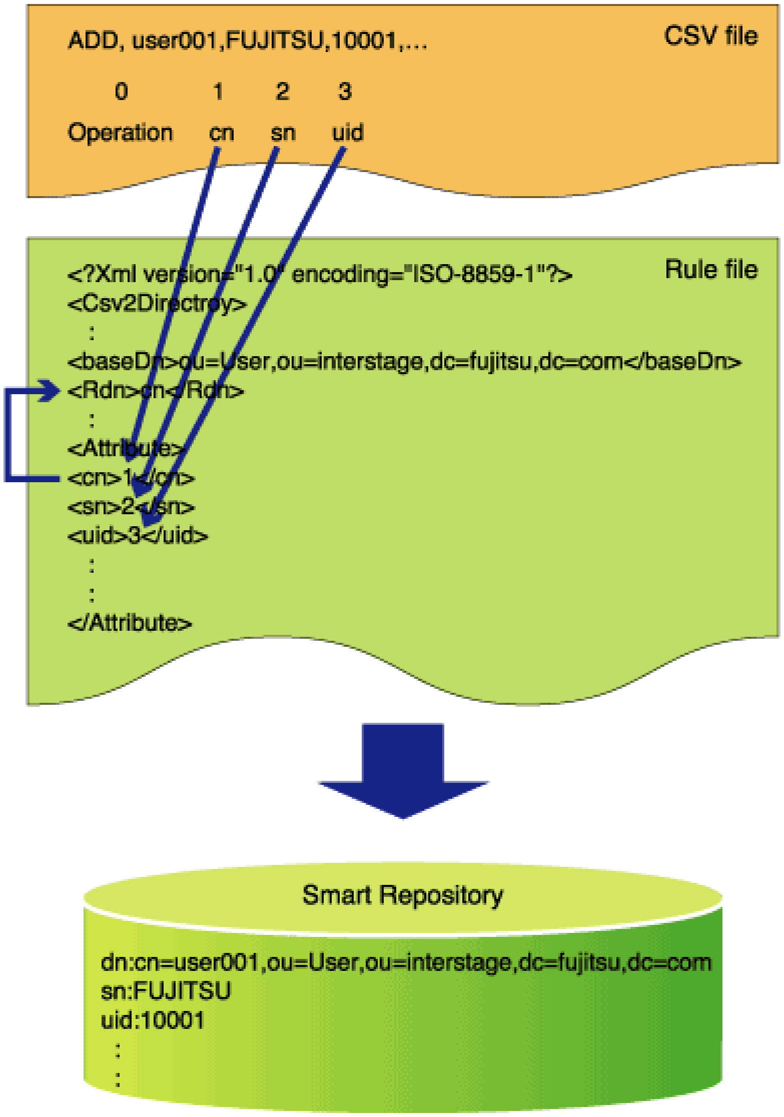
Contents of the first and subsequent items can be freely defined by specifying a rule file.

Specified value	Meaning
ADD	Adds an entry.
DEL	Deletes an entry.
MOD	Modifies an entry.

If 'MOD' is specified on an entry that does not exist in the repository, the 'ADD' operation is performed.

Rule File

The rule file is a file that defines the conversion rules used to register (modify and delete) CSV file information in the Smart Repository database. Figure 3-3 shows the relationship between the CSV file and rule file.



```
ADD, user001,FUJITSU,10001,...
```

```
<?Xml version="1.0" encoding="ISO-8859-1"?>
<Csv2Directroy>
  :
<baseDn>ou=User,ou=interstage,dc=fujitsu,dc=com</baseDn>
<Rdn>cn</Rdn>
  :
<Attribute>
<cn>1</cn>
<sn>2</sn>
<uid>3</uid>
  :
  :
</Attribute>
```

```
dn:cn=user001,ou=User,ou=interstage,dc=fujitsu,dc=com
sn:FUJITSU
uid:10001
  :
  :
```

Figure 3-3 Relationship between CSV and Rule File

This section explains the rule file format.

Since the following tags describe the XML declaration and DTD (document type definition), they must be included at the beginning of a rule file. It is recommended that tags are used by copying them from the sample file.

```
<?xml version="1.0" encoding="EUC-JP" ?>
<!DOCTYPE Csv2Directory [
<!ELEMENT Rule (name, baseDn, midDn?, Rdn+, DnChange?, objectClass+,
attributeSeparator?, unique*, CSV, fixed?)>
<!ELEMENT CSV (ldapop?, Attribute)>
<!ELEMENT ldapop (op?, ldapadd?, ldapdelete?, ldapmodify?)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT baseDn (#PCDATA)>
<!ELEMENT Rdn (#PCDATA)>
<!ELEMENT objectClass (#PCDATA)>
<!ELEMENT attributeSeparator (#PCDATA)>
<!ELEMENT op (#PCDATA)>
<!ELEMENT ldapadd (#PCDATA)>
<!ELEMENT ldapdelete (#PCDATA)>
!ELEMENT ldapmodify (#PCDATA)>
]>
```

The following explains the elements that constitute a rule file. Figure 3-4 is a configuration diagram of elements.

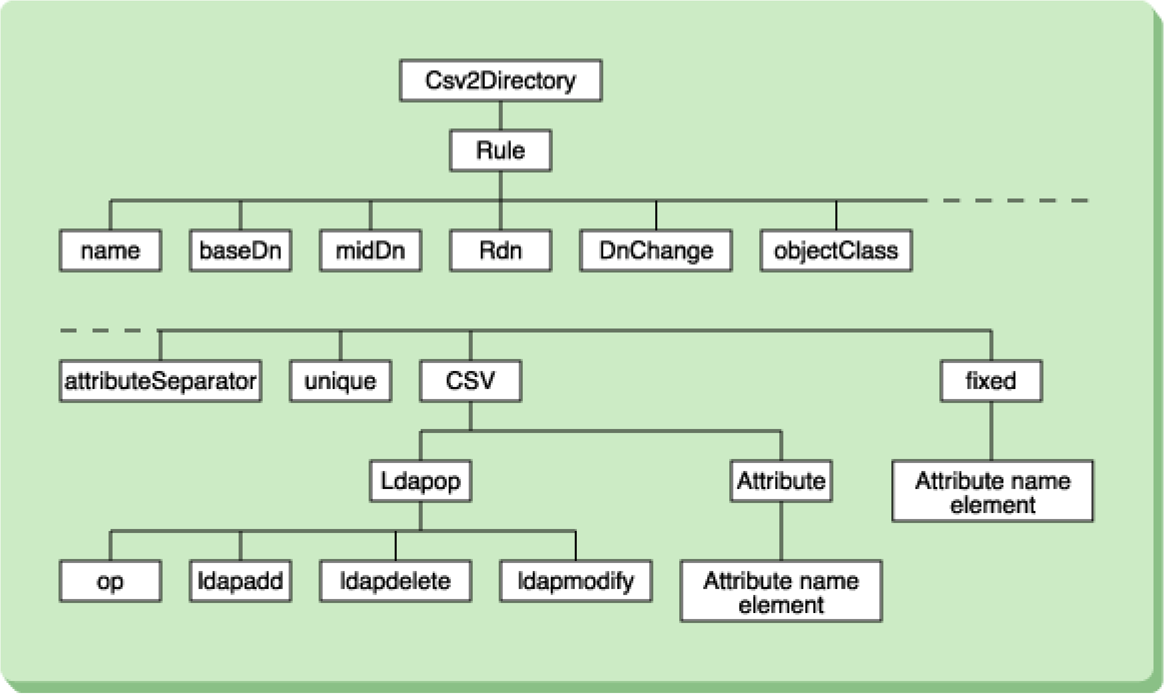


Figure 3-4 Configuration Diagram of Elements

Note

The following lists the general notes related to the description of a rule file:

- If no value of a tag is specified, the tag can be handled as no tag description.
- The tag name is case-sensitive. However, the attribute name tag, which is an attribute or fixed element, is case-insensitive.
- If the hierarchical position of a tag is correct, the order of occurrence of the tag does not matter. Conversely, if the description of the hierarchical position of a tag is incorrect, the tag will be ignored.
- If any tag other than those tags needed (element and attribute name tags explained above) for the description of a rule file is described, the tag will be ignored.
- The tags and values in the ldapop tag hierarchy and below are fixed. Do not change them. Do not move or copy them to other locations. If any of them is changed, no guarantee of operation can be provided.

- If two tags with the same name are described at different locations and they are in the same hierarchical position, they will be processed together.

The following explains each element.

Csv2Directory

Settings

No setting

Required or Optional

Required

This element can be set only once.

Lower Element

Rule

Rule

Settings

No setting

Required or Optional

Required

Upper Element

Csv2Directory

Lower Element

name, baseDn, midDn, Rdn, DnChange, objectClass, attributeSeparator, unique, CSV, fixed

name

Settings

This value does not affect command execution. Use the sample description as is.

Initial Value

None

Required or Optional

Required

This element can be set only once.

Upper Element

Rule

baseDn

Settings

Enter the base DN during entry operation in the DN format.

Initial Value

None

Required or Optional

Required

This element can be set only once.

Upper Element

Rule

midDn

Settings

If the target entry is not immediately below the base DN, specify an intermediate RDN for remedy in the DN format.

Initial Value

None

Required or Optional

Optional

This element can be set only once.

Upper Element

Rule

Rdn

Settings

Specify the attribute name to be the RDN of an entry. Depending on the Attribute element description, RDN may not be uniquely identified by the attribute name. In such a case, specify the item number of the CSV file. Item numbers cannot be concatenated using '+.'

It is invalid to specify duplicate values.

Initial Value

None

Required or Optional

Required

This element can be set more than once.

Upper Element

Rule

DnChange

Settings

Specify 1 if a DN change is considered to be a move. In this case, older (original) entries will be deleted when a DN is changed. If any value other than 1 is entered, only new entries will be created and older (original) entries will not be deleted.

Initial Value

1

Required or Optional

Optional

This element can be set only once.

Upper Element

Rule

objectClass

Settings

Specify objectClass to be specified for an entry. It is invalid to specify duplicate values.

Initial Value

None

Required or Optional

Required

This element can be set more than once.

Upper Element

Rule

attributeSeparator

Settings

Enter the separator character to be used for concatenating items when mapping from the CSV file. Optional strings may be specified. If multiple separators are entered, the separator specified first is adopted.

Initial Value

None

Required or Optional

Optional

Upper Element

Rule

unique

Settings

Specify the attribute to be checked for uniqueness under the base DN. Depending on the Attribute element description, the attribute may not be unique. In such a case, specify the item number of the CSV file. Item numbers cannot be concatenated using '+.'

Initial Value

None

Required or Optional

Optional

This element can be set less than twice.

Upper Element

Rule

CSV

Settings

No setting

Initial Value

None

Required or Optional

Required

Upper Element

Rule

Lower Element

Ldapop, Attribute

Ldapop

Settings

No setting. This tag is fixed. Do not change its hierarchical position.

Initial Value

None

Required or Optional

Optional

Upper Element

CSV

Lower Element

op, ldapadd, ldapdelete, ldapmodify

op

Settings

This is the item position of the CSV file that determines the operation type of entries. The first line is counted as the 0th line. This tag is fixed. Do not change its hierarchical position and value.

Initial Value

0

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

ldapadd

Settings

Specify a string to instruct entry addition. This tag is fixed. Do not change its hierarchical position.

Example: ADD

If, in this case, 'ADD' is described in the item position of the CSV file specified by the op element, entry addition is performed with information in the line.

A duplicate value must not be specified to the ldapadd, ldapdelete, and ldapmodify elements.

Initial Value

ADD

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

ldapdelete

Settings

Specify a string to instruct entry deletion. This tag is fixed. Do not change its hierarchical position.

Example: DEL

If 'DEL' is included in the item position of the CSV file specified by the op element, entries specified in the line after the word DEL are deleted.

A duplicate value must not be specified to the ldapadd, ldapdelete, and ldapmodify elements.

Initial Value

DEL

Specifiable Count

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

ldapmodify

Settings

Specify a string to instruct entry modification. This tag is fixed. Do not change its hierarchical position.

Example: MOD

In this case, 'MOD' is described in the item position of the CSV file specified by the op element, entries specified in the line followed by the word MOD are modified.

A duplicate value must not be specified to the ldapadd, ldapdelete, and ldapmodify elements.

Initial Value

MOD

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

Attribute

Settings

An attribute and the item position of the CSV file are associated by any element. Specify the attribute name to be set as a string of tags. For example, <cn>1</cn>.

Specify, as a lower element of this element, the attribute name element to be added to an entry or to be modified. The attribute name to be set must be variable. Specify, as a lower element, the item position of the target item in the CSV file by starting to count the item with 0. It is also possible to specify multiple items by concatenating them by '+.' Example: <description>8+1</description>

If the CSV file has more items than the maximum value of the item position set by the Attribute tag, the CSV file items exceeding the maximum number will be ignored.

If the CSV file has less items than the maximum value of the item position set by the Attribute tag, the lacking items are considered to have no corresponding values.

Initial Value

None

Required or Optional

Required

Upper Element

CSV

Lower Element

The name of an attribute to be added to an entry or to be modified is defined as a lower element name. Specify a lower element name whose attribute value is variable.

Example: <cn>1</cn>

fixed

Settings

A fixed value can be set for an attribute by any element. Specify the attribute name as a string of the tag.

As a lower element of this element, the attribute name element to be added to an entry or to be modified. The attribute name must be a fixed value.

Initial value

None

Required or Optional

Optional

This element can be set only once.

Upper element

Rule

Lower element

The name of an attribute to be added to an entry or to be modified is defined as a lower element name. Specify a lower element name whose attribute value is fixed.

Example: <o>fujitsu</o>

If the same attribute name as that of a lower element of the Attribute tag is specified, precedence is given to the name of the lower element of the fixed tag.

Adding, Deleting, and Modifying Entries Using the CSV file

Example of Adding Entries

The following section gives examples of adding user information entries.

For the object classes and attributes described in the example, see Appendix C - 'List of Object Classes' and Appendix B - 'List of Attributes' respectively.

Adding User Information Entries

The following examples illustrate how user information entries are added to the repository by associating the CSV file data with the user entry attributes listed below.

Table 3-8 CSV File Data

Item position	Item name	Attribute name
1	common name	Cn
2	Family name	Sn
3	Given name	givenName
4	User ID	Uid
5	Password	userPassword
6	Employee number	employeeNumber
7	E-mail address	Mail

CSV File

Specify 'ADD' in the 0th item position. In the subsequent item positions, according to the table above, describe the information to be added.

Example: CSV file for adding user information entries

```
ADD,user001,FUJITSU,user001,user001,u5zMEqXX,10001,user001@jp.interstage.com
ADD,user002,FUJITSU,user002,user002,iyaBWF09,10002,user002@jp.interstage.com
ADD,user003,FUJITSU,user003,user003,YNY62GCO,10003,user003@jp.interstage.com
ADD,user004,FUJITSU,user004,user004,mfQShkEK,10004,user004@jp.interstage.com
ADD,user005,FUJITSU,user005,user005,9pcurysl,10005,user005@jp.interstage.com
ADD,user006,FUJITSU,user006,user006,JqzLhqI6,10006,user006@jp.interstage.com
*1
```

*1 Each entry is describe in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file.

If all entries to be added have the same attribute type and attribute value, the description in the CSV file can be reduced by adding the fixed tag.

Example: Rule file for adding user information entries

```
<?xml version="1.0" encoding="EUC-JP" ?>
<!-- Prohibit corrections -->

<!DOCTYPE Csv2Directory [
<!ELEMENT Rule (name, baseDn, midDn?, Rdn+, DnChange?, objectClass+,
attributeSeparator?, unique*, CSV, fixed?)>
<!ELEMENT CSV (ldapop?, Attribute)>
<!ELEMENT ldapop (op?, ldapadd?, ldapdelete?, ldapmodify?)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT baseDn (#PCDATA)>
<!ELEMENT Rdn (#PCDATA)>
<!ELEMENT objectClass (#PCDATA)>
<!ELEMENT attributeSeparator (#PCDATA)>
<!ELEMENT op (#PCDATA)>
<!ELEMENT ldapadd (#PCDATA)>
<!ELEMENT ldapdelete (#PCDATA)>
<!ELEMENT ldapmodify (#PCDATA)>
]>
<!-- Prohibit corrections -->

<Csv2Directory>
    <Rule>
        <name>rule</name>

<!-- Define baseDn (required)-->

        <baseDn>ou=User,ou=interstage,o=fujitsu,dc=com</baseDn>

<!-- Define RDN (required/multiple RDN allowed/duplicate RDN not allowed) --
>
```

```
<!-- Enter either a unique number or attribute name -->

        <Rdn>cn</Rdn>

<!-- Whether a DN change is considered to be a move (optional)-->
<!-- Specify 1 if considered so -->

        <DnChange>1</DnChange>
        <objectClass>top</objectClass>
        <objectClass>person</objectClass>
        <objectClass>inetOrgPerson</objectClass>

<!-- Delimiter when an attribute value consists of multiple CSV items
(optional) -->
<!-- One blank character if not to be specified -->
<!-- The blank character cannot be specified -->

        <attributeSeparator>-</attributeSeparator>

<!-- Specify attributes that are not allowed duplication under baseDn -->
<!-- Enter either unique numbers or attribute names -->
<!–(optional/multiple attributes allowed/duplicate attributes not allowed) -
->

        <unique>uid</unique>

        <CSV>
<!-- Operation (add/delete/change) on the repository and CSV position
(optional) -->
<!-- If the operation method is described in the 0th position -->

            <ldapop>
                <op>0</op>
                <ldapadd>ADD</ldapadd>
                <ldapdelete>DEL</ldapdelete>
                <ldapmodify>MOD</ldapmodify>
            </ldapop>

<!-- Associate items of CSV and entry attributes (optional)-->

            <Attribute>
                <cn>1</cn>
                <sn>2</sn>
                <givenName>3</givenName>
                <uid>4</uid>
                <userPassword>5</userPassword>
                <employeeNumber>6</employeeNumber>
                <mail>7</mail>
            </Attribute>
        </CSV>

<!-- Define items that can be set as fixed values (optional)-->

        <fixed>
            <postalCode>105-7123</postalCode>
            <postalAddress>1-5-2 Higashi-Shimbashi Minato-ku</postalAddress>
            <st>Tokyo</st>
            <o>fujitsu</o>
        </fixed>
    </Rule>
</Csv2Directory>
```

Example of using the irepmodifyent Command

```
irepmodifyent -h hostname –p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -i add.csv   *1
```

*1 Make an entry in one line without starting a new line.

Example of Deleting Entries

The following example shows how to delete user information entries.

For the object classes and attributes described in the example, see 'List of Object Classes' and 'List Of Attributes' respectively.

The association of the CSV file data and user entry attributes is the same as that shown in the table in 'Adding user information entries.'

The following shows the description examples of the CSV file and rule file used to delete the following two user information entries:

```
dn:  cn=FUJITSU user001,ou=User,ou=interstage,o=fujitsu,dc=com
dn:  cn=FUJITSU user002,ou=User,ou=interstage,o=fujitsu,dc=com
```

CSV File

Specify 'DEL' in the 0th item position and then, in the subsequent item positions, describe the entries to be deleted.

Example: CSV file for deleting user information entries

```
DEL,user001,FUJITSU,user001,user001,u5zMEqXX,10001,user001@jp.interstage.com
DEL,user002,FUJITSU,user002,user002,JqzLhqI6,10006,user002@jp.interstage.com
*1
```

*1 Make one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file. Use the rule file shown above in 'Adding user information entries.'

Example of how to use the irepmodifyent command:

```
irepmodifyent –h hostname -p 389 –D "cn=manager,
ou=interstage,o=fujitsu,dc=com" -r rule.xml -i del.csv   *1
```

*1 Make an entry in one line without starting a new line.

Example of Modifying Entries

The following shows an example of modifying user information entries.

For the object classes and attributes described in the example, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

Note

If no user information entry to be modified exists, add the target entry.

Adding Attribute Values

The following explains how to describe the CSV file and rule file using a scenario in which the telephone number is added to the following entry:

```
dn:  cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
```

In the association between the CSV file data and user entry attributes (see table) the telephone number is the 8th item.

Item position	Item name	Attribute name
8	Telephone number	Telephonenumber

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be added. Describe the telephone number (telephonenumber) in the 8th item position.

Example: CSV file for adding the telephone number

```
MOD,user001,FUJITSU,user001,user001,u5zMEqXX,10001,user001@jp.interstage.com
,5555-0123   *1
```

*1   Describe one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file. Use the rule file shown above in 'Adding user information entries.'

Add the telephonenumber description to the Attribute tag.

Example: Rule file for adding the telephone number (Only the content inside the Attribute tag is shown)

```
<Attribute>
    <cn>1</cn>
    <sn>2</sn>
    <givenName>3</givenName>
    <uid>4</uid>
    <userPassword>5</userPassword>
    <employeeNumber>6</employeeNumber>
    <mail>7</mail>
    <telephonenumber>8</telephonenumber>
</Attribute>
```

Deleting Attribute Values

The following shows the description examples of the CSV file and rule file to delete the telephone number added in the example in 'Adding attribute values.'

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be deleted. If a telephone number (telephonenumber) is entered in the 8th item, delete the value from the line. Take care not to delete the comma after the 7th item.

Example: CSV file for deleting the telephone number

```
MOD,user001,FUJITSU,user001,user001,u5zMEqXX,10001,user001@jp.interstage.com
*1
```

*1   Describe one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file. For the CSV file (in the example of deleting the telephone number), use the same rule file as that shown above in the example in 'Adding attribute values'.

Deleting a Specific Attribute Value from Multiple Attribute Values

The following shows the description examples of the CSV file and rule file to delete the telephone number 5555-0123 from the following user information entries.

```
dn:  cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
cn:  user001
sn:  FUJITSU
givenName:  user001
uid:  user001
userPassword:  u5zMEqXX
employeeNumber:  10001
mail:  user001@jp.interstage.com
telephonenumber:  5555-0123
telephonenumber:  5555-6789
```

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be deleted. If telephone numbers (telephonenumber) are entered in the 8th and9th items, and the telephone number to be deleted is in the 8th item position, delete the value. Pay attention that the comma before and after the 8th item should not be deleted.

Example: CSV file for deleting one telephone number

```
MOD,user001,FUJITSU,user001,user001,u5zMEqXX,10001,user001@jp.interstage.com
,,5555-6789   *1
```

*1 Describe one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file.

Example: Rule file for deleting one telephone number (Only the content inside the Attribute tag is shown)

```
<Attribute>
    <cn>1</cn>
    <sn>2</sn>
    <givenName>3</givenName>
    <uid>4</uid>
    <userPassword>5</userPassword>
    <employeeNumber>6</employeeNumber>
    <mail>7</mail>
    <telephonenumber>8</telephonenumber>
    <telephonenumber>9</telephonenumber>
</Attribute>
```

Replacing Attribute Values

The following shows the description examples of the CSV file and rule file to replace the telephone number 5555-6789 in the following user information entries with 5555-9001.

```
dn:  cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
cn:  user001
sn:  FUJITSU
givenName:  user001
uid:  user001
userPassword:  u5zMEqXX
employeeNumber:  10001
mail:  user001@jp.interstage.com
telephonenumber:  5555-6789
```

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be replaced. If a telephone number (telephonenumber) is entered in the 8th item, delete the old one and enter the new one in its place in the file.

Example: CSV file for replacing the telephone number

```
MOD,user001,FUJITSU,user001,user001,u5zMEqXX,10001,user001@jp.interstage.com
,5555-9001   *1
```

*1   Describe one entry in one line.

Rule File

Describe the Attribute tag according to the order of each item in the CSV file. For the CSV file in the example of replacing the telephone number above, use the same rule file as that used in 'Adding attribute values' described above.

Example of using the irepmodifyent Command

```
irepmodifyent -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -i mod.csv
```

*1   Make an entry in one line without starting a new line.

Standard and Modification formats of LDIF

LDIF standard Format

The following explains the standard format to describe entry information.

For the object classes and attributes described in the examples, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

Example: Standard format of described two entries

```
version: 1
# First entry

dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user001
sn: Fujitsu

# Second entry

dn: cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
```

```
cn: user002
sn: Fujitsu
```

- version line

  In the first line of the LDIF file, specify the version of LDIF. If it is omitted, Version 1 is used by default. Specify Version 1 to use for the repository.

  1: Function specified by RFC2849

  0: LDIF function used by ldap-3.3 of the Michigan University

- Comment line

  A line starting with '#' is ignored as a comment line.

- Entry information

  Entry information consists of one or more entries. Each entry is separated by inserting one blank line. Each entry consists of DN (distinguished name), one or more object classes, and one or more attribute definitions . Describe entry information as shown below:

  ```
  dn: Entry DN
  objectclass: Object class
  objectclass: Object class
  Attribute type: Attribute value
  Attribute type: Attribute value
  ```

  Use the colon ':' to separate dn, objectclass, or the attribute type, and the value in each line. Blanks before and after ':' are ignored. If the content of an external file is set to an attribute value (no -b option in the ldapmodify command) or a binary value is set as an attribute value, no blank may be specified after ':' because it is not a delimiter between the attribute and the attribute value.

- Blank line

  Separates entry information.

Note

- – If the first line is blank, all lines in the LDIF file are ignored.
- – If blank lines continue, subsequent lines are ignored.

When a Line is Long

If DN or an attribute value is too long, it can be described in multiple lines. In that case, leave the space of one character blank in the head of the next line and start to the sequence of attribute values thereafter to indicate that the new line is continued from the preceding one. If a line starts with a blank character, it is considered to be a continuation line from the preceding line.

Example: When a long attribute value is wrapped around

```
dn: cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user002
sn: Fujitsu
description: user002 is good at English, German, and French.
 She has experience in overseas assignment.
```

Referencing an Attribute Value from an External File

To specify an external file as an attribute value, describe the command in the following format. It is not possible for DN to read from a file.

- If the -b option is used in the ldapmodify command

```
Attribute name: file name
```

- Otherwise

```
Attribute name:< file name   *1
```

*1 Do not insert any blank character between the ':' (colon) and '<' (less than). If there is a blank character between ':' and '<', a string described after ':' will be registered as an attribute value.

If an attribute value is specified in the above format, the contents of the specified file will be used as the value of the attribute. The file name is not stored in the repository.

The file name can be specified in the following formats:

– Specified with full pathname

Only text files using the ASCII code system characters can be specified. The file needs to be Base64-encoded in advance.

Windows

Enter the file name in the full path format starting with the drive name such as 'C:\.'

Solaris OE Linux

Enter the file name in the full path format starting with '/.'

– Specified using URL

  Specify the path to a file in the URL format. '\' (backslash) and '/' (slash) can be used as a delimiter of the path.

  Schemes (resource types pointed to by a URL) that can be specified with URL are file schemes only. The host name and port number specified in a URL are ignored. Thus, files that can be specified subsequently as full paths are local files only. If the file consists of characters, convert it into the UTF-8 format. If the file is a binary file, leave it in the binary format.

```
full pathname
```

Example: Windows Reading the attribute values from a file

```
#photo.jpg is binary

dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: user001
sn: Fujitsu
jpegPhoto:< file://C:\data\photo.jpg
```

Example: Solaris OE Linux Reading the attribute values from a file

```
#photo.jpg is binary

dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: user001
sn: Fujitsu
jpegPhoto:< file:///data/photo.jpg
```

Binary Notations

To specify a binary value as an attribute value, describe it in the following format:

- Describing Base64-encoded values directly (Part 1)

```
Attribute name:: attribute value (Base64-encoded)
```

- Describing Base64-encoded values directly (Part 2)

  ```
  Attribute name;binary:: attribute value (Base64-encoded)
  ```

- Specifying external file content

  ```
  Attribute name:< file://full pathname
  ```

  If external file content is specified as the value of a binary attribute, only the external file content is stored in the repository in the Base64-encoded format. The file name is not stored.

Example: Describing the Base64-encoded values directly

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: user001
sn: Fujitsu
jpegPhoto::gqCCo2C0ILTgtaC2Q0KgtyC3YLegt+C4A0KguKCooLkgqa
 C5g0KgueC6ILpguqC6w0KgvENCg==
```

LDIF Modification Format

The following explains the modification format to describe the change information of entries. In addition to the format described in 'LDIF standard format,' describe the target, type, and content of change.

1. DN of the entry to be changed
2. Change type (changetype line)

   Specify one of the following four types as the change type:

   – add

     Add the entry specified in the dn line to the repository.

   – delete

     Delete the entry specified in the dn line from the repository.

   – modify

     Modify the entry specified in the dn line.

   – modrdn

     Change RDN (relative distinguished name) of the entry specified in the dn line.

   If the changetype line is omitted, the change type is interpreted to mean the following:

   – If the -a option is specified in the ldapmodify command: add

   – If the -a option is not specified in the ldapmodify command: modify

3. Change content

Example: Adding one entry

```
version: 1
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user001
sn: Fujitsu
```

For the object classes and attributes described in the example, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

Next, the types of entry changes are explained in detail.

Addition, Deletion, and Modification of Entries and Identifier Changes by LDIF, and Unsupported LDIF Description

Adding Entries

Specify 'add' in the changetype line and then describe the attribute definition in the subsequent lines.

Example: Adding entries

```
dn: cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user002
sn: Fujitsu
```

For the object classes and attributes described in the example, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

Deleting Entries

Specify 'delete' in the changetype line

Example: Deleting entries

```
version: 1
dn: cn=user003,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: delete
```

For the object classes and attributes described in the example, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

Modifying Entries

To perform addition, deletion, or replacement on an attribute or attribute value of an entry, specify 'modify' in the changetype line. Specify the change method in the next line.

- add: attribute name

  Add the attribute to the entry specified in the dn line. If the attribute type is already in the entry, the attribute value is added.

- delete: attribute name

  Delete the attribute from the entry specified in the dn line. If there are multiple attribute values to the attribute type, all attribute values are deleted. To delete only one attribute value among the multiple attribute values, describe the attribute name and attribute value in the line following the delete line.

- replace: attribute name

  Replace the attribute of the entry specified in the dn line with the specified value. If the specified entry does not have the specified attribute, the attribute will be created.

If the attribute change type is omitted, the following assumption is made:

  - If the -r option is specified in the ldapmodify command: replace
  - If the -r option is not specified in the ldapmodify command: add

In the line following the attribute change type line, specify the attribute content to be changed. If duplicate changes are described consecutively, separate them by '-.'

Describe the changes in the following format:

```
dn: Entry DN
changetype: modify
Attribute change type (add|delete|replace): attribute type
Attribute type: attribute value
```

Adding Attribute Values

Specify 'add: attribute-name' in the line directly after 'changetype: modify'.

Example: Adding the mail attribute

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
add: mail
mail: user001@fujitsu.com
```

Example: Adding two telephonenumber attributes and one jpegPhoto attribute

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype:modify
add:telephonenumber
telephonenumber: 7777-1234
telephonenumber: 7777-5678
-
add:jpegPhoto
jpegPhoto:< file:///data/photo/photo.jpg
```

Deleting Attribute Values

Specify 'delete: attribute-name' in the line directly after 'changetype: modify'.

Example: Deleting the description attribute

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
delete: description
```

Deleting a Specific Attribute Value from Multiple Attribute Values

Specify 'delete' as the attribute change type.

The entry information of user001 looks like the following.

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user001
sn: Fujitsu
telephonenumber: 7777-1234
telephonenumber: 7777-5678
```

Example: Deleting the telephone number 7777-1234

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
delete: telephonenumber
telephonenumber: 7777-1234
```

As a result, the entry information of user001 looks like the following.

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user001
sn: Fujitsu
telephonenumber: 7777-5678
```

Replacing Attribute Values

Specify 'replace' as the attribute change type.

Example: Replacing the mail address user001@fujitsu.com with user001_fujitsu@fujitsu.com

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
replace: mail
mail: user001_fujitsu@fujitsu.com
```

Replacing a Specific Attribute Value Among the Multiple Attribute Values

Delete the target attribute value and then add a new value.

The entry information of user001 looks like the following.

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user001
sn: Fujitsu
telephonenumber: 7777-1234
telephonenumber: 7777-5678
```

Example: Replacing the telephone number 7777-1234 with 7777-9001

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype:modify
delete: telephonenumber
telephonenumber: 7777-1234
-
add:telephonenumber
telephonenumber: 7777-9001
```

As a result, the entry information of user001 looks like the following.

```
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: user001
sn: Fujitsu
telephonenumber: 7777-5678
telephonenumber: 7777-9001
```

For the object classes and attributes described in the example, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

Changing the Identifier of an Entry

Specify 'modrdn' in the changetype line. In the following line, specify the detailed method of changing the entry identifier.

The following two detailed methods of changing the entry identifier are available. Specify them in the following order:

1. newrdn: new RDN
2. deleteoldrdn: (1|0)

To delete an older RDN after changing to a new RDN, specify. '1.' To retain it as an attribute value, specify '0.'

'deleteoldrdn' can be omitted. If it is omitted, older RDN will be deleted.

Describe the identifier change in the following format.

```
dn: Entry DN
changetype: modrdn
newrdn: New RDN
deleteoldrdn: (1|0)
```

Example: Changing RDN of the user002 entry to user002. Fujitsu

```
dn: cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modrdn
newrdn: cn=user002. Fujitsu
deleteoldrdn: 1
```

For the object classes and attributes described in the examples, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

Unsupported LDIF Description

The following functions defined in 'RFC2849' (June. 2000) are not supported by Smart Repository:

- Operation on attributes without value

  No attribute without an attribute value can be registered.

- Display format of attribute values that end with a blank character

  Attribute values that end with a blank character are not output in the Base64 format.

- Designation of control

  The control function from LDIF cannot be specified.

- Designation OID

  Attributes specified by OID from LDIF cannot be specified.

- charaset syntax

  The languages used for attribute values cannot be specified.

The following shows some description examples.

Example

```
dn:: b3U95Za25qWt6YOoLG89QWlyaXVz
# dn:: ou=<JapaneseOU>
objectclass: top
objectclass: organizationalUnit
ou:: 5Za25qWt6Yoo
# ou:: <JapaneseOU>
ou;lang-ja:: 5Za25qWt6YOo
# ou;lang-ja:: <JapaneseOU>
ou;lang-ja;phonetic:: 44GI44GE44GO44KH44GG44G2
# ou;lang-ja:: <JapaneseOU_in_phonetic_representation>
ou;lang-en: User
description: Japanese office
```

Searching by Command

Repository entries can be searched by using the ldapsearch command. It is also possible to use a search filter to extract specific information.

For the search filter, see Appendix E – Search Filter

For the method of using this command, see 'Smart Repository operation command' in the Reference Manual (Command Edition).

Example

Windows

- Searching for entries whose attribute cn is 'user1' to extract information about the attribute sn

```
C:\Interstage\ID\Dir\sdk\C\bin\ldapsearch -p 389 -h hostname –D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W –b
"ou=interstage,o=fujitsu,dc=com" "cn=user1" sn   *1
```

*1 Make an entry in one line without starting a new line.

- Output all entries to a file (ldif.txt)

```
C:\Interstage\ID\Dir\sdk\C\bin\ldapsearch -p 389 -h hostname -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -b
"ou=interstage,o=fujitsu,dc=com" "objectclass=*" > ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

Solaris OE Linux

- Searching for entries whose attribute cn is 'user1' to extract information about the attribute sn

```
/opt/FJSVidsdk/C/bin/ldapsearch -p 389 -h hostname -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -b
"ou=interstage,o=fujitsu,dc=com" "cn=user1" sn   *1
```

*1 Make an entry in one line without starting a new line.

- Output all entries to a file (ldif.txt)

```
/opt/FJSVidsdk/C/bin/ldapsearch -p 389 -h hostname -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -b
"ou=interstage,o=fujitsu,dc=com" "objectclass=*" > ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

Adding Entries by Command

Entries can be added to the repository by using the ldapmodify or irepmodifyent command.

If entry information is specified in the standard input or LDIF file, use the ldapmodify command. For information about LDIF, see 'Using the Command to Manage Entries'.

If entry information is specified in the CSV file, use the irepmodifyent command. For information about CSV, see 'Using the Command to Manage Entries'.

For the method of using each command, see 'Smart Repository operation command' in the Reference Manual (Command Edition).

Examples

- Using the LDIF file in the ldapmodify command

Windows

```
C:\Interstage\ID\Dir\sdk\C\bin\ldapmodify -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

Solaris OE Linux

```
/opt/FJSVidsdk/C/bin/ldapmodify -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

- Using the CSV file in the ldapmodify command

```
irepmodifyent -h hostname –p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -i add.csv
```

*1 Make an entry in one line without starting a new line.

Deleting Entries by Command

Entries can be deleted from the repository using the ldapdelete command. The ldapmodify and irepmodifyent commands can also be used to delete entries.

The ldapdelete command can be used to delete entries by specifying the DN names to be deleted or a file containing the DN names. Note that, instead of the LDIF format, only DN names are specified for the ldapdelete command.

If entry information is specified in the standard input or a file, use the ldapmodify command.

If entry information is specified in the CSV file, use the irepmodifyent command. For information about CSV, see Using the CSV file in Using the Command to Manage Entries.

For the method of using each command, see 'Smart Repository operation command' in the Reference Manual (Command Edition).

Examples

- Using a file in the ldapdelete command

Windows

```
C:\Interstage\ID\Dir\sdk\C\bin\ldapdelete –h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W –f delete_input.txt   *1
```

*1 Make an entry in one line without starting a new line.

Solaris OE Linux

```
/opt/FJSVidsdk/C/bin/ldapdelete –h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W –f delete_input.txt   *1
```

*1 Make an entry in one line without starting a new line.

- Using the CSV file in the irepmodifyent command

```
irepmodifyent -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -i del.csv   *1
```

*1 Make an entry in one line without starting a new line.

Modifying Entries by Command

Entries in the repository can be modified by using the ldapmodify or irepmodifyent command.

If entry information is specified in the standard input or LDIF file, use the ldapmodify command. For information about LDIF, see Using the LDIF file in Using the Command to Manage Entries.

If entry information is specified in the CSV file, use the irepmodifyent command. For information about CSV, see Using the CSV file in Using the Command to Manage Entries

For the method of using each command, see 'Smart Repository operation command' in the Reference Manual (Command Edition).

Examples

- Using the LDIF file in the ldapmodify command

Windows

```
C:\Interstage\ID\Dir\sdk\C\bin\ldapmodify -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

Solaris OE Linux

```
/opt/FJSVidsdk/C/bin/ldapmodify -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

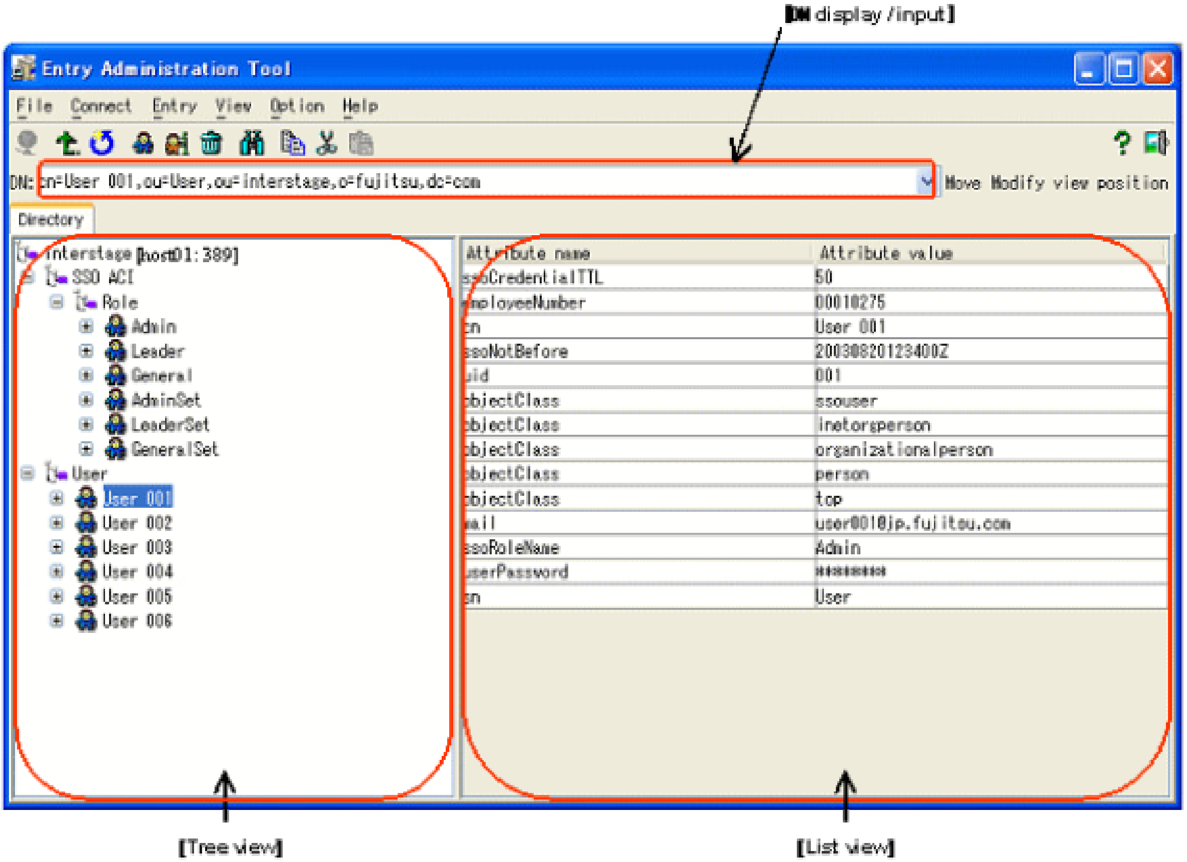
- Using the CSV file in the irepmodifyent command

```
irepmodifyent -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -i mod.csv   *1
```

*1 Make an entry in one line without starting a new line.

Using the Entry Administration Tool

The Entry Administration Tool is a tool to manage entries. Using the Entry Administration Tool, operations such as addition, modification, deletion, and searching of entries registered with the repository can be performed through a GUI.



DN: cn=User 001,ou=User,ou=interstage,o=fujitsu,dc=com

interstage [host01:389]
- SSO ACI
  - Role
    - Admin
    - Leader
    - General
    - AdminSet
    - LeaderSet
    - GeneralSet
- User
  - User 001
  - User 002
  - User 003
  - User 004
  - User 005
  - User 006

Attribute name	Attribute value
ssoCredentialTTL	50
employeeNumber	00010275
cn	User 001
ssoNotBefore	20030820123400Z
uid	001
objectClass	ssouser
objectClass	inetorgperson
objectClass	organizationalperson
objectClass	person
objectClass	top
mail	user001@jp.fujitsu.com
ssoRoleName	Admin
userPassword	********
sn	User

Figure 3-5 Entry Administration Tool window

1. DN display/input
2. Tree view
3. List view

DN Display/Input

Displays DN of the selected entry. DN can be entered or selected from the drop-down list.

Tree View

Displays entry information registered with the repository in the hierarchical configuration. Nodes in the tree can be opened and closed by the mouse or from the keyboard.

List View

Displays entries selected in [Tree view]. Two display modes are available: one mode displays attribute information about one entry, the second mode lists entries at the same level in the hierarchy.

Note

If an external file is specified as a binary attribute value, only the content of the external file is stored; the file name is not stored. Thus, if an entry containing a binary attribute is selected, only the data size of the binary file stored in the repository is displayed in the attribute value field of the binary attribute.

Operation Method

Start and operate the Entry Administration Tool using the following procedure:

1. Bitmap display is required

   On the machine that uses the Entry Administration Tool, configure a display and driver that can be specified with over 256 colors on the monitor.

   Solaris OE Linux

   A bitmap display is needed.

2. Start the Entry Administration Tool

   Windows

   Select [Programs] > [Interstage] > [Smart Repository] > [Entry Administration Tool] from the [Start] menu.

   Solaris OE Linux

   ```
   irepeditent
   ```

3. Login

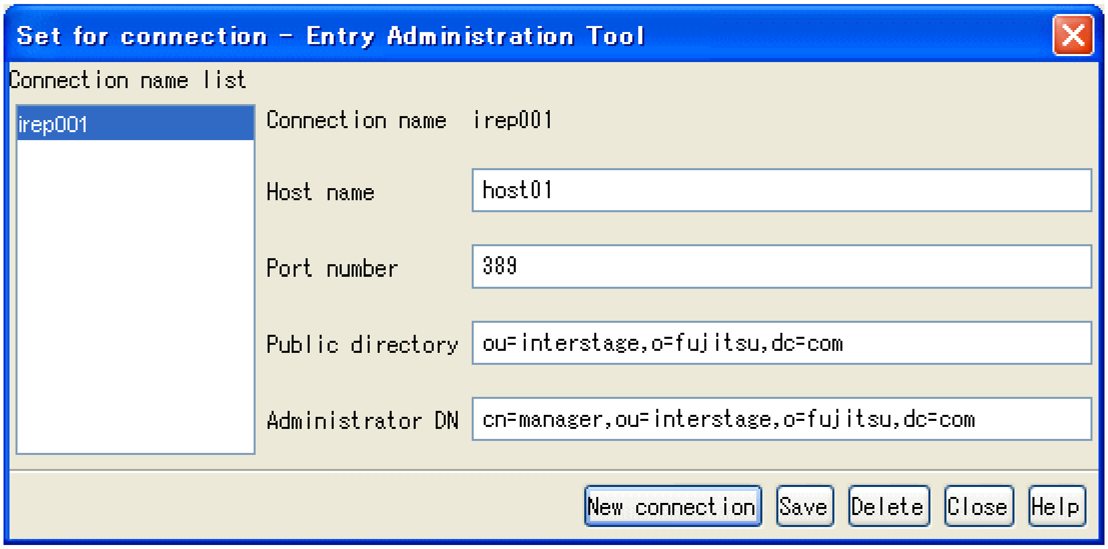
   Use either of the following methods to display the [Login] window:

   – Click [Login] from the [Connect] menu.

   – Click [Login] button on the tool bar.

     1. Select the connection destination from the [Connection destination]
     2. Enter the Administration DN password in the [Password]
     3. Click [Login]

   If it is the first login after installation of the product, or connection destination information is being added or changed, the connection information needs to be set. For details about connection, see the Entry Administration Tool Help.



Connection name irep001

Host name host01

Port number 389

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

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

Figure 3-6 Entry Administration Tool - Set for connection dialog

4. Initial display

   When connecting to the repository which operates entries after login, the Entry Administration Tool is initially displayed (the directory information tree of the connected repository is displayed in the left column 'Tree view').

   For details of adding, modifying and searching operation methods, refer to the explanation on the next pages and the Entry Administration Tool help.

Note

- If an external file is specified as a binary attribute value, only the content of the external file is stored; the file name is not stored. Thus, if an entry containing a binary attribute is selected, only the data size of the binary file stored in the repository is displayed in the attribute value field of the binary attribute.
- The Entry Administration Tool is mainly used for development and testing when setting up a directory by the system administrator. Create a dedicated application for entry management in user operation. For information about application development, see Chapter 5 - 'Creating an application (JNDI).'

Adding Entries

The Add an Entry and Import windows are provided to add entries. By opening these windows and entering settings and values, entries can be registered with the connected repository.

Adding Entries One by One

1. Select the upper entry of the entry to be added from [Tree view].
2. Select [Add...Ctrl+N] from the [Entry (E)] menu or right-click and select [Add... Ctrl+N] from the pop-up menu.
3. The Add an Entry window is displayed. Enter the attributes required for entries to be added to add entries.

For more details, see the Entry Administration Tool Help.

Adding Entries Using the LDIF File

1. Select [Import...F3] from the [Options (O)] menu.
2. The import window is displayed. In the field [LDIF file], specify the LDIF file containing information about the entry to be added. Specify the file by either of the following methods::
   - Clicking [Browse...] and browsing to the file.
   - Entering the path of the LDIF file.
3. Select the character set of the specified LDIF file from [Character set].
4. Select [Add] of the specified type.
5. Click [OK] to add the entry specified in the LDIF file.

For more details, see the Entry Administration Tool Help.

Deleting Entries

Entries can be deleted one by one or using the LDIF file.

Deleting Entries One by One

1. Select the entry to be deleted from [Tree view].
2. Select [Delete...Delete] from the [Entry (E)] menu or right-click and select [Delete...Delete] from the pop-up menu.

For more details, see the Entry Administration Tool Help.

Deleting Entries using the LDIF File

1. Select [Import...F3] from the [Options (O)] menu.
2. The import window is displayed. In the field [LDIF file], specify the LDIF file containing information about the entry to be added. Specify the file by either of the following methods::
   - Clicking [Browse...] and browsing to the file.
   - Enter the path of the LDIF file.
3. Select the character set of the specified LDIF file from [Character set].

4. Select [Modify] of the specified type.
5. Click [OK] to delete the entry specified in the LDIF file.

For more details, see the Entry Administration Tool Help.

Modifying Entries

The entry modification window and import window are provided to modify entries. By opening these windows and entering settings and values, entries can be modified with the connected repository.

Modifying Entries One by One

1. Select the entry to be modified from [Tree view].
2. Select [Modify... Ctrl+M] from the [Entry (E)] menu or right-click and select [Modify... Ctrl+M] from the pop-up menu.

For more details, see the Entry Administration Tool Help.

Modifying Entries using the LDIF File

1. Select [Import...F3] from the [Options (O)] menu.
2. The import window is displayed. In the field [LDIF file], specify the LDIF file containing information about the entry to be added. Specify the file by either of the following methods:
   - Clicking [Browse...] and browsing to the file.
   - Enter the path of the LDIF file.
3. Select the character set of the specified LDIF file from [Character set].
4. Select [Modify] of the specified type.
5. Click [OK] to modify the entry specified in the LDIF file.

For more details, see the Entry Administration Tool Help.

Searching for Entries

1. Select the entry to be searched for from [Tree view].
2. Select [Search...Ctrl+S] from the [View] menu.
3. The search window is displayed. Create a search filter on the search window to search for the entry.

For more details, see the Entry Administration Tool Help.

Changing the Entry Identifier

1. Select the entry whose identifier should be changed from [Tree view].
2. Select [Rename...F2] from the [Entry (E)] menu or right-click and select [Rename...F2] from the pop-up menu.

For more details, see the Entry Administration Tool Help.

Using SDK

Using SDK, applications that directly operate entries of Smart Repository can be developed. Applications can also be developed using the JNDI contained in the JDK.

Creating an Application using JNDI

Create an application by referring to Chapter 5 - 'Creating an Application (JNDI).'

Chapter 4

Operation and Maintenance

This chapter explains the environment setup required to use Smart Repository.

Starting/Stopping a Repository

This section explains how to start and stop a repository of Smart Repository.

Starting a Repository

The Interstage Management Console is used to start a repository within Smart Repository.

Log in after starting the Interstage Management Console.

To perform the startup operation, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

For information about startup of the Interstage Management Console, see Chapter 2 - 'Configuring the Interstage Management Console' in the Operator's Guide. For information about the screen operations, see Chapter 8 – 'Services' in the Operator's Guide.

Notes

- Startup time for each repository make take from several seconds to several minutes. The startup time will vary depending on the number of registered entries, operation mode, and machine performance.
- If the operating system is restarted while a repository is running, the repository may or may not start automatically, as follows:

  Windows

  A repository is automatically started when the [Startup Service] is set to [Automatic]. This option is located by selecting [Management Tools], and then [Service] from the Control Panel.

  Solaris OE Linux

  Any active repository will be automatically started.

Stopping a Repository

The Interstage Management Console is used to stop a repository within Smart Repository.

Log in after starting the Interstage Management Console.

To perform the stop operation, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

For information regarding the stopping of the Interstage Management Console, see Chapter 2 - 'Configuring the Interstage Management Console' in the Operator's Guide. For information about the screen operations, see Chapter 8 – 'Services' in the Operator's Guide.

Note

- If the operating system is restarted while a repository is stopped, the repository may or may not start automatically, as follows:

  Windows

  A repository is automatically started when the [Startup Service] is set to [Automatic]. This option is located by selecting [Management Tools], and then [Service] from the Control Panel.

  Solaris OE Linux

  Any stopped repository will not be automatically started.

Procedure for Changing the Password for the Slave during Replication Operation

This section explains the procedure for changing the slave password during a replication operation.

If the administrator DN password of a repository (in slave operation) is changed, a new password must set by selecting [Password for the connection] and then [Replication Connection Settings] for the repository in master operation.

The following shows a flow diagram of the procedure for changing the password of the slave during replication operation.

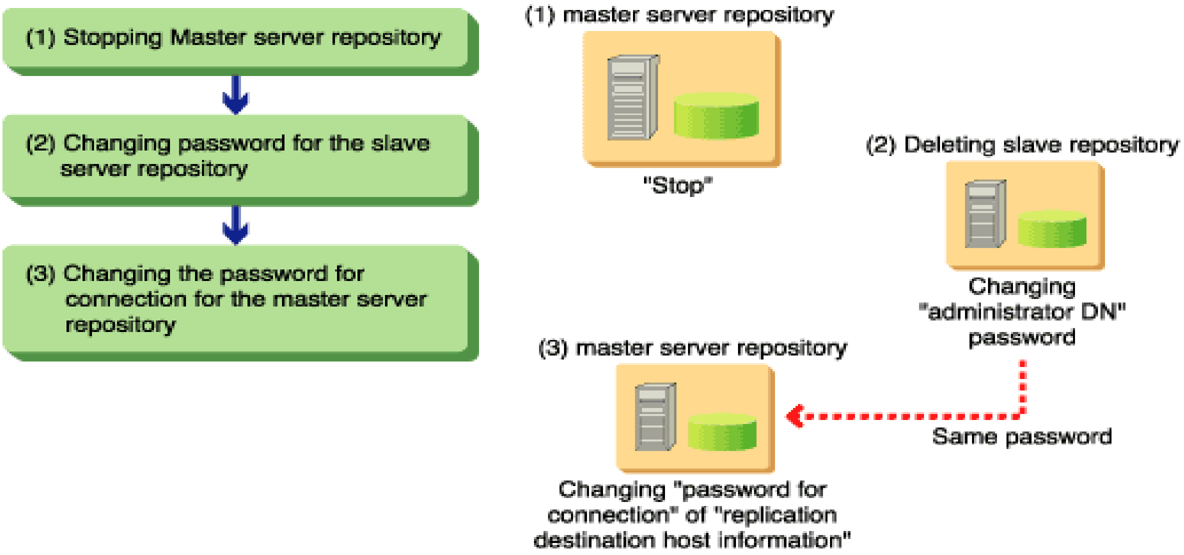

(1) Stopping Master server repository
(2) Changing password for the slave server repository
(3) Changing the password for connection for the master server repository
(1) master server repository
"Stop"
(2) Deleting slave repository
Changing "administrator DN" password
(3) master server repository
Same password
Changing "password for connection" of "replication destination host information"

Figure 4-1 Change a Password of the Slave.

Stopping a Repository of the Master Server

Use the Interstage Management Console to stop a repository of the master server. The procedure for doing this is as follows:

Stop the repository during master operation. This is performed using the Interstage Management Console connected to the master server machine.

Changing the Password of a Repository of the Slave Server

Change the password of a slave server repository as follows:

1. Stop the repository during slave operation. This is performed using the Interstage Management Console connected to the slave server machine.
2. Click the stopped repository in slave operation to display the [Settings] window.
3. Select 'Change' in [Change password?] and then, after a dialog box is displayed, click the [OK] button.
4. After [New Administrator DN password] and [New Administrator DN password (re-entry)] are displayed, set the same new password and then click the [Apply] button.
5. Start the repository using the Interstage Management Console.

Changing the Password of the Repository used to Connect to the Slave Server

Change the password of the master server repository as follows:

1. Using the Interstage Management Console that connected to a master server, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

   The [Repository : View Status] window is displayed.
2. Click the stopped repository (Described on 'Stopping a Repository of the Master Server') to display the [Settings] window, and then click the [show] to display detailed settings.
3. Select the name of the host where the slave operation repository's Administrator DN password has been changed on [Replication destination host list], and then click [Edit].
4. In the displayed [Password for the connection] of [Replication Connection Settings], set the password with a same value that has been set on slave server, and then click the [Update] button.
5. Start the repository using the Interstage Management Console.

Tuning

This section explains the environment setting tuning method for improving the search performance or reducing the server load.

Limiting the Time of Exclusive Use of the Repository per Search Request

An exclusive search request on a repository with a large amount of registered entry data will result in the slow response of Smart Repository. This time delay can be prevented by changing environment settings to limit the exclusive use of the repository for search requests.

To limit the duration of exclusive use of a repository by a search request, use the Interstage Management Console to change the environment settings, as follows:

1. Start the Interstage Management Console.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

   The [Repository : View Status] window will be displayed. If the repository is active, stop it.
3. Select the repository to change from the [Repository : View Status] window.
4. Click [Detailed settings] to display the detailed settings.
5. Specify the search time per search request in [Search Timeout].
6. Start the repository from the [Repository : View Status] window.

Refer to Chapter 8 - 'Services' in the Operator's Guide for the time range that can be specified in [Search Timeout].

Limiting the Number of Entries to be Searched per Search Request

An exclusive search request on a repository with a large amount of registered entry data will result in the slow response of Smart Repository. This delay can be prevented by changing environment settings to limit the number of entries to be searched per search request.

To limit the number of entries searched, per request, change the environment settings as follows:

1. Start the Interstage Management Console.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

- The [Repository: View Status] window will be displayed. If the repository is active, stop it.

3. From the [Repository: View Status] window, select the repository to change.
4. Click [Detailed settings] to display the detailed settings.

5. Specify the maximum number of entries to be searched per search request, in [Maximum number of searchable entries].
6. Start the repository from the [Repository: View Status] window.

Refer to Chapter 8 - 'Services' in the Operator's Guide for the range of allowable values for [Maximum number of searchable entries].

Changing the Connection Cutoff Time in Non-communication State

The connection cutoff time determines when the connection to the client program is interrupted in a non-communication state. The cutoff time can be customized for the environment.

To change the connection cutoff time in a non-communication state, use the Interstage Management Console to change the environment settings according to the following procedure:

1. Start the Interstage Management Console.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

   The [Repository: View Status] window will be displayed. If the repository is active, stop it.
3. Select the repository to change from the [Repository: View Status] window.
4. Specify the connection cutoff time in a non-communication state in [Connection Idle Timeout].
5. Start the repository from the [Repository: View Status] window.

Refer to Chapter 8 - 'Services' in the Operator's Guide for the range of allowable [Connection Idle Timeout] values.

Logs

Smart Repository outputs the following logs:

- Access history to Smart Repository
- Maintenance information of Smart Repository

Access History to Smart Repository

Smart Repository features an access log which stores access history. The following information is recorded in the log:

- Access date/time
- IP address
- Events
- Detailed information about events

Using the Interstage Management Console, it is possible to change the following settings:

- Output types of the access log
- Access log storage directory of the access log
- Rotation type of the access log

Setting the Access Log

The following procedure explains how to set the access log.

Setting the Access Log When Creating a New Repository

1. Start the Interstage Management Console.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and create a repository.
3. Click [View Status] to display detailed settings.
4. Specify [Output types], [Access log storage directory], and [Rotation Type] in [Access log settings]. Also specify [Size] and [Number of access log files to maintain] as required.

Changing the Access Log Settings of an Active Repository Server

1. Start the Interstage Management Console.
2. Stop the repository.
3. Change the repository setting.
4. Click [View] to display detailed settings.
5. Specify [Output types], [Access log storage directory], and [Rotation Type] in [Access log settings] and also specify [Size] and [Number of access log files to maintain] as required.

6. Start the repository from the [Repository : View Status] window.

   Refer to Chapter 8 - 'Services' in the Operator's Guide for further operating details.

Output Level of the Access Log

When all access history from the client is output to the access log, it can take a large amount of hard disk space. To manage this situation, events to be output to the access log can be changed in [Output types].

A combination of the following can be specified in [Output types].

- Client requests
- Server errors
- Normal server response
- Server search result of DN

Access Log Storage Destination

The access log is created under the following directory by default:

Windows

```
C:\Interstage\IREP\var\<repository-name>\log
```

Solaris OE Linux

```
/var/opt/FJSVirep/<repository-name>/log
```

The rules for generating the file name of the access log are as follows:

access_YYYYMMDD_XXXXX
YYYY: Year of the access log output
MM: Month of the access log output
DD: Day of the access log output
XXXXX: Smart Repository administration name (Both the content and number of digits can be changed)

Output example:

If the access log was output on April 1, 2003

```
access_20030401_81600
```

Note

- If the storage directory is changed, delete the old storage directory before the change and log information as required.

Rotation of the Access Log

The access log can be divided in accordance with the rotation.
The following types can be selected as [Rotation Type].

Rotation type	**Meaning**
Size	A new file is created after the specified size is reached.
Monthly	A new file is created each month. However, when the maximum size of one file is reached; a new file is automatically created.
Daily	A new file is created each day. However, when the maximum size of one file is reached; a new file is automatically created.

In addition to [Rotation Type]; [Size] and [Number of access log files to maintain] can also be specified.

In [Size], specify the size of one access log file in MByte.

In [Number of access log files to maintain], specify the number of generations of files to maintain.

Note

- If Smart Repository is restarted, the file is divided regardless of [Rotation Type].

Access Log Format

The following shows the output rules and format of the access log.

Output Form

- One record is output in one line.
- Items in one record are divided by the tab (0x09).
- If the content of 'DETAIL' (shown in the format below) is divided into multiple items, they will be divided by blanks.
- The access log is output in the 'UTF-8 format.'
- If any multi-byte character is contained in the access log, use an editor that supports the 'UTF-8 format' to reference it. If the 'UTF-8 format' cannot be handled, convert the code system of the access log from the 'UTF-8 format' to a code system that works with the editor.

Format

The following shows the format of the access log:

```
MM/DD  hh:mm:ss.nnnnnn  THREAD  CONN  OP  FD  REQ/RES  EVENT  DETAIL
```

Format Details

Table 4-1 lists the details of the access log format.

Table 4-1 Access Log Format Details

MM/DD hh:mm:ss.nnnnnn	Shows the date and time of the access log output MM: month DD: day hh: hour (24 hours) mm: minute ss: second nnnnnn: microsecond
THREAD	Shows the thread ID (hexadecimal) in Smart Repository that executed the request (for maintenance).
CONN	Shows the management number (connection ID) by which Smart Repository accepted the connection (for maintenance).
OP	Shows the management number (operation ID) by which Smart Repository accepted the request within one connection (for maintenance).
FD	Shows the file descriptor (fd) of the connection socket.
REQ/RES	Indicates whether a request or a response. --->: Request from a variety of clients to Smart Repository <---: Response from Smart Repository to a variety of clients
EVENT	Shows information about requests to Smart Repository and results of such requests. For more details, see the EVENT table.
DETAIL	Shows detailed information about EVENT. For more details, see the EVENT table.

Details of EVENT and DETAIL of the Access Log

Table 4-2 lists the details of EVENT and DETAIL of the access log.

Table 4-2 EVENT and DETAIL Access Log table

EVENT	DETAIL	Meaning	Output level [X: Output]			
			Output request information of the client	Output error response of the server	Output normal response of the server	Output search result response of the server
CONNECT	IP address: port number (host name)	Connection request from the client	X			
CONNECTION REJECTED	IP address: port number (host name)	Error response from the server (connection failure)		X		
DISCONNECT	IP address: port number (host name)	Normal response from the server (successful disconnection)			X	
TIMEOUT	IP address: port number (host name)	Error response from the server (timeout)		X		

EVENT	**DETAIL**	**Meaning**	**Output level [X: Output]**			
			Output request information of the client	**Output error response of the server**	**Output normal response of the server**	**Output search result response of the server**
BIND	Bind DN, protocol version	Authentication request bind DN from the client: Bind DN used for connecting to Smart Repository Protocol version: Protocol version of LDAP used for connecting to Smart Repository	X			
SEARCH	Search base, Search scope, Alias reference rule, Size limit, Time limit, Attribute acquisition method, Search filter	Search request from the client Search base: Entry to the search start position. "?" indicates that the search base is not specified. Search scope: 0: Searches the entries specified by the search base. 1: Searches the subordinator entries of the entries specified by the search base. 2: Searches the entries specified by the search base and entire entries below them. Alias reference rule: 0: No alias reference 1: Reference the alias only during searching.	X			

EVENT	**DETAIL**	**Meaning**	**Output level [X: Output]**			
			Output request information of the client	**Output error response of the server**	**Output normal response of the server**	**Output search result response of the server**
		2: Reference the alias only when searching the search base. 3: Reference the alias. Size limit: Maximum number of entries to be searched Time limit: Timeout period for searching Attribute acquisition method: 0: Searches for the attribute name and attribute value. Otherwise: Searches for the attribute name. Search filter: Search filter. 'empty' indicates that the search filter is not specified.				
COMPARE	DN to be compared	Comparison request from the client	X			
MODIFY	DN to be modified	Modification request from the client	X			

EVENT	DETAIL	Meaning	Output level [X: Output]			
			Output request information of the client	Output error response of the server	Output normal response of the server	Output search result response of the server
MODRDN	DN to be modified, New RDN, Old DN deletion flag	Identifier change request from the client DN to be modified: DN (old DN) before modification New RDN: New RDN Old DN deletion flag 0: Does not delete the old DN. Otherwise: Deletes the old DN.	X			
ADD	DN to be added	Addition request from the client	X			
DELETE	DN to be deleted	Deletion request from the client	X			
BIND OK	None	Normal response from the server (successful authentication)			X	
COMPARE OK	None	Normal response from the server (successful comparison)			X	
MODIFY OK	None	Normal response from the server (successful change)			X	

EVENT	**DETAIL**	**Meaning**	**Output level [X: Output]**			
			Output request information of the client	**Output error response of the server**	**Output normal response of the server**	**Output search result response of the server**
MODRDN OK	None	Normal response from the server (successful identifier change)			X	
ADD OK	None	Normal response from the server (successful addition)			X	
DELETE OK	None	Normal response from the server (successful deletion)			X	
BIND NG	Error code	Error response from the server (authentication failure)		X		
COMPARE NG	Error code	Error response from the server (comparison failure)		X		
MODIFY NG	Error code	Error response from the server (change failure)		X		
MODRDN NG	Error code	Error response from the server (identifier change failure)		X		
ADD NG	Error code	Error response from the server (addition failure)		X		
DELETE NG	Error code	Error response from the server (deletion failure)		X		
SEARCH OK	Number of found entries	Normal response from the server (successful search)			X	

EVENT	DETAIL	Meaning	Output level [X: Output]			
			Output request information of the client	**Output error response of the server**	**Output normal response of the server**	**Output search result response of the server**
SEARCH NG	Error code	Error response from the server (search failure)		X		
SEARCH ENT	Entry DN of the search result	Search result response from the server				X
UNBIND	None	Release request from the client	X			

The LDAP error code is output to the error code of DETAIL. For details of the LDAP error code, see 'LDAP error code' In Appendix B.

Analyzing the Access Log

The following explains how to analyze the access log by example:

```
08/01 13:40:22.436320    0020    0    0    6    --->    CONNECT
IP=127.0.0.1:40199(localhost)     (line 1)
08/01 13:40:22.440007    0004    0    0    6    --->    BIND
"cn=manager,ou=interstage,o=fujitsu,dc=com" 3     (line 2)
08/01 13:40:22.443245    0005    0    1    6    --->    ADD
"ou=interstage,o=fujitsu,dc=com"     (line 3)
08/01 13:40:37.837376    0006    0    2    6    --->    ADD
"cn=ssoUser1,o=Fujitsu Limited,c=jp"     (line 4)
08/01 13:40:37.838490    0007    0    2    6    <---    ADD     NG    53
(line 5)
08/01 13:41:22.493324    0008    0    3    6    --->    UNBIND     (line 6)
```

line 1

A request processed at 13:40:22.436320 on August 1.

This indicates that Smart Repository received a connection request (CONNECT) from an application whose IP address is '127.0.0.1(localhost)' and port number is '40199.'

line 2

A request processed at 13:40:22.440007 on August 1.

This indicates that an authentication request (BIND) was received. Since the value of CONN (connection ID) is '0', which is the same as that in line 1, the request can be assumed to have come from the same application as line 1.

line 3

A request processed at 13:40:22.443245 on August 1.

An addition request (ADD) to the entry tree 'ou=interstage,o=fujitsu,dc=com' was received.

line 4

A request processed at 13:40:37.837376 on August 1.

An addition request (ADD) to the entry tree 'cn=ssoUser1,o=Fujitsu Limited,c=jp' was received.

line 5

A request processed at 13:40:37.838490 on August 1.

An addition request (ADD) failed (NG) and the error code '53' was returned. The error code '53' is an error code of LDAP (For the meaning of the error code, see 'LDAP error code').

Since CONN (connection ID) is '0' and OP (operation ID) is '2,' the investigation of the access log (with the same CONN and OP) shows that this is a response to the request of line 4.

line 6

A request processed at 13:41:22.493324 on August 1.

A release request (UNBIND) was received.

Maintenance Information of Smart Repository

Smart Repository outputs maintenance information to assist troubleshooting. Maintenance information is output to the following directory. When a problem occurs, save the information in the following directory:

Windows

```
C:\Interstage\IREP\var\_system
C:\Interstage\IREP\var\<repository name>\tmp
```

Solaris OE Linux

```
/var/opt/FJSVirep/_system
/var/opt/FJSVirep/<repository name>/tmp
```

Maintenance information collects the following types of information. However, not all details are released due to their nature.

Maintenance information	Description
Message log	Message information output by Smart Repository is collected.
Trace log	When some failure or error occurs in Smart Repository, its contents are collected
Process information	Process ID and parameters during execution are collected.
IPC information	Information about acquired IPC resources is collected.

Solaris OE Linux

Managing the SSL Communication Environment

To ensure continual SSL communication, the Interstage certificate environment needs to be managed. The Certificates required to use SSL communication have a limited life, so new certificates must be obtained and registered in the Interstage certificate environment, before the current one expires. Additionally, the new CRL (certificate revocation list), if obtained, needs to be registered. For information about management of the Interstage certificate environment, see 'Setting and Use of the Interstage Certificate Environment' in the Security System Guide.

Backing up and Restoring Smart Repository

Smart Repository repositories, can be backed up using the irepbacksys command. For information about backup operation, see 'Maintenance (Resource Backup)' in Operator's Guide.

Notes

- The procedure for backing up and restoring resources can only be performed on the same operating system. Backup on Solaris OE and restore to Windows® is unsupported.
- Smart Repository version cannot restore the backed up repository resource in an environment that is older than the backed up environment.
- Only the access log and data in the Smart Repository database can be backed up and restored. User applications will not be backed up.

Optimizing the Repository

Frequent read/write operations to the database storage directory (of the repository) result in fragmentation of the hard disk drive. This causes slow read/write operations and a loss of useable space. Both space and performance can be improved by optimizing the hard disk drive through defragmentation. Periodically defragment the hard disk drive if entries are modified frequently. However, since defragmentation cannot reclaim all free space, the area that cannot be used may grow gradually, leading to insufficient disk space. In such a case, expand the hard disk area.

Note

If an accident, such as a system power failure, occurs during optimization of the repository, data may be damaged. Thus, be sure to back up the repository before optimizing it.

For information about the backup of repository, see Backing up and Restoring Smart Repository.

Optimize the repository as follows:

1. Use the Interstage Management Console to stop the repository to be optimized.
2. Execute the following optimization command:

   Example)

   Windows

   Repository name: rep001

   ```
   C:\Interstage\Enabler\server\bin\omsreorg.exe rep001 -r
   ```

   Solaris OE

   Repository name: rep001

   ```
   /opt/FJSVena/server/bin/omsreorg rep001 -r
   ```

   Linux

   Repository name: rep001

   ```
   /opt/FJSVena/Enabler/server/bin/omsreorg rep001 -r
   ```

If an error message is displayed when the optimization command is executing, take the action shown in the following table:

Message	Actions
Datastore not stopped.	Wait until the repository has stopped, and then re-execute the optimization command. Repository stopping time is dependant on hardware performance and the number of registered entries in the repository. A repository with approximately ten thousand entries (operated continually over an hour) will require an approximate time period of 10 minutes to stop.
Files of datastore were not closed properly. Datastore is inconsistent.	The repository was stopped because of a flawed write. Re-start the repository. Re-stop the repository, after starting the target repository, by using the Interstage Management Console. Wait until the repository has stopped, and then re-execute the optimization command.
Administration function currently active on datastore.	The optimization command is already operating. Wait until it has finished.

3. Use the Interstage Management Console to start the optimized repository.

Recovery in Stand-alone Mode

This section explains the repository recovery procedure for stand-alone mode.

Environment Has been Destroyed

If the environment is damaged, recreate a repository in stand-alone mode. The repository can be restored by using the backup directory (for Solaris OE/Linux, it is backup file). If there is no backup directory (for Solaris OE/Linux, it is backup file), the repository needs to be recreated.

The following describes the procedure used to restore the repository from the backup directory (for Solaris OE/Linux, it is backup file) for a stand-alone operation,

1. Stop the repository using Interstage Management Console.
2. Delete the repository stopped in step 1.
3. Use the ireprestsys command to restore the repository from the backup directory (for Solaris OE/Linux, it is backup file).

Example

Windows

Backup directory name: X:\Backup\irep\rep001_back

Repository name: rep001

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001
IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back
[rep001]
```

Solaris OE Linux

Backup file name: /backup/irep/rep001_back.tar.Z

Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

4. Use the Interstage Management Console to start the recreated repository.

Data in Database Has been Destroyed

When data in database has been destroyed, only restore the data in database.

Data in database can be restored to the status when it has been backed up by using the backup directory (for Solaris OE/Linux, it is backup file). If there is no backup directory (for Solaris OE/Linux, it is backup file), the data needs to be recreated.

The following procedure details how to restore data in the database of the repository in stand-alone mode:

1. Stop the repository using Interstage Management Console.
2. Delete the repository stopped in step 1.
3. Using the Interstage Management Console set the following items with same value of the repository deleted in step 2, and then create a new repository.
   - [Repository name]
   - [Public directory]
   - [Create default tree?]
   - [User password encryption method]
   - [Database storage directory]
4. Select [System] > [Service] > [Repository] > [Create a New Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository] > [Create a New Repository]). Click the [Create] button.
5. Use the ireprestsys command (with the -dataonly option) to restore the repository from the latest backup directory (for Solaris OE/Linux, it is backup file). Specify the same repository name as the backup repository.
6. A message displays, requesting confirmation to replace the database. To replace the database and continue restoring the repository, enter 'y' or 'Y'. To stop restoring the repository, enter 'n' or 'N'. If any other key is typed, the confirmation message is displayed again.

Example

Windows

Backup directory name: X:\Backup\irep\rep001_back

Repository name: rep001

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
Data already exists in database store.
(C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)
Are you sure of deleting data in database store? (y/n):y
IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back
[rep001]
```

Solaris OE

Backup file name: /backup/irep/rep001_back.tar.Z

Repository name: rep001

```
#ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

Linux

Backup file name: /backup/irep/rep001_back.tar.Z

Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

7. Use the Interstage Management Console to start repository.

   For details of the ireprestsys commands, see 'Backup commands' in the Reference Manual (Command Edition).

Monitoring of Operation in Replication Mode and Recovery

This section explains messages output, when problems occur during operation in replication mode, and the recovery procedure for restoring the repository.

Monitoring of Operation in Replication Mode

Solaris OE Linux

If a problem occurs in replication mode, messages beginning with irep15XXX are output to system log of the master server.

Windows

If a problem occurs in replication mode, messages beginning with irep15XXX are output to the event log.

By monitoring the log files, replication errors can be detected quickly.

See 'Messages beginning with irep15XXX' in 'Messages' for error messages and the associated [User action].

Restoring the Slave Repository in Replication Mode

The following procedure describes how to restore the slave repository in replication mode.

If the environment is damaged, the repository is restored by recreating a slave repository.

If data inside the database is damaged, only data in the slave repository is restored.

Environment Has been Destroyed

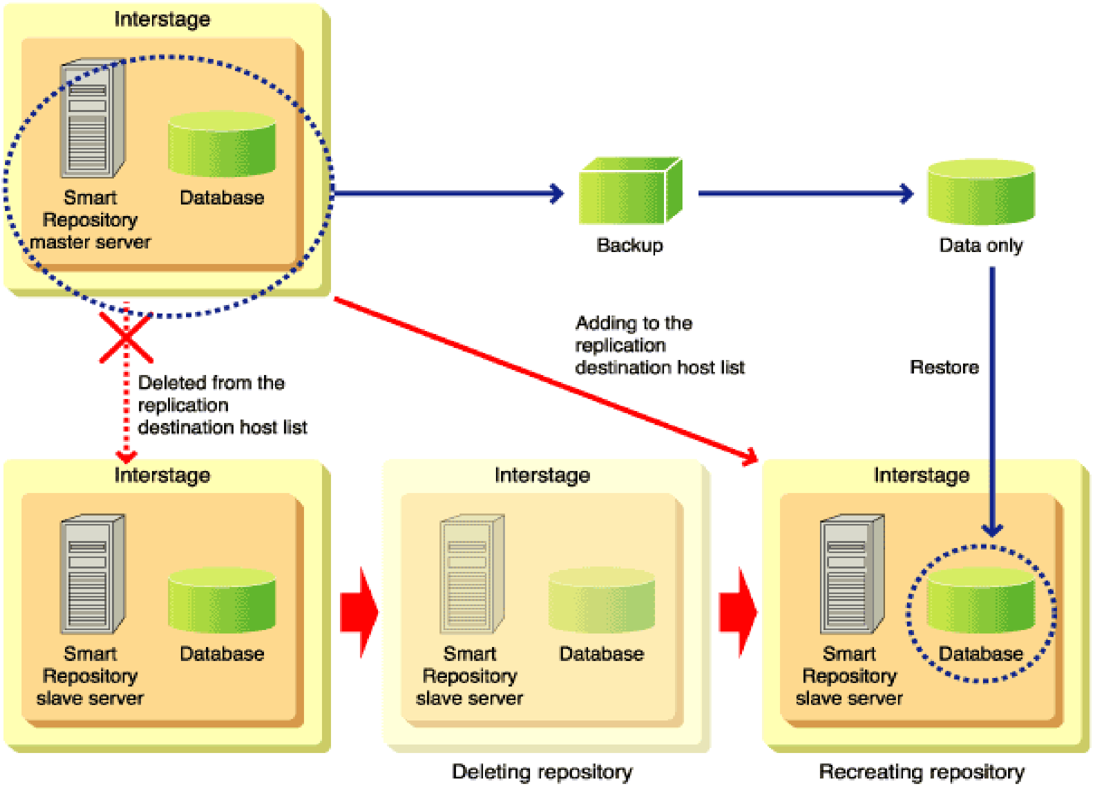

Interstage
Smart Repository master server
Database
Backup
Data only
Adding to the replication destination host list
Restore
Deleted from the replication destination host list
Interstage
Smart Repository slave server
Database
Interstage
Smart Repository slave server
Database
Deleting repository
Interstage
Smart Repository slave server
Database
Recreating repository

Figure 4-2 Environment Has been Destroyed

Operation on the Master Server

1. Stop the repository that has the same name as the restoring repository for the slave server. This step is performed using the Interstage Management Console
2. Use the ireprestsys command to backup the repository that has same name as the restoring repository for the slave server.
3. Transfer the backup directory (for Solaris OE/Linux, it is backup file) created in step 2 to the slave server.
4. Click [Detailed setting [show]] on the [Settings] window of the repository stopped in step 1.
5. Select and delete the host name of the slave server where the repository to be restored exists from [Replication destination host list].

Operation on the Slave Server

6. Stop the restoring repository using the Interstage Management Console
7. Delete the repository stopped in step 6.
8. Use the Interstage Management Console to ensure the following items have the same settings as the master repository by using [Create a New Repository] tab (after selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])) and then click the [Create] button.
   - [Repository name]
   - [Public directory]
   - [Create default tree?]
   - [User password encryption method]
   - [Database storage directory]
9. Use the ireprestsys command with the specified -dataonly option to restore the repository from the backup directory (for Solaris OE/Linux, it is backup file) in step 3.
10. Specify the same repository name as that of the backed up repository.
11. A message displays, requesting confirmation to replace the database. To replace the database and continue restoring the repository, enter 'y' or 'Y'. To stop restoring the repository, enter 'n' or 'N'. If any other key is typed, the confirmation message is displayed again.

    Example

    Windows

    Backup directory name: X:\Backup\irep\rep001_back
    Repository name: rep001

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
Data already exists in database store.
(C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)
Are you sure of deleting data in database store? (y/n):y
IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back
[rep001]
```

    Solaris OE

    Backup file name: /backup/irep/rep001_back.tar.Z
    Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

Linux

Backup file name: /backup/irep/rep001_back.tar.Z
Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

12. Using the Interstage Management Console, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]). Click the restored repository displayed on the [Repository : View Status] window.
13. Click [Detailed settings [View]] on the [Settings] window and then select 'Slave' from [Replication settings].
14. Set the host name of the master server in [Slave operation settings] and then click the [Apply] button.
15. Start the restored repository using the Interstage Management Console.

Operation on the Master Server

16. In the Interstage Management Console, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]). Open the [Repository : View Status] window. Click the repository with the same name as the restored slave repository displayed in the window.
17. Click [Detailed settings [View]] on the [Settings] window.
18. Click the [Add] button in [Replication destination host list].
19. Enter information about the restored slave repository to each item in [Replication Connection Settings] and then click the [Apply] button.
20. Start the restored master repository from the [Repository : View Status] window (found by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).

For details of the irepbacksys and ireprestsys commands, see 'Backup commands' in the Reference Manual (Command Edition).

Data in Database Has been Destroyed

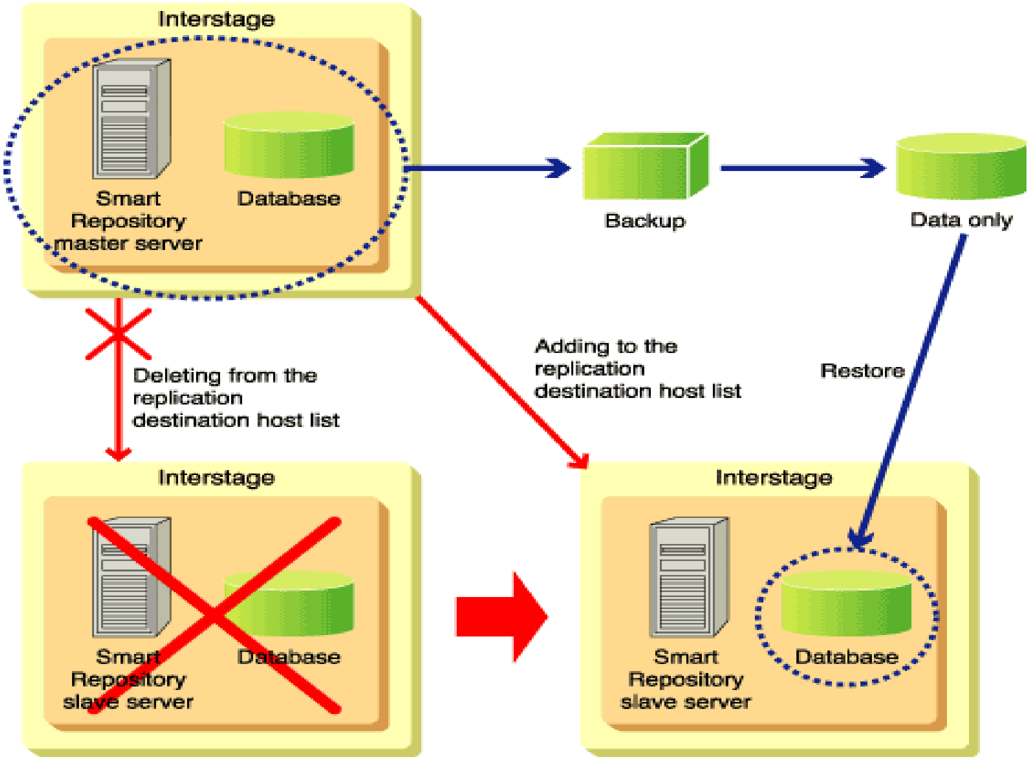

Interstage
Smart Repository master server
Database
Backup
Data only
Deleting from the replication destination host list
Adding to the replication destination host list
Restore
Interstage
Smart Repository slave server
Database
Interstage
Smart Repository slave server
Database

Figure 4-3 Data in Database Has been Destroyed

Operation on the Master Server

1. Stop the repository using the Interstage Management Console. If multiple repositories are defined, select the repository with the same name as that of the slave repository to be restored.
2. Use the irepbacksys command to back up the repository stopped in step 1.
3. Transfer the backup file created in step 2 to the slave server on which the repository to be restored exists.
4. Click [Detailed settings [show]] on the [Settings] window of the repository stopped in step 1.
5. From [Replication destination host list], select and delete the host name of the slave server on which the repository to be restored exists.

Operation on the Slave Server

6. In the Interstage Management Console, stop the repository to be restored.

7 Use the ireprestsys command with the specified -dataonly option to restore only data inside the database from the backed up directory (In Solaris OE/Linux case, it is backed up file) transferred in step 3. Specify the same repository name as that of the backup repository.

8. A message displays, requesting confirmation to replace the database. To replace the database and continue restoring the repository, enter 'y' or 'Y'. To stop restoring the repository, enter 'n' or 'N'. If any other key is typed, the confirmation message is displayed again.

   Example)

   Windows

   Backup directory name: X:\Backup\irep\rep001_back
   Repository name: rep001

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
Data already exists in database store.
(C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)
Are you sure of deleting data in database store? (y/n):y
IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back
[rep001]
```

   Solaris OE

   Backup file name: /backup/irep/rep001_back.tar.Z
   Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

   Linux

   Backup file name: /backup/irep/rep001_back.tar.Z
   Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.Z [rep001]
```

9. In the Interstage Management Console, start the restored repository.

Operation on the Master Server

10. In the Interstage Management Console, click the repository stopped in step 1 displayed in the [Repository: View Status] window (found by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).
11. Click [Detailed settings [View]] on the [Settings] window.
12. Click the [Add] button in [Replication destination host list].
13. Enter information about the restored slave repository to each item in [Replication Connection Settings] and then click the [Apply] button.
14. Use the Interstage Management Console to start the restored master repository.

For details of the irepbacksys and ireprestsys commands, see 'Backup commands' in the Reference Manual (Command Edition).

Restoring the Master Repository in Replication Mode

Using the master repository backed up directory (In Solaris OE/Linux case, it is backed up file), the master repository can be restored in replication mode. If there is no backed up directory (In the case of Solaris OE/Linux, it is a backed up file), the replication mode needs to be recreated.

Backed up Directories (or Files)

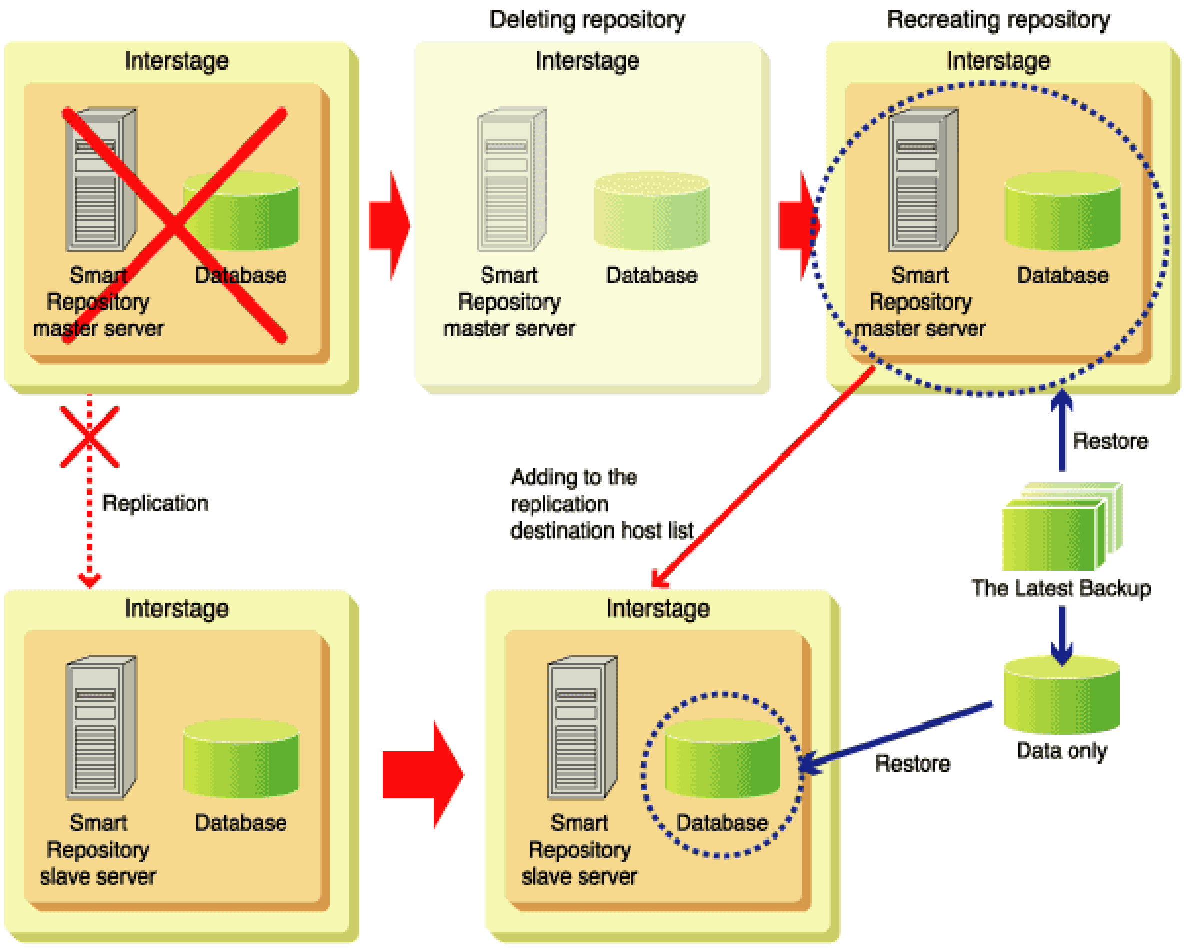

Deleting repository
Recreating repository
Interstage
Smart Repository master server
Database
Interstage
Smart Repository master server
Database
Interstage
Smart Repository master server
Database
Replication
Adding to the replication destination host list
Restore
The Latest Backup
Data only
Restore
Interstage
Smart Repository slave server
Database
Interstage
Smart Repository slave server
Database

Figure 4-4 Backed up Directories (or Files)

Operation on the Master Server

1. Stop the repository to be restored using the Interstage Management Console.
2. Delete the repository stopped in step 1.

Operation on the Slave Server

3. Using the Interstage Management Console, stop the repository with same process in step 1. If multiple repositories are defined, stop the repository with the same name as the master repository to be restored.
4. Use the ireprestsys command (with the specified -dataonly option) to restore the data from the backed up directory (In Solaris OE/Linux case, it is backed up file) of the master repository.
5. Use the Interstage Management Console to start the restored repository.

Operation on the Master Server

6. Use the ireprestsys command (with the -S option) to restore the master repository backup directory (for Solaris OE/Linux, it is backup file)
7. Select the restored repository as displayed in the [Repository : View Status] window.
8. Click [Detailed settings [show]] on the [Settings] window and then select 'Master' from [Replication Settings].
9. Click the [Add] button in [Replication destination host list].
10. Set information about the restored slave repository for each item in [Replication Connection Settings] and then click the [Apply] button.
11. Use the Interstage Management Console to start the restored master repository.

For details of the irepbacksys and ireprestsys commands, see 'Backup commands' in Reference Manual (Command Edition).

No Backed up Directories (or Files) Exist

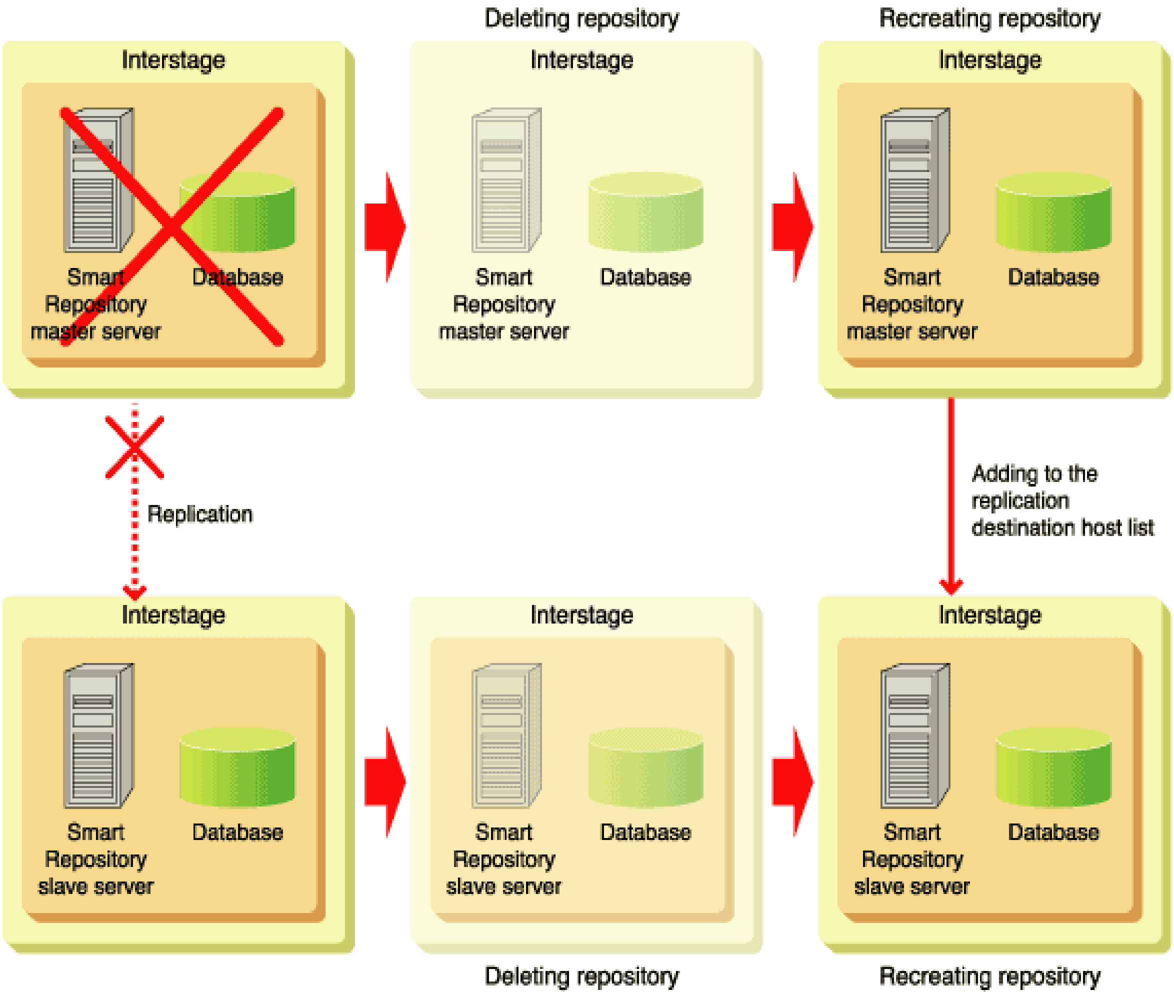

Deleting repository
Recreating repository
Interstage
Smart Repository master server
Database
Interstage
Smart Repository master server
Database
Interstage
Smart Repository master server
Database
Replication
Adding to the replication destination host list
Interstage
Smart Repository slave server
Database
Interstage
Smart Repository slave server
Database
Interstage
Smart Repository slave server
Database
Deleting repository
Recreating repository

Figure 4-5 No Backed Up Directories (or Files) Exist

Operation on the Master Server

1. Stop the repository to be restored using the Interstage Management Console.

Operation on the Slave Server

2. Use the Interstage Management Console to stop the repository, with the same name, as the master repository to be restored.
3. Delete the repository stopped in step 2.

Operation on the Master Server

4. Delete the repository stopped in step 1.
5. Create the replication mode. For details of the environment setup in replication mode, see 'Flow of the Environment Setup' in Chapter 2 - Environment Setup.

Chapter 5

Creating an Application (JNDI)

This chapter describes the method of creating an application using Smart Repository with JNDI.

To create an application in JNDI, an environment in which a Java program can be compiled is necessary. Check that either JDK 1.3 or JDK 1.4 has been installed. With a standard installation, JDK 1.4 is installed.

For a custom installation, either JDK 1.3 or JDK 1.4 must be installed separately.

How to Use JNDI

This section explains how to perform the following tasks to set up JNDI:

- Preparing a Development Environment
- Flow of Basic Operations

Preparing a Development Environment

In order to prepare the development environment, set up the environment variables required for compilation and for the operation of an application.

Windows

If using SSL, set up the following Java Archive (jar) files in CLASSPATH.

- C:\Interstage\ID\Dir\sdk\JAVA\lib\fjssl.jar

In JAVA_HOME, the following value has been automatically set during installation.

- For JDK1.3

  C:\Interstage\JDK13

- For JDK1.4

  C:\Interstage\JDK14

In PATH, set the following directory:

- C:\Interstage\ID\Dir\sdk\JAVA\lib

Solaris OE Linux

If using SSL, set up the following Java Archive (jar) files in CLASSPATH.

- /opt/FJSVidsdk/JAVA/lib/fjssl.jar

In JAVA_HOME, set either of the following directories:

- For JDK1.3

  /opt/FJSVawjbk/jdk13

- For JDK1.4

  /opt/FJSVawjbk/jdk14

In LD_LIBRARY_PATH, set the following directory:

- /opt/FJSVidsdk/JAVA/lib

When executing the created .class file, set up the storage path of the created .class file in CLASSPATH.

Flow of Basic Operations

To access a Smart Repository server in JNDI, it is necessary to perform the following steps.

- Set up environment properties
- Open a session and perform the initial setup and user authentication (simple authentication using passwords)
- Access the LDAP server
- Close the session

For the processes that can be requested when accessing a Smart Repository server, this section describes the following operations:

- Search entry
- Add entry
- Modifying the attribute value of an entry
- Delete entry.

Note

Smart Repository does not check the schema when an entry is modified.

If you incorrectly modify an entry, e.g., deleting a required attribute in an entry or adding to an object class an attribute that should not be added, the information in the repository will become inconsistent. When modifying an entry, ensure you are making the correct modification .

Setting an Environment Property

To access a repository server in SSL communications, set the following JNDI environment properties and system properties.

- JNDI environment properties
  - javax.naming.Context.INITIAL_CONTEXT_FACTORY
  - javax.naming.Context.PROVIDER_URL
  - javax.naming.Context.SECURITY_AUTHENTICATION
  - javax.naming.Context.SECURITY_PRINCIPAL
  - javax.naming.Context.SECURITY_CREDENTIALS
  - javax.naming.Context.SECURITY_PROTOCOL
  - 'java.naming.ldap.factory.socket'
- System properties
  - 'user.sslenvfile'
  - 'user.ssllogdir'

Environment Properties

Table 5-1 lists the environment properties in JNDI:

Table 5-1 JNDI Environment Properties

Property name	Value to be specified	Requirement level
javax.naming.Context.INITIAL_CONTEXT_FACTORY	When using LDAP make sure that you specify 'com.sun.jndi.ldap.LdapCtxFactory.'	R
javax.naming.Context.PROVIDER_URL	Specify the URL of a repository server. Specify it as 'ldap://host-name:port-number.'	R
javax.naming.Context.SECURITY_AUTHENTICATION	Specify the authentication mechanism to be used to bind to a repository server. For more information about the specification method, see 'Authentication mechanism.'	R
javax.naming.Context.SECURITY_PRINCIPAL	Specify a DN name to be used to bind to a repository server. The default value is anonymous (anonymous user).	
javax.naming.Context.SECURITY_CREDENTIALS	Specify a password to be used to bind to a repository server. The default value is no password.	
javax.naming.Context.SECURITY_PROTOCOL	Specify a security protocol to be used for communications with a repository server. For more information about the specification method, see 'Security protocol.'	S
'java.naming.ldap.version'	Specify a protocol version to be used for communications with a repository server. Specify '2' for LDAP version 2 or '3' for LDAP version 3. The default value is LDAP version 3.	
'java.naming.ldap.attributes.binary'	Specify one or more attributes with binary syntax. When specifying multiple attributes, use blanks to delimit them.	
'java.naming.ldap.deleteRDN	Specify whether the old RDN has been deleted during rename() processing. The default value is true.	

Property name	Value to be specified	Requirement level
'java.naming.ldap.typesOnly'	Specify 'true' or 'false' to select whether or not to return only an attribute type to search() and get Attributes(). The default value is false.	
'java.naming.ldap.ref.separator'	Specify a character to be used to encode a RefAddr object in a javaReferenceAddress attribute.	
'java.naming.ldap.factory.socket'	Specify the class name of a socket factory. For more information on the specification method, see 'Socket factory'.	S
'com.sun.jndi.ldap.trace.ber'	Specify an output stream into which an LDAP protocol trace should be written. Although this environment property is optional, it is recommended that users specify it as much as possible. For more information about the specification method, see 'LDAP protocol trace'	

Table 5-2 lists the system properties:

Table 5-2 System Properties

Property name	Value to be specified	Requirement level
user.sslenvfile	Specify the storage location (path) of an SSL environment definition file. For more information about the specification method, see 'SSL environment definition file'.	S
user.ssllogdir	Specify the storage location (path) of an SSL log file. For more information on the specification method, see 'SSL log file directory'	

R: Required

S: Required if SSL is used

Blank: Optional

javax.naming.Context.SECURITY_AUTHENTICATION

Authentication Mechanism

In this environment property, specify an authentication mechanism to be used to bind to a repository server. Valid values include 'none' or 'simple.'

Example:

```
env.put( Context.SECURITY_AUTHENTICATION, "none" );
```

The following values can be specified in authentication mechanism.

Value	Explanation
none	Specify authentication as anonymous (anonymous user).
simple	Specify simple authentication.

javax.naming.Context.SECURITY_PROTOCOL

Security Protocol

Specify a security protocol in this environment property. If the SSL library is being used, 'ssl' must be specified for this value.

Example:

```
env.put( Context.SECURITY_PROTOCOL, "ssl" );
```

java.naming.ldap.factory.socket

Socket Factory

In this environment property, specify the class name of a socket factory. If the SSL library is being used, specify the following value. If this environment property is omitted, SSL will not be used.

```
"com.fujitsu.ssl.FjSSLSocketFactory"
```

Example:

```
env.put( java.naming.ldap.factory.socket,
"com.fujitsu.ssl.FjSSLSocketFactory");
```

com.sun.jndi.ldap.trace.ber

LDAP Protocol Trace

In this environment property, specify an output stream (java.io.OutputStream object) into which an LDAP protocol trace should be written.

If problems occur (e.g. confirm access information in the LDAP protocol), take action to troubleshoot the problem. Users are recommended to specify this environment parameter before creating a JNDI application.

Example:

```
env.put( com.sun.jndi.ldap.trace.ber, System.out);
```

user.sslenvfile

SSL Environment Definition File

In this system property, specify the full path of an SSL environment definition file.

For information describing the method of creating an SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)'. This system property is required if SSL is being used.

Example:

Windows

```
prop.put( user.sslenvfile, "D:\\conf\\sslconfig.cfg");
```

Solaris OE Linux

```
prop.put( user.sslenvfile, "/conf/sslconfig.cfg");
```

user.ssllogdir

SSL Log File Directory

In this system property, specify an SSL log file directory. During SSL communications, a log file to be output by the SSL library will be stored in this SSL log file directory. Specify this system property to collect an SSL log when SSL is used.

Example:

Windows

```
prop.put( user.ssllogdir, "D:\\log");
```

Solaris OE Linux

```
prop.put( user.ssllogdir, "/log");
```

Opening a Session and Performing Initial Setup and User Authentication

To access a Smart Repository server by JNDI, it is necessary to open a session and perform initial setup and user authentication. At this point, use the 'Hashtable env' variables that have been set for the configuration of the environment properties.

If a session is opened, it is also necessary to close the session after gaining access to the Smart Repository server.

Example:

```
DirContext ctx = new InitialDirContext(env);
```

Note

Cases in which Multiple Sessions are Needed

The javax.naming.directory.InitialDirContext class performs initial setup and user authentication as soon as a session is opened. To modify user authentication information during processing, users must open a new session.

In this case, only close the sessions that have been started. In addition, use the javax.naming.ldap.InitialLdapContext class to modify the user authentication settings, etc. while the sessions are open. For information about the specification method, refer to the following example:

```
Hashtable env = new Hashtable(5, 0.75f);
env.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldap://host:389");

// Open a session by getting authentication as anonymous (anonymous user).
env.put(Context.SECURITY_AUTHENTICATION, "simple");
env.put(Context.SECURITY_PRINCIPAL, "");
env.put(Context.SECURITY_CREDENTIALS, "");
InitialLdapContext ctx = new InitialLdapContext(env,null);


// Getting authentication again as administrator.
ctx.addToEnvironment(Context.SECURITY_AUTHENTICATION, "simple");
ctx.addToEnvironment(Context.SECURITY_PRINCIPAL,
"cn=admin,ou=interstage,o=fujitsu,dc=com");
ctx.addToEnvironment(Context.SECURITY_CREDENTIALS, "admin");
ctx.reconnect(null);


// Close the session.
ctx.close();
```

Maximum Number of Sessions

The maximum number of sessions which can be maintained in one process is 1024. If an attempt is made to open a session when after the maximum has been exceeded, an SSLException will be thrown.

SSLException error type value (int): 99, SSL error code: 200002

Take the following actions on the application side:

- Coding to close the unnecessary session(s).
- If the session is reusable, decrease the number of sessions. For details on how to decrease the number, refer to 'Cases in which Multiple Sessions are Needed', above.
- Increasing the number of processes and then dividing the sessions among them is a way to limit the number of sessions in one process from the application side.

Accessing a Smart Repository Server

To access the Smart Repository server using JNDI, set 'com.sun.jndi.ldap.LdapCtxFactory' to the environmental property 'javax.naming.Context.INITIAL_CONTEXT_FACTORY'

For details of environmental property information, refer to 'Environmental property (ENVIRONMENT PROPERTIES)'.

Use the following JNDI methods to perform basic LDAP server access:

- search()

  Search for an entry.

- createSubcontext()

  Add an entry.

- modifyAttributes()

  Modify the attribute value of an entry.

- destroySubcontext()

  Delete an entry.

. Windows

For information on detailed usage, refer to Sample Programs or the sample programs stored in

'C:\Interstage\IREP\sample\JAVA.'

Solaris OE Linux

For information on detailed usage, refer to Sample Programs or the sample programs stored in '/opt/FJSVirep/sample/JAVA.'

Closing a Session

After you have completed a series of processing on a Smart Repository server, close a session.

Example:

```
ctx.close();   *
```

Note

ctx is an instance variable acquired as described in 'Opening a session and performing initial setup and user authentication.'

Acquiring an SSL Error

This section describes how to acquire an error on SSL.

From a message output by SSL, an error type and an error code can be acquired.

1. From an output message, extract error information using 'FjSSLSocket' as a key.

2. From error information, extract an error type using 'errtype=' as a key.
3. From error information, extract an SSL error code using 'SSLLerrorcode=' as a key.

Sample message:

```
com.fujitsu.ssl.SSLException: FjSSLSocket:SSL_Init error, errtype=10
SSLLerrorcode=10004c
```

An error type and an SSL error code can be acquired in the following way:

```
catch(NamingException ne){
        Throwable msg       = ne.getRootCause();
        String    msgStr    = null;
        int       ssl_error = -1;
        if ( msg != null ){
            /* Get an error message */
            msgStr = msg.toString();
            /* Acquire error information using "FjSSLSocket" as a key. (1)
*/
            ssl_error = msgStr.indexOf("FjSSLSocket");
        }
        /* When SSL is used */
        if ( ssl_error != -1 ){
            int index1 = msgStr.indexOf("errtype=") + "errtype=".length();
            int index2 = msgStr.indexOf("SSLLerrorcode=") +
"SSLLerrorcode=".length();
            if ( index1 != -1 ){
                /* Acquire an error type using "errtype=" as a key. (2) */
                String error = msgStr.substring(index1, index1 + 2);
                /* Print an error type */
                System.out.println("SSL Error type : " + error);
            }
            if ( index2 != -1 ){
                /* Acquire an SSL error code using "SSLLerrorcode=" as a key.
(3) */
                String error = msgStr.substring(index1, index1 + 2);
                /* Print a SSL error code */
                System.out.println("SSL Error code : " + error);
            }
        }
}
```

Error Types

Table 5-3 lists SSL Exception error types:

Table 5-3 SSL Error Types

SSL Exception error type	Error type value (int)	Description	User action
CERT_EXPIRED	1	The site certificate has expired.	See the user action for SSL error code, 0x00100008.
CA_CERT_EXPIRED	2	The certificate of the certificate authority (issuing authority certificate) has expired.	See the user action for SSL error code, 0x00100009.
VERIFY_CERT_ERROR	3	Failed to verify the certificate authority certificate or site certificate.	See the user action for SSL error code, 0x0010000C.
DEC_PRIKEY_ERROR	4	Failed to decrypt the private key.	See the user action for SSL error code, 0x00100012.
SVR_CERT_EXPIRED	5	The site certificate of the connection destination has expired.	See the user action for SSL error code, 0x00100018.
VERIFY_SVR_CERT_ERROR	6	Failed to verify the site certificate of the connection destination.	See the user action for SSL error code, 0x0010001A.
CLNT_CERT_EXPIRED	7	This site certificate has expired.	See the user action for SSL error code, 0x0010002E.
VERIFY_CLNT_CERT_ERROR	8	Failed to verify the site certificate.	See the user action for SSL error code, 0x00100035.
NOT_EXIST_SECRETKEY	9	There is no private key for the site certificate.	See the user action for SSL error code, 0x0010003B.
PARAM_ERROR	10	There is an error in the settings of the SSL environment definition file.	See the user action for each SSL error code.
MEMORY_ERROR	11	A memory shortage occurred.	See the user action for each SSL error code.
TIME_OUT	12	A timeout occurred.	See the user action for SSL error code, 0x00010001.
OTHER_ERROR	13	This is one of other errors.	See the user action for each SSL error code.
CONNECT_ERROR	14	An error occurred during connection with the server.	See the user action for SSL error codes, 0x00400001 to 0x0040000E.

SSL Exception error type	**Error type value (int)**	**Description**	**User action**
INVALID_ENVFILE	15	The environment file has a format error.	Check the format of the environment file.
LINK_ERROR	16	Failed to load a library.	See 'Preparing a development environment' and check that a necessary library is stored in the correct directory.
RETRY	17	Reception is disabled because transmission is in progress.	Try again after a while.
UNKNOWN_HOST	18	Cannot identify the host IP address.	Check that the host name and the IP address are correct.
NOT_SSL_ENVFILE	20	No environment file is specified or exists.	Specify a correct environment file.
SSL_VERSION_INVALID	21	There is an error in the specification of the SSL version.	Check the value of the SSL version.
INTERNAL_ERROR	99	Session has been opened when the number of sessions in the process has exceeded the allowable maximum of 1024.	Refer to the 'Maximum Number of Sessions '.

SSL Error Codes

For information about the values of SSL error codes, see 'SSL Error Codes.'

Sample Programs

Windows

JNDI sample programs are stored in 'C:\Interstage\IREP\sample\JAVA.'

Solaris OE Linux

JNDI sample programs are stored in '/opt/FJSVirep/sample/JAVA.'

List of Sample Program Files

The following lists the source documents for JNDI sample programs:

Source name	**Overview of processing**
AddEntry.java	Add an entry (for SSL operation).
DelEntry.java	Delete an entry (for SSL operation).
Modattrs.java	Read an attribute (for SSL operation).
Search.java *1	Perform entry search (for SSL operation).

*1 For information about Search.java, see Explanation of a Sample Program.

Execution Procedure of a Sample Program

This section explains the procedures from compilation to execution of a sample program.

1. Copy all the files in the sample program storage directory to a work directory.
2. According to the environment of a Smart Repository server to be connected, modify the parameter values in the sample source. For the applicable parameters, refer to the following list of parameters:

Table 5-4 Sample Program Parameters

Sample source	Parameter	Overview	Remarks
Common parameters	ldapurl	URL information of a repository server	Specify it as 'ldap://host-name:port-number.'
	binddn	DN to be used to bind to a repository server	
	password	Password to be used to bind to a repository server	
	sslenvfile	Storage location (path) of an SSL environment definition file	
	ssllogdir	Storage location (path) of an SSL log file	
AddEntry.java	add_dn	DN of an entry to be added	
	orig	Information of an attribute to be added (BasicAttributes object)	Set an attribute (BasicAttributes object) to be added.
DelEntry.java	del_dn	DN of an entry to be deleted	
Modattrs.java	mod_dn	DN of an entry to be modified	
	mods	Information about an attribute to be modified (ModificationItem object array)	Set the attribute (ModificationItem object) to be modified.
Search.java	s_base	Search base	
	filter	Search filter	

3. Compile the sample program based on the following compilation example. After compilation is executed, check that a class file has been created.

Example

The following shows a compilation example.

To use JDK1.4, enter:

Windows

```
C:\Interstage\JDK14\bin\javac Search.java
```

Solaris OE Linux

```
/opt/FJSVawjbk/jdk14/bin/javac Search.java
```

After compilation, a 'Search.class' file will be created.

4. Set up the storage path for the created .class file in CLASSPATH and execute the sample program as shown in the following execution example:

Example

The following text provides an example of execution.

To use JDK1.4, enter:

Windows

```
C:\Interstage\JDK14\bin\java Search
```

Solaris OE Linux

```
/opt/FJSVawjbk/jdk14/bin/java Search
```

Notes for Creating a JNDI Application

Execute the close() method for InitialDirContext, UNBIND will not be sent out immediately if:

- Not all search results have been extracted.
- The search results have not been abandoned.

In this case, connections are accumulated between the client and server until they are closed at the following timing. DISCONNECT will actually be sent out instead of UNBIND at the following timing.

- Timing at which the Java VM invokes finalize() upon exit from an application.
- Timing at which the Java VM performs garbage collection when the reference to variables in the search results becomes invalid.

If a servlet is run in JNDI or if a program repetitiously opens and closes a connection, the problem of not being able to connect to a Smart Repository server may occur.

To avoid accumulating connections, clear the search result using one of the following methods so that UNBIND is definitely sent out.

- Extracting all the search results

```
DirContext ctx = new InitialDirContext(env);
NamingEnumeration results = ctx.search("dc=com", "cn=User001",
constraints);
while (results != null && results.hasMore()){
    SearchResult sr = (SearchResult)results.next();
}
```

- Discarding the search results

```
DirContext ctx = new InitialDirContext(env);
NamingEnumeration results = ctx.search("dc=com", "cn=User001",
constraints);
results.close();
```

Explanation of a Sample Program

This section explains a sample program for performing an entry search. The sample listed below provides an example of a search performed on a specified repository server based on simple authentication using SSL and output of entry information.

For information on other sample programs, see their source files directly.

Windows

```
/* Copyright (c) 2004 FUJITSU LIMITED
 * All Rights Reserved.
 *
 * Perform entry search(For SSL)
 */

import java.util.Hashtable;
import java.util.Enumeration;
import java.util.Properties;

import javax.naming.*;
import javax.naming.directory.*;
import com.sun.jndi.ldap.*;

class Search {

/*
 *  Config parameters
 *     (It is necessary to modify the following parameters to accord to the
execution environment)
 */
public static final String ldapurl     = "ldap://localhost:636/";
public static final String binddn      =
"cn=manager,ou=interstage,o=fujitsu,dc=com";
public static final String password    = "secret";
public static final String sslenvfile  = "D:\\conf\\sslconfig.cfg";
public static final String ssllogdir   = "D:\\log";
public static final String s_base      = "ou=interstage,o=fujitsu,dc=com";
public static final String filter      = "cn=user001";

public static void main(String[] args) {

        Hashtable env = new Hashtable();
        env.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");

        /* Set environment properties */
        env.put(Context.PROVIDER_URL,              ldapurl   );
        env.put(Context.SECURITY_AUTHENTICATION,   "simple"  );
        env.put(Context.SECURITY_PRINCIPAL,        binddn    );
        env.put(Context.SECURITY_CREDENTIALS,      password  );
        /* Set environment properties for SSL */
        env.put("java.naming.ldap.factory.socket",
"com.fujitsu.ssl.FjSSLSocketFactory");
        env.put(Context.SECURITY_PROTOCOL,         "ssl"     );

        /* Get System property */
        Properties prop = System.getProperties();
        prop.put("user.sslenvfile",                sslenvfile);
        prop.put("user.ssllogdir",                 ssllogdir );

        try
        {
                /* Connnect to repository server*/
                DirContext ctx = new InitialDirContext(env);

                /* Specify search range */
                SearchControls constraints = new SearchControls();
                constraints.setSearchScope(SearchControls.SUBTREE_SCOPE);

                /*
                 * Execute search operation by search starting position
"ou=interstage,o=fujitsu,dc=com" and search filter "cn=User001"
                 */
                NamingEnumeration results = ctx.search(s_base, filter,
constraints);

                /* Indicate the search results */
                while (results != null && results.hasMore()) {
                        SearchResult si = (SearchResult)results.next();

                        /* Output entry name*/
                        System.out.println("name: " + si.getName());
                        Attributes attrs = si.getAttributes();
                        if (attrs == null) {
                                System.out.println("No attributes");
                        } else {
                                /* output attribute */
                                for (NamingEnumeration ae = attrs.getAll();
                                    ae.hasMoreElements(); ) {
                                        Attribute attr =
(Attribute)ae.next();
                                        String attrId = attr.getID();

                                        /* Output attribute value */
                                        for (Enumeration vals =
attr.getAll();
                                            vals.hasMoreElements();
                                            System.out.println(attrId + ": "
+ vals.nextElement()));
                                }
                        }
                        System.out.println();
                }
                ctx.close();
        }
        catch(NamingException ne)
        {
                Throwable msg       = ne.getRootCause();
                String    msgStr    = null;
                int       ssl_error = -1;

                if ( msg != null ) {
                        /* Get an error message */
                        msgStr = msg.toString();
                        /* Search a key to get error information */
                        ssl_error = msgStr.indexOf("FjSSLSocket");
                }
                /* Processing for SSL */
                if ( ssl_error != -1 ) {
                        int index1 = msgStr.indexOf("errtype=") +
"errtype=".length();
                        if ( index1 != -1 ) {
                                /* Get error type */
                                String error = msgStr.substring(index1,
index1 + 2);
                                /* Indicate error type */
                                System.out.println("SSL Error code : " +
error);
                        }
                }
                System.out.println("Search example failed.");
        }
        catch(Exception e)
        {
                System.out.println(e.getMessage());
                System.out.println(e.getLocalizedMessage());
        }
}

}
```

Solaris OE Linux

```
/* Copyright (c) 2003 FUJITSU LIMITED
 * All Rights Reserved.
 *
 * Perform entry search(For SSL)
 */

import java.util.Hashtable;
import java.util.Enumeration;
import java.util.Properties;

import javax.naming.*;
import javax.naming.directory.*;
import com.sun.jndi.ldap.*;

class Search {
```

```
/*
 *  Config parameters
 *     (It is necessary to modify the following parameters to accord to the
execution environment)
 */
public static final String ldapurl     = "ldap://localhost:636/";
public static final String binddn      =
"cn=manager,ou=interstage,o=fujitsu,dc=com";
public static final String password    = "secret";
public static final String sslenvfile  = "/conf/sslconfig.cfg";
public static final String ssllogdir   = "/log";
public static final String s_base      = "ou=interstage,o=fujitsu,dc=com";
public static final String filter      = "cn=user001";

public static void main(String[] args) {

        Hashtable env = new Hashtable();
        env.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");

        /* Set environment properties */
        env.put(Context.PROVIDER_URL,              ldapurl   );
        env.put(Context.SECURITY_AUTHENTICATION,   "simple"  );
        env.put(Context.SECURITY_PRINCIPAL,        binddn    );
        env.put(Context.SECURITY_CREDENTIALS,      password  );
        /*  Set environment properties for SSL */
        env.put("java.naming.ldap.factory.socket",
"com.fujitsu.ssl.FjSSLSocketFactory");
        env.put(Context.SECURITY_PROTOCOL,         "ssl"     );

        /* Get System property */
        Properties prop = System.getProperties();

        prop.put("user.sslenvfile",                sslenvfile);
        prop.put("user.ssllogdir",                 ssllogdir );

        try
        {
                /* Connect to repository server */
                DirContext ctx = new InitialDirContext(env);

                /* Specify search range */
                SearchControls constraints = new SearchControls();
                constraints.setSearchScope(SearchControls.SUBTREE_SCOPE);

                /*
                 * Execute search operation by search starting position
"ou=interstage,o=fujitsu,dc=com" and search filter "cn=User001"
                 */
                NamingEnumeration results = ctx.search(s_base, filter,
constraints);

                /* Indicate search results */
                while (results != null && results.hasMore()) {
                        SearchResult si = (SearchResult)results.next();
                        /* Output entry name */
                        System.out.println("name: " + si.getName());

                        Attributes attrs = si.getAttributes();
                        if (attrs == null) {
                                System.out.println("No attributes");
                        } else {
                                /* Output attribute */
                                for (NamingEnumeration ae = attrs.getAll();
                                    ae.hasMoreElements(); ) {
                                        Attribute attr =
(Attribute)ae.next();
                                        String attrId = attr.getID();

                                        /* Output attribute value */
                                        for (Enumeration vals =
attr.getAll();
                                            vals.hasMoreElements();
                                            System.out.println(attrId + ": "
+ vals.nextElement()));
                                }
                        }
                        System.out.println();
                }
                ctx.close();
        }
        catch(NamingException ne)
        {
                Throwable msg       = ne.getRootCause();
                String    msgStr    = null;
                int       ssl_error = -1;

                if ( msg != null ) {
                        /* Get an error message */
                        msgStr = msg.toString();

                        /* Search a key to get error information */
                        ssl_error = msgStr.indexOf("FjSSLSocket");
                }
                /* Processing for SSL */
                if ( ssl_error != -1 ) {
                        int index1 = msgStr.indexOf("errtype=") +
"errtype=".length();
                        if ( index1 != -1 ) {
                                /* Get error type */
                                String error = msgStr.substring(index1, 
index1 + 2);
                                /* Indicate error type */
                                System.out.println("SSL Error code : " + 
error);
                        }
                }
                System.out.println("Search example failed.");
        }
        catch(Exception e)
        {
                System.out.println(e.getMessage());
                System.out.println(e.getLocalizedMessage());
        }
}

}
```

Appendix A

Manipulating a Repository in a Cluster Environment

This appendix describes how to manipulate a repository in a cluster environment.

Notes

- The cluster environment setup must already be completed.
- A common operation procedure is used for each cluster environment (It is necessary to log on as an administrator).

  To modify a repository environment that has been operated in a cluster environment, use Interstage Management Console (access [System] > [Service] > [Repository] > [Repository Name] > [Settings] window (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository] > [Repository Name] > [Settings] window)). Then complete the procedure described in "Modifying a repository" below.
- In the shared disk path, specify a path that has been registered as a resource.

Windows

- Register a resource using Microsoft Cluster Server (MSCS) after completing the steps described in "Creating a repository."
- A repository operated in the MSCS cluster environment cannot be modified or deleted because the repository cannot be stopped. Modify or delete a repository operated in the MSCS cluster environment after deleting the repository resource registered on MSCS and stopping the repository.

Creating a Repository

This section describes how to create and set up a repository in Smart Repository using standalone mode and replication mode in a cluster environment.

Standalone Mode

This section describes how to create a repository in Smart Repository standalone mode in a cluster environment.

The active and standby nodes are assumed to be Nodes 1 and 2, respectively, in the initial setting of the cluster environment.

To create a repository:

1. Using the connected Interstage Management Console on the active node (Node 1), access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Create a New Repository] tab, make the repository settings in this window, and click [[Show] Detailed Settings].
2. In [Database Storage Directory] and [Access Log Storage Directory] shown in [Detailed Settings], specify the path of a shared disk and click [Create].
3. Windows

   On the active node (Node 1), execute the irepbacksys command to back up the repository information created in step 2 to a directory.

   Example

   ```
   irepbacksys -d X:\Backup\irep\rep001_back -R rep001 –confonly
   ```

   Solaris OE Linux

   On the active node (Node 1), execute the irepbacksys command to back up the repository information created in step 2 to a file.

   Example

   ```
   irepbacksys -f /backup/irep/rep001_back -R rep001 -confonly
   ```

4. Transfer the created backup file to the standby node (Node 2) using ftp or other methods.

5. Windows

   Switch clusters and make Node 2 the active node. On the active node (Node 2), execute the ireprestsys command to restore the repository information created in step 2 from the directory.

   Example

   ```
   ireprestsys -d X:\Backup\irep\rep001_back -R rep001 –confonly
   ```

   Solaris OE Linux

   Switch clusters and make Node 2 the active node. On the active node (Node 2), execute the ireprestsys command to restore the repository information created in step 2 from the file.

Example

```
ireprestsys -f /back/irep/rep001_back.tar.Z -R rep001 –confonly
```

6. Using the connected Interstage Management Console on the active node (Node 2), start the repository.

For details of the irepbacksys and ireprestsys commands, refer to "Backup Commands" in the "Reference Manual (Command Edition)."

Configuring Replication in a Cluster Environment

This section describes how to set up replication so that it can be used in Smart Repository.

In this section, the active and standby nodes are assumed to be Nodes 1 and 2, respectively, in the initial setting of the cluster environment.

Configuring Replication when Only the Master is in a Cluster Environment

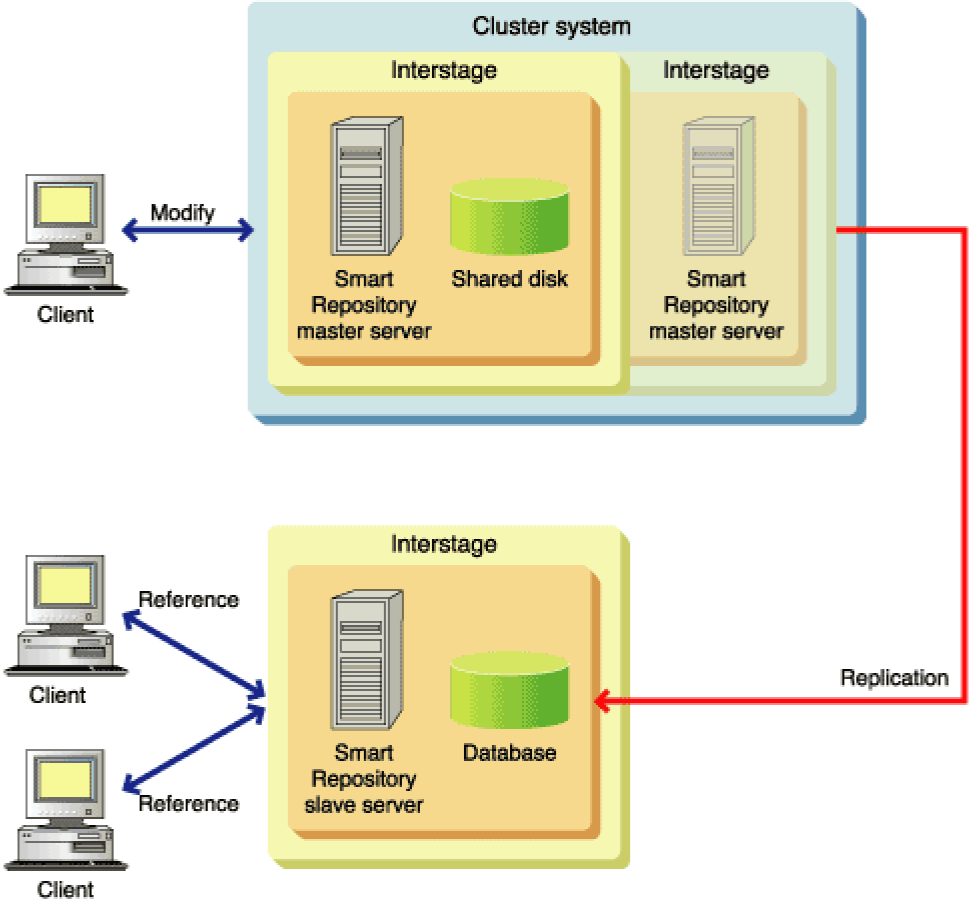


Figure A-1 Interstage Backup/Restore Procedure

Configuration Common to both Master and Slave

1. Create a repository.

   Using the connected Interstage Management Console on both master and slave machines in the replication configuration, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Create a New Repository] tab. Ensure that the same settings are used for both the master and slave for the following items, and then click the [Create] button.

   – [Repository Name]

   – [Public Directory]

   – [Create default tree?]

   – [User password encryption method]

   – [Database Storage Directory]

   To set up replication in a cluster environment, specify the same shared disk path as the database and access log storage directories.

Configuring the Slave

2. Using the connected Interstage Management Console on a machine as the slave, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Repository : View Status], click the repository created in step 1 in this window, and click [[Show] Detailed Settings] in the [Settings] window.

3. In [Replication settings], select "Slave" and, in the resulting [Slave Operation Settings], set the host name of a machine to be the master. In [Master host name], specify the physical host names of the active and standby nodes by delimiting them with a comma as shown below and then click the [Apply] button.

   Example:

   cluster01,cluster02

   Note

   In [Master host name] for [Slave operation settings], only up to two host names can be specified.

4. Using the Interstage Management Console, start the repository.

Configuring the Master

5. Using the connected Interstage Management Console on a machine to be the master, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Repository : View Status], click the repository created in step 1 of this window and then click [[Show] Detailed Settings] in the [Settings] window.

6. In [Replication settings], select "Master." A new [Replication destination host list] window is displayed.

7. Click the [Add] button and in the resulting [Replication Connection Settings], set the items.

8. Using Backup/Restore, duplicate the repository environment to the master's standby node (Node 2).

a) Windows

On the master's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a directory.

Example:

```
irepbacksys -d X:\Backup\irep\rep001_back -R rep001 –confonly
```

Solaris OE Linux

On the master's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a file.

Example:

```
irepbacksys -f /backup/irep/rep001_back -R rep001 –confonly
```

b) Transfer the backed up file to the master's standby node (Node 2) using ftp or another method.

c) Windows

Switch clusters and make Node 2 the active node. On the master's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from the directory.

Example:

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 –confonly
```

Solaris OE Linux

Switch clusters and make Node 2 the active node. On the master's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from the directory.

Example:

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 –confonly
```

9. Using the Interstage Management Console, start the repository on the active node (Node 2).

   For details of the irepbacksys and ireprestsys commands, refer to "Backup Commands" in the "Reference Manual (Command Edition)."

Configuring Replication when only the Slave is in a Cluster Environment

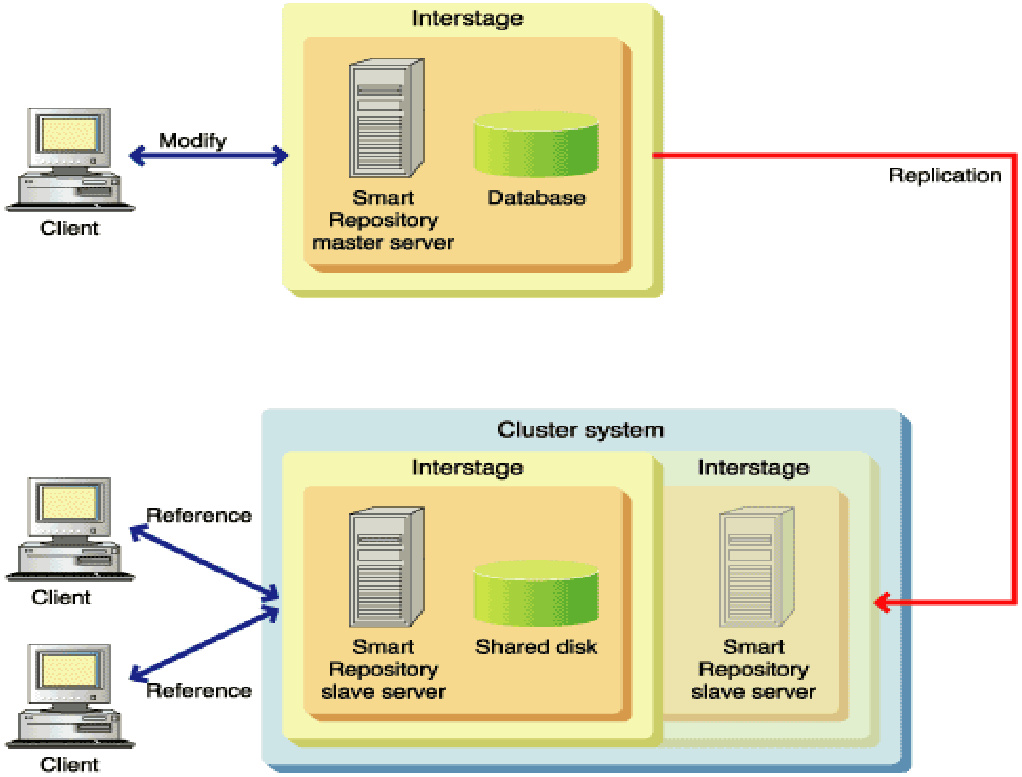


Figure A-2 Configuring Replication when only the slave is in a cluster environment

Configuration Common to both the Master and Slave Machines

1. Create a repository.

   Using the connected Interstage Management Console on both master and slave machines in the replication configuration, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Create a New Repository] tab. Ensure that the same settings are used for both the master and slave for the following items, and then click the [Create] button.

   – [Repository Name]

   – [Public Directory]

   – [Create default tree?]

   – [User password encryption method]

   – [Database Storage Directory]

To set up replication in a cluster environment, specify the same shared disk path as the database and access log storage directories.

Configuration of the Slave

2. Using the connected Interstage Management Console on a machine to be the slave, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Repository : View Status], click the repository created in step 1 in this window and then click [[Show] Detailed Settings] in the [Settings] window.
3. In [Replication settings], select "Slave" and, in the resulting [Slave Operation Settings], set the host name of a machine as the master.

4 Using Backup/Restore, duplicate the repository environment to the slave's standby node (Node 2).

a) Windows

On the slave's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a directory.

Example:

```
irepbacksys -d X:\Backup\irep\rep001_back -R rep001 –confonly
```

Solaris OE Linux

On the slave's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a file.

Example:

```
irepbacksys -f /backup/irep/rep001_back -R rep001 –confonly
```

b) Transfer the created backup file to the slave's standby node (Node 2) using ftp or another method.

c) Windows

Switch clusters and make Node 2 the active node. On the slave's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from the directory.

Example:

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 –confonly
```

Solaris OE Linux

Switch clusters and make Node 2 the active node. On the slave's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from a file.

Example:

```
ireprestsys -f /backup/irep/rep001_back.tar.Z -R rep001 –confonly
```

5. Using the Interstage Management Console, start the repository on the active node (Node 2).

Configuration of the Master

6. Using the connected Interstage Management Console on a machine as the master, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Repository : View Status], click the repository created in step 1 in this window, and click [[Show] Detailed Settings] in the [Settings] window.
7. In [Replication settings], select "Master." A new [Replication destination host list] window will be displayed.
8. Click the [Add] button and, in the resulting [Replication Connection Settings], set the items. In [Host Name], specify the logical host name of the cluster environment and then click the [Apply] button.
9. Using the Interstage Management Console, start the repository.

For details of the irepbacksys and ireprestsys commands, refer to "Backup Commands" in the "Reference Manual (Command Edition)."

Configuring Replication when both the Master and Slave are in a Cluster Environment

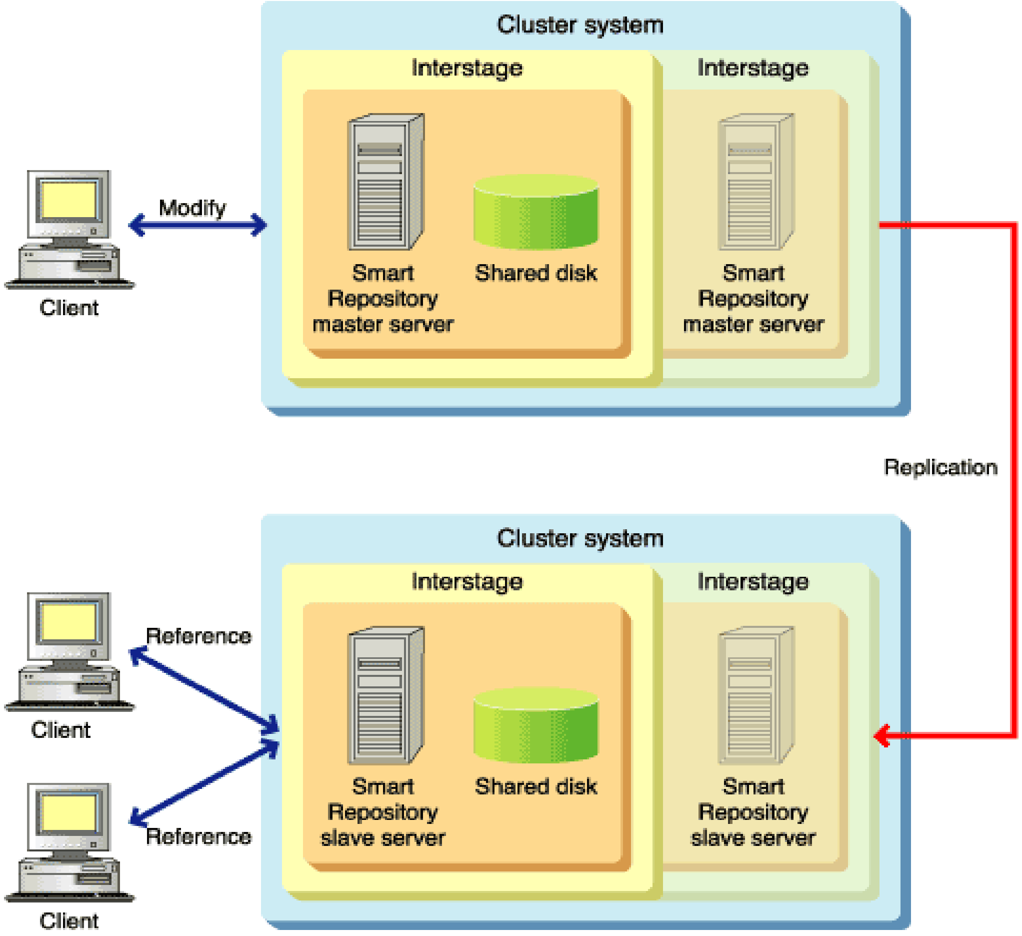


Figure A-3 Configuring Replication when both the master and slave are in a cluster environment

Configuration common to both Master and Slave Machines

1. Create a repository.

   Using the connected Interstage Management Console on both master and slave machines in the replication configuration, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Create a New Repository] tab. Ensure that the same settings are used for both the master and slave for the following items, and then click the [Create] button.

   – [Repository Name]

   – [Public Directory]

   – [Create default tree?]

   – [User password encryption method]

   – [Database Storage Directory]

To set up replication in a cluster environment, specify the same shared disk path as the database and access log storage directories.

Configuration on the slave machine

2. Using the connected Interstage Management Console on a machine as the slave, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Repository : View Status]. Click the repository created in step 1 in this window, and then click [[Show] Detailed Settings] in the [Settings] window.

3. In [Replication settings], select "Slave" and, in the resulting [Slave Operation Settings], set the host name of a machine as the master. In [Master host name], specify the physical host names of the master's active node (node 1) and standby node (node 2) by delimiting them with a comma as shown below and then click the [Apply] button.

   Example:

   ```
   cluster01,cluster02
   ```

   Note

   In [Master host name] of [Slave Operation Settings], a maximum of two host names can be specified.

4. Using Backup/Restore, duplicate the repository environment to the slave's standby node (Node 2).

   a) Windows

   On the slave's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a directory.

   Example:

   ```
   irepbacksys -d X:\Backup\irep\rep001_back -R rep001 –confonly
   ```

   Solaris OE Linux

   On the slave's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a file.

   Example:

   ```
   irepbacksys -f /backup/irep/rep001_back -R rep001 –confonly
   ```

b) Transfer the created backup file to the slave's standby node (Node 2) using ftp or another method.

c) Windows

Switch clusters and make the slave's Node 2 the active node. On the slave's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from the directory.

Example:

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 –confonly
```

Solaris OE Linux

Switch clusters and make the slave's Node 2 the active node. On the slave's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from the file.

Example:

```
ireprestsys -f /tmp/rep001.tar.Z -R rep001 –confonly
```

5. Using the Interstage Management Console, start the repository on the slave's active node (Node 2).

Configuration on the master machine

6. Using the connected Interstage Management Console on a machine as the master, access [System] > [Service] > [Repository] (If on the Admin Server, access [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), then [Repository : View Status], click the repository created in step 1 in this window, and click [[Show] Detailed Settings] in the [Settings] window.
7. In [Replication settings], select "Master." A new [Replication destination host list] window will be displayed.
8. Click the [Add] button and, in the resulting [Replication Connection Settings], set the items. In [Host Name], specify the logical host name of the cluster environment and click the [Apply] button.
9. Using Backup/Restore, duplicate the repository environment to the master's standby node (Node 2).

a) Windows

On the master's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a directory.

Example:

```
irepbacksys -d X:\Backup\irep\rep001_back –R rep001 –confonly
```

Solaris OE Linux

On the master's active node (Node 1), execute the irepbacksys command to back up the repository information created in step 1 to a file.

Example:

```
irepbacksys -f /tmp/rep001 –R rep001 –confonly
```

b) Transfer the created backup file to the master's standby node (Node 2) using ftp or another method.

c) Windows

Switch clusters and make the master's Node 2 the active node. On the master's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from the directory.

Example:

```
ireprestsys -d X:Backup\irep\rep001_back -R rep001 –confonly
```

Solaris OE Linux

Switch clusters and make the master's Node 2 the active node. On the master's active node (Node 2), execute the ireprestsys command to restore the repository information created in step 1 from the directory.

Example:

```
ireprestsys -f /tmp/rep001.tar.Z -R rep001 –confonly
```

10. Using the Interstage Management Console, start the repository on the master's active node (Node 2).

    For details of the irepbacksys and ireprestsys commands, refer to "Backup Commands" in the "Reference Manual (Command Edition)."

Modifying a Repository

Active and standby nodes are assumed to be Nodes 1 and 2 respectively, in the initial setting of the cluster environment.

1. Windows If modifying a repository operated in the MSCS cluster environment, it is necessary to set offline the general service resources for the target repository registered to MSCS.
2. Using the Interstage Management Console on the active node (Node 1), stop, modify, and then restart the repository.
3. Switch clusters and make Node 2 the active node. Then, perform the same operation as step 1.
4. Windows If a repository operated in the MSCS cluster environment has been modified, set online the resources that have been set offline in step 1.

Deleting a Repository

Active and standby nodes are assumed to be Nodes 1 and 2 respectively, in the initial setting of the cluster environment.

1. Windows If deleting a repository operated in the MSCS cluster environment, delete the general service resources of the target repository registered to MSCS.
2. Using the Interstage Management Console on the active node (Node 1), stop and delete the repository.
3. Switch clusters and make Node 2 the active node. Then, perform the same operation as step 1.

Appendix B

Error Codes

This appendix explains the error codes output by Smart Repository.

An LDAP error code notifies an error in LDAP.

An SSL error code notifies an error detected in the SSL library, if SSL is being used.

LDAP Error Codes

This section explains the meanings of the LDAP error codes and the required action.

Error code symbol	Message	Decimal	Hexadecimal
LDAP_SUCCESS	Success	0	0x00
LDAP_OPERATIONS_ERROR	Operations error	1	0x01
LDAP_PROTOCOL_ERROR	Protocol error	2	0x02
LDAP_TIMELIMIT_EXCEEDED	Timelimit exceeded	3	0x03
LDAP_SIZELIMIT_EXCEEDED	Sizelimit exceeded	4	0x04
LDAP_COMPARE_FALSE	Compare false	5	0x05
LDAP_COMPARE_TRUE	Compare true	6	0x06
LDAP_STRONG_AUTH_NOT_SUPPORTED	Strong authentication not supported	7	0x07
LDAP_STRONG_AUTH_REQUIRED	Strong authentication required	8	0x08
LDAP_PARTIAL_RESULTS	Partial results and referral received	9	0x09
LDAP_REFERRAL	Referral	10	0x0a
LDAP_ADMINLIMIT_EXCEEDED	Admin limit exceeded	11	0x0b
LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Unavailable critical extension	12	0x0c
LDAP_CONFIDENTIALITY_REQUIRED	Confidentiality required	13	0x0d
LDAP_SASL_BIND_IN_PROGRESS	SASL bind in progress	14	0x0e
LDAP_NO_SUCH_ATTRIBUTE	No such attribute	16	0x10
LDAP_UNDEFINED_TYPE	Undefined attribute type	17	0x11
LDAP_INAPPROPRIATE_MATCHING	Inappropriate matching	18	0x12
LDAP_CONSTRAINT_VIOLATION	Constraint violation	19	0x13
LDAP_TYPE_OR_VALUE_EXISTS	Type or value exists	20	0x14
LDAP_INVALID_SYNTAX	Invalid syntax	21	0x15
LDAP_NO_SUCH_OBJECT	No such object	32	0x20
LDAP_ALIAS_PROBLEM	Alias problem	33	0x21
LDAP_INVALID_DN_SYNTAX	Invalid DN syntax	34	0x22
LDAP_IS_LEAF	Object is a leaf	35	0x23

LDAP_ALIAS_DEREF_PROBLEM	Alias dereferencing problem	36	0x24
LDAP_INAPPROPRIATE_AUTH	Inappropriate authentication	48	0x30
LDAP_INVALID_CREDENTIALS	Invalid credentials	49	0x31
LDAP_INSUFFICIENT_ACCESS	Insufficient access	50	0x32
LDAP_BUSY	DSA is busy	51	0x33
LDAP_UNAVAILABLE	DSA is unavailable	52	0x34
LDAP_UNWILLING_TO_PERFORM	DSA is unwilling to perform	53	0x35
LDAP_LOOP_DETECT	Loop detected	54	0x36
LDAP_NAMING_VIOLATION	Naming violation	64	0x40
LDAP_OBJECT_CLASS_VIOLATION	Object class violation	65	0x41
LDAP_NOT_ALLOWED_ON_NONLEAF	Operation not allowed on nonleaf	66	0x42
LDAP_NOT_ALLOWED_ON_RDN	Operation not allowed on RDN	67	0x43
LDAP_ALREADY_EXISTS	Already exists	68	0x44
LDAP_NO_OBJECT_CLASS_MODS	Cannot modify object class	69	0x45
LDAP_RESULTS_TOO_LARGE	Results too large	70	0x46
LDAP_AFFECTS_MULTIPLE_DSAS	Affects multiple DSAs	71	0x47
LDAP_OTHER	Unknown error	80	0x50
LDAP_SERVER_DOWN	Can't contact LDAP server	81	0x51
LDAP_LOCAL_ERROR	Local error	82	0x52
LDAP_ENCODING_ERROR	Encoding error	83	0x53
LDAP_DECODING_ERROR	Decoding error	84	0x54
LDAP_TIMEOUT	Timed out	85	0x55
LDAP_AUTH_UNKNOWN	Unknown authentication method	86	0x56
LDAP_FILTER_ERROR	Bad search filter	87	0x57
LDAP_USER_CANCELLED	User cancelled operation	88	0x58
LDAP_PARAM_ERROR	Bad parameter to an ldap routine	89	0x59
LDAP_NO_MEMORY	Out of memory	90	0x5a
LDAP_CONNECT_ERROR	Can't connect to the LDAP server	91	0x5b
LDAP_NOT_SUPPORTED	Not supported	92	0x5c
LDAP_CONTROL_NOT_FOUND	Control not found	93	0x5d
LDAP_NO_RESULTS_RETURNED	No results returned	94	0x5e

LDAP_MORE_RESULTS_TO_ RETURN	More result to return	95	0x5f
LDAP_CLIENT_LOOP	Client loop	96	0x60
LDAP_REFERRAL_LIMIT_ EXCEEDED	Referral limit exceeded	97	0x61

LDAP_SUCCESS 0 (0x00)

Success

Explanation

Processing completed normally.

LDAP_OPERATIONS_ERROR 1 (0x01)

Operations error

Explanation

An object class may have been specified incorrectly.

User action

Specify a correct object class. For details of the object classes, see Appendix C - ‘List of Object Classes’ or Appendix D - ‘List of Attributes’.

LDAP_PROTOCOL_ERROR 2 (0x02)

Protocol error

Explanation

An operation request violated the LDAP protocol.

User Action

If this error occurs after creating an API and executing it, correct the API by referring to the Smart Repository samples and then re-execute.

This error may also occur if an extended function (or a function that cannot be used in Smart Repository) is used.

Refer to the following manuals to check whether any functions that cannot be used in Smart Repository were used:

'Restrictions on Smart Repository' in Product Notes

'Notes on Smart Repository' in Product Notes

LDAP_TIMELIMIT_EXCEEDED 3 (0x03)

Timelimit exceeded

Explanation

The search timeout was exceeded while searching for entries.

User Action

Increase the specified search time limit as a client search option.

If there is no improvement, change the connection DN to an administrator DN of the target repository. Alternatively, use the Interstage Management Console to increase the value of 'Search Timeout' from the Settings window of the target repository.

LDAP_SIZELIMIT_EXCEEDED 4 (0x04)

Sizelimit exceeded

Explanation

The maximum number of searchable entries was exceeded.

User Action

Increase the size limit as a client search option.

Use the Interstage Management Console to increase the value of 'Maximum number of searchable entries' from the Settings window of the target repository.

LDAP_COMPARE_FALSE 5 (0x05)

Compare false

Explanation

In a comparison operation, there was no match with the specified attribute value.

LDAP_COMPARE_TRUE 6 (0x06)

Compare true

Explanation

In a comparison operation, there was a match with the specified attribute value.

LDAP_STRONG_AUTH_NOT_SUPPORTED 7 (0x07)

Strong authentication not supported

Explanation

Smart Repository does not support the specified authentication method.

User Action

In Smart Repository, simple authentication or client authentication using SSL can be used. To use client authentication using SSL, see ‘Setting up an Environment for SSL Communication’ – ‘Setup of an SSL communication environment (between client and server)’ in Chapter Two – Environment Setup.

LDAP_STRONG_AUTH_REQUIRED 8 (0x08)

Explanation

Strong authentication required

Explanation

Authentication is required for the requested operation, or an authentication method not supported by Smart Repository was used.

- **Examples of error occurrence**

  An entry operation is performed by anonymous authentication.

  LDIF

```
dn:o=SR,o=fujitsu,dc=com
changetype:add
objectclass:top
objectclass:organization
o:SR
```

Message

```
adding new entry o=SR,o=fujitsu,dc=com
ldap_result(add) : Strong authentication required
errmsg : modifications require authentication
```

User Action

No entry can be modified or deleted when anonymous authentication is used. Re-execute after specifying the DN to be bound and the password.

Simple authentication or client authentication using SSL can be used. To use client authentication using SSL, see 'Setting up an Environment for SSL Communication' –‘Setup of an SSL communication environment (between client and server)’ in Chapter Two – Environment Setup.

LDAP_PARTIAL_RESULTS 9 (0x09)

Partial results and referral received

Explanation

Part of the processing results has been received.

User Action

This message may be output when a search within a repository with which entry referrals are registered is performed. Since the referral function cannot be used in Smart Repository, the directory server of another product may be connected. Check whether the connection destination is correct and then specify the correct server to Smart Repository.

LDAP_REFERRAL 10 (0x0a)

Referral

Explanation

A repository where referrals are registered was referenced.

User Action

Smart Repository never returns this code.

Since the referral function cannot be used in Smart Repository, the directory server of another product may be connected. Check whether the connection destination is correct and then specify the correct server to Smart Repository.

LDAP_ADMINLIMIT_EXCEEDED 11 (0x0b)

Admin limit exceeded

Explanation

A Smart Repository server limit has been exceeded.

User Action

Check whether a target repository message exists by referring to the system log of the repository server. If a message exists, take the action indicated by that message. If there is no message, use the Interstage Management Console to confirm that all settings in the Settings window of the target repository are correct, and correct any incorrect settings.

If this does not resolve the error, use the iscollectinfo command to collect diagnostic information and then contact your service engineer.

LDAP_UNAVAILABLE_CRITICAL_EXTENSION 12 (0x0c)

Unavailable critical extension

Explanation

The specified function cannot be used in Smart Repository.

User Action

The following causes can be assumed:

- A function that cannot be used in Smart Repository was used.

  Refer to the following manuals to check whether any functions that cannot be used in Smart Repository were used:

  'Limitations on Smart Repository' in Notes

  'Notes on Smart Repository' in Notes

Windows

- After creating a repository, the environment definition of the repository was modified manually.

  Restore the environment definition to its state before modification and then restart the repository for re-execution.

LDAP_CONFIDENTIALITY_REQUIRED 13 (0x0d)

mConfidentiality required

Explanation

There is an error in a specified attribute.

User Action

Check for errors in the specified attributes.

For attribute details, see Appendix D - ‘List of Attributes’.

It is also possible that a function that cannot be used in Smart Repository was used.

Refer to the following manuals to check whether any functions that cannot be used in Smart Repository were used:

'Limitations on Smart Repository' in Product Notes

'Notes on Smart Repository' in Product Notes

LDAP_SASL_BIND_IN_PROGRESS 14 (0x0e)

SASL bind in progress

Explanation

There is an error in a specified attribute.

User Action

Check for errors in the specified attributes.

For attribute details, see Appendix D - ‘List of Attributes’.

It is also possible that a function that cannot be used in Smart Repository was used.

Refer to the following manuals to check whether any functions that cannot be used in Smart Repository were used:

'Limitations on Smart Repository' in Product Notes

'Notes on Smart Repository' in Product Notes

LDAP_NO_SUCH_ATTRIBUTE 16 (0x10)

No such attribute

Explanation

There is no applicable attribute.

- **Examples of error occurrence**

  An object that is not defined in the object class was specified.

User Action

Check whether the specified attribute name is correct. If there are any errors, correct the attribute name and then re-execute. If no error is found, the attribute name may have been deleted, in which case re-execution is not required.

If this message is still output even if the attribute exists, use the iscollectinfo command to collect diagnostic information and then contact your service engineer.

For details of object classes and attributes, see Appendix C - ‘List of Object Classes’ and Appendix D - ‘List of Attributes’ respectively.

LDAP_UNDEFINED_TYPE 17 (0x11)

Undefined attribute type

Explanation

An attribute name not defined in the schema was specified.

- **Examples of error occurrence**

  If an attribute (aaa) that is not defined in the schema is added by LDIF.

  LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:add
objectclass:top
objectclass:person
objectclass:organizationalPerson
cn:User001
sn:Fujitsu
aaa:User001
```

  Message

```
adding new entry cn=User001,o=fujitsu,dc=com
ldap_result(add) : Undefined attribute type
errmsg : aaa: attribute type undefined
```

User Action

Check the attribute name for errors. If an error is found, correct it and then re-execute. For attribute name details, see Appendix D - 'List of Attributes'.

For details of object classes and attributes, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

LDAP_INAPPROPRIATE_MATCHING 18 (0x12)

Inappropriate matching

Explanation

An inappropriate combination was used.

User Action

Check the specified attributes.

LDAP_CONSTRAINT_VIOLATION 19 (0x13)

Constraint violation

Explanation

A restriction was violated.

- **Examples of error occurrence**

  An attribute (ssoPortNumber) whose single flag is true is specified multiple times.

  LDIF

```
dn:dc=my-domain,o=fujitsu,dc=com
objectClass:top
objectClass:ssoSite
objectClass:domain
dc:my-domain
ssoPortNumber:12345678
ssoPortNumber:87654321
```

  Message

```
adding new entry dc=my-domain,o=fujitsu,dc=com
ldap_result(add) : Constraint violation
errmsg : ssoPortNumber: multiple value provided
```

User Action

Check whether the operation on the specified attribute is correct. For details of the attributes, see Appendix D - ‘List of Attributes’.

If the operation on the specified attribute is correct, use the iscollectinfo command to collect diagnostic information and then contact your service engineer.

LDAP_TYPE_OR_VALUE_EXISTS 20 (0x14)

Type or value exists

Explanation

The specified attribute already exists.

- **Examples of error occurrence**

  If an attribute (sn:Fujitsu) with the same attribute value is added multiple times.

LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:add
objectclass:top
objectclass:person
cn:User001
sn:Fujitsu
sn:Fujitsu
```

Message

```
adding new entry cn=User001,o=fujitsu,dc=com
ldap_result(add) : Type or value exists
errmsg : sn: value #0 provided more than once
```

User Action

Check whether the attribute name is specified correctly when adding an attribute. If the specified attribute name is correct, the name cannot be added because an attribute of the same name already exists. Check whether the attribute value of the attribute name is correct. If the value is different from the attribute value to be added, modify the attribute value.

LDAP_INVALID_SYNTAX 21 (0x15)

Invalid syntax

Explanation

The content of the specified attribute value contradicts the attribute syntax.

- **Examples of error occurrence**

  An invalid attribute (x121Address:aaa) is registered with the attribute syntax.

LDIF

```
dn:o=SR,o=fujitsu,dc=com
changetype:add
objectclass:top
objectclass:organization
o:SR
x121Address:aaa
```

Message

```
adding new entry o=SR,o=fujitsu,dc=com
ldap_result(add) : Invalid syntax
errmsg : x121Address: value #0 invalid per syntax
```

User Action

Fix the problem by referring to 'List of Attributes' and then re-execute.

LDAP_NO_SUCH_OBJECT 32 (0x20)

No such object

Explanation

There is no applicable entry.

- **Examples of error occurrence**

  An entry (cn=User001,o=fujitsu,dc=com) that does not exist in the repository is modified.

LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:modify
add:givenName
givenName:User001
```

Message

```
modifying entry cn=User001,o=fujitsu,dc=com
ldap_result(modify) : No such object
errmsg : LDAP_NO_SUCH_OBJECT: DN: >cn=User001,o=fujitsu,dc=com<
```

User Action

Check for errors in the specified object name (entry), and check whether an upper tree exists. To add an entry when there is no upper tree, first create an upper tree and then re-execute.

LDAP_ALIAS_PROBLEM 33 (0x21)

Alias problem

Explanation

There is an error in the alias.

User Action

Check the specified alias. If it contains an error, correct the alias and then re-execute.

For details of object classes and attributes, see Appendix C - ‘List of Object Classes’ and Appendix D - ‘List of Attributes’.

LDAP_INVALID_DN_SYNTAX 34 (0x22)

Invalid DN syntax

Explanation

There is an error in the DN (identification name) format.

- **Example 1 of error occurrence**

  If an attempt is made to modify the identification name by specifying an undefined attribute name (a).

  Entry state within the repository (LDIF)

```
Dn:cn=User001,o=fujitsu,dc=com
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetOrgPerson
cn:User001
sn:Fujitsu
```

LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:modrdn
newrdn:a=User001
deleteoldrdn:1
```

Message

```
ldap_result(rename) : Invalid DN syntax
errmsg : invalid new RDN
```

- **Example 2 of error occurrence**

  If an attempt is made to modify the identification name by incorrectly specifying newrdn

  Entry state within the repository (LDIF)

```
dn:cn=User001,o=fujitsu,dc=com
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetOrgPerson
cn:User001
sn:Fujitsu
```

LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:modrdn
newrdn:User001
deleteoldrdn:1
```

newrdn must be correctly specified as newrdn:**cn=User001**

Message

```
ldap_result(rename) : Invalid DN syntax
errmsg : invalid new RDN
```

User Action

Check for errors in the specified DN. If an error is found, correct it and then re-execute. For details of the DN, see Chapter Three - ‘Entry Management’.

LDAP_IS_LEAF 35 (0x23)

Object is a leaf

Explanation

The requested processing cannot be performed on a leaf entry.

User Action

This message may be displayed if an attempt is made to move the specified tree to the same location or to a location under a specified tree. Re-execute after specifying the correct destination.

LDAP_ALIAS_DEREF_PROBLEM 36 (0x24)

Alias dereferencing problem

Explanation

No alias can be referenced.

User Action

Check for errors in the specified alias. If an error is found, correct it and then re-execute. For details of the attributes, see Appendix D - 'List of Attributes'.

LDAP_INAPPROPRIATE_AUTH 48(0x30)

Inappropriate authentication

Explanation

Authentication was rejected. This message is output if the specified DN has no userPassword attribute.

User Action

It is not possible to access the specified DN. Use the administrator DN for connection and then add the userPassword attribute to the specified DN.

LDAP_INVALID_CREDENTIALS 49 (0x31)

Invalid credentials

Explanation

Authentication failed because there is an error in the specified DN or password.

User Action

Check whether the specified DN is correct. If the DN is correct, there is an error in the password. Specify the correct password and then re-execute.

Note that there is a function in the addition of a replication host on the Interstage Management Console to automatically add a public directory to DN. For example, if cn for connection is correct with cn=manager, but the connected public directory is different, DN is determined to be incorrect.

The following examples show some other possible errors:

- The comma or the period of DN is specified incorrectly.
- Upper-case and lower-case alphabetical characters are distinguished, so if they are not specified correctly in the password, the password will be determined incorrect.

Windows

- An attempt may have been made to connect to DN with a password encrypted by an unsupported user password encryption method. Check whether this is the case.

  For details of user password encryption methods, see 'Major Functions of Smart Repository' - 'Automatic Encoding' - 'User password encryption method' in Chapter 1 - 'Overview'.

LDAP_INSUFFICIENT_ACCESS 50 (0x32)

Insufficient access

Explanation

There is no permission granted for the specified request.

User Action

Check whether the specification of the connected DN (such as a tree) is correct. If correct, the connected DN has no permission for the operation. Perform only permitted operations. For example, if connected as a general user user01, modification operations of user01 can be performed, but if a modification operation of a User02 entry is performed, this message is displayed.

LDAP_BUSY 51 (0x33)

DSA is busy

Explanation

There are too many requests to the repository to be accepted. Alternatively, an unrecoverable error may have occurred in Fujitsu Enabler.

User Action

The following causes can be assumed:

- If the repository server load is heavy

  Re-execute after waiting for a while.

- If an attempt was made to add or modify an inappropriate entry that contains an extremely large number of attributes (for example, more than 1000 attributes)

  Check whether the number of attributes of the entry to be added or modified is extremely large. If this is the case, reduce the number of attributes and then restart the relevant repository from the Interstage Management Console for re-execution.

  The number of attributes that can be added or modified for each entry depends on the performance of the server machine and the data size of the attribute values set to each attribute of an entry. Repeat re-execution, reducing the number of attributes per entry, until this phenomenon does not occur.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

LDAP_UNAVAILABLE 52 (0x34)

DSA is unavailable

Explanation

The repository service is currently not available.

User Action

Use the Interstage Management Console to check whether the repository is active.

- If the repository is stopped, activate it.
- If the repository is active, stop it and then restart it.
- If the repository is in an abnormal state, stop it and then activate it.

Solaris OE Linux

Use the ps command to check whether the omsservd process is active. If the omsservd process is inactive, activate it by using the enablerstart command.

After executing the enablerstart command, restart the repository to perform the entry operation again.

For details on how to use the enablerstart command, see 'Smart Repository Operation Commands' in the Reference Manual (Command Edition).

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

LDAP_UNWILLING_TO_PERFORM 53 (0x35)

DSA is unwilling to perform

Explanation

The repository rejected a request.

- **Example 1 of error occurrence**

  An attribute whose attribute value (binary) is 200 KB or more is registered.

  LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:add
objectclass:inetOrgPerson
cn:User001
sn:Fujitsu
jpegphoto:< file:///data/Fujitsu/User001.jpg
```

Message

```
adding new entry cn=User001,o=fujitsu,dc=com
ldap_result(add) : DSA is unwilling to perform
matched: The maximum length of a long binary attribute value is limited to
200000 bytes, attribute 'jpegPhoto' with 758781 bytes is not supported.
```

- **Examples 2 of error occurrence**

  An attribute whose attribute value contains 1999 bytes or more is registered.

LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:add
objectclass:inetOrgPerson
cn:User001
sn:Fujitsu
givenName:@@ ・・・ @@
```

Message

```
adding new entry cn=User001,o=fujitsu,dc=com
ldap_result(add) : DSA is unwilling to perform
errmsg : LDAP_UNWILLING_TO_PERFORM: The maximum
length of an attribute value is restricted to 1998 characters,
 but is 10000 .
```

User Action

The following causes can be assumed:

- If accessed using a DN that does not contain a public directory, check whether the specified DN is correct.
- If an entry that does not contain a public directory is accessed, check whether the specified entry is correct.
- If a public directory (top entry) has been deleted or an identification name has been modified, check whether the specified entry is correct. Deletion of a top entry or modification of an identification name is not permitted.
- If an attempt is made to register an entry with the same name as the administrator DN, or to modify an entry identification name to the same identification name as the administrator DN, check whether the specified entry is correct. Registration of an entry with the same identification name as the administrator DN or modification of an identification name to the same identification name as the administrator DN is not permitted.

The above actions are not permitted.

- In cases other than the above, the error occurs when adding a replication host using the Interstage Management Console
  - If the repository name of a slave is different, specify the same repository name for both the master and slave repositories.
  - If a host name that is different from the master host name is set for a slave, the connection destination may be incorrect or the setting for the slave may be incorrect. Implement the correct setting for the slave and then re-execute. If the setting is correct, check for errors in the network settings (IP address acquisition, host file description, DNS server/DHCP server specifications, DNS server/DHCP server settings, etc.) by contacting and checking with the network administrator. Examine the network environment, and re-execute after setting the network again.
  - If performed on a non-slave repository (started in standalone operation), re-execute after switching the repository in standalone operation to a repository in slave operation.
  - The master DN for the connection may not fit in with the slave administrator DN. Specify the master DN for the connection so that it fits in with the slave administrator DN and re-execute.
  - The master Password for the connection may not fit in with the slave administrator DN password. Specify the master Password for the connection so that it fits in with the slave administrator DN password and re-execute.
- If a login operation was performed without specifying the DN password, re-execute by specifying the correct password.
- This message may also be displayed if 1999 bytes or more were specified for DN or a binary attribute of 200 KB or more was specified.
- If a modification request to a slave has been performed, perform the modification request to the master repository.
- If no search base was specified for a search, re-execute by specifying the base parameter.
- Check whether any functions that cannot be used in Smart Repository were used by referring to the following manuals:

  'Restrictions on Smart Repository' in Product Notes

  'Notes on Smart Repository' in Product Notes

LDAP_LOOP_DETECT 54 (0x36)

Loop detected

Explanation

A loop was detected during referral processing.

User Action

Smart Repository never returns this code. The directory server of another product may be connected. Check whether the connection destination is correct and then specify the correct server to Smart Repository.

LDAP_NAMING_VIOLATION 64 (0x40)

Naming violation

Explanation

If the specified attribute is RDN (relative identification name), it cannot be deleted or modified.

This message is also output if the RDN value specified in the DN is different from the attribute value specified when adding an entry.

Alternatively, a request that could damage the directory information tree may have been received.

Example 1 of error occurrence

If an attempt is made to delete an attribute (cn) related to RDN

LDIF

```
dn:cn=User002,o=fujitsu,dc=com
changetype:modify
delete:cn
```

Message

```
modifying entry cn=User002,o=fujitsu,dc=com
ldap_result(modify) : Naming violation
errmsg : LDAP_NAMING_VIOLATION: It is not allowed to delete an attribute
which is part of the RDN
```

- **Example 2 of error occurrence**

If the RDN specified in DN and that specified in the attribute value are different (cn)

LDIF

```
dn:cn=aaa,o=fujitsu,c=jp
objectclass:top
objectclass:person
objectclass:organizationalPerson
cn:bbb
```

Message

```
adding new entry cn=aaa,o=fujitsu,c=jp
ldap_result(add) : Naming violation
errmsg : value of naming attribute 'cn' is not present in entry
```

User Action

For details of the attributes, see Appendix D - 'List of Attributes'.

LDAP_OBJECT_CLASS_VIOLATION 65 (0x41)

Object class violation

Explanation

There is an error in the specified object class. Alternatively, a required attribute is not specified in the object class or an attribute that cannot be used is specified.

- **Example 1 of error occurrence**

  An attempt is made to add an attribute (sn) that is not defined in the schema as an attribute of the specified object class (organization)

  LDIF

```
dn: o=SR,o=fujitsu,dc=com
changetype:add
objectClass: top
objectClass: organization
o: SR
sn:Fujitsu
```

  Message

```
adding new entry o=SR,o=fujitsu,dc=com
ldap_result(add) : Object class violation
errmsg : attribute 'sn' not allowed
```

- **Example 2 of error occurrence**

  If an attempt is made to add an entry by simultaneously specifying object classes (person and organization) that have no inheritance relationship.

  LDIF

```
dn:cn=aaa,o=fujitsu,dc=com
objectclass:top
objectclass:person
objectclass:organization
cn:aaa
sn:aaaa
```

Message

```
adding new entry cn=aaa,o=fujitsu,dc=com
ldap_result(add) : Object class violation
errmsg : invalid structural object class chain (person/organization)
```

User Action

The following causes can be assumed:

- An object class that is not supported by Smart Repository is specified.
- Object classes that have no inheritance relationship are specified simultaneously.
- A required attribute of an object class is not specified.
- An attribute that cannot be specified in an object class is specified.
- The object class or attribute specification method in the LDIF file is incorrect.

Check whether the object classes and attributes are specified correctly and then re-execute.

For details of the object classes and attributes, see Appendix C - 'List of Object Classes' and Appendix D - 'List of Attributes' respectively.

For information on how to specify an LDIF file, see 'Using the LDIF file' in Chapter Three – Entry Management.

This message may also be output if a function that cannot be used in Smart Repository is used.

Check whether any functions that cannot be used in Smart Repository were used by referring to the following manuals:

'Limitations on Smart Repository' in Notes

'Notes on Smart Repository' in Notes

LDAP_NOT_ALLOWED_ON_NONLEAF 66 (0x42)

Operation not allowed on nonleaf

Explanation

The requested processing can only be performed on leaf entries. Deletion or DN modification (identification name renaming) of an entry with a subordinate entry cannot be performed in one operation.

User Action

Perform deletion or DN modification of entries one by one from a leaf (lowest) entry.

LDAP_NOT_ALLOWED_ON_RDN 67 (0x43)

Operation not allowed on RDN

Explanation

The requested processing cannot be performed on a relative identification name (RDN).

LDAP_ALREADY_EXISTS 68 (0x44)

Already exists

Explanation

There is already an entry with the same name as that of the entry to be added.

- **Example 1 of error occurrence**

  An attempt is made to add an entry that already exists.

  LDIF

```
dn:cn=User001,o=fujitsu,dc=com
objectclass:top
objectclass:person
cn:User001
sn:Fujitsu
```

Message

```
adding new entry cn=User001,o=fujitsu,dc=com
ldap_result(add) : Already exists
errmsg : LDAP_ALREADY_EXISTS: Rdn already member of the current parent node
```

User Action

Check for errors in the specified entry. If no error is found, refer to the entry attributes and make any required corrections.

LDAP_NO_OBJECT_CLASS_MODS 69 (0x45)

Cannot modify object class

Explanation

The specified object class is a structure type class that required attributes depend on, so it is not possible to delete or modify its values.

- **Example of error occurrence**

  If an attempt is made to delete the object class attribute (inetOrgPerson) that determines the entry type

  Entry state within the repository (LDIF)

  Inheritance relationship: top < person < organizationalPerson < inetOrgPerson

```
dn:cn=User001,o=fujitsu,dc=com
changetype:add
objectclass:top
objectclass:person
objectclass:organizationalPerson
objectclass:inetOrgPerson
cn:User001
sn:Fujitsu
```

LDIF

```
dn:cn=User001,o=fujitsu,dc=com
changetype:modify
delete:objectclass
objectclass:inetOrgPerson
```

Message

```
ldap_result(modify) : Cannot modify object class
errmsg : LDAP_NO_OBJECT_CLASS_MODS: Cannot remove structural objectclass:
>inetOrgPerson<
```

LDAP_RESULTS_TOO_LARGE 70 (0x46)

Results too large

Explanation

The number of processing result entries exceeds the maximum number of searchable entries.

User Action

Use the Interstage Management Console to increase the value of 'Maximum number of searchable entries' from the Settings window of the target repository.

LDAP_AFFECTS_MULTIPLE_DSAS 71 (0x47)

Affects multiple DSAs

Explanation

The specified function cannot be used in Smart Repository.

User Action

This error may occur if a function that cannot be used in Smart Repository is used.

Check whether any functions that cannot be used in Smart Repository were used by referring to the following manuals:

'Limitations on Smart Repository' in Product Notes

'Notes on Smart Repository' in Product Notes

LDAP_OTHER 80 (0x50)

Unknown error

Explanation

An error that does not have an LDAP error code was detected.

User Action

- Communication with the repository is not possible. Check for errors in the host name and port number of the connection destination.
- Check whether the repository is active by using the Interstage Management Console.
  - If the repository is stopped, activate the repository.
  - If the repository is active, stop it and then restart it.
  - If the repository is in an abnormal state, stop it and then activate it.

- This error may occur if a processing request that exceeds the system scale supported by Smart Repository is made or a function that cannot be used in Smart Repository is used.

  Use the following manuals to check whether the supported system scale was exceeded or a function that cannot be used in Smart Repository was used.

  – 'Restrictions on Smart Repository' in Product Notes

  – 'Notes on Smart Repository' in Product Notes

Solaris OE Linux

- Use the ps command to check whether the omsservd process is active. If the omsservd process is inactive, activate it using the enablerstart command. After executing the enablerstart command, restart the repository to perform the entry operation again.

  For details on how to use the enablerstart command, see 'Smart Repository Operation Commands' in the Reference Manual (Command Edition).

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

LDAP_SERVER_DOWN 81 (0x51)

Can't contact LDAP server

Explanation

Communication with the repository is not possible.

User Action

- It is not possible to communicate with the repository. Check for errors in the host name and port number of the connection destination.
- Contact the network administrator to check for errors in the network environment settings (for example, host file setting, DNS server/DHCP server specifications, DNS server/DHCP server settings, etc.). If any errors are found, correct the network environment and then reset it.
- There is insufficient physical memory for Smart Repository operation. End any unnecessary programs and secure sufficient memory for Smart Repository. If Fujitsu Enabler and all repository operations are stopped, and there is less physical memory capacity available than that required by Smart Repository, the physical memory capacity is insufficient. Refer to 'Memory Requirements' in the Tuning Guide for details on the memory capacity required by Smart Repository. Extend the memory if it is still insufficient after ending unnecessary programs.
- If the repository is active, check whether a timeout has occurred by referring to the access log. If TIMEOUT is recorded in the access log, a timeout has occurred. For information on the access log, see 'Logs' in Chapter 4 - 'Operation and Maintenance'.

  Use the Interstage Management Console to check whether the value of 'Connection Idle Timeout' is too short from the environment settings window of the target repository.

  Other possible causes of timeout include network congestion (where normal communication cannot be conducted due to an increased communication volume); heavy load on the machine on which the repository is active; and heavy load on the machine on which applications are operating.

  If Smart Repository is overloaded, distribute the load by using the replication mode. If the load on the client side is heavy, lighten the load.

  - For user applications, retry can avoid this error.

  If SSL is used for communication with the repository server (and the number of clients is large and the frequency of access to Smart Repository is high) the above actions may not result in any improvement. In this case, consider lightening the server load by, for example, using the SSL accelerator.

- Use the Interstage Management Console to check whether the repository is active.
  - If the repository is stopped, activate the repository.
  - If the repository is active, stop it and then restart it.
  - If the repository is in an abnormal state, stop it and then activate it.

Solaris OE Linux

- The file descriptor (fd) that can be used by client applications may be insufficient. Use ulimit(1) or setrlimit(2) to increase the available file descriptor and then re-execute.
- Use the ps command to check whether the omsservd process is active. If the omsservd process is inactive, activate it using the enablerstart command. After executing the enablerstart command, restart the repository to perform the entry operation again.

  For details on how to use the enablerstart command, see 'Smart Repository Operation Commands' in the Reference Manual (Command Edition).

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

LDAP_LOCAL_ERROR 82 (0x52)

Local error

Explanation

There is a client program error.

User Action

This message may be output when using a protocol extension.

Check whether any functions that cannot be used in Smart Repository were used by referring to the following manuals:

'Limitations on Smart Repository' in Notes

'Notes on Smart Repository' in Notes

If LDIF is used, re-execute from the entry in which an error occurred.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

LDAP_ENCODING_ERROR 83 (0x53)

Encoding error

Explanation

An error was detected while encoding the sent data.

User Action

This error may occur with a protocol extension memory shortage. Terminate unnecessary programs to secure the required memory space and then re-execute.

Windows

If there is no improvement after terminating unnecessary programs, increase the memory or extend the virtual memory.

Solaris OE Linux

If there is no improvement after terminating unnecessary programs, increase the memory or extend the swap area.

For the amount of memory space required for Smart Repository operation, see 'Memory Requirements' in the Tuning Guide.

Linux Windows Solaris OE

If SDK has been used, the parameter of API is wrong. Correct the parameter.

LDAP_DECODING_ERROR 84 (0x54)

Decoding error

Explanation

An error was detected while decoding the received data.

User Action

This error may occur if memory is exhausted using, for example, protocol extensions. Terminate unnecessary programs to secure the required memory space and then re-execute.

Windows

If there is no improvement after terminating unnecessary programs, increase the memory or extend the virtual memory.

Solaris OE Linux

If there is no improvement after terminating unnecessary programs, increase the memory or extend the swap area.

For the amount of memory space required for Smart Repository operation, see 'Memory Requirements' in the Tuning Guide.

LDAP_TIMEOUT 85 (0x55)

Timed out

Explanation

A timeout occurred.

User Action

Increase the specified search time limit as a client search option.

If there is no improvement, change the connected DN to the administrator DN of the target repository or use the Interstage Management Console to increase the value of 'Search Timeout' from the Settings window of the target repository.

LDAP_AUTH_UNKNOWN 86 (0x56)

Unknown authentication method

Explanation

An undefined authentication method was specified.

User Action

Functions created by API may not be supported. Alternatively, a function that cannot be used in Smart Repository may have been used.

Check whether any functions that cannot be used in Smart Repository were used by referring to the following manuals:

'Limitations on Smart Repository' in Product Notes

'Notes on Smart Repository' in Product Notes

LDAP_FILTER_ERROR 87 (0x57)

Bad search filter

Explanation

There is an error in the search filter format.

User Action

Refer to 'Search Filter' and then re-execute.

LDAP_USER_CANCELLED 88 (0x58)

User cancelled operation

Explanation

Processing was canceled by a user request.

LDAP_PARAM_ERROR 89 (0x59)

Bad parameter to an ldap routine

Explanation

There is an error in the specified parameter.

User Action

Correct the API used in the created applications. For details of the API functions, see Chapter Five

LDAP_NO_MEMORY 90 (0x5a)

Out of memory

Explanation

A memory shortage occurred.

User Action

Terminate unnecessary programs to secure the required memory space and then re-execute.

Windows

If there is no improvement after terminating unnecessary programs, increase the memory or extend the virtual memory.

Solaris OE Linux

If there is no improvement after terminating unnecessary programs, increase the memory or extend the swap area.

For the amount of memory space required for Smart Repository operation, see 'Memory Requirements' in the Tuning Guide.

LDAP_CONNECT_ERROR 91 (0x5b)

Can't connect to the LDAP server

Explanation

Failed to establish a connection with the repository.

User Action

- Communication with the repository is not possible. Check for errors in the host name and port number of the connection destination.
- Contact the network administrator to check for errors in the network environment settings (for example, host file setting, DNS server/DHCP server specifications, DNS server/DHCP server settings, etc). If any errors are found, correct the network environment and then reset it.
- This message may be generated when the load of a network or a repository server is high.
  - In the case of a user application, it is avoidable by retrying at the time of error generation.

  When SSL is being used between repository servers, and there are many clients or a high access frequency to Smart Repository, the above action may not resolve the error. In this case, try lightening the server load by using an SSL accelerator.
- Use the Interstage Management Console to check whether the repository is active.
  - If the repository is stopped, activate the repository.
  - If the repository is active, stop it and then restart it.
  - If the repository is in an abnormal state, stop it and then activate it.

Solaris OE Linux

- Contact the network administrator to check for errors in the network environment settings (for example, host file setting, DNS server/DHCP server specifications, DNS server/DHCP server settings, etc.). If any errors are found, correct the network environment and then reset it.
- Use the ps command to check whether the omsservd process is active. If the omsservd process is inactive, activate it using the enablerstart command. After executing the enablerstart command, restart the repository to perform the entry operation again.

  For details on how to use the enablerstart command, see 'Smart Repository Operation Commands' in the Reference Manual (Command Edition).

If there is still no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

LDAP_NOT_SUPPORTED 92 (0x5c)

Not supported

Explanation

The specified function is not supported.

User Action

Check whether any functions that cannot be used in Smart Repository were used by referring to the following manuals:

'Limitations on Smart Repository' in Product Notes

'Notes on Smart Repository' in Product Notes

If LDAP V3 extended function has been used, check whether the protocol version setting is correct.

LDAP_CONTROL_NOT_FOUND 93 (0x5d)

Control not found

Explanation

There is no applicable control.

User Action

The specified function cannot be used.

LDAP_NO_RESULTS_RETURNED 94 (0x5e)

No results returned

Explanation

No result was notified.

LDAP_MORE_RESULTS_TO_RETURN 95 (0x5f)

More result to return

Explanation

There are still results to be notified.

LDAP_CLIENT_LOOP 96 (0x60)

Client loop

Explanation

A loop was detected on the client.

User Action

Smart Repository never returns this code. The directory server of another product may be connected. Check whether the connection destination is correct and then specify the correct server to Smart Repository.

LDAP_REFERRAL_LIMIT_EXCEEDED 97 (0x61)

Referral limit exceeded

Explanation

This message may be output when a repository where referrals are registered is referenced.

User Action

Since the referral function cannot be used in Smart Repository, the directory server of another product may be connected. Check whether the connection destination is correct and then specify the correct server to Smart Repository.

SSL Error Codes

This section explains the meanings of the SSL error code and the required action.

0x00000000

Explanation

The process ended normally.

User action

Continue with processing.

0x00010001

Explanation

A timeout occurred during SSL connection.

User Action

- LDAP client (ldapmodify, ldapsearch, ldapdelete, user applications)

  If the connection destination is not operating correctly, take action to resolve the connection destination issue.

  If the connection destination is operating correctly:

  - The load of the repository server is heavy

    For user applications, retry can avoid the error.

    If SSL is used for communication with the repository server, and the number of clients is large and the frequency of access to Smart Repository is high, the above action may not resolve the error. If there is no improvement, consider lightening the server load by, for example, using the SSL accelerator.

  - Otherwise

    The timer value may be too short. Increase the timer value (ssl_timer) in the SSL environment definition file or the value of ssl_timer in the SSLENV structure and then re-execute.

    For information about the timer value (ssl_timer) in the SSL environment definition file, see Setting an SSL Environment Definition File (Client) in Chapter Two - Environment Setup

  - If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

- Other than LDAP client

  Use the iscollectinfo command to collect diagnostic information and then contact your service engineer.

0x00020001

Explanation

A memory shortage occurred in the SSL library.

User Action

Terminate unnecessary programs or secure sufficient memory for Smart Repository operation. For the memory capacity required for Smart Repository operation, see the following:

'Memory Requirements' in the Tuning Guide.

0x00020002

Explanation

A memory shortage occurred in the SSL library.

User Action

Terminate unnecessary programs or secure sufficient memory for Smart Repository operation. For the memory capacity required for Smart Repository operation, see the following:

'Memory Requirements' in the Tuning Guide.

0x00100001

Explanation

There is a certificate verification method error.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL.

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, make sure all services and server applications are stopped. For the methods of starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring the Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If the above actions do not resolve the error or there is no resource backup available, re-establish an Interstage Certificate Environment. For the setup of an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after correctly setting the certificate verification method (ssl_verify) in the SSL environment definition file or ssl_verify in the SSLENV structure. For the certificate verification method (ssl_verify), see Setting an SSL Environment Definition File (Client) in Chapter Two - Environment Setup.

0x00100002

Explanation

Cannot find the SSL environment definition file. Alternatively, the setting for the encryption method is incorrect.

User Action

If the JNDI or ldap commands are used with the user application, check whether the specified SSL environment file exists. The SSL environment definition file is specified by the following methods.

- JNDI

  system property 'user.sslenvfile'

- LDAP command

  -Z option

If the SSL environment definition file exists, take the action described below. This action is dependant on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, make sure all services and server applications are stopped. For the methods of starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring the Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If the above actions do not resolve the error or there is no resource backup available, re-establish an Interstage Certificate Environment. For the setup of an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after correctly setting the encryption algorithm (crypt) in the SSL environment definition file or crypt in the SSLENV structure.

  For the encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x00100008

Explanation

The site certificate has expired.

User Action

Acquire a new site certificate from the CA and register it for the Interstage Certificate Environment or certificate/key management environment.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide' - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  For the methods of acquiring and registering certificates, refer to the following in the order indicated and take the required action:

1) 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'

2) 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x00100009

Explanation

The CA Certificate has expired.

User Action

Acquire a new certificate from the CA and register it for the Interstage Certificate Environment or certificate/key management environment.

- Interstage Certificate Environment

  For the expiry date of the CA Certificate, check the latest information by displaying the following windows and then clicking the [Refresh] button in the last window.

  On the Interstage Management Console, select [System] > [Security] > [Certificates] > [CA Certificates] > [List] tab (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificates] > [List] tab)

  For the expiry date of the site certificate, check the latest information by displaying the following windows and then clicking the [Refresh] button in the last window.

On the Interstage Management Console, select [System] > [Security] > [Certificates] > [Site Certificates] > [List] tab (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [Site Certificates] > [List] tab)

To acquire and register a certificate, use either of the following methods:

- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  Take the required action using the following procedure:

  - 1. Check the expiry date of the CA Certificate using the cmdspcert command.
  - 2. Acquire and register new CA Certificates and site certificates in place of the expired CA Certificate and site certificate.

  For information on acquiring certificates, follow the instructions of each CA. For cmdspcert command details, see 'SSL Environment Setting Commands' in the Reference Manual (Command Edition).

  For information on registering certificates, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x0010000C

Explanation

CA Certificate or site certificate verification failed.

User Action

There is an error in the registration order of the certificates required to verify the certificate indicated by the certificate nickname. Correct and register the certificates in the Interstage certificate environment or certificate/key management environment one by one from the CA certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'

- Certificate/key management environment

  For the methods of acquiring and registering certificates, refer to the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x0010000D

Explanation

An unsupported encryption method is specified.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or there is no resource backup available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting the encryption algorithm (crypt) in the SSL environment definition file or crypt in the SSLENV structure.

  For the encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File' in Chapter Two - Environment Setup.

0x00100012

Explanation

Decryption of the private key failed.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or there is no resource backup available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  The certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before starting to restore the certificate/key management environment ensure that no programs are using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement or there is no resource backup available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

If there is still no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00100016

Explanation

Analysis of the site certificate failed.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or there is no resource backup available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  The certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before starting to restore the certificate/key management environment ensure that no programs are using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement or there is no resource backup available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

If there is still no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00100017

Explanation

Analysis of the CA Certificate failed.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or there is no resource backup available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  The certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before starting to restore the certificate/key management environment ensure that no programs are using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement or there is no resource backup available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

If there is still no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00100018

Explanation

The site certificate of the connection destination has expired.

User Action

Acquire a new site certificate from the CA at the connection destination and register it for the Interstage Certificate Environment of the connection destination.

To acquire and register a certificate, use either of the following methods:

- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

0x00100019

Explanation

Analysis of the connection destination site certificate failed.

User Action

The Interstage Certificate Environment of the connection destination may have been damaged. Restore the Interstage Certificate Environment of the connection destination from the resources backed up at the connection destination. Before restoring the Interstage Certificate Environment at the connection destination, ensure that all services and server applications are stopped at the connection destination. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring the Interstage Certificate Environment resources, see the following:

'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

For information on setting up an Interstage Certificate Environment, see the following:

'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

0x0010001A

Explanation

Verification of the connection destination site certificate failed.

User Action

To verify that the connection destination is correct, register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment of the local host one by one from the CA Certificate of the root CA.

To acquire and register a certificate, use either of the following methods:

- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'

0x00100020

Explanation

No nickname was specified for the site certificate.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring the Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Although it is possible to omit the user certificate nickname (user_cert_name) in the SSL environment definition file or user_cert in the SSLENV structure, the manner in which it was omitted is incorrect.

  To omit the user certificate nickname (user_cert_name) from the SSL environment definition file, do not describe the user_cert_name line or insert '#' at the beginning of the line.

  To omit user_cert from the SSLENV structure, set NULL to user_cert.

  If the user certificate nickname (user_cert_name) in the SSL environment definition file or user_cert in the SSLENV structure is omitted, all site certificates registered for the certificate/key management environment are assumed.

  For information on the user certificate nickname (user_cert_name), see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010002A

Explanation

There is an error in the CRL management directory.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or there is no resource backup available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  The certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before starting to restore the certificate/key management environment ensure that no programs are using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement or there is no resource backup available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

0x0010002B

Explanation

No site certificate could be received due to either of the following reasons:

- No site certificate was registered at the connection destination.
- The connection destination rejected the transmission of the site certificate.

User Action

The connection destination must acquire site certificates from the CA and register the site certificates for the Interstage Certificate Environment or certificate/key management environment one by one from the CA Certificate of the root CA, and then send them.

It is also necessary to register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  – If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  – If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

1) 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'

2) 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

Note the following points if deleting certificates to correct the certificate registration order:

– If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

– If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

If there is still no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x0010002C

Explanation

There is an error in the SSL protocol version setting.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring the Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting a value that can be set as an SSL version (ssl_version) in the SSL environment definition file.

  If a value that cannot be set to ssl_verify in the SSLENV structure is set, it is assumed that SSL should not be used (the same processing as ldap_init()).

  For information on the SSL version (ssl_version) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010002D

Explanation

The CA Certificate or site certificate has been canceled.

User Action

Acquire a new CA Certificate or site certificate from the CA and then register it for the Interstage Certificate Environment or certificate/key management environment.

Check the serial number of the canceled certificate using either of the following methods:

- Save CRL in a file with the extension 'crl' in the Windows(R) environment and right-click the saved file. After a menu is displayed, click [Open] in the menu to display the [Certificate revocation list] window. Click the [Revocation list] tab in the [Certificate revocation list] window to check the serial number of the canceled certificate.
- Register CRL with an entry using the Entry Management Tool and then check the serial number of the canceled certificate from the Invalid certificates list viewer.

Confirm the canceled certificate as described below and then acquire and register a new certificate to take the place of the canceled certificate.

- Interstage Certificate Environment

  Check the canceled certificate using the following procedure:

  – 1. On the Interstage Management Console, select [System] > [Security] > [Certificates] > [Site Certificates] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [Site Certificates]), and then click the [Refresh] button on the [List] tab to acquire the latest information. Then, reference the serial number of the site certificate to check the canceled site certificate.

  – 2. On the Interstage Management Console, select [System] > [Security] > [Certificates] > [CA Certificates] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificates]), and then click the [Refresh] button on the [List] tab to acquire the latest information. Then, reference the serial number of the CA Certificate to check the canceled CA Certificate.

  To acquire and register a certificate, use either of the following methods:

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  Check the canceled certificate using the following procedure:

  - 1. Use the cmlistcert command to check the certificates registered in the certificate/key management environment.

2. Use the cmdspcert command to check the canceled certificate by referencing the serial number of each registered certificate.

   For details of the cmlistcert and cmdspcert commands, see the following:

   'SSL Environment Setting Commands' in the Reference Manual (Command Edition)

   For the methods of acquiring and registering certificates, see the following in the indicated order and take the required action:

   - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'

   - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x0010002E

Explanation

Access from the connection destination was rejected because an expired site certificate was received.

User Action

Acquire a new site certificate from the CA at the connection destination and then register it for the Interstage Certificate Environment or certificate/key management environment of the connection destination.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the indicated order and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'

  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x00100035

Explanation

Verification of the received site certificate failed.

User Action

Register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the indicated order and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x00100036

Explanation

There is an error in the operation control directory.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment. For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting the operation control directory of the certificate/key management environment to be used to the operation control directory (cert_path) in the SSL environment definition file or cert_path in the SSLENV structure.

  For information on the operation control directory (cert_path) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010003B

Explanation

No private key corresponding to the site certificate could be found in the Interstage Certificate Environment or certificate/key management environment.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been restored while the Interstage Management Console was operating. Stop the Interstage Management Console and then restart it. For information on starting and stopping the Interstage Management Console, see the following:

  'Interstage Operation Using the Interstage Management Console' in the Interstage Operator's Guide - 'Starting and Stopping the Interstage Management Console'

  If there is no improvement, the Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement after restoring the Interstage Certificate Environment or there is no resource backup available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Register the private key corresponding to the site certificate for the certificate/key management environment.

  For the registration of private keys, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmenterkey'

  If there is no improvement, the certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before restoring the certificate/key management environment, ensure that there are no programs using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement after restoring the certificate/key management environment or there is no resource backup available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

0x0010003D

Explanation

There is an error in the token label.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring the Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or there is no resource backup available, re-establish an Interstage Certificate Environment. For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting the token label of the certificate/key management environment to be used to the token label (tkn_lbl) in the SSL environment definition file or tkn_lbl in the SSLENV structure. For information on the token label (tkn_lbl) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010003E

Explanation

There is an error in the nickname of the site certificate.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  Specify the required site certificate in the SSL configuration used by the repository according to the following procedure:

  – 1. If the repository is already active, stop the repository using the Interstage Management Console.

- 2. Click the [Refresh] button in the following window to check the SSL configuration used by the repository:

  On the Interstage Management Console, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), and then click [General Settings] on the [View Status] tab of the repository in use.

  If the repository is a master, also check the SSL configuration used by the repository for replication by clicking the [Refresh] button in the following window:

  On the Interstage Management Console, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]), and then click [Replication connection settings] in [Detailed setting [View]] on the [View Status] tab of the repository in use.

- 3. Click the [Refresh] button in the following window and then specify the site certificate required for the SSL configuration. If no site certificate is registered, acquire and register a site certificate.

  On the Interstage Management Console, select [System] > [Security] > [SSL] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [SSL]), and then click [Environment setup] in the SSL configuration of the used repository on the [List] tab.

- 4. Start the repository.

  To acquire and register a certificate, use either of the following methods:

- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  Check whether the user certificate nickname of the SSL environment definition file corresponds to the site certificate nickname in use.

  - The nickname does not correspond:

    Ensure that the user certificate nickname (user_cert_name) of the SSL environment definition file corresponds with the site certificate nickname in use, and then re-execute the process.

  - The nickname corresponds:

    The certificate of the nickname specified in the user certificate nickname (user_cert_name) of the SSL environment definition file may not have been registered as a site certificate.

    Specify -own option for cmentcert command to register the site certificate.

  For detail of user certificate nickname, refer to 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010003F

Explanation

There is an error in the nickname of the client CA certificate.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL.

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  The certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before restoring the certificate/key management environment, ensure that there are no programs using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement or no resource backup is available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

0x00100040

Explanation

There is no path list for the site certificate.

User Action

There is an error in the registration order of the certificates required to verify the certificate indicated by the certificate nickname. Correct and register the certificates in the Interstage Certificate Environment or certificate/key management environment one by one from the CA certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'
  Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate '
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x00100041

Explanation

There is no path list for the CA Certificates.

User Action

The registration order of the certificates is invalid. Correct and register certificates in the Interstage certificate environment or certificate/key management environment one by one from the CA certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  – If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  – If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  – 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate '

  – 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

  Note the following points if deleting certificates to correct the certificate registration order:

  – If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  – If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x00100042

Explanation

No path list exists in the received site certificate.

User Action

Register the certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate '
  - 2 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x00100043

Explanation

No path list exists for the CA Certificates.

User Action

To verify that the connection destination is correct, register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment of the local host one by one from the CA Certificate of the root CA.

To acquire and register a certificate, use either of the following methods:

- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'

0x00100044

Explanation

The path of the received certificate is incomplete.

User Action

Register the CA Certificates required to verify the certificate received from the connection destination for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

- 1 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
- 2 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x00100045

Explanation

The path of the connection destination site certificate is incomplete.

User Action

If the connection destination uses a certificate for testing, stop using the certificate for testing at the connection destination. Instead, site certificates must be acquired from the CA at the connection destination and certificates for the Interstage Certificate Environment of the connection destination registered one by one from the CA Certificate of the root CA.

Whether or not the connection destination uses a certificate for testing, to verify that the connection destination is correct it is necessary to register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment of the local host one by one from the CA Certificate of the root CA.

To acquire and register a certificate, use either of the following methods:

- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
- 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'

0x00100046

Explanation

The path of the site certificate is incomplete.

User Action

The registration order of the certificates required to verify the certificate indicated by the certificate nickname is invalid. Correct and register the certificates in the Interstage Certificate Environment or certificate/key management environment one by one from the CA certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  – If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  – If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'
  Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  – 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate '

- 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x00100047

Explanation

The path of the CA Certificate is incomplete.

User Action

The registration order of certificates is invalid. Correct and register certificates in the Interstage certificate environment or certificate/key management environment one by one from the CA certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate '
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x00100048

Explanation

Analysis of the received certificate failed.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL.

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  The certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before restoring the certificate/key management environment, ensure that no programs are using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement or no resource backup is available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

If there is still no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00100049

Explanation

Verification of the CA Certificate failed.

User Action

The registration order of certificates is invalid. Correct and register certificates in the Interstage certificate environment or certificate/key management environment one by one from the CA certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

0x0010004A

Explanation

The CA Certificate has been canceled.

User Action

Acquire a new CA Certificate from the CA and then register it for the Interstage Certificate Environment or certificate/key management environment.

After opening CRL in Internet Explorer, the serial number of the canceled certificate can be referenced. Check the serial number of the canceled certificate using the following procedure and then acquire and register a new certificate to replace the canceled certificate.

- Interstage Certificate Environment

  Check the canceled certificate using the following procedure:

  On the Interstage Management Console, select [System] > [Security] > [Certificates] > [CA Certificates] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificates]), and then reference the serial number of the CA Certificate on the [List] tab to check the canceled CA Certificate.

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  Check the canceled certificate using the following procedure:

  - 1. Use the cmlistcert command to check the certificates registered for the certificate/key management environment.

  - 2. Use the cmdspcert command to check the canceled certificate by referencing the serial number of each registered certificate.

  For cmlistcert and cmdspcert command details, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition)

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'

  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x0010004B

Explanation

There is an error in the slot information directory.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL.

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring the Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment. For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting the slot information directory name of the certificate/key management environment to be used to the slot information directory (slot_path) in the SSL environment definition file or slot_path in the SSLENV structure. For information on the slot information directory (slot_path) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010004C

Explanation

There is an error in the token label.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment. For information on setting up an Interstage Certificate Environment, see the following:

'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting the token label of the certificate/key management environment to be used to the token label (tkn_lbl) in the SSL environment definition file or tkn_lbl in the SSLENV structure. For information on the token label (tkn_lbl) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010004D

Explanation

There is an error in the user PIN. Alternatively, the user PIN may not be encrypted.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been restored while the Interstage Management Console was operating. Stop the Interstage Management Console and then restart it. For information on starting and stopping the Interstage Management Console, see the following:

  'Interstage Operation using the Interstage Management Console' in the Interstage Operator's Guide - 'Starting and Stopping the Interstage Management Console'

  If there is no improvement, the Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is still no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting the user PIN of the certificate/key management environment to be used to the user PIN (tkn_pwd) in the SSL environment definition file.

Encrypt the user PIN (tkn_pwd) in the SSL environment definition file after correcting it.

If there is an error with the user PIN (tkn_pwd) specified in the SSL environment definition file, the user PIN (tkn_pwd) may not be encrypted. Encrypt the user PIN (tkn_pwd) using the 'irepencupin' command.

For information on the user PIN (tkn_pwd) in the SSL environment definition file, refer to the 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup. For detail of the user PIN (tkn_pwd) encryption of the SSL environment definition file, refer to the 'Encrypting the user PIN (client)'.

0x0010004E

Explanation

SSL environment definition file may have been destroyed. Alternatively, the operating management directory is incorrect.

User Action

If the JNDI user application or LDAP command is used, check the content of the specified SSL environment definition file. For details of the content of the SSL environment definition file, refer to Setting an SSL Environment Definition File (Client) in Chapter Two of the Smart Repository Operator’s Guide.

If the SSL environment definition file has not been destroyed, take the action described below. The action taken is dependant on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  Re-execute processing after setting the operation control directory of the certificate/key management environment to be used to the operation control directory (cert_path) in the SSL environment definition file or cert_path in the SSLENV structure. For information on the operation control directory (cert_path) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

0x0010005A

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

If any of the following errors is returned together with this error, take the action indicated by that error number:

- 0x00300017
- 0x00300022
- 0x9001013E
- 0x90020068
- 0x90030068
- 0x90040068
- 0x90050068
- 0x90060068
- 0x900b0074
- 0x9011013e
- 0x90130068
- 0x90140068
- 0x90150068
- 0x9016013e

If there is no improvement after taking the indicated action or if this error occurs alone, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00150001

Explanation

The connection was broken while processing a request with the connection destination.

User Action

- Replication operation

  Match the settings of the following items in the SSL configuration used by the master repository with those used by the slave repository.

  – SSL protocol version

  – Encryption method

  Check for errors in the host name and port number of the connection destination.

- Connection between the LDAP client (ldapmodify, ldapsearch, ldapdelete, user application) and repository

  Match the following settings:

  - The SSL version (ssl_version) in the SSL environment definition file used by the LDAP client and the SSL protocol version of the SSL configuration used by the repository
  - The encryption algorithm (crypt) in the SSL environment definition file used by the LDAP client and the encryption method of the SSL configuration used by the repository

  Check for errors in the host name and port number of the connection destination.

- Common items

  After correcting the SSL configuration, restart the repository that uses the SSL configuration so that it is reflected in the repository.

  Check the connection destination system log for any recorded messages. If a message was recorded, take the indicated action at the connection destination.

  For information on the SSL version (ssl_version) and encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter 2 - Environment Setup.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00200001

Explanation

An internal conflict occurred inside the SSL library.

User Action

Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00200002

Explanation

The number of sessions in one process has exceeded the allowable maximum of 1024.

User Action

On the application side, limit the number of session in one process to less than 1024. For details, refer to the following manual.

'Maximum number of sessions ' in the 'Flow of Basic Operations' in Chapter 5 – Creating an Application (JNDI).

0x00300004

Explanation

The directory specified in the SSL environment definition file is incorrect.

User Action

If the specified directory on the slot information directory (slot_path) or operation control directory (cert_path) is a read-only device (or other reason), specify a correct directory and then re-execute.

For details of the SSL environment definition file, refer to the Setting an SSL Environment Definition File (Client) in Chapter Two of the Smart Repository Operator's Guide.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00300017, 0x00300022

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00400001 - 0x0040000E

Explanation

A socket access error occurred while using SSL.

User Action

- Communication with the connection destination repository is not possible. Check for errors in the host name and port number of the connection destination.
- Use the Interstage Management Console to check whether the repository is active.

  If the repository is stopped, activate the repository.

  If the repository is active, stop it and then restart it.

  If the repository is in an abnormal state, stop it and then activate it.
- Contact the network administrator to check for network environment setting errors (for example, host file setting, DNS server/DHCP server specifications, DNS server/DHCP server settings). If an error is found, correct the network environment and then reset it.

- Error code: 0x00400004, detail code: 145(0x91)

  This error code may be output if the repository server load is heavy.

  – For user applications, retry can avoid the error.

  – For the ldapmodify, ldapsearch, and ldapdelete commands, re-execute the command.

  – For replication connection checks, recheck the connection.

  – For replication operations, check whether the connection destination repository is active using the above method.

  If SSL is used for communication with the repository server, and the number of clients is large and the frequency of access to Smart Repository is high, there may be no improvement. In this case, consider lightening the server load by, for example, using the SSL accelerator.

If there is still no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00500003

Explanation

The SSL protocol version does not match that of the connection destination.

User Action

- Replication operation

  Match the SSL protocol version of the master repository SSL configuration to the version of the slave repository.

- Connection between the LDAP client (ldapmodify, ldapsearch, ldapdelete, user application) and repository

  Match the SSL version (ssl_version) of LDAP client's SSL environment definition file to the SSL protocol version of the repository's SSL configuration.

- Common items

  After correcting the SSL configuration, restart the repository that uses the SSL configuration so that it is reflected in the repository.

  Check the connection destination system log for any recorded messages. If a message was recorded, take the indicated action at the connection destination.

  For information on the SSL version (ssl_version) and encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter 2 - Environment Setup.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00500004

Explanation

The SSL protocol version or encryption method does not match that of the connection destination.

User Action

- Replication operation

  Match the settings of the following items in the SSL configuration used by the master repository with those used by the slave repository.

  - SSL protocol version
  - Encryption method

- Connection between the LDAP client (ldapmodify, ldapsearch, ldapdelete, user application) and repository

  Match the following settings:

  - The SSL version (ssl_version) in the SSL environment definition file used by the LDAP client and the SSL protocol version of the SSL configuration used by the repository
  - The encryption algorithm (crypt) in the SSL environment definition file used by the LDAP client and the encryption method of the SSL configuration used by the repository

- Common items

  After correcting the SSL configuration, restart the repository that uses the SSL configuration so that the SSL configuration is reflected in the repository.

  Check the connection destination system log for any recorded messages. If a message was recorded, take the indicated action at the connection destination.

  For information on the SSL version (ssl_version) and encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x0050000D

Explanation

Non-SSL data or data not based on the SSL protocol attempted to access the SSL port.

User Action

A protocol other than SSL may have been used for access. Check whether the protocol, connection destination host name, or port number is correct.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x0050000F, 0x00600001

Explanation

The SSL protocol version or encryption method does not match that of the connection destination.

User Action

- Replication operation

  Match the settings of the following items in the SSL configuration used by the master repository with those used by the slave repository.

  – SSL protocol version

  – Encryption method

- Connection between the LDAP client (ldapmodify, ldapsearch, ldapdelete, user application) and repository

  Match the following settings:

  – The SSL version (ssl_version) in the SSL environment definition file used by the LDAP client and the SSL protocol version of the SSL configuration used by the repository

  – The encryption algorithm (crypt) in the SSL environment definition file used by the LDAP client and the encryption method of the SSL configuration used by the repository

- Common items

  After correcting the SSL configuration, restart the repository that uses the SSL configuration so that it is reflected in the repository.

  Check the connection destination system log for any recorded messages. If a message was recorded, take the indicated action at the connection destination.

  For information on the SSL version (ssl_version) and encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter 2 - Environment Setup.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00700001, 0x00700002

The meaning and action to be taken vary according to the detail code.

The detail codes are shown below:

- Ldapmodify, ldapsearch, and ldapdelete

  Within the parentheses () of the displayed message

Detail code

0x00020028
0x00020029
0x0002002a
0x0002002b
0x0002002c
0x0002002d
0x0002002e
Others

0x00020028

Explanation

The SSL connection failed or was terminated.

User Action

- Replication operation

  Match the settings of the following items in the SSL configuration used by the master repository with those used by the slave repository.

  - SSL protocol version
  - Encryption method

- Connection between the LDAP client (ldapmodify, ldapsearch, ldapdelete, user application) and repository

  Match the following settings:

  - The SSL version (ssl_version) in the SSL environment definition file used by the LDAP client and the SSL protocol version of the SSL configuration used by the repository
  - The encryption algorithm (crypt) in the SSL environment definition file used by the LDAP client and the encryption method of the SSL configuration used by the repository

- Common items

  After correcting the SSL configuration, restart the repository that uses the SSL configuration so that the SSL configuration is reflected in the repository.

  Check the connection destination system log for recorded messages. If a message was recorded, take the indicated action at the connection destination.

  For information on the SSL version (ssl_version) and encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter 2 - Environment Setup.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00020029

Explanation

Verification of the connection destination site certificate failed. A CA Certificate required for verification is not registered.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  If the local host uses a certificate for testing, stop using the certificate for testing. Instead, acquire site certificates from the CA at the local host and register the certificates for the Interstage Certificate Environment of the local host one by one from the CA Certificate of the root CA.

  Regardless of whether the local host uses a certificate for testing, register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment of the local host one by one from the CA Certificate of the root CA.

  To acquire and register a certificate, use either of the following methods:

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide' - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  – If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  – If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  Register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  – 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'

  – 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x0002002a

Explanation

Failed to verify the CA Certificate or site certificate.

User Action

The registration order of the certificates required to verify the certificate indicated by the certificate nickname is invalid. Correct and register the certificates in the Interstage certificate environment or certificate/key management environment one by one from the CA certificate of the root CA.

- Interstage Certificate Environment

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x0002002b

Explanation

An unsupported site certificate has been received.

User Action

Acquire supported site certificates from the CA at the connection destination and then register them for the Interstage Certificate Environment or certificate/key management environment one by one from the CA Certificate of the root CA.

Also register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

For information on supported certificates, see the following:

'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Certificates and Private Keys'

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x0002002c

Explanation

A CA Certificate or site certificate has been canceled.

User Action

Acquire a new CA Certificate or site certificate from the CA and then register it for the Interstage Certificate Environment or certificate/key management environment.

After opening CRL in Internet Explorer, the serial number of the canceled certificate can be referenced. Check the serial number of the canceled certificate using the following procedure and then acquire and register a new certificate to replace the canceled certificate.

- Interstage Certificate Environment

  Check the canceled certificate using the following procedure:

1. On the Interstage Management Console, select [System] > [Security] > [Certificates] > [Site Certificates] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [Site Certificates]), and then reference the serial number of the site certificate on the [List] tab to check the canceled site certificate.
2. On the Interstage Management Console, select [System] > [Security] > [Certificates] > [CA Certificates] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificates]), and then reference the serial number of the CA Certificate on the [List] tab to check the canceled CA Certificate.

   To acquire and register a certificate, use either of the following methods:

   - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
   - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  Check the canceled certificate using the following procedure:

  - Use the cmlistcert command to check the certificates registered for the certificate/key management environment.
  - Use the cmdspcert command to check the canceled certificate by referencing the serial number of each registered certificate.

For cmlistcert and cmdspcert command details, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition)

For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

- 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
- 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x0002002d

Explanation

Connection destination access was denied because an expired site certificate was received.

User Action

Acquire a new site certificate from the CA at the connection destination and then register it for the Interstage Certificate Environment or certificate/key management environment of the connection destination.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
  - 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

0x0002002e

Explanation

Verification of the connection destination site certificate failed. A CA Certificate required for verification is not registered.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  If the local host uses a certificate for testing, stop using the certificate for testing. Instead, acquire site certificates from the CA at the local host and register the certificates for the Interstage Certificate Environment of the local host one by one from the CA Certificate of the root CA.

  Regardless of whether the local host uses a certificate for testing, register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment of the local host one by one from the CA Certificate of the root CA.

  To acquire and register a certificate, use either of the following methods:

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'

  – 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  – If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  – If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  Register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  – 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate '

  – 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

  Note the following points if deleting certificates to correct the certificate registration order:

  – If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.

  – If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For the information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

Others

Explanation

An unexpected error was detected in an SSL function.

User Action

Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x00700003

The meaning and action to be taken vary according to the detail code.

The detail codes are shown below:

- ldapmodify, ldapsearch, and ldapdelete

  Within the parentheses () of the displayed message

Detail Code

0x0001
0x0004
0x0005
Others

0x0001

Explanation

The SSL protocol version or encryption method does not match that of the connection destination.

User Action

- Replication operation

  Match the settings of the following items in the SSL configuration used by the master repository with those used by the slave repository.

  – SSL protocol version

  – Encryption method

- Connection between the LDAP client (ldapmodify, ldapsearch, ldapdelete, user application) and repository

  Match the following settings:

  – The SSL version (ssl_version) in the SSL environment definition file used by the LDAP client and the SSL protocol version of the SSL configuration used by the repository

  – The encryption algorithm (crypt) in the SSL environment definition file used by the LDAP client and the encryption method of the SSL configuration used by the repository

- Common items

  After correcting the SSL configuration, restart the repository that uses the SSL configuration so that the SSL configuration is reflected in the repository.

  Check the connection destination system log for any recorded messages. If a message was recorded, take the indicated action at the connection destination.

  For information about the SSL version (ssl_version) and encryption algorithm (crypt) in the SSL environment definition file, see 'Setting an SSL Environment Definition File (Client)' in Chapter Two - Environment Setup.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x0004

Explanation

No site certificate could be received for either of the following reasons:

- No site certificate was registered at the connection destination.
- The connection destination rejected the transmission of the site certificate.

User Action

The connection destination must acquire site certificates from the CA, register site certificates for the Interstage Certificate Environment or certificate/key management environment one by one from the CA Certificate of the root CA, and then send them.

It is also necessary to register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

- Interstage Certificate Environment

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

  Note the following points if deleting certificates to correct the certificate registration order:

  - If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
  - If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete' Certificate/key management environment

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

- 1. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'
- 2. 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

Note the following points if deleting certificates to correct the certificate registration order:

- If a site certificate is deleted, the corresponding private key will also be deleted. If only a site certificate remains as a file, it is not possible to re-register the site certificate.
- If a CA Certificate is deleted, the CA Certificate and site certificates issued by the CA cannot be used.

For information on deleting certificates, see the following:

'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x0005

Explanation

Verification of the connection destination site certificate failed. A CA Certificate required for verification is not registered.

User Action

Register the CA Certificates required to verify the connection destination site certificate for the Interstage Certificate Environment or certificate/key management environment of the local host one by one from the CA Certificate of the root CA.

- Interstage Certificate Environment

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'scsdelete'

  To acquire and register a certificate, use either of the following methods:

  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with CSR'
  - 'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring the Interstage Certificate Environment with PKCS#12'

- Certificate/key management environment

  For information on deleting certificates, see the following:

  'SSL Environment Setting Commands' in the Reference Manual (Command Edition) - 'cmrmcert'

  For the methods of acquiring and registering certificates, see the following in the order indicated and take the required action:

  - 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Creating a Secret Key and Acquiring a Certificate'

  - 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment' - 'Registering the Certificate and CRL'

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

Others

Explanation

An unexpected error was detected in an SSL function.

User Action

Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x9001013E

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90020068

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90030068

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90040068

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90050068

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90060068

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x900B0065

Explanation

A user other than the user who created the certificate/key management environment used the certificate/key management environment.

User Action

A certificate/key management environment must be used by the user who created it. Alternatively, create and use a new certificate/key management environment. For information on the creation of a certificate/key management environment, see 'Client' in 'Setting Up an Environment for SSL Communication'.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x900B0074

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x9011013E

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90130068

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90140068

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x90150068

Explanation

An authority error occurred when referencing the CA Certificates.

User Action

Take the following action depending on the certificate and private key management environment that has been set up to conduct encrypted communication via SSL:

- Interstage Certificate Environment

  The Interstage Certificate Environment may have been damaged. Restore the Interstage Certificate Environment from the backed up resources. Before restoring the Interstage Certificate Environment, ensure that all services and server applications are stopped. For information on starting and stopping services and server applications, see the manuals of the services and server applications. For information on restoring Interstage Certificate Environment resources, see the following:

  'Maintenance (Resource Backup)' in the Interstage Operator's Guide - 'Backing Up and Restoring Resources' - 'Restore Procedure' - 'Restoring Interstage Certificate Environment Resources'

  If there is no improvement or no resource backup is available, re-establish an Interstage Certificate Environment.

  For information on setting up an Interstage Certificate Environment, see the following:

  'Setting and Use of an Interstage Certificate Environment' in the Security System Guide - 'Configuring Environments'

- Certificate/key management environment

  The certificate/key management environment may have been damaged. Restore the certificate/key management environment from the backed up resources. Before restoring the certificate/key management environment, ensure that no programs are using the certificate/key management environment.

  The certificate/key management environment must be restored using a method that corresponds with the method used to create backup copies.

  If there is no improvement or no resource backup is available, re-establish a certificate/key management environment.

  For information on setting up a certificate/key management environment, see the following:

  'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' in the Security System Guide - 'Environment Setting for Certificate/Key Management Environment'

Alternatively, the file descriptors (fd) that can be used by the client may be insufficient.

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

0x9016013E

Explanation

The file descriptors (fd) that can be used by the client may be insufficient.

User Action

- JNDI

  Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

If there is no improvement, collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

Others

Explanation

An unexpected error was detected in an SSL function.

User Action

Collect diagnostic information by executing the iscollectinfo command and then contact your service engineer.

Appendix C

Smart Repository Object Classes

This appendix describes the object classes that can be used in Smart Repository.

[A]

account

applicationEntity

applicationProcess

[C]

certificationAuthority

certificationAuthority-V2

corbaContainer

corbaObject

corbaObjectReference

country

cRLDistributionPoint

[D]

dcObject

deltaCRL

device

dmd

dNSDomain

document

documentSeries

domain

domainRelatedObject

dSA

[F]

friendlyCountry

[G]

groupOfNames

groupOfUniqueNames

[I]

inetOrgPerson

[J]

javaContainer

javaMarshalledObject

javaNamingReference

javaObject

javaSerializedObject

[L]

labeledURIObject

locality

[O]

organization

organizationalPerson

organizationalRole

organizationalUnit

[P]

person

pilotDSA

pilotOrganization

pilotPerson (newPilotPerson)

pkiCA

pkiUser

[Q]

qualityLabelledData

[R]

residentialPerson

RFC822localPart

room

[S]

simpleSecurityObject

ssoResource

ssoRole

ssoRoleSet

ssoSite

ssoUser

strongAuthenticationUser

[T]

top

[U]

uidObject

userSecurityInformation

List of Objects

[A]

account

Definition

Define computer account information. This object class is defined in RFC1274.

OID

0.9.2342.19200300.100.4.5

Base Class

top

Type

STRUCTURAL

Required Attributes

uid(userID)	The user ID of an account.

Optional Attributes

description	A description for this entry.
seeAlso	The DN information related to this entry.
l (localityName)	A related country, city, or other geographical area.
o (organizationName)	An organization name.
ou (organizationUnitName)	An organization unit name.
host	The host name of a computer.

applicationEntity

Definition

Define an application entity. This object class is defined in RFC2256.

OID

2.5.6.12

Base Class

top

Type

STRUCTURAL

Required Attributes

presentationAddress	The OSI display address of the entry.
cn (commonName)	A common name or full name.

Optional Attributes

supportedApplicationContext	A description of the entry.
seeAlso	The DN information related to this entry.
ou (organizationUnitName)	An organization unit name.
o (organizationName)	An organization name.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

applicationProcess

Definition

Define an application process. This object class is defined in RFC2256.

OID

2.5.6.11

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

seeAlso	The DN information related to this entry.
ou (organizationUnitName)	An organization unit name.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

[C]

certificationAuthority

Definition

Define the information related to the certificate issuing authority (Certificate Authorities CAs) of a directory. This object class is defined in RFC2256.

OID

2.5.6.16

Base Class

top

Type

AUXILIARY

Required Attributes

authorityRevocationList	A list of revoked certificate authorities.
certificateRevocationList	A list of revoked user certificates.
cACertificate	A CA certificate.

Optional Attributes

crossCertificatePair	A cross certificate.

certificationAuthority-V2

Definition

Define the information related to the certificate issuing authority (Certificate Authorities, CAs) of a directory.

OID

2.5.6.16.2

Base Class

certificationAuthority

Type

AUXILIARY

Optional Attributes

deltaRevocationList	A list of revoked deltas

corbaContainer

Definition

Define the container of a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.2.10

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

corbaObject

Definition

Define a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.2.9

Base Class

top

Type

ABSTRACT

Optional Attributes

corbaRepositoryId	A Repository ID implemented by a CORBA object.
description	DN information related to an account.

corbaObjectReference

Definition

Define a CORBA object reference.

OID

1.3.6.1.4.1.42.2.27.4.2.11

Base Class

corbaObject

Type

AUXILIARY

Required Attributes

corbaIor	A character string representation of IOR of a CORBA object

country

Definition

Define a country. This object class is defined in RFC2256.

OID

2.5.6.2

Base Class

top

Type

STRUCTURAL

Required Attributes

c (countryName)	A two-character code defined by ISO to indicate a country name in the directory.

Optional Attributes

searchGuide	Search criteria information.
description	DN information related to an account.

cRLDistributionPoint

Definition

Define the way in which CRL information can be obtained.

OID

2.5.6.19

Base Class

top

Type

STRUCTURAL

Required Attributes

Cn (commonName)	A common name or full name.

Optional Attributes

certificateRevocationList	A list of revoked user certificates.
authorityRevocationList	A list of revoked certificate authorities.
deltaRevocationList	A list of revoked deltas.

[D]

dcObject

Definition

Define the domain component of the entry. This object class is defined in RFC2247.

OID

1.3.6.1.4.1.1466.344

Base Class

top

Type

AUXILIARY

Required attributes

dc (domainComponent)	A DNS domain.

deltaCRL

Definition

Define a list of revoked deltas. This object class is defined in RFC2587.

OID

2.5.6.23

Base Class

top

Type

AUXILIARY

Optional attributes

deltaRevocationList	A list of revoked deltas.

device

Definition

Define information on network devices such as printers.

OID

2.5.6.14

Base Class

top

Type

STRUCTURAL

Required Attributes

Cn (commonName)	A common name or full name.

Optional Attributes

serialNumber	A serial number.
seeAlso	The DN information related to this entry.
Owner	The distinguished name of the responsible person.
ou (organizationUnitName)	An organization unit name.
o (organizationName)	An organization name.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

dmd

Definition

Define directory management domain information.

OID

2.5.6.20

Base Class

top

Type

STRUCTURAL

Required Attributes

dmdName	The administration permission required to operate a directory management domain (DMD) and a directory server.

Optional Attributes

userPassword	A user password.
searchGuide	Search criteria information.
seeAlso	The DN information related to this entry.
businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
preferredDeliveryMethod	The preferred method of contact or message delivery.
telexNumber	A telex number.
teletexTerminalIdentifier	The identifier of a telex terminal.
telephoneNumber	A telephone number.
internationaliSDNNumber	An international ISDN number.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

dNSDomain

Definition

Define a DNS resource record.

OID

0.9.2342.19200300.100.4.15

Base Class

domain

Type

STRUCTURAL

Optional Attributes

aRecord	An Address DNS resource.
mDRecord	The equivalent of an MD record in DNS.
mXRecord	A Mail Exchange DNS resource.
nSRecord	A Name Server DNS resource.
sOARecord	A Start of Authority DNS resource.
cNAMERecord	The proper name of a DNS resource.

document

Definition

The document object class is used to define entries which represent documents.

OID

0.9.2342.19200300.100.4.6

Base Class

top

Type

STRUCTURAL

Required Attributes

documentIdentifier	The unique identifier of a document.

Optional Attributes

cn (commonName)	A common name or full name.
description	DN information related to an account.
seeAlso	The DN information related to this entry.
l (localityName)	A related country, city, or other geographical area.
o (organizationName)	An organization name.
ou (organizationUnitName)	An organization unit name.
documentTitle	The title of the document.
documentVersion	The version of the document.
documentAuthor	The distinguished name of the document author.
documentLocation	The location of the original copy of the document.
documentPublisher	A user or organization that published the document.

documentSeries

Definition

Define a document series.

OID

0.9.2342.19200300.100.4.9

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional attributes

description	DN information related to an account.
seeAlso	The DN information related to this entry.
telephonenumber	A telephone number.
l (localityName)	A related country, city, or other geographical area.
o (organizationName)	An organization name.
ou (organizationUnitName)	An organization unit name.

domain

Definition

Define a DNS domain.

OID

0.9.2342.19200300.100.4.13

Base Class

top

Type

STRUCTURAL

Required Attributes

dc (domainComponent)	DNS domain.

Optional (Attributes

associatedName	An entry in the organizational DIT entry related to a DNS domain.
o (organizationName)	An organization name.
description	DN information related to an account.
businessCategory	The type of business in which the entry is engaged.
seeAlso	The DN information related to this entry.
searchGuide	The search criteria information.
userPassword	A user password.
l (localityName)	A related country, city, or other geographical area.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
street (streetAddress)	The building name and street number of the entry.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
postalAddress	A postal address.
postalCode	A postal code.
postOfficeBox	A post-office box.
facsimileTelephoneNumber (fax)	A FAX number.
internationaliSDNNumber	An international ISDN number.
telephoneNumber	A telephone number.
teletexTerminalIdentifier	The identifier of a telex terminal.

telexNumber	A telex number.
preferredDeliveryMethod	The preferred method of contact or message delivery.
destinationIndicator	The address information required to provide the telegram service.
registeredAddress	A registered emergency contact address.
x121Address	The x121 address of the user.

domainRelatedObject

Definition

Define an entry that is the DNS domain equivalent of the X.500 domain representing an organization or organization unit. This object class is defined in RFC1274.

OID

0.9.2342.19200300.100.4.17

Base Class

top

Type

AUXILIARY

Required Attributes

associatedDomain	An entry in the organizational DIT entry related to the DNS domain.

dSA

Definition

Define DSA information. This object class is defined in RFC2256.

OID

2.5.6.13

Base Class

applicationEntity

Type

STRUCTURAL

Optional Attributes

knowledgeInformation	Knowledge information.

[F]

friendlyCountry

Definition

Define a friendly country. This object class is defined in RFC2256.

OID

0.9.2342.19200300.100.4.18

Base Class

country

Type

STRUCTURAL

Required Attributes

co (friendlyCountryName)	A country name.

[G]

groupOfNames

Definition

Define a group name. This object class is defined in RFC2256.

OID

2.5.6.9

Base Class

top

Type

STRUCTURAL

Required Attributes

member	The distinguished name of a group name member.
cn (commonName)	A common name or full name.

Optional Attributes

businessCategory	The type of business in which the entry is engaged.
seeAlso	The DN information related to this entry.
owner	The distinguished name of a responsible person.
ou (organizationUnitName)	An organization unit name.
O (organizationName)	An organization name.
description	The description of the entry.

groupOfUniqueNames

Definition

Define a group of unique names. This object class is defined in RFC2256.

OID

2.5.6.17

Base Class

top

Type

STRUCTURAL

Required Attributes

uniqueMember	A group of names associated with an entry where each name was given a uniqueIdentifier to distinguish it.
cn (commonName)	A common name or full name.

Optional Attributes

businessCategory	The type of business in which the entry is engaged.
seeAlso	The DN information related to this entry.
owner	The distinguished name of a responsible person.
ou (organizationUnitName)	An organization unit name.
o (organizationName)	An organization name.
description	A description of the entry.

[I]

inetOrgPerson

Definition

Define an entry of an Internet user of an organization. This object class is defined in RFC2789.

OID

2.16.840.1.113730.3.2.2

Base Class

organizationalPerson

Type

STRUCTURAL

Optional Attributes

Audio	A sound file.
businessCategory	The type of business in which the entry is engaged.
carLicense	An automobile license plate number.
departmentNumber	A department number.
displayName	The display name of the entry.
employeeNumber	An employee number.
employeeType	An employment type.
givenName (gn)	The generation information of the name.
homePhone (homeTelephoneNumber)	A home telephone number.
homePostalAddress	A home address.
initials	Initials.
jpegPhoto	A JPEG photo.
labeledURI	A Uniform Resource Identifier (URI).
mail (rfc822Mailbox)	An email address.
manager	The distinguished name of a manager.
mobile (mobileTelephoneNumber)	A mobile telephone number.
o (organizationName)	An organization name.
pager (pagerTelephoneNumber)	A pager number.
photo	A photo.

roomNumber	The room number of an object.
secretary	A secretary or assistant.
uid (userid)	A user ID.
userCertificate	A user certificate.
x500uniqueIdentifier	Used to differentiate objects when a DN has been reused. For example: x500uniqueIdentifier: '0000000000000'B
preferredLanguage	The preferred language.
userSMIMECertificate	An S/MINE certificate.
userPKCS12	User PKCS#12.

[J]

javaContainer

Definition

Define the container for a JAVA object.

OID

1.3.6.1.4.1.42.2.27.4.2.1

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

javaMarshalledObject

Definition

Define a JAVA Marshaled object.

OID

1.3.6.1.4.1.42.2.27.4.2.8

Base Class

javaObject

Type

AUXILIARY

Required Attributes

javaSerializedData	Java serialized data.

javaNamingReference

Definition

Define a JNDI reference.

OID

1.3.6.1.4.1.42.2.27.4.2.7

Base Class

javaObject

Type

AUXILIARY

Optional Attributes

javaReferenceAddress	The address of a JNDI reference.
javaFactory	The location from which to load an object factory identified with the javaFactory attribute.

javaObject

Definition

Define a JAVA object.

OID

1.3.6.1.4.1.42.2.27.4.2.4

Base Class

top

Type

ABSTRACT

Required Attributes

javaClassName	A Java class name or interface name.

Optional Attributes

javaClassNames	The class name of an object factory that can be used to create an instance of an object identified by the attribute javaClassName.
javaCodebase	The URL of a class definition.
javaDoc	The JAVA document of a class.
description	A description of the entry.

javaSerializedObject

Definition

Define a JAVA serialized object.

OID

1.3.6.1.4.1.42.2.27.4.2.5

Base Class

javaObject

Type

AUXILIARY

Required Attributes

javaSerializedData	Java serialized data.

[L]

labeledURIObject

Definition

Define URL value information and an existing directory object. This object class is defined in RFC2079.

OID

1.3.6.1.4.1.250.3.15

Base Class

top

Type

AUXILIARY

Optional Attributes

labeledURI	A Uniform Resource Identifier (URI). Example: labeledURI: http://www.fujitsu.com

locality

Definition

Define a locality or geographical area. This object class is defined in RFC2256.

OID

2.5.6.3

Base Class

top

Type

STRUCTURAL

Optional Attributes

street (streetAddress)	The building name and street number of the entry.
seeAlso	The DN information related to this entry.
searchGuide	Search criteria information.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	The description of the entry.

[O]

organization

Definition

Define an organization. This object class is defined in RFC2256.

OID

2.5.6.4

Base Class

top

Type

STRUCTURAL

Required Attributes

o (organizationName)	An organization name.

Optional Attributes

userPassword	A user password.
searchGuide	Search criteria information.
seeAlso	The DN information related to this entry.
businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
preferredDeliveryMethod	The preferred method of contact or message delivery.
telexNumber	A telex number.
teletexTerminalIdentifier	The identifier of a telex terminal.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	The description of the entry.

organizationalPerson

Definition

Define a user who is an employee or a relevant person in an organization. This object class is defined in RFC2256.

OID

2.5.6.7

Base Class

person

Type

STRUCTURAL

Optional Attributes

Title	A title.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
preferredDeliveryMethod	A desired contact or message delivery method.
telexNumber	A telex number.
teletexTerminalIdentifier	The identifier of a telex terminal.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
ou (organizationUnitName)	An organization unit name.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.

organizationalRole

Definition

Define the role of an organization. This object class is defined in RFC2256.

OID

2.5.6.8

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
preferredDeliveryMethod	The preferred method of contact or message delivery.
telexNumber	A telex number.
teletexTerminalIdentifier	The identifier of a telex terminal.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
seeAlso	The DN information related to this entry.
roleOccupant	The distinguished name of the user acting in the role defined in the organizationalRole entry.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
ou (organizationUnitName)	An organization unit name.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	The description of the entry.

organizationalUnit

Definition

Define an organization unit. This object class is defined in RFC2256.

OID

2.5.6.5

Base Class

top

Type

STRUCTURAL

Required Attributes

ou (organizationalUnit)	An organization unit name.

Optional Attributes

userPassword	A user password.
searchGuide	The search criteria information.
seeAlso	The DN information related to this entry.
businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
preferredDeliveryMethod	The preferred method of contact or message delivery.
telexNumber	A telex number.
teletexTerminalIdentifier	The identifier of a telex terminal.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	The description of the entry.

[P]

person

Definition

Define a person. This object class is defined in RFC2256.

OID

2.5.6.6

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.
sn (surname)	A family name or last name.

Optional Attributes

userPassword	A user password.
telephoneNumber	A telephone number.
seeAlso	The DN information related to this entry.
description	The description of the entry.

pilotDSA

Definition

Define a pilot DSA.

OID

0.9.2342.19200300.100.4.21

Base Class

dSA

Type

STRUCTURAL

Optional Attributes

dSAQuality	Define the quality of a DSA.

pilotOrganization

Definition

Define a pilot Organization.

OID

0.9.2342.19200300.100.4.20

Base Class

organization organizationalUnit

Type

STRUCTURAL

Optional Attributes

buildingName	The name of a building.

pilotPerson (newPilotPerson)

Definition

Define a pilot Person.

OID

0.9.2342.19200300.100.4.4

Base Class

person

Type

STRUCTURAL

Optional Attributes

uid (userid)	A user ID.
textEncodedORAddress	A text-encoded originator/recipient (X.400) address.
mail (rfc822Mailbox)	An email address.
drink (favoriteDrink)	A favorite drink.
roomNumber	The room number of the object.
userClass	The category of computer user.
homePhone (homeTelephoneNumber)	A home telephone number.

homePostalAddress	A home address.
secretary	A secretary or assistant.
personalTitle	A personal title.
preferredDeliveryMethod	The preferred method for contact or message delivery.
businessCategory	The type of business in which the entry is engaged.
janetMailbox	An email address that can be used by a U.K. user
otherMailbox	The value of an email box type other than X.400 and RFC822.
mobile (mobileTelephoneNumber)	A mobile telephone number.
pager (pagerTelephoneNumber)	A pager number.
organizationalStatus	A category by which the user is often referred to in an organization.
mailPreferenceOption	Environment information indicating whether the user name should be included on a mailing list.
personalSignature	A signature file.

pkiCA

Definition

Define PKICA information. This object class is defined in RFC2587.

OID

2.5.6.22

Base Class

top

Type

AUXILIARY

Optional Attributes

authorityRevocationList	A list of revoked certificate authorities.
certificateRevocationList	A list of revoked user certificates.
cACertificate	A CA certificate.
crossCertificatePair	A cross certificate.

pkiUser

Definition

Define PKI user information. This object class is defined in RFC2587.

OID

2.5.6.21

Base Class

top

Type

AUXILIARY

Optional Attributes

userCertificate	A user certificate.

[Q]

qualityLabelledData

Definition

Define permission information for a DIT subtree.

OID

0.9.2342.19200300.100.4.22

Base Class

top

Type

AUXILIARY

Required Attributes

dsaQuality	The quality of a DSA.

Optional Attributes

subtreeMinimumQuality	The minimum data quality in a DIT subtree.
subtreeMaximumQuality	The maximum data quality in a DIT subtree.

[R]

residentialPerson

Definition

Define a person’s residential information. This object class is defined in RFC2256.

OID

2.5.6.10

Base Class

person

Type

STRUCTURAL

Required Attributes

l (localityName)	A related country, city, or other geographical area.

Optional Attributes

businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
preferredDeliveryMethod	The preferred method of contact or message delivery.
telexNumber	A telex number.
teletexTerminalIdentifier	The identifier of a telex terminal.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.

RFC822localPart

Definition

Define an entry that specifies the local part of an RFC822 email address. This object class is defined in RFC2256.

OID

0.9.2342.19200300.100.4.14

Base Class

domain

Type

STRUCTURAL

Optional Attributes

cn (commonName)	A common name or full name.
sn (surname)	A family name or last name.
description	The description of the entry.
seeAlso	The DN information related to this entry.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
postalAddress	A postal address.
postalCode	A postal code.
postOfficeBox	A post-office box.
street (streetAddress)	The building name and street number of the entry.
facsimileTelephoneNumber (fax)	A FAX number.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
telexNumber	A telex number.
teletexTerminalIdentifier	The identifier of a telex terminal.
preferredDeliveryMethod	The preferred method of contact or message delivery.
destinationIndicator	The address information required to provide the telegram service.
registeredAddress	A registered emergency contact address.
x121Address	The x121 address of the user.

room

Definition

Define a room.

OID

0.9.2342.19200300.100.4.7

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

roomNumber	The room number of the object.
description	The description of the entry.
seeAlso	The DN information related to this entry.
telephoneNumber	A telephone number.

[S]

simpleSecurityObject

Definition

Define simple security. This is used if the main object class does not have the attribute 'userPassword'. This object class is defined in RFC2256.

OID

0.9.2342.19200300.100.4.19

Base Class

top

Type

AUXILIARY

Required Attributes

userPassword	A related country, city, or other geographical area.

ssoResource

Definition

Define the resource information for SSO.

OID

1.2.392.200001.65.1.8.6.4

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

ssoRoleName	The role to which the user belongs or a role that can access a resource, etc.
ssoUserAttribute	An attribute name to be notified to a Web application.

ssoRole

Definition

Define role information for SSO.

OID

1.2.392.200001.65.1.8.6.1

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

ssoAuthType	An authentication type necessary to give the user or the role.

ssoRoleSet

Definition

Define a set of roles for SSO.

OID

1.2.392.200001.65.1.8.6.2

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

ssoRoleName	The role to which the user belongs or a role that can access a resource, etc.

ssoSite

Definition

Define the site information for SSO.

OID

1.2.392.200001.65.1.8.6.3

Base Class

top

Type

AUXILIARY

Optional Attributes

ssoPortNumber	A port number.

ssoUser

Definition

Define the user information for SSO.

OID

1.2.392.200001.65.1.8.6.0

Base Class

top

Type

AUXILIARY

Optional Attributes

ssoRoleName	The role to which the user belongs or a role that can access a resource, etc.
ssoAuthType	An authentication type necessary to give the user or the role.
ssoCredentialTTL	The validity period of a credential.
ssoUserStatus	Used to manage the user's lock status.
ssoNotBefore	The date and time at which the user becomes valid.
ssoNotAfter	The date and time at which the user becomes invalid.
ssoFailureCount	The maximum number of password authentication retries before the system is locked.
ssoLockTimeStamp	The time at which the system locks because the password authentication failed consecutively more than the specified number of times.
dnQualifier	A DN prefix.

strongAuthenticationUser

Definition

Define a strong authentication user. This object class is defined in RFC2256.

OID

2.5.6.15

Base Class

top

Type

AUXILIARY

Required Attributes

userCertificate	A user certificate.

[T]

top

Definition

Used as a base class for all the objects.

OID

2.5.6.0

Type

ABSTRACT

Optional Attributes

objectClass	An object.

[U]

uidObject

Definition

Define a UID object. This object class is defined in RFC2377.

OID

1.3.6.1.1.3.1

Base Class

top

Type

AUXILIARY

Required Attributes

uid (userid)	A user ID.

userSecurityInformation

Definition

Define user security information. This object class is defined in RFC2256.

OID

2.5.6.18

Base Class

top

Type

AUXILIARY

Optional Attributes

supportedAlgorithms	The name of a supported algorithm.

Appendix D

Smart Repository Attributes

This appendix describes the attributes that can be used in Smart Repository.

For the meanings of matching rules and attribute syntax, see "Matching Rules" and "Attribute Syntax" in "Attribute Definitions" in "Schemata That Can Be Used in Smart Repository."

Comparison and collation can only be carried out on attributes for which matching rules are described.

[A]

aRecord

associatedDomain

associatedName

audio

authorityRevocationList

[B]

buildingName

businessCategory

[C]

c (countryName)

cACertificate

carLicense

certificateRevocationList

cn (commonName)

cNAMERecord

co (friendlyCountryName)

corbaIor

corbaRepositoryId

crossCertificatePair

[D]

dc (domainComponent)

deltaRevocationList

departmentNumber

description

destinationIndicator

displayName

distinguishedName

dITRedirect

dmdName

dnQualifier

documentAuthor

documentIdentifier

documentLocation

documentPublisher

documentTitle

documentVersion

drink (favoriteDrink)

[E]

email (emailAddress) (pkcs9email)

employeeNumber

employeeType

[F]

facsimileTelephoneNumber (fax)

[G]

generationQualifier

givenName (gn)

[H]

homePhone (homeTelephoneNumber)

homePostalAddress

host

houseIdentifier

[I]

info

initials

internationaliSDNNumber

[J]

janetMailbox

javaClassName

javaClassNames

javaCodebase

javaDoc

javaFactory

javaReferenceAddress

javaSerializedData

jpegPhoto

[K]

knowledgeInformation

[L]

l (localityName)

labeledURI

[M]

mail (rfc822Mailbox)

mailPreferenceOption

manager

mDRecord

member

mobile (mobileTelephoneNumber)

mXRecord

[N]

name

nSRecord

[O]

o (organizationName)

objectClass

organizationalStatus

otherMailbox

ou (organizationalUnit)

owner

[P]

pager (pagerTelephoneNumber)

personalTitle

physicalDeliveryOfficeName

postalAddress

postalCode

postOfficeBox

preferredLanguage

[R]

registeredAddress

roleOccupant

roomNumber

[S]

secretary

seeAlso

serialNumber

singleLevelQuality

sn (surname)

sOARecord

ssoAuthType

ssoCredentialTTL

ssoFailureCount

ssoLockTimeStamp

ssoNotAfter

ssoNotBefore

ssoPortNumber

ssoRoleName

ssoUserAttribute

ssoUserStatus

st (stateOrProvinceName)

street (streetAddress)

subtreeSpecification

supportedAlgorithms

supportedApplicationContext

[T]

telephoneNumber

telexNumber

textEncodedORAddress

title

[U]

uid (userid)

uniqueIdentifier

uniqueMember

userCertificate

userClass

userPassword

userPKCS12

userSMIMECertificate

[X]

x121Address

x500UniqueIdentifier

List of Attributes

[A]

aRecord

Definition

Set an Address DNS resource.

OID

0.9.2342.19200300.100.1.26

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

associatedDomain

Definition

Set a DNS domain related to a DIT object. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.37

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String

associatedName

Definition

Set an entry in the organizational DIT entry related to a DNS domain. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.38

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

audio

Definition

Set a sound file.

OID

0.9.2342.19200300.100.1.55

Attribute Syntax

Audio,binary

Note

If this attribute is registered, ";binary" does not need to be added.

Maximum Length

250000

authorityRevocationList

Definition

Set a list of revoked certificate authorities. This attribute is defined in RFC2256.

OID

2.5.4.38

Attribute Syntax

Certificate List

Note

If this attribute is registered, ";binary" does not need to be added.

[B]

buildingName

Definition

Set the name of a building. This attribute is defined in RFC3112.

OID

0.9.2342.19200300.100.1.48

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

businessCategory

Definition

Set the type of business in which the entry is engaged. This attribute is defined in RFC2256.

OID

2.5.4.15

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

128

[C]

c (countryName)

Definition

Set a two-character code defined by ISO to indicate a country name in the directory. This attribute is defined in RFC2256.

For example, set the two-character code for Japan as follows:

countryName: jp or c: jp

OID

2.5.4.6

Attribute Syntax

single-valued

Base Attribute

name

cACertificate

Definition

Set a CA certificate. This attribute is defined in RFC2256.

OID

2.5.4.37

Attribute Syntax

Certificate, binary

Note

If this attribute is registered, ";binary" does not need to be added.

carLicense

Definition

Set an automobile license plate number. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.1

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

certificateRevocationList

Definition

Set a list of revoked user certificates. This attribute is defined in RFC2256.

OID

2.5.4.39

Attribute Syntax

Certificate List, binary

Note

If this attribute is registered, ";binary" does not need to be added.

cn (commonName)

Definition

Set a common name or full name. This attribute is defined in RFC2256.

OID

2.5.4.3

Base Attribute

name

cNAMERecord

Definition

Set the proper name of a DNS resource. This attribute is defined in RFC2256.

OID

0.9.2342.19200300.100.1.31

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

co (friendlyCountryName)

Definition

The country attribute is used to show the two-character country code and "friendlyCountryName" attribute.

OID

0.9.2342.19200300.100.1.43

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

corbaIor

Definition

Set a character string representation for an IOR of a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.1.14

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String, single-valued

corbaRepositoryId

Definition

Set a repository ID implemented by a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.1.15

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

crossCertificatePair

Definition

Set a cross certificate. This attribute is defined in RFC2256.

OID

2.5.4.40

Attribute Syntax

Certificate Pair

Note

If this attribute is registered, ";binary" does not need to be added.

[D]

dc (domainComponent)

Definition

Set a DNS domain. This attribute is defined in RFC1274/2247.

OID

0.9.2342.19200300.100.1.25

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String, single-valued

deltaRevocationList

Definition

Set a list of revoked deltas. This attribute is defined in RFC2256.

OID

2.5.4.53

Attribute Syntax

Certificate List, binary

Note

If this attribute is registered, ";binary" does not need to be added.

departmentNumber

Definition

Set a department number. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.2

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

description

Definition

Set the description of the entry. This attribute is defined in RFC2256.

OID

2.5.4.13

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

1024

destinationIndicator

Definition

Set the address information required for the telegram service. This attribute is defined in RFC2256.

OID

2.5.4.27

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Printable String

Maximum Length

128

displayName

Definition

Set the display name of the entry. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.241

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String, single-valued

distinguishedName

Definition

Set an entry DN (distinguished name).

The following is an example.

Example: dn: cn=user001,o=User,ou=interstage,o=fujitsu,dc=com

OID

1.3.6.1.4.1.1466.115.121.1.12

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

dITRedirect

Definition

Set this attribute when a person gets a new organization DN by, for example, starting work at a new workplace.

The following is an example.

Example: ditRedirect: cn=user001,o=User,ou=interstage,o=fujitsu,dc=com

OID

0.9.2342.19200300.100.1.54

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

dmdName

Definition

Set the administration permission required to operate a directory management domain (DMD) and a directory server. This attribute is defined in RFC2256.

OID

2.5.4.54

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

dnQualifier

Definition

Set a DN prefix. This attribute is defined in RFC2256.

OID

2.5.4.46

Matching Rules

Equality: caseIgnoreMatch

Ordering: caseIgnoreOrderingMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Printable String

documentAuthor

Definition

Set the DN (distinguished name) of the document author. This attribute is defined in RFC1274.

As the attribute value, set the DN of the document author. The following is an example.

Example: documentAuthor: cn=Taro Fujitsu, o=User,ou=interstage,o=fujitsu,dc=com

OID

0.9.2342.19200300.100.1.14

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

documentIdentifier

Definition

Set the unique identifier of a document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.11

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

documentLocation

Definition

Set the location of the original copy of a document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.15

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

documentPublisher

Definition

Set the user or organization that published the document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.56

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

documentTitle

Definition

Set the title of the document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.12

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

documentVersion

Definition

Set the version of the document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.13

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

drink (favouriteDrink)

Definition

Set a favorite drink. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.5

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

[E]

email(emailAddress)(pkcs9email)

Definition

Set the email address of a DN. This attribute is defined in RFC2459.

OID

1.2.840.113549.1.9.1

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String

Maximum Length

128

employeeNumber

Definition

Set an employee number. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.3

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String, single-valued

Maximum Length

256

employeeType

Definition

Set an employment type. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.4

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

[F]

facsimileTelephoneNumber(fax)

Definition

Set a FAX number. This attribute is defined in RFC2256.

OID

2.5.4.23

Attribute Syntax

Facsimile Telephone Number

[G]

generationQualifier

Definition

Set the generation information of the name. This attribute is defined in RFC2256.

OID

2.5.4.44

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

givenName(gn)

Definition

Set a given name or first name. This attribute is defined in RFC2256.

OID

2.5.4.42

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

[H]

homePhone(homeTelephoneNumber)

Definition

Set a home telephone number. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.20

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

homePostalAddress

Definition

Set a home address. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.39

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Postal Address

host

Definition

Set the host name of the computer. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.9

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

houseIdentifier

Definition

Set the identifier of a house. This attribute is defined in RFC2256.

OID

2.5.4.51

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

32768

[I]

info

Definition

Set general information. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.4

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

2048

initials

Definition

Set initials. This attribute is defined in RFC2256.

OID

2.5.4.43

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

internationaliSDNNumber

Definition

Set an international ISDN number. This attribute is defined in RFC2256.

OID

2.5.4.25

Matching Rules

Equality: numericStringMatch

Substr: numericStringSubstringsMatch

Attribute Syntax

Numeric String

Maximum Length

36

[J]

janetMailbox

Definition

Set an email address that can be used by a U.K. user. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.46

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String

Maximum Length

256

javaClassName

Definition

Set a Java class name or interface name.

OID

1.3.6.1.4.1.42.2.27.4.1.6

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String, single-valued

javaClassNames

Definition

Set the class name of an object factory that can be used to create an instance of an object identified using the JavaClassName attribute.

OID

1.3.6.1.4.1.42.2.27.4.1.13

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

javaCodebase

Definition

Set the URL specifying the location of a class definition.

OID

1.3.6.1.4.1.42.2.27.4.1.7

Matching Rules

Equality: caseExactIA5Match

Attribute Syntax

IA5 String

javaDoc

Definition

Specify the JAVA document of a class.

OID

1.3.6.1.4.1.42.2.27.4.1.12

Matching Rules

Equality: caseExactIA5Match

Attribute Syntax

Directory String

javaFactory

Definition

Set the location used to load an object factory identified using the javaFactory attribute.

OID

1.3.6.1.4.1.42.2.27.4.1.10

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String, single-valued

javaReferenceAddress

Definition

Set the sequence of a JNDI reference address.

OID

1.3.6.1.4.1.42.2.27.4.1.11

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

javaSerializedData

Definition

Set Java serialized data.

OID

1.3.6.1.4.1.42.2.27.4.1.8

Attribute Syntax

Octet String, single-valued

jpegPhoto

Definition

Set a JPEG photo. This attribute is defined in RFC2798.

OID

0.9.2342.19200300.100.1.60

Attribute Syntax

JPEG

Note

If this attribute is registered, ";binary" does not need to be added.

[K]

knowledgeInformation

Definition

Set knowledge information. This attribute is defined in RFC2256.

OID

2.5.4.2

Matching Rules

Equality: caseIgnoreMatch

Attribute Syntax

Directory String

Maximum Length

32768

[L]

l (localityName)

Definition

Set a related country, city, or other geographical area. This attribute is defined in RFC2256.

OID

2.5.4.7

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

labeledURI

Definition

Set a Uniform Resource Identifier (URI). This attribute is defined in RFC2079.

OID

1.3.6.1.4.1.250.1.57

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

ldapSyntaxes

Definition

Set an LDAP attribute syntax. This attribute is defined in RFC2252.

OID

1.3.6.1.4.1.1466.101.120.16

Matching Rules

Equality: objectIdentifierFirstComponentMatch

Attribute Syntax

1.3.6.1.4.1.1466.115.121.1.54

[M]

mail (rfc822Mailbox)

Definition

Set an email address. This attribute is defined in RFC2252.

OID

0.9.2342.19200300.100.1.3

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String

Maximum Length

256

mailPreferenceOption

Definition

Set environment information indicating whether the user should be included on a mailing list. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.47

Attribute Syntax

INTEGER

manager

Definition

Set the distinguished name (DN) of a manager. This attribute is defined in RFC1274.

As the attribute value, set the DN of a manager. The following is an example.

Example: manager: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

0.9.2342.19200300.100.1.10

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

mDRecord

Definition

Set the MD record. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.27

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

member

Definition

Set the DN (distinguished name) of each member of a group. This attribute is defined in RFC2256.

As the attribute value, set the DN of a member to be included in a group. The following is an example.

Example: To include as a group member cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com, enter:

member: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.31

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

mobile(mobileTelephoneNumber)

Definition

Set a mobile telephone number. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.41

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

mXRecord

Definition

Set a Mail Exchange DNS resource.

OID

0.9.2342.19200300.100.1.28

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

[N]

name

Definition

Set the super type of an attribute used for naming. This attribute does not exist as a value in an entry.

OID

2.5.4.41

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

32768

nSRecord

Definition

Set a Name Server DNS resource.

OID

0.9.2342.19200300.100.1.29

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

[O]

o(organizationName)

Definition

Set an organization name. This attribute is defined in RFC2256.

OID

2.5.4.10

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

objectClass

Definition

Set an object class. This attribute is defined in RFC2256.

OID

2.5.4.0

Matching Rules

Equality: objectIdentifierMatch

Maximum Length

256

organizationalStatus

Definition

Set the category by which the user is typically referred to in an organization. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.45

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

otherMailbox

Definition

Set the value of an email box type other than X.400 and rfc822. This attribute is defined in RFC1274.

As the attribute value, set the value of an email box type. The following is an example.

Example: otherMailbox: internet $ user001@interstage.fujitsu.com

OID

0.9.2342.19200300.100.1.22

Attribute Syntax

Other Mailbox

ou(organizationalUnitName)

Definition

Set an organization unit name. This attribute is defined in RFC2256.

OID

2.5.4.11

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

owner

Definition

Set the DN (distinguished name) of a responsible person. This attribute is defined in RFC2256.

As the attribute value, set the distinguished name of a responsible person. The following is an example.

Example: owner: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.32

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

[P]

pager(pagerTelephoneNumber)

Definition

Set a pager number. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.42

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

personalTitle

Definition

Set a personal title. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.40

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

physicalDeliveryOfficeName

Definition

Set the name of the city, town, or village in which the office is located. This attribute is defined in RFC2256.

OID

2.5.4.19

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

128

postalAddress

Definition

Set a postal address. This attribute is defined in RFC2256.

OID

2.5.4.16

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreListSubstringsMatch

Attribute Syntax

Postal Address

postalCode

Definition

Set a postal code. This attribute is defined in RFC2256.

OID

2.5.4.17

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

40

postOfficeBox

Definition

Set a post-office box. This attribute is defined in RFC2256.

OID

2.5.4.18

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

40

preferredLanguage

Definition

Set a desired language. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.39

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String, single-valued

[R]

registeredAddress

Definition

Set a registered emergency contact address. This attribute is defined in RFC2256.

OID

2.5.4.26

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreListSubstringsMatch

Attribute Syntax

Postal Address

Base Attribute

postalAddress

roleOccupant

Definition

Set the DN (distinguished name) of the user acting in the role defined in the organizationalRole entry. This attribute is defined in RFC2256.

As the attribute value, set the DN of a user. The following is an example.

Example: roleOccupant: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.33

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

roomNumber

Definition

Set the room number of an object. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.6

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

[S]

secretary

Definition

Set the DN (distinguished name) of a secretary or assistant. This attribute is defined in RFC1274.

As the attribute value, set the DN of a secretary or assistant. The following is an example.

Example: secretary: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

0.9.2342.19200300.100.1.21

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

seeAlso

Definition

Set the DN information related to this entry. This attribute is defined in RFC2256.

As the attribute value, set the DN information. The following is an example.

Example: seeAlso: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.34

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

serialNumber

Definition

Set a serial number. This attribute is defined in RFC2256.

OID

2.5.4.5

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Printable String

Maximum Length

64

singleLevelQuality

Definition

Set the single level quality in the DIT. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.50

Attribute Syntax

Data Quality Syntax, single-valued

sn(surname)

Definition

Set a family name or last name. This attribute is defined in RFC2256.

OID

2.5.4.4

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

sOARecord

Definition

Specifies a type SOA (Start of Authority) DNS resource record.

OID

0.9.2342.19200300.100.1.30

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

ssoAuthType

Definition

It specifies an authentication type required for the user or the role.

OID

1.2.392.200001.65.1.8.4.1

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String, single-valued

Maximum Length

256

ssoCredentialTTL

Definition

Set the validity period of a credential.

OID

1.2.392.200001.65.1.8.4.2

Matching Rules

Equality: integerMatch

Attribute Syntax

INTEGER, single-valued

Maximum Length

8

ssoFailureCount

Definition

Set a number of times the password authentication can fail.

OID

1.2.392.200001.65.1.8.4.8

Matching Rules

Equality: integerMatch

Attribute Syntax

INTEGER, single-valued

Maximum Length

8

ssoLockTimeStamp

Definition

Set the time at which the system locks because the password authentication failed successively more than the permitted number of times.

OID

1.2.392.200001.65.1.8.4.9

Matching Rules

Equality: generalizedTimeMatch

Ordering: generalizedTimeOrderingMatch

Attribute Syntax

Generalized Time, single-valued

Maximum Length

64

ssoNotAfter

Definition

Set the date and time at which the user becomes invalid.

OID

1.2.392.200001.65.1.8.4.5

Matching Rules

Equality: generalizedTimeMatch

Ordering: generalizedTimeOrderingMatch

Attribute Syntax

Generalized Time, single-valued

Maximum Length

64

ssoNotBefore

Definition

Set the date and time at which the user becomes valid.

OID

1.2.392.200001.65.1.8.4.4

Matching Rules

Equality: generalizedTimeMatch

Ordering: generalizedTimeOrderingMatch

Attribute Syntax

Generalized Time, single-valued

Maximum Length

64

ssoPortNumber

Definition

Set a port number.

OID

1.2.392.200001.65.1.8.4.6

Matching Rules

Equality: integerMatch

Attribute Syntax

INTEGER, single-valued

Maximum Length

8

ssoRoleName

Definition

Set a role to which the user belongs or a role that can access a resource, etc.

OID

1.2.392.200001.65.1.8.4.0

Matching Rules

Equality: caseIgnoreMatch

Attribute Syntax

Directory String

Maximum Length

32

ssoUserAttribute

Definition

Set an attribute name to be notified to a Web application.

OID

1.2.392.200001.65.1.8.4.7

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

ssoUserStatus

Definition

Set the user's lock status.

OID

1.2.392.200001.65.1.8.4.3

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String, single-valued

Maximum Length

256

st(stateOrProvinceName)

Definition

Set the name of the state or province in which the entry is located. This attribute is defined in RFC2256.

OID

2.5.4.8

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

street(streetAddress)

Definition

Set the building name and block number of the entry. This attribute is defined in RFC2256.

OID

2.5.4.9

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

128

subtreeMaximumQualitymemo

Definition

Set the maximum data quality in a DIT subtree. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.52

Attribute Syntax

Data Quality Syntax, single-valued

subtreeSpecification

Definition

Set the data specifications in a DIT subtree. This attribute is defined in RFC1274.

OID

2.5.18.6

Attribute Syntax

Subtree Specification, single-valued

supportedAlgorithms

Definition

Set the name of a supported algorithm. This attribute is defined in RFC2256.

OID

2.5.4.52

Attribute Syntax

Supported Algorithm

Note

If this attribute is registered, ";binary" does not need to be added.

supportedApplicationContext

Definition

Set an OSI application context identifier. This attribute is defined in RFC2256.

OID

2.5.4.30

Matching Rules

Equality: objectIdentifierMatch

Attribute Syntax

OID

[T]

telephoneNumber

Definition

Set a telephone number. This attribute is defined in RFC2256.

OID

2.5.4.20

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

Maximum Length

32

telexNumber

Definition

Set a telex number. The telex number can be in the following format:

actual-number "$" country "$" answerback
In the above format, "actual-number" is the syntactic representation of the number portion of the telex number to be encoded, "country" the telex country code, and "answerback" is the answerback code of the telex terminal. This attribute is defined in RFC2256.

OID

2.5.4.21

Attribute Syntax

Telex Number

textEncodedORAddress

Definition

Set a text-encoded originator/recipient (X.400) address.

OID

0.9.2342.19200300.100.1.2

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

title

Definition

Set a title. This attribute is defined in RFC2256.

OID

2.5.4.12

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

[U]

uid (userid)

Definition

Set a user ID. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.1

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

uniqueIdentifier

Definition

Set a specific item used to differentiate two entries when a distinguished name has been reused. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.44

Matching Rules

Equality: caseIgnoreMatch

Attribute Syntax

Directory String

Maximum Length

256

uniqueMember

Definition

Set a group of names related to an entry where each name was given a uniqueIdentifier to ensure its uniqueness. This attribute is defined in RFC2256.

OID

2.5.4.50

Matching Rules

Equality: uniqueMemberMatch

Attribute Syntax

Name and Optional UID

userCertificate

Definition

Set a user certificate. This attribute is defined in RFC2256.

OID

2.5.4.36

Attribute Syntax

Certificate, binary

Note

If this attribute is registered, ";binary" does not need to be added.

userClass

Definition

Set the computer user category. This attribute is defined in RFC1274.

OID

2.5.4.36

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

userPassword

Definition

Set a user password. This attribute is defined in RFC2256/2307.

OID

2.5.4.35

Matching Rules

Equality: octetStringMatch

Attribute Syntax

Octet String

Maximum Length

128

userPKCS12

Definition

Set user PKCS#12. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.216

Attribute Syntax

Binary

Note

If this attribute is registered, ";binary" does not need to be added.

userSMIMECertificate

Definition

Set an S/MINE certificate. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.40

Attribute Syntax

Binary

Note

If this attribute is registered, ";binary" does not need to be added.

[X]

x121Address

Definition

Set a user X.121 address. This attribute is defined in RFC2256.

OID

2.5.4.24

Matching Rules

Equality: numericStringMatch

Substr: numericStringSubstringsMatch

Attribute Syntax

Numeric String

Maximum Length

15

x500UniqueIdentifier

Definition

Set to differentiate objects when a DN has been reused. This attribute is defined in RFC2256.

OID

2.5.4.45

Matching Rules

Equality: bitStringMatch

Attribute Syntax

Bit String

Appendix E

Search Filter

This appendix shows a search filter (based on RFC1558) that can be used by a Smart Repository client and provides an example of its use.

Search Filter Syntax

The syntax of the search filter is described in the following RFC documents:

- RFC1960 "A String Representation of LDAP Search Filters"
- RFC2254 "The String Representation of LDAP Search Filters"

Example

- Equal (=)

  Search for entries whose cn is User001.

```
cn=User001
```

- Greater (>=), less (<=)

  Search for entries whose dnQualifier is greater than 0.

```
dnQualifier>=0
```

- Present (=*)

  Search for all entries that contain cn.

```
cn=*
```

- Substring (string*)

  Search for entries whose cn begins with Fujitsu.

```
cn=Fujitsu*
```

- AND (&)

  Search for entries whose cn is User001 and whose sn is Fujitsu.

```
(&(cn=User001)(sn=Fujitsu))
```

- OR (|)

  Search for entries whose givenName is User001 or User002.

```
(|(givenName=User001)(givenName=User002))
```

Note

- When specifying a search filter, enclose it with double quotation marks.
- Up to two search conditions can be specified using OR.

  A search filter such as the one specified below is invalid.

```
(|(givenName=User001)(givenName=User002)(mail=*))
```

Specifying Special Characters

If any of the special characters listed below are specified values to be searched for in the search filter value, the character must be specified as a hexadecimal number after escaping it with "\" (backslash).

The following table lists the special characters that must be specified as a hexadecimal number:

Special character	Hexadecimal number
*	0x2a
(	0x28
)	0x29
\	0x5c

Note

To set "AB(C)" to the value of search filter, specify as follows:

```
(o=AB\28C\29)
```

Index