FUJITSU Software
Interstage Application Server

Single Sign-on Operator's Guide

Windows/Solaris/Linux

B1WS-1089-03ENZ0(00)
April 2014

Preface

Purpose of this Document

This manual describes the environment setup and operation procedures required for Interstage Single Sign-on (SSO) operation.

Note

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

Intended Readers

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

- Basic knowledge of the OS used
- The Internet
- SSL
- Apache
- Web Server
- LDAP and X.500
- Basic knowledge of Java application development using JAAS for Java application development
- Basic knowledge of Active Directory to use Active Directory Linkage

Structure of This Document

The structure of this manual is as follows:

Chapter 1 Overview

This chapter provides an outline and explanation of the concepts (including system configuration) and functions of Interstage Single Sign-on.

Chapter 2 Environment Setup (SSO Administrators)

This chapter explains how to set up the authentication infrastructure environment for Interstage Single Sign-on.

Chapter 3 Environment Setup (Business Server Administrators)

This chapter explains how to set up the business system environment that is needed for Interstage Single Sign-on.

Chapter 4 Operation and Maintenance

This chapter provides details on the operation and maintenance of Interstage Single Sign-on.

Chapter 5 Single Sign-on Customization

This chapter explains how to customize Interstage Single Sign-on.

Chapter 6 Troubleshooting

This chapter explains how to troubleshoot problems in Interstage Single Sign-on.

Chapter 7 Developing Applications

This chapter provides an explanation of the application interface provided by Interstage Single Sign-on. In addition, it also provides information on how to develop applications for Interstage Single Sign-on.

Appendix A Notes on Previous Versions

This appendix provides notes on using previous versions and the service ID file. In addition, it also details improved messages and session management.

Appendix B Samples of User Program Descriptions

This appendix provides samples of the user programs that are required to operate the SSO repository for Interstage Single Sign-on.

Appendix C Entry Attributes to be Registered in SSO Repository

This appendix provides user information, role configurations, and protection resources that are registered in the SSO repository, which are required for authentication and authorization for Interstage Single Sign-on.

Appendix D Preparations for SSL Communication

This appendix provides information on how to create an SSL communication environment, including notes on creating a certificate environment, preparing the repository, and registering certificates.

Appendix E Settings of the Load Balancer

This appendix provides the load balancer settings that are required when load balancing is used.

Appendix F Settings for Active Directory Linkage

This appendix provides information on the settings required for Active Directory linkage.

Appendix G Settings for Performing Certificate Authentication in a System that Performs Session Management

This appendix provides the environment configuration required for using certificate authentication in systems in which session management is performed.

Appendix H Prevention of Caching of Contents

This appendix outlines how the prevention of contents caching is the default security setting in Interstage Single Sign-on, and, where this causes problems (e.g. when file downloads are required), how to configure the environment so as to allow the caching of contents.

Appendix I Settings for Protection Resource in Authentication Server

This appendix provides notes and examples on setting up protection resource information, such as environment configuration files and configuration files.

Conventions

Representation of Platform-specific Information

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

Windows32	Indicates that this product (32-bit) is running on Windows.
Windows64	Indicates that this product (64-bit) is running on Windows.
Windows32/64	Indicates that this product (32/64-bit) is running on Windows.
Solaris32	Indicates that this product (32-bit) is running on Solaris.
Solaris64	Indicates that this product (64-bit) is running on Solaris.
Solaris32/64	Indicates that this product (32/64-bit) is running on Solaris.
Linux32	Indicates that this product (32-bit) is running on Linux.
Linux64	Indicates that this product (64-bit) is running on Linux.
Linux32/64	Indicates that this product (32/64-bit) is running on Linux.

Abbreviations

Read occurrences of the following Components as their corresponding Service.

Service	Component
CORBA Service	ObjectDirector
Component Transaction Service	TransactionDirector

Export Controls

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

Trademarks

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

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

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

Copyrights

April 2014 Third Edition

November 2012 First Edition

Contents

Chapter 1 Overview

This chapter provides an outline and description of the functions in the Interstage Single Sign-on (SSO) application.

1.1 What Is Single Sign-on

A business information system uses multiple Web Servers together. Users usually need to enter the each their ID and password for Web server

The Single Sign-on function enables the user to obtain authorization to access multiple Web Servers by a single sign-on (Authentication) operation.

The Single Sign-on function provides an authentication and authorization infrastructure for multiple Web servers comprising an enterprise system.

Authentication

Authentication is the process used to verify the validity and identification of the person who uses the system.

Authorization

Authorization is the process used to make sure that the user who requests access to a resource is allowed to access that resource. It is to confirm that a user who requests access to a resource, for example, a HTML document, image data, voice data on a Web server, and a CGI application operating on a Web server is allowed to access the resource.

1.1.1 Problems in Conventional Systems

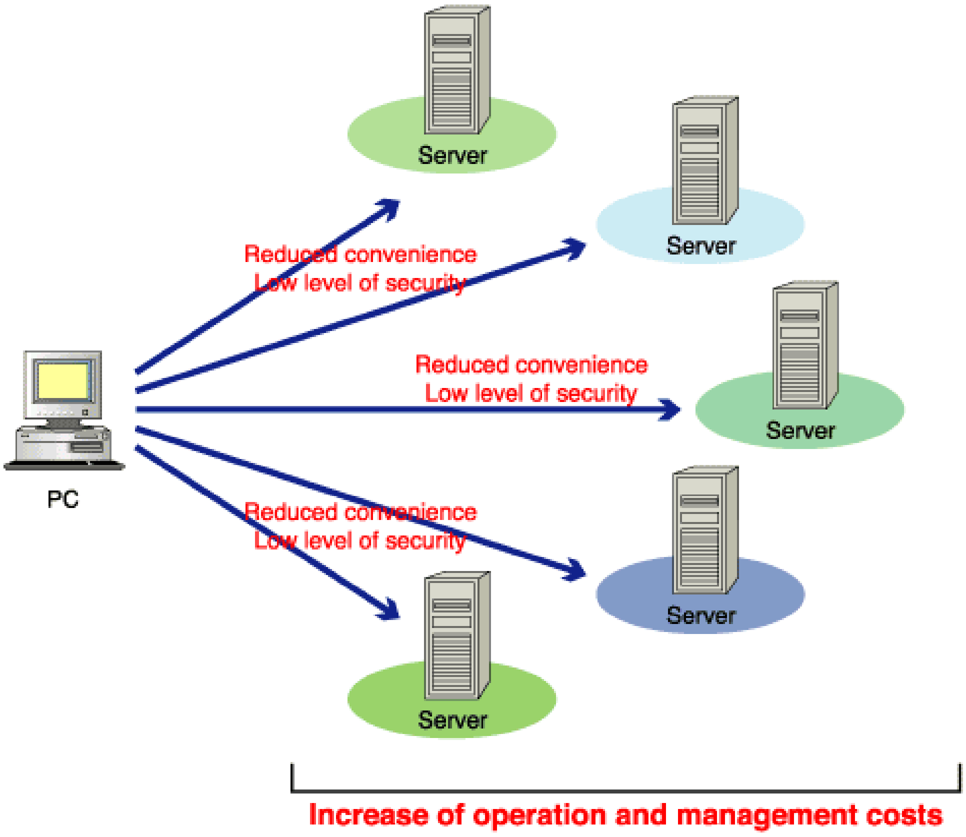
It is often stated that a company cannot fully adapt to changes in the market and grow unless their business information system is constructed on application servers based on Internet technology. This means that not all-in-one information systems are used, but the system that can be flexibility to adapt to changes is used by the construction on the Web servers adapted to needs and purposes of individual, and operation it integrally.

However, problems often occur in business information systems that use multiple Web servers.

User authentication is essential to business information systems, so conventional systems must supply Web servers with this functionality.

Common problems such as listed on the following page faced to system administrators and users.

Figure 1.1 Problems in Conventional Systems



Reduced User Convenience

Since each system has an authentication function, a user must be authenticated every time they use the system. User information (user ID and password) is also managed for each system and therefore user must enter the user ID and password for authentication of each system. The user must also memorize and manage the user ID and password for each system. These restrictions make users to be inconvenience to use and access system.

Increase of Operation Cost

Every time a user is added, changed, or deleted because of a personnel change (or for other reasons), the administrator for each individual system must perform maintenance on the associated user and access control details. This means that the cost and time required for management of this activity is quite significant.

Increase of Development Cost

Since a security function must be developed for each system, the time and costs required for this development increases.

Low Level of Security

The total security level of an information system that contains multiple subsystems is equivalent to the lowest security level of its subsystems. This means that even if a subsystem is equipped with an advanced security function based on the latest security architecture, the advanced security function only has an effect on the total system security when all other subsystems have been used within the advanced system.

1.1.2 Effects of Single Sign-on

Interstage Single Sign-on can solve the problems associated with conventional information systems.

Improving User Convenience

Each user can securely access various Web systems by using a single pair user ID and password.

Reduction of Operation Cost

The system management and maintenance that is required when users are added, changed, or deleted because of personnel changes can be integrated. This means that the associated costs for system management and maintenance can be reduced.

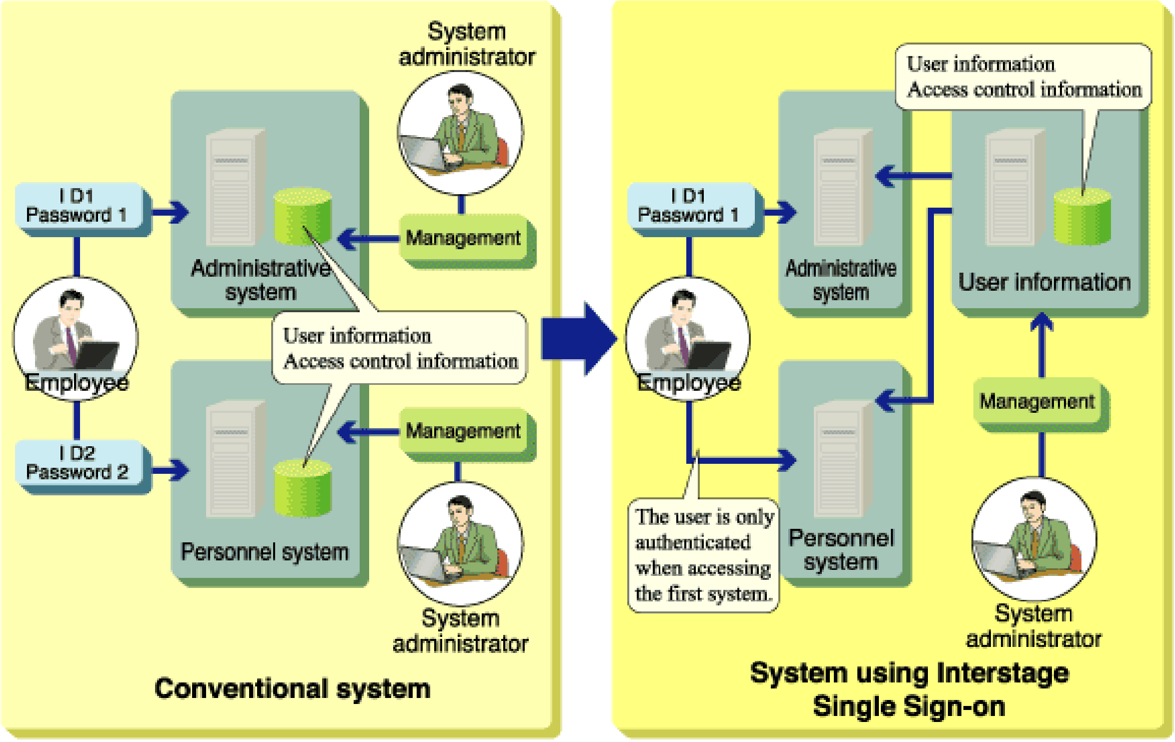
Reduction of Development Cost

The need for security function development for each system is also eliminated and this means that the associated development costs can be reduced.

Realization of High Security Level

The level of security can be increased using an integrated method and as a result the total system can utilize the latest security architecture that is available.

Figure 1.2 Comparison of a Conventional System and an Interstage Single Sign-on system

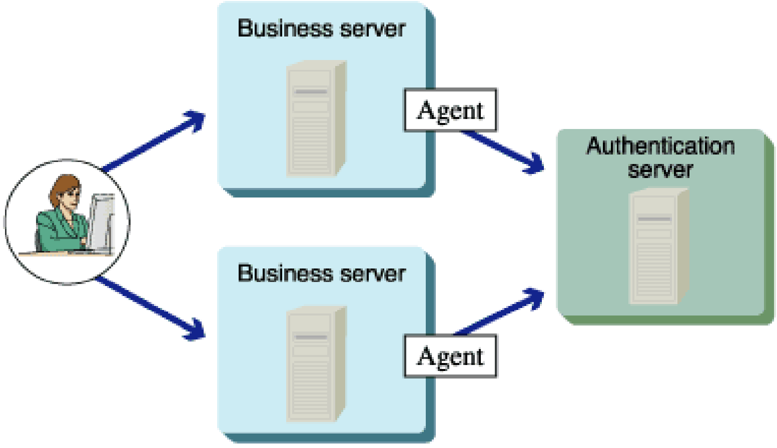


1.1.3 Implementation Method

Interstage Single Sign-on uses an implementation method called the "agent style" to implement the Single Sign-on.

The agent style locates an agent on each business server, where the necessity for user authentication is determined. When authentication is necessary, the authentication server is requested to perform authentication. The agent style also allows the original network configuration to be used after Interstage Single Sign-on is installed.

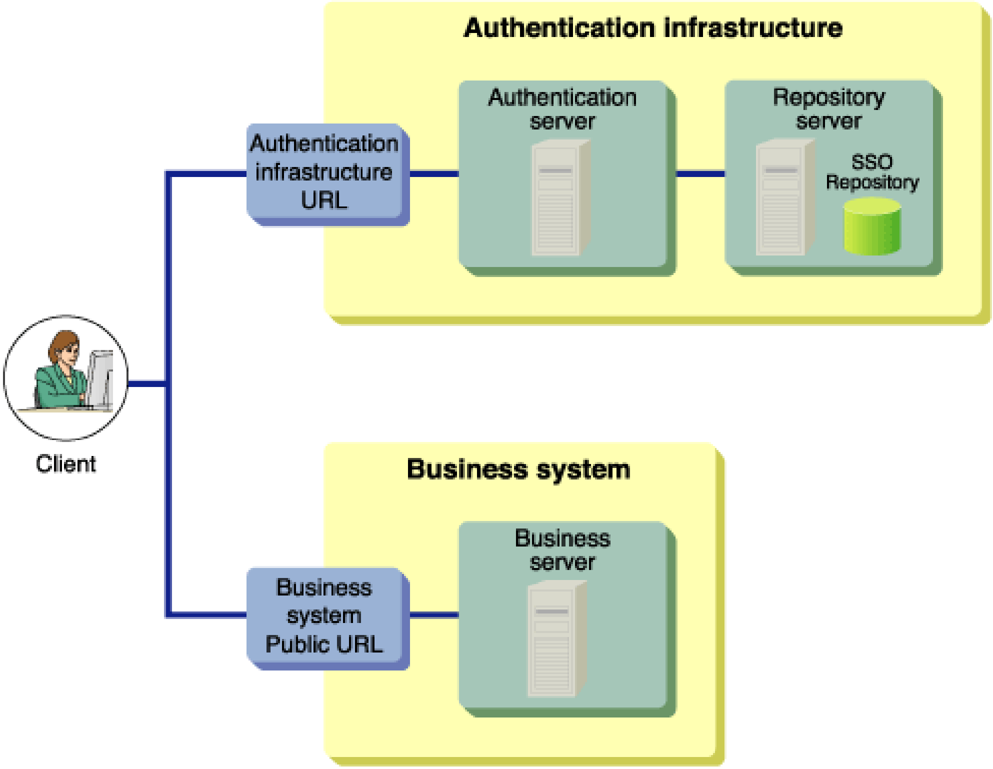
Figure 1.3 Implementation Method



1.2 Basic System Configuration

The Interstage Single Sign-on system basically consists of an authentication infrastructure, a business system, and clients. The authentication infrastructure has an authentication server, a repository server, and an SSO repository. The business system has a business server.

Figure 1.4 Basic System Configuration


Authentication infrastructure
Authentication infrastructure URL
Authentication server
Repository server
SSO Repository
Client
Business system
Business system Public URL
Business server

Users access the system from a Web browser on a client.

The user can use the system in the following two ways:

- Specifying the Authentication infrastructure URL through a Web browser

  Before accessing a business system, the user is authenticated by accessing the Authentication infrastructure URL through the Web browser. When authentication is successful, subsequent accesses to the business system are enabled.

- Specifying the Business system public URL through the Web browser

  The user accesses the business system through the Web browser without being aware of the authentication infrastructure.

  If the user accesses the business system without being authenticated, the Web browser is automatically directed to the Authentication infrastructure URL and requested to perform user authentication. When authentication is successful, the Web browser is automatically directed back to the URL specified first.

1.2.1 Authentication Infrastructure

The authentication infrastructure retains the user information required for authentication, and requests each user to present a pair of user ID and password to certificate and authenticate.

The authentication infrastructure consists of an authentication server, repository server, and SSO repository.

Note

All access to the Authentication infrastructure uses SSL communication. For details, refer to "Authentication infrastructure URL".

Authentication Server

The authentication server requests each user to present a pair of user ID and password or a certificate, and authenticate the user.

The authentication server compares the user ID and Password (or certificate presented by the user) with the user information previously set in the repository server to determine whether the user can use the Single Sign-on system.

Repository Server

The repository server manages the information necessary for user authentication, such as user IDs and passwords, and the information to authorize users to access the public URL path to the business system.

According to the request from the authentication server, the repository server fetches the user information necessary for authentication from the SSO repository. The fetched information is then transferred to the authentication server.

Two types of repository server are available: Repository server (update system) and repository server (reference system).

By placing a load balancer in front of the repository server (update system) and increasing the number of repository servers (update system), requests from the authentication server can be distributed and availability can be improved.

The repository server (reference system) is installed when system availability needs to be increased and a load balancer is not used. If the repository server (reference system) to which the authentication server requests authentication has failed, repository server (reference system) to the authentication request destination is switched automatically to respond to the authentication request from the relevant client.

SSO Repository

The SSO repository is a single directory used to control the information about all users of the operating system, and the resources associated with each business server.

For the SSO repository, Interstage Directory Service is used. For details on the Interstage Directory Service, refer to the "Directory Service Operator's Guide".

Active Directory can also be used as a directory service for registering user information. Refer to 'Linking to Active Directory' for more information.

Basic Configurations of Authentication Infrastructure

The following describes the basic configurations of the authentication infrastructure.

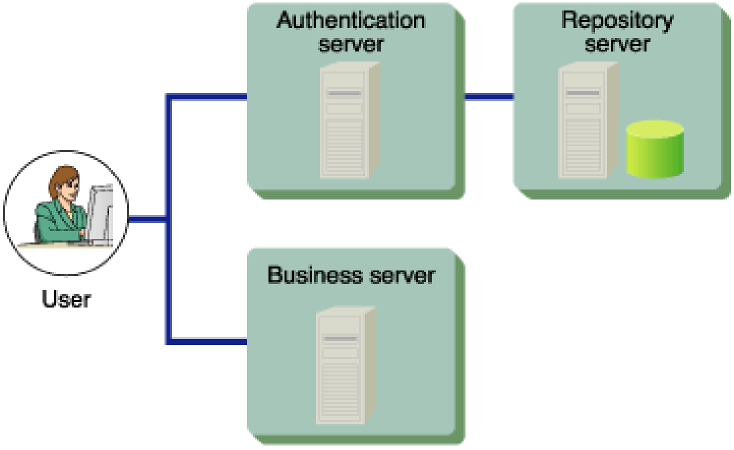
Six configuration patterns are supported to meet different system-scale requirements, e.g., load balancing and increase of system availability.

1. When Setting Up the Authentication Server on One Machine and the Repository Server on Another Machine (Middle-scale System)

This system configuration is suitable when the number of users in the business system and the number of simultaneous accesses to the business system are low in volume.

If the number of users within a business system increase and simultaneous access also increases, authentication servers can be added to change the system configuration in order to match the setup described in item 2 below.

Figure 1.5 Setting Up the Authentication on One Machine and the Repository Server on Another Machine (Middle Scale System)

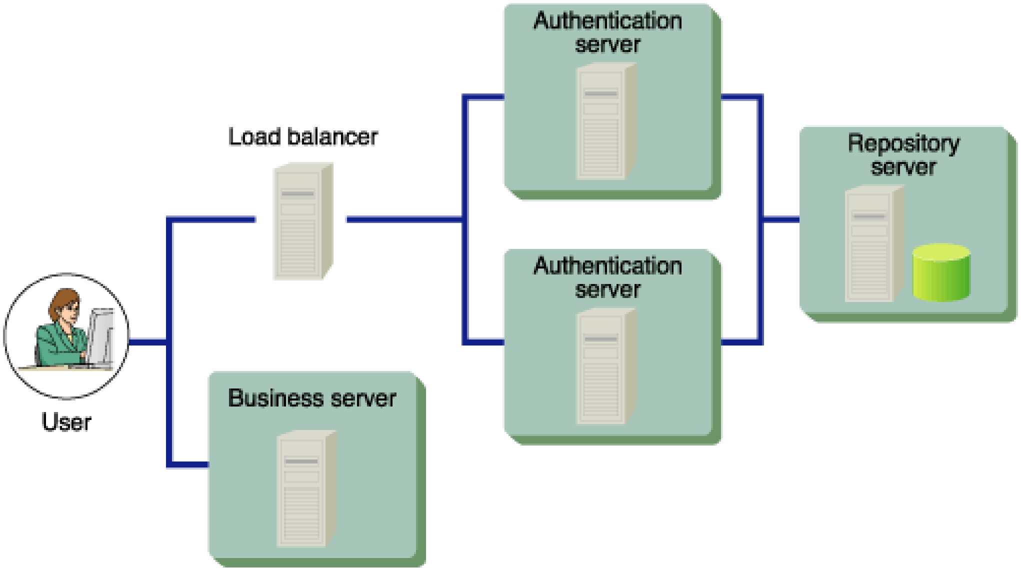


2. Setting Up the Authentication Server on Multiple Machines and the Repository Server on a Machine (Middle-scale System: Balancing the Authentication Server Load)

This configuration is suitable when the number of users of the business system and the volume of simultaneous access to that business system is large.

This system configuration places a load balancer before multiple authentication servers to balance the load of the authentication servers. Three or more authentication servers can be implemented.

Figure 1.6 Setting Up the Authentication Server on Multiple Machines and the Repository Server on a Machine (Middle Scale System- Balancing the Authentication Server Load)



3. Setting Up the Authentication Server on Multiple Machines and Increasing the Number of Machines on which the Repository Server (update system) is Installed (Large-scale System: Balancing the Repository Server (update system) Load)

This system configuration is suitable when the number of users in the business system and the number of simultaneous accesses to the business system are high, and you want to extend the system by increasing the number of machines on which the repository server (update system) is installed.

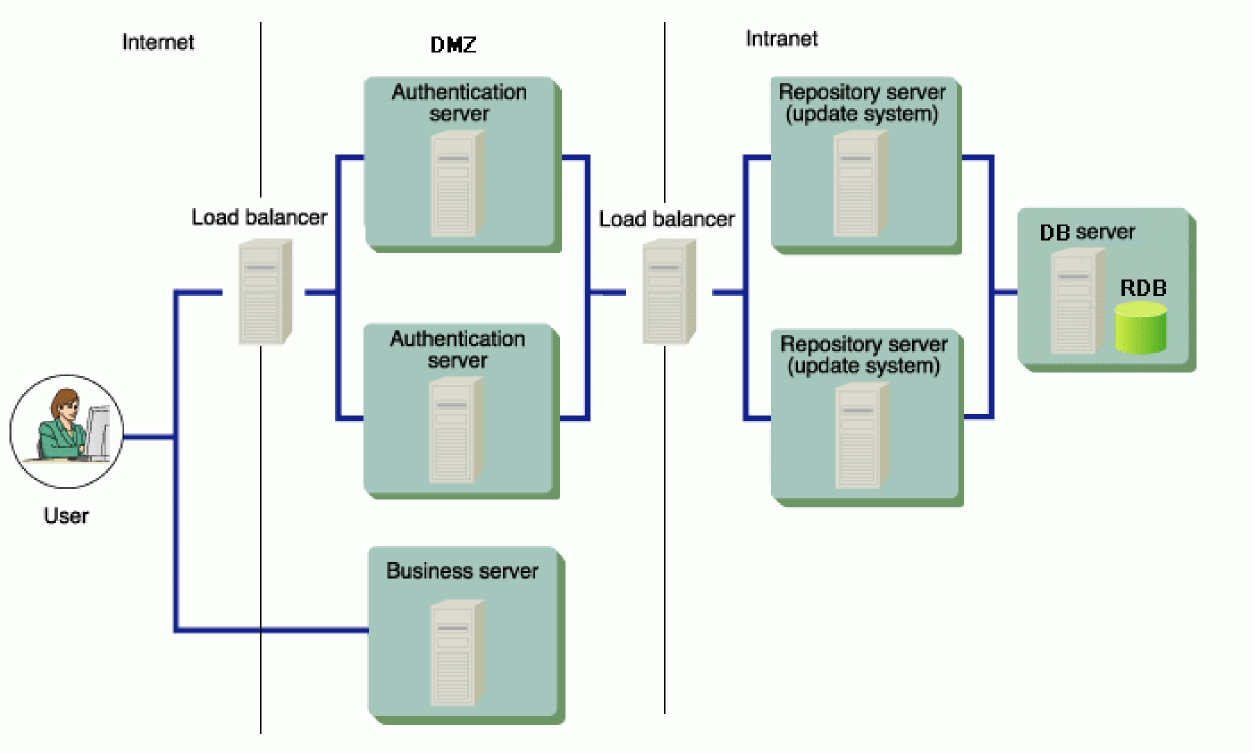
This system configuration places a load balancer between the authentication server and the repository server (update system). Since more than one repository server (update system) is installed, the load on the repository server (update system) is balanced from, for example, authentication requests and session evaluation from the authentication server.

More than three authentication servers and repository servers can be installed.

If this system configuration is used, the following type of SSO repository is required:

- An SSO repository that uses RDB as the database type.
- An SSO repository that uses a database that that can be shared.

Figure 1.7 Setting Up the Authentication Server on Multiple Machines and Increasing the Number of Machines on which the Repository Server (update system) is Installed



4. When Setting Up the Authentication Server and the Repository Server on Multiple Machines Individually (Large-scale System)

This system configuration has multiple repository servers that are used separately as update and reference systems. Multiple repository servers have been used in this setup in order to share and balance the processing load as needed.

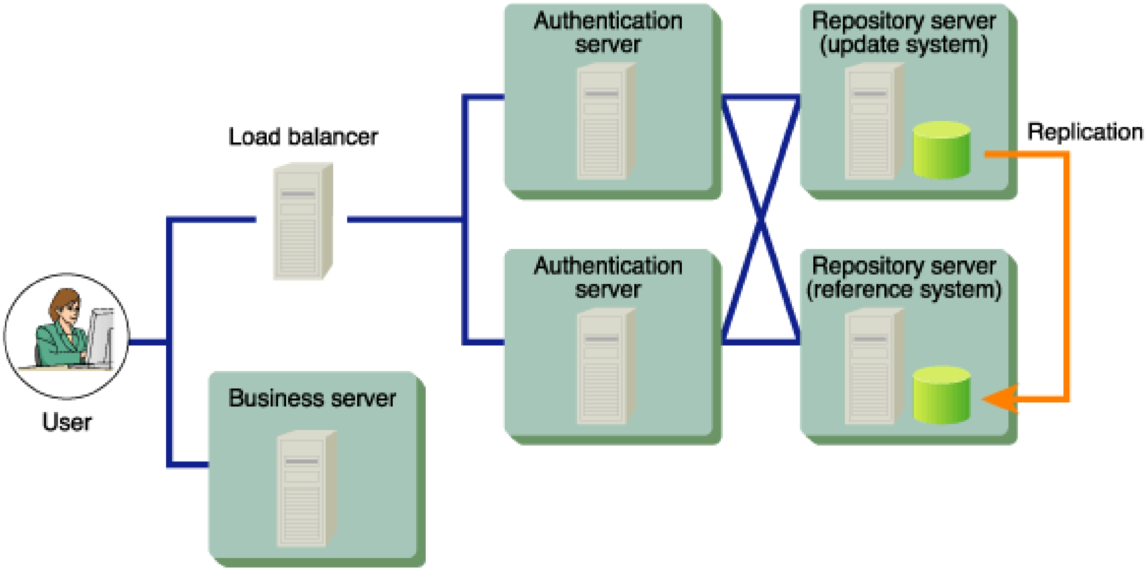
This system configuration positions a load balancer between the client and multiple authentication servers, to balance the load of the authentication servers. This configuration also uses multiple repository servers to balance the load on repository servers during authentication processing.

Multiple repository servers (reference systems) can be allocated for an authentication server. With multiple repository servers, even if a repository server (reference system) stops (fails), the system can continue operation by switching the repository server to another (reference system). A repository server (update system) can be also operated as a repository server (reference system). If a repository server (update system) stops (fails), the system is automatically stopped.

The information stored in the SSO repositories of update and reference systems must always be maintained to be the same status by the repository replication function.

Two or more repository servers (reference systems) can be installed.

Figure 1.8 Setting Up the Repository Server and Authentication Server on Multiple Machines Individually (Large Scale System)



5. Setting Up the Repository Server and Authentication Server on a Single Machine and Increasing the Number of Machines that are installed (Large-Scale System)

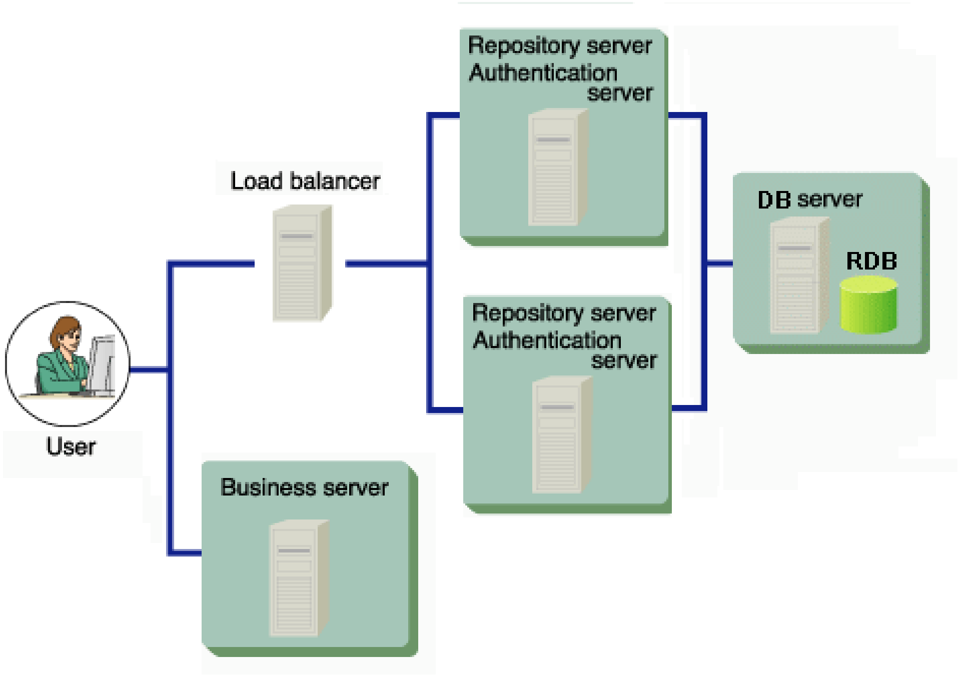
In this system configuration, the authentication infrastructure (repository server and authentication server) is set up on one machine, and because more than one machine is installed, the load on the repository server and authentication server is balanced. This system configuration is suitable for a large-scale system in which the number of users in the business system and the number of simultaneous accesses to the business system are high.

This system configuration places a load balancer before the authentication infrastructure (repository server and authentication server). More than three authentication servers and repository servers can be installed.

If this system configuration is used, the following type of SSO repository is required:

- An SSO repository that uses RDB as the database type.
- An SSO repository that uses a database that that can be shared.

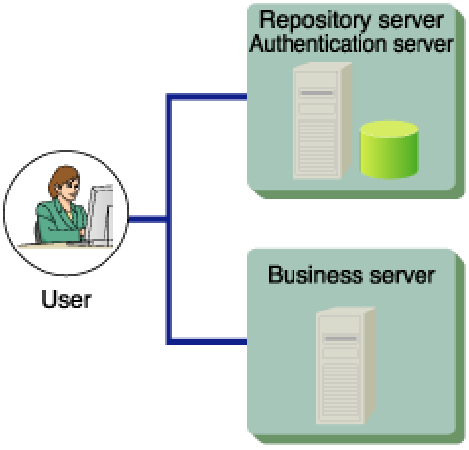
Figure 1.9 Setting Up the Repository Server and Authentication Server on a Single Machine and Increasing the Number of Machines that are installed (Large-Scale System)



6. Setting Up the Repository Server and the Authentication Server on a Single Machine (Small-scale System)

This system configuration sets up the authentication infrastructure (repository and authentication servers) on one machine. This configuration is suitable for a small-scale system in which the number of business system users and the number of simultaneous accesses to the business system are small.

Figure 1.10 Setting Up the Repository Server and Authentication Server on a Single Machine (Small Scale System)



1.2.2 Business System

The business system provides users with Web-based services.

The business system basically consists of a business server and Web Systems operated on the business server.

Business Server

In request for business system access from a user, the business server requests the authentication infrastructure in order to authenticate the user. At this point, the business server also authorizes the authenticated user to use the access-target services.

The business server that is available to add to the business system of Interstage Single Sign-on must be operated on the following Web servers.

Windows32/64

- Interstage HTTP Server
- Microsoft(R) Internet Information Services

Solaris32/64

- Interstage HTTP Server

Solaris32

- Sun Java System Web Server

Linux32/64

- Interstage HTTP Server

For details about Web servers that can be used as business servers, refer to "Web servers that incorporate a business server" in the chapter "Environment Setup (Business Server Administrators)".

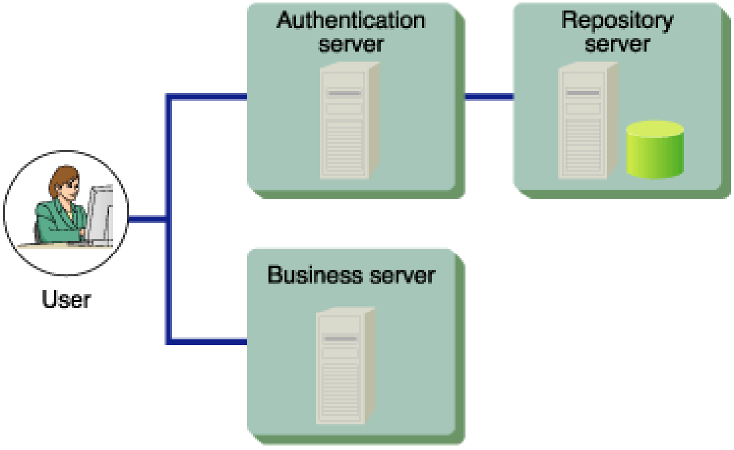
Basic Configurations of Business System

The following two configuration patterns are available for the business system.

1. When Setting Up a Business Server on a Machine

A business server is set up on a machine.

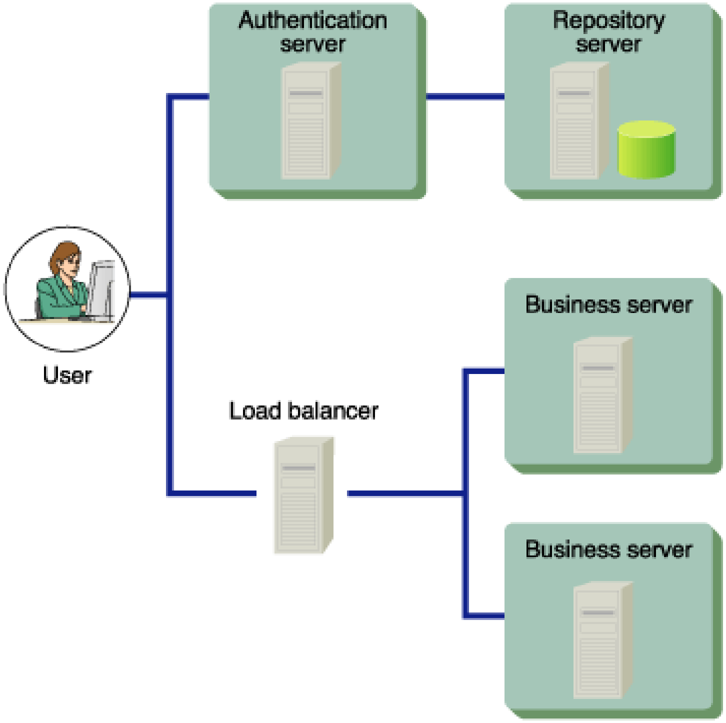
Figure 1.11 Setting Up a Business Server on a Machine



2. When Setting Up Business Servers on Multiple Machines

This system configuration positions a load balancer between the client and multiple business servers, to balance the load of the business servers. Three or more business servers can be implemented.

Figure 1.12 Setting Up Business Servers on Multiple Machines



1.2.3 Client

With Interstage Single Sign-on, a user uses the business system from a Web browser on a client.

Supported Web Browsers

The following table lists the Web browsers that can be used on the client.

Table 1.1 Supported Web Browsers

Web browser	Version and level
Windows(R) Internet Explorer(R)	7.0, 8.0, 9.0, 10.0
Mozilla(R) Firefox (*1)	3.0 to 3.6, 4.0, 5.0, 6.0, 7.0, 8.0, 9.0, 10.0, 11.0, 12.0, 13.0, 14.0, 15.0, 16.0, 17.0, 18.0, 19.0, 20.0, 21.0, 22.0, 23.0, 24.0

*1 Windows(R) is the only supported operating system.

Web Browser Setup

- Set up the browser to accept cookies.
- Validate Java scripts.
- When using proxy servers, set up the browser so that both authentication and business servers are connected through proxy servers.
- Set up the browser to use SSL3.0 and TLS1.0.

To use Integrated Windows Authentication, configure the settings so that Integrated Windows Authentication is used. (*1)
*1 Windows(R) Internet Explorer(R) will be the only target.

Registration with Web Browser for Certification Authority Certificate

Register the certificate of the CA that issued the site certificate in the Web browser. This site certificate is required for the use of SSL for communication with the authentication infrastructure. For details about how to register authentication certificate with the Web browser, refer to "Setting and Use of the Interstage Certificate Environment"-"Configuring Certificate Settings" in the "Security System Guide".

Application of Security Patch

The client system may be attacked and cookies may be stolen when a problem occurs in the Web browser being used. If such a trouble is detected, the developer of the Web browser releases a security patch. The system administrator must instruct all users of the operating system to always apply the latest security patches to their browsers.

About Proxy Servers

When a load balancer is used for load balancing, the proxy server through which a client is connected may be varied per access according to load balancer settings. Since the authentication and business servers recognize the proxy server address as the client address, if the proxy server is varied, the client address will be different between the access to the authentication server and the access to the business server.

If it occurs, the Single Sign-on operation cannot be validated. To avoid this problem, ensure the load balancer is set up so that access to the same client always uses the same proxy server.

For example, when "Balancing for each node" is specified for IPCOM, every request from the same client is connected to the same server.

Using Interstage Single Sign-on in more than one window

If Interstage Single Sign-on is used in more than one window, a window that is opened may inherit authentication information, depending on both the type of Web browser used and the way in which the window is opened.

If authentication information is inherited, the Web browser can use the new window without having to sign on again. However, if authentication information is not inherited, the Web browser must sign on again in order to use the new window that has been opened.

Using Basic Authentication in Windows(R) Internet Explorer(R)

If the Basic Authentication dialog for password authentication is canceled, and repeated operations result in the dialog being displayed continuously, authentication may fail. This is true even if the user ID/password that is entered is correct.

In this case, re-enter the correct user ID/password in the Basic Authentication dialog, and re-execute authentication.

1.3 Administrators

To operate Interstage Single Sign-on, the SSO (Single Sign-on) administrator must not only manage the authentication infrastructure but also coordinate with the administrator of the business server linked to Single Sign-on.

SSO Administrator

The SSO administrator manages the authentication infrastructure.

Based on the information obtained from the business server administrator, the SSO administrator registers users in the SSO repository, deletes users from the SSO repository or changes registered user information.

Business Server Administrator

The business server administrator manages the business system.

The business server administrator decides the resources to be protected by the business server and protection policies, including the criteria for the users who can access protected resources and delivers the information to register the business system in the authentication infrastructure to the SSO administrator. For details, refer to "Designing a Business System".

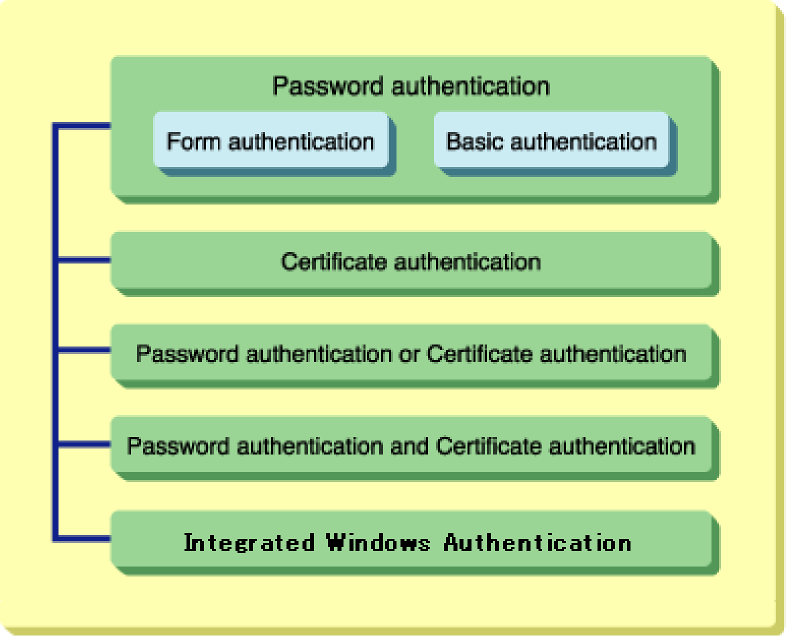
1.4 Authentication

Authentication is the operation used to check the validity of any person who attempts to use the system.

This section explains the authentication function provided with Interstage Single Sign-on.

Interstage Single Sign-on supports the following authentication methods for user authentication:

Figure 1.13 Authentication


Password authentication
Form authentication
Basic authentication
Certificate authentication
Password authentication or Certificate authentication
Password authentication and Certificate authentication
Integrated Windows Authentication

For details about Password authentication, Form authentication, Basic authentication, and Certificate authentication, refer to "Password and Certificate Authentication".

For details about "Password authentication or Certificate authentication" and "Password authentication and Certificate authentication", refer to "Combinations of Authentication Methods".

For details about "Integrated Windows Authentication", refer to "Integrated Windows Authentication".

Note

The following authentication can only be performed in systems in which session management is not used:

- Basic authentication
- Certificate authentication without an IC card

1.4.1 Password and Certificate Authentication

Interstage Single Sign-on supports the following two authentication methods for user authentication. Both methods can be used in combination.

- Password Authentication
- Certificate Authentication

Note

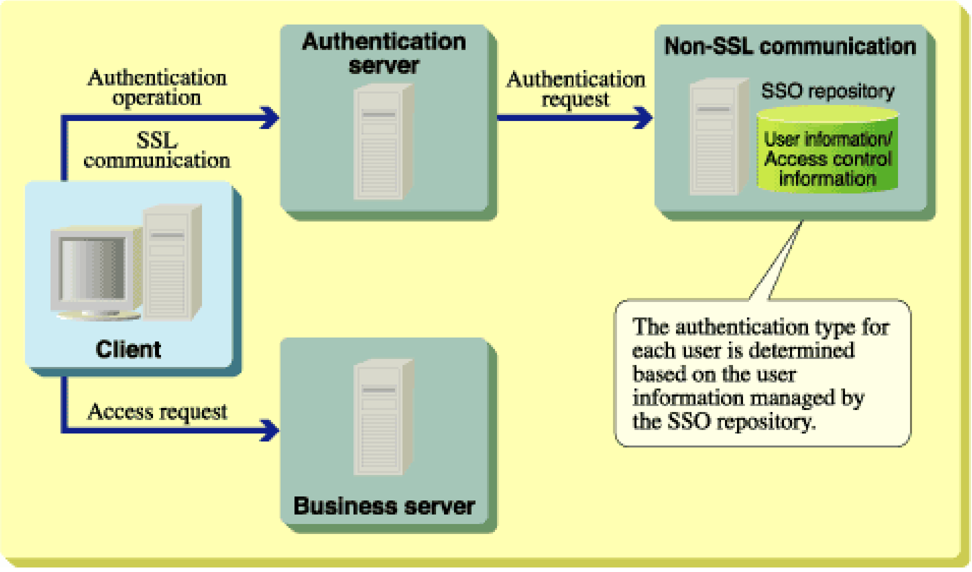
- Certificate authentication without an IC card can only be used in systems in which session management is not used.

With Interstage Single Sign-on, the two authentication methods can be specified separately or in combination for the resources as access control targets for each user.

The authentication method for a user is set according to ssoAuthType, a user information entry managed by the SSO repository of the repository server.

Also, a re-authentication interval can be specified for authentication. When a re-authentication interval is specified, an authenticated user is requested to be authenticated again after a specified time elapses from the first authentication. This function prevents unauthorized use of the Web system by a third person even if a user leaves the client computer for long after authentication.

Figure 1.14 Password and Certificate Authentication


Authentication server
Authentication operation
SSL communication
Authentication request
Non-SSL communication
SSO repository
User information/ Access control information
Client
Access request
Business server
The authentication type for each user is determined based on the user information managed by the SSO repository.

Password Authentication

Password authentication is the process used to authenticate a user via a paired user ID and password. This means that if a computer used by the user is undefined, the user can be easily authenticated.

Password authentication is simple, but there is a risk that a user's password could be stolen or spoofed. Take appropriate security measures when managing the password.

In Interstage Single Sign-on, the users enters their user ID and password in the form authentication page for password authentication

Table 1.2 Password Authentication

User ID/password input screen (*1)	Explanation	Written name in subsequent explanations
Form authentication page	Web page in which the authentication form is embedded	Form authentication
Basic authentication dialog	Standard authentication window of the Web browser	Basic authentication

*1 The Basic authentication dialog can only be used for input of the user ID/password in systems in which session management is not used. In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Environment Settings] > [Detailed Settings[Show]] > [Password Authentication Settings] and then set [Input User ID/Password].

When the user accesses the business system, the form authentication page appears for form authentication, and the basic authentication dialog appears for basic authentication. The user is prompted to enter the user ID and password.

Valid user ID and password pairs must be registered in the SSO repository beforehand. Only users who present a user ID and password pair that matches a valid registered pair are authenticated successfully.

If the form authentication is used, users can access the Authentication infrastructure URL directly through a Web browser for authentication, and users can also access the business system.

If users access the Authentication infrastructure directly, ask the user to access the following URL:

```
Authentication infrastructure URL/ssoatcag (*1)(*2)
```

In the following explanation, the URL above is replaced with "URL of Form authentication"

*1 Specify the port number of Authentication infrastructure URL even if 443 is specified.

*2 If the Authentication infrastructure URL is confirmed after setting the business server, on the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]], and then check the setting for [Authentication infrastructure URL] under [Authentication Infrastructure Information Settings].

Example

If Authentication infrastructure URL is used as "https://authserver.fujitsu.com", the URL of Form authentication page is the following:

```
https://authserver.fujitsu.com:443/ssoatcag
```

Note

If the incorrect URL is specified, the following error occurs and the authentication may fail.

- The following message outputs on the Web browser, even if authentication is performed. Or re-authentication is required.
  - Waiting
- If client authentication is processed through SSL communication, the request window of the client certificate is displayed several times.
- The following message is displayed on the Web browser, and output message: sso02012 to the system log.
  - "403 Not Found"
  - "The page cannot be displayed"

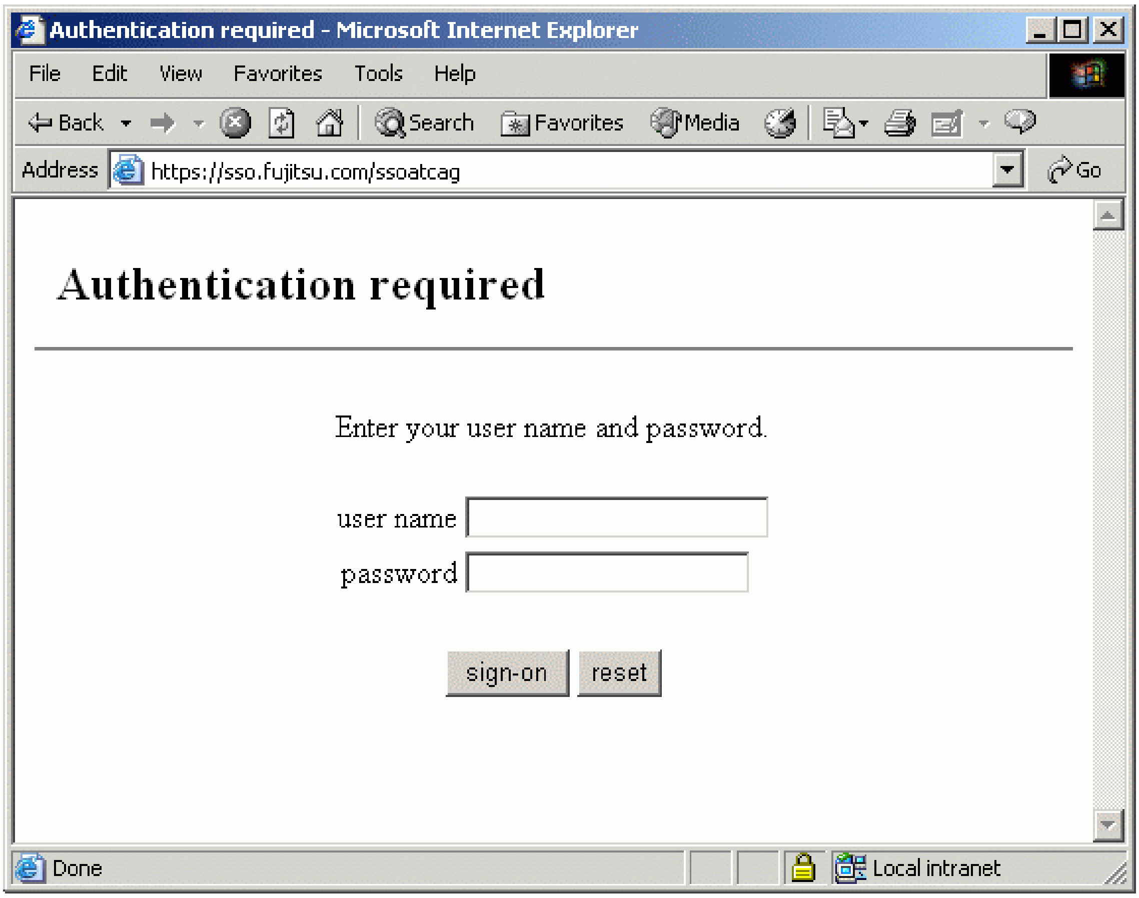
The following examples show the form authentication page and dialogs that are displayed by each Web browser for basic authentication.

Note that the User ID is treated as the User Name.

Example

An example of the form authentication page is shown below.

Figure 1.15 Form Authentication Page



https://sso.fujitsu.com/ssoatcag

Authentication required

Enter your user name and password.

user name

password

sign-on reset

The form authentication page can be customized. For details on how to customize the page, refer to "Customizing Messages Displayed on a Web Browser".

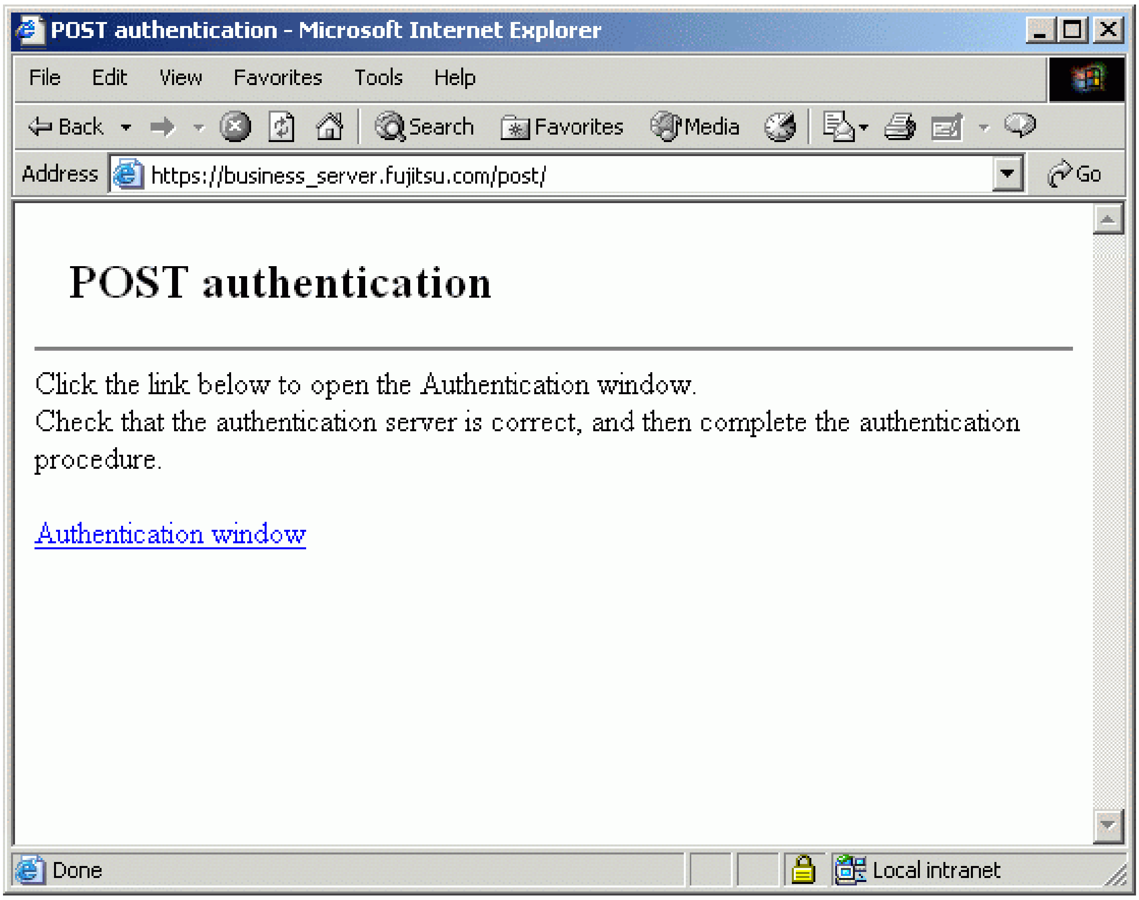
When a POST request is authenticated, the unauthenticated page displays. When the link that opens the authentication page is clicked, the authentication page is displayed in a new window. Authentication can be performed here.

The unauthenticated page can be customized. For customization method details, refer to "Customizing Messages Displayed on a Web Browser".

Example

An example of the Unauthenticated page is shown below.

Figure 1.16 Unauthenticated Page



POST authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://business_server.fujitsu.com/post/
Go
Done
Local intranet

POST authentication

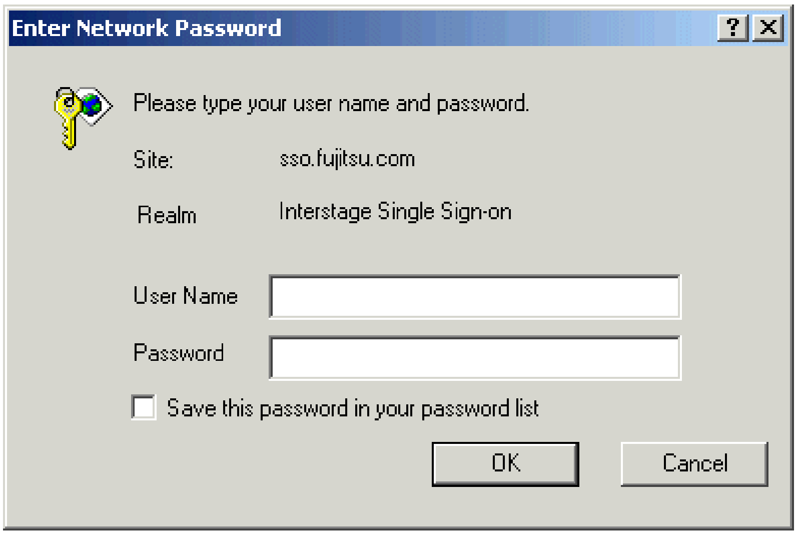
Click the link below to open the Authentication window.
Check that the authentication server is correct, and then complete the authentication procedure.

Authentication window

Example

Basic authentication dialog for Windows(R) Internet Explorer(R)

Figure 1.17 Authentication Window for Windows(R) Internet Explorer


Enter Network Password

Please type your user name and password.

Site: sso.fujitsu.com

Realm Interstage Single Sign-on

User Name

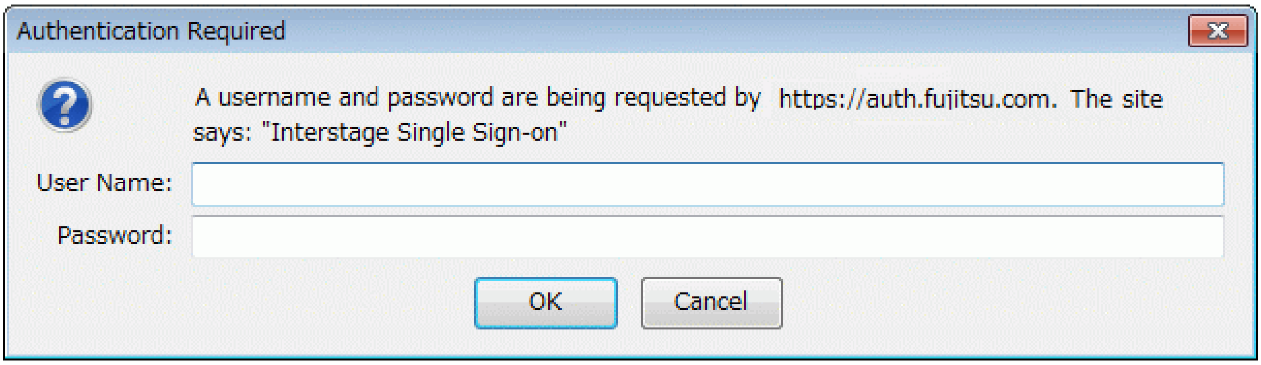
Password

□ Save this password in your password list

Example

Basic authentication dialog for Mozilla(R) Firefox

Figure 1.18 Authentication Window for Mozilla(R) Firefox


Authentication Required

A username and password are being requested by https://auth.fujitsu.com. The site says: "Interstage Single Sign-on"

User Name:

Password:

Note

If password authentication is being executed with basic authentication, a user cannot directly access the Authentication infrastructure URL using, for example, a Web browser.

Certificate Authentication

This authentication method is used to authenticate a user with a certificate. This method is convenient when the computer to be used is specified.

To use certificate authentication in a system where session management is used, settings must be made in the environment configuration file for the authentication server so that certificate authentication is allowed. Refer to "Settings for Performing Certificate Authentication in a System that Performs Session Management" for more information about these settings.

In systems in which session management is not used, authentication can be performed by registering the certificate in the Web browser used by the authenticated user. In this case, the presentation of the certificate is requested from the Web browser when the user accesses the business system or authentication infrastructure URL.

Note: Client authentication settings are required in the SSL environment settings in order for certificate authentication to be performed. For details on client authentication settings, refer to "2.4.1 SSL Communication Environment Setup".

Certificate Information

For certificate authentication by Interstage Single Sign-on, the owner name (Subject), owner alias (Subject Alternative Name) and extension information contained in the presented certificate is referenced. Therefore, one of the following items of information must be stored in the certificate.

Certificate information referenced by Interstage Single Sign-on

- Mail address (mail)
- Employee number (employeeNumber)
- User ID (uid)
- Serial number (serialNumber)
- DN qualifier (dnQualifier)
- Name (cn)

If same attribute is specified for the owner name (Subject), owner alias (Subject Alternative Name) and extension information contained in the presented certificate, the following is referenced.

- For Mail address, the value that is set in the owner alias (Subject Alternative Name) and extension information is valid.
- For except mail address, the value that set in the owner name (Subject) is valid.

To set the certificate information, such as owner name and owner alias, on the Interstage Management Console, select, [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]]. Then, make settings for [Attributes used for Authentication] under [Certificate Authentication Settings].

The following examples show the certificate selection windows that are displayed for certificate authentication in Web browsers. If multiple certificates have been registered in a Web browser, select the certificate on this window to be presented to the Web server.

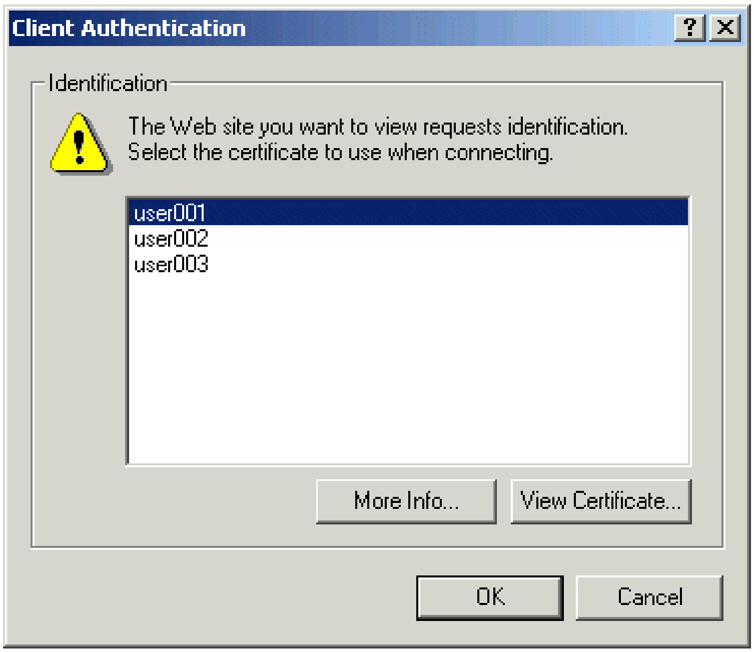
If only one certificate has been registered in a Web browser, the certificate can be used automatically without the certificate selection window displayed. For further details about how to display the certificate selection window, refer to "Certificate selection windows".

For details about how to register certificates in a Web browser, refer to the Security System Guide.

Example

Certificate selection window of Windows(R) Internet Explorer(R)

Figure 1.19 Certificate Selection Window for Windows(R) Internet Explorer(R)



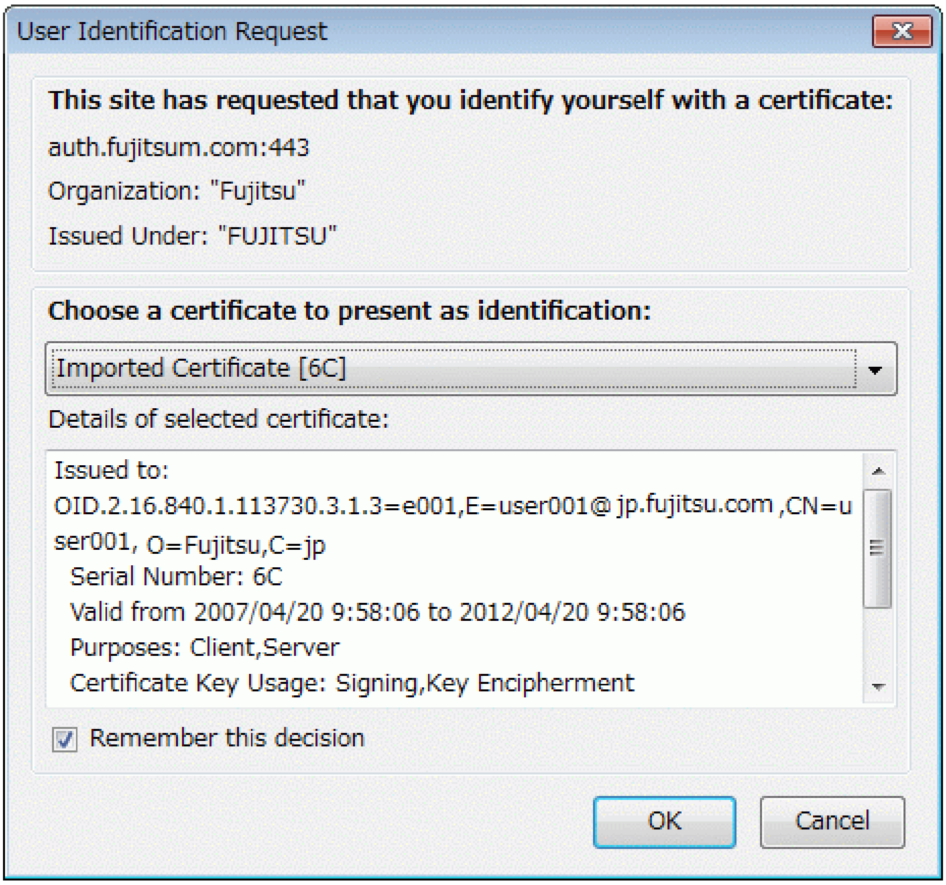
The Web site you want to view requests identification.
Select the certificate to use when connecting.

user001
user002
user003

Example

Certificate selection window of Mozilla(R) Firefox

Figure 1.20 Certificate Selection Window for Mozilla(R) Firefox



User Identification Request

This site has requested that you identify yourself with a certificate:

auth.fujitsum.com:443

Organization: "Fujitsu"

Issued Under: "FUJITSU"

Choose a certificate to present as identification:

Imported Certificate [6C]

Details of selected certificate:

Issued to: OID.2.16.840.1.113730.3.1.3=e001,E=user001@jp.fujitsu.com,CN=user001, O=Fujitsu,C=jp
Serial Number: 6C
Valid from 2007/04/20 9:58:06 to 2012/04/20 9:58:06
Purposes: Client,Server
Certificate Key Usage: Signing,Key Encipherment

☑ Remember this decision

Certificates Supported by Interstage Single Sign-on

Interstage Single Sign-on supports certificates that can be used in Interstage certificate environments and certificate/key management environments that use the SMEE commands.

Refer to the Security System Guide for more information.

Checking the Effectiveness of the Certificate

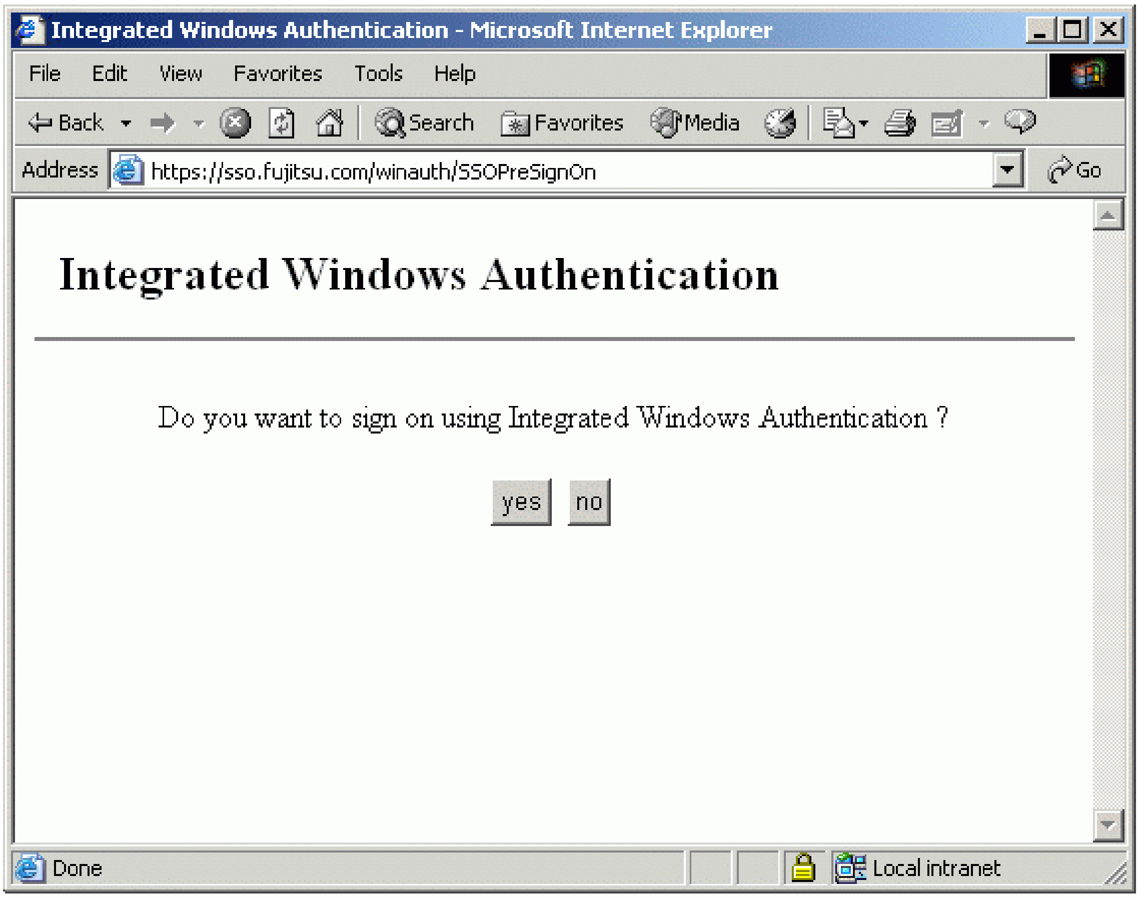
The certificate used for certificate authentication can be checked for effectiveness by the authentication server. The effectiveness is checked based on the certificate revocation list (CRL) registered in the authentication server. The CRL lists revoked certificates. If a certificate listed in the CRL is presented, then authentication fails.

1.4.2 Integrated Windows Authentication

In Integrated Windows Authentication, the user ID and password that were specified when the user logged on to Windows are used to authenticate the user. The user can therefore use Interstage Single Sign-on by logging on to Windows.

Following the Windows logon, the sign-on confirmation window of Integrated Windows Authentication shown below is displayed when the user accesses a protection resource via the user's Web browser.

With Integrated Windows Authentication, services can be used by clicking [Yes]. If the user does not sign on using Integrated Windows Authentication, it is still possible to perform operations that are authenticated using a password or certificate by clicking [No] in the following window. It is also possible to cancel Integrated Windows Authentication.



Integrated Windows Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.com/winauth/SSOPreSignOn
Go

Integrated Windows Authentication

Do you want to sign on using Integrated Windows Authentication ?

yes
no
Done
Local intranet

The user operation procedures for each authentication type are shown below.

[Using Integrated Windows Authentication]

1. In the certificate selection window, click the [Cancel].
2. In the Integrated Windows Authentication window, click [Yes].

[Using Certificate Authentication]

1. In the certificate selection window, select the certificate to be used for certificate authentication.
2. In the Integrated Windows Authentication window, click [No].

[Using Password Authentication]

1. In the certificate selection window, click [Cancel].
2. In the Integrated Windows Authentication window, click [No].
3. In the form authentication window, enter the user ID and password.

To use Integrated Windows Authentication, in the Interstage Management Console of the authentication server, click the [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab. In [Detailed Settings [Show]], set the [Authentication method] of [Authentication method Setting].

The Integrated Windows Authentication Sign-on confirmation window can be customized. For details of the customization method, refer to "Customizing Messages Displayed on a Web Browser".

Encryption ciphers used in Integrated Windows Authentication

When Integrated Windows Authentication is used, confidential information is encrypted before being exchanged between Active Directory and the Integrated Windows Authentication application. The encryption cipher for the confidential information can be selected from the following:

Encryption cipher	Explanation
AES128-CTS-HMAC-SHA1-96	This is the highest strength encryption cipher. Select this encryption cipher if the restrictions of the operating systems described below do not cause a problem.
RC4-HMAC	Select this encryption cipher if AES128-CTS-HMAC-SHA1-96 cannot be used.
DES-CBC-CRC	This encryption cipher was used in V9.x and earlier. Compared with the other encryption ciphers, this is of low strength, therefore it should only be selected when building an environment which is the same as V9.x or earlier.

However, it may not always be possible to use a specific encryption cipher, depending on Active Directory or the client operating system.

The encryption ciphers which can be used in each operating system are shown below.

Server-side operating system which is used to run Active Directory

OS	AES128-CTS-HMAC-SHA1-96	RC4-HMAC	DES-CBC-CRC
Windows Server(R) 2003(*1)	No	No	Yes
Windows Server(R) 2003 Service Pack1 or later (*1)	No	Yes (*2)	Yes
Windows Server(R) 2003 R2	No	Yes	Yes
Windows Server(R) 2008(*3)	Yes	Yes	Yes
Windows Server(R) 2008 R2	Yes	Yes	No
Windows Server(R) 2012	Yes	Yes	No

*1 Except Windows Server(R) 2003 R2.

*2 Microsoft(R) Windows Server(R) 2003 Service Pack 1 or later Support Tools must be installed.

*3 Except Windows Server(R) 2008 R2.

Client-side operating system which is used to run Integrated Windows Authentication

OS	AES128-CTS-HMAC-SHA1-96	RC4-HMAC	DES-CBC-CRC
Windows(R) XP	No	Yes	Yes
Windows Vista(R)	Yes	Yes	Yes
Windows 7	Yes	Yes	No
Windows 8	Yes	Yes	No

Additionally, for details on how to set the encryption cipher, refer to "Appendix - Settings for Active Directory Linkage" > "Using Active Directory as the Directory Service for Registering User Information" > "Configure Integrated Windows Authentication" in the "Single Sign-on Operator's Guide".

Note

- For linkage with Microsoft(R) Windows Server(R) 2008, the required Active Directory update program must be applied to the Windows Server(R) being linked. For details on the Active Directory update program required for the linkage, refer to the "Product Notes", section "Supported Software" > "Software Products Required for Application Execution" > "Other Functions".
- Windows(R) Internet Explorer(R) is the only Web browser that can be used in the client. In the Web browser, click [Tools] - [Internet Options] - [Advanced], and select "Enable Integrated Windows Authentication".
- There is no need to add each Interstage Single Sign-on server to the domain in which Active Directory is set.
- If Integrated Windows Authentication is used, the basic authentication dialog cannot be used as the user ID/password input window.
- If reauthentication is required following an interval since the previous authentication, the Integrated Windows Authentication sign-on confirmation window is displayed. If Integrated Windows Authentication sign-on is selected in this window, it is still possible for

services to be used without performing reauthentication. If Integrated Windows Authentication is used, tell users to use the screensaver password security function to reduce the threat of misuse by a third party in their absence.

- Users are not locked out even if authentication using Integrated Windows Authentication fails continuously. However, it is possible to lock users out with user lockout control if incorrect passwords are entered when users log in to Windows. The SSO administrator can also lock users out with the user program in the situations below. For details on user lock out methods, refer to 'Locking a User' in the Appendix 'Samples of User Program Descriptions.'
    - When the Interstage Directory Service is being used as the directory service for registering user information
    - When Active Directory is being used as the directory service for registering user information and an extended schema for single sign-on is also being used
- If the Interstage Directory Service is being used as the directory service for registering user information, then user information managed in the SSO repository must be associated with and managed in the Active Directory. For details on how to associate both sets of user information, refer to 'Using Interstage Directory Service as the Directory Service for Registering User Information' in the Settings for Active Directory Linkage appendix.

  It is recommended that the ID management tool is used to ensure that the user information is associated.
- For systems where users can re-authenticate using either a password or certificate without signing on using Integrated Windows Authentication and where Active Directory is being used, the single sign-on schema must be extended for Active Directory. Refer to 'Extended Schema Settings for Single Sign-on' for information about how to extend the single sign-on schema for Active Directory.
- To use repository server load balancing, use a system configuration that places more than one repository server (update system). Refer to 'Load Balancing' for more information about this system configuration.
- If the authentication server has been registered in the domain of the ActiveDirectory to be linked to, network settings must be configured. For details on these settings, refer to the "Product Notes", section "Notes on Interstage Operation" > "Notes on Interstage Single Sign-on" > "Notes on Integrated Windows Authentication".

1.4.3 Combinations of Authentication Methods

Interstage Single Sign-on supports the following authentication methods as combinations of password authentication and certificate authentication. Authentication methods can be selected for each user.

Authentication Method	Description
password authentication	This authentication method uses a user ID and password pair. Either form authentication or basic authentication can be used. (*1)
certificate authentication	This authentication method uses the certificate obtained at SSL client authentication. (*2)
password authentication or certificate authentication	Success of authentication is assumed only when either password authentication or certificate authentication is successful.
password authentication and certificate authentication	Success of authentication is assumed only when both password authentication and certificate authentication are successful.
Integrated Windows Authentication	This authentication method uses the user ID and password specified for Windows logon. If Integrated Windows Authentication sign-on is not performed, it is possible to perform authentication using password or certificate authentication.

*1 Basic authentication can only be performed in systems in which session management is not used.

*2 Certificate authentication without an IC card can only be used in systems in which session management is not used.

Password Authentication or Certificate Authentication

Success of authentication is assumed when either password authentication or certificate authentication is successful.

This authentication method is appropriate for users who always receive certificate authentication, and either need to access a resource remotely during a business trip, or cannot use the certificate for some reason. These users can gain access using password authentication. The authentication operation is flexible.

This authentication method first requests the user to receive certificate authentication. When certificate authentication is successful, success of authentication is assumed. If the user fails in certificate authentication or presents no certificate, the user is requested to receive password authentication. When password authentication is successful, success of authentication is assumed. If the user fails password authentication, failure in authentication is assumed.

When the user has registered only one certificate or has not registered any certificate, the user can also use the registered certificate without displaying the certificate selection window or display the password authentication window without displaying the certificate selection window. For further details about how to display the certificate selection window, refer to "Certificate Selection Windows".

Password Authentication and Certificate Authentication

This authentication method only assumes authentication has been successful when both password authentication and certificate authentication have been successfully completed.

This method of authentication firstly requests the user to receive certificate authentication. When certificate authentication is successful, the user is then requested to complete password authentication. When password authentication has been completed, the authentication process has been successful. If password authentication fails, the authentication process may fail.

When the user has registered only one certificate, the user can also use the registered certificate without displaying the certificate selection window. For details about how to display the certificate selection window, refer to "Certificate Selection Windows".

Note

When the Web browser is Netscape Communicator, the certificate selection window may be displayed twice. If it occurs, operate same action for both windows.

1.4.4 Certificate Selection Windows

If no certificate (or only one certificate) has been registered in the client computer, the display of the certificate selection window can be suppressed during certificate authentication.

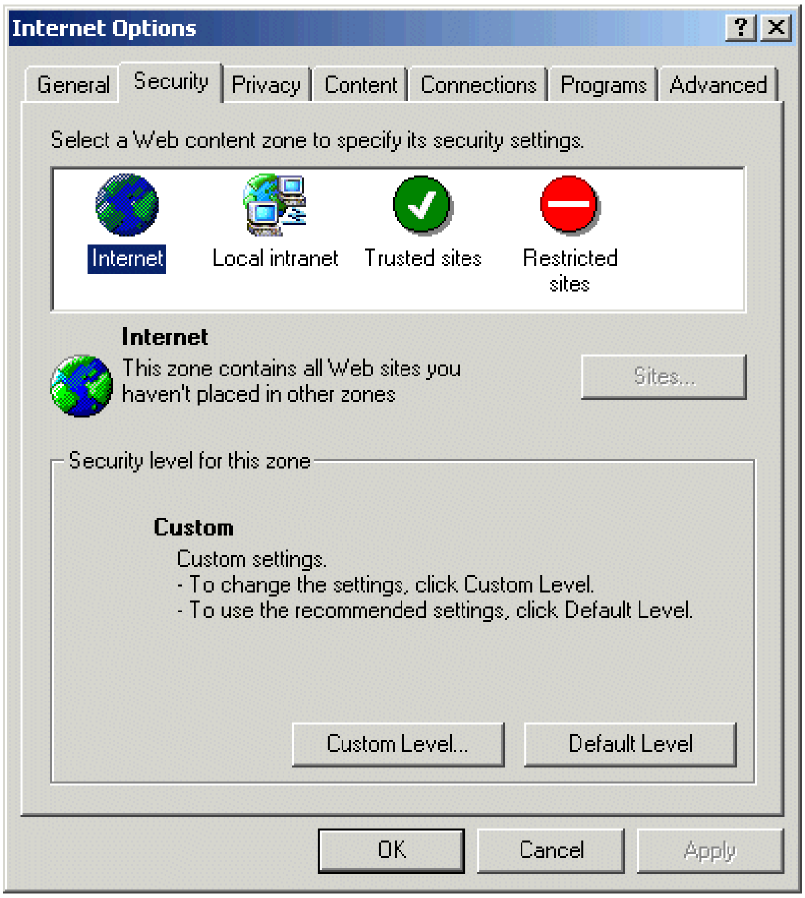
The following section explains how to suppress display of the certificate selection window. As the display procedure for the certificate selection window varies depending on the type and the version of the Web browser, refer to the manual for the relevant Web browser.

Example

Windows(R) Internet Explorer(R)

Select [Tools] > [Internet Options], and from the [Security] tab, select [Custom level].

Figure 1.21 Internet Options



Select a Web content zone to specify its security settings.

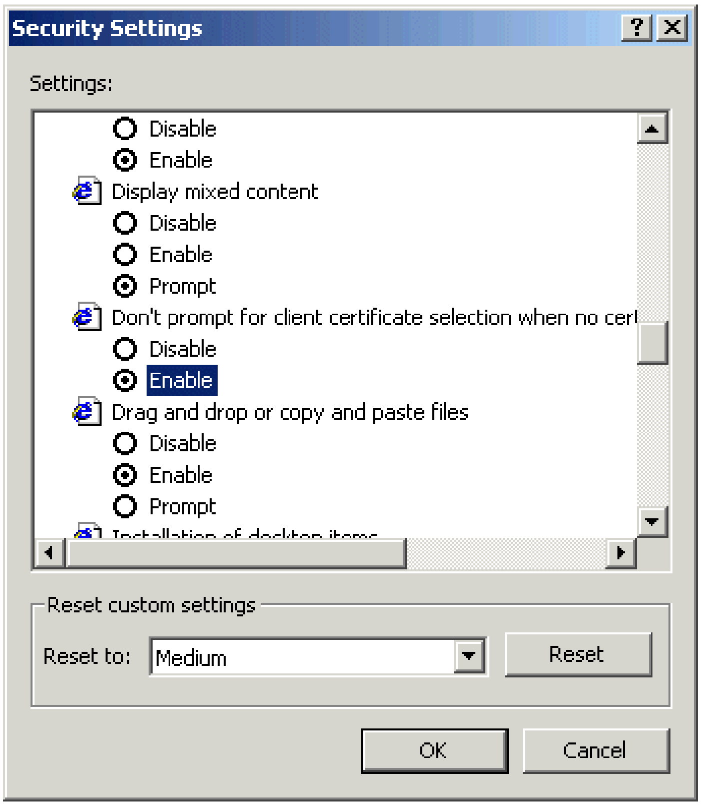
Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

Select "Enable" for [Don't prompt for client certificate selection when no certificates or only one certificate exists].

Figure 1.22 Security Settings



Settings:

○ Disable
● Enable

Display mixed content
○ Disable
○ Enable
● Prompt

Don't prompt for client certificate selection when no cert
○ Disable
● Enable

Drag and drop or copy and paste files
○ Disable
● Enable
○ Prompt

Installation of desktop items

Reset custom settings

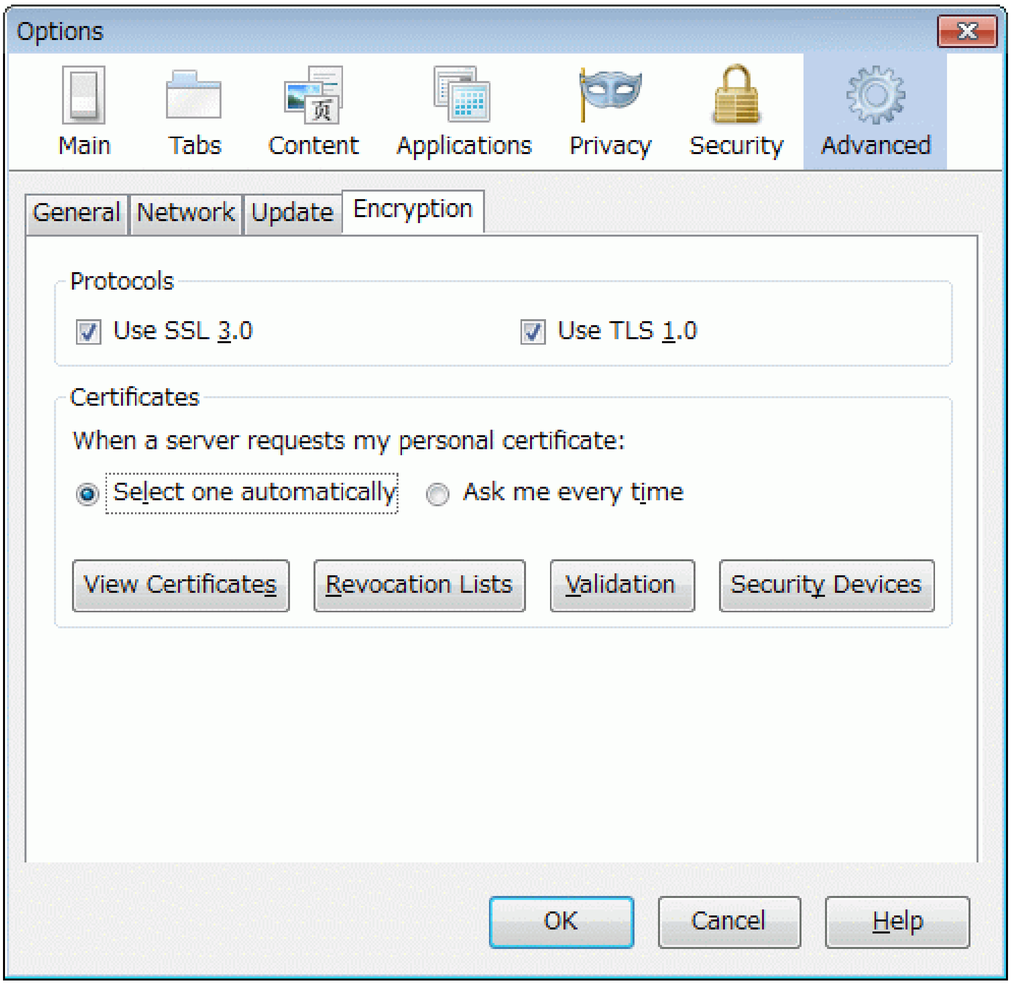
Reset to: Medium

Example

Mozilla(R) Firefox

The setting are configured using [Tools] > [Options] > [Advanced] > [Encryption] - [Certificates] - [When a server requests my personal certificate] - [Select one automatically].

Figure 1.23 Security Settings



☑ Use SSL 3.0 ☑ Use TLS 1.0

When a server requests my personal certificate:

● Select one automatically ○ Ask me every time

1.4.5 User Information

User information is managed in the SSO repository, and includes the user ID, password and authentication method for each user managed by Interstage Single Sign-on. The following user information can be set for each user according to system operation requirements.

The following table lists the main setting items for user information.

Table 1.3 User Information

Item	Description
Authentication method	One of the following authentication method: Password authentication Certificate authentication (*1) Password authentication or certificate authentication Password authentication and certificate authentication
User ID	User ID of the user. Only one user ID must be set for a user.

Item	Description
Password	Password of the user. Only one password must be set for a user.
Information to identify the user at certificate authentication	Certificate information that can identify the user with the certificate used by the user during certification authentication. This information does not need to be set when certificate authentication is not applied.
Role name/role set name	Name of the role or role set assigned to the user. Multiple roles or role sets can be set. The role and role set names set in user information must be those defined by role configuration.
Re-authentication interval	Interval of the time from authentication to subsequent re-authentication required.
Validity period start time	Date and time when the user starts using Single Sign-on.
Validity period end time	Date and time when the user ends the use of Single Sign-on.

*1 Certificate authentication can only be set up for systems that do not perform session management or for systems that perform session management and where certificate authentication is allowed.

For details of roles and role sets, refer to "Relationships between Roles, Users, and Resources".

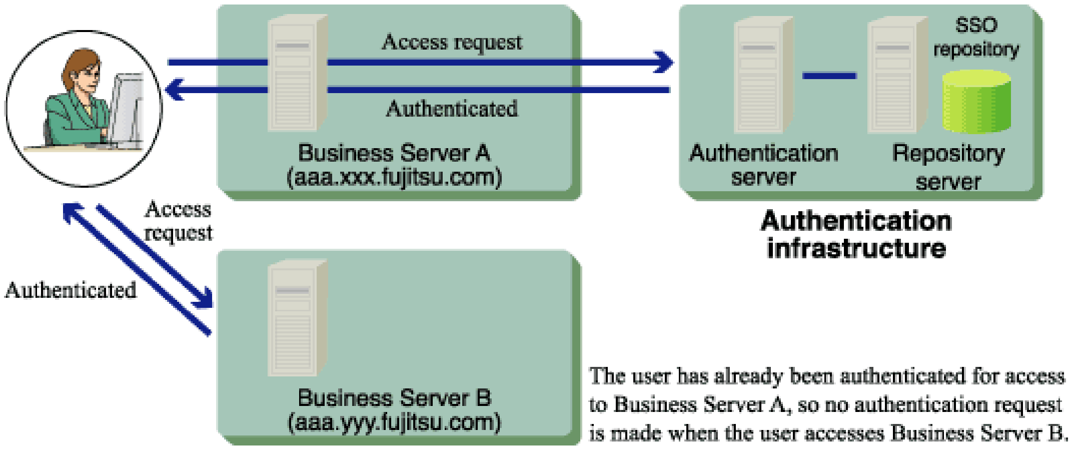
1.4.6 Authentication Information

After a user is authenticated, information such as the user ID and authentication method is transferred as authentication information in a cookie format to the business, authentication and repository servers.

1.4.7 Authentication in a Multi-domain Environment

Authentication and authorization Interstage Single Sign-on are also available for an environment where the business system and authentication infrastructure belong to different domains.

Figure 1.24 Authentication in a Multi-domain Environment

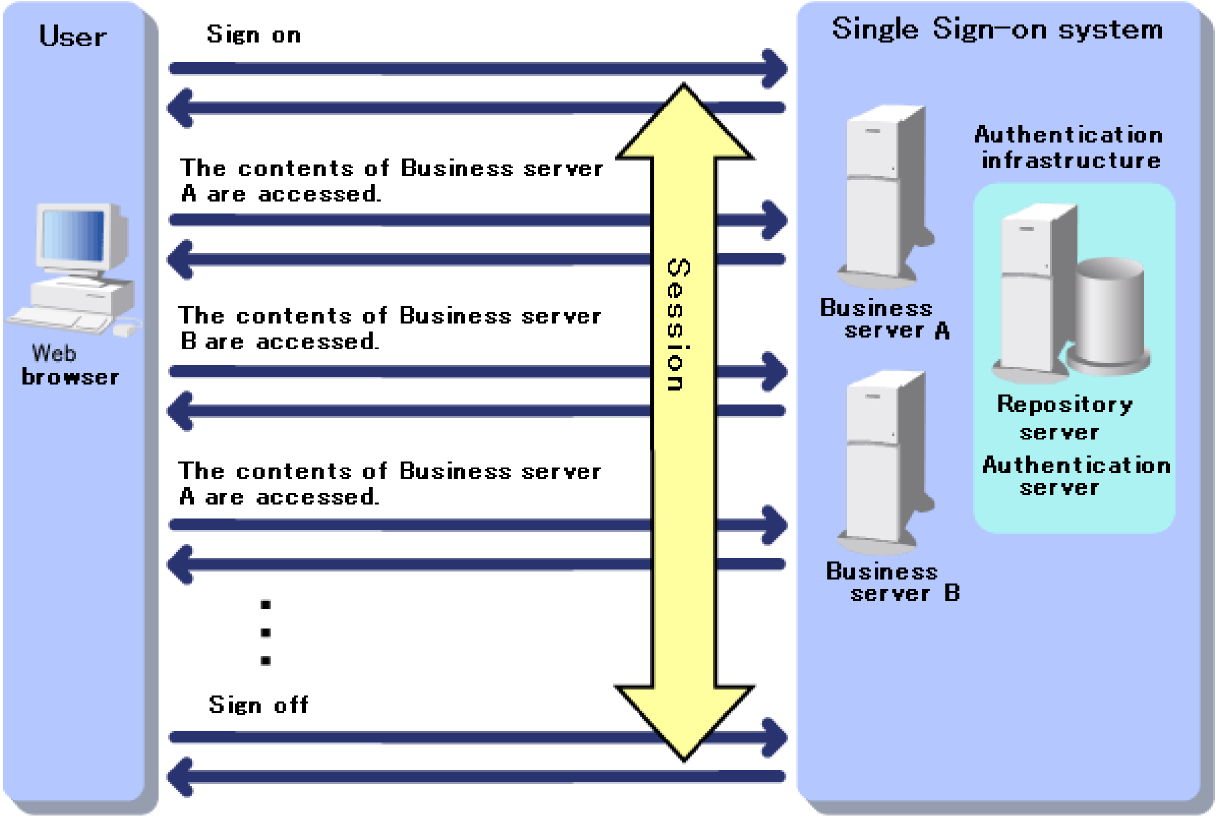


1.4.8 Session Management

In Interstage Single Sign-on, the validity period for authentication information for each user can be managed to reduce the risk of illegal access.

The authentication information is valid from when the user signs on to the Single Sign-on system from the Web browser (authentication) until the user signs off from the Single Sign-on system. This period is called a "session". When the user signs off, the authentication information is rendered invalid.

Figure 1.25 The Duration of a Single Sign-on Session


User
Sign on
Single Sign-on system
The contents of Business server A are accessed.
Authentication infrastructure
Web browser
The contents of Business server B are accessed.
Session
Business server A
Repository server
Authentication server
The contents of Business server A are accessed.
Business server B
Sign off

In Interstage Single Sign-on, the following functions are offered for management of the user session:

- Idle surveillance

  A user that has not accessed the Single Sign-on system for a certain period of time can be signed off automatically.

- Prevention of multiple Sign-on

  In systems in which Session Management is used, Sign-on from more than one Web browser by the same user ID is prevented.

- Forced Sign-on

  A user can disable an unnecessary session and sign on again.

- Forced Sign-off

  The SSO administrator can sign off by force a user who is already signed on to the Single Sign-on system.

- Sign-off

  A user can use a Sign-off button and link on the Business server contents to sign off from the Single Sign-on system.

- Notice of the previous Sign-on date

  A user can check the date of the previous Sign-on, by performing the notified Previous Sign-on date check.

To manage the session for the user, in the Interstage Management Console of the Repository server (update system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Session management detailed settings[Show]] > [Session management Setting] > [Use Session management?].

Session management is performed on the Repository server (update system). This is referred to from now on as the "session management server".

Notes

- Sessions managed in Interstage Single Sign-on are not linked with sessions managed in business systems.

- To switch from a system that does not use session management to one that does, the environment settings must be changed. For details about the procedure, refer to "Switching to an application to perform session management".

- If session management is used, SSL can be used in the Repository server.
- If certificate authentication is used on a system where session management is being performed, services can continue to be used without re-authenticating even if the following functions are executed. Be sure to conduct thorough user training in order to reduce the risk of illegal access by third parties while users are away from their computers.
    - Functions that will be disabled
        - Idle surveillance
        - Sign-off
        - Forced Sign off
    - User instruction
        - Perform idle monitoring using the protection function provided by the screen saver password.
        - The Web browser should be closed when signing off.

1.4.9 Disabling the Session

In Interstage Single Sign-on, the following settings can be made to reduce the risk of illegal access by a third party while the user is away from their computer.

- Idle surveillance

  A user that has not accessed the Single Sign-on system for a certain period of time is signed off automatically and asked to perform authentication again.

- Re-authentication Interval

  If a certain period of time is exceeded following the user signing on to the Single Sign-on system, the user is asked to perform authentication again.

If session management is used, the Idle surveillance and Re-authentication Interval can both be set to ensure a more secure application environment.

If session management is not used, only the Re-authentication Interval can be set.

Idle Surveillance

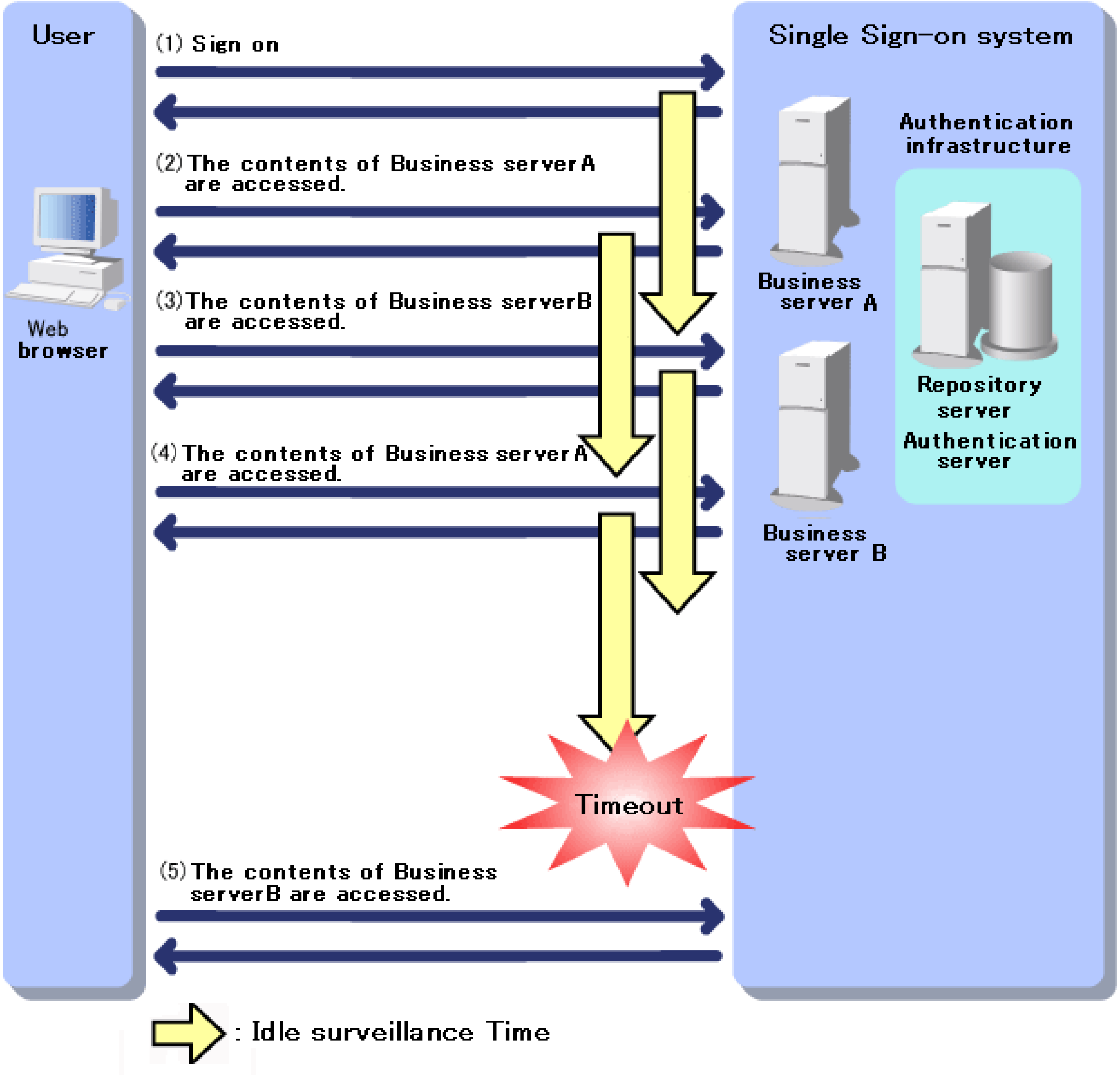
In Interstage Single Sign-on, monitoring of the idle status starts as soon as the user has signed on to the Single Sign-on system. If there is no access for the period set as the Idle surveillance Time, user authentication is disabled automatically.

If the Single Sign-on system is accessed from more than one Web browser, the idle status is monitored for each Web browser.

If the Idle surveillance Time is exceeded, there is a timeout. If a user accesses the Single Sign-on system after the timeout, they are asked to perform authentication again so that the Business server contents they were accessing before the timeout occurred can be restarted.

An overview of the Idle surveillance operation is shown below.

Figure 1.26 Overview of the Idle Surveillance Feature


User
Web browser
(1) Sign on
(2) The contents of Business server A are accessed.
(3) The contents of Business server B are accessed.
(4) The contents of Business server A are accessed.
Timeout
(5) The contents of Business serverB are accessed.
Single Sign-on system
Business server A
Business server B
Authentication infrastructure
Repository server
Authentication server
: Idle surveillance Time

(1)Sign on to the Single Sign-on system is performed. From this point, the idle status is monitored.

(2)The contents of Business server A are accessed within the Idle surveillance Time range. For this reason, there is no timeout. Monitoring of the idle status continues.

(3)The contents of Business server B are accessed within the Idle surveillance Time range. For this reason, there is no timeout. Monitoring of the idle status continues.

(4)The contents of Business server A are accessed within the Idle surveillance Time range. For this reason, there is no timeout. Monitoring of the idle status continues.

(5)The contents of Business server B are accessed. The Idle surveillance Time has been exceeded, so there is a timeout. For this reason, a message is output in the user Web browser prompting you that the session is invalid and asking you to perform authentication again.

To set the Idle surveillance time, in the Interstage Management Console of the Repository server (update system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Session management detailed settings [Show]] > [Idle surveillance] > [Idle surveillance time].

Re-authentication Interval

In Interstage Single Sign-on, after the user has signed on to the Single Sign-on system, if the period of time set for the Re-authentication Interval is exceeded, the user is asked to perform authentication again.

The Re-authentication Interval is monitored for each IP address. Whenever there is a connection from a different client, the user is asked to perform authentication again regardless of the Re-authentication Interval settings.

The user is asked to perform authentication again so that the Business server contents they were accessing before the timeout occurred can be restarted.

The Re-authentication Interval can be set for each user or Single Sign-on system as shown below.

- For each user

  Set "ssoCredentialTTL" (Re-authentication Interval) for the user information registered in the SSO repository.

- For each Single Sign-on system

  In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]] > [Operation after Authentication], and set [Re-authentication Interval].

For details of the configurations on the Interstage Management Console, refer to the Operator's Guide.

Notes

- If the Re-authentication Interval is set both for users and Single Sign-on systems, the settings for users take priority.

- When "certificate authentication" is used as the authentication method for the user, or when the user has been authenticated by certificate authentication with "password authentication or certificate authentication" used as the authentication method, the client (Web browser) automatically presents the certificate to the Web server at re-authentication.

  Therefore, the window requesting re-authentication is not shown to the user. Note that, when users are setting up the Authentication Server on multiple machines and the Repository Server on one machine, or setting up the Authentication Server and the Repository Server on multiple machines, the window requesting re-authentication may display even when the authentication method is "certificate authentication" or "password authentication or certificate authentication."

- When the remaining time for the validity period registered as user information in the SSO repository is shorter than the set Re-authentication Interval, the validity period registered as user information in the SSO repository has priority over the Re-authentication Interval. For details about the validity period when set as user information, refer to "User Validity Period" of "Restrictions on Authentication".

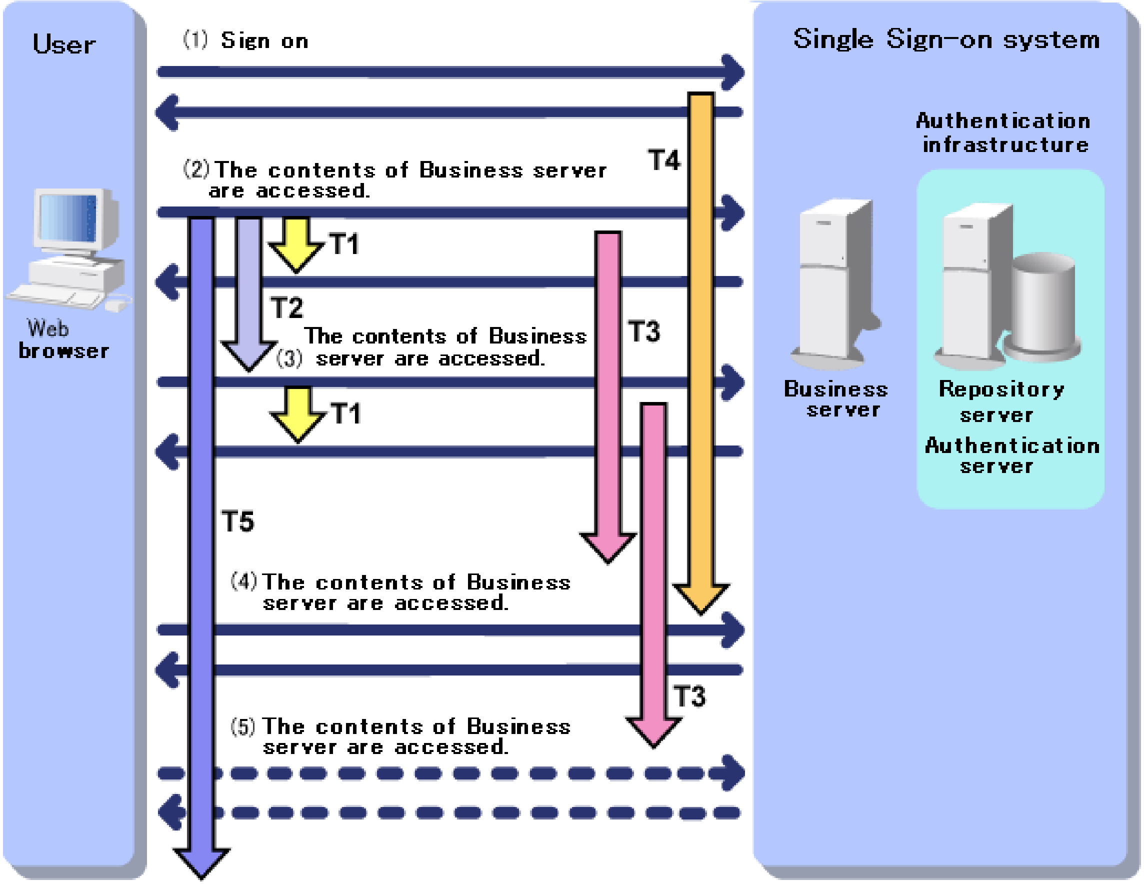
- In systems in which session management is not used, to reduce the risk of unauthorized use by third persons, it is strongly recommended that "0" should not be set as the Re-authentication Interval for each user or as the standard Re-authentication Interval.

Idle surveillance and Re-authentication Interval

If session management is used, Idle surveillance and the Re-authentication Interval can both be set to reduce the risk of illegal access by a third party during the Idle surveillance Time while the user is away from their computer, to ensure a more secure application environment.

Notes about setting the Idle surveillance Time and the Re-authentication Interval

Figure 1.27 View of Response Times, and Surveillance and Re-Authentication Periods


User
Web browser
Single Sign-on system
Authentication infrastructure
Business server
Repository server
Authentication server
(1) Sign on
(2) The contents of Business server are accessed.
(3) The contents of Business server are accessed.
(4) The contents of Business server are accessed.
(5) The contents of Business server are accessed.
T1
T2
T3
T4
T1
T5
T3

T1 : The time from when the user accesses the Business Server contents until a response is returned

T2 : The average time between accesses to the Business server contents

T3 : Idle surveillance Time

T4 : Re-authentication Interval

T5 : Business Server Contents Timeout Monitoring Time

To prevent invalid timeouts, consider the following methods before making the settings.

T1 + T2 < T3 < T4 < T5

- Idle surveillance Time (T3)

  Consider the time required for one access to the Business server contents (T1: this is the time from when the user accesses the Business Server contents until a response is returned), and the average time between subsequent accesses to the Business server contents (T2). Set a time for T1+ T2 that exceeds the time set for the Idle surveillance Time.

- Re-authentication Interval (T4)

  Set a time for the Re-authentication Interval that exceeds the time set for the Idle surveillance Time, so that the Re-authentication Interval re-authentication does not occur before there is an Idle surveillance timeout.

- Business Server Contents Timeout surveillance Time (T5)

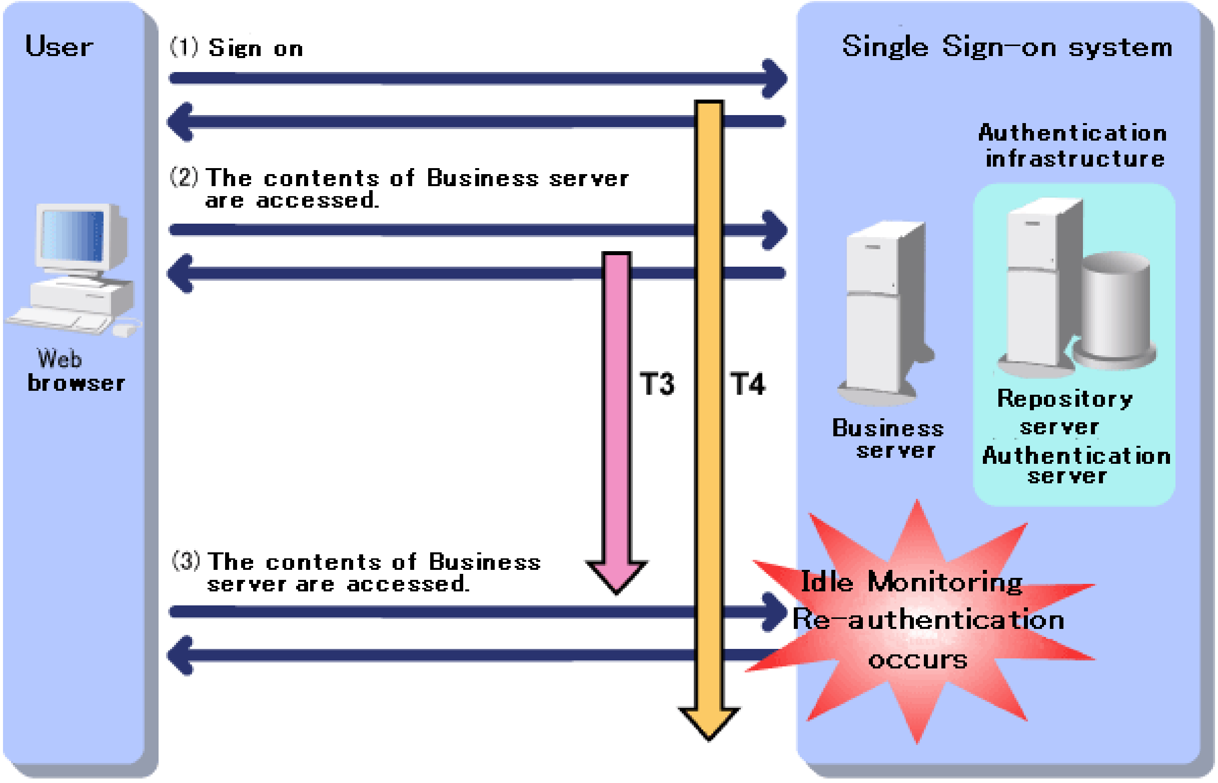
  If the Timeout surveillance Time is set for the Business server contents, set a time that exceeds the time set for the Idle surveillance Time and the Re-authentication Interval.

The settings for the Idle surveillance Time and the Re-authentication Interval and examples of operation are described below.

Example

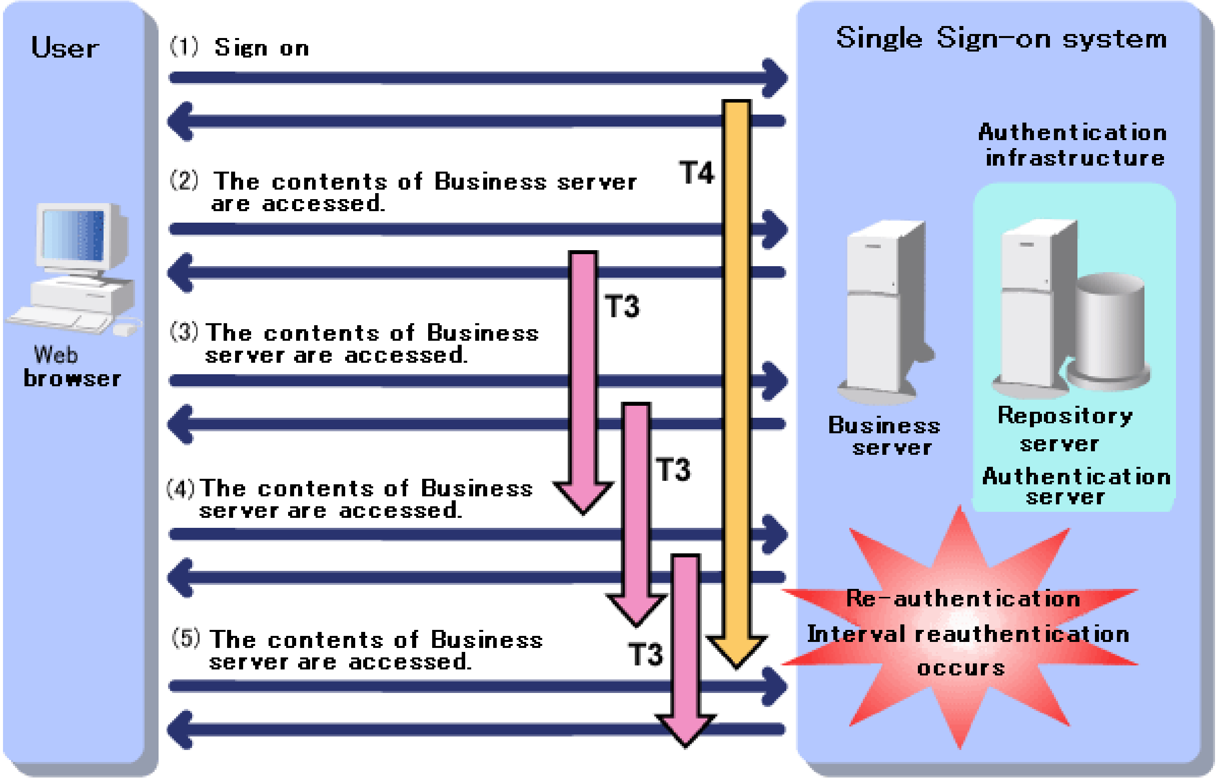
The Idle surveillance Time (T3) is [15] minutes, and the Re-authentication Interval (T4) is [30] minutes.

Figure 1.28 Idle surveillance is exceeded


User
Web browser
(1) Sign on
(2) The contents of Business server are accessed.
T3
T4
(3) The contents of Business server are accessed.
Single Sign-on system
Authentication infrastructure
Business server
Repository server
Authentication server
Idle Monitoring Re-authentication occurs

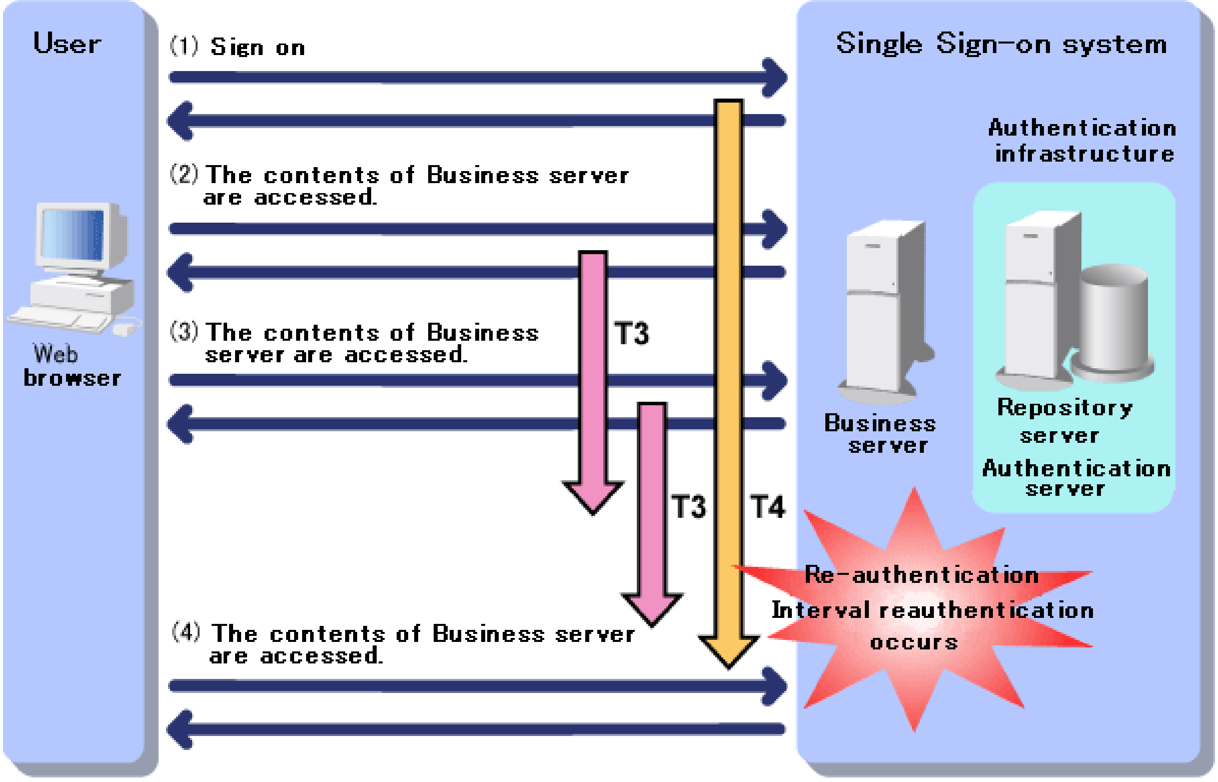
At the point when the Business server contents are accessed in (3), the time set for the Re-authentication Interval (T4: [30] minutes) is not exceeded but the time set for the Idle surveillance Time (T3: [15] minutes) is. Idle surveillance re-authentication occurs.

Figure 1.29 Re-authentication Interval is exceeded


User
Web browser
(1) Sign on
(2) The contents of Business server are accessed.
T4
T3
(3) The contents of Business server are accessed.
T3
(4) The contents of Business server are accessed.
(5) The contents of Business server are accessed.
T3
Single Sign-on system
Authentication infrastructure
Business server
Repository server
Authentication server
Re-authentication Interval reauthentication occurs

At the point when the Business server contents are accessed in (5), there is no timeout because the time set for Idle surveillance Time (T3: [15] minutes) is not exceeded. The time set for Re-authentication Interval (T4: [30] minutes) is exceeded, however, so Re-authentication Interval re-authentication occurs.

Figure 1.30 Both Idle surveillance time and Re-authentication Interval are exceeded


User
Web browser
(1) Sign on
(2) The contents of Business server are accessed.
(3) The contents of Business server are accessed.
T3
T3
T4
(4) The contents of Business server are accessed.
Single Sign-on system
Authentication infrastructure
Business server
Repository server
Authentication server
Re-authentication Interval reauthentication occurs

At the point when the Business server contents are accessed in (4), the time set for both Idle surveillance Time (T3) and Re-authentication Interval (T4) is exceeded, so Re-authentication Interval re-authentication occurs.

1.4.10 Restrictions on Authentication

In Interstage Single Sign-on, if Session Management is used, the following settings can be made with session management to prevent illegal access.

- User validity period

  The period for access to the Single Sign-on system by the user can be restricted so that authentication outside the validity period is invalid and access to the Single Sign-on system is denied.

- Lockout

  If an invalid password is entered a certain number of times during user ID/password authentication, authentication fails and access to the Single Sign-on system is denied.

- Prevention of multiple Sign-on

  In systems in which Session Management is used, access from more than one Web browser using the same user ID is denied.

User Validity Period

Validity periods can be set for users in Interstage Single Sign-on.

For example, if the information on new employees is stored in the SSO repository in advance, settings can be made to validate authentication on the beginning date of employment and specify the projected end date of employment as the validity period end date.

Thus, authentication can be invalidated temporarily, and user validity periods can be set without deletion of user information from the SSO repository.

Set the user validity period by specifying values in "ssoNotBefore" and "ssoNotAfter" for the user information in the SSO repository.

For details about the user information in the SSO repository, refer to "User Information Entry".

Lockout

In order to protect users against unauthorized access, the lockout function restricts authentication and disables access to the resources managed by Interstage Single Sign-on.

If a user inputs invalid passwords (user ID and password) for a specified number of consecutive times, the user is locked and the use of the Single Sign-on system is restricted to disable the user from attempting the input of any more passwords.

The SSO administrator can also forcibly lock users out by operating the SSO repository using the user program. For details on user lockout methods, refer to 'Locking a User' in the Appendix 'Samples of User Program Descriptions.'

The locked user fails authentication until the userID is unlocked.

The count for successive authentication failures is reset when the user succeeds in password authentication.

Note

- If a user fails in authentication using a certificate, the user is requested to input the user ID and password. Since the user for which certificate authentication failed is the one set for [Certificate Authentication], [Password/Certificate Authentication], authentication fails even if the user ID and password entered are correct. In this case, click [Cancel] in the [Input User ID/Password] window.

  When the user inputs a user ID and a password to the user ID/password request window, the user is regarded as a lockout target and the count for successive authentication failures is increased by one, even if the input user ID and password are valid.

- Locked users cannot use Interstage Single Sign-on (even for certificate authentication) until they are unlocked.

- Users are not locked out even if Integrated Windows Authentication authentication fails continuously.

The Interstage Management Console is used to configure the Lockout settings. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]] > [Lockout Settings], and set [User lock] and [When releasing user lock?].

The SSO administrator uses the Interstage Management Console to release the lock. For details about the method, refer to "Releasing user locks".

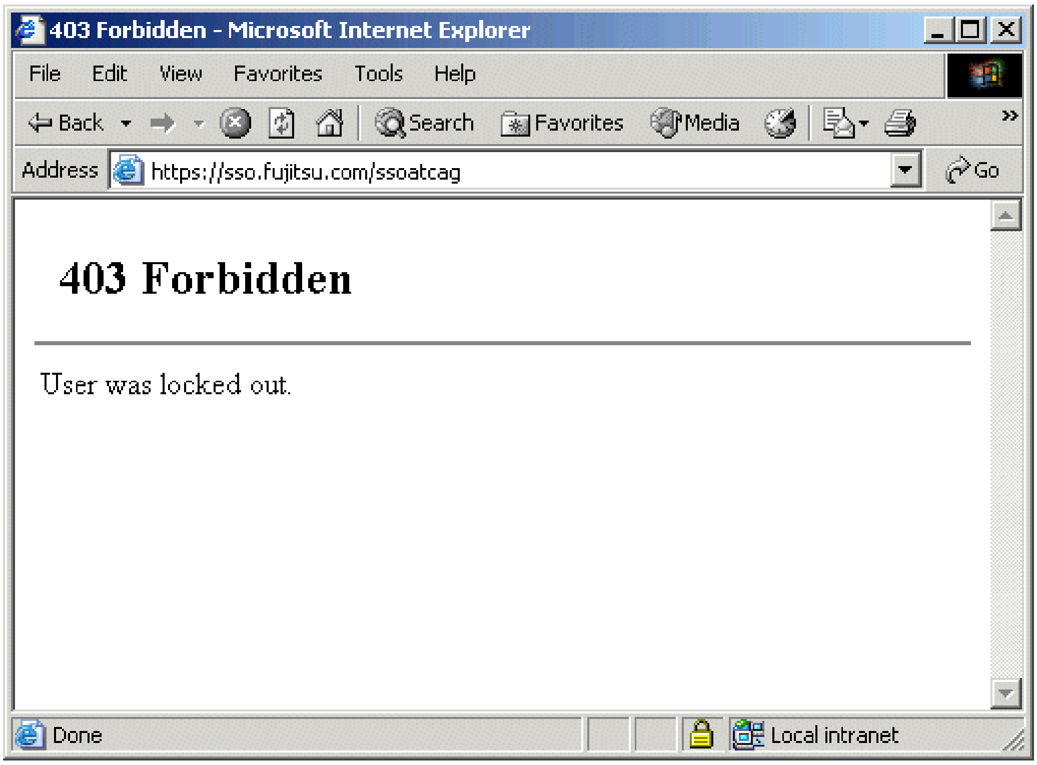
For automatic lock release applications, the lock is released at the first authentication after a specified period of time.

If a user has failed password authentication for a specified consecutive number of times and is locked by the lockout function, a message is sent to the user's client computer.

The message shown in the following figure notifies the user when authentication has failed. The display of this message is configured in the environment setup on the authentication server. To activate this setting, on the Interstage Management Console select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]] > [Communication Settings with Business system]. Then select [Yes] for [Notify Cause of Authentication Failure to user?].

If [No] is selected, the message "User name or password is invalid." is displayed on the browser. For further details, refer to "Messages that can be Customized".

Figure 1.31 Screen Displayed when User is Locked Out

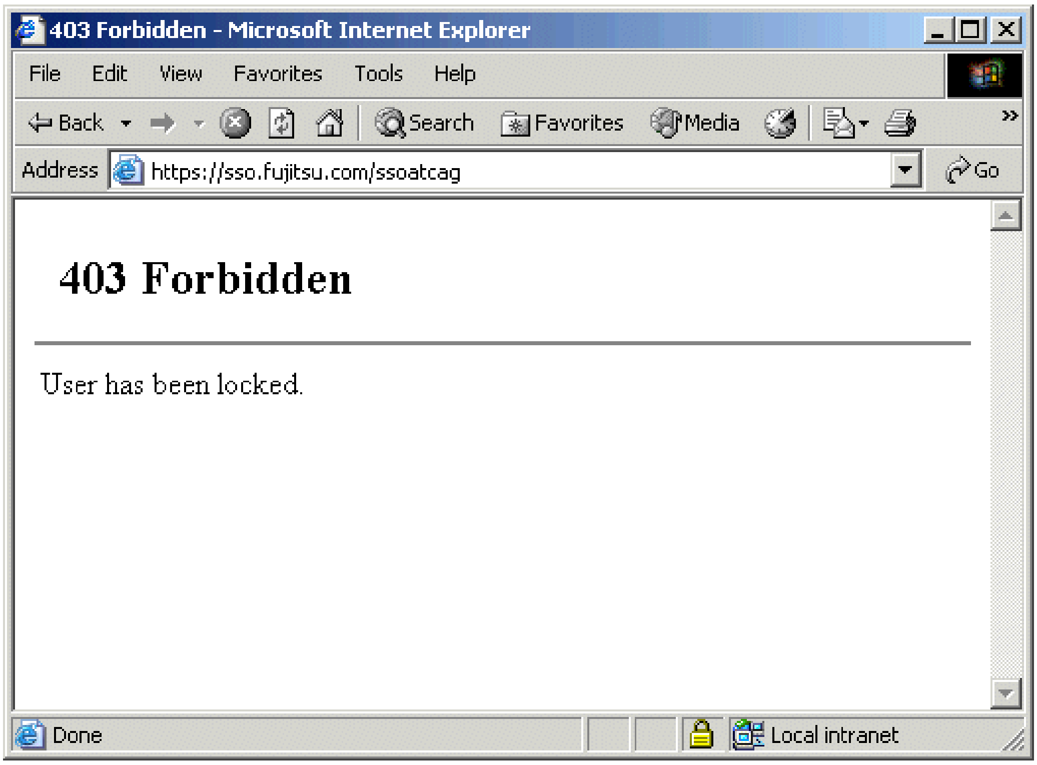

403 Forbidden - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.com/ssoatcag
Go
Done
Local intranet

403 Forbidden

User was locked out.

When a locked user performs authentication, the following window is displayed on the Web browser.

Figure 1.32 Screen Displayed when User has been Locked


403 Forbidden - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.com/ssoatcag
Go
Done
Local intranet

403 Forbidden

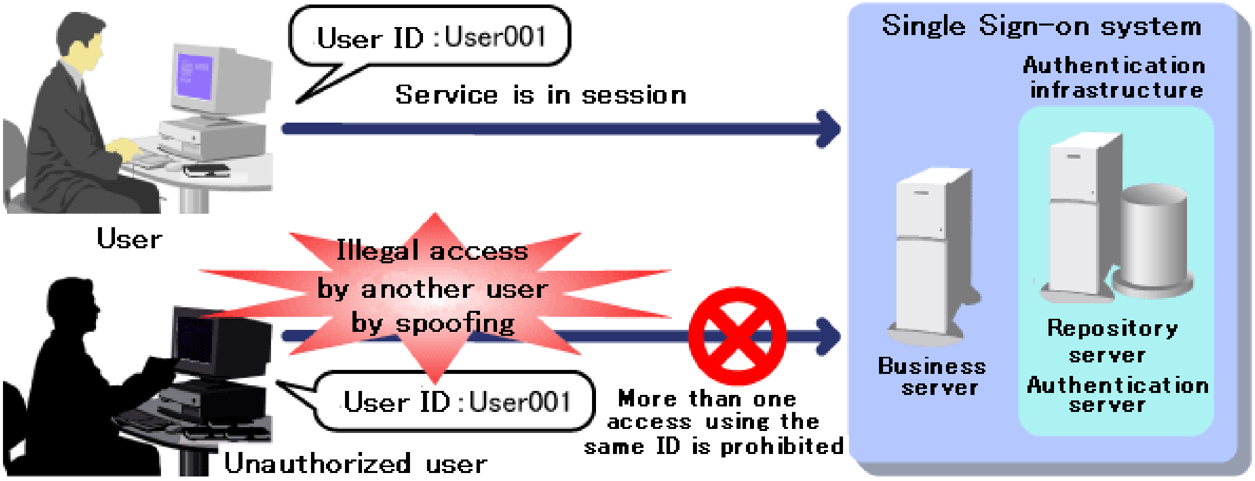
User has been locked.

Prevention of Multiple Sign-on

In systems in which Session Management is used, access from more than one Web browser by the same user ID (multiple Sign-on) is prevented.

The risk of illegal access by a third party can be reduced with the prevention of multiple Sign-on.

Figure 1.33 Multiple Sign-on Prevention



1.4.11 Sign-off

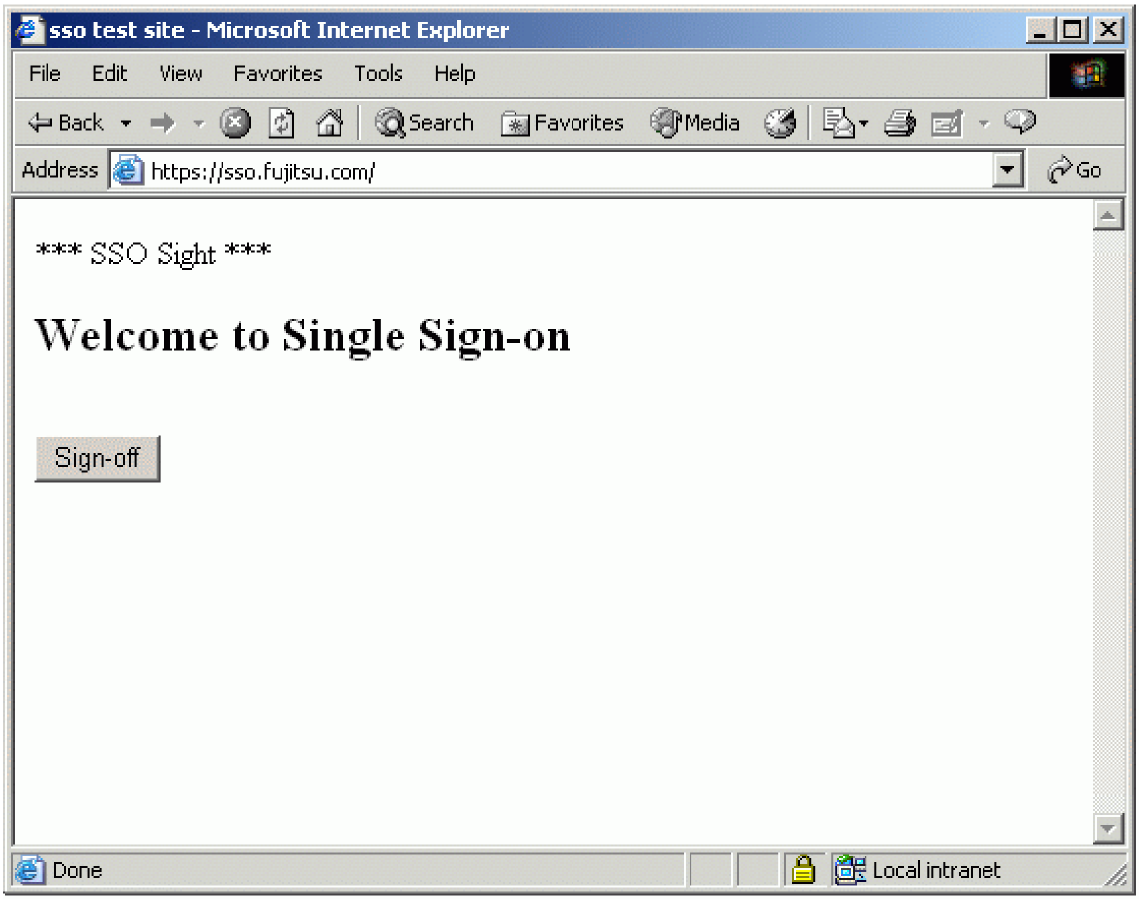
Users of the Single Sign-on system can use the Sign-off link added to the authentication infrastructure to sign off from the Single Sign-on system without closing the Web browser. In this case, authentication is disabled.

An example of how to use the [Sign-off] button to sign off is described below.

Example

1. Click the [Sign-off] button that has been added to the Business server contents.

Figure 1.34 Using Sign-Off

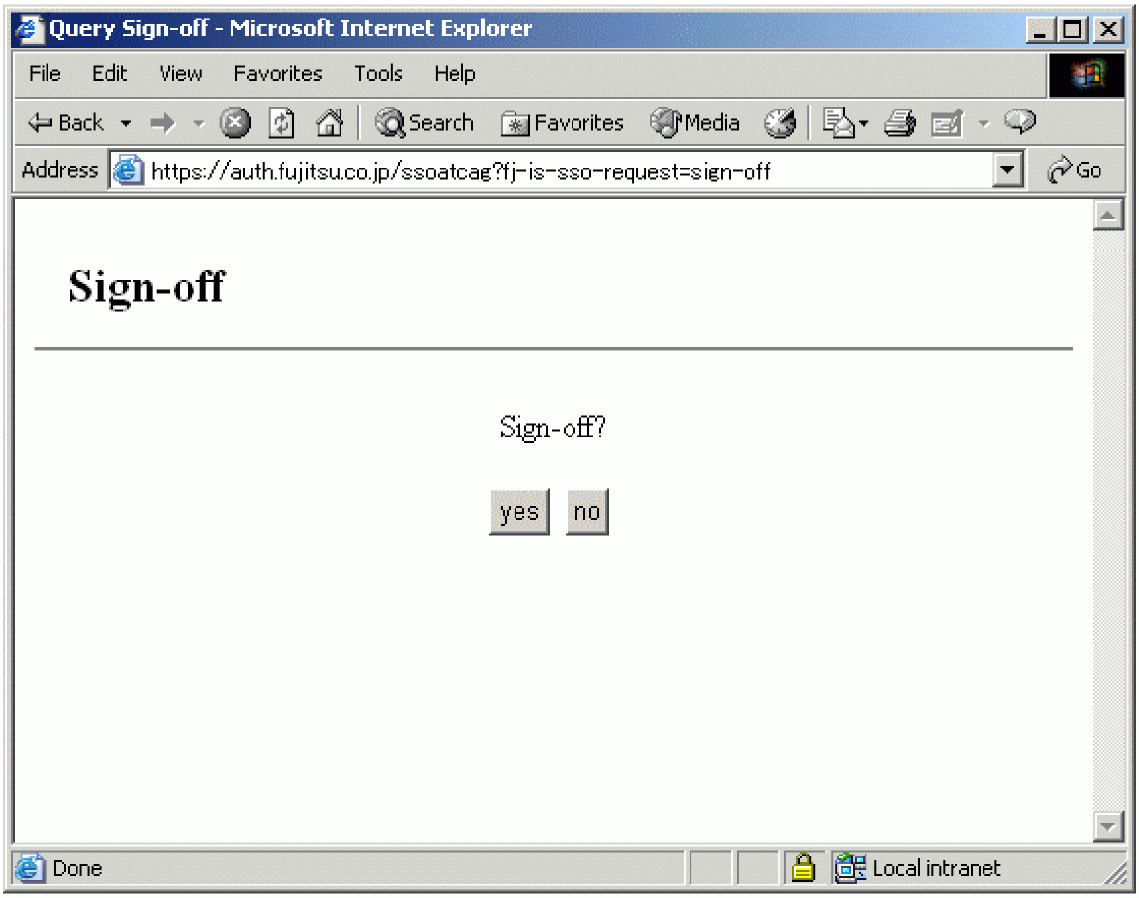

sso test site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.com/
Go
Sign-off
Done
Local intranet

*** SSO Sight ***

Welcome to Single Sign-on

2. The following Sign-off confirmation is output.

Figure 1.35 Sign-Off Confirmation Message



Query Sign-off - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://auth.fujitsu.co.jp/ssoatcag?fj-is-sso-request=sign-off
Go

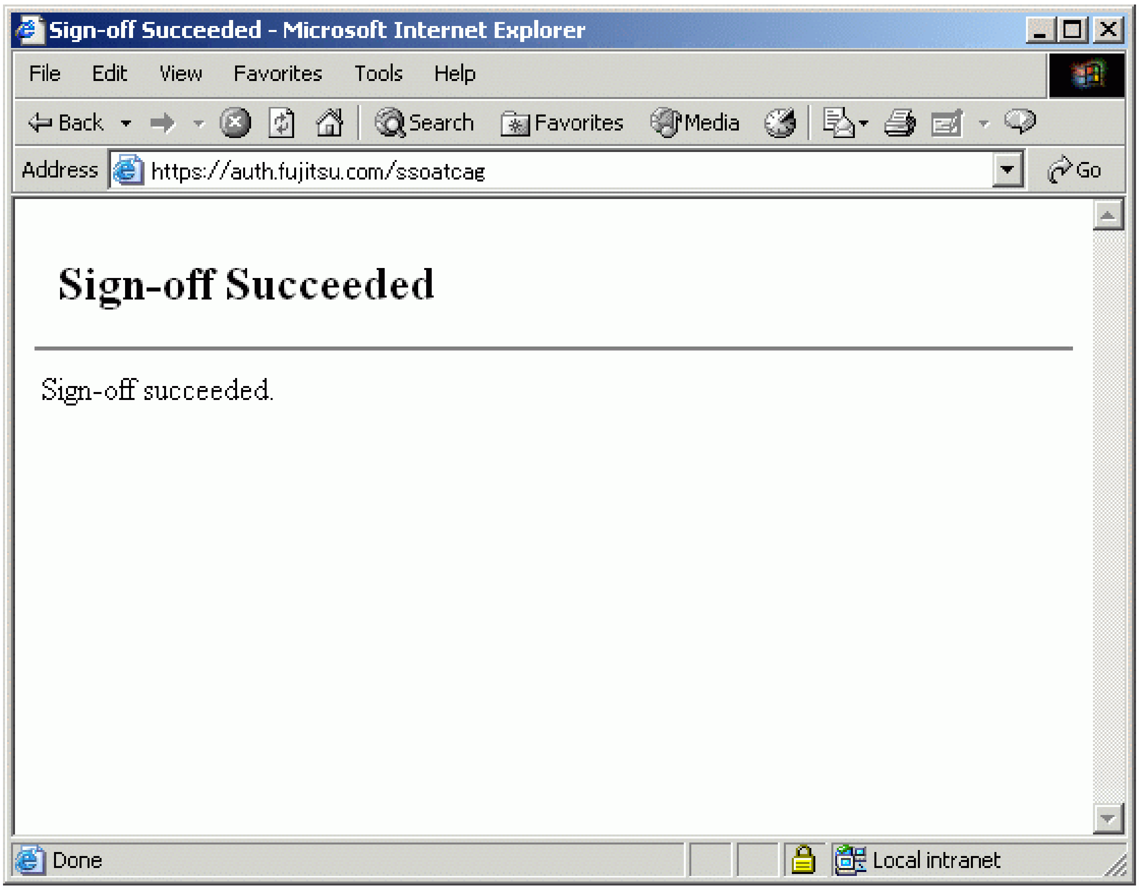
Sign-off

Sign-off?

yes
no
Done
Local intranet

3. If [Yes] is clicked, the following Sign-off completion message is output and Sign-off is complete.

Figure 1.36 Sign-Off Completion Message


Sign-off Succeeded - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
https://auth.fujitsu.com/ssoatcag
Go
Done
Local intranet

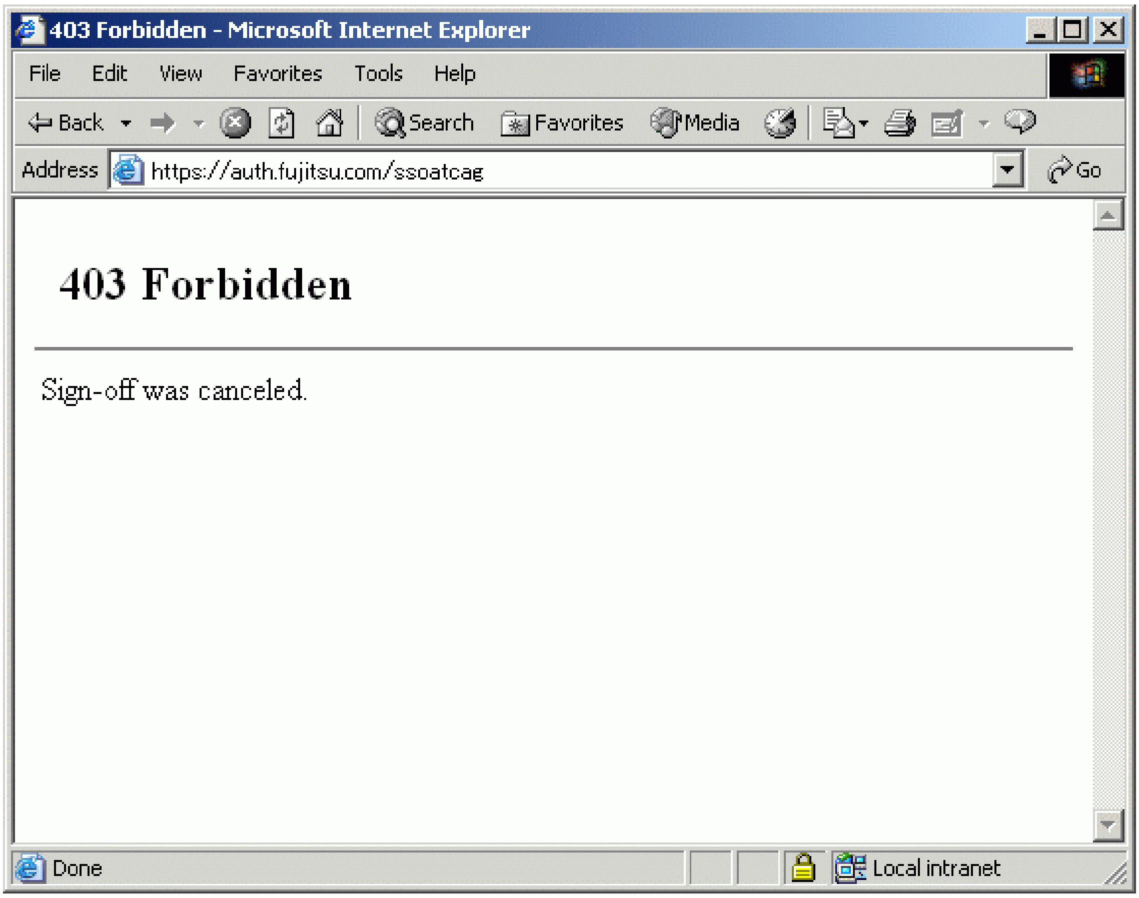
Sign-off Succeeded

Sign-off succeeded.

4. If [No] is clicked, the following Sign-off cancellation message is output and Sign-off is cancelled.

5. To switch business systems and continue, click the Web browser [Back] button.

Figure 1.37 Sign-Off Cancellation Message



403 Forbidden - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://auth.fujitsu.com/ssoatcag
Go
Done
Local intranet

403 Forbidden

Sign-off was canceled.

As described in the example, the administrator must provide a method for the user to perform Sign-off. These methods are shown below.

- Business Server Administrator

  Creating the Sign-off Business server contents

  Provide a Sign-off link on the Business server contents. Set the [Sign-off] button on the Business server contents and customize the Web page so that the user accesses the Sign-off URL at the time of Sign-off. For details about adding the link, refer to "Customizing the Web page for Sign-off".

- SSO administrator

  Customizing the Sign-off query message

  The Sign-off query message can be customized to display to the user in the application window. The Sign-off completion and cancellation message can also be customized.

  Messages can also be customized by editing the following message file that is stored on the Authentication server. For details about customizing messages, refer to "Customizing Messages Displayed on a Web browser".

  - Sign-off query message

    200querysignoff_en.template

  - Sign-off completion message

    200signoff_en.template

  - Sign-off cancellation message

    403cancelsignoff_en.template

1.5 Authorization

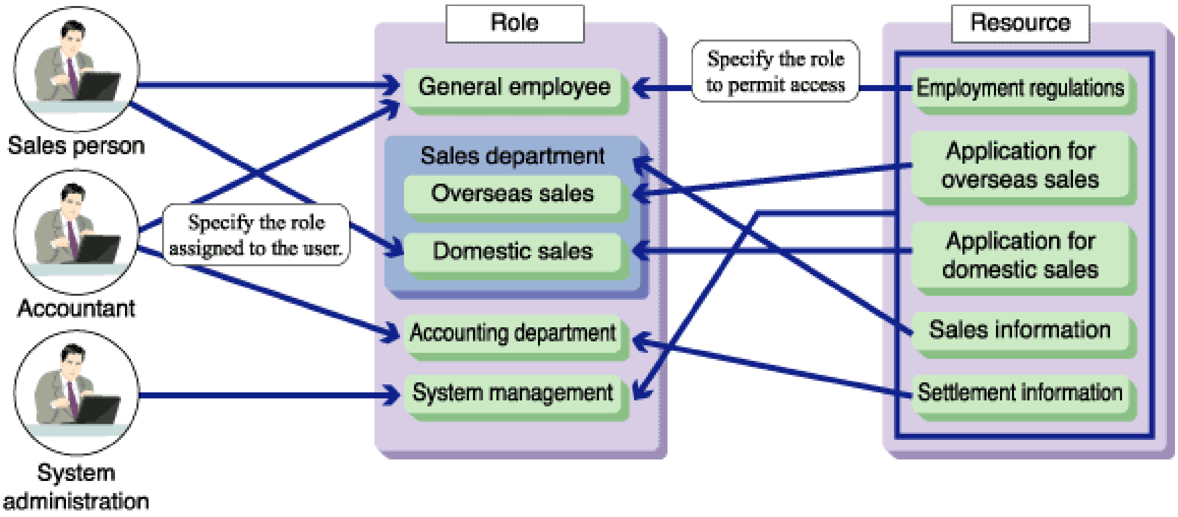
Authorization is the process that is used to make sure that the user who requests access to a resource is allowed to access the resource. A user who requests access to a resource, for example, a HTML document, image data, or voice data disclosed on a Web server or a CGI application operating on a Web server; is checked to allow access to the resource.

Interstage Single Sign-on authorizes users' access based on the concept of "role," which is an attribute indicating a department or business. Whether a user is allowed to access a resource is determined according to the relationship between the role of the user and the role set for the access target resource. The relationships between resources and roles are managed as access control information.

1.5.1 Relationships between Roles, Users, and Resources

Roles are defined based on actual departments and businesses, e.g., "general employee" and "domestic sales," and assigned to user information. On the other hand, the roles required to access resources, including the HTML and CGI resources disclosed by the Web services on business servers, are set for the respective resources. When a user accesses a resource, the user must succeed in authentication and have the role that is set for the target resource.

Figure 1.38 Relationships Between, Roles, Users and Resources



In the above example:

- The roles "general employee" and "accounting department" are assigned to the accountant.
- The role "general employee" is permitted to access only the resource "employment regulations."
- The role "accounting department" is permitted to access only the resource "settlement information."
- Therefore, the accountant can access only the resources "employment regulations" and "settlement information."

Multiple roles can be grouped as a role set. In the above example:

- The role set "sales department" contains two roles, such as "overseas sales" and "domestic sales."
- Because the resource "sales information" permits both "overseas sales" and "domestic sales" to access the resource, the role set "sales department" can be set for the resource.
- Because the resource "application for domestic sales" is intended to permit only the role "domestic sales" to access the resource, only the role "domestic sales" should be assigned to the resource.

As described above, the concept of role can be used to implement authorization in a flexible manner.

1.5.2 Information Required for Authorization Using Roles

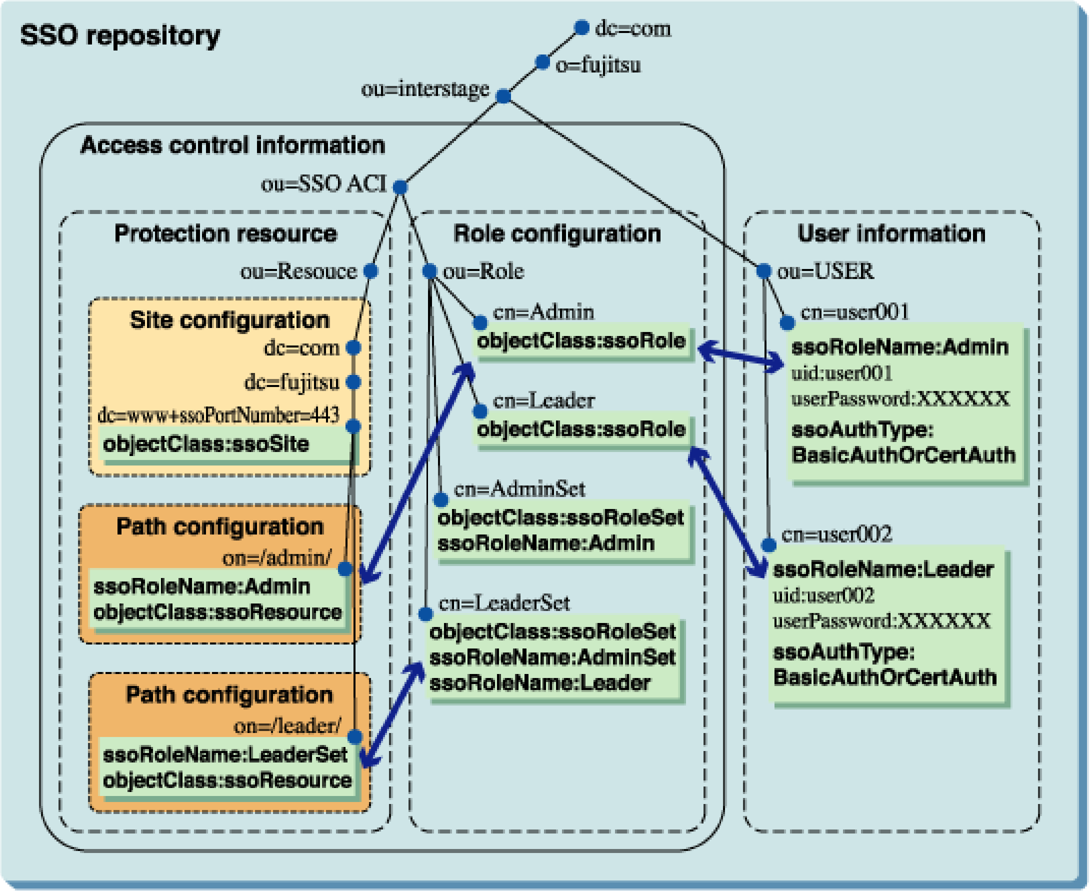
The following information required for the authorization using roles must be registered in the SSO repository.

1. Role Configuration

2. 1.4.5 User Information
3. Protection Resource

The following shows examples of configurations in the SSO repository. Access control information is a set of role configuration and protection resource information.

Figure 1.39 Information Required for Authorization Using Roles



Role Configuration

The role or role set name to be used is registered as a role configuration.

Roles are used to authorize the users who access the business system. Roles must be designed on the basis of the departments and businesses of the users who use the business system. To define a post, e.g., "general employee" or "manager," or a department, e.g., "accounting department" or "administration department," as a role, use the role name that corresponds to the post or department as shown in the table below to define it in the SSO repository.

When multiple roles are grouped and defined as a role set according to the hierarchy of organization and assigned to resource information, the system has the flexibility to accommodate the future changes in organization.

Note

Interstage Single Sign-on provides authorization with a role. Please be sure to perform a role configuration to the SSO repository. Unless role configuration is performed, a repository server does not start.

Table 1.4 Examples of Roles

Post/department	Role name
General employee	Employee
Executive officer	Executives
Accounting department	finance department

Post/department	Role name
Administration department	administration department

Table 1.5 Example of Role Set

Post/department	Role set name	Contained role
All employees	all	employee, executives

User Information

For details of user information, refer to "User information".

Protection Resource

If authentication and authorization are required for users to access resources such as HTML documents and CGI applications disclosed in the business system, define those resources as protection resources.

Protection resource information consists of site and path configurations.

Site Configuration

The site configuration defines the site name of the business system. The format of site name is "fully qualified domain name (FQDN) + port number." FQDN is the host name that includes domain name.

When the Business system public URL is "https://www.fujitsu.com:443/index.html", the site name is "www.fujitsu.com:443".

Path Configuration

The path configuration specifies the name of the directory or file that is disclosed on the site defined by the site configuration and requires authentication and authorization for access. When a directory name is specified (when the path name ends with "/"), all resources under the specified directory are the targets of authentication and authorization.

In addition, the names of the roles and role sets that are permitted to access the specified directories or files are specified. Multiple roles and role sets can be specified.

The specification of path configurations used for authentication and authorization is described below:

- When a directory or folder that is not defined by path configuration is accessed, the relevant resource is disclosed unconditionally.
- When only a directory or folder is specified and roles or role sets are not defined for the resource, the resource is disclosed to only authenticated users.
- When a directory or folder is specified and roles or role sets are defined for the resource, the resource is disclosed to only the users who are authenticated and permitted to access the resource.

Extended user information can be set in the path configuration, and by doing so, information about the user's authentication can be sent to the Web application. For details about the extended user information, refer to "Linkage with Web Applications".

Note

- If a role or role set name set in the path configuration is not defined by role configuration, access control information cannot be updated on the business server. The role and role set names set in the path configuration must be the same as that defined by the role configuration.
- If a path that does not need to be made a target of access control was set for the protection path, then response might take some time when business system protection resources are accessed. Only set a path that needs to be a target of access control, so that it becomes a protection path.

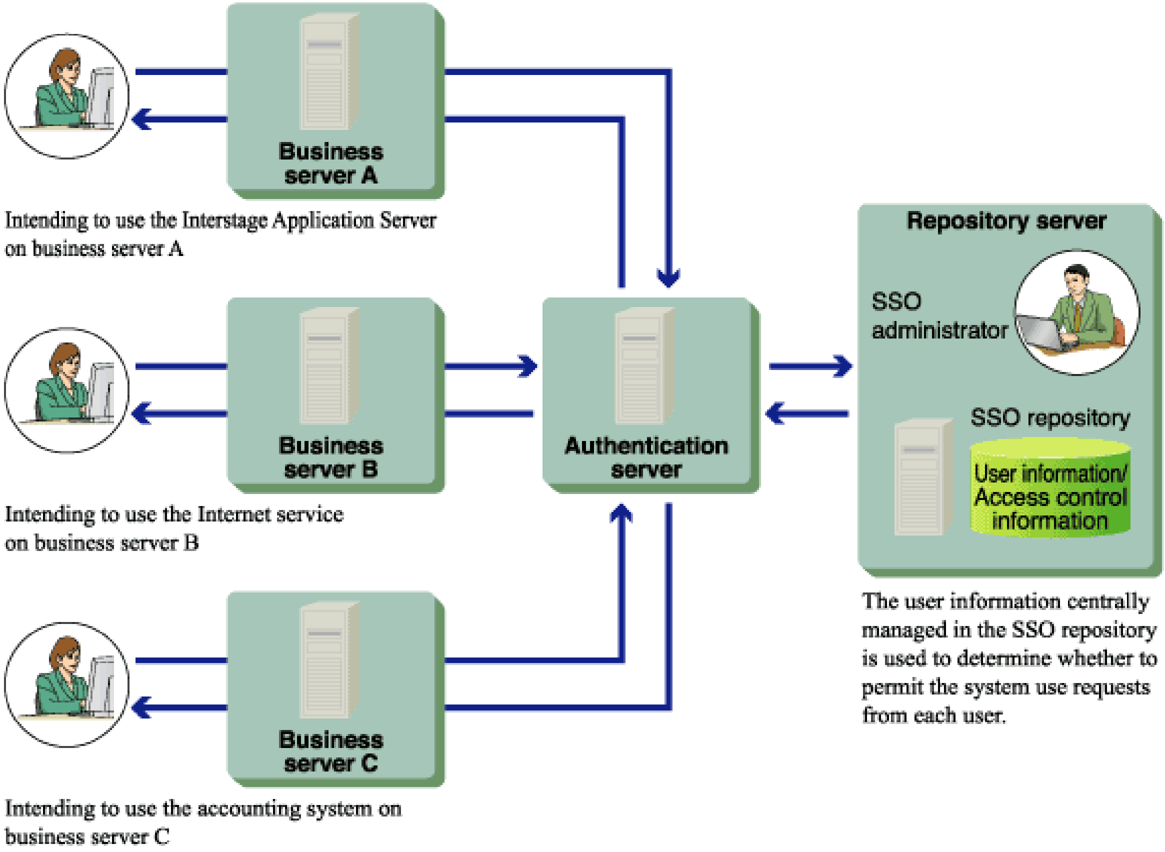
1.5.3 Centralized Management of User and Access Control Information

The user and access control information concerning the users of multiple systems can be centrally managed using the SSO repository to reduce the system administrators' load.

Example

The following diagram illustrates the centralized management using one SSO repository of the user and access control information concerning business servers A, B, and C.

Figure 1.40 Centralized Management of User and Access Control Information


Business server A
Intending to use the Interstage Application Server on business server A
Business server B
Intending to use the Internet service on business server B
Business server C
Intending to use the accounting system on business server C
Authentication server
Repository server
SSO administrator
SSO repository
User information/ Access control information
The user information centrally managed in the SSO repository is used to determine whether to permit the system use requests from each user.

1.5.4 Updating Access Control Information

The business server retains the access control information fetched from the SSO repository to reduce the load on the repository server and increase the processing speed of the business server itself.

If the access control information (role configurations, protection resources) registered in the SSO repository has been changed, access control information retained in the business server must be updated.

The following describes the methods of updating the access control information in the business server.

- Updating Access Control Information from the Interstage Management Console

  On the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Update access control information], and click [Update] to update the access control information. This operation can be performed even while the business server is active.

- Updating Access Control Information Automatically at Business Server Startup

  Access control information can be updated automatically at the startup of business server according to an environment setting. On the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]] to check or change the environment setting.

  Then, check or change the setting for [When updating Access Control Information?] under [Access Control Information]. When "Execute when Business server is started" is selected, the access control information is updated at the startup of business server.

When the access control information is updated, the Business server accesses the [Authentication server URL] specified when the Business system setup file is downloaded. For details about the Business system setup file, refer to "Downloading Business System Setup File".

To check/update [Authentication server URL] after the Business server setup, in the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]] > [Authentication Infrastructure Information Settings] > [Authentication server URL].

In systems in which session management is not used, the Business server accesses the [Repository Server URL] specified when the Business system setup file is downloaded. To check/update [Repository Server URL], in the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]] > [Authentication Infrastructure Information Settings] > [Repository Server URL].

After updating [Authentication server URL] or [Repository Server URL], restart the Business server.

Notes

- Changes to access control information (role configurations, protection resources) of the SSO repository are not reflected in business server authentication. To enable reflection of such changes, access control information must be updated in the business server.
- Note that, if "access control information is not updated at the start of the business server," is set, changing of the SSO repository is not reflected even if the business server is restarted.
- If the access control information is updated while the business server is active, make sure that you access a protection resource after the update. This is important to ensure that authentication and authorization can be performed normally. If authentication or authorization is not performed normally, updating may have failed.

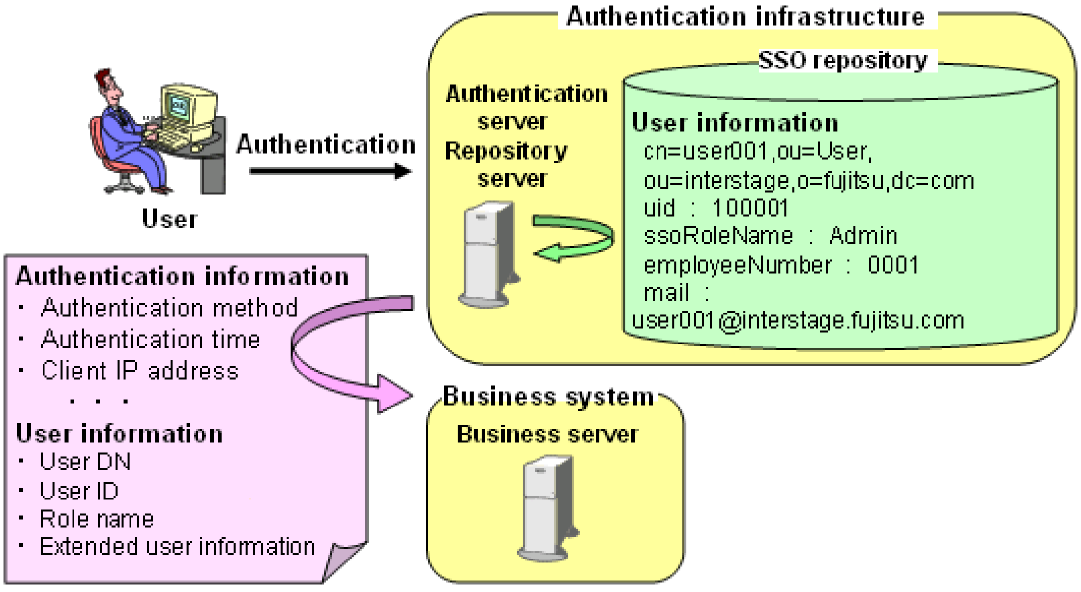
  If updating of access control information has failed, the business server responds to every access from user with message "500 Internal Server Error".

  Check those messages output to the system log which begin with "sso", take corrective action, and stop and restart the business server. For details of message contents, refer to "Messages Beginning with 'sso'" in the Messages.
- If an error message is output after the access control information has been updated on the Interstage Management Console, the business server remains in the status to perform authorization according to the old access control information. In that case, stop the business server or take another measure as required until the business server has recovered from the error and the information is updated normally.

1.5.5 Linkage with Web Applications

Web applications can receive authentication information (such as the time a user authenticated and the authentication type used) as well as the user information stored in the SSO repository.

Web applications can also acquire arbitrary information stored in the SSO repository (for users that authenticated) as extended user information.



Authentication and User information is acquired using the following methods:

- Java application interface

  The Java application interface provided by Interstage Single Sign-on can be used to develop a Servlet application to receive authentication information from the client. For details, refer to "Developing Java Applications".

- HTTP request header

  User information can be set in the HTTP request header and posted to an application. The application can acquire the user information via a Web application interface, for example CGI. For further details, refer to "Setting User Information Report with Environment Variables".

Note

Extended user information is only available if session management is being used. To use this information, make settings in the [Extended user information] of [Information notified to the Business System], which is displayed by selecting [System] > [Security] > [Single Sign-on] > [Authentication Infrastructure] > [Repository Server] from the Interstage Management Console, and then clicking [Repository server detailed settings [Show]] in the [Settings] tab.

1.6 High-Performance and High-Reliability System

Interstage Single Sign-on supports high-performance and high-reliability systems such as client certificate verification, high-speed SSL communication, load balancing, and increased availability.

1.6.1 Load Balancing

Load on the authentication server or the repository server will increase if authentication requests or session evaluation requests from multiple users converge. This load can be balanced, and therefore eased, by increasing the number of machines on which these servers (repository or authentication) are installed.

Refer to "Setting Up the Authentication Server on Multiple Machines and the Repository Server on a Machine (Middle-scale System: Balancing the Authentication Server Load)" earlier in this chapter, for more information.

Refer to "Increasing the number of machines on which the repository server (update system) is installed" for more information.

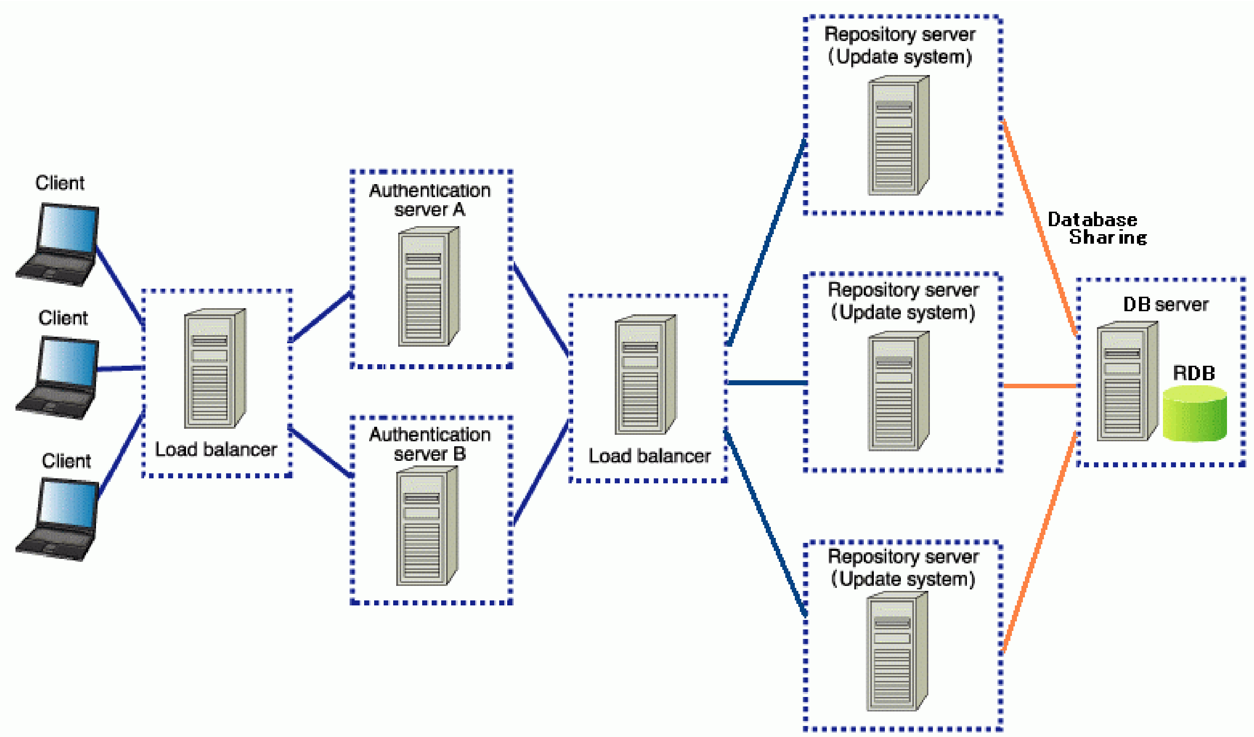
It is possible to use the old version with a compatible system configuration. However, it is not possible to use a repository server (reference system) if the following operation is performed in the environment after migration.

- Only Integrated Windows Authentication is authenticated.

To alleviate problems with the load on the repository server it is recommended that the number of repository servers (update system) be increased and that the system be configured to use load balancing.

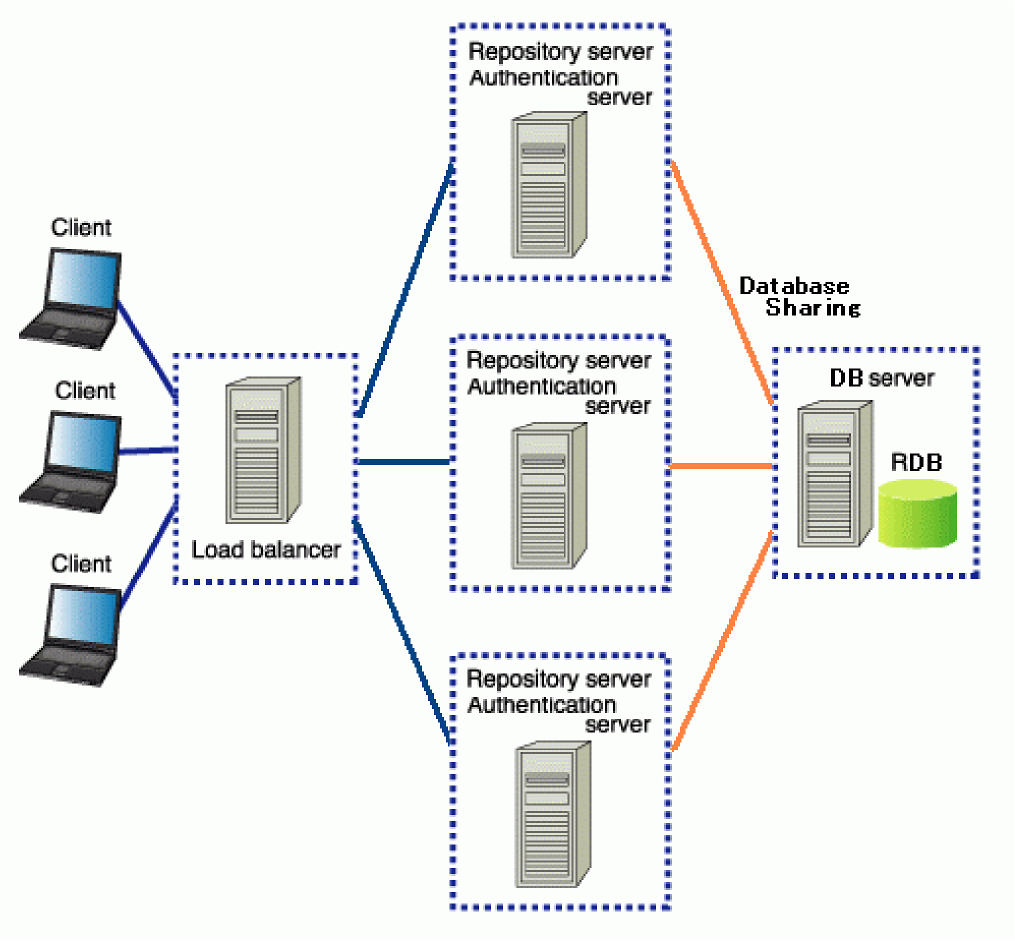
Increasing the Number of Machines on which the Repository Server (Update System) is Installed

The load on the repository server (update system) caused by requests such as authentication and session evaluation from the authentication server can be balanced by increasing the number of machines on which the repository server (update system) is installed.



In the above figure, the system configuration places a load balancer between the authentication server and the repository server, and because more than one repository server (update system) is installed the load on the repository server (update system) is balanced.

In the figure shown below, a load balancer is placed before a small-scale system in which the repository server and authentication server are set up on one machine, and because more than one repository server and authentication server are installed load balancing is possible.



Note

- The SSO repository must be updated from more than one repository server (update system), and the update must be reflected immediately. Create the SSO repository using the Directory Service database sharing function.
- The load balancer must be set so that more than one repository server (update system) logically uses one host name.
- The versions and editions that can be used on each server are different.

  Refer to 'Notes about Setting up Single Sign-on Systems Containing Mixed Versions and Editions' under 'Notes on Interstage Single Sign-on' in the 'Product Notes' for information about which versions and editions can be used.

Balancing on the Repository Server (Update System) and the Repository Server (Reference System)

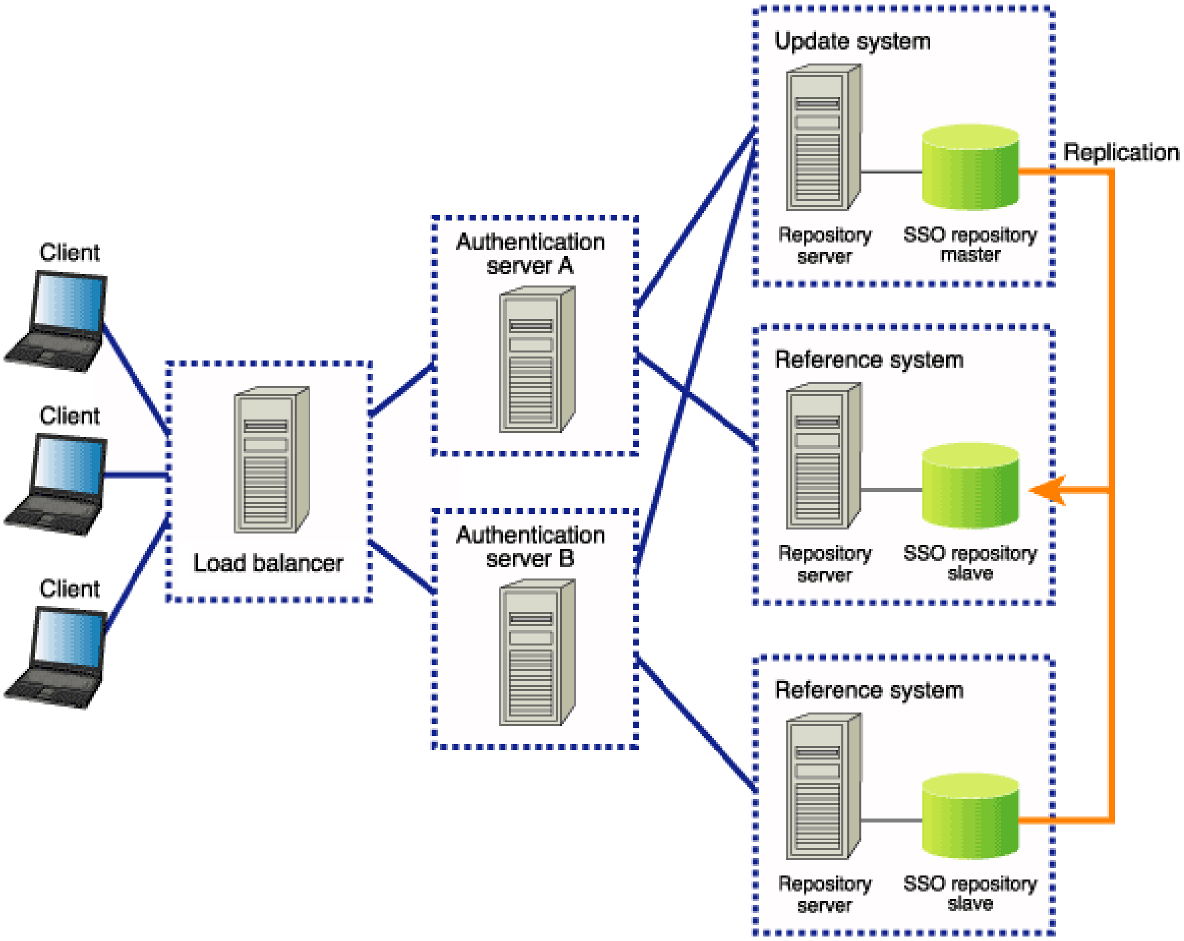
The authentication processing on the repository server can be distributed to two repository servers, repository server (update system) and repository server (reference system) in order to balance the load of authentication processing on the repository server (reference system).

To distribute authentication processing to the repository server (update system) and repository server (reference system), select, on the Interstage Management Console, [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]].

Then, specify the repository server (update system) and repository server (reference system) for [Communication Settings with Repository server] and [Communication Settings with repository Server (reference system)].

For details about the configurations on the Interstage Management Console, refer to the Operator's Guide.

Figure 1.41 Load Balancing among Authentication and Repository Servers



The figure above shows the load balancing among authentication and repository servers.

Authentication requests from clients are distributed to each authentication server by a load balancer.

By specifying one repository server (update system) and multiple repository servers (reference system), each authentication server is connected to a repository server (reference system) at the time of the authentication request, and to a repository server (update system) at the time of final confirmation.

Load balancing for repository servers (reference system) can be achieved by specifying different repository servers (reference system) in each authentication server.

When the information in the SSO repository of the repository server (update system) is updated, the updated content can be reflected in the SSO repository of the repository servers (reference systems) automatically by using the Interstage Directory Service replication function.

When a different repository server (reference system) is assigned to each authentication server as the one to be connected preferentially, the load on repository server (reference system) can be balanced.

For an example of setting a system configuration in which the repository server (update system) and repository server (reference system) are arranged to distribute the repository server (reference system) load, see "When Setting Up the Authentication Server and the Repository Server on Multiple Machines Individually" of "Basic Configurations of Authentication Infrastructure" of "Authentication Infrastructure".

Note

- When repository servers are used separately for update and reference systems, the contents of SSO repositories (master and slave) must be synchronized with each other to prevent illegal authentication due to data inconsistency. A synchronizing method is to copy the content of the SSO repository (master) into the SSO repository (slave) by using the Interstage Directory Service replication function.
- The repository server (update system) and repository server (reference system) both need to be the same edition/version.
- The load balancer must be set up so that all authentication servers logically have the same host name.

- To perform SSL communication on the authentication servers, the owner name of each certificate to be used for SSL communication must be the same on every authentication server. In details, the host name of the load balancer must be specified as the owner name of the certificate for SSL communication when the certificate is obtained and registered. For further information about the application for the certificate and its registration, refer to "Preparations for SSL Communication".

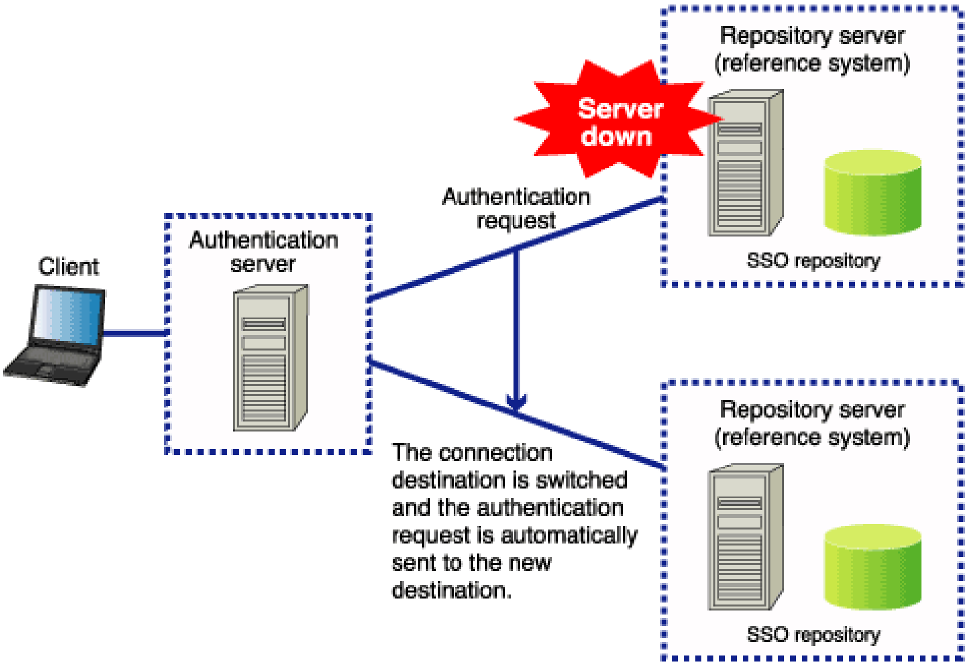
- The load balancer must be set up so that the requests from the same client transfer to the same authentication servers.

1.6.2 Increase of System Availability

When multiple repository servers (reference systems) are allocated to the authentication server, the system configuration can include active and standby repository servers (reference systems). This system configuration allows the system to continue operation even if a repository server (reference system) fails or an error is posted from an SSO repository.

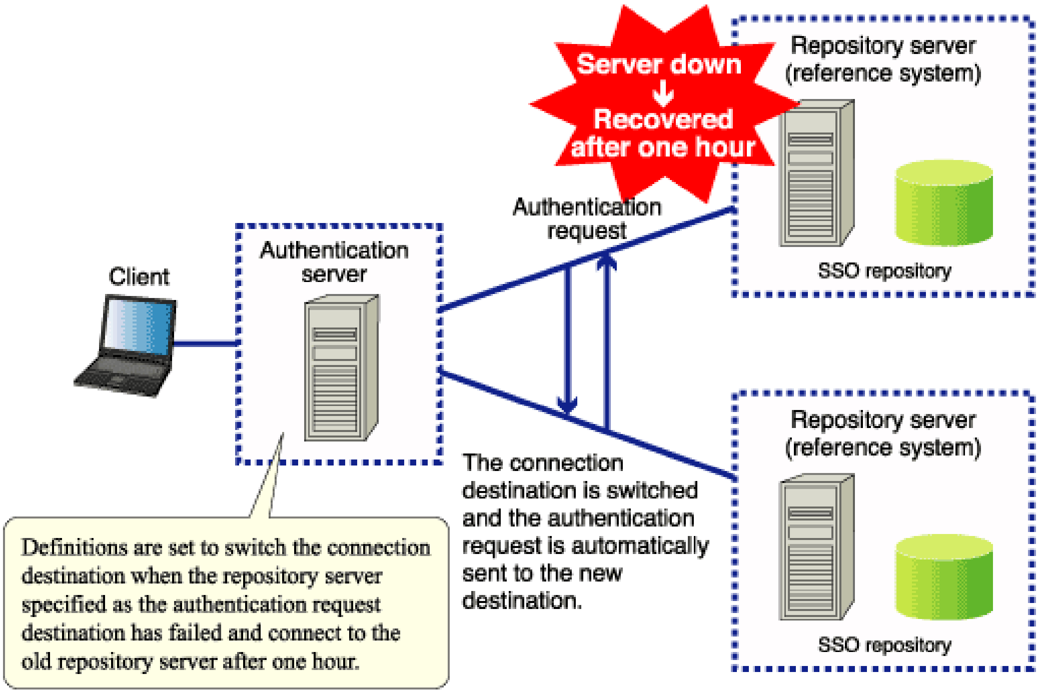
For example, if the repository server (reference system) that is requested to perform authentication processing by the authentication server has failed, a destination of the authentication request is automatically switched to another repository server (reference system) and the system can respond to the authentication request from the client.

Figure 1.42 Increasing System Availability


Repository server (reference system)
Server down
Authentication request
SSO repository
Client
Authentication server
The connection destination is switched and the authentication request is automatically sent to the new destination.
Repository server (reference system)
SSO repository

When the re-connection interval specified as an environment setting on the authentication server has elapsed after the automatic switching of authentication request destination, repository server (reference system), an attempt is made automatically to connect to the repository server (reference system) that was the destination for the old authentication request.

Figure 1.43 Standby Repository takes over in the Event of a Failure



Definitions are set to switch the connection destination when the repository server specified as the authentication request destination has failed and connect to the old repository server after one hour.

The connection destination is switched and the authentication request is automatically sent to the new destination.

This means that the Interstage Single Sign-on service can operate without a halt when multiple repository servers (reference systems) are installed.

To check the sequence of connections to the repository servers (reference systems) from the authentication server, select, on the Interstage Management Console, [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]]. The sequence of connections is indicated by [Repository server (reference system) URL] under [Communication Settings with Repository server (reference system)].

The authentication server attempts to connect to all the specified repository servers (reference systems) sequentially. If the authentication server cannot connect to any other repository servers, it attempts to connect to the first repository server (reference system) again. If the first repository server also cannot be connected, the authentication server notifies the user of the failure in authentication.

Note that the repository server (update system) can be operated as a repository server (reference system). When the repository server (update system) is specified as the last repository server (reference system) to be connected in the setting for [Communication Settings with Repository server (reference system)], the authentication server attempts to connect to the repository server (update system) after it has failed in attempts to connect to every repository server (reference system).

Notes

- Use repository servers with the same edition/version as the repository servers (update and reference systems).
- System availability can increase by using multiple repository servers (update systems). Note that Interstage Application Server Enterprise Edition supports the increase of system availability by using a cluster configuration of repository servers (update systems).
- If the repository server (update system) stops operation as the result of some problem, user authentication fails even when the repository server (reference system) can operate normally.

1.6.3 Linkage with SSL Accelerator

Interstage Single Sign-on allows SSL Accelerator to be installed between the client and authentication server to speed up client certificate authentication and SSL communication.

The speed of SSL can be increased by installing the SSL Accelerator between the Authentication server and the Repository server, or between the client and business server.

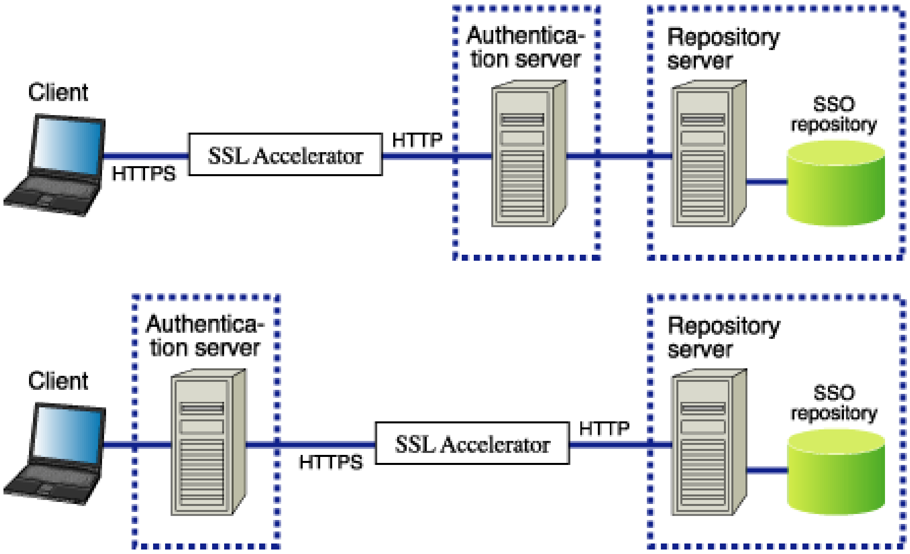
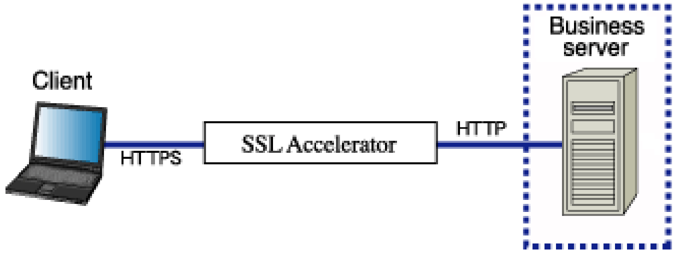


Figure 1.44 SSL Accelerator links the Client and Authentication Server



If the SSL Accelerator is installed between the client and the Authentication server, define the settings so that the SSL Accelerator is linked with the Authentication server. If the SSL Accelerator is installed between the Authentication server and the Repository server, there is no need to configure the Authentication server and Repository server settings. There is no need to configure the Business server settings to install SSL Accelerator between the client and the Business server.

To install SSL Accelerator between the client and the Authentication server, SSL Accelerator must be set up as follows:

Client Authentication

Configure the settings shown in the table below, depending on the user authentication method used in the Interstage Single Sign-on application. For details of the settings, refer to the SSL Accelerator manual.

Authentication method	Settings contents
Password authentication	Configure the settings so that client authentication is not used. (*1)
Certificate authentication	Configure the settings so that client authentication is used. (*1)
Password authentication and certificate authentication	
Password authentication or certificate authentication	Configure the settings so that submission of the client certificate is requested but authentication is not performed.

*1 The settings can also be configured so that submission of the client certificate is requested but authentication is not performed.

Notification of Certificate

When the authentication method is "certificate authentication" or "password or certificate authentication", or "password authentication and certificate authentication," define the HTTP header to notify the authentication server of the certificate sent from the client. For details about the configuration method, refer to the relevant SSL accelerator instruction manual.

The defined HTTP header must be set on the authentication server. On the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]]. Then, set the defined HTTP header name as [HTTP header name for user certificate acquisition] under [Certificate Authentication Settings].

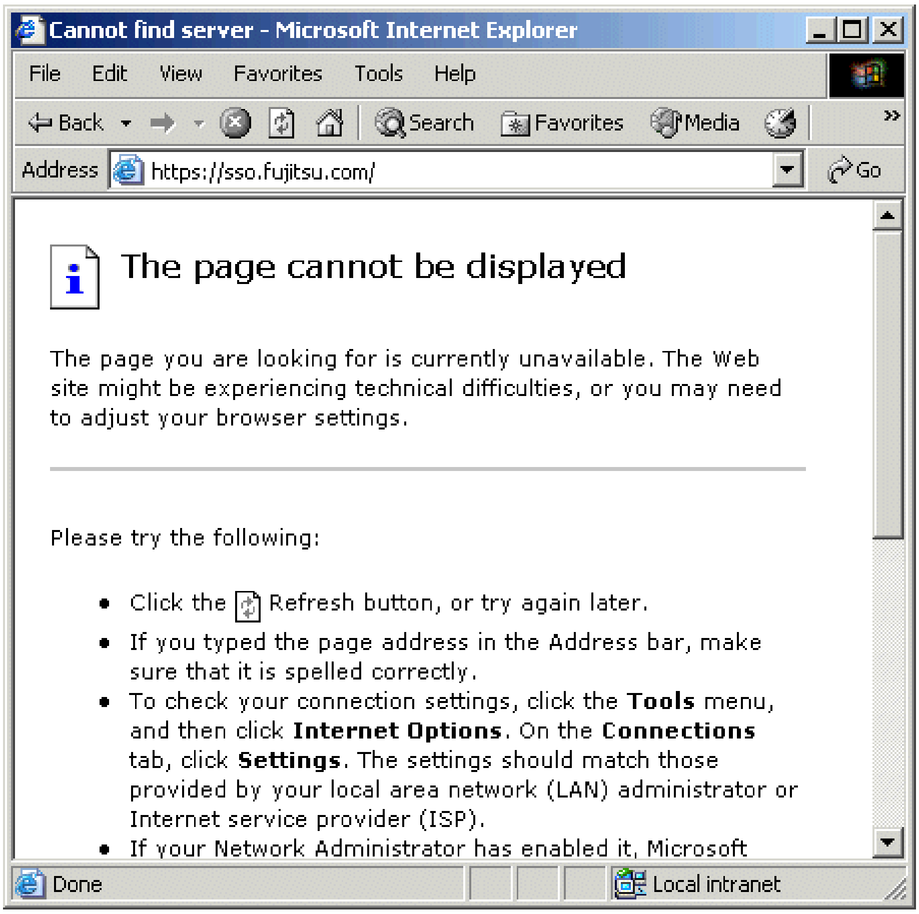
This setting is not required when SSL Accelerator is used for the business system.

For details about the configurations on the Interstage Management Console, refer to the Operator's Guide.

Notes

- If an expired certificate is used, depending on the product used in SSL Accelerator the message "500 Internal Server Error" may be sent to the Web browser. In this case, acquire a new certificate and register it in the Web browser.
- Configure the settings so that confirmation of the certificate validity is performed in the authentication server.
- If client authentication is not used, or for integration with SSL Accelerator that is set for client authentication, user authentication methods cannot be mixed. Use the same authentication method at all users.
- For integration with SSL Accelerator that is set for client authentication, the certificate must be selected when authentication is requested. If the sending of the certificate was canceled, communication processing in SSL Accelerator is disconnected, the window shown below is displayed, and access to the requested resource is canceled.

Figure 1.45 Example of Screen Shown when Page cannot be Displayed



Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.com/
Go
Done
Local intranet

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft

1.6.4 Linkage with Application Gateway

The reverse function offered in Application Gateway can be used to access a safer intranet from a client on the Internet.

The reverse function can be used to set up the following systems:

- A Single Sign-on system in which access from a client on the Internet and a client in an intranet is possible
- A Single Sign-on system in which only access from a client on the Internet is possible

In the above systems, the following operation can also be executed, depending on the communication method between Application Gateway and the authentication server:

- Non-SSL communication between Application Gateway and the authentication server
- SSL communication between Application Gateway and the authentication server

The settings for a system that can be set up using the Application Gateway reverse function are explained below.

Note

- In a system that has linkage with Application Gateway, the following can be used as the authentication method for a user accessing from the Internet.
    - Password authentication
- When SSL communication is used between the Application Gateway and authentication server, security can be further enhanced.

1. Single Sign-on System that can be Accessed from the Clients on the Internet and in the Intranet

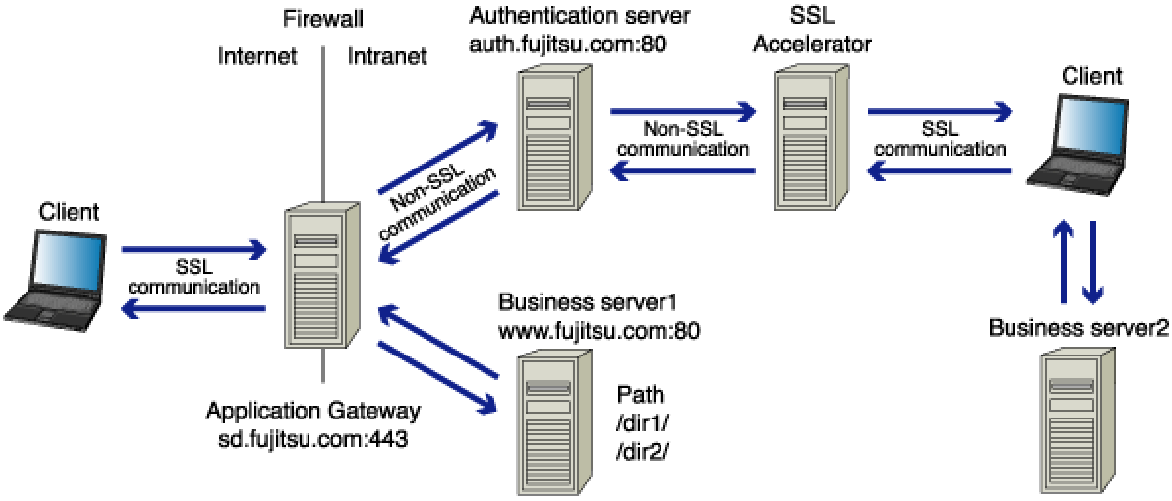
The following describes the Single Sign-on system that can be accessed from both the clients on the Internet and also those in the intranet.

Note the following point for the operations of this system.

- The URL information on the business system in the intranet may also be transmitted as a URL parameter to the client who accesses the system via the Internet.

Using non-SSL Communication between Application Gateway and Authentication Server

Figure 1.46 Using non-SSL Communication between Application Gateway and Authentication Server



For operation using this system configuration, SSL Accelerator must be installed between the authentication server and client in the intranet. The port number of SSL Accelerator must be the same as that used by Application Gateway.

Note

This system cannot be configured if the mechanism that is used for communication with the virtual IP address is used in the SSL accelerator.

Setup of Application Gateway

- Reverse Settings

    Examples of the reverse settings in the figure above are shown in the table below.

    In the URL for the directory from which the request originated that is entered in the business server reverse settings, specify a directory layer for each business server. Example: /www1/, /www2/.

Table 1.6 Reverse Settings

Request-source URL	Conversion control	Relay-destination URL	Remarks
https://sd.fujitsu.com:443/www1/	<---------->	http://www.fujitsu.com:80/	Reverse settings of Business server
https://sd.fujitsu.com:443/auth/	<---------->	http://auth.fujitsu.com:80/	Reverse settings of Authentication server
https://sd.fujitsu.com:443/auth/	<----------	https://auth.fujitsu.com:443/	

When "Set-Cookies Header" is specified in the HTTP response header, and path and domain that are specified to "Set-Cookies Header" are same as directory and server name of Relay-destination URL that is defined in the above table, set path and domain as to replace the compatible Request-source URL.

Setup of authentication server

- For a small-scale system

  When using a small-scale system, on the Interstage Management Console of the authentication server, select the [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication infrastructureSettings] tab > [Setup Repository server and Authentication server to a single server.]. Select a Web server that does not use SSL in [General Settings]> [Use Web server].

- For a middle-scale or large-scale system

  When using a medium-scale or large-scale system, on the Interstage Management Console of the authentication server, select the [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication infrastructureSettings] tab > [Setup Repository server and Authentication server to the separate servers.]. Select [Create a new Authentication server], and specify the Authentication infrastructure setup file in [File Settings], and then click [Next]. Select a Web server that does not use SSL in [General Settings]> [Use Web server].

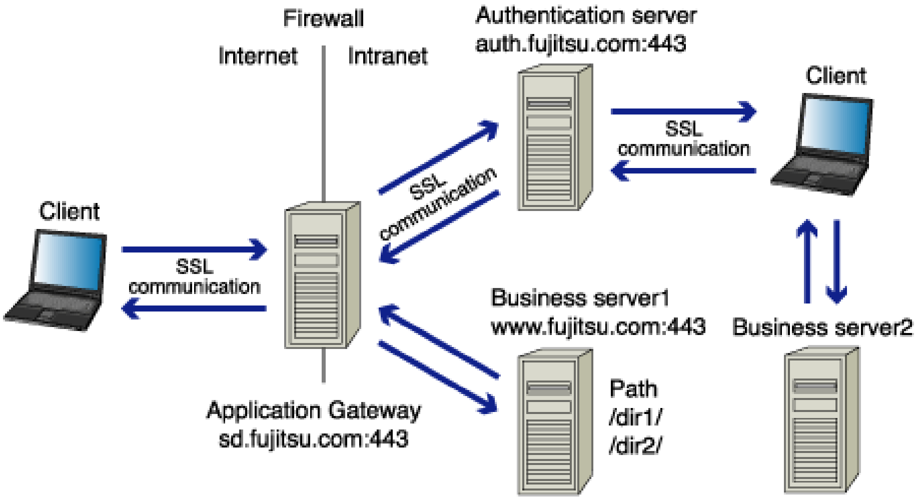
Business system setup file settings (*1)

In the Interstage Management Console of the Repository server (if more than one is used, the update system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Business system setup file] > [Detailed Settings [Show]] > [Authentication Infrastructure Information Settings], and in [Authentication server URL], specify the URL used by the Business system to reference the Authentication server For details about the URL, refer to 1.7.4 URL Used by the Business System to Reference the Authentication Server.

*1 These settings are only necessary if Session Management is used.

Using SSL Communication between Application Gateway and Authentication Server

Figure 1.47 Using SSL Communication between Application Gateway and Authentication Server



To operate using this system configuration, use the following settings.

Setup of Application Gateway

- Reverse Settings

  Examples of the reverse settings in the figure above are shown in the table below.

  In the URL for the directory from which the request originated that is entered in the business server reverse settings, specify a directory layer for each business server. Example: /www1/, /www2/.

Table 1.7 Reverse for Application Gateway

Request-source URL	Conversion control	Relay-destination URL	Remarks
https://sd.fujitsu.com:443/www1/	<---------->	https://www.fujitsu.com:443/	Reverse settings of Business server
https://sd.fujitsu.com:443/auth/	<---------->	https://auth.fujitsu.com:443/	Reverse settings of Authentication server

When "Set-Cookies Header" is specified in the HTTP response header, and path and domain that are specified to "Set-Cookies Header" are same as directory and server name of Relay-destination URL that is defined in the above table, set path and domain as to replace the compatible Request-source URL.

Setup of authentication server

To create SSL configurations on the authentication server, select [System] > [Security] > [SSL] > [Create a new SSL Configuration] tab. Then, specify "No" for [Verify Client Certificate?] under [General Settings].

2. Single Sign-on System that can be Accessed Only from the Clients on the Internet

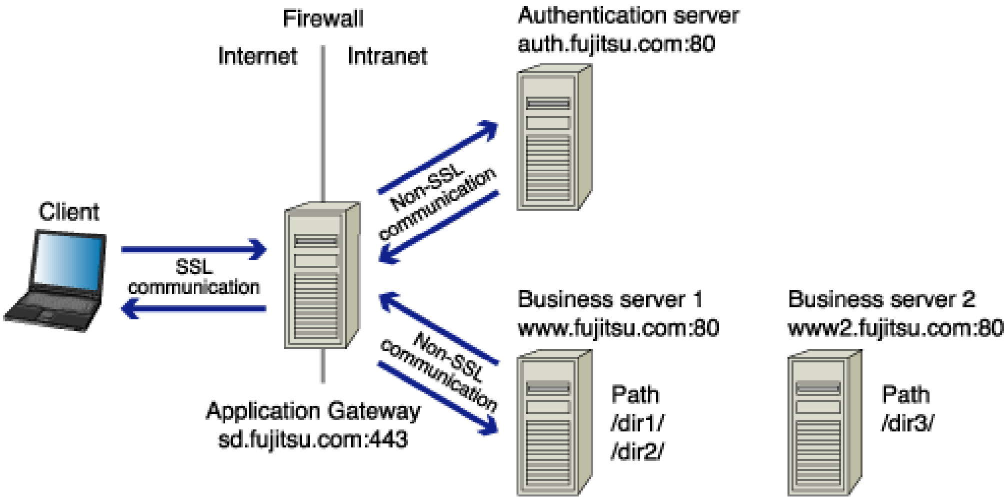
The following describes the Single Sign-on system that can be accessed only from the clients on the Internet.

Note the following points for the operations of this system.

- The clients in the intranet cannot access the protection resources in the business system.
- Note the following points for the design of business systems.
  - The first layer of the URL path of each business system must be unique.
  - The root path ("/") of the business system cannot be accessed by clients.

Using non-SSL communication between Application Gateway and Authentication Server

Figure 1.48 Using non-SSL Communication between Application Gateway and Authentication Server



To operate using this system configuration, make the following settings.

Setup of Application Gateway

- Reverse Settings

  Examples of the reverse settings in the figure above are shown in the table below.

  In the business system reverse settings, make sure that the path part for the URL for the directory from which the request originated and the URL for the directory from which the relay originated are the same. Specify everything in the first directory layer of the business system URL.

Table 1.8 Examples of Reverse Settings

Request-source URL	Conversion control	Relay-destination URL	Remarks
https://sd.fujitsu.com:443/dir1/	<---------->	http://www.fujitsu.com:80/dir1/	Reverse settings of Business server 1
https://sd.fujitsu.com:443/dir1/	<----------	https://sd.fujitsu.com:443/dir1/	
https://sd.fujitsu.com:443/dir2/	<---------->	http://www.fujitsu.com:80/dir2/	
https://sd.fujitsu.com:443/dir2/	<----------	https://sd.fujitsu.com:443/dir2/	
https://sd.fujitsu.com:443/dir3/	<---------->	http://www2.fujitsu.com:80/dir3/	Reverse settings of Business server 2
https://sd.fujitsu.com:443/dir3/	<----------	https://sd.fujitsu.com:443/dir3/	
https://sd.fujitsu.com:443/auth/	<---------->	http://auth.fujitsu.com:80/	Reverse settings of Authentication server
https://sd.fujitsu.com:443/auth/	<----------	https://sd.fujitsu.com:443/	Reverse settings required for adding the business servers

  When "Set-Cookies Header" is specified in the HTTP response header, and path and domain that are specified to "Set-Cookies Header" are same as directory and server name of Relay-destination URL that is defined in the above table, set path and domain as to replace the compatible Request-source URL.

Setup of authentication server

- For a small-scale system

  When using a small-scale system, on the Interstage Management Console of the authentication server, select the [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication infrastructureSettings] tab > [Setup Repository server and Authentication server to a single server.]. Select a Web server that does not use SSL in [General Settings]> [Use Web server].

- For a middle-scale or large-scale system

  When using a medium-scale or large-scale system, on the Interstage Management Console of the authentication server, select the [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication infrastructure Settings] tab > [Setup Repository server and Authentication server to the separate servers.]. Select [Create a new Authentication server], and specify the Authentication infrastructure setup file in [File Settings], and then click [Next]. Select a Web server that does not use SSL in [General Settings]> [Use Web server].

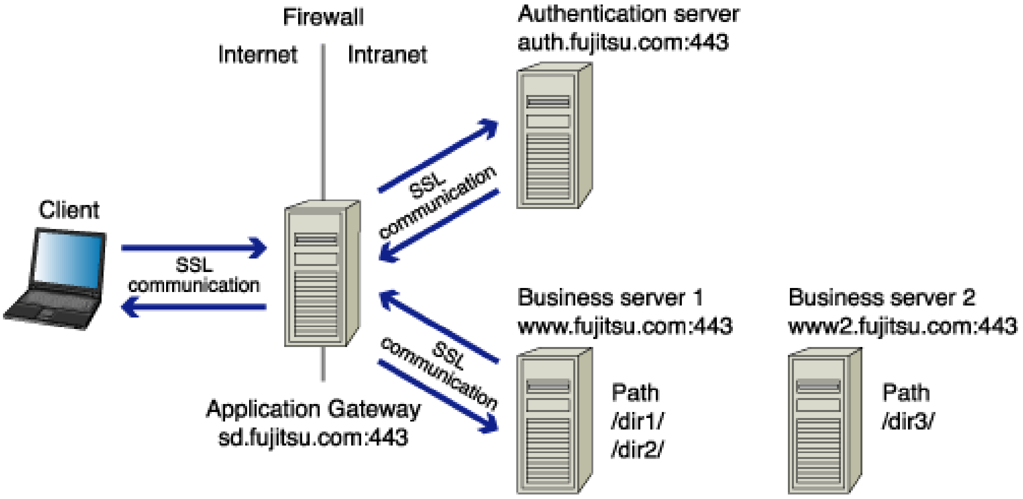
Business system setup file settings (*1)

In the Interstage Management Console, of the Repository server (if more than one is used, the update system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Business system setup file] > [Detailed Settings [Show]] > [Authentication Infrastructure Information Settings], and in [Authentication server URL], specify the URL used by the Business system to reference the Authentication server For details about the URL, refer to 1.7.4 URL Used by the Business System to Reference the Authentication Server.

*1 These settings are only necessary if Session Management is used.

Using SSL Communication between Application Gateway and Authentication Server

Figure 1.49 Using SSL Communication between Application Gateway and Authentication Server



Setup of Application Gateway

- Reverse Settings

  Examples of the reverse settings in the figure above are shown in the table below.

  In the business system reverse settings, make sure that the path part for the URL for the directory from which the request originated and the URL for the directory from which the relay originated are the same. Specify everything in the first directory layer of the business system URL.

Table 1.9 Reverse Settings for Application Gateway Setup

Request-source URL	Conversion control	Relay-destination URL	Remarks
https://sd.fujitsu.com:443/dir1/	<---------->	https://www.fujitsu.com:443/dir1/	Reverse settings of Business server 1
https://sd.fujitsu.com:443/dir2/	<---------->	https://www.fujitsu.com:443/dir2/	
https://sd.fujitsu.com:443/dir3/	<---------->	https://www2.fujitsu.com:443/dir3/	Reverse settings of Business server 2
https://sd.fujitsu.com:443/auth/	<---------->	https://auth.fujitsu.com:443/	Reverse settings of Authentication server
https://sd.fujitsu.com:443/	<----------	https://sd.fujitsu.com:443/	Reverse settings required for adding the business servers

When "Set-Cookies Header" is specified in the HTTP response header, and the path and domain that are specified to "Set-Cookies Header" are the same as the directory and server name of the Relay-destination URL defined in the abobe table, set the path and domain so as to replace the compatible Request-source URL.

Setup of authentication server

To create SSL configurations on the authentication server, select [System] > [Security] > [SSL] > [Create a new SSL Configuration] tab. Then, specify "No" for [Verify Client Certificate?] under [General Settings].

1.7 Choosing URLs

This section describes the Authentication infrastructure URL, the Business system public URL, the Repository server URL, and the URL used by the Business system to reference the Authentication server.

1.7.1 Authentication Infrastructure URL

The authentication infrastructure URL is determined according to its combination with the load balancer, SSL Accelerator, or Application Gateway installed before the authentication server.

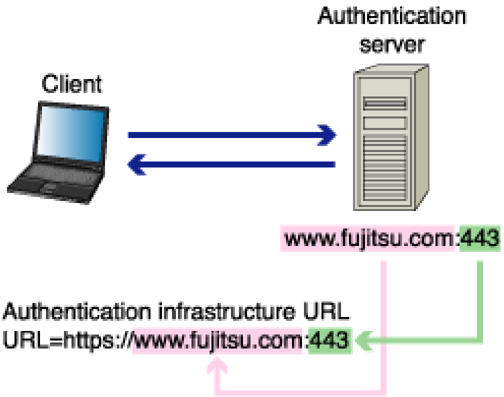
Basically, the authentication infrastructure URL consists of the FQDN and the port number of the device or the product installed before the authentication server, but it may differ according to the device and product combination.

The following describes examples of combinations with the load balancer, SSL Accelerator, and Application Gateway.

Combining no Other Equipment or Product

The FQDN and port number for the Authentication infrastructure URL are the same as those used by the authentication server.

Figure 1.50 Combination of no Other Equipment or Product

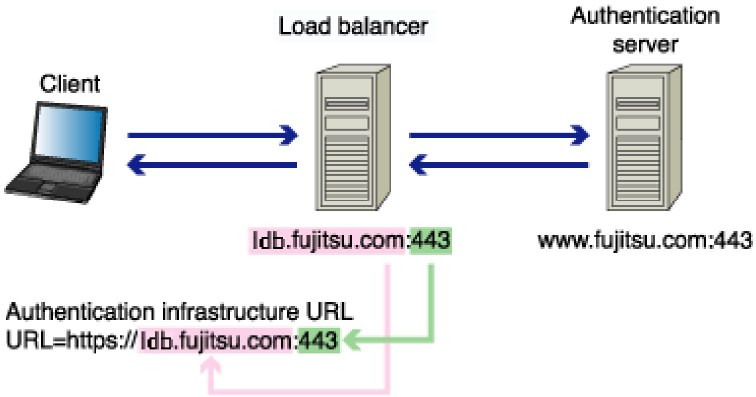

Authentication server
Client
www.fujitsu.com:443
Authentication infrastructure URL
URL=https://www.fujitsu.com:443

Using a Load Balancer to Balance the Authentication Server Load

The FQDN and port number of the Authentication infrastructure URL are identical to those of the virtual IP address that is set for the load balancer.

For the virtual IP address, refer to the load balancer manual.

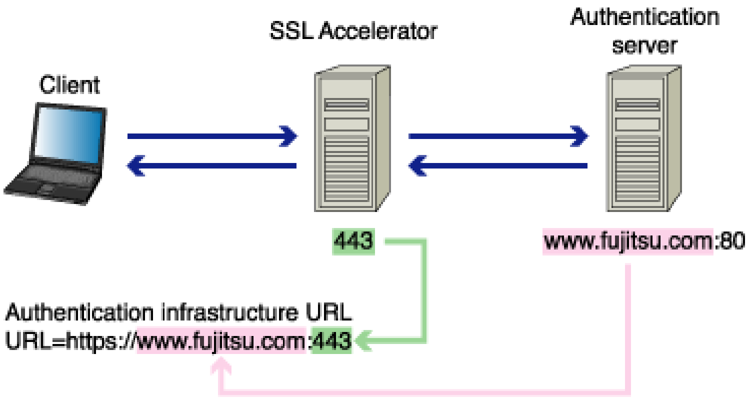
Figure 1.51 Using a load balancer to Balance the Authentication Server Load



Using SSL Accelerator

The FQDN and port number of the Authentication infrastructure URL are identical to the FQDN of the authentication server and the port number of SSL Accelerator, respectively.

Figure 1.52 Using SSL Accelerator

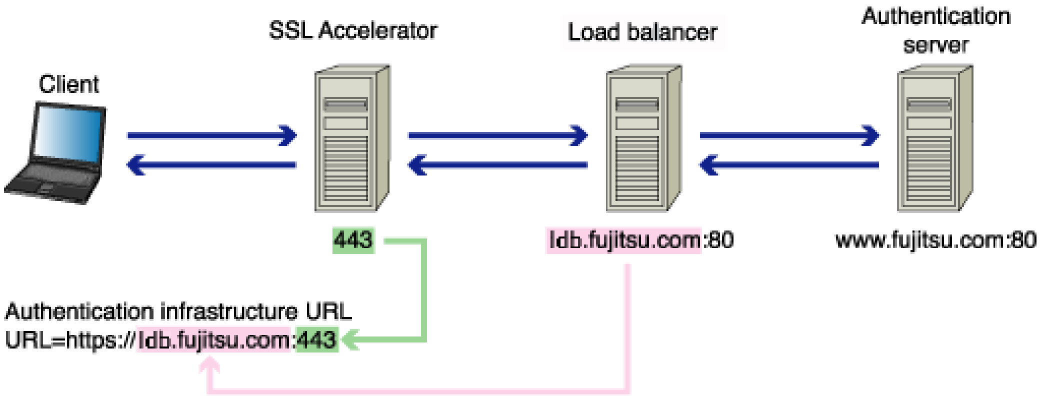

SSL Accelerator
Authentication server
Client
443
www.fujitsu.com:80
Authentication infrastructure URL
URL=https://www.fujitsu.com:443

Using Both SSL Accelerator and Load Balancer

The FQDN and port number of the Authentication infrastructure URL are identical to the FQDN of the virtual IP address set for load balancer and the port number of SSL Accelerator, respectively.

For the virtual IP address, refer to the load balancer manual.

Figure 1.53 Using Both SSL Accelerator and load balancer

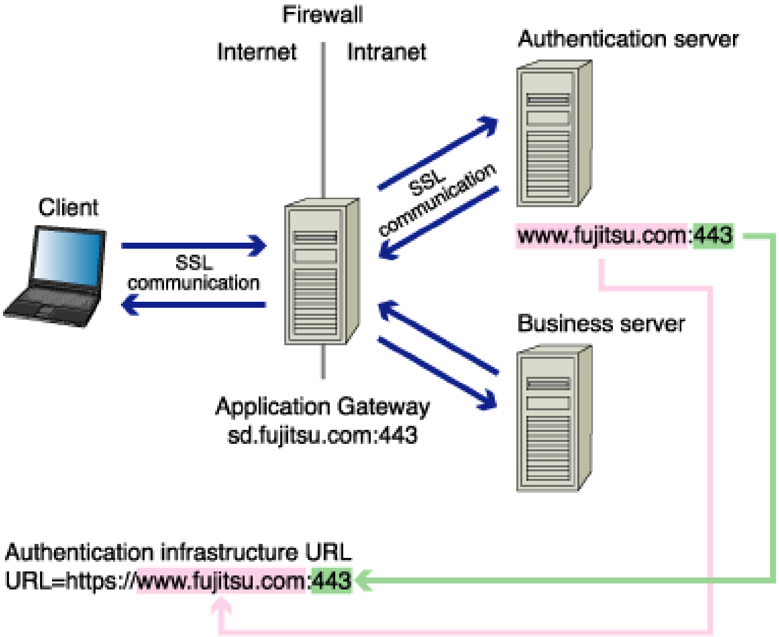


Linking with Application Gateway and using SSL Communication between Application Gateway and Authentication Server

The FQDN and port number of the Authentication infrastructure URL are identical to the authentication server (*1).

The Authentication infrastructure URL is different from the URL viewed from the client.

Figure 1.54 Linking with Application Gateway and Using SSL Communication between Application Gateway and Authentication Server



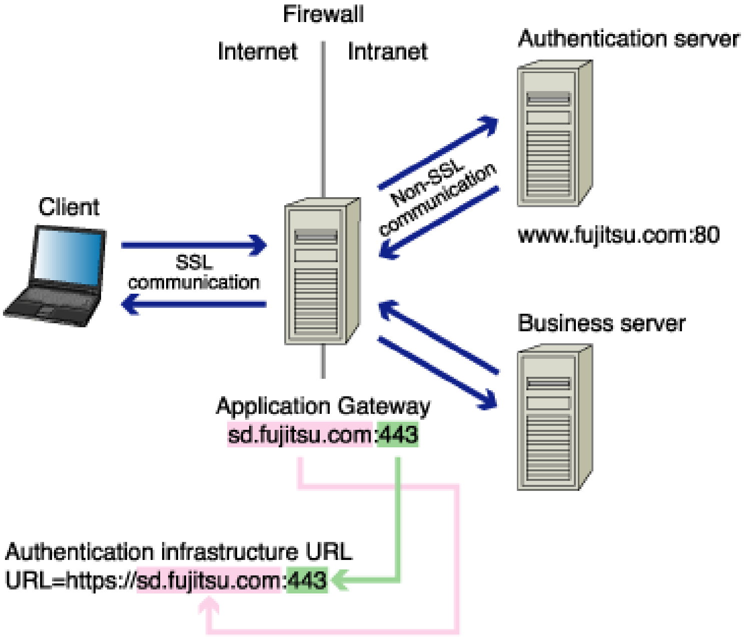
*1 When load balancer or SSL Accelerator is installed between Application Gateway and authentication server, assume that Application Gateway as the client and obtain the Authentication infrastructure URL based on the previous explanation. Use the FQDN and port number of the obtained URL as substitutes for those used in the authentication server.

Linking with Application Gateway and Using Non-SSL Communication between Application Gateway and Authentication Server

To enable the clients only on the Internet to access

The FQDN and port number of the Authentication infrastructure URL are the FQDN and the port number of Application Gateway, respectively. The scheme name of the Authentication infrastructure URL is "https".

Figure 1.55 Linking with Application Gateway and Using Non-SSL Communication between Application Gateway and Authentication Server

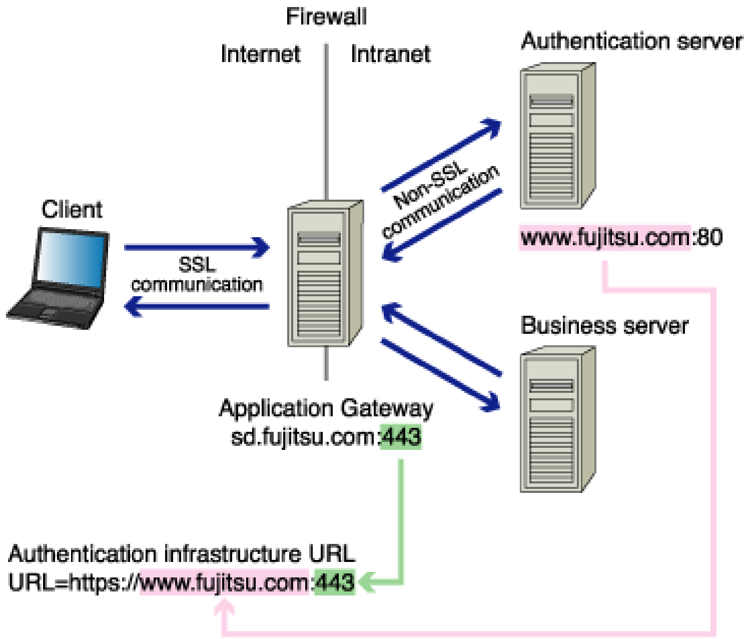


To enable access for the clients both on the Internet and in the intranet

The FQDN and port number of the Authentication infrastructure URL are the FQDN of the authentication server (*1) and the port number of Application Gateway, respectively. The scheme name of the Authentication infrastructure URL is "https".

The Authentication infrastructure URL is different from the URL viewed from the client.

Figure 1.56 Non-SSL Communication between Application Gateway and Authentication Server Viewed from the Client



*1 When load balancer is installed between Application Gateway and authentication server, assume Application Gateway as the client and obtain the Authentication infrastructure URL based on the information from the explanation described in the abobe figure. Use the FQDN of the obtained URL as a substitute for the FQDN of the authentication server.

Note

When using SSL Accelerator with the mechanism that uses the virtual IP address as transfer measure, the FQDN of the Authentication infrastructure URL is the FQDN of the IP address set for SSL Accelerator.

1.7.2 Business System Public URL

The business system public URL is determined according to its combination with the load balancer, SSL Accelerator, or Application Gateway that is installed before the business server.

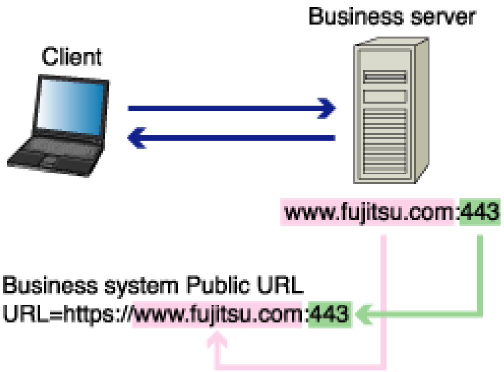
Basically, the business system public URL consists of the FQDN and the port number of the device or the product installed before the business server. However, it may differ according to the device and product combination.

The following describes examples of combinations with load balancer, SSL Accelerator, and Application Gateway.

Combining No Other Equipment or Product

The FQDN and port number of the Business system public URL are identical to those of the business server.

Figure 1.57 Combining No Other Equipment or Product

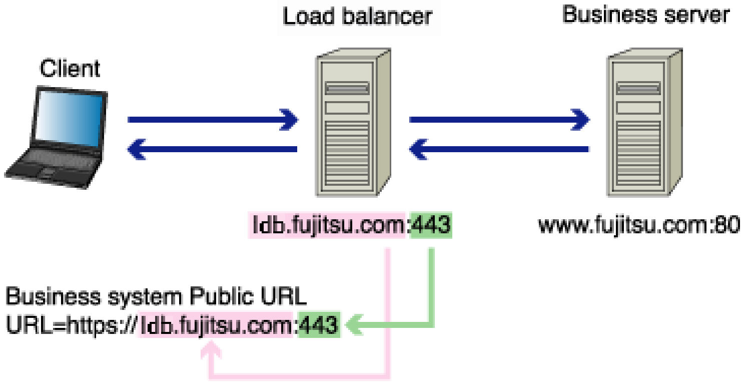


Using a load balancer to Balance the Business Server Load

The FQDN and port number of the Business system public URL are identical to those of the virtual IP address set for load balancer.

For details about the virtual IP address, refer to the load balancer manual.

Figure 1.58 Using a load balancer to Balance the Authentication Server Load

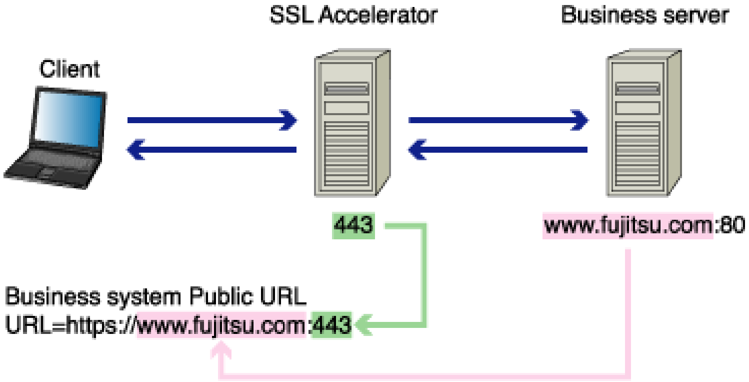


Using SSL Accelerator

The FQDN and port number of the Business system public URL are identical to the FQDN of the business server and the port number of SSL Accelerator, respectively.

For details about the virtual IP address, refer to the load balancer manual.

Figure 1.59 Using SSL Accelerator

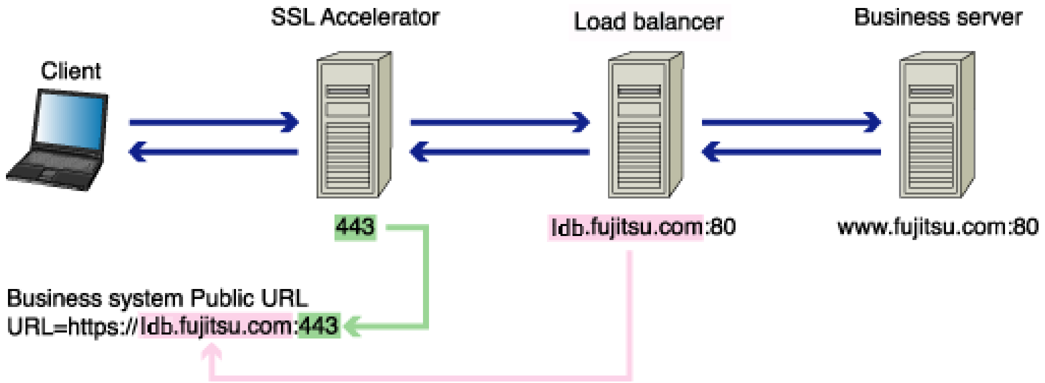


Using both SSL Accelerator and Load Balancer

The FQDN and port number of the Business system public URL are identical to the FQDN of the virtual IP address set for load balancer and the port number of SSL Accelerator respectively.

For details about the virtual IP address, refer to the load balancer manual.

Figure 1.60 Using Both SSL Accelerator and Load Balancer

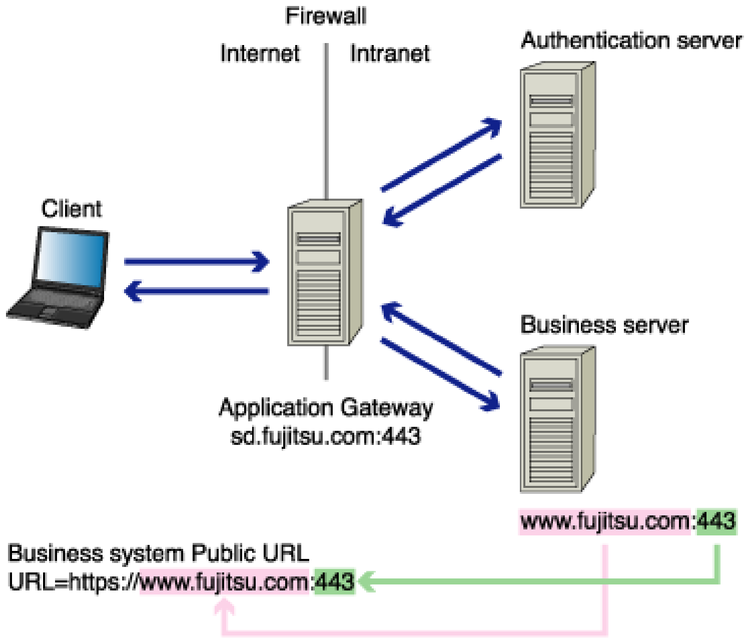


Linking with Application Gateway and Enabling the Clients both on the Internet and in the Intranet to Access (*1)

The FQDN and port number of the Business system public URL are identical to those of the business server (*2).

The Business system public URL is different from the URL viewed from the client.

Figure 1.61 Linking with Application Gateway and Enabling Clients on the Internet and Intranet to Access



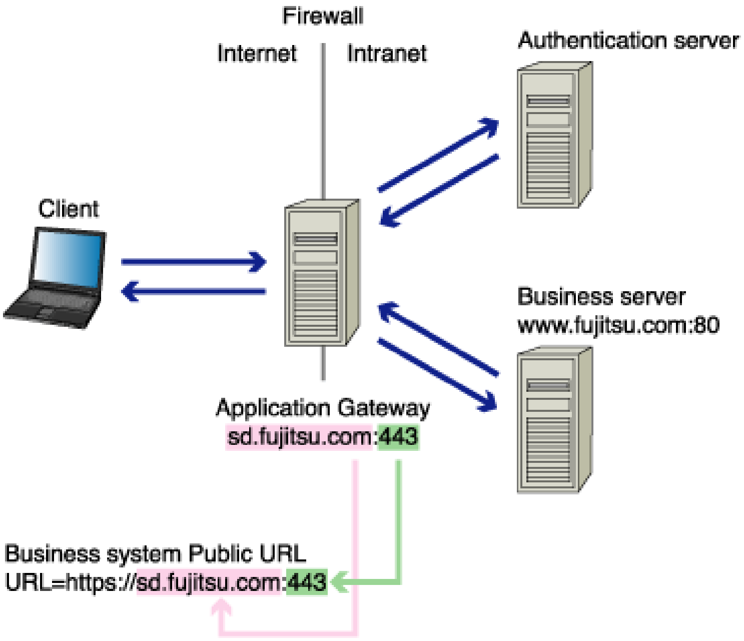
*1 For further details, refer to "Linkage with Application Gateway".

*2 When load balancer or SSL Accelerator is installed between Application Gateway and business server, assume Application Gateway as the client and obtain the Business system public URL according to the above explanation. Use the FQDN and port number of the obtained URL as substitutes for those of the business server.

Linking with Application Gateway and Enabling Only the Clients on the Internet to Access (*1)

The FQDN and port number of the Business system public URL are identical to those of Application Gateway.

Figure 1.62 Linking with Application Gateway and Enabling only Internet Clients to Access



For further details, refer to "1.6.4 Linkage with Application Gateway".

Note

When using SSL Accelerator with the mechanism that uses the virtual IP address as transfer measure, the FQDN of the Business system public URL are the FQDN of the IP address set for SSL Accelerator.

1.7.3 Repository Server URL

The repository server URL is determined according to its combination with the SSL Accelerator, load balancer, or cluster system that is installed before the repository server.

Basically, the repository server URL consists of the FQDN and the port number of the device or the product installed before the repository server, but it may differ according to the device and product combination.

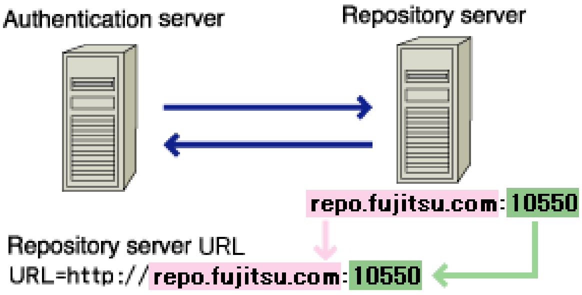
The cluster system is supported only by Interstage Application Server Enterprise Edition. If the repository server is set up on more than one machine, only the repository server (update system) supports cluster systems. For further details about the cluster system, refer to the High Availability System Guide for Interstage Application Server Enterprise Edition.

Combining no Other Equipment or Product

Not Using a Cluster System

When you are not using a cluster system, the Repository server FQDN and port number do not have other values.

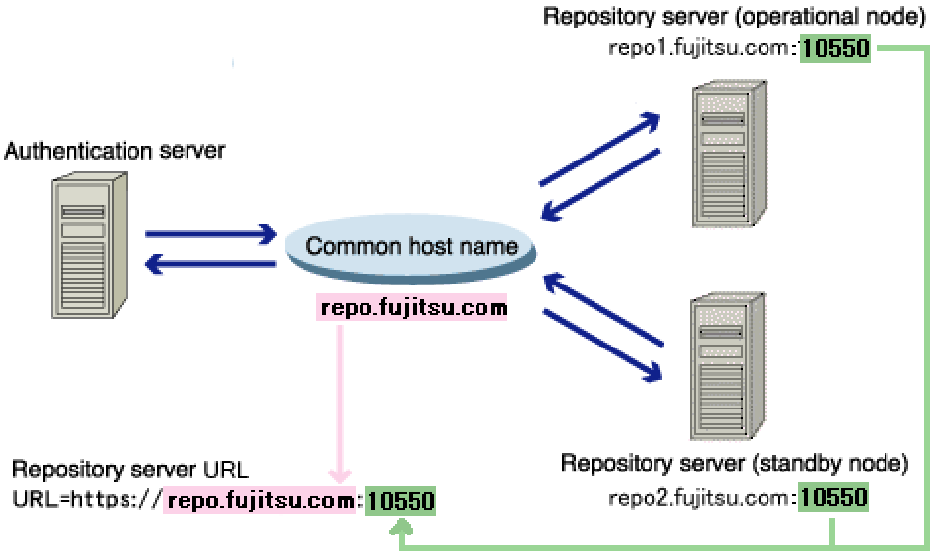
Figure 1.63 Not Using a Cluster System



In a cluster system, however, the Repository server FQDN is the common FQDN for the active and standby nodes in the cluster system. The port number remains the Repository server port number.

Using a Cluster System

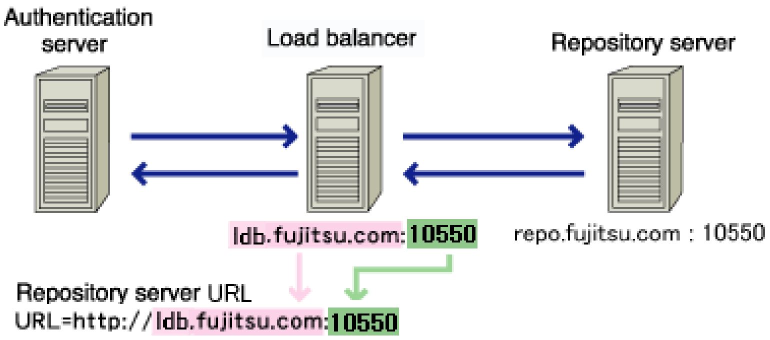
Figure 1.64 Using a Cluster System



Using a Load Balancer to Perform Repository Server (Update System) Load Balancing

The FQDN and port number of the repository server are identical to those of the virtual IP address that was set in the load balancer. (*1)

For details about the virtual IP address, refer to the load balancer manual.



*1 If SSL Accelerator is placed before the load balancer, the FQDN of the repository server is the FQDN of the virtual IP address set in the load balancer, and the port number is the SSL Accelerator port number.

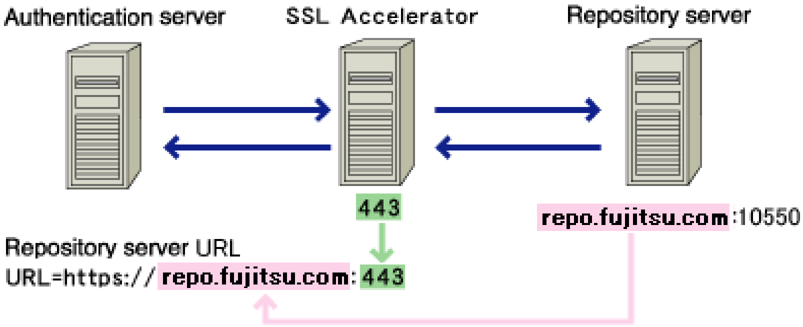
Using SSL Accelerator

Not Using a Cluster System

When you are not using a cluster system, the Repository server FQDN remains the Repository server FQDN. The port number is the SSL Accelerator port number.

For details about the virtual IP address, refer to the SSL Accelerator manual.

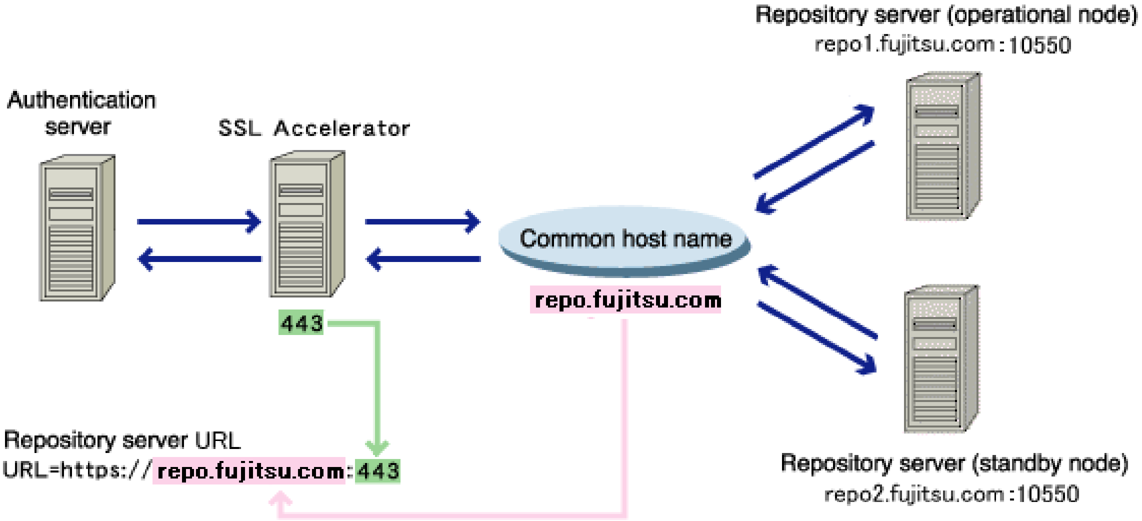
Figure 1.65 Not Using a Cluster System



In a cluster system, however, the Repository server FQDN is the common FQDN for the active and standby nodes in the cluster system, and the port number is the SSL Accelerator port number.

Using a Cluster System

Figure 1.66 Using a Cluster System



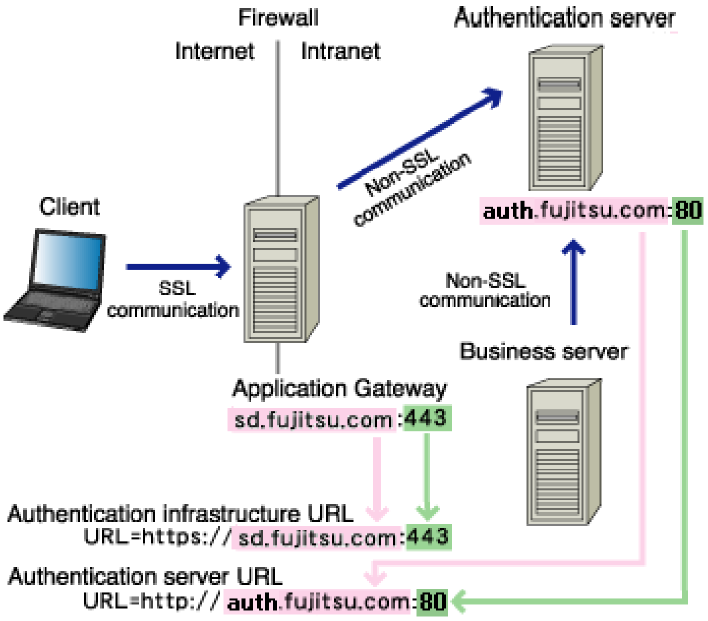
1.7.4 URL Used by the Business System to Reference the Authentication Server

The URL for the referencing of the Authentication server by the Business system is basically the same as the URL for the Authentication infrastructure. As shown in the configuration below, however, they must be different.

Linking with Application Gateway and Using Non-SSL Communication between Application Gateway and Authentication Server

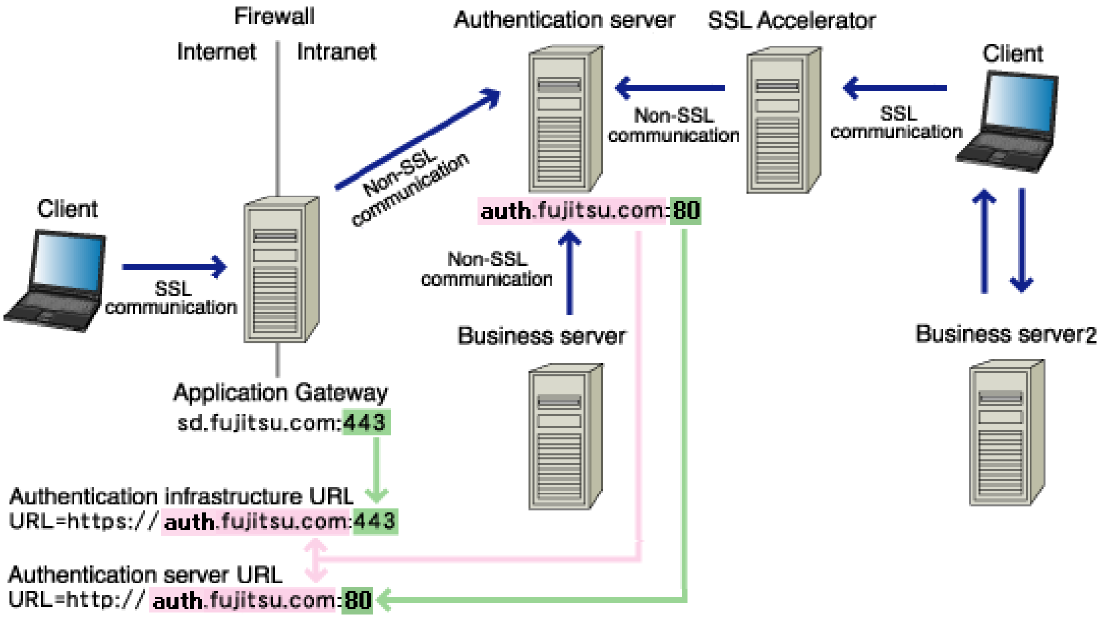
To enable the clients only on the Internet to access

Figure 1.67 Linking with Application Gateway and Using Non-SSL Communication between Application Gateway and Authentication Server



To enable access for the clients both on the Internet and in the intranet

Figure 1.68 Non-SSL Communication between Application Gateway and Authentication Server Viewed from the Client



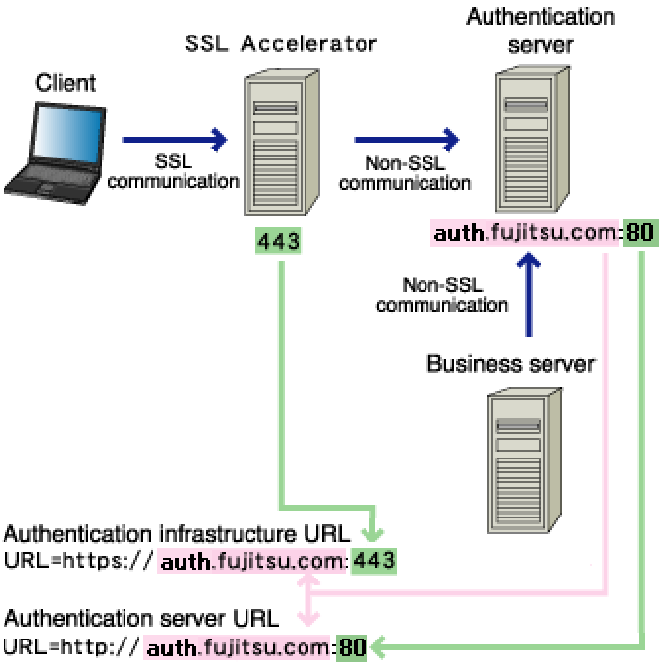
As shown in the configuration below, communication efficiency can be improved because SSL is not used for communication between the Business server and the Authentication server. Non SSL communication should only be used if security can be sufficiently guaranteed, however.

In a load balancing configuration in which the SSL accelerator and load balancer are used on one device and the authentication server and repository server are set up on one machine, operations in which communication performance is improved are not possible.

SSL Combining other Mechanisms and Products when the Authentication Server is SSL Accelerator

Using SSL Accelerator

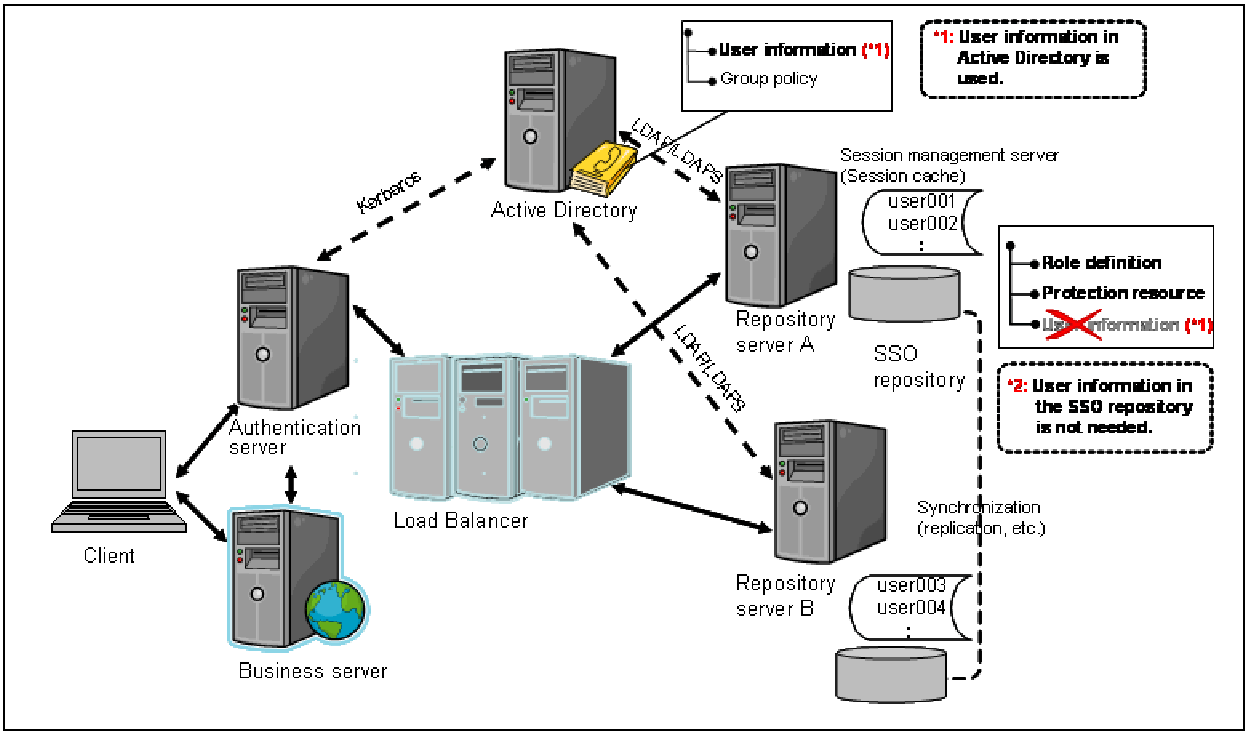
Figure 1.69 Using SSL when the Authentication Server is SSL Accelerator



1.8 Linking to Active Directory

Active Directory can be used as the directory service for managing user information with Interstage Single Sign-on.

Users can access protected resources from Web browsers after logging in to Windows, and can use services by authenticating with Integrated Windows Authentication.



To link to Active Directory where user information is stored without the extended schema of single sign-on, the associations between the user information managed by Active Directory and the role configurations for Interstage Single Sign-on must be registered within the SSO repository.

Refer to "Using Active Directory as the Directory Service for Registering User Information" for information about the procedure for creating systems that link to Active Directory and for information about how to establish associations between Active Directory and Interstage Single Sign-on.

Also, by using an extended schema for single sign-on, users can re-authenticate using password authentication or certificate authentication without having to sign on using Integrated Windows Authentication.

Refer to 'Extended Schema Settings for Single Sign-on' for information about how to extend the single sign-on schema for Active Directory.

Refer to 'Integrated Windows Authentication' for information about Integrated Windows Authentication.

Notes

- Linkage to an Active Directory that uses a referral function is not possible.
- The password for user accounts connecting to Active Directory can contain between 1 and 128 alphanumeric characters, symbols or spaces.

  This password is defined in the [Active Directory Settings] of [Repository], which is displayed by selecting [System] > [Security] > [Single Sign-on] > [Authentication Infrastructure] > [Repository Server] from the Interstage Management Console for the repository server, and then clicking [Repository server detailed settings [Show]] in the [Settings] tab.
- If an extended schema for single sign-on is not used, a user validity period cannot be set because user information is registered with Active Directory. For the validity period start time, design the operation so that the target user is disabled with Active Directory until the service start time. Similarly, for the validity period end time, use the account expiration (validity period) function for the Active Directory.
- If an extended schema for single sign-on is not used, the time of the previous sign-on can be checked using Active Directory functions as the time when the user logged on to the Windows system.

Chapter 2 Environment Setup (SSO Administrators)

This chapter explains the setup for the authentication infrastructure environment.

Use the Interstage Management Console to set up the Interstage Single Sign-on environment. Refer to the Operator's Guide for details of starting the Interstage Management Console and for details of the items to be defined in the Interstage Management Console.

Refer to the Directory Service Operator's Guide for details of creating an SSO repository that configures the authentication infrastructure.

Notes

- The Interstage Single Sign-on function may not be installed as part of the standard installation, depending on the edition, for more details, refer to the "Installation Guide".
- All access to the Authentication infrastructure uses SSL communication. For details, refer to "Authentication infrastructure URL".
- Refer to the Security System Guide in advance to securely set up and operate the system.
- The Administrator's authority is required to set up the authentication infrastructure environment.

2.1 Environment Setup Flow

Authentication infrastructure environment setup includes the following four operations:

- 2.2 Preparation for Environment Setup (SSO repository design, preparation for a user program)
- 2.2.3 Preparing Messages Displayed on a Web Browser
- 2.4 Setup of Authentication Server
- 2.6 Registering a Business System

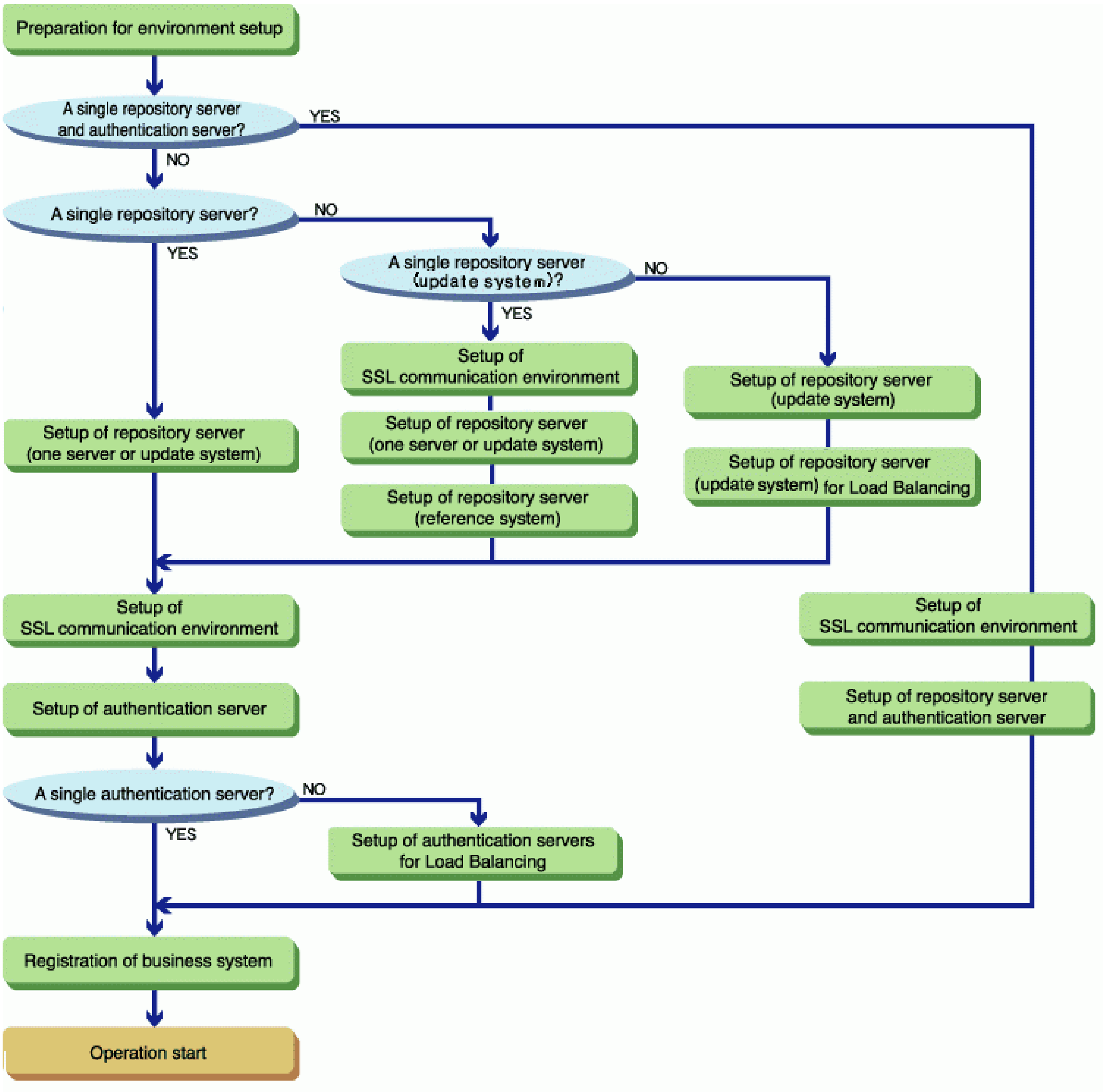
Set up the environment as to operation, as the steps required for setup will depend on the system configuration.

The authentication infrastructure configuration spreadsheet (an Excel file) is provided to assist the setup of the authentication infrastructure environment. This file helps users to calculate connection information between servers to be configured in the Interstage Management Console.

Refer to 2.1.2 Using the Authentication Infrastructure Configuration Spreadsheet for details of how to use the configuration spreadsheet.

2.1.1 Flow of Environment Setup by Systems

Figure 2.1 Flow of Environment Setup


Preparation for environment setup
A single repository server and authentication server?
YES
NO
A single repository server?
NO
YES
A single repository server (update system)?
NO
YES
Setup of SSL communication environment
Setup of repository server (update system)
Setup of repository server (one server or update system)
Setup of repository server (one server or update system)
Setup of repository server (update system) for Load Balancing
Setup of repository server (reference system)
Setup of SSL communication environment
Setup of SSL communication environment
Setup of authentication server
Setup of repository server and authentication server
A single authentication server?
NO
YES
Setup of authentication servers for Load Balancing
Registration of business system
Operation start

The following table shows the steps required for the environment setup of various types of systems:

Table 2.1 Environment Setup

	Setting up the authentication server on one machine and the repository server on another	Setting up the authentication server on multiple machines and the repository server on one machine	Setting up the authentication server on multiple machines and adding a repository server (update system)	Setting up the authentication server and the repository server on multiple machines individually	Adding an authentication server to authentication infrastructure already set up	Adding a repository server (reference system) to authentication infrastructure already set up (multiserver system)	Adding a repository server (update system) to an authentication infrastructure already set up and using on multiple machines	Setting up the repository server and the authentication server on a single machine	Adding a repository server and authentication server on one machine to an authentication infrastructure already set up
Preparation for Environment Setup	Preparation for Environment Setup	Preparation for Environment Setup	Preparation for Environment Setup	Preparation for Environment Setup				Preparation for Environment Setup	
Repository server setup				Constructing an SSL Communication Environment for a SSO Repository (Master)		Constructing an SSL Communication Environment for a SSO Repository (Master) (*1)			
	Creation of SSO repository	Creation of SSO repository	Creation of SSO repository	Creation of SSO repository				Creation of SSO repository	
	Registering user information and role configuration in SSO repository	Registering user information and role configuration in SSO repository	Registering user information and role configuration in SSO repository	Registering user information and role configuration in SSO repository				Registering user information and role configuration in SSO repository	
	Setting up repository server (server in single configuration or update system server in multiple configuration)	Setting up repository server (server in single configuration or update system server in multiple configuration)	Setting up repository server (server in single configuration or update system server in multiple configuration)	Setting up repository server (server in single configuration or update system server in multiple configuration)					
				Work for setting up		Work for setting up			

	Setting up the authentication server on one machine and the repository server on another	Setting up the authentication server on multiple machines and the repository server on one machine	Setting up the authentication server on multiple machines and adding a repository server (update system)	Setting up the authentication server and the repository server on multiple machines individually	Adding an authentication server to authentication infrastructure already set up	Adding a repository server (reference system) to authentication infrastructure already set up (multiserver system)	Adding a repository server (update system) to an authentication infrastructure already set up and using on multiple machines	Setting up the repository server and the authentication server on a single machine	Adding a repository server and authentication server on one machine to an authentication infrastructure already set up
				repository server (reference system)		repository server (reference system)			
			Adding a repository server (update system) for load distribution				Adding a repository server (update system) for load distribution		
Setup of authentication server	Setting up of SSL communication environment	Setting up of SSL communication environment	Setting up of SSL communication environment	Setting up of SSL communication environment				Setting up of SSL communication environment	
	Setting up one authentication server	Setting up one authentication server	Setting up one authentication server	Setting up one authentication server					
		Adding authentication server for load distribution	Adding authentication server for load distribution	Adding authentication server for load distribution	Adding authentication server for load distribution				
						Setting the repository server (reference system) information in authentication server			
								Setting up Repository	

	Setting up the authentication server on one machine and the repository server on another	Setting up the authentication server on multiple machines and the repository server on one machine	Setting up the authentication server on multiple machines and adding a repository server (update system)	Setting up the authentication server and the repository server on multiple machines individually	Adding an authentication server to authentication infrastructure already set up	Adding a repository server (reference system) to authentication infrastructure already set up (multiserver system)	Adding a repository server (update system) to an authentication infrastructure already set up and using on multiple machines	Setting up the repository server and the authentication server on a single machine	Adding a repository server and authentication server on one machine to an authentication infrastructure already set up
								Server and Authentication Server on a Single Machine	
									Adding a repository server and authentication server on one machine for load distribution
Registering Business System	Registering Business System	Registering Business System	Registering Business System	Registering Business System				Registering Business System	
Note Use of authentication infrastructure configuration spreadsheet	The authentication infrastructure configuration spreadsheet (middle-scale system) is available.	The authentication infrastructure configuration spreadsheet (middle-scale system) is available.		The authentication infrastructure configuration spreadsheet (large-scale system) is available. (*2)				The authentication infrastructure configuration spreadsheet (small-scale) is available.	

*1 This work is not required if the SSL communication environment has been set up in the active repository server (update system).

*2 The configuration spreadsheet for the Interstage Directory Service environment setup (an Excel file) is provided by Interstage Directory Service. Using this spreadsheet when creating the SSO master and slave repositories to be used as the standard databases, you can accurately set up the Interstage Management Console. Refer to 'Using the Standard Database' in the 'Creating a Load Distribution Environment (Replication Mode)' appendix of the Directory Service Operator's Guide for details of the configuration spreadsheet for Interstage Directory Service environment setup.

2.1.2 Using the Authentication Infrastructure Configuration Spreadsheet

The authentication infrastructure configuration spreadsheet (an Excel file) is provided to assist the setup of the authentication infrastructure environment. This file helps users to calculate connection information between servers to be set in the Interstage Management Console. Fetch the sheet from the following storage directory as necessary. Refer to [Procedure for Use] in the sheet for details of how to use it.

Filenames and Location of the Authentication Infrastructure Configuration Spreadsheet

File name of the Authentication Infrastructure Configuration Spreadsheet:

- SSO_Auth_L.xls, SSO_Auth_noSession_L.xls (*1)

  Use this sheet to set up on multiple machines a repository server that uses replication

- SSO_Auth_M.xls, SSO_Auth_noSession_M.xls (*2)(*3)

  Use this sheet to set up on multiple machines a repository server or an authentication server that uses a load balancer, or to set up a separate authentication server and repository server with one machine for each.

- SSO_Auth_S.xls

  Use this sheet to set up a repository server and authentication server on a single machine.

*1 If session management is used, refer to "SSO_Auth_L.xls". If session management is not used, refer to "SSO_Auth_noSession_L.xls".

*2 If session management is used, refer to "SSO_Auth_M.xls". If session management is not used, refer to "SSO_Auth_noSession_M.xls".

*3 If the repository server is set up on multiple machines, for "Host name common to the Repository servers + Domain" in a cluster system under [Input of the Number of Servers] in this sheet, set the information for the load balancer that is positioned before the repository server.

Location of the Authentication Infrastructure Configuration Spreadsheet:

Folder 'ApplicationServer\tuning' of Manual package

Conditions for Using the Authentication Infrastructure Configuration Spreadsheet

The authentication infrastructure configuration spreadsheet supports Microsoft(R) Excel. Ensure that either Microsoft(R) Excel 2003 or later is installed on your computer.

This sheet uses macros. Configure the Microsoft(R) Excel security level to enable macros. Refer to Microsoft(R) Excel Help for details of how to set the security level.

Contact your system administrator before changing the Microsoft(R) Excel security level.

The following procedure describes how to set the security level to use the authentication infrastructure configuration spreadsheet in Microsoft(R) Excel 2003:

1. Start Microsoft(R) Excel 2003 and from the menu bar, select [Tool (T)] > [Macro (M)] > [Security (S)].
2. The macro security setting window appears. Select [Medium (M)] in the [Security level] tab.
3. Click OK.
4. Quit Microsoft(R) Excel and restart.
5. From the menu bar, select [File (F)] > [Open (O)] to open the authentication infrastructure configuration spreadsheet.
6. The dialog asks whether to enable the macro. Click [Enable macro (E)].

After using this sheet, restore the security level as necessary.

2.2 Preparation for Environment Setup

Prepare a user program and design an SSO repository before environment setup.

2.2.1 Designing an SSO Repository

In Interstage Single Sign-on, the SSO repository collectively manages information required for authentication and authorization. This section explains the items to be designed before creation of an SSO repository.

Designing Information to be Registered in the SSO Repository

Three information items are registered in the SSO repository: Role configuration, user information, and protection resources. To set up a new authentication infrastructure, role configuration and user information must be designed.

- Role configuration

  Role configuration is mandatory for authorization in Interstage Single Sign-on. Design this information according to the organizational structure and user position. Refer to 'Role Configuration' of 'Information Required for Authorization Using Roles' for details.

- User information

  User information indicates information on the user who uses Interstage Single Sign-on. Design the user ID/password, and role configuration for association for each user. Refer to 'User Information' for details.

Take care not to create invalid SSO repository data when designing role configuration and user information.

The SSO repository data check sheet (an Excel file) is provided. This check sheet contains the notes on SSO repository design. Fetch the check sheet from the following storage directory when designing role configuration and user information.

File Name and Location of the SSO Repository Data Check Sheet

File Name of the SSO Repository Data Check Sheet:

SSO_Data_Chk.xls

Location of the SSO Repository Data Check Sheet:

Folder 'ApplicationServer\tuning' of Manual package

Register role configuration and user information in the created SSO repository. Design and register protection resources when adding a business system.

Designing a Registration Destination Entry

Design an entry in which role configuration, user information, and protection resources are to be registered in the SSO repository.

Define the registration destination entry when creating an SSO repository.

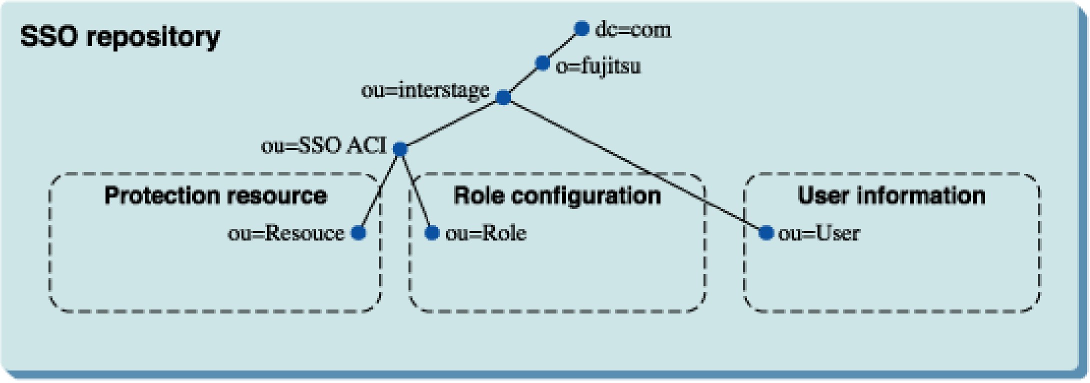
The following table shows examples of registration destination entries:

Example

Table 2.2 Registration Destination Entries

Management information	Registration destination entry
Role configuration	ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
User information	ou=User,ou=interstage,o=fujitsu,dc=com
Protection resource	ou=Resource,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

Figure 2.2 Registration Destination Entries



In the Interstage Management Console, when the default value is specified in [Public directory] in creating an SSO Repository, the registration destination entries shown in the above table are created. Samples provided by Interstage Single Sign-on for registering role configuration and user information have been created with the registration destination entries shown in the abobe figure.

Examples of SSO Repository Design

Role Configuration

Example

This example shows a design of registering three roles classified by roles/organization and one role set having two among the three roles in the following registration destination entry:

Role configuration registration destination entry: ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

Table 2.3 Register Roles

Role/organization	Role/role set name	Name of role contained in the role set
All employees	All	employee, executives
Executive	Executives	-
Employee	Employee	-
Administration department	Administration	-

User Information

Example

This example shows a design of registering information about two users in the following registration destination entry:

User information registration destination entry: ou=User,ou=interstage,o=fujitsu,dc=com

Table 2.4 Register User Information

Item	User information	
	user001 cn=user001	user002 cn=user002
Authentication method	Certificate authentication	Certificate authentication
User ID	user001	user002
Password	00123401	00123402
Information identifying a user at certificate authentication	user001@ interstage.fujitsu.com	user002@ interstage.fujitsu.com
Role name/role set name	Executives	employee, administration
Re-authentication interval	60 minutes	60 minutes
Validation start date	00:00:00, January 1, 2004	00:00:00, January 1, 2004
Expiration date	00:00:00, December 31, 2004	00:00:00, December 31, 2004

Registration Destination Entry

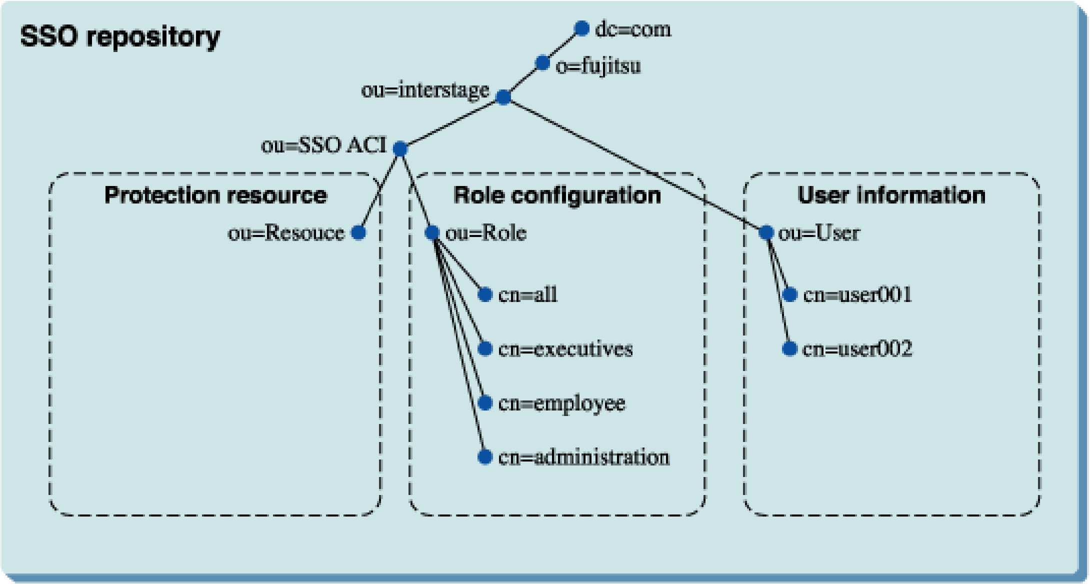
Example

The following example shows the registration of role configuration and user information as registration destination entries:

Role configuration registration destination entry: ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

User information registration destination entry: ou=User,ou=interstage,o=fujitsu,dc=com

Figure 2.3 Role Configuration and User Information Registration Destinations



2.2.2 Preparation for a User Program

To install Interstage Single Sign-on, prepare a user program for operating the SSO repository in the following ways:

- Registering role configuration in the SSO repository
- Registering user information in the SSO repository
- Deleting user information from the SSO repository
- Adding a user role
- Deleting a user role
- Displaying user lock status
- Locking a user
- Displaying and changing the user validity period
- Changing the user password

This manual describes an example of coding a user program in Java. Create a user program that fits in with your operation based on the example. Refer to 'Samples of User Program Descriptions' for details.

Create a user program for operating an SSO repository based on the correct design of an SSO repository. Take care not to create invalid SSO repository data.

Allocate the user program to a place that fits in with your operation, giving due consideration to security.

Refer to '2.3.2.3 Role Configuration Entry' and '2.3.2.4 User Information Entry' for details of the entry attributes of role configuration and user information in Interstage Single Sign-on.

2.2.3 Preparing Messages Displayed on a Web Browser

Prepare the messages that are displayed on a Web browser when Interstage Single Sign-on is running.

The following messages can be changed depending on the application:

- Messages displayed for form authentication
- Authentication error messages
- Messages displayed for Integrated Windows Authentication

To match these messages to the authorization error messages, when changing a message, ask the business server administrator about the messages that are displayed on a Web browser.

For details about changing messages, refer to "Customizing Messages Displayed on a Web Browser".

2.3 Repository Server Setup

This section describes the procedure for setting up a repository server that configures the authentication infrastructure.

Use the Interstage Management Console of the machine in which a repository server is set up. Refer to the Operator's Guide for details of starting the Interstage Management Console. Refer to the Operator's Guide for details of the items to be defined in the Interstage Management Console.

Setting up a Repository Server in the System with a Single Repository Server

Perform the following procedure to set up a repository server in a single-repository server configuration:

Set up a repository server

1. Creating an SSO Repository
2. Registering User Information and Role Configuration in the SSO Repository
3. Constructing a Repository Server (One Server or Update System)

Setting up a Repository Server in the Multiple Repository Server Configuration

Perform the following procedure to set up a repository server in the multiple-repository server configuration:

Adding a Repository Server (Update System) and Using Load Balancing

Set up a repository server (update system)

The procedure is the same as shown in "Set up a repository server" under "Setting up a Repository Server in the System with a Single Repository Server".

Adding a Repository Server (update system)

The procedure is the same as shown in "Setting up a repository server when adding a repository server (update system)".

Using Load Balancing with a Repository Server (Update System) and Repository Server (Reference System)

Using a Standard Database as the SSO Repository

Constructing an SSL Communication Environment for a SSO Repository (Master)

Set up a repository server (update system)

Perform the procedure described in "Repository server setup" in "Setting up a Repository Server in the System with a Single Repository Server".

Set up a repository server (reference system)

Perform the procedure described in "Set up a Repository Server (Reference System)" in "Using a standard database as the SSO repository" in "Setting up a Repository Server for Addition of a Repository Server (Reference System)".

Using a Relational Database (RDB) as the SSO Repository

Constructing an SSL Communication Environment for a SSO Repository (Master)

Set up a repository server (update system)

Perform the procedure described in "Repository server setup" in "Setting up a Repository Server in the System with a Single Repository Server".

Set up a repository server (reference system)

Perform the procedure described in "Set up a Repository Server (Reference System)" in "Using a relational database (RDB) as the SSO repository" in "Setting up a Repository Server for Addition of a Repository Server (Reference System)".

Setting up a Repository Server when Adding a Repository Server (Update System)

Perform the following procedure to add a repository server (update system) during operation:

Adding a repository server (update system) for load distribution

Setting up a Repository Server for Addition of a Repository Server (Reference System)

Perform the following procedure to add a repository server (reference system) during operation:

Using a Standard Database as the SSORepository

Constructing an SSL Communication Environment for a SSO Repository (Master)

This step is not required when an SSL communication environment has been set up in the SSO repository (master).

Adding a Repository Server (Reference System)

1. Back up the SSO repository data for the repository server (update system).
2. Set up an SSL communication environment of the repository server (reference system).
3. Create an SSO repository (slave) for the repository server (reference system).
4. Restore the SSO repository in the repository server (reference system).
5. Change the setting of the SSO repository for the restored repository server (reference system).
6. Set up for adding the repository server (reference system).
7. Change the setting of the SSO repository for the repository server (update system).

Using a Relational Database (RDB) as the SSO Repository

Constructing an SSL Communication Environment for a SSO Repository (Master)

This step is not required when an SSL communication environment has been set up in the repository server (update system).

Adding a Repository Server (Reference System)

1. Create an SSO repository.
2. Set up for adding the repository server (reference system).

Notes

SSL communication can be used in the Repository server in systems that do not use session management. If a repository server operates using SSL communication, set SSL in the Web server (Interstage HTTP Server) used by the repository server and set up an SSL communication environment in the repository server. Use the repository server Interstage Management Console to configure SSL. Click [System] > [Services] > [Web Server] > [Web Server Name] > [SSL].

For details about the procedure to set SSL in the Repository server, refer to "Setting up the SSL communication environment in the Repository server".

2.3.1 Creating an SSO Repository

Create an SSO repository to set up a new authentication infrastructure.

If a repository server (update system) is added and load balancing is used, refer to the chapter 'Creating a Load Distribution Environment' of the "Directory Service Operator's Guide" and create an SSO repository for sharing use of the database.

The SSO repository in the replication format can be created and used when distributing the load of the repository server (update system) using the Active Directory in the user information registration destination directory service. For the details about the replication format of SSO repository, refer to "Creating a Load Distribution Environment (Replication Mode)" in the "Directory Service Operator's Guide."

If a relational database (RDB) is used as the SSO repository, refer to "Environment Setup" in the "Directory Service Operator's Guide" before creating the repository.

If a standard database is used as the SSO repository, perform the procedure below in the Interstage Management Console of the machine in which a repository server is set up. Refer to the Operator's Guide for details of the items to be defined in the Interstage Management Console.

The SSO administrator must undertake the role of the repository administrator as described in the Interstage Management Console.

1. Select [Services] and then [Repository] from the System menu. Click on the [Create a New Repository] tab.
2. Specify items as described below.

   Items with (*1) can be specified only when creating an SSO repository; they cannot be changed after the SSO repository has been created. Take special care when setting these values.

   General Settings

   - Repository Name (*1)

     Specify the name of an SSO repository to be created.

   - Administrator DN (*1)

     Specify a DN (distinguished name) of the administrator that manages the SSO repository to be created in the DN (distinguished name) format. (Example: cn=manager)

   - Administrator DN password

     Specify a password for the SSO administrator.

   - Administrator DN password (re-enter)

     Re-enter the password for the SSO administrator.

   - Public Directory (*1)

     'ou=interstage,o=fujitsu,dc=com' has been specified. Change this directory as necessary.

   - Repository database

     Click 'Standard DB'.

   - Database Storage Directory (*1)

     The following directory has been specified. Change the directory as necessary.

     Windows32/64

     'C:\Interstage\Enabler\EnablerDStores\IREP'

     Solaris32/64

     '/var/opt/FJSVena/EnablerDStores/FJSVirep'

     Linux32/64

     '/var/opt/FJSVena/DStores/FJSVirep'

   - Cache Size

     The default is '1,000 pages'. One page consists of 4 kilobytes. Change the value as necessary.

   Detailed settings

   Connection Settings

   - Port Type to be used

     Select 'non-SSL'.

     If it is necessary for a user application to access the SSO repository using SSL communication, select 'both. In this case, specify [SSL Port number] and [SSL configuration].

     Note that the SSO repository must be able to non-SSL communication, therefore 'SSL' should not be selected.

   - Port number

     Specify a port number to be used in non-SSL communication.

   - Enable SSL encryption? (*1)

   - SSL Port number

     Specify the port number used in SSL communication.

Specify this to select 'Yes' in [Enable SSL encryption?].

- SSL configuration

  Select the SSL configuration used in SSL communication.

  Specify this to select 'Yes' in [Enable SSL encryption?].

- Connection idle Timeout

  The default is '900 seconds'. Change the value as necessary.

Security Settings

- User password encryption method (*1)

  The default is 'SHA256'. Change the value as necessary.

Search Settings

- Maximum number of searchable entries

  Maximum number of entries that can be searched The default is '500 entries'. Change the value as necessary.

- Search Timeout

  The default is '3,600 seconds'. Change the value as necessary.

Access log Configuration

- Output Access Log?

  Always select 'Yes'.

- Output level

  Select 'Client requests' and 'Server errors'. Select other items as necessary.

- Access log storage directory

  Change the value as necessary.

- Rotation Type

  Change the value as necessary.

- Size

  Change the value as necessary.

- Number of access log files

  Change the value as necessary.

3. The status of the SSO repository appears. Check the details.

4. Check the checkbox of the created SSO repository and click the Start button to start the SSO repository.

Note

In Linux (64 bit), standard databases cannot be used. A relational database (RDB) must be used as the SSO repository. For details, refer to the "Directory Service Operator's Guide".

2.3.2 Registering User Information and Role Configuration in the SSO Repository

Register user information and role configuration in the SSO repository with the user program. Refer to 2.2.2 Preparation for a User Program, for details about the user program.

A CSV data file or LDIF file can also be used to register user information and role configuration in the SSO repository.

Refer to 2.3.2.1 Using a CSV Data File and 2.3.2.2 Using an LDIF File for details.

Refer to 2.3.2.3 Role Configuration Entry and 2.3.2.4 User Information Entry for details of the entry attributes of role configuration and user information in Interstage Single Sign-on.

2.3.2.1 Using a CSV Data File

A large quantity of user information managed by the personnel database, may be added to the SSO repository at system installation, or at another time. To facilitate this, a CSV data file extracted from the personnel database can be used to add entries to the SSO repository in batch. Periodic updates of user information may be required when personnel transfer or new employees join. In this case, a CSV data file containing only updated information can be used to add user information to the SSO repository.

This section explains how to register user information and role configuration using a CSV data file based on the sample CSV data file provided by Interstage Single Sign-on.

The following paragraphs explain the procedure for registering entries using the CSV data file. Refer to the Directory Service Operator's Guide for details of the CSV format.

Execute the irepaddrole command to register a role and irepmodifyent command to register user information from the CSV data file. Refer to 'Directory Service Operation Commands' in the Reference Manual (Command Edition) for details of the command.

The CSV data file can also be used to delete or update information. Refer to the Directory Service Operator's Guide for details of how to delete or update information.

Note

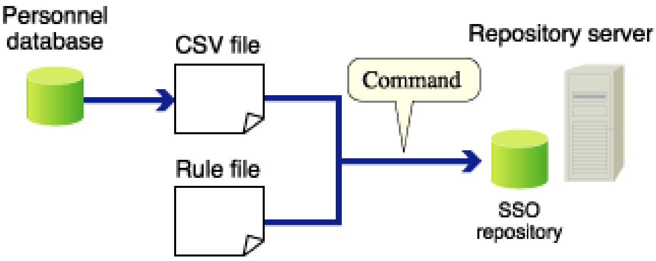
The CSV file contains a password. Ensure that you take sufficient action to protect the CSV file.

For details about securing your data, Refer to 'Security Measures' of 'Interstage Single Sign-on' of 'Security Risks' in the Security System Guide.

Perform the following procedure to add entries using the CSV data file:

1. Extract data in CSV format from the personnel database.
2. Create a rule file.
3. Execute the role configuration import command.
4. Execute the user information import command.

Figure 2.4 Add Entries using the CSV Data File



The sample files provided by Interstage Single Sign-on are as follows:

Sample File Names and Storage Directory

Sample CSV file for entry addition:

sample_add.csv

Sample rule file:

- sample_rule.xml

Sample storage directory:

Windows32/64

C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv

Solaris32/64 Linux32/64

/opt/FJSVssosv/sample/English/csv

1. Extract Data in CSV Format from the Personnel Database

Use the database function to extract user information in CSV format from the personnel database. Extract the following user information items from the database:

Table 2.5 User Information Items

Row	Item
Row 1	First and last name
Row 2	Last name
Row 3	First name
Row 4	User ID
Row 5	Password
Row 6	Employee number
Row 7	Mail address
Row 8	Role name

The data in CSV format that corresponds to the above data is as follows:

```
user001,Fujitsu,user001,100001,user001,100001,user001@interstage.fujitsu.com,Admin
user002,Fujitsu,user002,100002,user001,100002,user002@interstage.fujitsu.com,Admin
user003,Fujitsu,user003,100003,user003,100003,user003@interstage.fujitsu.com,Leader
user004,Fujitsu,user004,100004,user004,100004,user004@interstage.fujitsu.com,Leader
user005,Fujitsu,user005,100005,user005,100005,user005@interstage.fujitsu.com,General
user006,Fujitsu,user006,100006,user006,100006,user006@interstage.fujitsu.com,General
```

2. Create a Rule File

To register CSV data in the SSO repository, the data must be associated with SSO repository information. For the association, create a rule file and set a mapping rule. Refer to the Directory Service Operator's Guide for details of the mapping rule.

Refer to 2.3.2.3 Role Configuration Entry and 2.3.2.4 User Information Entry for details of the entry attributes that can be changed depending on the operating environment of Interstage Single Sign-on.

Associating CSV Data with User Information Entry Attributes

Associate the data in CSV format with the user entry attributes as shown in the following table, and register the associated data in the SSO repository.

Table 2.6 Associate CSV Data with User Information Entry Attributes

Row	Item	User information entry attribute
Row 1	First and last name	cn
Row 2	Last name	sn
Row 3	First name	givenName
Row 4	User ID	uid
Row 5	Password	userPassword
Row 6	Employee number	employeeNumber
Row 7	Mail address	mail
Row 8	Role name	ssoRoleName

CSV Data

In the CSV data, specify operation for the SSO repository in row 0.

```
ADD,user001,Fujitsu,user001,100001,user001,100001,user001@interstage.fujitsu.com,Admin
ADD,user002,Fujitsu,user002,100002,user002,100002,user002@interstage.fujitsu.com,Admin
ADD,user003,Fujitsu,user003,100003,user003,100003,user003@interstage.fujitsu.com,Leader
ADD,user004,Fujitsu,user004,100004,user004,100004,user004@interstage.fujitsu.com,Leader
ADD,user005,Fujitsu,user005,100005,user005,100005,user005@interstage.fujitsu.com,General
ADD,user006,Fujitsu,user006,100006,user006,100006,user006@interstage.fujitsu.com,General
```

Rule File

The rule file associates the above CSV data with the user information entry attributes as shown below. In the example of the role file, the following items are set:

Rule Name

sso rule

Public Directory

ou=User,ou=interstage,o=fujitsu,dc=com

Entry Attribute that Uniquely Identifies the User

uid

Operation

ADD (addition)

Attributes to be set According to CSV Data

cn, sn, givenName, uid, userPassword, employeeNumber, mail, ssoRoleName

Attributes to be set as a Fixed Value

ssoAuthType, ssoCredentialTTL, ssoNotBefore (*1)

*1 In the following example, the date is specified in the format YYYYMMDDHHMMSS+XXXX. '+XXXX' refers to the time difference from UTC (Universal Time Coordinate). In cases where '-XXXX' is used, it means the same as above.

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

<!-- Cannot be modified -->

<!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)>

]>
<!-- Cannot be modified -->


<Csv2Directory>

    <Rule>
        <name>sso rule</name>

<!-- Define baseDn (mandatory).  -->
```

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

<!-- Define attributes to be added before baseDn (arbitrary).  -->

<!-- Not required for SSO

        <midDn>ou=8,ou=9,ou=10</midDn>
-->

<!-- Define RDN (Mandatory:  Multiple values allowed:  Same value not
allowed).  -->

<!-- Enter a unique number or attribute name.  -->

        <Rdn>cn</Rdn>

<!-- Specify whether the changed DN is assumed to be moved (arbitrary).  -->

<!-- If assumed, specify 1.  -->

        <DnChange>1</DnChange>

<!-- Define objectClass.  -->

        <objectClass>top</objectClass>
        <objectClass>person</objectClass>
        <objectClass>organizationalPerson</objectClass>
        <objectClass>inetOrgPerson</objectClass>
        <objectClass>ssoUser</objectClass>

<!-- Delimiter when creating an attribute value from multiple CSV items
(arbitrary) -->

<!-- When specifying nothing, a null character is assumed.  -->

<!-- A null character cannot be specified.  -->

        <attributeSeparator>-</attributeSeparator>

<!-- Specify the attribute that does not allow any same value under baseDn.  -->

<!-- Specify a unique number or attribute name.  -->

<!-- (Arbitrary:  Multiple values allowed:  Same value not allowed) -->

        <unique>uid</unique>

        <CSV>
            <!-- An item number of CSV indicating a processing item
 (addition, deletion, or change) (arbitrary).  -->

            <ldapop>
                <op>0</op>
                <ldapadd>ADD</ldapadd>
                <ldapdelete>DEL</ldapdelete>
                <ldapmodify>MOD</ldapmodify>
                <ldapmove>MOV</ldapmove>
            </ldapop>

<!-- Mapping between each of CSV items and directory attributes (arbitrary) -->

            <Attribute>
                <cn>1</cn>
                <sn>2</sn>
                <givenName>3</givenName>
                <uid>4</uid>
                <userPassword>5</userPassword>
                <employeeNumber>6</employeeNumber>
                <mail>7</mail>
                <ssoRoleName>8</ssoRoleName>
            </Attribute>
        </CSV>

<!-- Define attributes to be set as fixed values (arbitrary).  -->

        <fixed>
            <ssoAuthType>basicAuthOrCertAuth</ssoAuthType>
            <ssoCredentialTTL>60</ssoCredentialTTL>
            <ssoNotBefore>20010101090000+0900</ssoNotBefore>
        </fixed>
    </Rule>
</Csv2Directory>
```

3. Execute the Role Configuration Import Command

To add entry data according to the mapping rules, execute irepaddrole command provided by Interstage Directory Service on the machine in which a repository server is set up.

After execution of the irepaddrole command, fetch entry information and check whether entry data has been added correctly. Refer to 'Entry Management' in the Directory Service Operator's Guide for details of how to operate the entry.

Example

Windows32/64

For the administrator DN and Bind password, specify the administrator DN and administrator DN password that were set when the SSO repository was created in the Interstage Management Console. In the following example, 389 is specified for the port number of the SSO repository and 'cn=manager,ou=interstage,o=fujitsu,dc=com' is specified for the administrator DN:

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

Rule file: C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_rule.xml

CSV file: C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_add.csv

Role configuration registration destination entry: ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

Enter the administrator DN password if you are prompted to enter the Bind password. The entered password is not displayed.

```
C:\>irepaddrole -h localhost -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r
C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_rule.xml -i
C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_add.csv -b "ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com"
Enter Bind password:
IREP: INFO: irep13570: adding new entry cn=Admin,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry cn=Leader,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry cn=General,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
C:\>
```

Solaris32/64 Linux32/64

For the administrator DN and Bind password, specify the administrator DN and administrator DN password that were set when the SSO repository was created in the Interstage Management Console. In the following example, 389 is specified for the port number of the SSO repository and 'cn=manager,ou=interstage,o=fujitsu,dc=com' is specified for the administrator DN:

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

Rule file: /opt/FJSVssosv/sample/English/csv/sample_rule.xml

CSV file: /opt/FJSVssosv/sample/English/csv/sample_add.csv

Role configuration registration destination entry: ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

Enter the administrator DN password if you are prompted to enter the Bind password. The entered password is not displayed.

```
# irepaddrole -h localhost -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r
/opt/FJSVssosv/sample/English/csv/sample_rule.xml -i
/opt/FJSVssosv/sample/English/csv/sample_add.csv -b "ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com"
Enter Bind password:
UX:IREP: INFO: irep13570: adding new entry cn=Admin,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=Leader,ou=Role,ou=SSO
 ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=General,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
#
```

Note

Ensure that you take sufficient action to protect your administrator DN password.

For details about securing your data, refer to 'Security Measures' of 'Interstage Single Sign-on' of 'Security Risks' in the Security System Guide.

4. Execute the User Information Import Command

To add entry data according to the mapping rules, execute the irepmodifyent command provided by Interstage Directory Service on the machine in which a repository server is set up.

After execution of the irepmodifyent command, fetch entry information and check whether entry data has been added correctly. Refer to 'Entry Management' in the Directory Service Operator's Guide for details of how to operate the entry.

Example

Windows32/64

For the administrator DN and Bind password, specify the administrator DN and administrator DN password that were set when the SSO repository was created in the Interstage Management Console. In the following example, 389 is specified for the port number of the SSO repository and 'cn=manager,ou=interstage,o=fujitsu,dc=com' is specified for the administrator DN:

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

Rule file: C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_rule.xml

CSV file: C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_add.csv

Enter the administrator DN password if you are prompted to enter the Bind password. The entered password is not displayed.

```
C:\>irepmodifyent -h localhost -p 389 -D
 "cn=manager,ou=interstage,o=fujitsu,dc=com" -r
 C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_rule.xml -i
C:\Interstage\F3FMsso\ssoatcsv\sample\English\csv\sample_add.csv
Enter Bind password:
IREP: INFO: irep13570: adding new entry
cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry
 cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry
cn=user003,ou=User,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry
cn=user004,ou=User,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry
cn=user005,ou=User,ou=interstage,o=fujitsu,dc=com
```

```
IREP: INFO: irep13570: adding new entry
cn=user006,ou=User,ou=interstage,o=fujitsu,dc=com
C:\>
```

Windows32/64 Linux32/64

For the administrator DN and Bind password, specify the administrator DN and administrator DN password that were set when the SSO repository was created in the Interstage Management Console. In the following example, 389 is specified for the port number of the SSO repository and 'cn=manager,ou=interstage,o=fujitsu,dc=com' is specified for the administrator DN:

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

Rule file: /opt/FJSVssosv/sample/English/csv/sample_rule.xml

CSV file: /opt/FJSVssosv/sample/English/csv/sample_add.csv

Enter the administrator DN password if you are prompted to enter the Bind password. The entered password is not displayed.

```
# irepmodifyent -h localhost -p 389 -D
 "cn=manager,ou=interstage,o=fujitsu,dc=com" -r
/opt/FJSVssosv/sample/English/csv/sample_rule.xml -i
/opt/FJSVssosv/sample/English/csv/sample_add.csv
Enter Bind password:
UX:IREP: INFO: irep13570: adding new entry
cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry
cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry
cn=user003,ou=User,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry
cn=user004,ou=User,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry
cn=user005,ou=User,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry
cn=user006,ou=User,ou=interstage,o=fujitsu,dc=com
#
```

Note

Ensure that you take sufficient action to protect your administrator DN password.

For details about securing your data, refer to 'Security Measures' of 'Interstage Single Sign-on' of 'Security Risks' in the Security System Guide.

2.3.2.2 Using an LDIF File

This section explains how to register user information and role configuration based on the sample LDIF file provided by Interstage Single Sign-on. Perform the following procedure to register entries using the LDIF file. Execute the ldapmodify command to register entries using the LDIF file.

Refer to the Directory Service Operator's Guide for details of the LDIF file. Refer to the Reference Manual (Command Edition) for details of the ldapmodify command.

The LDIF file also can be used to delete or update information. Refer to the Directory Service Operator's Guide for details of how to delete or update information.

1. Creating an LDIF File
2. Executing the ldapmodify Command

1. Creating an LDIF File

Specify in the LDIF file role configuration and user information to be registered in the SSO repository. Modify role configuration and user information set in the sample LDIF file as necessary.

Refer to 2.3.2.3 Role Configuration Entry and 2.3.2.4 User Information Entry for details of the entry attributes of role configuration and user information.

Note the following points for creating an LDIF file:

- Do not insert a blank line at the beginning of the LDIF file. If a blank line is inserted, none of the entries in the LDIF file are registered.
- Insert a blank line between entry information items to separate entry information. If two or more blank lines continue, subsequent entries are not registered.

If the default value of [Public directory] has been changed during creation of an SSO repository, change the bold characters of the sample LDIF file to the directory set in [Public directory].

The following section shows the name of the sample LDIF file and storage directory:

LDIF File Name

sample.ldif

LDIF file storage directory

Windows32/64

C:\Interstage\F3FMsso\ssoatcsv\sample\English\ldif

Solaris32/64 Linux32/64

/opt/FJSVssosv/sample/English/ldif

```
#
#
# Interstage Single Sign-on
#
#       Repository(Directory) Entry sample LDIF
#
#
#******************************************************
#
# Role definition
#
#******************************************************
# Entry: Role: Admin
dn: cn=Admin,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
                    <- Registration destination entry of role name "Admin"

objectClass: ssoRole               <- Mandatory object class

objectClass: top                   <- Mandatory object class

cn: Admin                          <- Role name

# Entry: Role: Leader
dn: cn=Leader,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
                    <- Registration destination entry of role name "Leader"

objectClass: ssoRole               <- Mandatory object class

objectClass: top                   <- Mandatory object class

cn: Leader                         <- Role name

# Entry: Role: General
dn: cn=General,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
                    <- Registration destination entry of role name "General"

objectClass: ssoRole               <- Mandatory object class

objectClass: top                   <- Mandatory object class

cn: General                        <- Role name
```

```
# Entry: RoleSet: AdminSet
dn: cn=AdminSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
               <- Registration destination entry of role set name "AdminSet"

ssoRoleName: Admin                 <- Role to be set in role set

objectClass: ssoRoleSet            <- Mandatory object class

objectClass: top                   <- Mandatory object class

cn: AdminSet                       <- Role set name

# Entry: RoleSet: LeaderSet
dn: cn=LeaderSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
              <- Registration destination entry of role set name "LeaderSet"

ssoRoleName: AdminSet              <- Role set to be set in role set

ssoRoleName: Leader                <- Role to be set in role set

objectClass: ssoRoleSet            <- Mandatory object class

objectClass: top                   <- Mandatory object class

cn: LeaderSet                      <- Role set name

# Entry: RoleSet: GeneralSet
dn: cn=GeneralSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com
             <- Registration destination entry of role set name "GeneralSet"

ssoRoleName: LeaderSet             <- Role set to be set in role set

ssoRoleName: General               <- Role to be set in role set

objectClass: ssoRoleSet            <- Mandatory object class

objectClass: top                   <- Mandatory object class

cn: GeneralSet                     <- Role set name


#******************************************************
#
# User definition
#
#******************************************************
# Entry: User: user001
dn: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com
                   <- Registration destination entry of user "user001"

objectClass: top                   <- Mandatory object class

objectClass: person                <- Mandatory object class

objectClass: organizationalPerson  <- Mandatory object class

objectClass: inetOrgPerson         <- Mandatory object class

objectClass: ssoUser               <- Mandatory object class

uid: 100001                         <- User ID at password authentication
```

```
userPassword: user001                <- Password at password authentication

mail: user001@interstage.fujitsu.com         <- Mail address

employeeNumber: 100001             <- Employee number

ssoRoleName: Admin                 <- Role name

ssoAuthType: basicAuthOrCertAuth   <- Authentication method

ssoCredentialTTL: 60               <- Re-authentication interval

ssoNotBefore: 20010101090000+0900  <- Use start time

sn: Fujitsu                        <- Last name

cn: user001                  <- First and last name

# Entry: User: user002
dn: cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com
                  <- Registration destination entry of user "user002"

objectClass: top                   <- Mandatory object class

objectClass: person                <- Mandatory object class

objectClass: organizationalPerson  <- Mandatory object class

objectClass: inetOrgPerson         <- Mandatory object class

objectClass: ssoUser               <- Mandatory object class

uid: 100002                        <- User ID at password authentication

userPassword: user002               <- Password at password authentication

mail: user002@interstage.fujitsu.com        <- Mail address

employeeNumber: 100002             <- Employee number

ssoRoleName: Admin                 <- Role name

ssoAuthType: basicAuthOrCertAuth   <- Authentication method

ssoCredentialTTL: 60               <- Re-authentication interval

ssoNotBefore: 20010101090000+0900  <- Use start time

sn: Fujitsu                        <- Last name

cn: user002                 <- First and last name


# Entry: User: user003
dn: cn=user003,ou=User,ou=interstage,o=fujitsu,dc=com
                   <- Registration destination entry of user "user003"

objectClass: top                   <- Mandatory object class

objectClass: person                <- Mandatory object class

objectClass: organizationalPerson  <- Mandatory object class
```

```
objectClass: inetOrgPerson         <- Mandatory object class

objectClass: ssoUser               <- Mandatory object class

uid: 100003                         <- User ID at password authentication

userPassword: user003                <- Password at password authentication

mail: user003@interstage.fujitsu.com         <- Mail address

employeeNumber: 100003             <- Employee number

ssoRoleName: Leader                <- Role name

ssoAuthType: basicAuth             <- Authentication method

ssoCredentialTTL: 60               <- Re-authentication interval

ssoNotBefore: 20010101090000+0900  <- Use start time

sn: Fujitsu                        <- Last name

cn: user003                  <- First and last name


# Entry: User: user004
dn: cn=user004,ou=User,ou=interstage,o=fujitsu,dc=com
                   <- Registration destination entry of user "user004"

objectClass: top                   <- Mandatory object class

objectClass: person                <- Mandatory object class

objectClass: organizationalPerson  <- Mandatory object class

objectClass: inetOrgPerson         <- Mandatory object class

objectClass: ssoUser               <- Mandatory object class

uid: 100004                         <- User ID at password authentication

userPassword: user004                <- Password at password authentication

mail: user004@interstage.fujitsu.com         <- Mail address

employeeNumber: 100004             <- Employee number

ssoRoleName: Leader                <- Role name

ssoAuthType: basicAuth             <- Authentication method

ssoCredentialTTL: 60               <- Re-authentication interval

ssoNotBefore: 20010101090000+0900  <- Use start time

sn: Fujitsu                        <- Last name

cn: user004                  <- First and last name


# Entry: User: user005
dn: cn=user005,ou=User,ou=interstage,o=fujitsu,dc=com
                 <- Registration destination entry of user "user005"
```

```
objectClass: top                   <- Mandatory object class

objectClass: person                <- Mandatory object class

objectClass: organizationalPerson  <- Mandatory object class

objectClass: inetOrgPerson         <- Mandatory object class

objectClass: ssoUser               <- Mandatory object class

uid: 100005                       <- User ID at password authentication

userPassword: user005              <- Password at password authentication

mail: user005@interstage.fujitsu.com       <- Mail address

employeeNumber: 100005             <- Employee number

ssoRoleName: General               <- Role name

ssoAuthType: basicAuthAndCertAuth  <- Authentication method

ssoCredentialTTL: 60               <- Re-authentication interval

ssoNotBefore: 20020101090000+0900  <- Use start time

sn: Fujitsu                        <- Last name

cn: user005                <- First and last name


# Entry: User: user006
dn: cn=user006,ou=User,ou=interstage,o=fujitsu,dc=com
                  <- Registration destination entry of user "user006"

objectClass: top                   <- Mandatory object class

objectClass: person                <- Mandatory object class

objectClass: organizationalPerson  <- Mandatory object class

objectClass: inetOrgPerson         <- Mandatory object class

objectClass: ssoUser               <- Mandatory object class

uid: 100006                        <- User ID at password authentication

userPassword: user006               <- Password at password authentication

mail: user006@interstage.fujitsu.com        <- Mail address

employeeNumber: 100006             <- Employee number

ssoRoleName: General               <- Role name

ssoAuthType: CertAuth              <- Authentication method

ssoCredentialTTL: 60               <- Re-authentication interval

ssoNotBefore: 20020101090000+0900  <- Use start time

ssoNotAfter: 20021201085959+0900   <- Use exit time
```

```
sn: Fujitsu                        <- Last name
cn: user006                 <- First and last name
```

2. Executing the ldapmodify Command

Specify the created LDIF file and execute the ldapmodify command to register user information and role configuration in the SSO repository.

After executing the ldapmodify command, fetch entry information and check whether user information and role configuration have been registered correctly. Refer to 'Entry Management' in the Directory Service Operator's Guide for details of how to operate the entry.

Example

Windows32/64

For the administrator DN and password, specify the administrator DN and administrator DN password that were set when the SSO repository was created in the Interstage Management Console. In the following example, 389 is specified for the port number of the SSO repository and 'cn=manager,ou=interstage,o=fujitsu,dc=com' is specified for the administrator DN:

LDIF file: C:\Interstage\F3FMsso\ssoatcsv\sample\English\ldif\sample.ldif

Role configuration registration destination entry: ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

User information registration destination entry: ou=User,ou=interstage,o=fujitsu,dc=com

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

Enter the administrator DN password if you are prompted to enter the password. The entered password is not displayed.

```
C:\> C:\Interstage\bin\ldapmodify -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -a -f
C:\Interstage\F3FMsso\ssoatcsv\sample\English\ldif\sample.ldif
Enter LDAP Password:
adding new entry "cn=Admin,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=Leader,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=General,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=AdminSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=LeaderSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=GeneralSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user003,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user004,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user005,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user006,ou=User,ou=interstage,o=fujitsu,dc=com"
C:\>
```

Solaris32/64 Linux32/64

For the administrator DN and password, specify the administrator DN and administrator DN password that were set when the SSO repository was created in the Interstage Management Console. In the following example, 389 is specified for the port number of the SSO repository and 'cn=manager,ou=interstage,o=fujitsu,dc=com' is specified for the administrator DN:

LDIF file: /opt/FJSVssosv/sample/English/ldif/sample.ldif

Role configuration registration destination entry: ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

User information registration destination entry: ou=User,ou=interstage,o=fujitsu,dc=com

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

Enter the administrator DN password if you are prompted to enter the password. The entered password is not displayed.

```
# /opt/FJSVirepc/bin/ldapmodify -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -a -f
/opt/FJSVssosv/sample/English/ldif/sample.ldif
```

```
Enter LDAP Password:
adding new entry "cn=Admin,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=Leader,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"adding new entry
"cn=General,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=AdminSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=LeaderSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=GeneralSet,ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user002,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user003,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user004,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user005,ou=User,ou=interstage,o=fujitsu,dc=com"
adding new entry "cn=user006,ou=User,ou=interstage,o=fujitsu,dc=com"
#
```

Note

Ensure that you take sufficient action to protect the administrator password.

For details about securing your data, refer to 'Security Measures' of 'Interstage Single Sign-on' of 'Security Risks' in the Security System Guide.

2.3.2.3 Role Configuration Entry

This section describes the entry used to register role configuration in the SSO repository. Specify the role name and role set name in the user information and protection resources.

Specify each attribute depending on its required function. Since the number characters allowed for each attribute depends on the SSO repository, it may not always be possible to set the number. The role name and role set name must both be unique.

<Role>

The entry used to register a role in the SSO repository is described below.

Object Classes

The role registered in the SSO repository is managed by the following object classes. Specify the following object classes when registering a role in the SSO repository:

Table 2.7 Role Object Class

Object class	Description
top	Basic LDAP object class
ssoRole	SSO role information

Attributes

Specify the name of a role as an attribute of the above object classes.

Table 2.8 ssoRole Attributes

Role object class	Attribute name	Explanation
ssoRole	cn	Name
	ssoAuthType	Authentication method Not used in this version
	ssoSessionInfo	Information used for the Interstage Single Sign-on (*1)

*1 Settings are required when the Active Directory in the directory service in which user information is registered is used, and the Single Sign-on extended schema is not used.

(1) cn

Description

Specify the name of a role.

The role name specified here is set in the ssoRoleName attribute of user information and the role set entry.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), Hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), hyphen (-), equal sign (=), asterisk (*), slash (/), vertical line (|), underscore (_), single quotation mark ('), colon (:), period (.), caret (^), back quotation mark (`), tilde (~)

Size that can be Specified

512 bytes

Example of Specification

Admin

Notes

- Specify this attribute only once.
- Use only alphanumeric characters and symbols when providing user information using environment variables.
- Specified values are not case-sensitive.
- The role name or role set name must be defined only once.

(2) ssoAuthType

Description

This attribute is not used in this version.

Note

Do not specify or change this attribute.

(3) ssoSessionInfo

Description

Set the attribute value used for Active Directory role/role set.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), backslash (\), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), less than (<), greater than (>), plus (+), hyphen (-), equal sign (=), asterisk (*), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), colon (:), semicolon (;), comma (,), period (.), caret (^), back quotation mark (`), tilde (~)

Size that can be Specified

512 bytes

Example of Specification

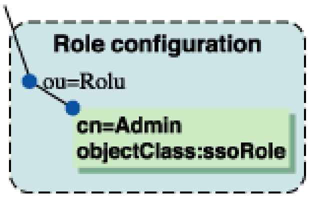
05:CN=SALES DEPT.I,CN=Users,DC=ad,DC=local

Note

Specified values are not case-sensitive.

Example of Role

Figure 2.5 Example of Role



<Role set>

The entry used to register a role set in the SSO repository is described below.

Object Classes

The role set registered in the SSO repository is managed by the object classes shown in the table below. Specify the following object classes when registering a role set in the SSO repository.

Table 2.9 Role Set Object Class

Object class	Description
top	Basic LDAP object class
ssoRoleSet	SSO role set information

Attributes

Specify the name of a role set and role to be included in the role set as the attributes of the above object classes.

Table 2.10 ssoRoleSet Attributes

Role set object class	Attribute name	Explanation
ssoRoleSet	cn	Name
	ssoRoleName	Role name
	ssoSessionInfo	Information used for the Interstage Single Sign-on (*1)

*1 Settings are required when the Active Directory in the directory service in which user information is registered is used, and the Single Sign-on extended schema is not used.

(1) cn

Description

Specify the name of a role set.

The role set name specified here is set in the ssoRoleName attribute of user information and the role set entry.

The Following Characters are Valid

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), Hash(#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), hyphen (-), equal sign (=), asterisk (*), slash (/), vertical line (|), underscore (_), single quotation mark ('), colon (:), period (.), caret (^), back quotation mark (`), tilde (~)

Size that can be Specified

512 bytes

Example of Specification

AdminSet

Notes

- Specify this attribute only once.
- Specified values are not case-sensitive.
- The role name or role set name must be defined only once.

(2) ssoRoleName

Description

Specify a role to be included in the role set or a role set.

When specifying multiple roles or role sets, specify the ssoRoleName attribute more than once.

Always specify this attribute.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), backslash (\), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), less than (<), greater than (>), plus (+), hyphen (-), equal sign (=), asterisk (*), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), colon (:), semicolon (;), period (.), caret (^), back quotation mark (`), tilde (~)

Size that can be Specified

512 bytes

Example of Specification

Admin

Notes

- Specified values are not case-sensitive.
- Overlapped roles or role sets are invalid.
- Specify only existing roles or role sets.
- If a loop is created in the configuration of a role set, the loop portion becomes invalid.

(3) ssoSessionInfo

Description

Set the attribute value used for Active Directory role/role set.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), backslash (\), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), less than (<), greater than (>), plus (+), hyphen (-), equal sign (=), asterisk (*), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), colon (:), semicolon (;), comma (,), period (.), caret (^), back quotation mark (`), tilde (~)

Size that can be Specified

512 bytes

Example of Specification

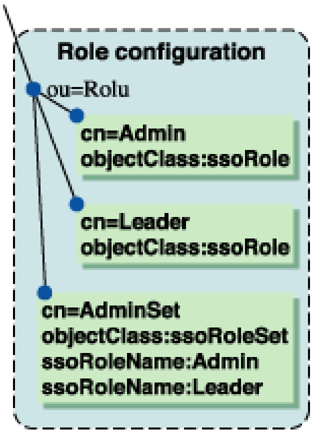
05:CN=SALES DEPT.I,CN=Users,DC=ad,DC=local

Note

Specified values are not case-sensitive.

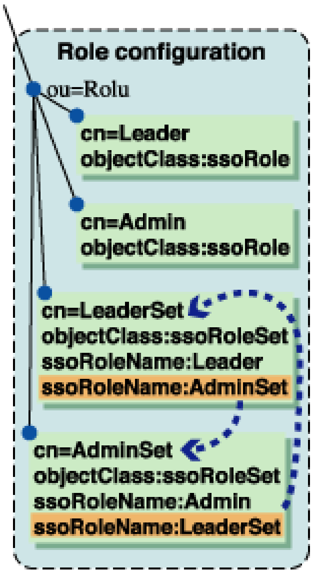
Example of Role Set

Figure 2.6 A Role Set



Example of Role Set Whose Configuration Includes a Loop (Looped Portion is Assumed to be Invalid)

Figure 2.7 A Role Set with a Loop



In the abobe figure:

- Role set 'LeaderSet' indicates role 'Leader' and role set 'AdminSet.'
- Role set 'AdminSet' indicates role 'Admin' and role set 'LeaderSet.'
- Role set 'LeaderSet' set in role set 'AdminSet' causes a loop. In this case, role set 'LeaderSet' indicated by role set 'AdminSet' becomes invalid.
- Finally, role set 'LeaderSet' is assumed to be a role set that indicates role 'Leader' and role 'Admin.'

2.3.2.4 User Information Entry

This section explains the entry used to register user information in the SSO repository.

The user information definition consists of general definitions that target a person, and special definitions that target network devices such as printers. Specify each definition entry depending on its required function. Since the number of characters allowed for each attribute depends on the SSO repository, it may not always be possible to set the number.

	General definitions	Special definitions
- Attributes that must always be specified	- cn - sn	- cn

	General definitions	Special definitions
- Attributes that must be set for executing password authentication	- uid - userPassword	- uid
- Attributes that must be set for executing certificate authentication (*1)	- mail - employeeNumber - uid - dnQualifier	- serialNumber
Attributes that must be specified depending on operation	ssoAuthType ssoRoleName ssoCredentialTTL ssoNotBefore ssoNotAfter	ssoAuthType ssoRoleName ssoCredentialTTL ssoNotBefore ssoNotAfter
Attributes that need not be specified	ssoUserStatus ssoFailureCount ssoLockTimeStamp ssoSessionInfo	ssoUserStatus ssoFailureCount ssoLockTimeStamp ssoSessionInfo

*1 If the attribute for identifying user information uniquely from the owner name information in the certificate does not use cn, one of the above attributes must be set.

Note

If Integrated Windows Authentication is performed, add any attribute that sets the user logon name registered in the ActiveDirectory. Refer to the Appendix "Settings for Active Directory linkage" for details.

Object Classes

The user registered in the SSO repository is managed by the following object classes. When the user information is registered with the SSO repository, it should be constructed with the following object classes.

General Definitions

Table 2.11 General Definitions Object Class

User information object class	Description
top	Basic LDAP object class
person	User information
organizationalPerson	
inetOrgPerson	
ssoUser	SSO user information

Special Definitions

Table 2.12 Special Definitions Object Class

User information object class	Description
top	Basic LDAP object class
device	Network device information for devices such as printers
uidObject	User ID information (*1)
ssoUser	SSO user information

*1 This must be set if session management or password authentication is used.

Attributes

Specify the user ID, password, and authentication method as the attributes of the above object classes. The following attributes are used in Interstage Single Sign-on:

General Definitions

Table 2.13 Attributes Used by Interstage Single Sign-on

User information object class	Attribute name	Explanation
person	cn	Name Example: user001
	sn	Last name Example: Fujitsu
	userPassword	Password Example: user001
organizationalPerson	No attribute is required in SSO operation.	-
inetOrgPerson	uid	User ID Example: user001
	employeeNumber	Employee number Example: 000001
	mail	E-mail address Example: user001@interstage.fujitsu.com
ssoUser	ssoRoleName	Role name or role set name Example: Admin
	ssoAuthType	Authentication method Example: basicAuthOrCertAuth
	ssoCredentialTTL	Re-authentication interval Example: 60
	ssoUserStatus	User status
	ssoNotBefore	Validity period start date Example: 20030101000000+0900
	ssoNotAfter	Expiration date Example: 20030102000000+0900
	ssoFailureCount	Number of authentication failures due to invalid user name or password
	ssoLockTimeStamp	Lockout time
	ssoSessionInfo	SSO session information
	dnQualifier	DN qualifier

Special Definitions

Table 2.14 Attributes Used by Interstage Single Sign-on

User information object class	Attribute name	Explanation
device	cn	Name Example: Device10000
	serialNumber	Serial number Example: 1234-1234-AB
uidObject	uid	User ID Example: user001
ssoUser	ssoRoleName	Role name or role set name Example: Admin
	ssoAuthType	Authentication method Example: basicAuthOrCertAuth
	ssoCredentialTTL	Re-authentication interval Example: 60
	ssoUserStatus	User status
	ssoNotBefore	Validity period start date Example: 20030101000000+0900
	ssoNotAfter	Expiration date Example: 20030102000000+0900
	ssoFailureCount	Number of authentication failures due to invalid user name or password
	ssoLockTimeStamp	Lockout time
	ssoSessionInfo	SSO session information

(1) cn

Description

Specify the first and last name to identify the user entry.

Always specify this attribute.

In applications using certificate authentication, the name that is set to identify the user must be unique.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), hyphen (-), equal sign (=), slash (/), vertical line (|), underscore (_), single quotation mark ('), colon (:), period (.), caret (^), back quotation mark (`), tilde (~)

Example of Specification

user001

Notes

- Specified values are not case-sensitive.
- This attribute must not contain consecutive spaces ( ).

(2) sn

Description

Specify the last name. It is a mandatory attribute of the person object class.

This must be set for general definitions.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), hyphen (-), equal sign (=), slash (/), vertical line (|), underscore (_), single quotation ('), colon (:), period (.), caret (^), back quotation mark (`), tilde (~)

Example of Specification

Fujitsu

Note

Specified values are not case-sensitive.

(3) userPassword

Description

Specify the password used for user password authentication.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), back slash (\), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), less than sign (<), greater than sign (>), plus sign (+), hyphen (-), equal sign (=), asterisk (*), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), colon (:), semicolon (;), comma (,), period (.), caret (^), back quotation mark (`), tilde (~)

Example of Specification

user001

Notes

- Specified values are case-sensitive.
- If a character set in this attribute does not belong to the group of valid characters, user authentication fails.
- Do not set this attribute more than once. If it is set more than once, user authentication may not be executed correctly.

(4) uid

Description

Specify the user ID used for user password authentication.

Specify a unique ID.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), back slash (\), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), plus sign (+), hyphen (-), equal sign (=), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), semicolon (;), comma (,), period (.), caret (^), back quotation mark (`), tilde (~)

Size that can be Specified

256 bytes (if session management is used)

Example of Specification

user001

Notes

- Specified values are not case-sensitive.
- This attribute must not contain consecutive spaces ( ).

- If an invalid character is used for this attribute, user authentication fails.
- If this attribute is specified more than once, user authentication is not performed correctly.

(5) employeeNumber

Description

Specify the number allocated for each user, e.g., employee number.

If the employee number is used to identify the user in the certificate authentication process, specify a unique number.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), back slash (\), hash(#), dollar mark ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), plus sign (+), hyphen (-), equal sign (=), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), colon (:), semicolon (;), comma (,), period (.), caret (^), back quotation mark (`), tilde (~)

Example of Specification

000001

Notes

- Specified values are not case-sensitive.
- This attribute must not contain consecutive spaces ( ).

(6) mail

Description

Specify the E-mail address.

If the E-mail address is used to identify the user in the operation using certificate authentication, specify a unique address.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), back slash (\), hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), plus sign (+), hyphen (-), equal sign (=), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), colon (:), semicolon (;), comma (,), period (.), caret (^), back quotation mark (`), tilde (~)

Example of Specification

user001@interstage.fujitsu.com

Notes

- Specified values are not case-sensitive.
- This attribute must not contain consecutive spaces ( ).

(7) serialNumber

Description

Specify the serial number.

If the serial number is used to identify the user in the certificate authentication process, specify a unique number.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), single quotation mark ('), left parenthesis ((), right parenthesis ()), plus sign (+), comma (,), hyphen (-), period (.), slash (/), colon (:), equal sign (=), question mark (?)

Example of Specification

1234-1234-AB

Notes

- Specified values are not case-sensitive.
- This attribute must not contain consecutive spaces ( ).

(8) ssoRoleName

Description

Specify the name of a role or role set to which the user belongs. This attribute can be specified more than once if the user belongs to multiple roles.

The Following Characters are Valid:

- Alphanumeric characters
- Space ( ), exclamation mark (!), question mark (?), at symbol (@), back slash (\),hash (#), dollar sign ($), percent (%), ampersand (&), left parenthesis ((), right parenthesis ()), left brace ({), right brace (}), left bracket ([), right bracket (]), less than sign (<), greater than sign (>), plus sign (+), hyphen (-), equal (=), asterisk (*), slash (/), vertical line (|), underscore (_), double quotation mark ("), single quotation mark ('), colon (:), semicolon (;), period (.), caret (^), back quotation mark (`), tilde (~)

Size that can be Specified

512 bytes

Example of Specification

Admin

Note

If a role or roleset that is not registered in the role configuration is set in this attribute (including cases in which a role or roleset no longer exists because it has been deleted), this attribute is ignored. If, as a result of the attribute being ignored, no role belongs to the user, that user will not be able to access a site protected by Interstage Single Sign-on.

(9) ssoAuthType

Description

Specify the user authentication method.

The default value is 'basicAuthOrCertAuth.'

- basicAuth: Password authentication
- certAuth: Certificate authentication
- basicAuthAndCertAuth: Password authentication and certificate authentication
- basicAuthOrCertAuth: Password authentication or certificate authentication

The Following Character types are Valid:

- basicAuth
- certAuth
- basicAuthAndCertAuth
- basicAuthOrCertAuth

Example of Specification

basicAuthOrCertAuth

Notes

- Specified values are not case-sensitive.

- If "certAuth" is set in the system that performs the session management with no permission for certificate authentication, user authentication fail. To set "certAuth", the settings that allow certificate authentication in the system that performs the session management are required. For details about how to set certificate authentication, refer to "Settings for Performing Certificate Authentication in a System that performs Session Management" in Appendix G.

(10) ssoCredentialTTL

Description

Specify the re-authentication interval as a range between 30 to 1440 minutes.

If 0 is specified and session management is used, this setting is treated as "1440". If 0 is specified and session management is not used, re-authentication is not performed.

Character Types that can be Specified

- Numbers

Example of Specification

60

Note

If a value less than 30 is specified, the value defaults to 30 minutes. If a value greater than 1440 is specified, the value defaults to 1440 minutes (24 hours).

(11) ssoUserStatus

Description

This attribute specifies the lock status of the user account as follows:

- good: Not locked

- locked: Locked

Example of Specification

good

Note

[Release user lock] of the Interstage Management Console is used to unlock the user account. Refer to 'Release lockout' for details of how to unlock the user account.

This attribute can operate in user programs to lock out users. Refer to "Locking a user" in the Appendix "Samples of User Program Descriptions" for information concerning user programs that lock out users.

(12) ssoNotBefore

Description

Specify the date when user Single Sign-on is started.

If the user uses Single Sign-on before the specified date, authentication fails.

Specify the format of YYYYMMDDHHMMSS+XXXX.(*1) For Greenwich Mean Time, specify the format of YYYYMMDDHHMMSSZ. If this attribute is omitted, the user can immediately use Single Sign-on.

Note that this attribute represents Daylight Savings Time.

- YYYY: Year (four digits of the year)
- MM: Month (two digits)
- DD: Day (two digits)
- HH: Hour (two digits for 24 hours)
- MM: Minute (two digits)
- SS: Second (two digits)

Character Types that can be Specified

- Numbers

Example of Specification

20030101000000+0900

Notes

- Set a different date and time for ssoNotBefore and ssoNotAfter. If the same date and time is specified, user authentication fails.
- Set a date and time for ssoNotBefore that is earlier than the date and time set for ssoNotAfter. If the date and time set for 'ssoNotBefore' is later than the date and time set for 'ssoNotAfter', user authentication fails.
- Specify a date between '20000101000000' and '20371231235959' in ssoNotBefore and ssoNotAfter regardless of Japan time or Greenwich Mean Time. If a date out of range is specified, user authentication fails.
- When using the Active Directory in the directory service that the user information is registered and the Single Sign-on schema is extended in the Active Directory, the "YYYYMMDDHHMMSS.0+ XXXX"(*1) format will be used. For the settings with GMT, the "YYYYMMDDHHMMSS.0Z" format will be used.

*1 '+XXXX' refers to the time difference from UTC (Universal Time Coordinate). In cases where '-XXXX' is used, it means the same as above.

(13) ssoNotAfter

Description

Specify the date after which Single Sign-on is not available to users. If the user uses Single Sign-on after the specified date, authentication fails.

Specify the date in the format YYYYMMDDHHMMSS+XXXX. (*1) For Greenwich Mean Time, specify the date in the format YYYYMMDDHHMMSSZ. If this attribute is omitted, the user can use Single Sign-on for an indefinite period.

Note that this attribute represents Daylight Savings Time.

- YYYY: Year (four digits of the year)
- MM: Month (two digits)
- DD: Day (two digits)
- HH: Hour (two digits for 24 hours)
- MM: Minute (two digits)
- SS: Second (two digits)

Character Types that can be Specified

- Numbers

Example of Specification

20030102000000+0900

Notes

- Set a different date and time for ssoNotBefore and ssoNotAfter. If the same date and time is specified, user authentication fails.
- Set a date and time for 'ssoNotAfter' that is later than the date and time set for 'ssoNotBefore'. If the date and time set for 'ssoNotAfter' is earlier than the date and time set for 'ssoNotBefore', user authentication fails.
- Specify a date between '20000101000000' and '20371231235959' in ssoNotBefore and ssoNotAfter regardless of Japan time or Greenwich Mean Time. If a date out of range is specified, user authentication fails.
- When using the Active Directory in the directory service that the user information is registered and the Single Sign-on schema is extended in the Active Directory, the "YYYYMMDDHHMMSS.0+ XXXX"(*1) format will be used. For the settings with GMT, the "YYYYMMDDHHMMSS.0Z" format will be used.

*1 '+XXXX' refers to the time difference from UTC (Universal Time Coordinate). In cases where '-XXXX' is used, it means the same as above.

(14) ssoFailureCount

Description

This attribute specifies the number of user authentication failures due to incorrectly entering the user name/password.

If the correct user name/password is specified and authentication succeeds, this attribute is reset to 0. This value is set by the repository server.

Note

Do not specify or change this attribute.

(15) ssoLockTimeStamp

Description

This attribute specifies the date when the user was locked by the repository server in (Greenwich Mean Time (YYYYMMDDHHMMSSZ).

Note

This attribute can operate in user programs to lock out users. Refer to "Locking a user" in the Appendix "Samples of User Program Descriptions" for information concerning user programs that lock out users.

Enter settings in the "YYYYMMDDHHMMSSZ" or "YYYYMMDDHHMMSS+XXXX" format to set values in user programs. Set a date and time between "20000101000000" and "20371231235959", regardless of whether the time is set in Japan time or Greenwich Mean Time. User authentication will fail if a date and time outside of this range is set.

(16) ssoSessionInfo

Description

Internal information required for using session management was set from the Repository server.

Note

Do not specify or change this attribute.

(17) dnQualifier

Description

Specify the DN qualifier.

If the DN qualifier is used to identify the user in the certificate authentication process, specify a unique number.

Character Types that can be Specified

- Alphanumeric characters
- Space ( ), single quotation mark ('), left parenthesis ((), right parenthesis ()), plus sign (+), comma (,), hyphen (-), period (.), slash (/), colon (:), equal sign (=), question mark (?)

Notes

- Specified values are not case-sensitive.
- This attribute must not contain consecutive spaces ( ).

2.3.3 Constructing a Repository Server (One Server or Update System)

This section explains how to set up one repository server or an update-system repository server in multiple-repository server configuration.

The setup described below is performed using the Interstage Management Console on the machine where the repository server is to be set up. Refer to the Operator's Guide for details of the items to be defined on the Interstage Management Console.

To set up a repository server, the SSO Repository must be previously created. Refer to 2.3.1 Creating an SSO Repository for an explanation of SSO Repository creation.

1. Select the Web server (Interstage HTTP Server) where the repository server is to be created. If there is no Web server for creating a repository server, create a new Interstage single sign-on dedicated Web server.

2. If the repository server is to use SSL communication, enter relevant SSL settings in the Web server selected or created in Step 1. Refer to "Setting up an SSL Communication Environment for a Repository Server" in the Appendix "Preparations for SSL Communication" for information on how to configure SSL.
3. Select [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure] and then click the [Authentication infrastructure Settings] tab.
4. Select [Setup Repository server and Authentication server to the separate servers.], and click [Next]. The window for selecting a server to be created is displayed.
5. Select [Create a new Repository server] > [Repository server (update system)], and click [Next].
6. The selection screen of the Directory Service that is used for the user information registration destination is displayed.
7. Select the Directory Service in which the user information is registered, and click the [Next]. When Active Directory is used, check [Use a Single Sign-on extended schema] if required.
8. [General Settings] is displayed.
9. Enter [Authentication infrastructure URL] and [Repository server (update system) URL], in [Web Server used], select the name of the Web server selected or created in Step 1, and in [Repository Name], select the SSO repository to be used. If the repository server (update system) is being added and load balancing is to be used, in [Repository server (update system) URL], set the URL of the load balancer that is positioned before the repository server.
10. When the Active Directory is selected for the directory service of the user information registration destination, input [Active Directory Settings] and [User Information Registration Entry].
11. Click [Create].
12. The repository server is created. A list of the created servers is displayed. It is possible to check the Web server name and the port number used by a server.
13. Activate the created repository server. Refer to 'Starting a Repository Server' in 'Operation and Maintenance', for an explanation of repository server start.
14. Download the authentication infrastructure setup file necessary for setting up the authentication server or repository server (update system).

    Downloading the Authentication Infrastructure Setup File

    > Download the authentication infrastructure setup file from the Interstage Management Console of the machine where the repository server (update system) was created.
    >
    > On the Interstage Management Console, click [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure] and then click the [Authentication infrastructure setup file] tab. Set the [Password], and click [Download] to download the authentication infrastructure setup file to the machine on which the Web browser is operating.
    >
    > The authentication infrastructure setup file is important for security, and is encrypted using the password. Protect the password from exposure to third parties. After the authentication server or repository server (reference system) is set up, always delete the password.

Note

Combinations below cannot be used for the machine that constructs the repository server.

- SSL is used to connect with the Directory Service in the operation security.
- SSL is used to connect with the Active Directory in the repository server

The following methods should be used instead if the above combination is used.

- SSL is not used to connect with the Directory Service in the operation security.

  The Directory Service that the operation security is connected to should be located in the machine that constructs the repository server. The SSO repository can also be shared. In doing so, security can be secured even if the operation security does not use SSL for the connection with the Directory Service.

- SSL is not used to connect with the Active Directory in the repository server

  Using functionality such as IPCOM IPSec-VPN to ensure the security of the communication path between the repository server and the Active Directory. By doing so, the repository server can ensure the security even if it does not use SSL for the connection with the Active Directory.

2.3.4 Adding a Repository Server (Update System) for Load Distribution

This section describes how to add a repository server (update system) for load distribution.

If load balancing of repository servers (update system) is to be implemented, the environment of the repository server (update system) being created must be the same as that of the existing repository server (update system).

The sections below describe how to use the ssobackup command to export the repository server (update system) environment from the export machine where the repository server (update system) is already constructed, and how to use the ssorestore command to import the repository server (update system) environment to the import machine where the repository server (update system) is being added.

Refer to "Backup commands" in the "Reference Manual (Commands)" for details of the ssobackup and ssorestore commands.

Load Balancer Settings

The load balancer is required to manage the session. For details about how to set the load balancer, refer to "Load distribution of the repository server (update system)."

Preparing the Import Machine

Prepare a machine that has the same disk configuration as the export machine.

Fetching Export Machine Resources

1. On the export machine, execute the ssobackup command with the -sv option specified to extract the repository server resources to a resource storage file. (*1) Also export the following resources:
   - Interstage HTTP Server (*1)
   - Interstage directory service (*2)
2. If the repository server or Interstage directory service uses SSL communication, export the Interstage certificate environment resources. (*1)
3. Transfer the resources extracted in Steps 1 and 2 above to the import machine. Ensure that the resources are not intercepted by a third party during transfer. At the time of transfer, do not change the file authorities of the resource storage files extracted in Step 1 above.

Constructing the Import Machine Environment

1. Execute the ssorestore command at the import machine to import the repository server resources. (*1) Also import the following resources:
   - Interstage HTTP Server (*1)
   - Interstage directory service (*2)
2. If the repository server or Interstage directory service uses SSL communication, import the Interstage certificate environment resources that were extracted from the export machine. (*1)
3. Start all the repository servers.

   Refer to "Starting a Repository Server" for information on how to start repository servers.
4. Delete the resource storage files that were extracted from the export machine.

*1 Refer to "Moving Resources to Another Server" under "Maintenance (Resource Backup)" in the "Operator's Guide" for information on exporting and importing resources.

*2 When the Interstage directory service is used for the user information registration destination directory service, a database sharing environment must be created. Refer to the chapter 'Creating a Load Distribution Environment' in the "Directory Service Operator's Guide" for information on how to create a database sharing environment.

Notes

- When repository server load balancing is used, the Interstage single sign-on systems of the multiple repository servers must all be the same version and edition and have the same install directory. The platform must also be the same.
- The resource storage files fetched from the repository server are critical files for security. Ensure that these file are deleted after the repository server is constructed.
- When migrating a repository server from an older version or level, check that the definition items specifying that load balancing is not used for the repository server (update system) are not added to the repository server environment configuration file.

2.3.5 Constructing an SSL Communication Environment for a SSO Repository (Master)

For replication between SSO repositories, data must be transferred from the master SSO repository of the repository server (update system) to the slave SSO repository of the repository server (reference system). SSL communication is performed by the repository server (reference system).

To enable SSL communication for performing replication, the SSL communication environment must be set up on the SSO repository (master).

To use a relational database (RDB) as the SSO repository, refer to 'Setting up an Environment for SSL Communication" chapter of the "Directory Service Operator's Guide", and set up the SSL communication environment.

To use replication in the SSO repository that is to be used a standard database, set up the SSL communication environment according to the procedure described below.

This setup is unnecessary when one repository server (reference system) is to be added to an already set-up authentication infrastructure, and the SSL communication environment is already set up on the active repository server.

1. Setting SSL Communication

    1. Preparations for SSL communication (acquiring the SSL site certificate and registering it in the Interstage certificate environment)

        When the site certificates for the repository server (update system) and repository server (reference system) are issued by different certificate authorities, the certificate for the repository server (reference system) must also be registered in the repository server (update system). For details, refer to 2.4.1.1 Preparations for SSL Communication.

    2. Setup for SSL communication (creation of SSL configuration for replication)

        On the Interstage Management Console, select [Security] and then [SSL] from the [System] menu. From the [Create a new SSL Configuration] tab, perform setup for SSL communication as follows:

        - Configuration Name

            Set the name identifying the SSL configuration.

        - Site Certificate Nickname

            Set the nickname that was specified when the SSL certificate was registered in the Interstage certificate environment as described in 2.4.1.1 Preparations for SSL Communication. The registered SSL site certificate can be accessed in the Interstage Management Console by selecting [Security] and then [Certificates] on the [System] menu. Click [Site Certificate] to access the SSL site certificate.

        - Protocol Version

            Select 'SSL 3.0' only.

        - Client certificate

            Select 'Yes (Authenticate when client certificate is presented).'

- Encryption Method

  Change the encryption method when necessary.

- Nickname of Certificate of Certificate Authority

  Change the nickname when necessary.

For details of the above items, refer to the Operator's Guide.

2. Confirming the Validity of a Certificate

In addition to the above setup, the validity of the certificate must be confirmed. This process includes acquiring and registering the CRL in the Interstage certificate environment. When the site certificates for the repository server (update system) and repository server (reference system) are issued by different authorities, acquire the CRL from the certificate authority that issued the certificate of the repository server (reference system). Then register this CRL on the repository server (update system).

For details, refer to 2.4.1.3 Preparations for Confirming Validity of Certificate Authentication.

Note

Replication using SSL communication can protect confidential information since risks such as electrical interception, alteration, and spoofing are avoided by SSL client-server authentication, and communication between respective SSO repositories is encrypted. SSL communication is, therefore, highly recommended for security.

2.3.6 Adding a Repository Server (Reference System)

This section explains how to set up a repository server (reference system) when two or more repository servers are to be set up.

This section describes how to set up the Repository server (reference system) that is used as a standard database as the SSO repository.

To use a relational database (RDB) as the SSO repository, refer to the chapter "Environment Setup" in the "Directory Service Operator's Guide", and create the SSO repository. Refer to "Setting up for Adding the Repository Server (Reference System)" and set up the Repository server (reference system).

2.3.6.1 Backing up the SSO Repository of the Repository Server (Update System)

To create the SSO repository (slave) used as a standard database of the repository server (reference system), back up the data of the SSO repository (master) used as a standard database of the repository server (update system). Restore the backed-up data onto the repository server (reference system).This section explains how to back up the data of the SSO repository (master) used as a standard database.

Back up the SSO repository (master) data of the repository server (update system) according to the following procedure:

Windows32/64

1. On the Interstage Management Console of the repository server (update system), select [Services] and then [Repository] from the System menu.
2. On [Repository: View Status], check the check box of the SSO repository for master operation. Then click the [Stop] button to stop the SSO repository.
3. On the repository server (update system), execute the irepbacksys command with the -dataonly option specified. Back up the SSO repository data in the directory. Execute the irepbacksys command as the administrator.

Solaris32/64 Linux32/64

1. On the Interstage Management Console of the repository server (update system), select [Services] and then [Repository] from the System menu.
2. On [Repository: View Status], check the check box of the SSO repository for master operation. Then click the [Stop] button to stop the SSO repository.
3. On the repository server (update system), execute the irepbacksys command with the -dataonly option specified. Back up the SSO repository data in a file. Execute the irepbacksys command as the administrator.

Refer to 'Backup Commands' in the Reference Manual (Command Edition) for details of the *irepbacksys* command.

Example

Windows32/64

Backup destination directory: C:\WINDOWS\temp\backup

SSO repository name: ssorep

Specify the backup destination directory as the directory in which the SSO repository data is to be backed up.

After execution of the irepbacksys command, the backup folder is created under the C:\WINDOWS\temp folder.

```
C:\>irepbacksys -d C:\WINDOWS\temp\backup -R ssorep -dataonly
IREP: INFO: irep11000: Backup has completed.  C:\WINDOWS\temp\backup [ssorep]
```

Solaris32/64 Linux32/64

Backup file name (without extension): /home/user1/backup

SSO repository name: ssorep

Specify the backup file name as the name of the file in which the SSO repository data is to be backed up. In this case, the specified file name must not include the extension.

After execution of the irepbacksys command, the /home/user1/backup.tar.gz is created.

```
# irepbacksys -f /home/user1/backup -R ssorep -dataonly
UX:IREP: INFO: irep11000: Backup has completed. /home/user1/backup.tar.gz[ssorep]
```

2.3.6.2 Setting up the SSL Communication Environment for the SSO Repository (Slave)

To use SSL communication for replication between SSO repositories used as a standard database, the SSL communication environment must be set up on the SSO repository (slave).

This setup is unnecessary when the SSL communication environment is already set up on the repository server (reference system).

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

1. Setting SSL Communication

    1. 1.Preparations for SSL communication (acquiring SSL site certificate and registering it in Interstage certificate environment)

        When the site certificates for the repository server (update system) and repository server (reference system) are issued by different authorities, the certificate of the repository server (reference system) must also be registered in the repository server (update system. For details, refer to 2.4.1.1 Preparations for SSL Communication.

    2. SSL communication setup (creation of SSL configuration for replication) using the Interstage Management Console

        Select [Security] and then [SSL] from the System menu. On the [Create a new SSL Configuration] tab, set up SSL communication as follows:

        - Configuration Name

          Enter the name identifying the SSL configuration.

        - Site Certificate Nickname

          Enter the nickname that was specified when the SSL certificate was registered in the Interstage certificate environment as described in 2.4.1.1 Preparations for SSL Communication. The registered SSL site certificate can be accessed on the Interstage Management Console by selecting the [Security] and then [Certificate] from the System menu. Click [Site Certificate] to view the site certificate.

        - Protocol Version

          Select 'SSL 3.0' and 'TLS 1.0'.

        - Client Certificate

          Select 'Yes (Authenticate when client certificate is presented)'.

        - Encryption Method

          Change the encryption method when necessary.

- Nickname of Certificate Authority

  Change the nickname when necessary.

For details of the above items, refer to the Operator's Guide.

2. Confirming the Validity of the Certificate

In addition to the above setup, the validity of the certificate authentication must be confirmed. This process includes acquiring and registering the CRL in the Interstage certificate environment. When the site certificates for the repository server (update system) and repository server (reference system) are issued by different authorities, acquire the CRL from the certificate authority that issued the certificate of the repository server (update system). Then register this CRL in the machine of the repository server (reference system).For details, refer to 2.4.1.3 Preparations for Confirming Validity of Certificate Authentication.

Note

- Replication using SSL communication can protect confidential information since risks such as electrical interception, alteration, and spoofing are avoided by SSL client-server authentication, and communication between respective SSO repositories is encrypted. SSL communication is, therefore, highly recommended for security.
- To set up the SSL communication environment on the repository server (reference system), do not use a site certificate for test.

2.3.6.3 Creating an SSO Slave Repository of the Repository Server (Reference System)

Create the SSO repository used as a standard database for slave operation of replication on the machine on which the repository server (reference system) is set up. On the Interstage Management Console of the machine on which this repository server (reference system) is to be set up, perform the following procedure:

1. Select [Services] and then [Repository] from the System menu. Click the [Create a New Repository] tab.
2. Specify the items as described below, and click the Create button.

   Descriptions in bold indicate settings that must be the same as those of the SSO repository (master). Items marked with (*1) can be specified only when the SSO repository is to be created. These items cannot be changed after the SSO repository is created. Carefully set these items. For other items, check values and change them when necessary.

   General Settings

   - Repository Name (*1)

     Enter the same name as that of the SSO repository (master) that was created for the repository server (update system).

   - Administrator DN (*1)

     Enter the DN (distinguished name) of the administrator who manages the created SSO repository. This value must be specified in dn=distinguished-name format (example: cn=manager).

   - Administrator DN password

     Enter the password for the SSO administrator.

   - Administrator DN password (re-enter)

     Enter the password for the SSO administrator again.

   - Public Directory (*1)

     Set the same directory as that for the SSO repository (master) that was created for the repository server (update system).

   - Repository database (*1)

     Set the same directory as that for the SSO repository (master) that was created for the repository server (update system).

   - Database Storage Directory (*1)

     Set the same directory as that of the SSO repository (master) that was created for the repository server (update system).

   - Cache Size

     The default value is '1000' pages. One page consists of 4 KB. Change this value when necessary.

   Detailed Settings

Connection Settings

- Port Type to be used

  Select 'both'.

- Port number

  Specify the port number for non-SSL communication.

- SSL Port number

  Specify the port number for SSL communication. The default value is '636'. Change this value when necessary.

- SSL configuration

  Select the SSL configuration for replication that was defined in 2.3.6.2 Setting up the SSL Communication Environment for the SSO Repository (Slave)

- Connection idle Timeout

  The default value is '900 seconds'. Change the value as necessary.

Security Settings

- User password encryption method (*1)

  The default is 'SHA256'. Change the value as necessary.

Search Settings

- Maximum number of searchable entries

  Maximum Number of Entries to be Retrieved. The default value is '500'. Change this value when necessary.

- Retrieval Processing Timeout

  The default value is '3600' seconds. Change this value when necessary.

Access Log Configuration

- Output Access Log

  Always select 'Yes'.

- Output Level

  Select 'Client requests' and 'Server errors'. For other cases, select other items.

- Storage Directory

  Change the directory when necessary.

- Rotation Type

  Change the type when necessary.

- Size

  Change the size when necessary.

- Number of Log Files to Maintain

  Change the value when necessary.

3. Confirm the displayed status of the SSO repository (slave).

On the Interstage Management Console of the machine where the repository server (update system) was created, confirm the setting status of the SSO repository (master). Select [Services] and then [Repository] from the System menu. On [Repository: View Status], select the SSO repository that was created for the master system. Confirm the settings on the [General Settings], or that displayed after clicking [Detailed Settings [Show]].

Note

If the [Administrator DN password] of the SSO slave repository was changed during replication operation, the [Replication connection Settings] of the SSO master repository must be edited. Refer to the Directory Service Operator's Guide for details.

2.3.6.4 Restoring the SSO Repository in the Repository Server (Reference System)

To create the SSO slave repository used as a standard database of the repository server (reference system), back up the data of the SSO repository (master) used as a standard database of the repository server (update system) and restore it to the repository server (reference system).

This section explains how to restore the data of the SSO master repository used as a standard database of the repository server (update system) to the repository server (reference system).

The SSO master repository data of the update system repository server is restored according to the following procedure:

Windows32/64

1. To restore the repository server (reference system), transfer the backup destination directory that was created as described in 2.3.6.1 Backing up the SSO Repository of the Repository Server (Update System).

   Ensure that there is adequate security in place to prevent third parties from electronically intercepting data during the above transfer. Always delete the directory after use.

2. On the machine of the repository server (reference system), execute the ireprestsys command with the -dataonly option specified to restore data in the backup destination directory. The same SSO repository name as the name of the backed-up SSO repository must be specified in this command.

Solaris32/64 Linux32/64

1. To restore the repository server (reference system), transfer the backup file that was created as described in 2.3.6.1 Backing up the SSO Repository of the Repository Server (Update System).

   Ensure that there is adequate security in place to prevent third parties from electronically intercepting data during the above transfer. Always delete the file after use.

2. On the machine of the repository server (reference system), execute the ireprestsys command with the -dataonly option specified to restore the backup file. The same SSO repository name as the name of the backed-up SSO repository must be specified in this command.

Refer to 'Backup Commands' in the Reference Manual (Command Edition) for details of the ireprestsys command.

Example

Windows32/64

Backup destination directory : C:\WINDOWS\temp\backup

SSO repository name: ssorep

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

The same SSO repository name as the name of the backed-up SSO repository must be specified in the command.

A message asking the user to confirm if they want to overwrite the database is displayed. To replace it and continue restoring the data, enter 'y'.

```
C:\>ireprestsys -d C:\WINDOWS\temp\backup -R ssorep -dataonly
Data already exists in database store.  (C:\Interstage\Enabler\EnablerDStores\IREP\ssorep\data)
Are you sure of deleting data in database store? (y/n):y
IREP: INFO: irep11001: Restore has completed.  C:\WINDOWS\temp\backup [ssorep]
```

Solaris32/64

Backup file name: /home/user1/backup.tar.gz

SSO repository name: ssorep

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

The same SSO repository name as the name of the backed-up SSO repository must be specified in the command.

A message asking the user to confirm that they wish to replace the database is displayed. Then enter y.

```
# ireprestsys -f /home/user1/backup.tar.gz -R ssorep -dataonly
Data already exists in database store.  (/var/opt/FJSVena/EnablerDStores/FJSVirep/ssorep/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.  /home/user1/backup.tar.gz[ssorep]
```

Linux32/64

Backup file name: /home/user1/backup.tar.gz

SSO repository name: ssorep

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

The same SSO repository name as the name of the backed-up SSO repository must be specified in the command.

A message asking the user to confirm that they wish to replace the database is displayed. Then enter y.

```
# ireprestsys -f /home/user1/backup.tar.gz -R ssorep -dataonly
Data already exists in database store.  (/var/opt/FJSVena/DStores/FJSVirep/ssorep/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.  /home/user1/backup.tar.gz[ssorep]
```

2.3.6.5 Changing the Settings of the SSO Repository of the Restored Repository Server (Reference System)

Set replication slave operation for the restored SSO repository used as a standard database as described in 2.3.6.4 Restoring the SSO Repository in the Repository Server (Reference System). Perform the following procedure on the Interstage Management Console of the repository server (reference system):

1. Select [Services] and then [Repository] from the System menu, and select the SSO repository for slave operation on [Repository: View Status].
2. Click [Detailed Settings [Show]], and select 'Slave' as the [Operation mode] of [Replication Settings].
3. In the newly displayed [Slave operation Settings], enter the host name of the machine of the repository server (update system).
4. Click [Update].
5. Check the check box of the updated SSO repository, and click [Start] to start the SSO repository.

2.3.6.6 Setting up for Adding the Repository Server (Reference System)

This section explains how to set up the repository server (reference system). On the Interstage Management Console of the machine where the repository server is to be set up, perform the following procedure. Refer to the Operator's Guide for details of the items to be defined on the Interstage Management Console.

You will need an authentication infrastructure setup file to set up the repository server (reference system). Refer to Downloading the Authentication Infrastructure Setup File under 2.3.3 Constructing a Repository Server (One Server or Update System) or how to create the authentication infrastructure setup file. To create the repository server (reference system), the slave SSO repository must be created in advance. Refer to 2.3.6.3 Creating an SSO Slave Repository of the Repository Server (Reference System) for details on how to create the SSO repository (slave) used as a standard database. The following procedure describes how to set up the repository server (reference system):

1. Select the Web server (Interstage HTTP Server) where the repository server (reference system) is to be created.
2. If there is no Web server for creating a repository server (reference system), create a new Interstage single sign-on dedicated Web server.
3. If the repository server (reference system) is to use SSL communication, enter the SSL settings in the Web server selected or created in Step 1. Refer to "Setting up an SSL Communication Environment for a Repository Server" for information on how to create SSL definitions.
4. Select [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure] and then click the [Authentication infrastructure Settings] tab.

5. Select [Setup Repository server and Authentication server to the separate servers.], and click [Next]. The selection window for the server to be created is displayed.
6. Select [Create a new Repository server] and then [Repository server (reference system)], and click [Next].
7. [File Settings] is displayed. Specify the Authentication infrastructure setup file downloaded from the Repository server (update system) in [Authentication infrastructure setup file].
8. Enter the password that was set for the Authentication infrastructure setup file, and then click [Next].
9. [General Settings] is displayed. In [Web Server used], select the name of the Web server selected or created in Step 1. In [Repository name], select the SSO repository that is to be used, and then click [Create].
10. The repository server is created. A list of the created servers is displayed. It is now possible to check the port number used by a server.
11. Activate the created repository server. Refer to 'Starting a Repository Server' in 'Operation and Maintenance', for an explanation of repository server start.
12. Delete the authentication infrastructure setup file.

Notes

- When the Windows(R) Internet Explorer(R) is used as the browser, an authentication infrastructure setup file with an absolute path length that exceeds 200 bytes may not be able to be specified with the Browse button. In this case, change the location of the authentication infrastructure setup file so that its absolute path length is shorter.
- The authentication infrastructure setup file is important for security. Always delete this file after the repository server (reference system) is set up.

2.3.6.7 Changing the Settings of the SSO Repository of the Repository Server (Update System)

Set the information on the SSO slave repository used as a standard database of the added repository server (reference system) in the SSO master repository used as a standard database of the repository server (update system). Perform the following procedure on the Interstage Management Console of the repository server (update system):

1. Click [Services] and then [Repository] from the System menu, and from the [Repository: View Status] window select the SSO repository for master operation.
2. Click [Detailed Settings [Show]]. Go to Step 3 when 'Master' is selected as the [Operation mode] of [Replication Settings].

   When 'Master' is not selected, select 'Master'. [Replication destination host list] is displayed.
3. Click [Add], and enter the machine information of the repository server (reference system) to be added in each item field of the newly displayed [Replication connection Settings] Click [Update].

   - Host name

     Enter the host name of the SSO slave repository.
   - Port number

     Enter the [SSL Port number] that was set for the SSO slave repository.
   - Enable SSL encryption?

     Select 'Yes'.
   - Present client certificate?

     Select 'Yes' or 'No'.
   - SSL configuration

     When 'Yes' is selected in [Present client certificate?], select the SSL configuration for replication that was defined as described in "Setup of the SSL communication environment for repository server (update system)".
   - DN for the connection

     Enter the same administrator DN as that specified for the SSO repository (slave).

- Password for the connection

  Enter the same password as the administrator DN password specified for the SSO repository (slave).

4. Check the check box of an SSO repository for which settings are changed, and click [Start] to start the SSO repository.

2.4 Setup of Authentication Server

This section explains the procedure for setting up of the authentication server that provides the authentication infrastructure. Use the Interstage Management Console to set up the authentication server.

2.4.1 SSL Communication Environment Setup

The SSL environment must be set up before the authentication infrastructure.

The flow of setting up SSL communication environment is shown below.

SSL Communication using Authentication Server

If using SSL communication on the authentication server, perform the following steps according to the operating conditions:

1. Required settings

   Refer to 2.4.1.1 Preparations for SSL Communication.

   Refer to 2.4.1.2 Settings for SSL Communication.

2. Confirming validity of certificate

   In addition to the above settings, perform the operations explained in 2.4.1.3 Preparations for Confirming Validity of Certificate Authentication.

3. Operation using Application Gateway

   In addition to the above settings, perform the operations explained in 2.4.1.5 Settings for Operation using Application Gateway.

SSL Communication using SSL Accelerator

To execute SSL communication using the SSL accelerator, configure the settings according to the operation shown below.

1. Required settings

   Refer to Settings for 2.4.1.4 Settings for SSL Communication Using SSL Accelerator

2. Confirming validity of certificate

   In addition to the above settings, perform the operations explained in 2.4.1.3 Preparations for Confirming Validity of Certificate Authentication.

SSL Communication using Application Gateway

For operation using non-SSL communication between the Application Gateway complete the following settings according to the operating conditions:

1. Required settings

   Refer to 2.4.1.5 Settings for Operation using Application Gateway.

2. Confirming validity of certificate

   In addition to the above settings, perform the operations explained in 2.4.1.3 Preparations for Confirming Validity of Certificate Authentication.

2.4.1.1 Preparations for SSL Communication

For SSL communication using each server, acquire the site certificates and register them in the Interstage certificate environment. For explanations of site certificate acquisition and registration in the Interstage certificate environment, refer to 'Setting and Use of the Interstage Certificate Environment' of the Security System Guide.

When the site certificate is already acquired and registered, the registered site certificate can be used.

The following is an example of preparations for SSL communication.

Setting Access Permission of Interstage Certificate Environment Solaris32/64 Linux32/64

To set up the Interstage certificate environment, an owner group with permission to access the Interstage certificate environment must be created. The created owner group must be specified in the -g option of the scsmakeenv command when the Interstage certificate environment is set up.

The effective users who are to be registered in the owner group of the Interstage certificate environment must be already set in the User directive of the environment configuration file (httpd.conf) of the Interstage HTTP server.

For an explanation of the access permission of the Interstage certificate environment, refer to 'Setting and Use of the Interstage Certificate Environment' of the Security System Guide.

Creating the Interstage Certificate Environment and Signing Request of a Certificate for SSL Communication

Specify distinguished names such as country code, alphanumeric first and last name, alphanumeric organization name, alphanumeric organizational unit name, prefecture name, and municipality name to create a certificate signing request (CSR) for signing requesting the certificate for the SSL communication. The Interstage certificate environment is also created at this time.

Use the scsmakeenv command to create the certificate signing request (CSR). Send the CSR to a certificate authority to request to issue the certificate.

For information on how to create the certificate signing request (CSR), refer to Appendix D, 'Creating the Interstage certificate environment and Signing Request of a Certificate for SSL Communication'.

For information on certificate authority, refer to "Security System Guide."

Registering the Certificates for SSL Communication

The site certificate issued by a certificate authority and the CA certificate of the certificate authority that issued the site certificate must be acquired and registered.

Use the certificate and CRL registration command (scsenter) to register these certificates.

For information on registering the certificates in the Interstage certificate environment, refer to 'Registering the Certificates for SSL Communication'.

2.4.1.2 Settings for SSL Communication

SSL configuration must be defined using the Interstage Management Console.

To define the SSL configuration, select the [Security] and then [SSL] from the System menu. Click the [Create a new SSL Configuration] tab, and then perform [General Settings]. Select the nickname of the confirmed site certificate, and define the SSL configuration.

Refer to the Operator's Guide for an explanation of the start of the Interstage Management Console. Refer to the Operator's Guide for details of the items to be defined on the Interstage Management Console.

Set each item of the SSL environment configuration as follows:

- Configuration Name

  Set the identifying the SSL configuration. The configuration name specified here is used for setting the authentication server.

- Site Certificate Nickname

  Enter the nickname that was specified when the site certificate was registered in the Interstage certificate environment as described in 2.4.1.1 Preparations for SSL Communication. The registered site certificate can be accessed on the Interstage Management Console by selecting [Security] and then [Certificate] from the System menu and then clicking [Site Certificate].

- Protocol Version

  Select 'SSL 3.0' and 'TLS 1.0'.

- Verify Client Certificate?

  To use certificate authentication, select 'Yes (Authenticate when client certificate is presented)'. If you do not want to use certificate authentication, select "No".

- Encryption Method

  When necessary, change the method. Refer to the Operator's Guide.

- CA Certificate Nickname

  When necessary, change the nickname. Refer to the Operator's Guide.

2.4.1.3 Preparations for Confirming Validity of Certificate Authentication

The validity of a certificate can be confirmed using the certificate revocation list (CRL) at certificate authentication. The following explains the preparations for certificate validity confirmation.

SSL Communication using Authentication Server

If using SSL communication on the authentication server, perform the following steps.

1. Registering the Certificate of the CRL-issuing Authority (*1)

2. Registering CRL

*1 Register the CRL that was issued from a certificate authority that was not specified in the site certificate described in 2.4.1.1 Preparations for SSL Communication.

SSL Communication using SSL Accelerator or Application Gateway

When the authentication infrastructure uses SSL Accelerator or Application Gateway perform the following describes:

1. Creating Interstage certificate environment (*2)

2. Registering the Certificate of the CRL-issuing Authority

3. Registering CRL

*2 If the Interstage certificate environment is already created, there is no need to perform this task.

2.4.1.4 Settings for SSL Communication Using SSL Accelerator

To use SSL Accelerator, perform the settings depending on the operating conditions. Refer to "Linkage with SSL Accelerator" for an explanation of setting SSL Accelerator.

2.4.1.5 Settings for Operation using Application Gateway

To operate using Application Gateway the environment for the Application Gateway must be set up. For details, refer to the explanation for the setting of the Application Gateway for 'Linkage with Application Gateway'.

2.4.2 Setting up One Authentication Server

Set up an authentication server as follows using the Interstage Management Console of the machine on which the authentication server is to be set up. For details of the items to be defined on the Interstage Management Console, refer to the Operator's Guide.

An authentication infrastructure setup file is required to set up the authentication server. Refer to Downloading the Authentication Infrastructure Setup File under 2.3.3 Constructing a Repository Server (One Server or Update System) for an explanation of creating the authentication infrastructure file.

1. Select the Web server (Interstage HTTP Server) where the authentication server is to be created.

   If there is no Web server for creating an authentication server, create a new Interstage single sign-on dedicated Web server.

2. If the authentication server is to use SSL communication, enter the relevant SSL settings in the Web server selected or created in Step 1.

3. Select [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure] and then the [Authentication infrastructure Settings] tab.

4. Select [Setup Repository server and Authentication server to the separate servers.], and then click [Next].

5. The window for selecting a server to be created is displayed. Select [Create a new Authentication server], and then click [Next].

6. [File Settings] is displayed. Specify the Authentication infrastructure setup file downloaded from the Repository server (update system) in [Authentication infrastructure setup file].

7. Enter the password that was set for the Authentication infrastructure setup file, and then click [Next].

8. [General Settings] is displayed. In [Web Server used], select the name of the Web server selected or created in Step 1

   When SSL communication uses SSL Accelerator specify the HTTP header that is used by SSL Accelerator to post the user certificate in [HTTP header name for user certificate acquisition].

9. If the Interstage directory service is used in the user information registration destination directory service to perform the integrated Windows authentication, select "Integrated Windows Authentication" for [Authentication method] under [Authentication method Setting], and enter the [Integrated Windows Authentication Setting].

10. If separate update system and reference system repository servers are used, specify [Repository server (reference system) URL]. Up to five repository servers can be set at a time. To set six or more repository servers (reference system), create an authentication server. Then click [Authentication server] and the [Settings] tab, and select [Detailed Settings [Show]]. Specify the servers using [Repository server (reference system) URL] of [Communication Settings with Repository server (reference system)].

    In this item, the same host name cannot be specified two or more times. A repository server (update system) can also be specified.

11. Click [Create]. The authentication server is created. A list of the created servers is displayed. It is now possible to check the Web server name and the port number used by a server.

12. Activate the authentication server.

    Refer to 'Starting an Authentication Server' in 'Operation and Maintenance', for an explanation of authentication server start.

13. Delete the authentication infrastructure setup file.

Notes

- To perform integrated Windows authentication, construct the authentication server, and then prepare it to be federated with Active Directory. Refer to "Settings for Active Directory linkage" and set the Integrated Windows authentication. Upon completion, start the Integrated Windows authentication application. For details about how to start the Integrated Windows authentication application, refer to "Starting an Authentication Server,"

- When the Windows(R) Internet Explorer(R) is used as the browser, an authentication infrastructure setup file with an absolute path length exceeding 200 bytes may not be able to be specified with the Browse button. In this case, change the location of the authentication infrastructure setup file so that its absolute path length is shorter.

- The authentication infrastructure setup file is important for security. Always delete this file after the authentication server is set up.

2.4.3 Adding an Authentication Server for Load Distribution

This section explains the process of adding an authentication server for load distribution.

To distribute the authentication server load using a load balancer, the authentication server must be constructed with the same environment as the already constructed authentication server.

The sections below describe how to use the ssobackup command to export the authentication server environment from the export machine where the authentication server is already constructed, and how to use the ssorestore command to import the authentication server environment to the import machine where the authentication server is being added.

Refer to "Backup commands" in the "Reference Manual (Commands)" for details of the ssobackup and ssorestore commands.

The ssobackup command also exports the messages that are displayed on Web browsers. Therefore, these messages must be customized before the authentication server is exported. Refer to "Customizing Messages Displayed on a Web Browser" for details of how to customize the messages displayed on Web browsers.

Load Balancer Settings

Load balancer settings are required to manage the session. For details of how to set the load balancer, refer to "Load distribution of the authentication server".

Preparing the Import Machine

Prepare a machine that has the same disk configuration as the export machine.

Fetching Export Machine Resources

1. At the export machine, execute the ssobackup command with the -ac option specified to extract the authentication server resources to the resources storage files. (*1) Also export the following resources:

   - Interstage HTTP Server (*1)

2. If SSL communication is to be used at the authentication server, also export the Interstage certificate environment. (*1)

3. If Integrated Windows Authentication is used, export the IJServer resources. (*1)

4. Transfer the resources fetched in Steps 1 to 3 above to the import machine.

   Ensure that the resources are not intercepted by a third party during transfer. At the time of transfer, do not change the file authorities of the resource storage files extracted in Step 1 above.

Constructing the Import Machine Environment

1. Execute the ssorestore command at the import machine to import the authentication server resources. (*1) Also import the following resources:

   - Interstage HTTP Server (*1)

2. When SSL communication is used by the authentication server, (*1) import the Interstage certificate environment resources that were fetched from the export machine.

   When SSL communication is used by the authentication server but using the same certificate for the load-balancing machines is not permitted, newly acquire a site certificate and register it in the site certificate environment as described in 2.4.1.1 Preparations for SSL Communication. In this case, the nickname of the site certificate to be used when requesting the certificate for SSL communication must be the same as that specified in the authentication server already installed. Also the nickname of the CA certificate to be used at registering the certificate for SSL communication must be the same as that specified in the already set authentication server.

3. If Integrated Windows Authentication is used, import the IJServer resources that were fetched from the export machine. (*1)

4. If a repository server (reference system) is being constructed, on the Interstage Management Console, select [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure] and [Authentication server]. On the [Settings] tab, click [Detailed Settings [Show]]. The environment of the exported authentication server for copying is set in [Repository server (reference system) URL] of [Communication Settings with Repository server (reference system)]. Therefore, change this environment depending on the operating conditions, and click [Update].

   For details of the items to be set on the Interstage Management Console, refer to the Operator's Guide.

5. Start any Integrated Windows Authentication applications in use in all of the authentication servers.

   Refer to 'Starting an Integrated Windows Authentication application' for information on this process.

6. Start all the authentication servers.

   Refer to 'Starting an Authentication Server' for an explanation of the authentication server start.

7. Delete the resource storage files used for the resources fetched from the export machine.

*1 Refer to "Moving Resources to Another Server" under "Maintenance (Resource Backup)" in the "Operator's Guide" for information concerning exporting and importing resources.

Notes

- For load distribution of the authentication server, the related multiple authentication servers must have the Interstage Single Sign-on of the same version, edition, and installation directory. The same platform must also be used.

- The load balancer must be set up so that the requests from the same client transfer to same authentication servers.
- The resource storage files fetched from the authentication server are important for security. After the authentication server is set up, always delete the environment information file.

2.4.4 Setting the Reference System Repository Server Information in the Authentication Server

When a repository server (reference system) is set up, the information on the repository server must be set in the authentication server using the Interstage Management Console according to the following procedure. Refer to the Operator's Guide for details of the items to be set on the Interstage Management Console.

1. Select [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure], and then from [Authentication server] click the [Settings] tab.
2. Set the repository server (reference system) URL in [Repository server (reference system) URL] of [Communication Settings with Repository server (reference system)] of [Detailed Settings [Show]]. Then click [Update].
3. After the reference system repository server is set, start the authentication server.

   Refer to 'Starting an Authentication Server' for an explanation of the authentication server start.

2.5 Constructing a Repository Server and Authentication Server

This section describes the procedures for constructing an authentication infrastructure, comprised of a repository server and an authentication server, on one machine.

2.5.1 Setting up a Repository Server and Authentication Server on a Single Machine

This section explains how to set a repository server and an authentication server on a single machine according to the following procedure using the Interstage Management Console. Refer to the Operator's Guide for details of the items to be set on the Interstage Management Console.

1. Select the Web server (Interstage HTTP Server) where the repository server and authentication server are to be created. If there is no Web server for creating a repository server and an authentication server, create a new Interstage single sign-on dedicated Web server.
2. If the authentication server is to use SSL communication, enter the SSL settings in the Web server selected or created in Step 1.
3. Select [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure] and then click the [Authentication infrastructure Settings] tab.
4. Select [Setup Repository server and Authentication server to a single server.] and click [Next].
5. The selection screen of the directory service that is used for the user information registration destination is displayed.
6. Select the directory service to register the user information, and then click the [Next].
7. [General Settings] is displayed. Set the [Authentication infrastructure URL] and [Repository Server (update system) URL]. In [Web Server used], select the name of the Web server selected or created in Step 1, and in [Repository name], select the SSO repository that is to be used.

   When SSL communication uses SSL Accelerator the HTTP header that is used by SSL Accelerator to post the user certificate must be specified in [HTTP header name for user certificate acquisition].
8. If Active Directory is selected in the directory service of the user information registration destination , input [Active Directory Settings] and [User Information Registration Entry].
9. Click [Create] to create the repository server and authentication server. A list of the created servers is displayed. It is now possible to check the Web server name and the port number used by a server.
10. After the repository server and authentication server are created, start the repository server. When the repository server is started, the authentication server is also started. Refer to 'Starting a Repository Server' for an explanation of the repository server start.

Note

To check the Web server (Interstage HTTP Server) host used in the repository server, in the Interstage Management Console click [System] > [Services] > [Web Server] > [Web Server Name] > [Virtual Host] > [_default_: Repository Server Port Number].

2.5.2 Adding a Repository Server and Authentication Server on One Machine for Load Distribution

This section describes how to add a repository server and authentication server on one machine for load distribution.

If a load balancer is used to distribute the repository server and authentication server load, the new repository server and authentication server must be created with the same environment as the existing repository server and authentication server.

The sections below describe how to use the ssobackup command to export the repository server and authentication server environment from the export machine where the repository server and authentication server are already constructed. They also describe how to use the ssorestore command to import the repository server and authentication server environment to the import machine where the repository server and authentication server are being added.

Refer to "Backup commands" in the "Reference Manual (Commands)" for details of the ssobackup and ssorestore commands.

The ssobackup command also exports the messages that are displayed on Web browsers. Therefore, these messages must be customized before the authentication server is exported. Refer to "Customizing Messages Displayed on a Web Browser" for details of how to customize the messages displayed on Web browsers.

Load Balancer Settings

Load balancer settings are required to manage the session. For details of how to set the load balancer, refer to "Load distribution of the repository server and the authentication server that are built on same machine."

Preparing the Import Machine

Prepare a machine that has the same disk configuration as the export machine.

Fetching Export Machine Resource

1. On the export machine, execute the ssobackup command with the -sv option and -ac option specified to extract the repository server and authentication server resources to a resource storage file. (*1) Also export the following resources:

   - Interstage HTTP Server (*1)

   - Interstage directory server (*2)

2. If the authentication server uses SSL communication, export the Interstage certificate environment resources. (*1)

3. If Integrated Windows Authentication is used, export the IJServer resources. (*1)

4. Transfer the resources extracted in Steps 1 to 3 above to the import machine.

   Ensure that the resources are not intercepted by a third party during transfer. At the time of transfer, do not change the file authorities of the resource storage files extracted in Step 1 above.

Constructing the Machine Environment

1. 1.Execute the ssorestore command at the machine to import the repository server and authentication server resources. (*1) Also import the following resources:

   - Interstage HTTP Server (*1)

   - Interstage directory service (*2)

2. If the authentication server uses SSL communication, import the Interstage certificate environment resources that were extracted from the export machine. (*1)

   If the authentication server uses SSL communication and use of the same certificates is not permitted at the load balancing machine, refer to "Preparations for SSL communication" and obtain new site certificates, and register them to the Interstage certificate environment. Use the nicknames set at the already installed authentication server machine for both the site certificate nickname set when applying for certificates used for SSL communication, and the Certificate Authority certificate nickname that is set when registering certificates used for SSL communication.

3. If Integrated Windows Authentication is used, import the IJServer resources that were fetched from the export machine. (*1)

4. Start any Integrated Windows Authentication applications in use in all the authentication servers.

   Refer to 'Starting an Integrated Windows Authentication application' for information on this process.

5. Start all of the repository servers. Starting the repository servers also starts the authentication servers.

   Refer to "Starting a Repository Servers" for information on how to start repository servers.

6. Delete the resource storage files that were fetched from the export machine.

*1 Refer to "Moving Resources to Another Server" under "Maintenance (Resource Backup)" in the "Operator's Guide" for information concerning exporting and importing resources.

*2 A database sharing environment must be created. Refer to the chapter 'Creating a Load Distribution Environment' in the "Directory Service Operator's Guide" for information on how to create a database sharing environment.

Notes

- When repository server and authentication server load balancing is used, the Interstage single sign-on systems of the multiple repository servers and authentication servers must all be the same version and edition and have the same install directory. The platform must also be the same.

- The resource storage files fetched from the repository server and authentication server are critical files in terms of security. Ensure these file are deleted after the repository server is constructed.

- For load balancer/SSL accelerator applications on a single device, communication performance cannot be improved by using non-SSL communication between the business server and authentication server. When the business system setup file is downloaded, the authentication infrastructure URL must be specified as the authentication server URL referenced by the business system. For details on system configurations that will improve communication performance, refer to "1.7.4 URL Used by the Business System to Reference the Authentication Server".

2.6 Registering a Business System

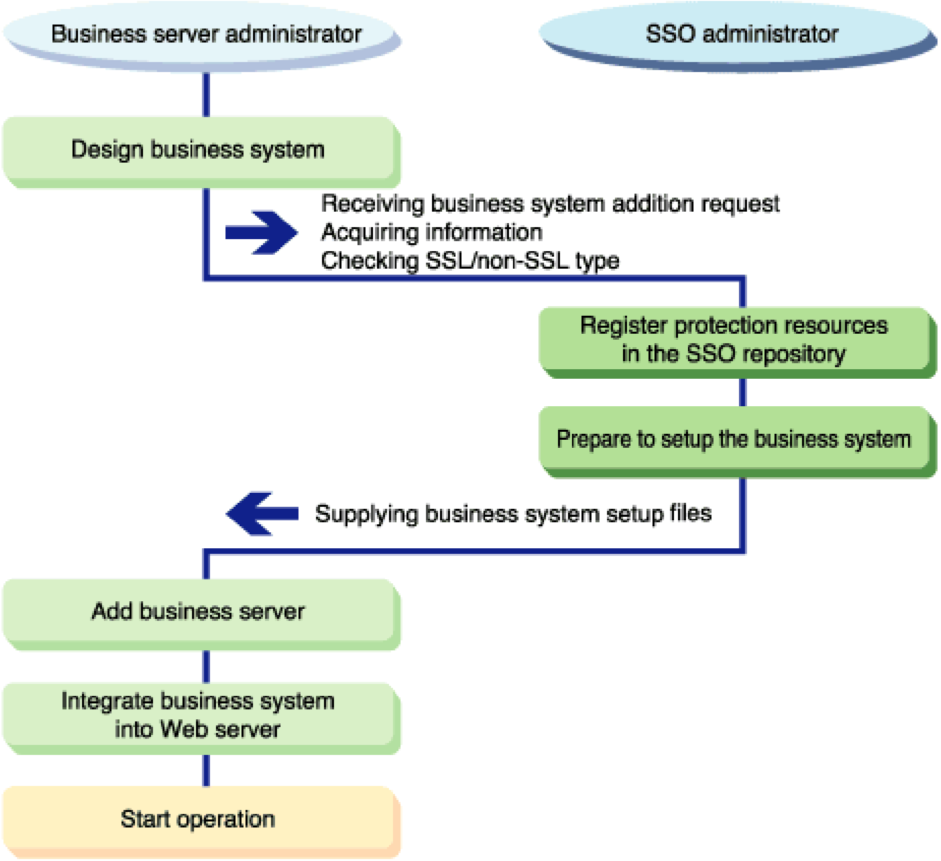
If a business server administrator requests an SSO administrator to add a business system to the Interstage Single Sign-on system, the SSO administrator registers the business system.

This section explains SSO-administrator's work for business system addition.

2.6.1 Registration Flow of Business System

If a business server administrator requests an SSO administrator to add a business system to the Interstage Single Sign-on system, the SSO administrator registers the business system. Refer to 'Environment Setup (Business Server Administrators)' for an explanation of business-server-administrator's work.

Figure 2.8 Registration Flow of Business Systems


Business server administrator
SSO administrator
Design business system
Receiving business system addition request
Acquiring information
Checking SSL/non-SSL type
Register protection resources in the SSO repository
Prepare to setup the business system
Supplying business system setup files
Add business server
Integrate business system into Web server
Start operation

2.6.2 Information to be Acquired from Business Server Administrator

When a business server administrator requests you to add a business system to the Interstage Single Sign-on system, acquire the following information from the business server administrator:

- Business system public URL
- Path configuration to be authorized
- Use of SSL communication
- Use of Interstage Portalworks linkage
- Version and edition of Interstage

When non-SSL communication is not permitted in the Single Sign-on system, request the business system administrator for SSL support.

Note

Access to protection resources on the business server is restricted by the Interstage Single Sign-on system. However, if SSL communication is not used on the business server, protection resources on the network may be electrically intercepted. SSL communication on the business server avoids such interception. Operating the business server using SSL communication is highly recommended.

2.6.3 Registering Protection Resources

The following information that was acquired from the business server administrator must be registered in the SSO repository:

- Business system public URL
- Path configuration to be authorized

2.6.3.1 Registering Site Configuration of Business System

The site configuration of the business system must be registered.

Perform the following operations on the Interstage Management Console of the machine on which the repository server (update system) was set up. Refer to the Operator's Guide for details of the items to be defined on the Interstage Management Console.

1. Select the [Security] and then [Single Sign-on] from the System menu. Click [Authentication infrastructure] and [Repository server]. Click [Protection resource] and then click the [Create a New Site configuration] tab.
2. Set [FQDN and Port number] in [Site Configuration Settings].

   When a load balancer is installed before the business server, the host name of the virtual IP address that was set in the load balancer must be set in the business system public URL. When SSL Accelerator is installed before the business server, the port number of SSL Accelerator must be set in the business system public URL.
3. Click [Create]. The added site configuration is displayed on the [Protection resource: List]. It is now possible to check the FQDN and port number of the business system.

Notes

When this system is linked with the Application Gateway and can be accessed only by clients on the Internet, multiple business systems may have the same public URL. Therefore, the new site configuration may be already registered. In this case, as the above registration procedure is unnecessary, go to 'Registering protection path', below. Refer to '2.4.1.5 Settings for Operation using Application Gateway' for details.

2.6.3.2 Registering Protection Path

Access control information must be set for Web contents to be opened on the business server. In addition to the access control information, set the access control path and access permission role. Also, in the path configuration, set the extended user information that will be notified to the web application.

Perform the following procedure on the Interstage Management Console of the machine on which the repository server (update system) was created. Refer to the Operator's Guide for details of the items to be defined on the Interstage Management Console.

1. To notify the extended user information to the Web application, take the following steps. In the [System] menu, select [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server]. In the [Settings] tab, select [Repository server detailed settings [show]] and set the [Extended user information] for the [Information notified Business System].
2. Select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] >[Protection resource]. A list of defined sites is displayed in the [Protection resource] tree. Select the site for which a protection path is to be set.
3. Click [Protection path] in the tree. A list of path configurations is displayed. Click the [Create a New Path configuration] tab.
4. In [Path], set the path that is to be access-controlled. To control the access to a directory, always write "/" at the end of the path. To control the access to a file, do not write "/" at the end of the path.
5. To set the extended user information in the path configuration, set [Notify extended user information].
6. After the path to be access-controlled is set, select the name of the role or role set that can access the path. To permit the access by all users that are registered in the SSO repository, specify nothing as the role name or role set name.
7. Click [Create] to display a list of the specified paths and role information. It is now also possible to check them.
8. Request the business server administrator to update the access control information.

Refer to 'Information Required for Authorization Using Roles' in 'Overview' for an explanation of permission by a role. Refer to 'Setting User Information Report with Environment Variables' in 'Developing Applications' for an explanation of the user attributes to be posted at authorization setting.

Note

When this system is linked with the Application Gateway and can be accessed only by clients on the Internet, multiple business systems may have the same public URL. To avoid such duplication, these business systems must be designed to have different protection paths.

If an already registered protection path was reported by the business server administrator, request the business server administrator to review the business system design to prevent the protection paths from duplicating.

Refer to 2.4.1.5 Settings for Operation using Application Gateway for details.

2.6.4 Preparations for Setting up a Business System

When the business server administrator sets up a business system, a business system setup file must be created.

The SSO administrator must prepare the business system setup file and distribute it to the business server administrator.

Downloading Business System Setup File

Download the business system setup file according to the following procedure using the Interstage Management Console of the machine on which the repository server (update system) was set up. Refer to the Operator's Guide for details of the items to be defined on the Interstage Management Console.

1. Select the [Security] and then [Single Sign-on] from the System menu. Select [Authentication infrastructure] and then click the [Business system setup file] tab.

2. Enter necessary items.

   To link the business system to Interstage Portalworks, select [Yes] in [Linkage with Interstage Portalworks?], and specify a domain name as the authentication validity range.

3. When being linked with Interstage Security Director or system configurations that will improve the communication performance by using non-SSL communication between the business server and the authentication server, the authentication server URL referenced by the business system and the authentication infrastructure URL are different from the authentication infrastructure URL. Click [Detailed Settings [Show]] and specify the URL in [Authentication server URL] of [Authentication Infrastructure Information Settings].

   For details about the URL of the Authentication server referenced by the Business system, refer to "1.7.4 URL Used by the Business System to Reference the Authentication Server"

4. Click [Download] to download the business system setup file to the machine on which the Web browser is operating.

5. Send the business system setup file to the business server administrator, and then delete the business system setup file.

The business system setup file is important for security, and is encrypted with a password. Ensure the password is protected from unauthorized access. Pass the password and downloaded information file to the business server administrator by secure means. The password must be arranged with the business server administrator in advance so that the correctness of the distributed business system setup file can be confirmed.

Notes

- In the business system with the same domain, the business system setup file that was created by specifying 'Yes' in [Linkage with Interstage Portalworks?] cannot be used together with the business system setup file that was created by specifying 'No' in [Linkage with Interstage Portalworks?].

- The business system setup file is important for security. Be sure to delete this file after it was sent to the business server administrator.

2.7 More Secure Use

Communication data and authentication information between servers are encrypted in the Interstage Single Sign-on system. The following method makes operation more secure:

- Using firewall

  A firewall controls access to data that flows between networks.

  Using a firewall, authentication servers and repository servers can be set in an independent, secure network. Since accesses using the Interstage Single Sign-on system are controlled, invalid accesses are avoided.

  To use a firewall, separately prepare a firewall product.

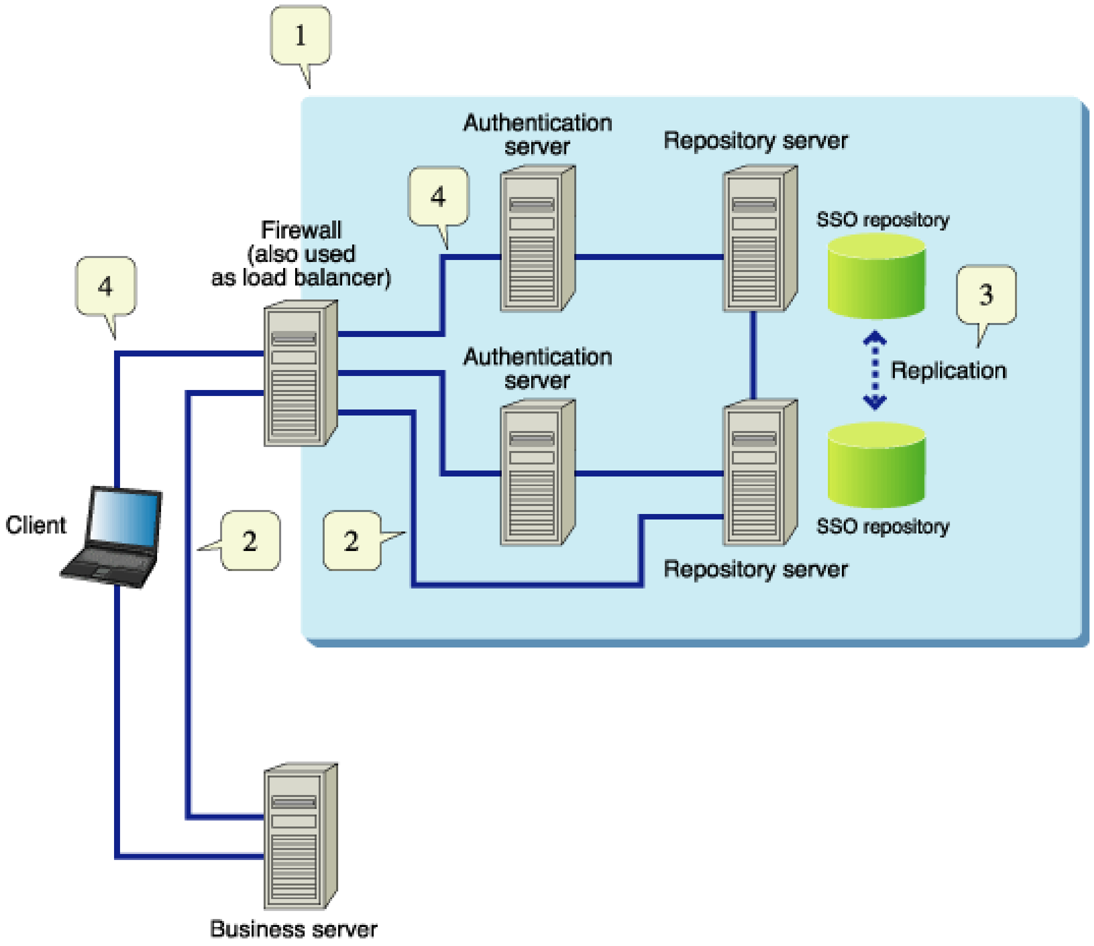
2.7.1 Using a Firewall

When a firewall is set, a group of authentication servers and repository servers must be set up in an independent network, and all accesses to the authentication serves and repository servers pass through the firewall.

Any accesses from other than business servers or clients are blocked by the filtering function of the firewall.

The following shows an example of the Interstage Single Sign-on configuration using a firewall:

Figure 2.9 Interstage Single Sign-on Using a Firewall



1. A firewall is installed so that authentication servers and repository servers make up an independent, secure network.
2. If session management is not used, the access control is set in the firewall so that accesses to repository servers through the firewall can be made only from the business server, and other accesses are blocked as invalid accesses.
3. Replication is secure because it is performed within the network protected by the firewall.
4. SSL communication is set for authentication servers to prevent electrical interception or alteration by encrypting communication from clients.

For an explanation of installing the firewall and setting filtering function, refer to the manual of the product in which the firewall is to be set up.

The following table lists an example of general filtering conditions common to the firewall products:

Table 2.15 Firewall Filtering Conditions

Service	Sender	Receiver	Processing
http (repository-server port number/tcp)	Business server	Repository server	Transmitting
https (authentication-server port number/tcp)	Client	Authentication server	Transmitting
domain-udp (port number: 53/udp)	Authentication server	DNS server	Transmitting

Chapter 3 Environment Setup (Business Server Administrators)

This chapter explains the flow of, and method for, setting up the business system environment.

Use the Interstage Management Console to set up the Interstage Single Sign-on environment. Refer to the Operator's Guide for details of starting the Interstage Management Console. Refer to the Operator's Guide for details of the items to be defined in the Interstage Management Console.

Notes

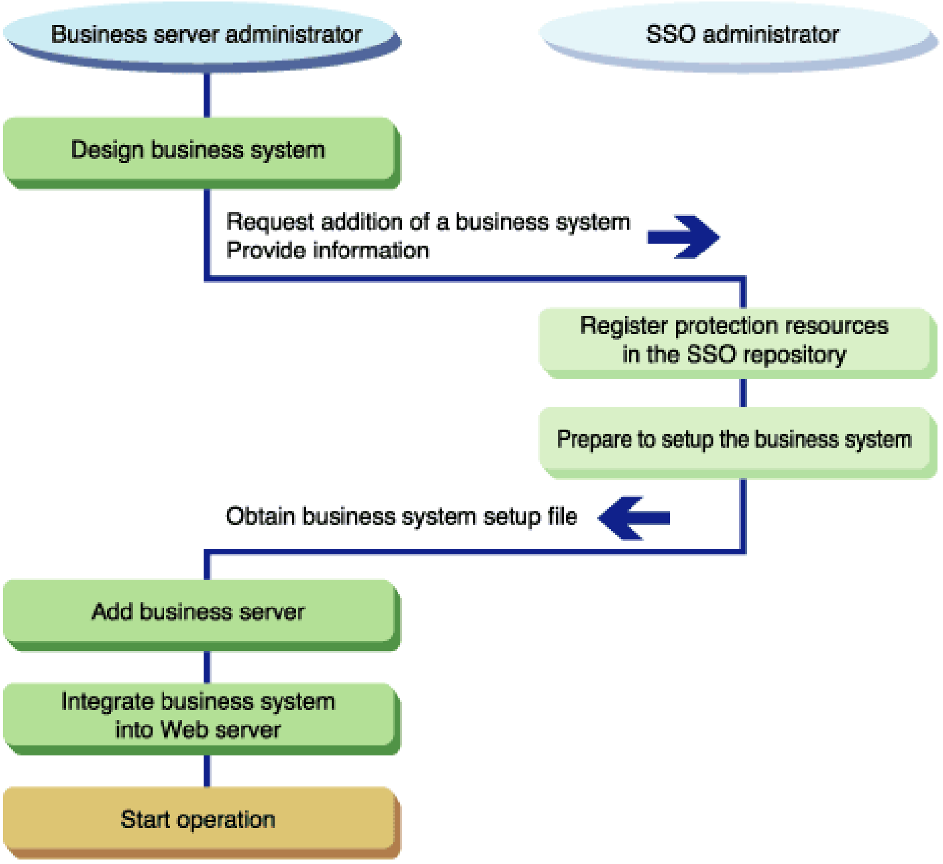
- Refer to the Security System Guide for information on how to set up and operate the system.
- Administrator's authority is required to set up the business system environment.

3.1 Environment Setup Flow

This section explains how to add a business system. Refer to "Registering a Business System" for further information.

The following figure shows the flow of environment setup as follows:

Figure 3.1 Environment Setup Flow


Business server administrator
SSO administrator
Design business system
Request addition of a business system
Provide information
Register protection resources in the SSO repository
Prepare to setup the business system
Obtain business system setup file
Add business server
Integrate business system into Web server
Start operation

Remarks

To add a business system, you need to setup the target Web system and the Web services (all services other than authentication and authorization) in advance:

- To operate the business system using SSL communication, configure the settings for SSL communication.
- Set the port number for the Web server.
- Prepare and setup Web services and Web contents.

- Configure the Web system and Web services for operation.

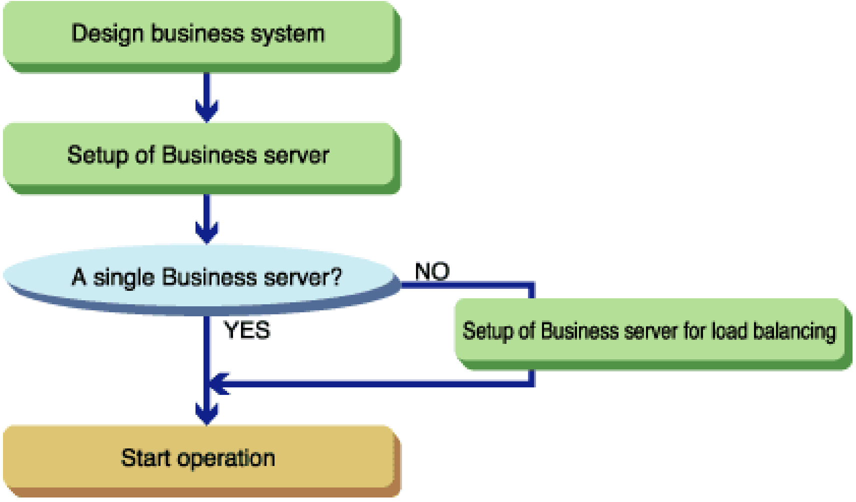
For details regarding the set up of Web system and Web service environments, refer to the Web server manual.

The configuration spread sheet (Excel file) for business systems is also provided to support the calculation of connection information between servers to be set up on the Internet Management Console during setup of the business system environment.

For details about the configuration spreadsheet for business systems, refer to "Using the Configuration Spreadsheet for Business Systems."

3.1.1 Environment Setup Flow by Case

Figure 3.2 Environment Setup Flow by Case


Design business system
Setup of Business server
A single Business server?
NO
YES
Setup of Business server for load balancing
Start operation

The stages required to set up the environment according to the operating mode is listed in the following table.

Table 3.1 Environment Setup According to Operating Mode

System configuration	Setting up a business server on a server	Setting up business servers on multiple servers	Adding a business server to the set up business system
Designing a business system	Designing a business system.	Designing a business system.	
Setting up the first business server	Setting up the first business server.	Setting up the first business server.	
	Integrating into the Web server	Integrating into the Web server	
Setting up the second and subsequent business servers		Setting up the second and subsequent business servers for load balancing.	Setting up the second and subsequent business servers for load balancing.
		Integrating into the Web server	Integrating into the Web server
Using the configuration spread sheet for business systems as required.	Using the configuration spreadsheet for the business system "SSO_Business.xls"	Using the configuration spreadsheet for the business system "SSO_Business.xls"	

3.1.2 Using the Configuration Spreadsheet for Business Systems

The configuration spreadsheet (Excel file) for business systems is provided to support the calculation of connection information between servers during setup of the business system environment when using the Internet Management Console. Access and run the file from the following storage destination, as required. For details about how to use the file, refer to [Procedure for Use] in this spreadsheet.

File Name and Storage Destination of Configuration Spreadsheet for Business Systems

File name of configuration spreadsheet for business systems

SSO_Business.xls

Storage destination of configuration spreadsheet for business systems

"ApplicationServer\tuning" folder of the Manual package

Conditions for Using the Business System Configuration Spreadsheet

The business system configuration spreadsheet supports Microsoft(R) Excel. Ensure that Microsoft(R) Excel 2003 or later is installed on your computer.

This spreadsheet uses a macro. Set the Microsoft(R) Excel security level beforehand to enable this macro. Refer to Help for Microsoft(R) Excel for details of how to set the security level.

Contact your system administrator before changing the Microsoft(R) Excel security level.

The following procedure can be used for setting and enabling the macro security level in Microsoft(R) Excel 2003:

1. From Microsoft(R) Excel 2003 select [Macros], then [Security] from the Tool menu to display the macro security setting window.
2. Select [Medium] on the [Security level] page and click OK.
3. Close Microsoft(R) Excel and restart.
4. From the menu bar, select Open from the File menu and choose the business system configuration spreadsheet.
5. The dialog box asks if you want to enable the macro. Click [Enable macro].

After using this spreadsheet, restore the security level as necessary.

3.2 Designing a Business System

This provides notes on the operations that are required, and the content that must be created in the protection resource, before constructing the business server.

3.2.1 Preparing Messages Displayed on a Web Browser

Prepare the messages that are displayed on a web browser when Interstage Single Sign-on is running.

The following messages can be changed depending on the application:

- Authorization Error Messages

To change a message, ask the SSO administrator about the messages that are displayed on a web browser.

For details about changing messages, refer to "Customizing Messages Displayed on a Web Browser" in "Single Sign-on Customization".

3.2.2 Requesting to Add a Business System

The business system administrator must clarify and report the following items to the SSO administrator when adding a business system to the Interstage Single Sign-on:

- Business system public URL
- Path configuration to be authenticated
- Whether to use SSL communication
- Whether to use Interstage Portalworks linkage
- Interstage version and edition
- Changing messages that are displayed in the web browser

If the business system does not support SSL, the SSO administrator must check whether a non-SSL connection is permitted.

Caution

Interstage Single Sign-on controls access to protect resources in the business server. However, if the business server is not operated in SSL communication mode, the protected resources may be tapped from the network. Operating the business server in SSL communication mode enables the communication contents to be encrypted and protected from tapping. It is strongly recommended to operate the business server in SSL communication mode.

Notes

- Interstage Single Sign-on disables change of the business system public URL being operated. If the public URL is to be changed, the business system must be set up again.
- To set up a business system that links with Application Gateway and can be accessed from clients only on the Internet, prevent all the first hierarchies of the URL path of the business system from being the same as those of other business systems. The root path ("/") of the business system cannot be accessed from the clients. For details, refer to "Linkage with Application Gateway."

3.2.3 Editing Web Pages for Sign-off

Edit existing Business system Web pages so that Sign-off can be performed without closing the web browser.

For details about editing web pages for Sign-off, refer to "Customizing Web pages for Sign-off" in "Single Sign-on Customization".

3.2.4 Notes on Creating the Contents

This provides notes on creating the contents in the protection resource.

3.2.4.1 Note on Using the Frame Page

This section explains the points that should be taken into account when content that uses frames and inline frames is created.

- Setting multiple content in a frame as protected resources

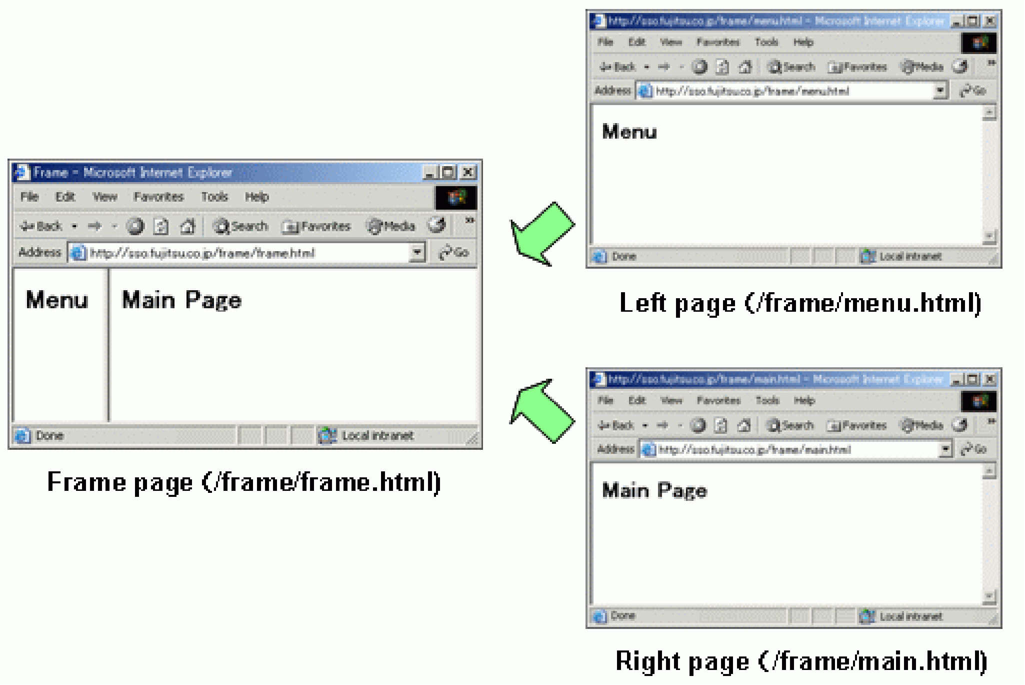
If the contents in the frame are set in the protection resource, the authentication screen may be displayed in one or more contents within the frame.

If one or more contents within the frame are set in the protection resource, set the frame page in the protection resource.

Example

To create the contents using the frame shown below and to set the entire page in the protection resource, set the frame page (/frame/frame.html) in the protection resource.

Figure 3.3 Frame page


Menu
Main Page
Frame page (/frame/frame.html)
Menu
Left page (/frame/menu.html)
Main Page
Right page (/frame/main.html)

- Using Firefox as the client web browser

  If Firefox was used as the client web browser, the content in the frame that has been set as a protected resource may sometimes be cached. In this case, that content that was cached after sign-off may sometimes be displayed.

  If Firefox is used as the client web browser, take one of the following actions:

  - Set the frame page as a protected resource.

  - In the web application that is used to create the frame page, set the values shown below in the HTTP response header to inhibit the web browser cache:

    - Cache-Control:no-cache,no-store

    - Pragma:no-cache

3.2.4.2 Notes on Using the POST Method

If the period for user authentication validity has expired or the user has not been authorized, and the POST method is used to access the protection resource, the operation differs depending on the content-type value of the HTTP request header, as shown below.

If the content-type is other than "application/x-www-form-urlencoded", take action depending on the operation. For example, customize the message displayed in the web browser by changing it to a message that asks you to gain authentication by accessing another (i.e., a different) protection resource.

Using "application/x-www-form-urlencoded" in the content-type

The Unauthenticated page is displayed (*1)

The user can continue to use the business server after authentication

.

Using other than "application/x-www-form-urlencoded" in the content-type

Depending on the status of the user authentication, the following messages are displayed in the web browser (*2)

The user can use the business server by accessing another protection resource to gain authentication.

- Access by a user who is not authenticated

  Authentication is needed. Try again after authentication.

- Access by a user whose authentication has expired

  Authentication has been expired.

*1 For details about the Unauthenticated page, refer to "Password and Certificate Authentication".

*2 For details about the message displayed in the web browser, refer to "Authorization Error Messages".

3.3 Setting up Business Servers

This section explains the procedure for setting up business servers. The Interstage Management Console is used to add business servers.

3.3.1 Setting up the First Business Server

The SSO administrator (who has completed registration of a business system), notifies the business server administrator regarding the business system setup file and its password.

The business server administrator uses the business system setup file to add a business server.

The Interstage Management Console (for the server on which the business server is to be set up) is used to take the following steps. For details about the items defined on the Interstage Management Console, refer to the Operator's Guide.

Creating the Interstage Certificate Environment

If it has not already been created, create the Interstage certificate environment required for using SSL communication with the Authentication server. For details about creating the Interstage certificate environment, refer to "Creating the Interstage certificate environment".

Setting up Business Servers

Windows32/64

1. Select [Security] > [Single Sign-on] > [Business system] and the [Addition of Business server] tab from the System menu.
2. [File Settings] is displayed. In [Business system setup file] and [Password of file], specify the Business system setup file and password provided by the SSO administrator, and then click [Next].
3. [General Settings] is displayed. Enter the required options.

   If Interstage HTTP Server is used as the Web server, select the information about the Web server containing the business server in [Web Server used] > [Web Server name] and [Host].
4. If Interstage HTTP Server is not being used, select [Others (Excluding Interstage HTTP Server)] for [Web server to use] and set [Port number].
5. To update access control information automatically when the business server is started, select [Execute when Business server is started] for [When updating Access Control Information?].
6. To use Single Sign-on JavaAPI, select [Yes] in [Use Single Sign-on JavaAPI].
7. Click the [Add] button to display a list of servers.
8. It is now possible to check the name of the added business system, port number, Web server name, and business system public URL.
9. In the following cases, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab to click [Detailed Settings [Show]]. Specify "No" for [Enable Client IP Address Check?] in [Authentication Information Settings].
   - Cluster environment
   - Using proxy server or IPCOM
   - Linked with Interstage Portalworks
   - Using the authentication server or business server valid for both IPv4 and IPv6 communication.
10. To link with Interstage Portalworks, click [Detailed settings [Show]] in [System] > [Security] > [Single sign-on] > [Business system] > [Business system name] > [Settings] tab, specify "Yes" to [Notify User Information?] in [Linkage with Web applications].
11. Click the [Update] button.

12. Delete the business system setup file.

Note

- If the arrangement of devices (such as a load balancer) and products is not configured using Interstage HTTP Server, check the following Interstage HTTP Server settings using the Interstage Management Console and configure the settings so that they are the same as the FQDN of the business system public URL.

    - If the business server is contained in the namebase virtual host:

      The host name of the server used as the virtual host

    - If the business server is not contained in the namebase virtual host:

      The server host name or IP address

- If multiple Web servers are to be used as business servers for Single Sign-on on one system, assign a different name to the access log file of each business server. If the same file name is assigned, the access log cannot be collected normally.

- If Windows(R) Internet Explorer(R) is used as a web browser, a business system setup file with an absolute path name exceeding 200 bytes in length may not be able to be specified using the Browse button. In this case, allocate the business system setup file so that the absolute path is sufficiently short.

- When a business server is started, the configurations of all business servers on the same system are checked for errors. If one of the configurations is invalid, information is output to the system log. In this case, the Web server starts, but returns the message "500 Internal Server Error" for all accesses from the user.

- The business system setup file is important for security. After the business server has been set up, ensure that the business system setup file is deleted.

- For security reasons, Interstage Single Sign-on prevents caching on the web browser. However, preventing the cache may have an impact on the operation of the web application. For details on how to set the web browser to allow caching, refer to "Prevention of Caching of Contents".

Solaris32/64

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

2. [File Settings] is displayed. In [Business system setup file] and [Password of file], specify the Business system setup file and password provided by the SSO administrator, and then click [Next].

3. [General Settings] is displayed. Enter the required options.

   If Interstage HTTP Server is used as the Web server, select the information about the Web server containing the business server in [Web Server used] > [Web Server name] and [Host].

4. If Interstage HTTP Server is not being used, select [Others (Excluding Interstage HTTP Server)] for [Web server to use] and set [Port number].

   If [Others (Excluding Interstage HTTP Server)] has been selected, set the effective user name of the Web server. For details about the effective user name, refer to "To change the effective user name of the Web server for the business server."

5. To update access control information automatically when the business server is started, select [Execute when Business server is started] for [When updating Access Control Information?].

6. To use Single Sign-on JavaAPI, select [Yes] in [Use Single Sign-on JavaAPI].

7. Click the [Add] button.

8. A list of servers is displayed. It is now possible to check the name of the added business system, port number, Web server name, and business system public URL.

9. In the following cases,, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab to click [Detailed Settings [Show]]. Set [Enable Client IP Address Check?] in [Authentication Information Settings] to "No".

    - Cluster environment

    - Using proxy server or IPCOM

    - Linked with Interstage Portalworks

    - Using the authentication server or business server valid for both IPv4 and IPv6 communication.

10. To link with Interstage Portalworks, click [Detailed settings [Show]] in [System] > [Security] > [Single sign-on] > [Business system] > [Business system name] > [Settings] tab, specify "Yes" to [Notify User Information?] in [Linkage with Web applications].

11. Click the [Update] button.

12. Delete the business system setup file.

13. If there are other business servers built on the machine, then restart them.

Note

- If the arrangement of devices (such as a load balancer) and products is not configured using Interstage HTTP Server, check the following Interstage HTTP Server settings using the Interstage Management Console and configure the settings so that they are the same as the FQDN of the business system public URL.

    - If the business server is contained in the namebase virtual host:

      The host name of the server used as the virtual host

    - If the business server is not contained in the namebase virtual host:

      The server host name or IP address

- If multiple Web servers are to be used as business servers for Single Sign-on on one system, assign a different name to the access log file of each business server. If the same file name is assigned, the access log cannot be collected normally.

- If Windows(R) Internet Explorer(R) is used as a web browser, a business system setup file with an absolute path name exceeding 200 bytes in length, may not be able to be specified using the Browse button. In this case, allocate the business system setup file so that the absolute path is sufficiently short.

- When a business server is started, the configurations of all business servers on the same system are checked for errors. If one of the configurations is invalid, information is output to the system log. In this case, the Web server starts, but returns the message "500 Internal Server Error" for all accesses from the user.

- The business system setup file is important for security. After the business server has been set up, ensure that the business system setup file is deleted.

- For security reasons, Interstage Single Sign-on prevents caching on the web browser. However, preventing the cache may have an impact on the operation of the web application. For details on how to set the web browser to allow caching, refer to "Prevention of Caching of Contents".

Linux32/64

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

2. [File Settings] is displayed. In [Business system setup file] and [Password of file], specify the Business system setup file and password provided by the SSO administrator, and then click [Next].

3. [General Settings] is displayed. Enter the required options.

   Select the information about the Web server containing the business server in [Web Server used] > [Web Server name] and [Host].

4. To update access control information automatically when the business server is started, select [Execute when Business server is started] for [When updating Access Control Information?].

5. To use Single Sign-on JavaAPI, select [Yes] in [Use Single Sign-on JavaAPI].

6. Click the [Add] button.

7. A list of servers is displayed. It is now possible to check the name of the added business system, port number, Web server name, and business system public URL.

8. In the following cases,, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab to click [Detailed Settings [Show]]. Specify "No" for [Enable Client IP Address Check?] in [Authentication Information Settings].

    - Cluster environment

    - Using proxy server or IPCOM

    - Linked with Interstage Portalworks

    - Using the authentication server or business server valid for both IPv4 and IPv6 communication

9. To link with Interstage Portalworks, click [Detailed settings [Show]] in [System] > [Security] > [Single sign-on] > [Business system] > [Business system name] > [Environment settings] tab, specify "Yes" for [Notify User Information?] in [Linkage with Web applications].

10. Click the [Update] button.

11. Delete the business system setup file.

12. If there are other business servers built on the machine, then restart them.

Note

- If the arrangement of devices (such as load balancer) and products is not configured using Interstage HTTP Server, check the following Interstage HTTP Server settings using the Interstage Management Console and configure the settings so that they are the same as the FQDN of the business system public URL.

    - If the business server is contained in the namebase virtual host:

    - The host name of the server used as the virtual host

    - If the business server is not contained in the namebase virtual host:

    - The server host name or IP address

- If Windows(R) Internet Explorer(R) is used as a web browser, a business system setup file with an absolute path name that exceeds 200 bytes in length, may not be able to be specified by using the Browse button. In this case, allocate the business system setup file so that the absolute path is sufficiently short.

- When a business server is started, the configurations of all business servers on the same system are checked for errors. If one of the configurations is invalid, information is output to the system log. In this case the Web server starts, but returns the message "500 Internal Server Error" for all accesses from the user.

- The business system setup file is important for security. After the business server has been set up, ensure that the business system setup file is deleted.

- For security reasons, Interstage Single Sign-on prevents caching on the web browser. However, preventing the cache may have an impact on the operation of the web application. For details on how to set the web browser to allow caching, refer to "Prevention of Caching of Contents". "

Web Servers that Incorporate a Business Server

Note the following points about Web servers that incorporate a business server.

Windows32/64

- Multiple types of Web servers can be used as the business servers for Single Sign-on in one system.

    - The following Web servers can be operated concurrently as business servers:

        - Interstage HTTP Server

        - Microsoft(R) Internet Information Service

- If Microsoft(R) Internet Information Services are to be used, operation using multiple sites is not supported.

  Set up a business server for Single Sign-on for only one site. If it is set up for multiple sites, access is controlled for only the first site accessed after the Web server is started.

  If an SSL port is used in Microsoft(R) Internet Information Services, the TCP port (a non-SSL port) is also opened, and multiple sites are used. In this case, take either of the following actions:

    - Deploy the SSL Accelerator before the business server without using a Microsoft(R) Internet Information Services SSL port.

    - Set up a firewall before the business server so that the Microsoft(R) Internet Information Services TCP port cannot be accessed.

Solaris32

- Multiple types of Web servers can be used as business servers for Single Sign-on in one system. To use multiple types of Web servers, be sure to make the effective user name of the Web servers the same. For details about the effective user name of the Web server, refer to "Changing the Effective User for the Web Server" in the "Operation and Maintenance" chapter
  - Interstage HTTP Server and Sun Java System Web Server can be operated concurrently as business servers.
- If Sun Java System Web Server is to be used, operation using the virtual server is not supported.

  If access control for Single Sign-on is set up for the virtual server, it is not access controlled normally.

3.3.2 Setting up the Second and Subsequent Business Servers for Load Balancing

This section explains how to add business servers for load balancing.

If a load balancer is used to distribute business server load, the second and subsequent servers must be configured with the same environment as the first server.

In the procedure described below, the business server environment is exported from the export machine on which the business server has already been set up (using the ssobackup command). It is then imported to the import machine on which the business server has been added (using the ssorestore command). For details about the ssobackup, and ssorestore command, refer to "Backup Commands" in the Reference Manual (Command Edition).

The ssobackup command is also used for exporting messages to be displayed in a web browser. Customize these messages before exporting the business server. For details about how to customize messages for display in a web browser, refer to "Customizing Messages Displayed on a Web Browser".

Preparation Before Load Balancing

When adding a new load balancer to an existing business system:

- Set the host name of the installed business server in the load balancer so that the business system public URL is not changed. For details about the business system public URL, refer to "Business System Public URL".

Preparation of the Import Machine

1. Prepare a machine with the same disk configuration as the machine used for export.
2. If the business system setup file notified from the SSO administrator is invalid, all business servers to be added for load balancing are re-created. Therefore, before fetching environment information on the business server, confirm that the access from the client is correctly authenticated and authorized in the export machine.

Downloading the Resources of the Export Machine

1. Execute the ssobackup command using the -az option on the export machine to extract the business server resources to the resource storage file. (*1)
2. Export the Interstage certificate environment resources. (*1)
3. Export the resources of the Web server used in the business system. (*2)
4. When developing Java applications, export the IJServer resources. (*1)
5. Transfer the resources fetched in step 1 to 3 to the import machine.

   Transfer the resources carefully so that unauthorized parties cannot access it. During transfer, do not change the permission of the resource storage file fetched in step 1.

Setting up the Environment on the Import Machine

1. Import the Interstage certificate environment fetched from the export machine. (*1)
2. Import the Web server resources so that the Web system, and Web service environments on the export machine are the same.(*2)
3. Execute the ssorestore command on the import machine to import the business server resources. (*1)
4. When developing Java applications, import the IJServer resources that were fetched from the export machine. (*1)

5. Delete the resource storage file fetched from the export machine.

*1 For details about exporting and importing resources, refer to "Maintenance (Resource Backup)" - "Moving Resources to Another Server" in the "Operator's Guide".

*2 When using Interstage HTTP Server as the Web server, refer to "Maintenance (Resource Backup)" - "Moving Resources to Another Server" in the "Operator's Guide", and then export/import the resources.

Notes

- If business server load is to be distributed, the version, edition, and install directory of Interstage Single Sign-on for multiple business servers must be the same.
- The load balancer must be set up so that the requests from a particular client transfer to the relevant authentication servers.
- Configure the following settings when the load balancer is IPCOM
  - Operation Mode: bridge
  - Measure of load Balancing and uniqueness of connection: Balancing for each node
- The resource storage file fetched from the business server is important for security. After the business server is set up, be sure to delete the environment information file.

3.4 Integrating into the Web Server

Business server is integrated into a Web server.

Use the procedure of your Web server to install a business server and restart the Web server. For details about how to start a Web server, refer to "Starting a Business Server."

Windows32/64 Solaris32/64

To use multiple Web servers on one server, integrate a business server in all Web servers to be used as the business system for Single Sign-on.

3.4.1 Integrating into Interstage HTTP Server

If Interstage HTTP Server is used, the Interstage Single Sign-on module is automatically integrated into Interstage HTTP Server.

However the Interstage Single Sign-on module is only automatically integrated into Interstage HTTP Server when the port number specified in the Business system public URL and the port number used by Interstage HTTP Server, match.

3.4.2 Integrating into Sun Java System Web Server 6.1

To use Sun Java System Web Server 6.1 edit the environment configuration file for Sun Java System Web Server.

The following sections show the items that need to be added to the environment configuration file if Sun Java System Web Server is required for operation as a business server.

For details on the environment configuration file for Sun Java System Web Server, refer to the Sun Java System Web Server manual.

Environment Configuration File Name and Storage Destination

Environment configuration file name

magnus.conf

obj.conf

Storage destination of environment configuration file

<Sun Java System Web Server installation path>/https-INSTANCE_NAME/config (*1)

*1 https-INSTANCE_NAME is the name of the server set up by the user. For example, it becomes https-www.fujitsu.com if the server name is https-www.fujitsu.com

Additional Options for magnus.conf

(1) Adding the "Init" directive

Table 3.2 Adding Interstage Single Sign-on library read-only settings

Parameter	Settings
fn	"load-modules"
shlib	"/opt/FJSVssoaz/lib/ssoatzipl.so"
funcs	"GetFilterVersion,HttpFilterProc,sso_error,sso_postproc"

Table 3.3 Configuring Interstage Single Sign-on initialization function settings

Parameter	Settings
fn	"GetFilterVersion"
EarlyInit	yes

Example of How to Edit the magnus.conf File

The following example shows how to edit the magnus.conf file:

Example

```
Init fn="load-modules" shlib=" " funcs="GetFilterVersion,HttpFilterProc,sso_error,sso_postproc "
Init fn="GetFilterVersion" EarlyInit=yes(*1)
```

*1 Describe the "Init" directive on the first line of the magnus.conf file.

Additional Options for obj.conf

(1) Adding the Default object (<Object name=default>) to the Directive

Table 3.4 Adding the "NameTrans" Directive

Parameter	Settings
fn	"HttpFilterProc"

Table 3.5 Adding the "Error" Directive

Parameter	Settings
fn	"sso_error"

Example

```
<Object name=default>
NameTrans fn="HttpFilterProc"
Error fn="sso_error"
...
</Object>
```

(2) Adding an Interstage Single Sign-on object (<Object ppath="/fj-is-sso">)

Table 3.6 Adding the "Object" Tag

Parameter	Settings
ppath	"/fj-is-sso"

Table 3.7 Adding the "Service" Directive

Parameter	Settings
fn	"sso_postproc"

Example

```
<Object ppath="/fj-is-sso">
Service fn="sso_postproc"
</Object>
```

Example of How to Edit the obj.conf File

The following example shows how to edit the obj.conf file.

Example

```
<Object name=default>
NameTrans fn="HttpFilterProc"(*1)
Error fn="sso_error"
...
</Object>

<Object ppath="/fj-is-sso">
Service fn="sso_postproc"
</Object>
```

*1 Describe the "NameTrans" directive at the start of <Object name=default>, and the "Error" directive immediately after the "NameTrans" directive.

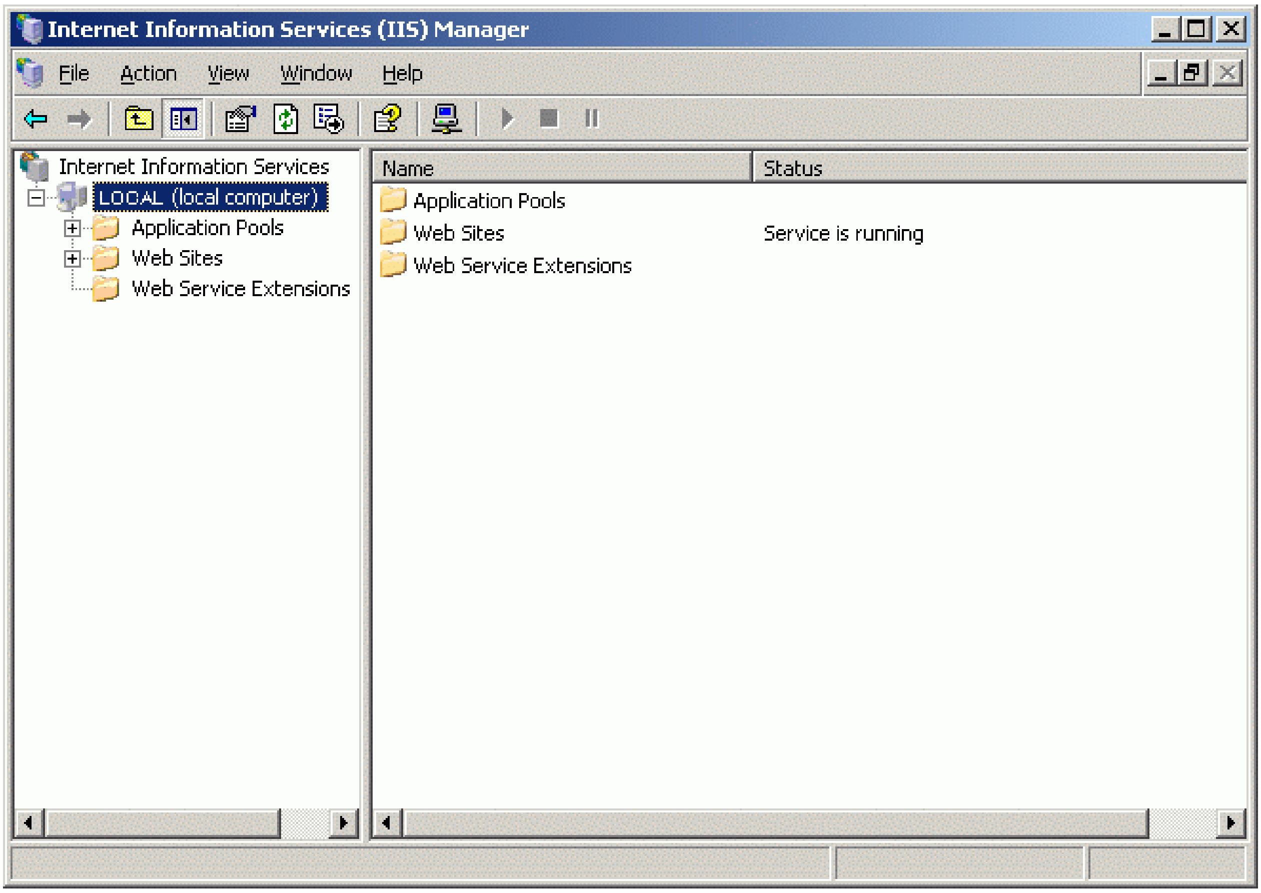
3.4.3 Integrating with Microsoft(R) Internet Information Services 6.0

This section explains the procedure to integrate a business server into Microsoft(R) Internet Information Services (IIS). In this example Microsoft(R) Windows Server(R) 2003 is used to explain the procedure for integration of a business server into the Web site used under Microsoft(R) Internet Information Services 6.0.

If Microsoft(R) Internet Information Services 6.0 is used, , the system must be restarted after it has been installed. If the system is not restarted, business server programs may not be readable.

1. From Windows, click [Start] > [Programs] > [Administrative Tools] > [Internet Information Services (IIS) Manager].

Figure 3.4 Internet Information Services (IIS) Manager

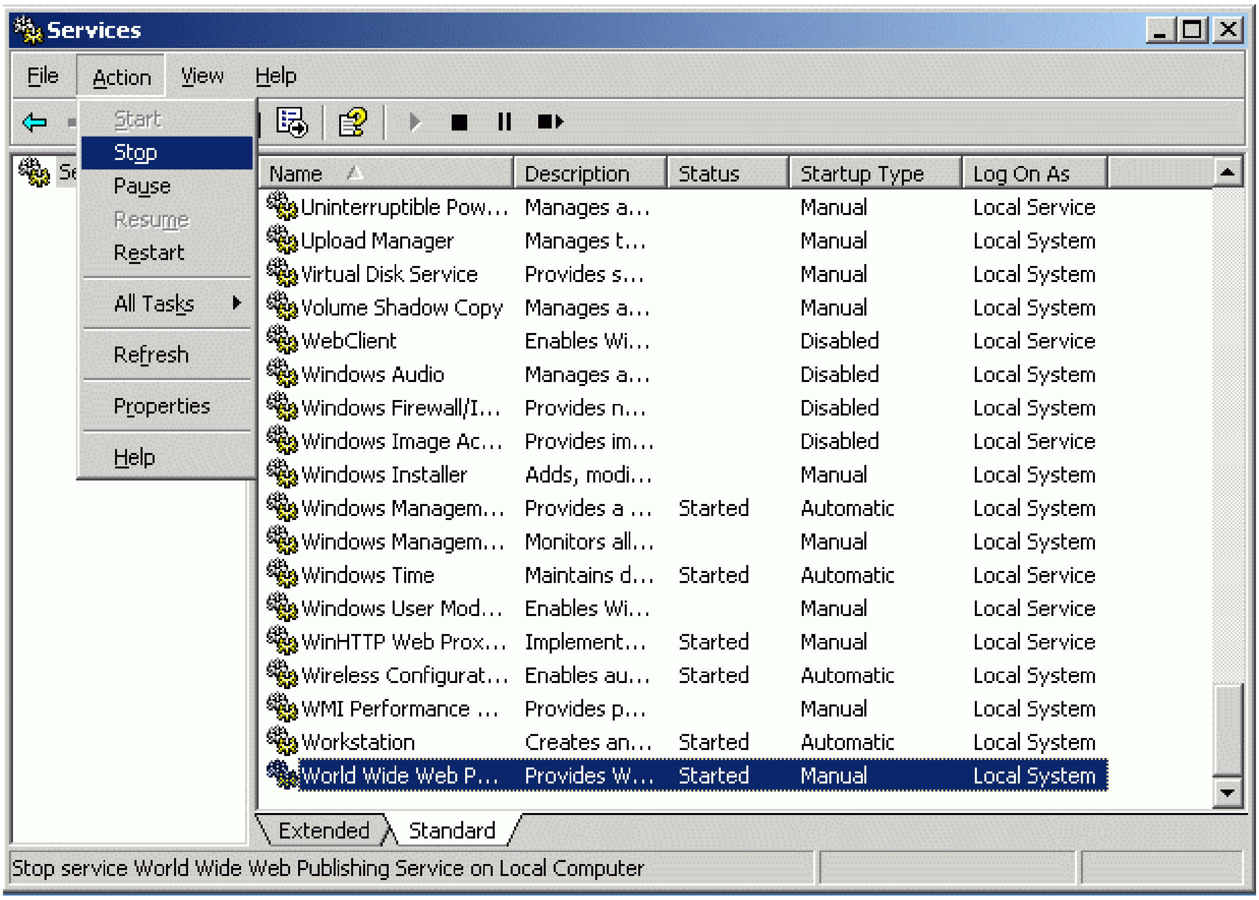


Name	Status
Application Pools	
Web Sites	Service is running
Web Service Extensions	

If Microsoft(R) Internet Information Services is running, stop it.

To stop Microsoft(R) Internet Information Services, from Windows, click [Start] > [Programs] > [Administrative Tools] > [Services], and then click [World Wide Web Publishing Service]. In the Action menu, click [Stop].

Figure 3.5 Stop Microsoft(R) Internet Information Services



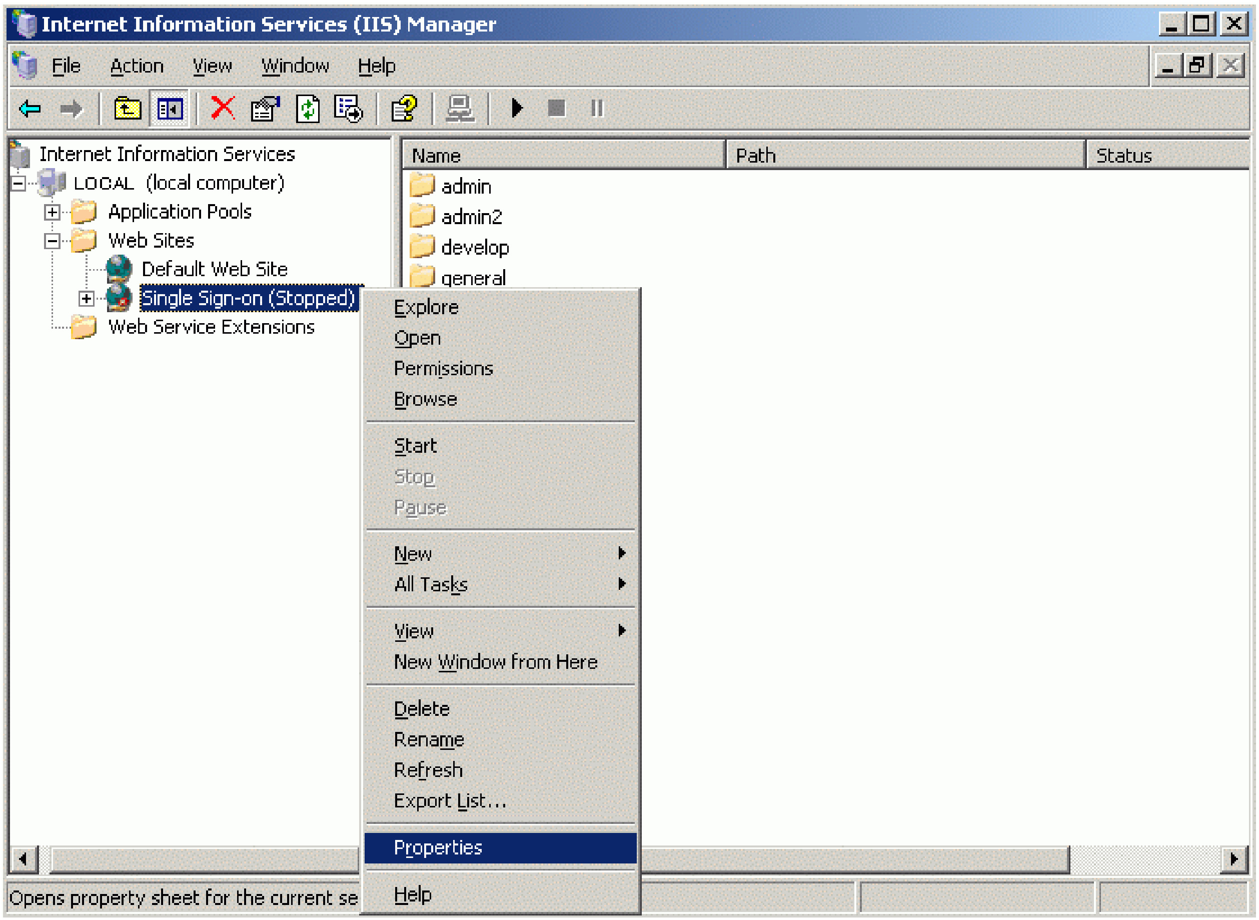
Name	Description	Status	Startup Type	Log On As
Uninterruptible Pow...	Manages a...		Manual	Local Service
Upload Manager	Manages t...		Manual	Local System
Virtual Disk Service	Provides s...		Manual	Local System
Volume Shadow Copy	Manages a...		Manual	Local System
WebClient	Enables Wi...		Disabled	Local Service
Windows Audio	Manages a...		Disabled	Local System
Windows Firewall/I...	Provides n...		Disabled	Local System
Windows Image Ac...	Provides im...		Disabled	Local Service
Windows Installer	Adds, modi...		Manual	Local System
Windows Managem...	Provides a ...	Started	Automatic	Local System
Windows Managem...	Monitors all...		Manual	Local System
Windows Time	Maintains d...	Started	Automatic	Local Service
Windows User Mod...	Enables Wi...		Manual	Local Service
WinHTTP Web Prox...	Implement...	Started	Manual	Local Service
Wireless Configurat...	Enables au...	Started	Automatic	Local System
WMI Performance ...	Provides p...		Manual	Local System
Workstation	Creates an...	Started	Automatic	Local System
World Wide Web P...	Provides W...	Started	Manual	Local System

Stop service World Wide Web Publishing Service on Local Computer

2. Select the Web site into which the business server is to be integrated.

In the following example a business server is integrated into a Web site called 'Single Sign-on'.

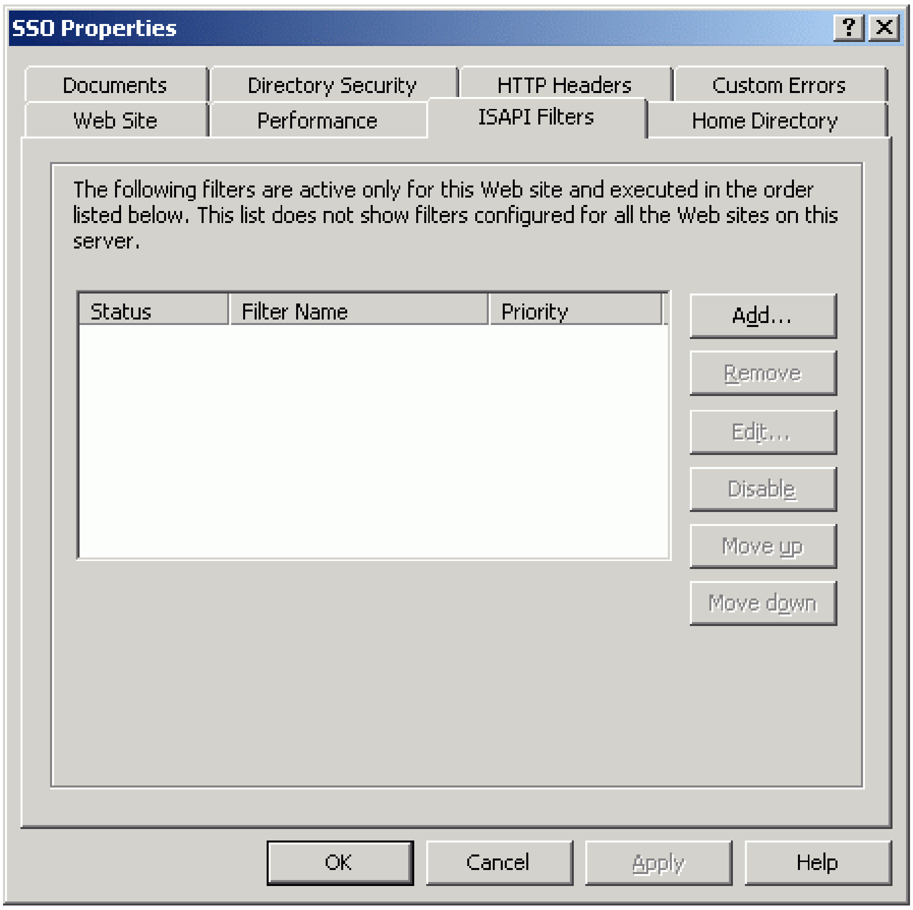
Figure 3.6 Select a Web Site for Integration



3. Right-click, and then click Properties to open the Properties dialog. Click the [ISAPI Filters] tab, and then click the Add button.

   Note that, if the ISAPI filter has already been set, after adding the business server program to the ISAPI filter in step 5, you must change the order so that the business server program is displayed at the top.

Figure 3.7 Select Properties



The following filters are active only for this Web site and executed in the order listed below. This list does not show filters configured for all the Web sites on this server.

Notes

If the business server program added cannot be selected (is grayed out) immediately after step 5, then you must change the order so that the business server program is displayed at the top.

4.1. Perform the tasks up until step 21.

4.2. Access a path other than the protection path for Microsoft(R) Internet Information Services that has started.

By performing the above tasks, it will be possible to select the business server program added in step 5.

4.3. Stop Microsoft(R) Internet Information Services.

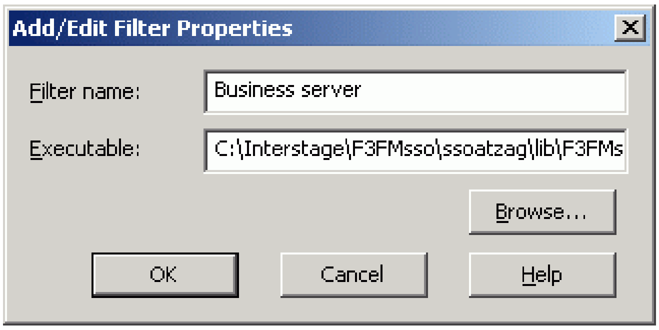
4.4. Change the order so that the business server program that was added to the ISAPI filter is displayed at the top.

4.5. Start Microsoft(R) Internet Information Services.

4. Enter a filter name, and in Executable, specify the business server program giving the absolute path for the executable file. Then click [OK].

   In the following example, "Business server" is specified for the Filter name and "C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll" for the Executable file.

   Figure 3.8 Specify Business Server

   Add/Edit Filter Properties

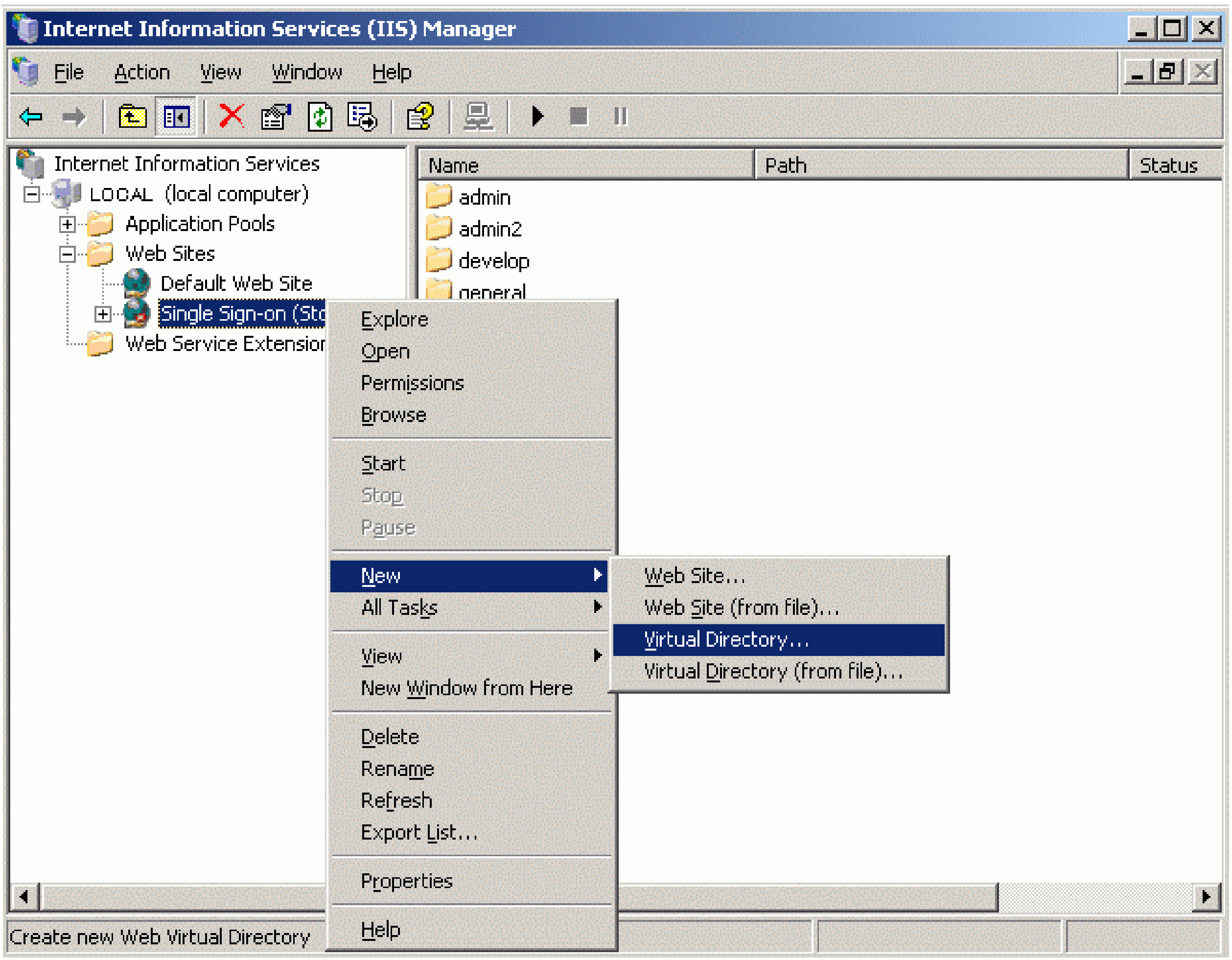
   Filter name: Business server

   Executable: C:\Interstage\F3FMsso\ssoatzag\lib\F3FMs

5. Select the website for integrating the business server.

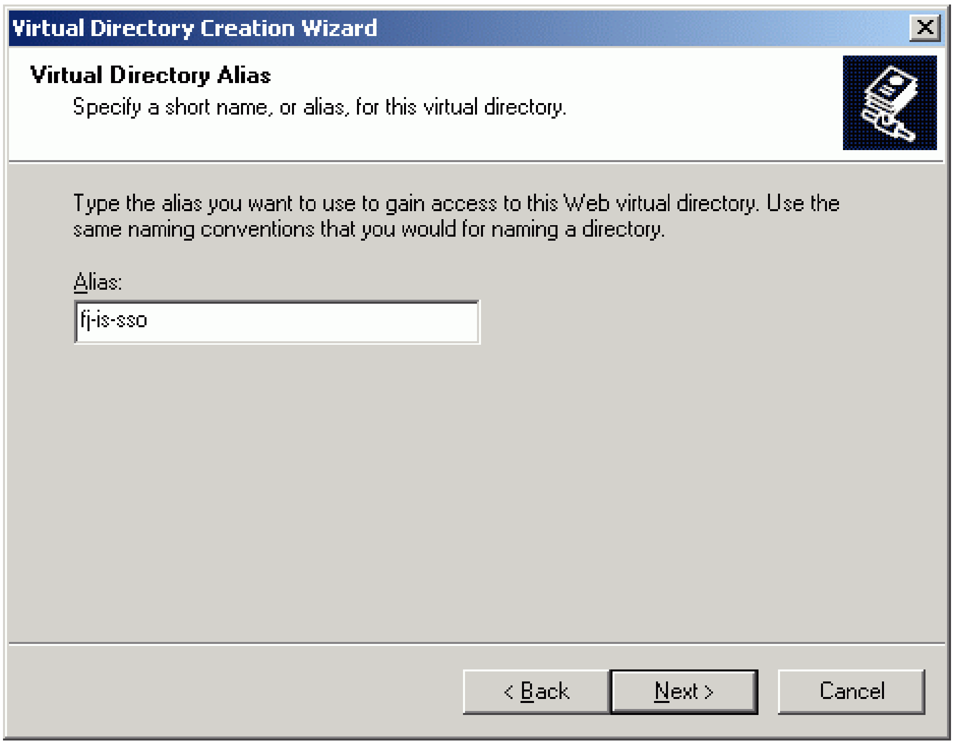
   Select [New] > [Virtual Directory], and open the Virtual Directory Creation Wizard window.

   Figure 3.9 Open the Virtual Directory Creation Wizard window

6. Set "fj-is-sso" as the virtual directory alias.

Figure 3.10 Set the Virtual Directory Alias



Virtual Directory Creation Wizard

Virtual Directory Alias

Specify a short name, or alias, for this virtual directory.

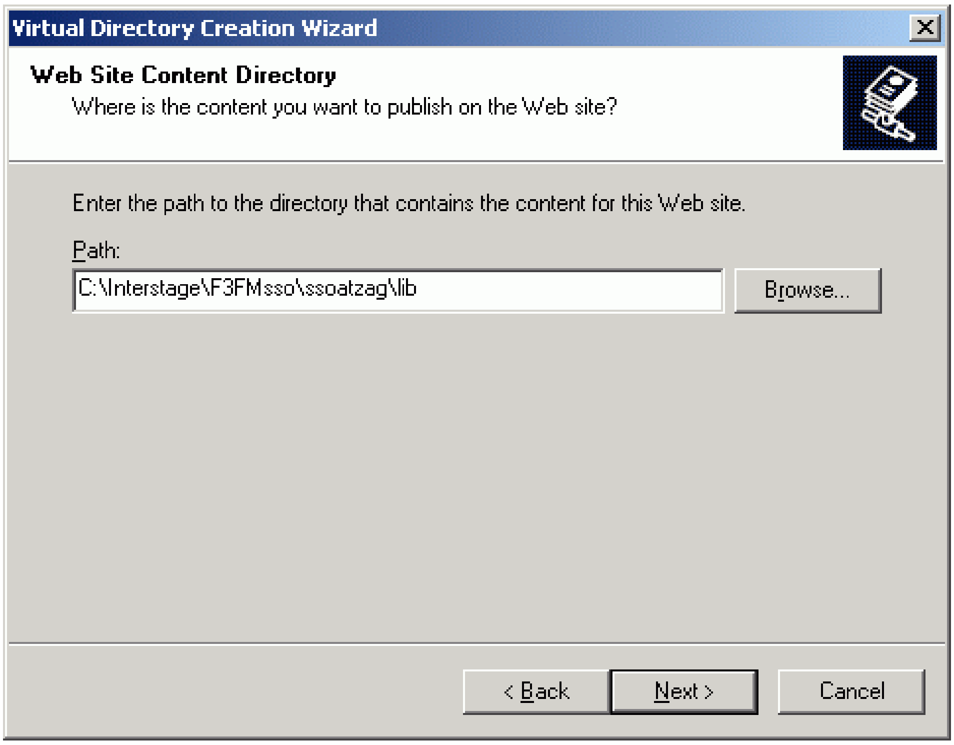
Type the alias you want to use to gain access to this Web virtual directory. Use the same naming conventions that you would for naming a directory.

Alias:
fj-is-sso

7. Specify the business server program storage directory as the web Site contents directory.

In the following example, "C:\Interstage\F3FMsso\ssoatzag\lib" is set as the path.

Figure 3.11 Set the Web Site Contents Directory



Virtual Directory Creation Wizard

Web Site Content Directory

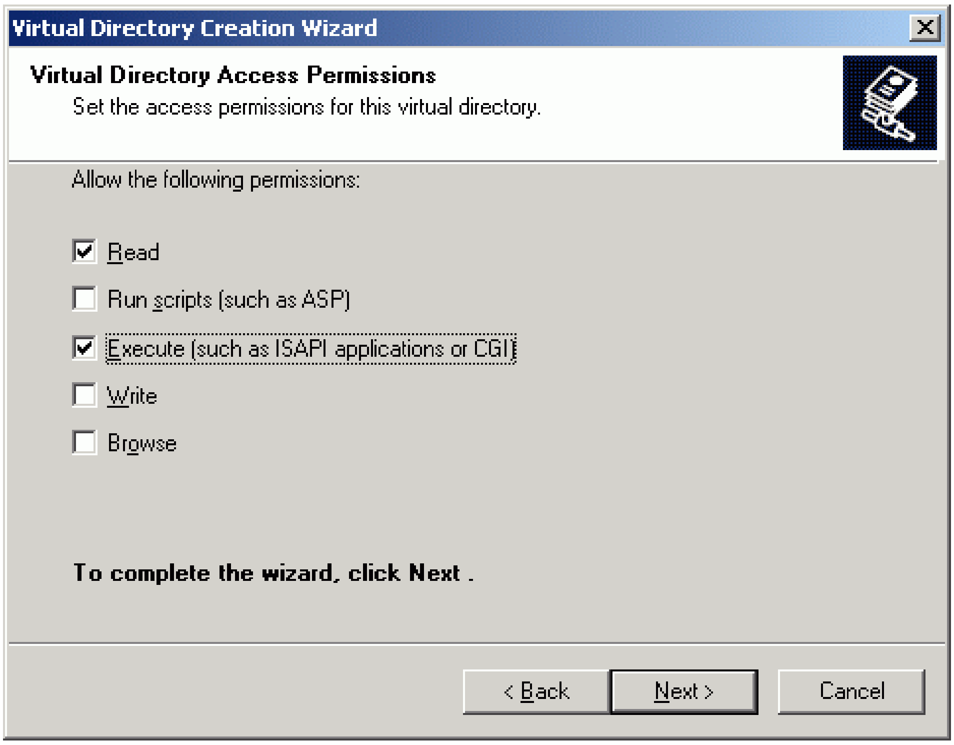
Where is the content you want to publish on the Web site?

Enter the path to the directory that contains the content for this Web site.

Path:
C:\Interstage\F3FMsso\ssoatzag\lib

8. Set read-only as the access permission for the virtual directory, and execution permission for ISAPI applications.

Figure 3.12 Set Access Permissions



Virtual Directory Creation Wizard

Virtual Directory Access Permissions

Set the access permissions for this virtual directory.

Allow the following permissions:

☑ Read

☐ Run scripts (such as ASP)

☑ Execute (such as ISAPI applications or CGI)

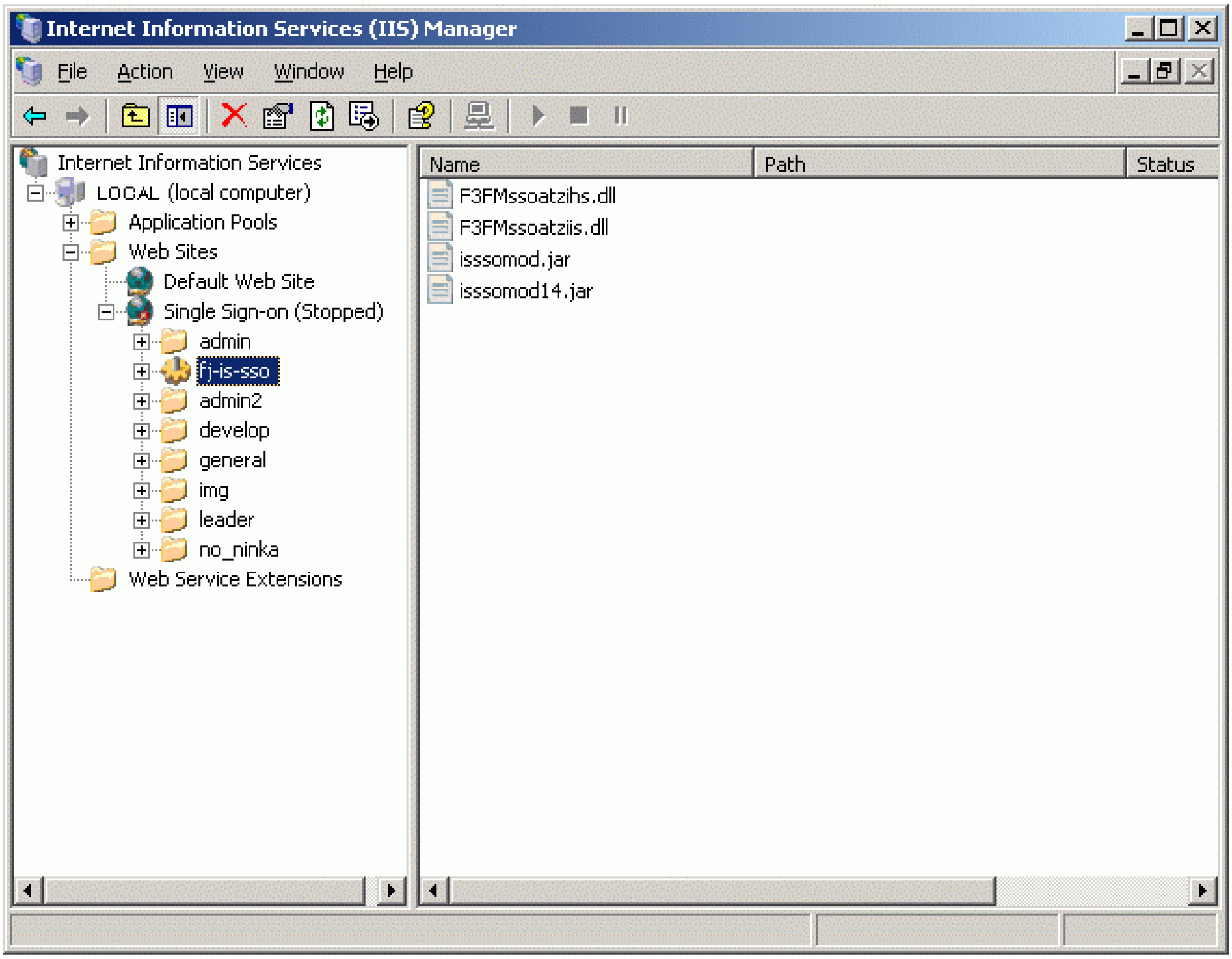
☐ Write

☐ Browse

To complete the wizard, click Next .

Close the Virtual Directory Creation Wizard window.

Figure 3.13 Return to the Internet Information Services Manager

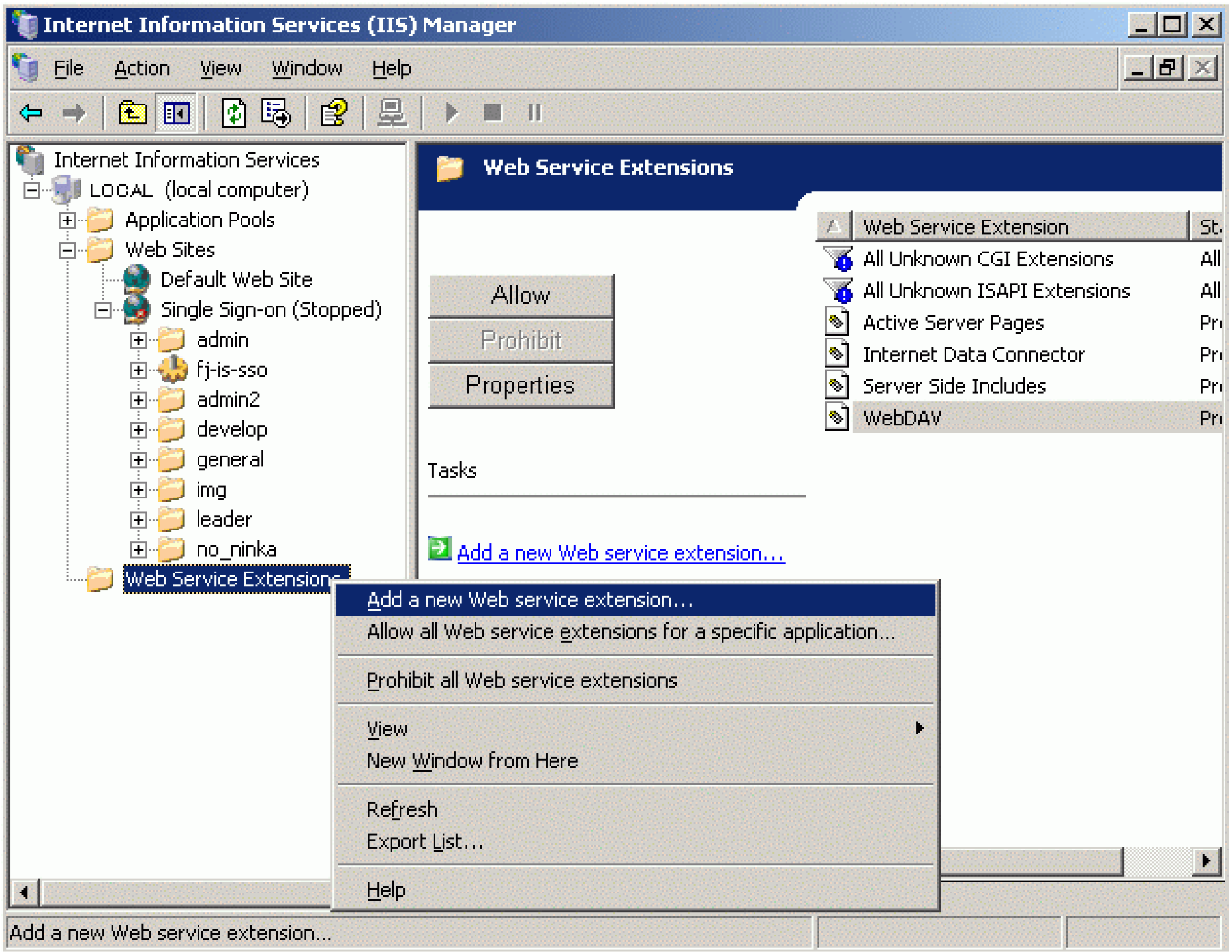


Name	Path	Status
F3FMssoatzihs.dll		
F3FMssoatziis.dll		
isssomod.jar		
isssomod14.jar		

9. Add the business server file to the Web service extension.

   Select the Web service extension, and then select [Add Web service extension].

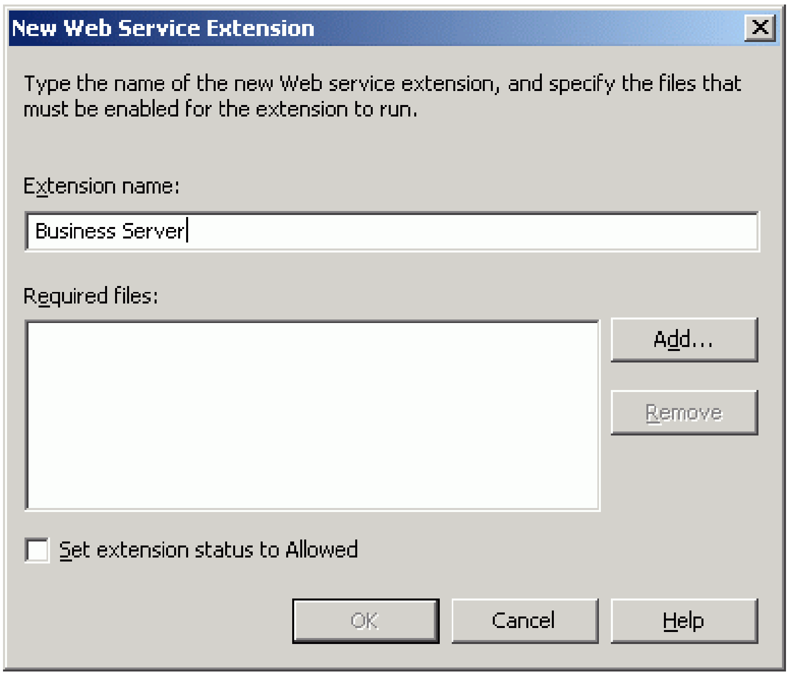
Figure 3.14 Add the Web Service Extension



10. Set the extension name.

In the example below, the extension name is "Business Server".

Figure 3.15 Set the Extension Name



New Web Service Extension

Type the name of the new Web service extension, and specify the files that must be enabled for the extension to run.

Extension name:

Business Server

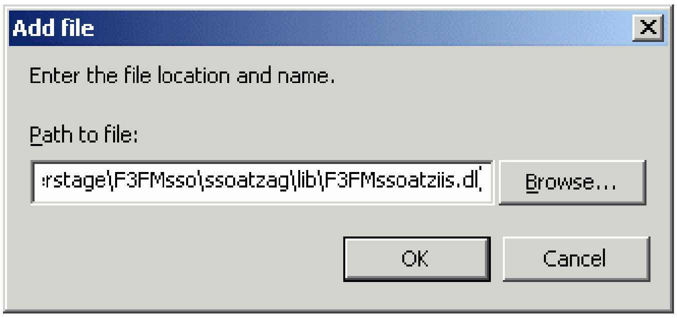
Required files:

11. In the [Add File] window that is opened by clicking [Add], set the absolute path for the business server program.

In the following example, "C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll" is set as the path.

After the settings are complete, click [OK].

Figure 3.16 Enter the Location of the Business Server Program File



Add file

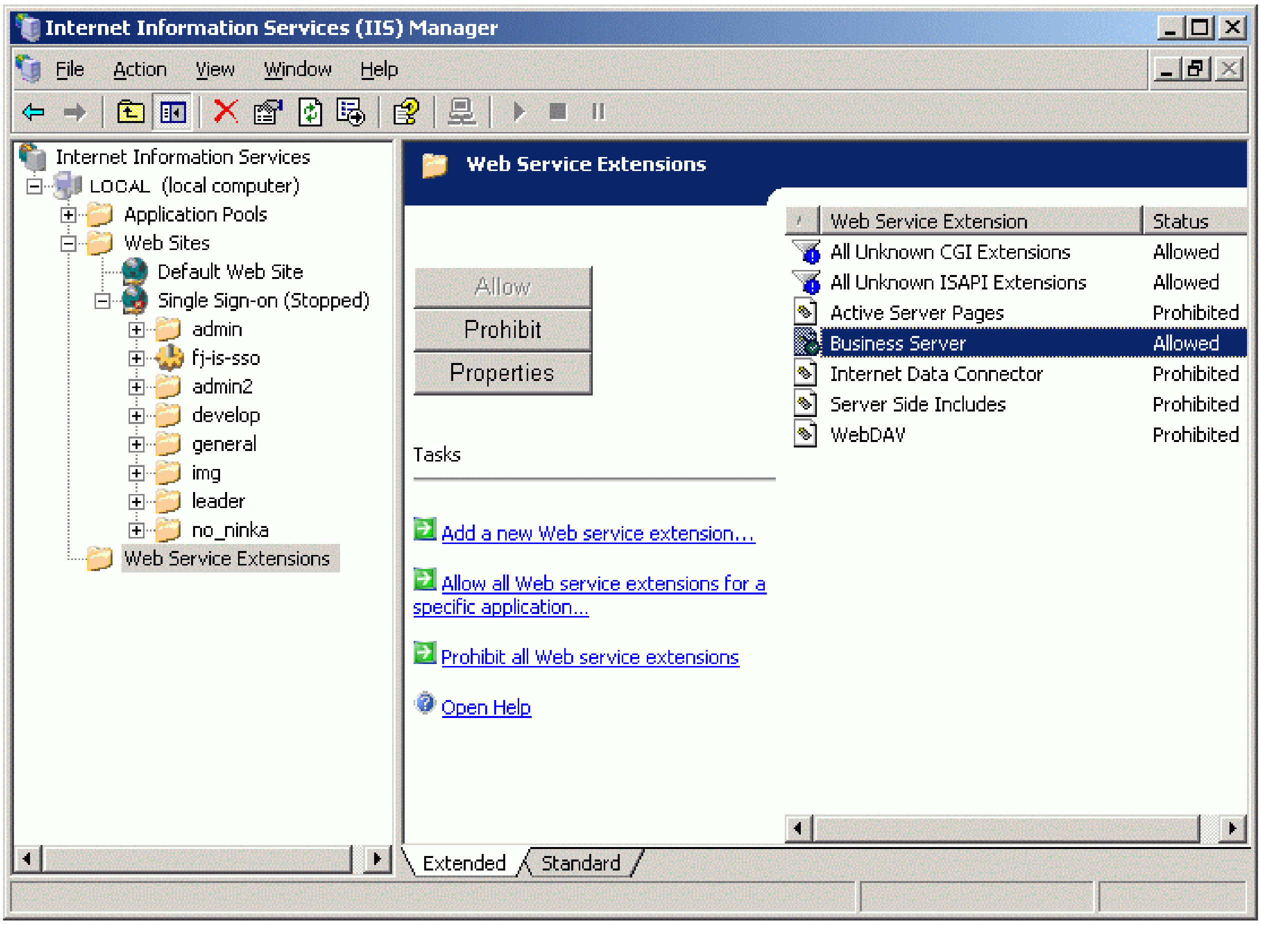
Enter the file location and name.

Path to file:

rstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll

12. Set the permissions for the Web service extension.

Figure 3.17 Set Web Service Extension Permissions

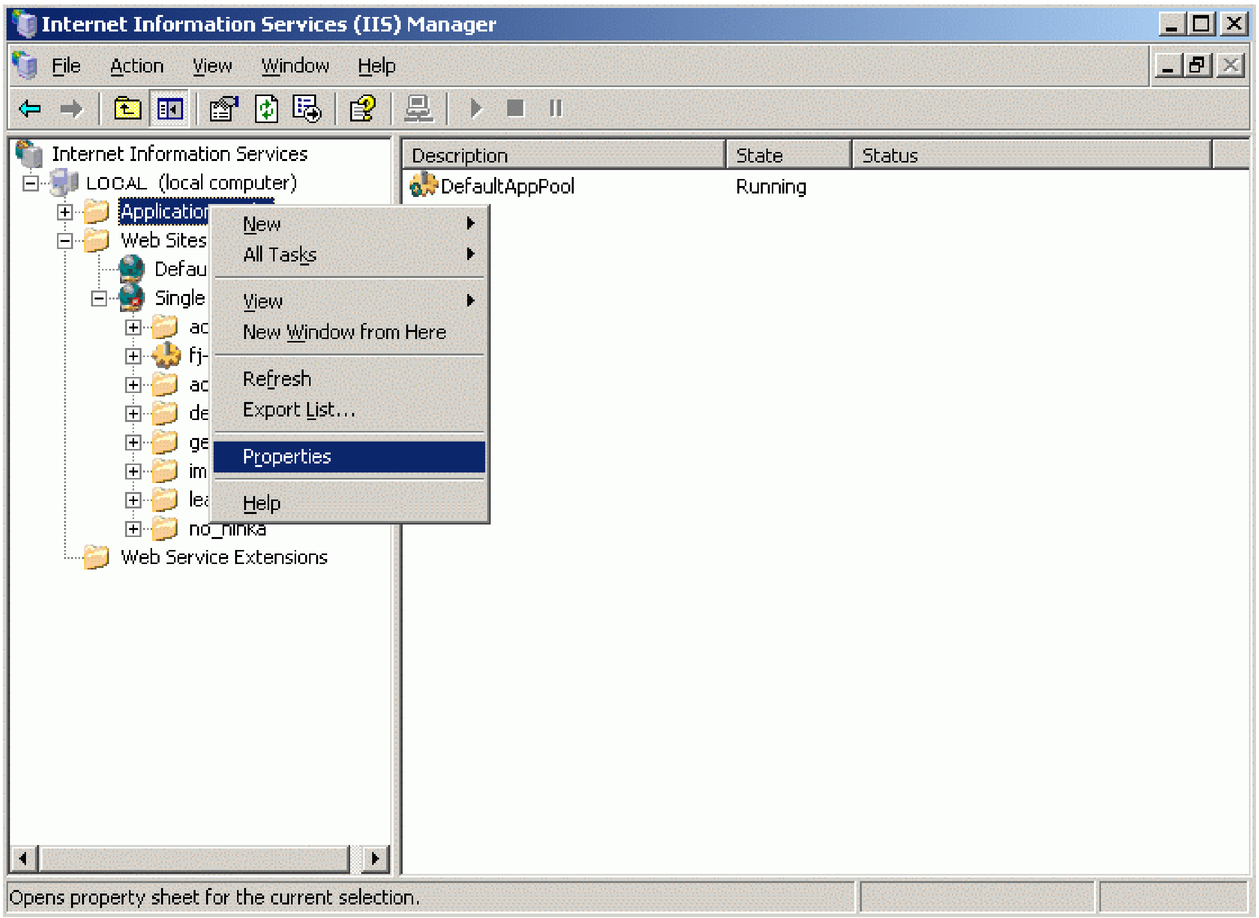


Web Service Extensions

Web Service Extension	Status
All Unknown CGI Extensions	Allowed
All Unknown ISAPI Extensions	Allowed
Active Server Pages	Prohibited
Business Server	Allowed
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
WebDAV	Prohibited

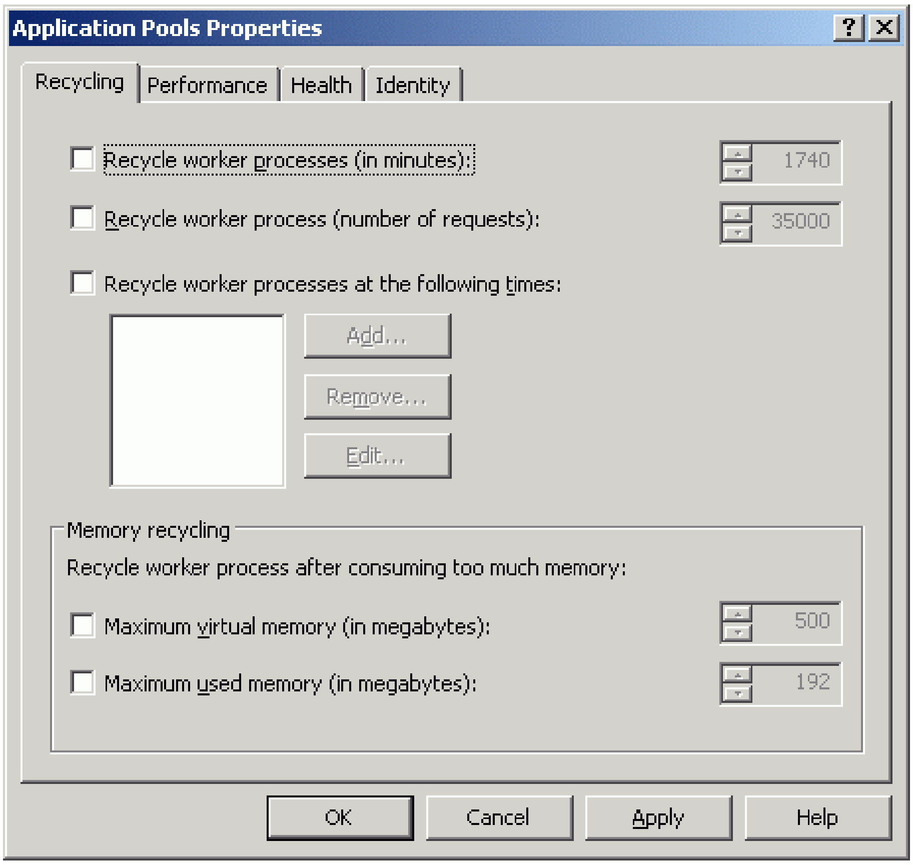
13. Click Application Pools.

Figure 3.18 Select Application Pools



14. Right-click, and click Properties to open the Properties dialog. Click the [Recycle] tab, clear all check box items.

Figure 3.19 Select Properties



□ Recycle worker processes (in minutes): 1740

□ Recycle worker process (number of requests): 35000

□ Recycle worker processes at the following times:

Memory recycling

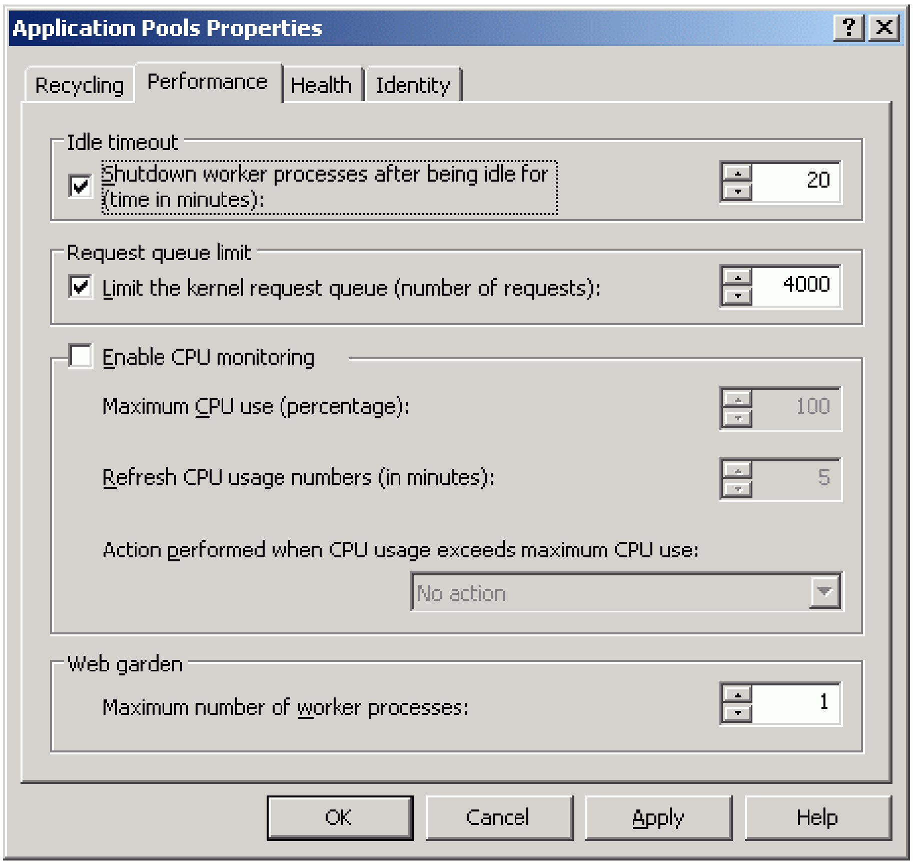
Recycle worker process after consuming too much memory:

□ Maximum virtual memory (in megabytes): 500

□ Maximum used memory (in megabytes): 192

15. Click the [Performance] tab, under [Web garden], in [Maximum number of worker processes], specify "1".

Figure 3.20 Select Properties



Application Pools Properties

Recycling | Performance | Health | Identity

Idle timeout

☑ Shutdown worker processes after being idle for (time in minutes): 20

Request queue limit

☑ Limit the kernel request queue (number of requests): 4000

☐ Enable CPU monitoring

Maximum CPU use (percentage): 100

Refresh CPU usage numbers (in minutes): 5

Action performed when CPU usage exceeds maximum CPU use: No action

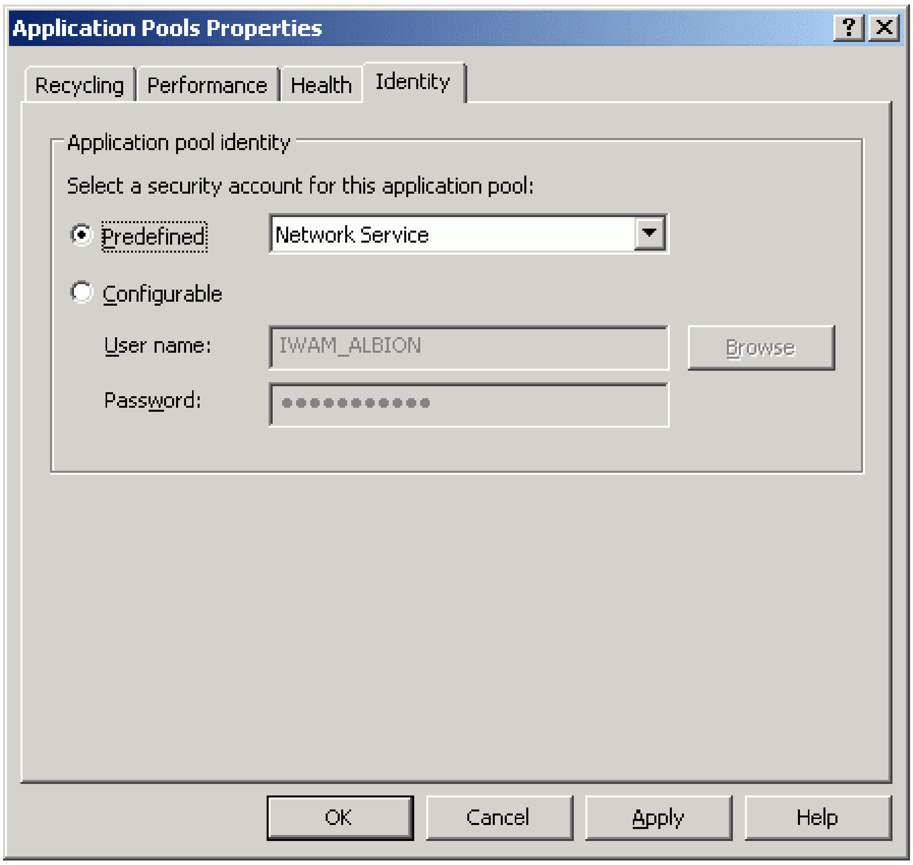
Web garden

Maximum number of worker processes: 1

16. Click the [Identity] tab, in [Application pool identity], select "Network Service" or "Local System", and then click [OK].

    In the example below, "Network Service" is selected.

    Figure 3.21 Select Properties



Application pool identity

Select a security account for this application pool:

● Predefined: Network Service

○ Configurable

User name: IWAM_ALBION

Password: ●●●●●●●●●●●●

17. In the selected security account, set the access authority so that "Full Control" is assigned to the Interstage certificate environment folder. For details about Interstage certificate environment access authority settings, refer to "Configuring Environments" - "Setup and Use of Interstage Certificate Environments" in the "Security System Operator's Guide".

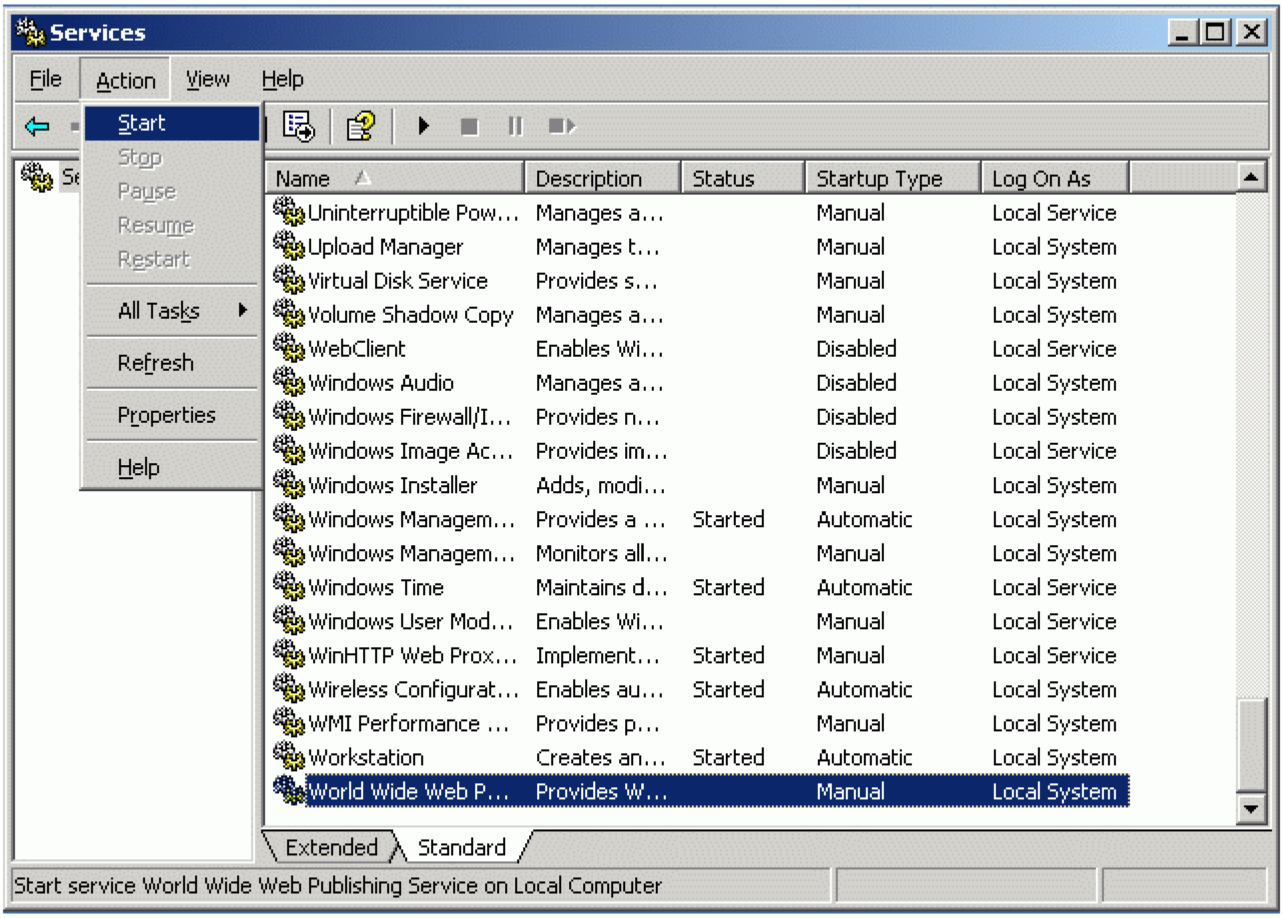
18. To run Interstage Application Server on Windows Server(R) x64 Editions (32-bit compatible), issue the command below to read the ISAPI filter for 32 bit.

```
cscript %SystemDrive%\inetpub\AdminScripts\adsutil.vbs set w3svc/AppPools/Enable32bitAppOnWin64
1
```

19. When complete, start Microsoft(R) Internet Information Services.

    To start Microsoft IIS, from Windows, click [Start] > [Programs] > [Administrative Tools] > [Services], and select [World Wide Web Publishing Service]. From the [Action] menu, select [Start].

    Figure 3.22 Start Microsoft IIS



Name	Description	Status	Startup Type	Log On As
Uninterruptible Pow...	Manages a...		Manual	Local Service
Upload Manager	Manages t...		Manual	Local System
Virtual Disk Service	Provides s...		Manual	Local System
Volume Shadow Copy	Manages a...		Manual	Local System
WebClient	Enables Wi...		Disabled	Local Service
Windows Audio	Manages a...		Disabled	Local System
Windows Firewall/I...	Provides n...		Disabled	Local System
Windows Image Ac...	Provides im...		Disabled	Local Service
Windows Installer	Adds, modi...		Manual	Local System
Windows Managem...	Provides a ...	Started	Automatic	Local System
Windows Managem...	Monitors all...		Manual	Local System
Windows Time	Maintains d...	Started	Automatic	Local Service
Windows User Mod...	Enables Wi...		Manual	Local Service
WinHTTP Web Prox...	Implement...	Started	Manual	Local Service
Wireless Configurat...	Enables au...	Started	Automatic	Local System
WMI Performance ...	Provides p...		Manual	Local System
Workstation	Creates an...	Started	Automatic	Local System
World Wide Web P...	Provides W...		Manual	Local System

Start service World Wide Web Publishing Service on Local Computer

For details regarding Microsoft(R) Internet Information Services sites, refer to Microsoft(R) Internet Information Services Help.

3.4.4 Integrating with Microsoft(R) Internet Information Services 7.0 or 7.5

This section explains the procedure to integrate a business server into Microsoft(R) Internet Information Services (IIS). In this example Microsoft(R) Windows Server(R) 2008 is used to explain the procedure for integration of a business server into the Web site used under Microsoft(R) Internet Information Services 7.0.

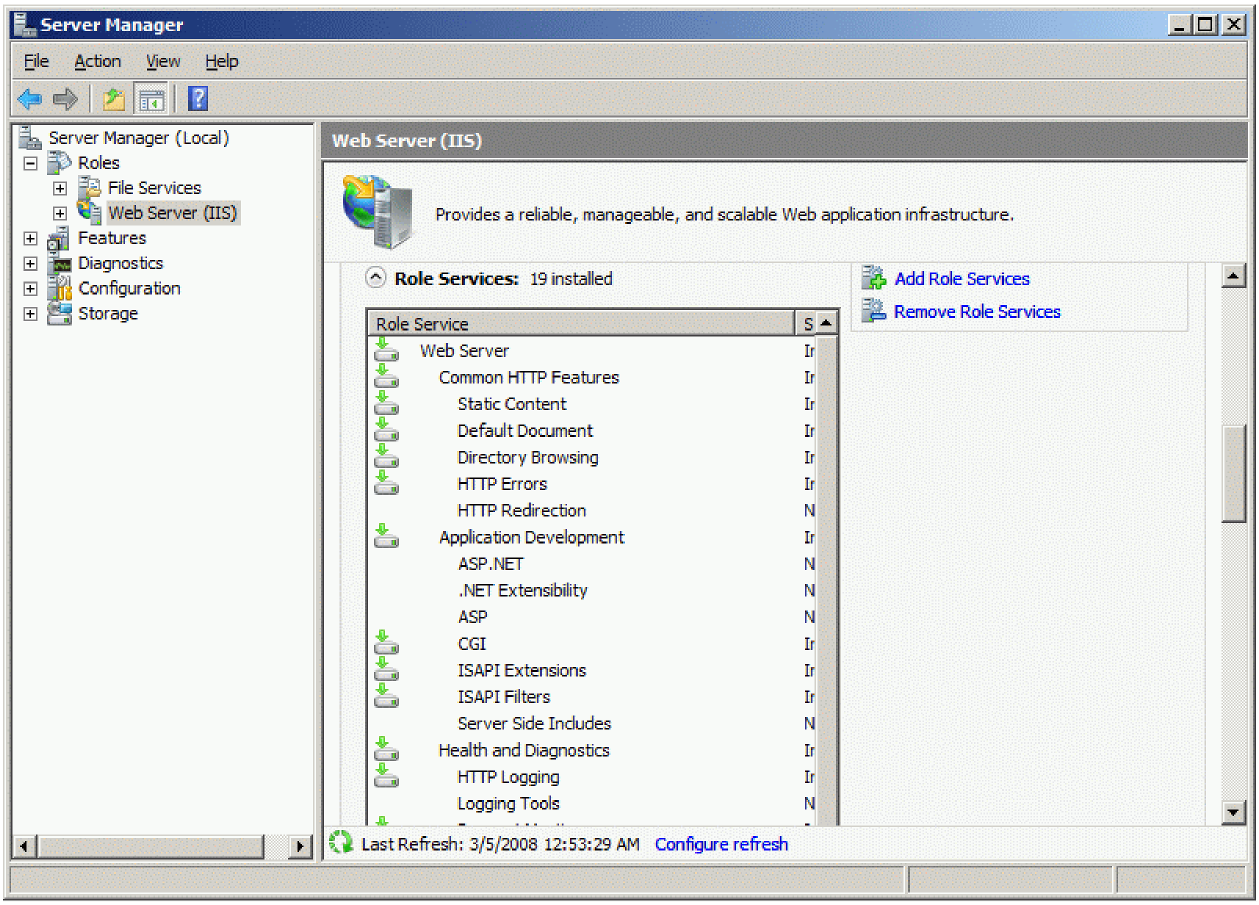
If Microsoft(R) Internet Information Services 7.0 or 7.5 is used, after it has been installed, the system must be restarted. If the system is not restarted, business server programs may not be readable.

1. Check that the following role service is installed in the Web server. If the role service is not installed, install it.

    - ISAPI Extensions

- ISAPI Filters

Figure 3.23 Internet Information Services (IIS) Manager



Provides a reliable, manageable, and scalable Web application infrastructure.

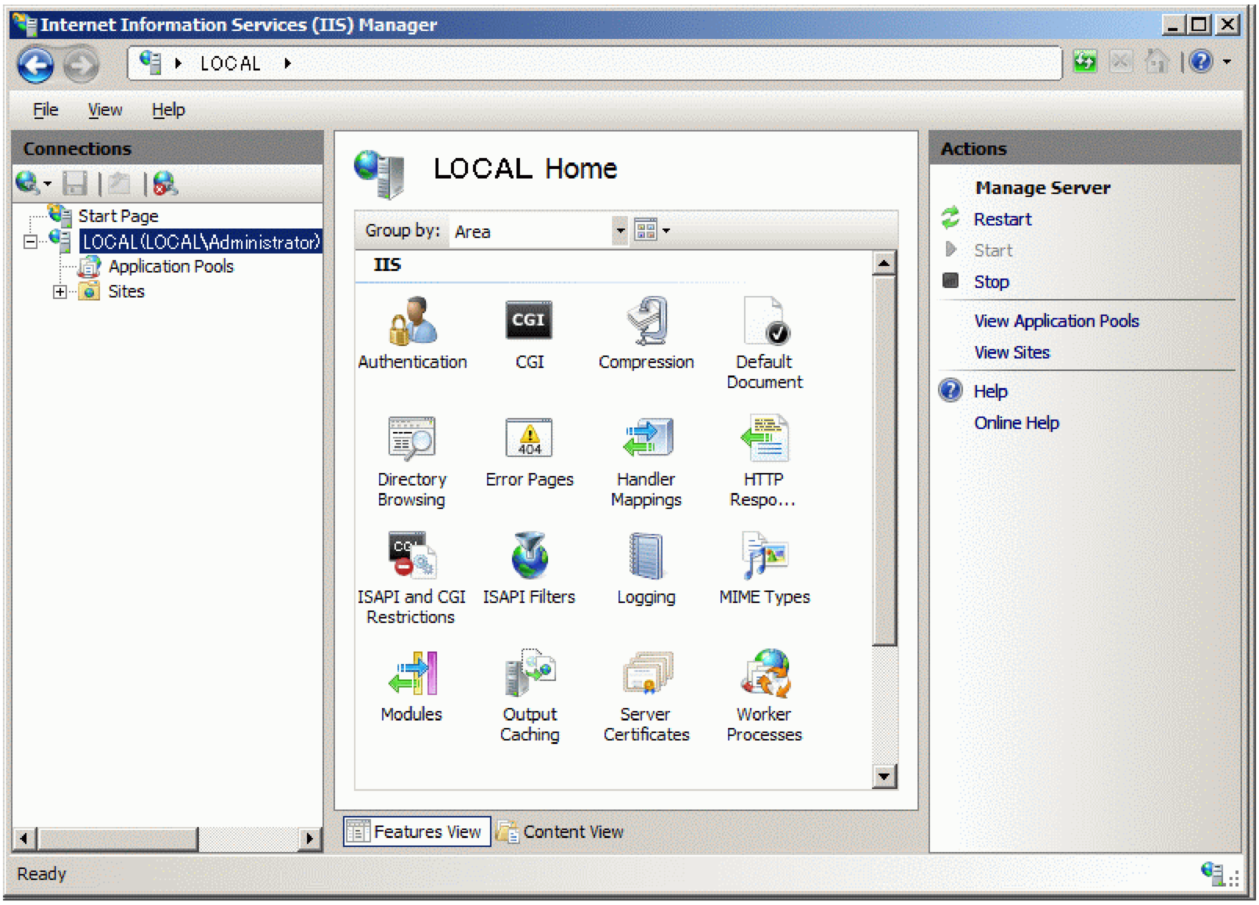
Role Services: 19 installed

Role Service	S
Web Server	Ir
Common HTTP Features	Ir
Static Content	Ir
Default Document	Ir
Directory Browsing	Ir
HTTP Errors	Ir
HTTP Redirection	N
Application Development	Ir
ASP.NET	N
.NET Extensibility	N
ASP	N
CGI	Ir
ISAPI Extensions	Ir
ISAPI Filters	Ir
Server Side Includes	N
Health and Diagnostics	Ir
HTTP Logging	Ir
Logging Tools	N

Last Refresh: 3/5/2008 12:53:29 AM

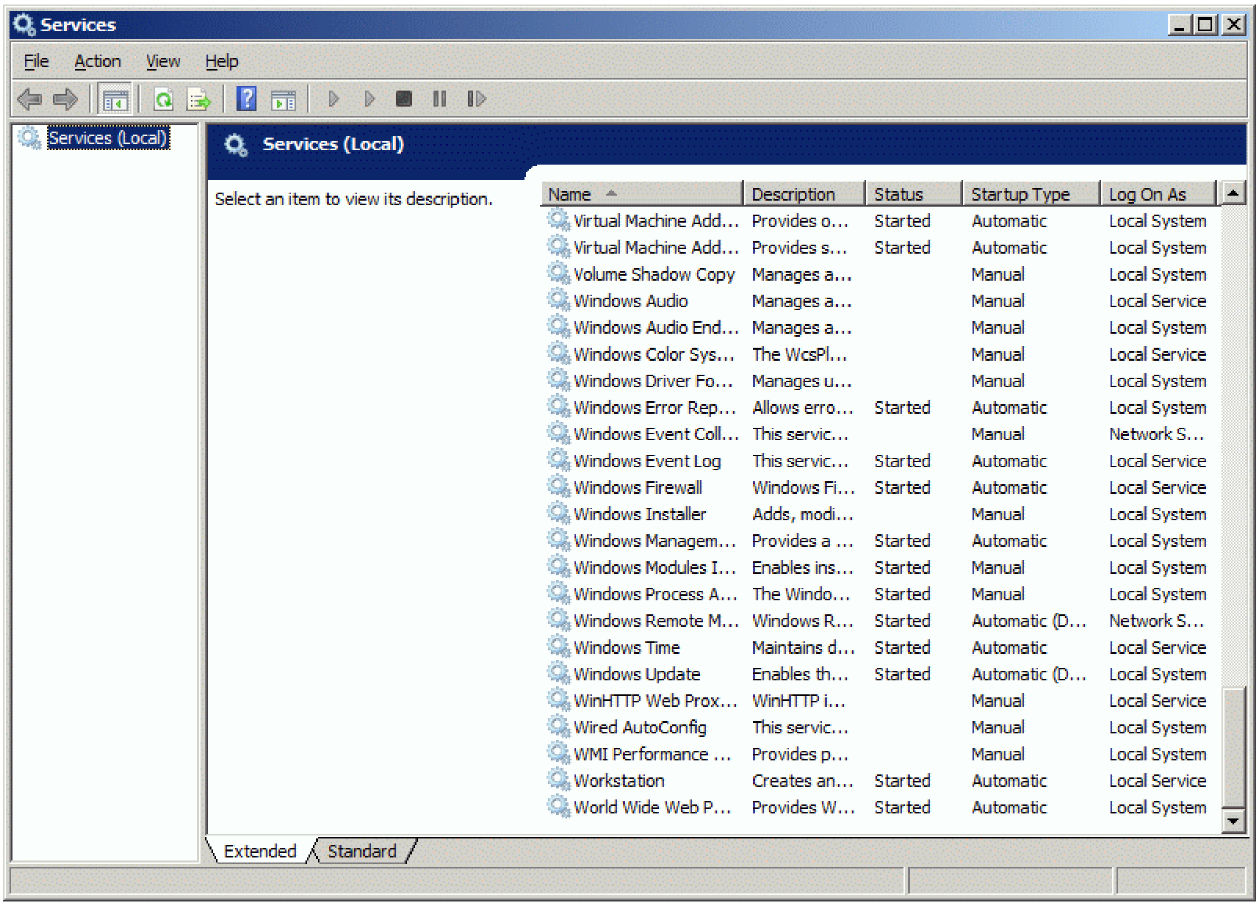
2. Select [Administrative Tools] > [Internet Information Services (IIS) Manager] in [Start] menu.

Figure 3.24 Stop Microsoft IIS



Stop Microsoft(R) Internet Information Services if already running. To stop, select [Administrative Tools] > [Services] in [Start] menu, and select [World Wide Web Publishing Service] in the Window. Select [Stop] from the list.

Figure 3.25 Stop the Microsoft(R) Internet Information Services

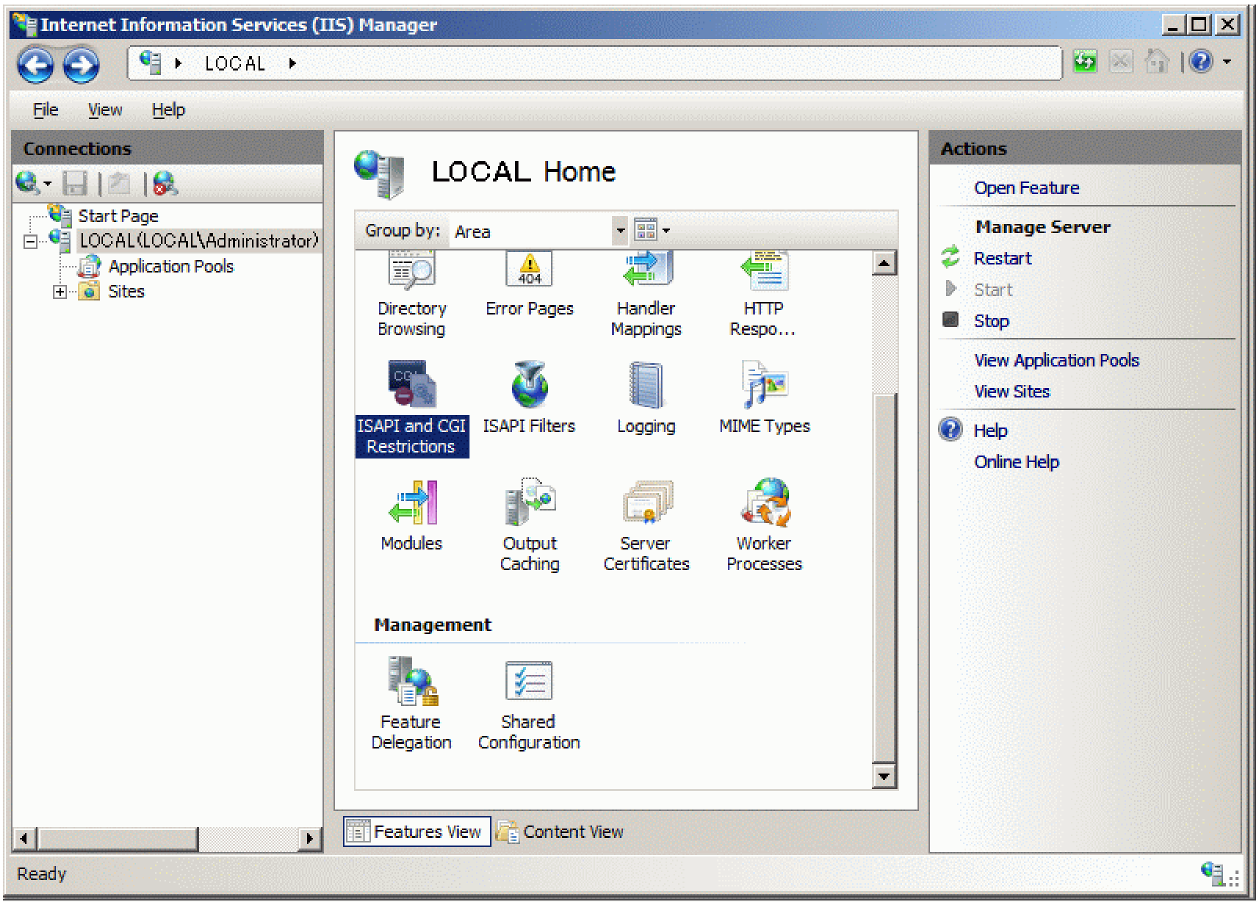


Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Virtual Machine Add...	Provides o...	Started	Automatic	Local System
Virtual Machine Add...	Provides s...	Started	Automatic	Local System
Volume Shadow Copy	Manages a...		Manual	Local System
Windows Audio	Manages a...		Manual	Local Service
Windows Audio End...	Manages a...		Manual	Local System
Windows Color Sys...	The WcsPl...		Manual	Local Service
Windows Driver Fo...	Manages u...		Manual	Local System
Windows Error Rep...	Allows erro...	Started	Automatic	Local System
Windows Event Coll...	This servic...		Manual	Network S...
Windows Event Log	This servic...	Started	Automatic	Local Service
Windows Firewall	Windows Fi...	Started	Automatic	Local Service
Windows Installer	Adds, modi...		Manual	Local System
Windows Managem...	Provides a ...	Started	Automatic	Local System
Windows Modules I...	Enables ins...	Started	Manual	Local System
Windows Process A...	The Windo...	Started	Manual	Local System
Windows Remote M...	Windows R...	Started	Automatic (D...	Network S...
Windows Time	Maintains d...	Started	Automatic	Local Service
Windows Update	Enables th...	Started	Automatic (D...	Local System
WinHTTP Web Prox...	WinHTTP i...		Manual	Local Service
Wired AutoConfig	This servic...		Manual	Local System
WMI Performance ...	Provides p...		Manual	Local System
Workstation	Creates an...	Started	Automatic	Local Service
World Wide Web P...	Provides W...	Started	Automatic	Local System

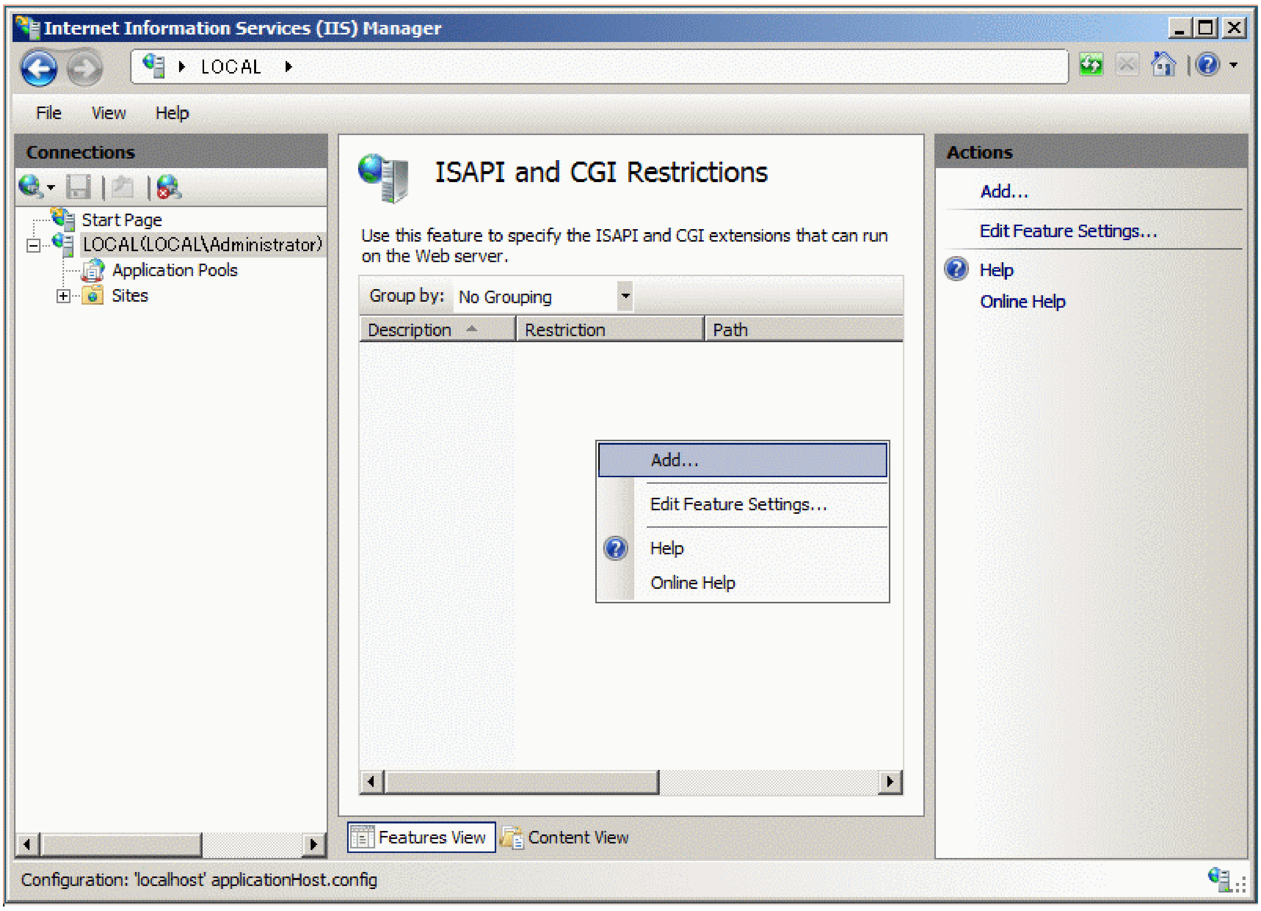
3. Select the host name and select [ISAPI and CGI Restrictions] in [Features View].

Figure 3.26 Select a Web Site for Integration



4. Add [ISAPI and CGI Restrictions]

Figure 3.27 Select Properties

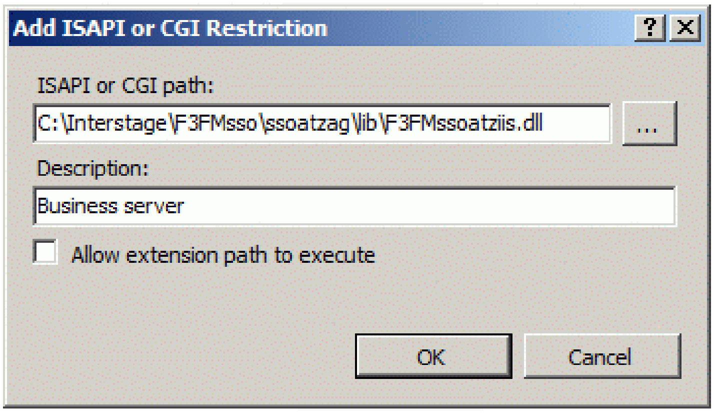

Internet Information Services (IIS) Manager
LOCAL
File View Help
Connections
Start Page
LOCAL(LOCAL\Administrator)
Application Pools
Sites
ISAPI and CGI Restrictions
Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.
Group by: No Grouping
Description
Restriction
Path
Add...
Edit Feature Settings...
Help
Online Help
Features View
Content View
Actions
Add...
Edit Feature Settings...
Help
Online Help
Configuration: 'localhost' applicationHost.config

Set the business server program in "ISAPI or CGI path" with the absolute path.

Examples below set "C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll in "ISAPI or CGI path" and the "Business server" in the "Description".

Click the [OK] button after completing the settings.

Figure 3.28 Specify ISAPI or CGI path


Add ISAPI or CGI Restriction

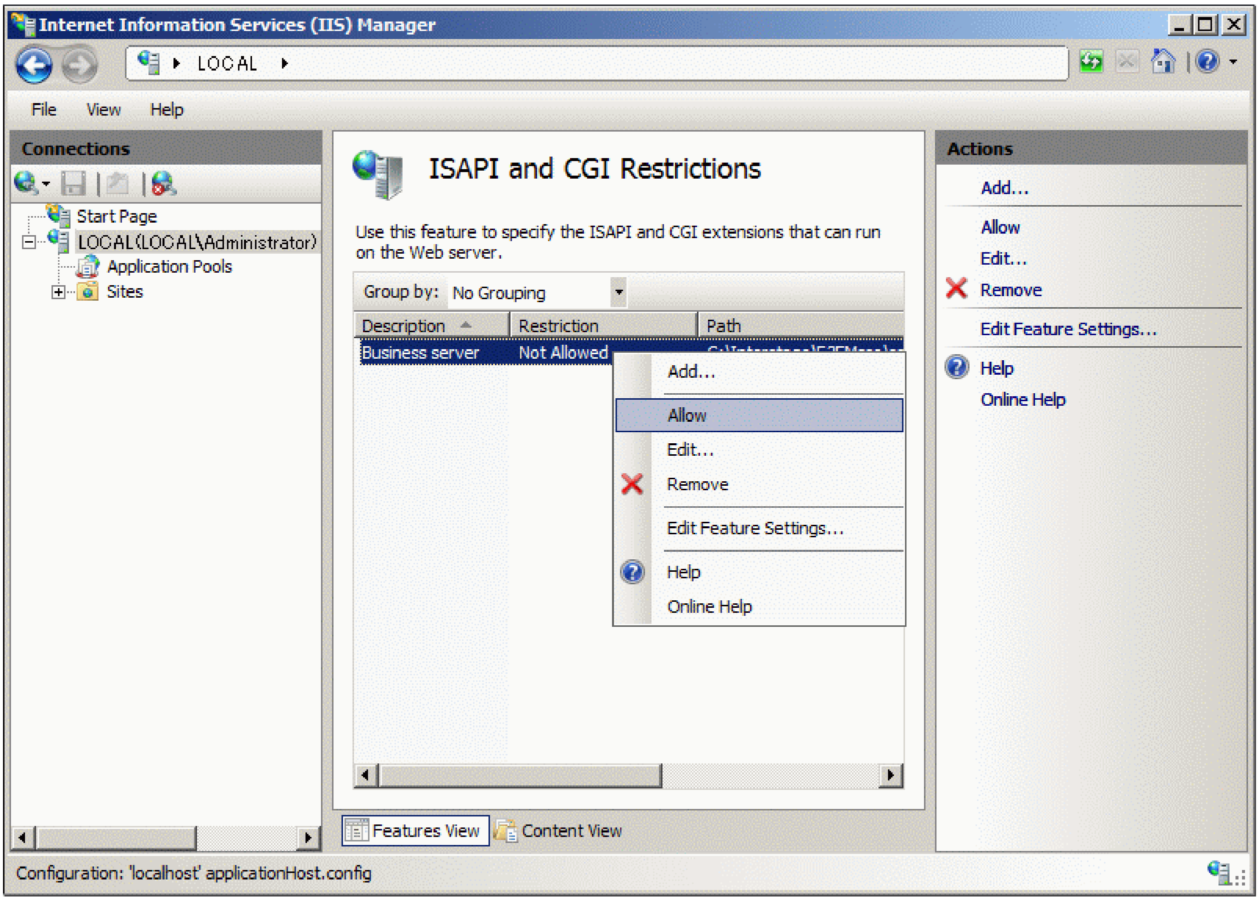
ISAPI or CGI path: C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll

Description: Business server

□ Allow extension path to execute

5. Change the added ISAPI to Allow

Figure 3.29 Specify Business Server



Internet Information Services (IIS) Manager

ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Group by: No Grouping

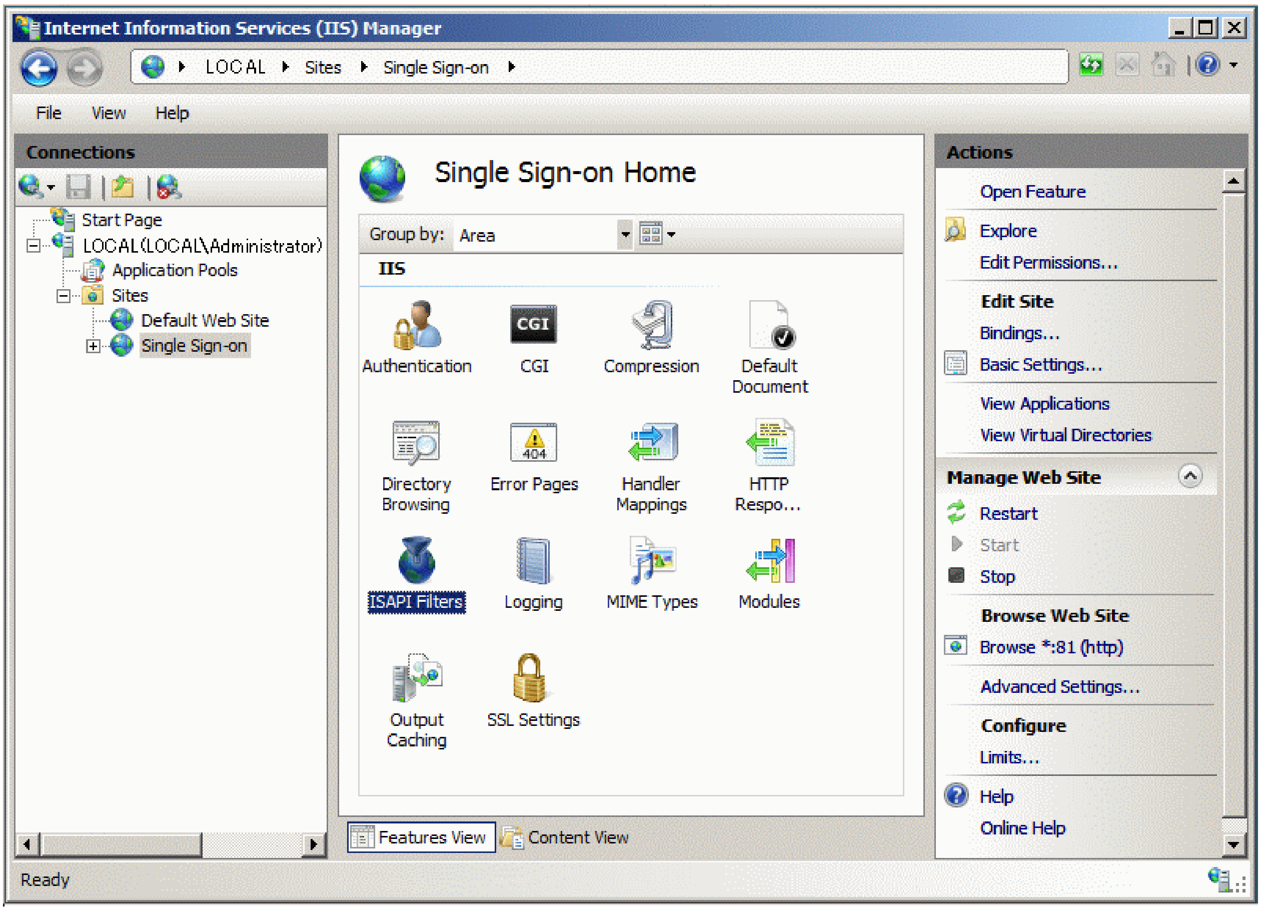
Description	Restriction	Path
Business server	Not Allowed	

Configuration: 'localhost' applicationHost.config

6. Select the site to integrate the business server and then select [ISAPI Filters] of [Features View].

   The example below shows how to integrate the server on the site called "Single Sign-on."

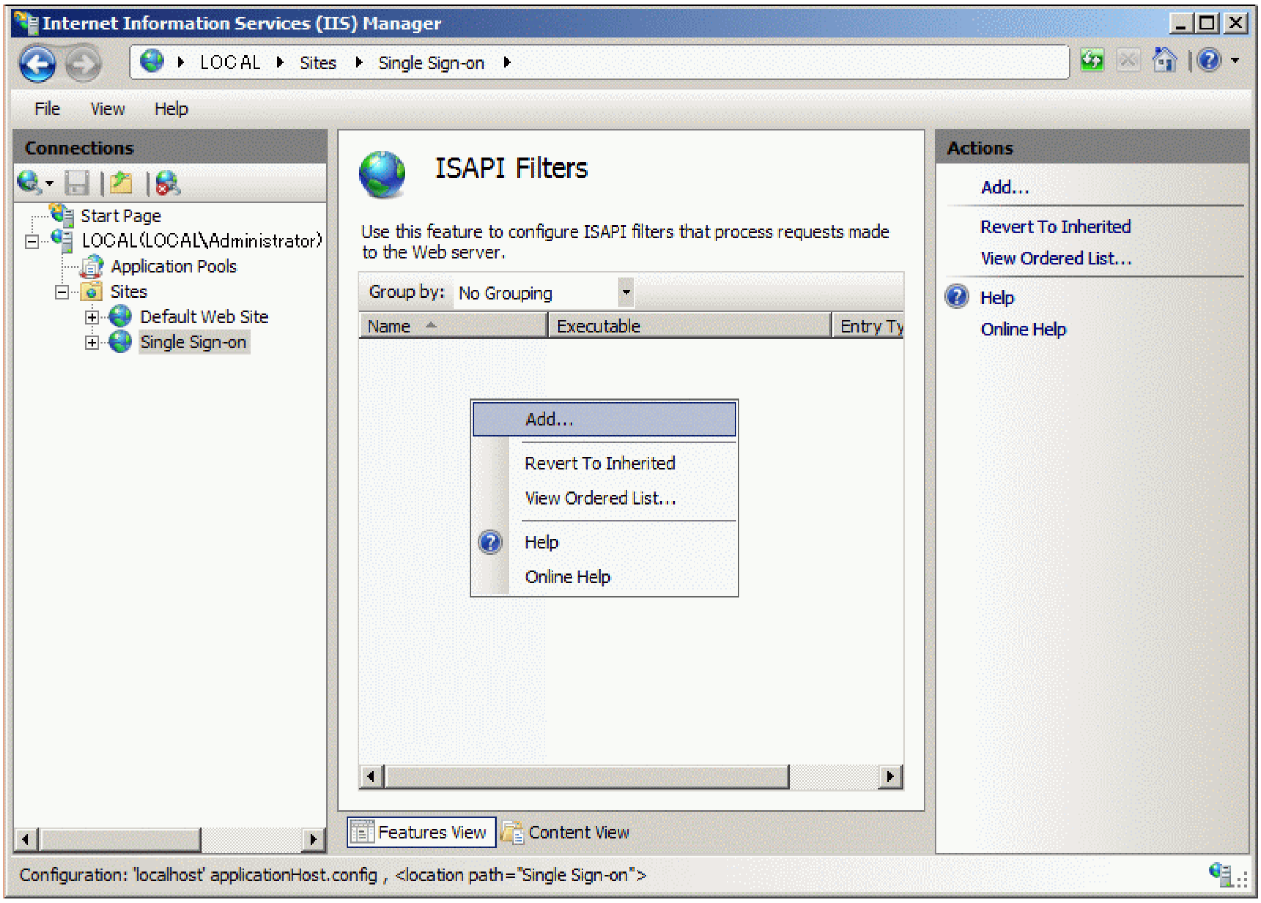
Figure 3.30 Open the Virtual Directory Creation Wizard window



7. Add [ISAPI Filters]

Note that, if the ISAPI filter has already been set, after adding the business server program to the ISAPI filter, you must change the order so that the business server program is displayed at the top.

Figure 3.31 Set the Virtual Directory Alias



Use this feature to configure ISAPI filters that process requests made to the Web server.

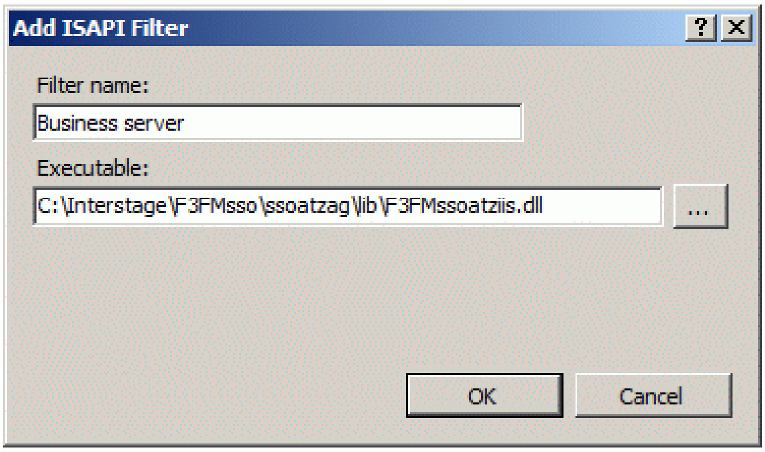
Configuration: 'localhost' applicationHost.config , <location path="Single Sign-on">

Set the business server program in [ISAPI Filters] with the absolute path.

The examples below set the "Business server" in the filter name and "C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll" in the executable file.

Click the [OK] button after completing the settings.

Figure 3.32 Specify ISAPI Filters

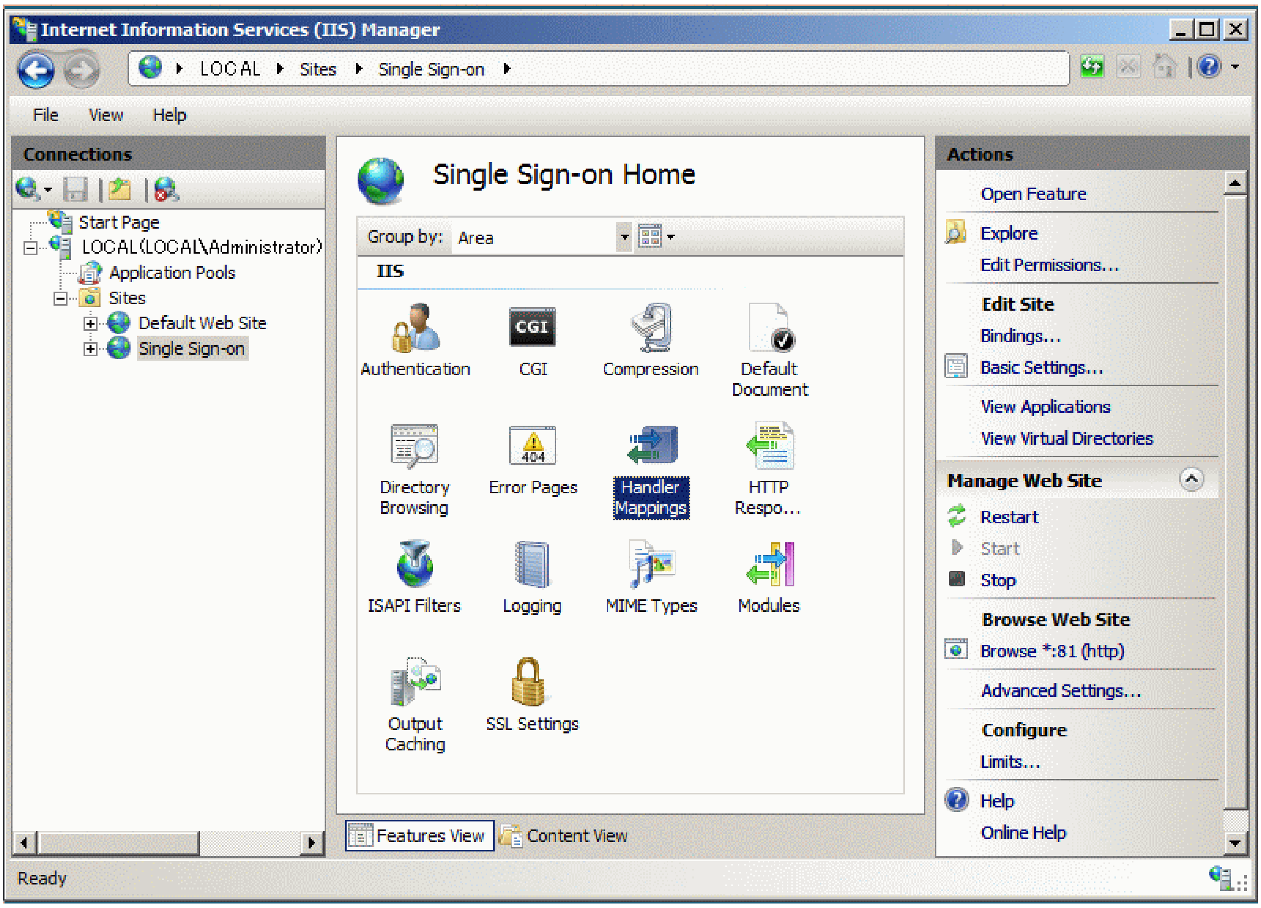


Filter name: Business server

Executable: C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll

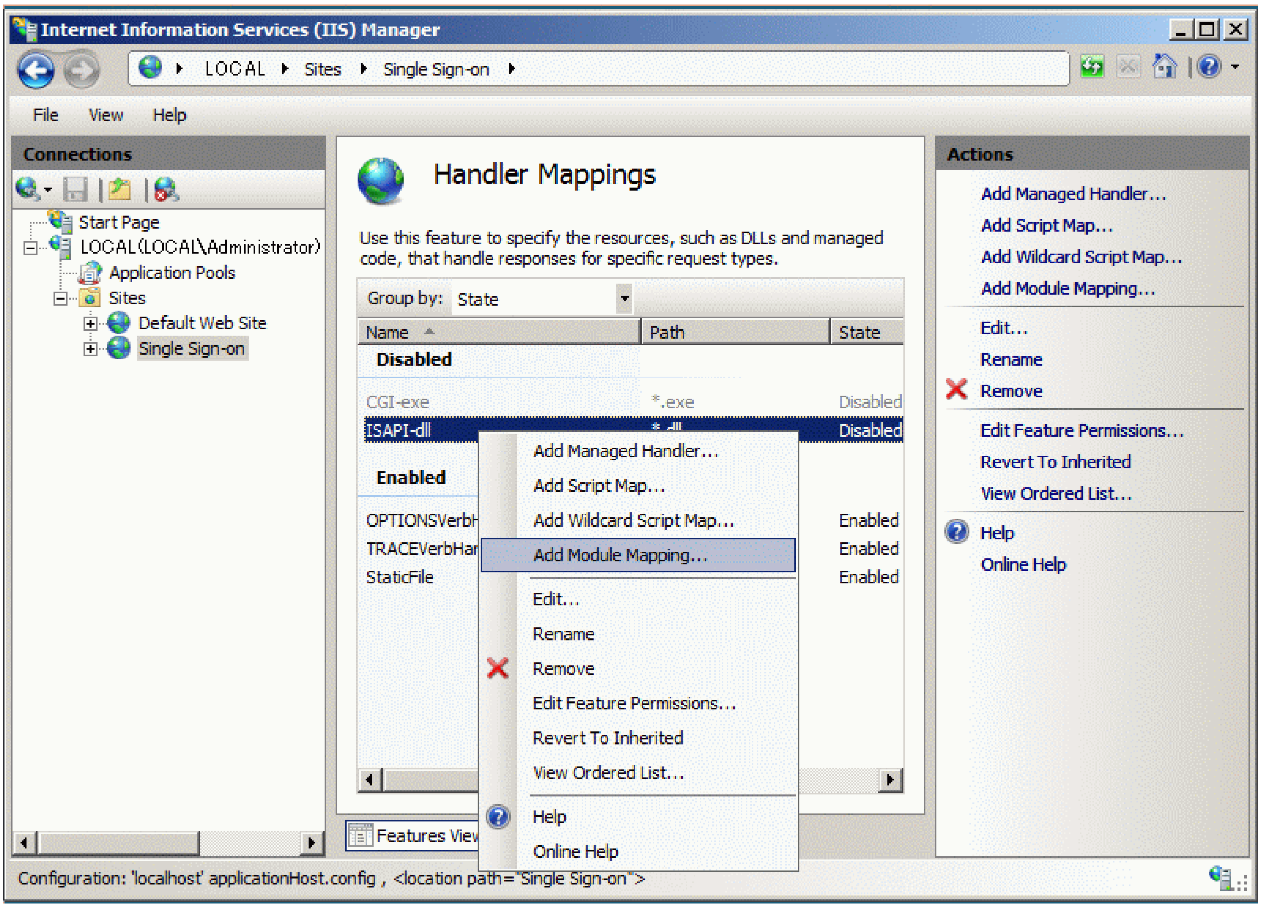
8. Select the site to integrate the business server and select [Handler Mappings] of [Features View].

Figure 3.33 Set the Web Site Contents Directory



9. Add [Module Mapping]

Figure 3.34 Set Access Permissions



Use this feature to specify the resources, such as DLLs and managed code, that handle responses for specific request types.

Name	Path	State
Disabled		
CGI-exe	*.exe	Disabled
ISAPI-dll	*.dll	Disabled
Enabled		
OPTIONSVerbH		Enabled
TRACEVerbHar		Enabled
StaticFile		Enabled

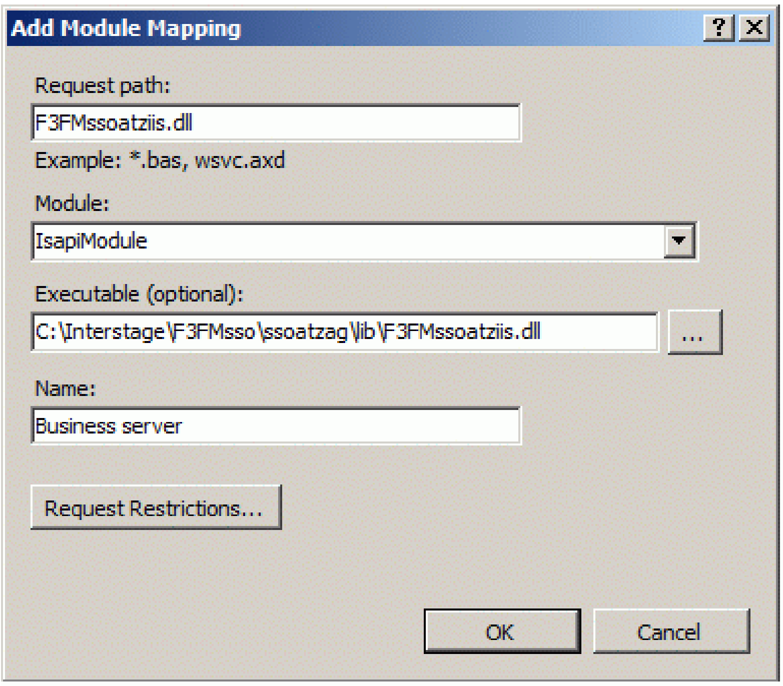
Configuration: 'localhost' applicationHost.config , <location path="Single Sign-on">

Set "F3FMssoatziis.dll" in the "Request path", "IsapiModule" in "Module" and the business server program absolute path in "Executable (optional)".

The examples below set "C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll" in the executable file and the "Business server" in the name.

Click the [OK] button after completing the settings.

Figure 3.35 Add Module Mapping



Add Module Mapping

Request path: F3FMssoatziis.dll

Example: *.bas, wsvc.axd

Module: IsapiModule

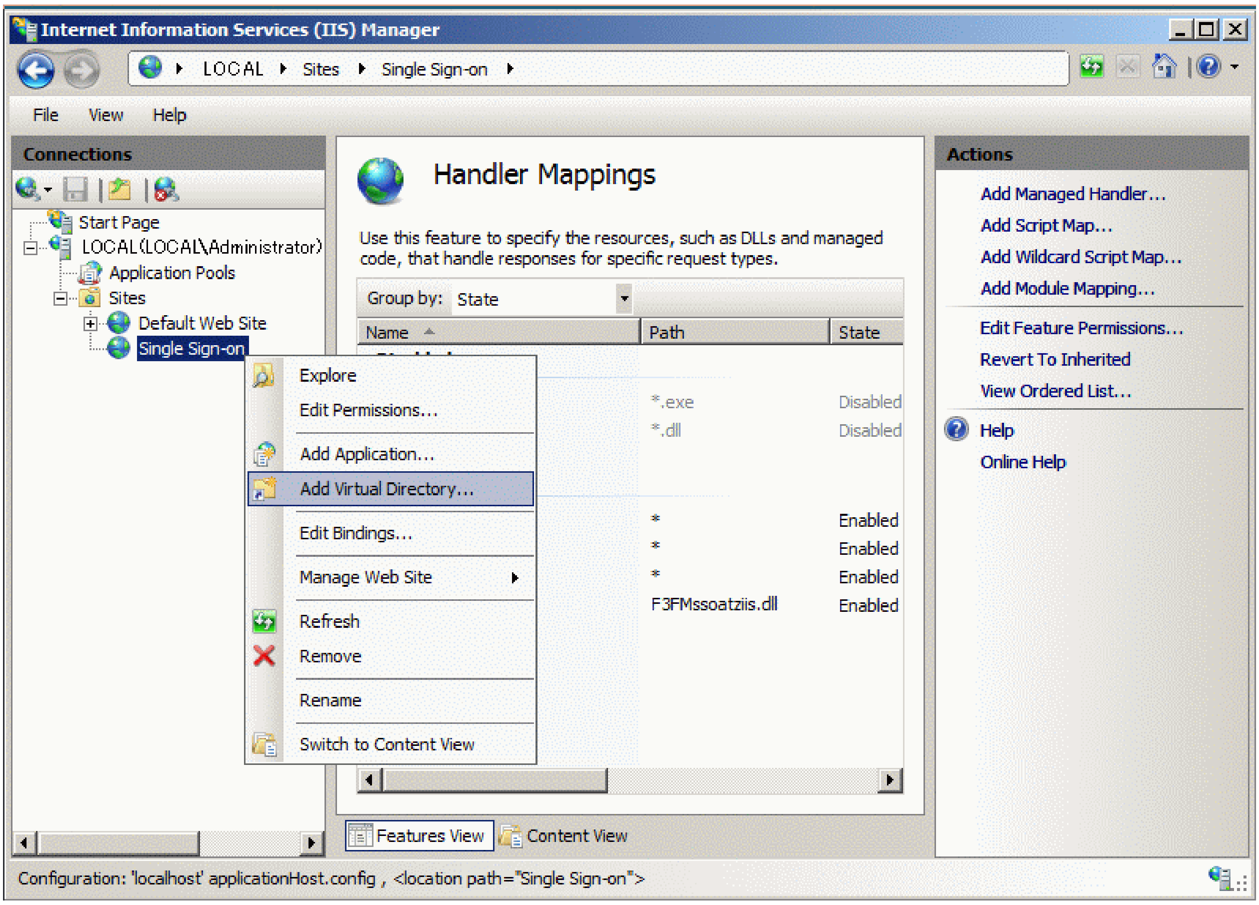
Executable (optional): C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll

Name: Business server

10. Select the site to integrate the business server.

Select [Add Virtual Directory] and add the virtual directory.

Figure 3.36 Return to the Internet Information Services Manager



Internet Information Services (IIS) Manager

LOCAL ▸ Sites ▸ Single Sign-on ▸

Handler Mappings

Use this feature to specify the resources, such as DLLs and managed code, that handle responses for specific request types.

Group by: State

Name	Path	State
	*.exe	Disabled
	*.dll	Disabled
	*	Enabled
	*	Enabled
	*	Enabled
	F3FMssoatziis.dll	Enabled

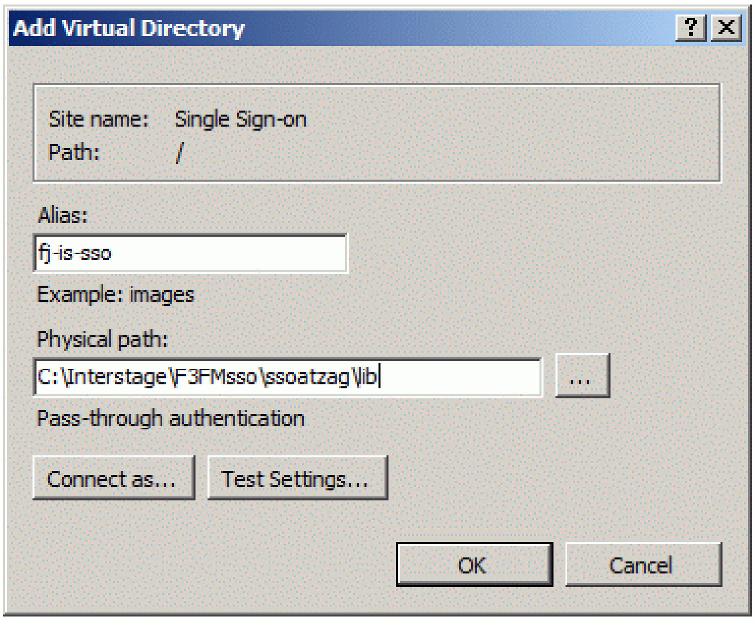
Configuration: 'localhost' applicationHost.config , <location path="Single Sign-on">

Set "fj-is-sso" in the [Alias] and the business server program absolute path in the Physical path.

The example below shows the settings of "C:\Interstage\F3FMsso\ssoatzag\lib" in the "Physical path".

Click **OK** after completing the settings.

Figure 3.37 Add Virtual Directory



Add Virtual Directory

Site name: Single Sign-on

Path: /

Alias: fj-is-sso

Example: images

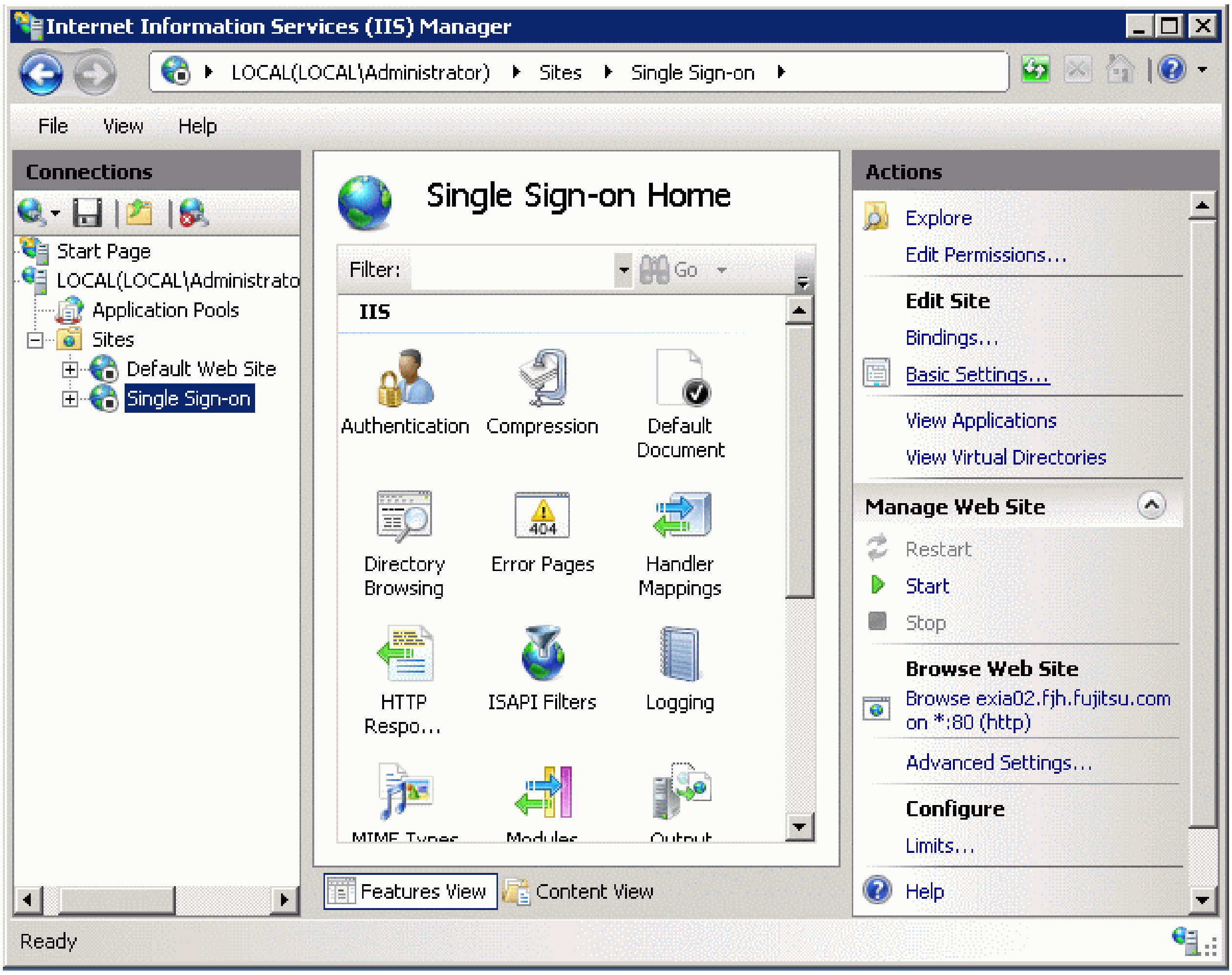
Physical path: C:\Interstage\F3FMsso\ssoatzag\lib

Pass-through authentication

11. Select the site that will embed the business server.

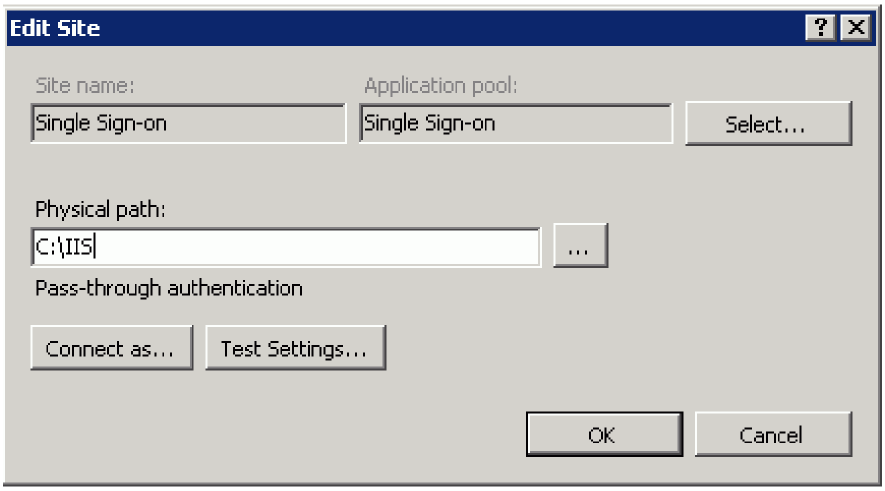
    Click [Basic Settings] on the Actions menu.

Figure 3.38 Click [Basic Settings] on the Actions menu



Confirm an application pool.

Figure 3.39 Confirm an application pool



Site name: Single Sign-on

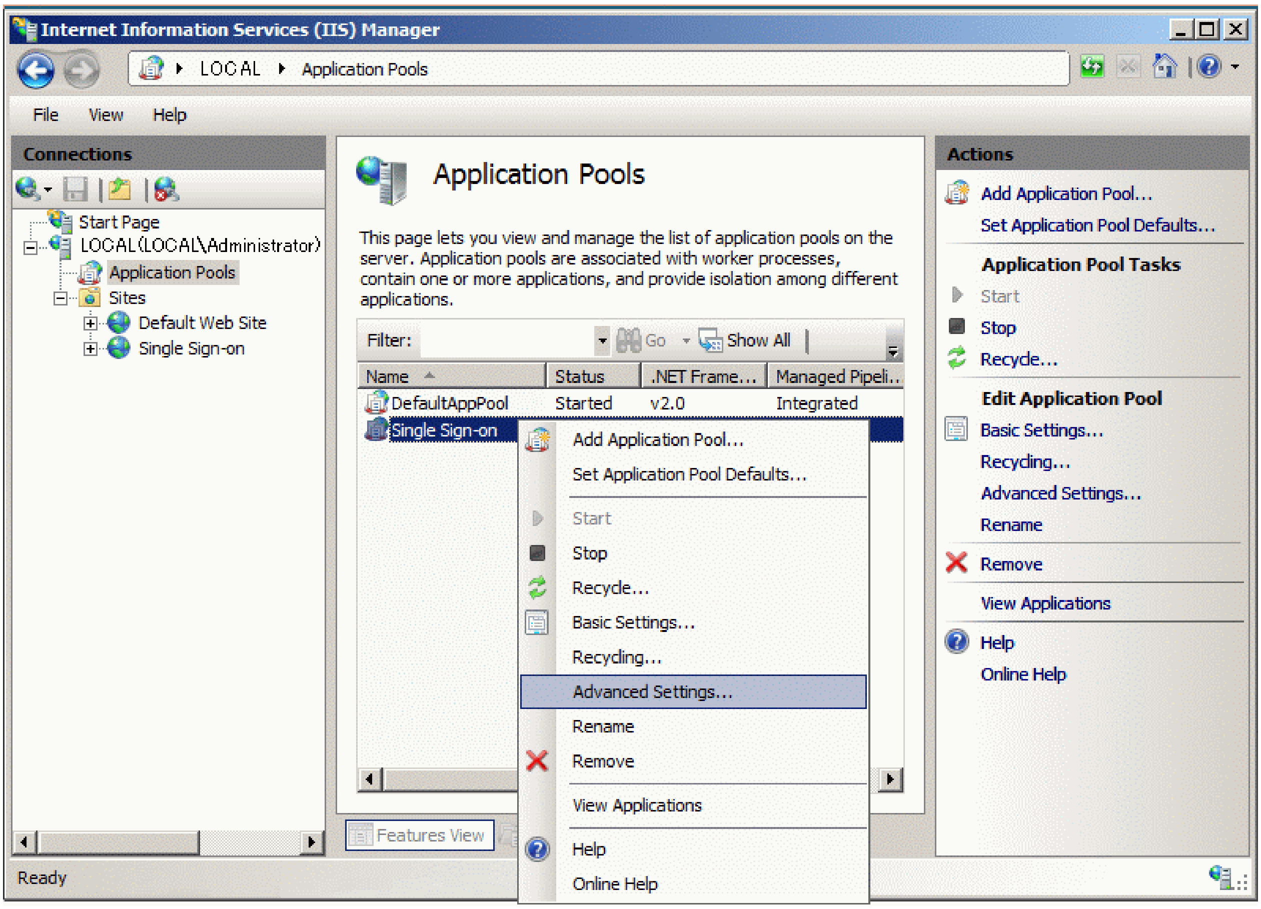
Application pool: Single Sign-on

Physical path: C:\IIS

12. Select [Application Pools] to display the list of application pools.

    Select the application pool that was confirmed in step 11, and then select [Advanced Settings].

Figure 3.40 Add the Web Service Extension



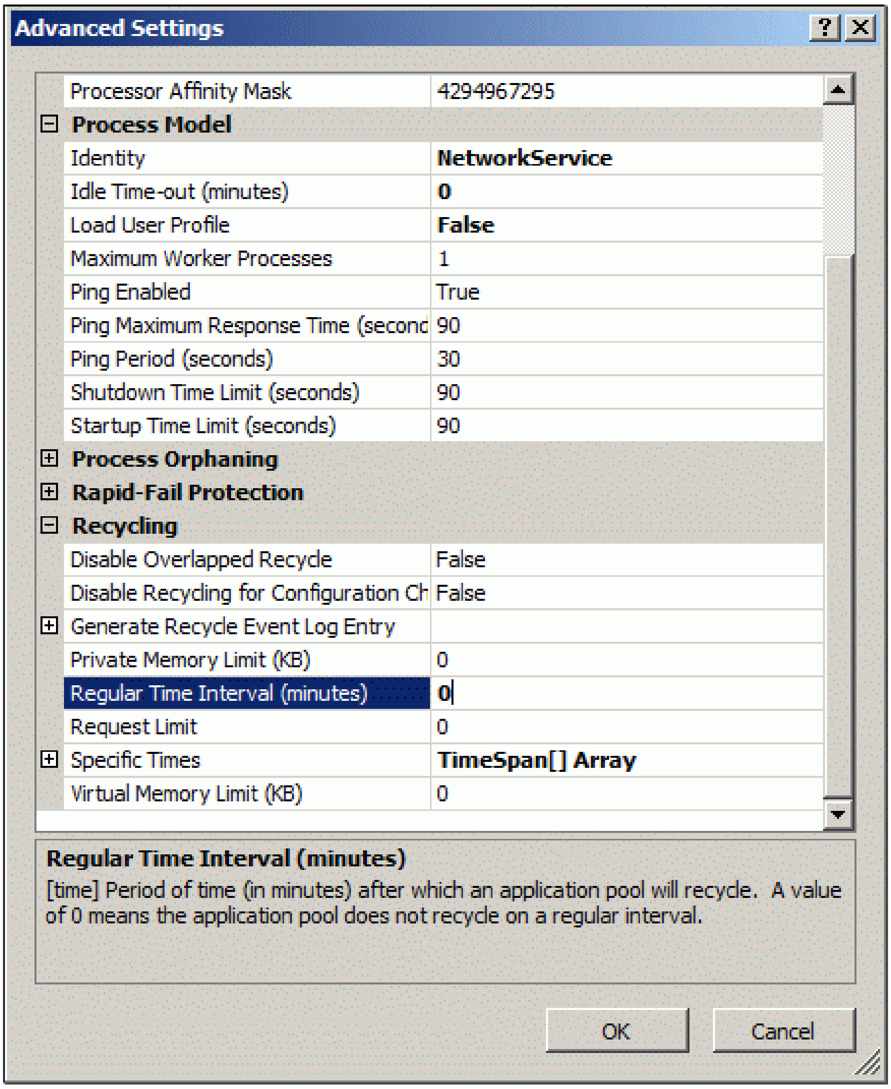
This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Frame...	Managed Pipeli...
DefaultAppPool	Started	v2.0	Integrated
Single Sign-on			

If the application pool that was selected is incorrect, the sso00202 error message may sometimes be output to the system log during an operation.

13. Set "0" in [Idle Time-out (minutes)] of [Process Model] in Advanced Settings, "1" in [Maximum Worker Processes] of [Process Model], and "0" in [Regular Time Interval (minutes)] of [Recycling].

Figure 3.41 Set the Extension Name



Advanced Settings

Processor Affinity Mask	4294967295
⊟ **Process Model**	
Identity	**NetworkService**
Idle Time-out (minutes)	**0**
Load User Profile	**False**
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90
⊞ **Process Orphaning**	
⊞ **Rapid-Fail Protection**	
⊟ **Recycling**	
Disable Overlapped Recycle	False
Disable Recycling for Configuration Ch	False
⊞ Generate Recycle Event Log Entry	
Private Memory Limit (KB)	0
Regular Time Interval (minutes)	**0**
Request Limit	0
⊞ Specific Times	**TimeSpan[] Array**
Virtual Memory Limit (KB)	0

Regular Time Interval (minutes)

[time] Period of time (in minutes) after which an application pool will recycle. A value of 0 means the application pool does not recycle on a regular interval.

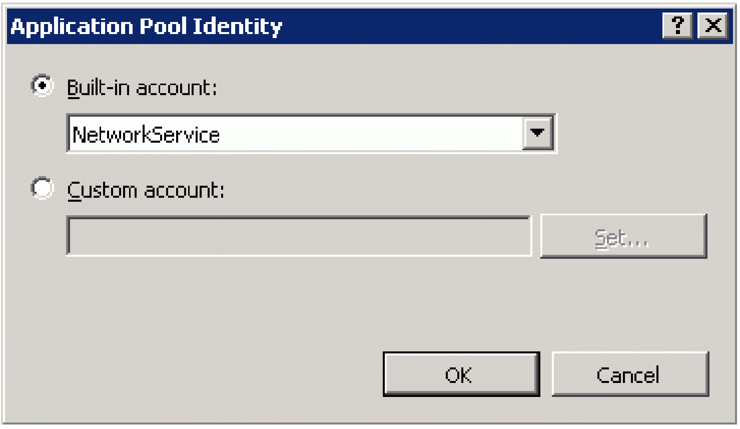
Next, click [Process Model] - [Identity] - [...], then from [Application Pool Identity] - "Built-in account", set one of the following:

- ApplicationPoolIdentity
- NetworkService
- LocalSystem

Click the [OK] button.

In the following example, "Built-in account" - "NetworkService" is set for [Application Pool Identity].

Figure 3.42 Set the Built-in Account



Application Pool Identity

● Built-in account:

NetworkService

○ Custom account:

Note

- [ApplicationPoolIdentity] can be selected in Windows Server(R) 2008 Service Pack2 or later, and Windows Server(R) 2008 R2 or later.
- If the [Process Model] - [Identity] update is not correct, the business server may fail to start and the sso03004 error message may be output to the system log.

14. 14.In the security account selected by [Process Model] ID, set the access authority to gain access to the Interstage certificate environment folder with [Full control],

[Process Model] - [Identity]	Access permission set
ApplicationPoolIdentity	IIS_IUSRS group
NetworkService	NETWORK SERVICE
LocalSystem	SYSTEM

For details of access authority in the Interstage certificate environment, refer to "Configuring Environments" - "Settings of access authority of the Interstage certificate environment" in the "Security System Operator's Guide."

15. To run Interstage Application Server on Windows Server(R) x64 Editions (32-bit compatible),,set [32 bit application Affinity Enabled] of [(General)] in detailed settings to "True."

16. Upon completing all the processes, start Microsoft(R) Internet Information Services. To start, select [Administrative Tools] > [Services] from [Start] menu, select [World Wide Web Publishing Service] from Windows and select [Action]. Select [Start] from the list.

For details regarding Microsoft(R) Internet Information Services sites, refer to Microsoft(R) Internet Information Services Help.

3.5 Setting the Access Permission for Operation Resources of a Web Server Used by a Business Server

The Web server used by a business server can use access log functions to record the request contents. These access logs contain important information that controls authentication and authorization of the users.

To ensure more trustworthy use, set the access permission for the business server to prevent its access log from leaking out.

This section explains how to set the access permission for the Web server access logs.

Windows32/64

Only permit users who belong to the Administrators group and SYSTEM, to access the access log output destination folder.

Use Windows Explorer to set access permission for the folder, to users with Administrator permission.

The following table lists examples of access log output destinations. In this example, the access log output destinations may differ depending on the operating environment.

Table 3.8 Windows Access Log Output Destinations

Web server	Example of access log output folder
Interstage HTTP Server	C:\Interstage\F3FMihs\servers\FJapache\logs\
Microsoft(R) Internet Information Services	C:\inetpub\logs\LogFiles\W3SVC1\

For details about the settings for Microsoft(R) Internet Information Services, refer to Microsoft(R) Internet Information Services Help.

Solaris32/64

Permit only the owner and group to access the access log output destination directory. To set the access permission for the files and directory, use the chmod command and chown command.

Set the access permission as a super user (root).

Table 3.9 Solaris Access Log Output Destinations

Web server	Example of access log output destination directory
Interstage HTTP Server	/var/opt/FJSVihs/servers/FJapache/logs/
Solaris32 Sun Java System Web Server	/usr/iplanet/servers/https-server-name/logs/

Linux32/64

Permit only the owner and group to access the access log output destination directory. To set the access permission for the files and directory, use the chmod command and chown command.

Set the access permission as a super user (root).

Table 3.10 Linux Access Log Output Destinations

Web server	Example of access log output destination directory
Interstage HTTP Server	/var/opt/FJSVihs/servers/FJapache/logs/

Chapter 4 Operation and Maintenance

This chapter explains the operation and maintenance of Interstage Single Sign-on, including starting and stopping the system. It includes the following sections:

4.1 Starting Single Sign-on

This section explains how to start the servers.

4.1.1 Starting a Repository Server

To start a repository server, use the Interstage Management Console on the server where the repository server has been set up. Before starting the repository server, ensure that the SSO repository has started.

For details on starting the Interstage Management Console, refer to the Operator's Guide. For details on using the Interstage Management Console window, refer to the Operator's Guide.

Starting an SSO Repository

Use the Interstage Management Console to select [System] > [Services] > [Repository] > [Repository: View Status], and then start the SSO repository.

If a relational database (RDB) is used as the SSO repository, the RDB system must already be running.

For details on starting the SSO repository and RDB system, refer to the "Directory Service Operator's Guide".

Starting a Repository Server

Starting Interstage HTTP Server starts a repository server. Use the Interstage Management Console to select [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Name: Status]. Click [Start] to start the repository server. Select the Web server that is integrated with the repository server for "Web Server name". If the repository server starts normally, information is output to the system log.

If the authentication server and repository server have been set up on the same server, both the authentication server and repository server will start automatically when Interstage HTTP Server starts.

Depending on the number of role configuration entries and site configuration entries registered in the SSO repository, delays may be experienced when starting Interstage HTTP Server. If a delay occurs, a message "ihs81364: A timeout occurred." will be displayed on the Interstage Management Console for the server in which the repository server has been installed. If no error message is displayed in the system log, wait for a short time, and then check that the Web server that is integrated with the repository server has started in the [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Name:Status] window.

Starting the SSO Repository Automatically

When a relational database (RDB) is used for the SSO repository, the RDB system does not start automatically when the system starts up. For details on starting the RDB system automatically, refer to the "Directory Service Operator's Guide".

Windows32/64

Service linkage with the SSO repository enables the SSO repository and the repository server, to be started when the service is started. For details regarding service linkage with the SSO repository, refer to "Service Linkage with SSO Repository."

4.1.2 Starting an Authentication Server

To start an authentication server, use the Interstage Management Console on the server where the authentication server has been set up. The repository server must be running correctly in order for the authentication server to operate.

To use Integrated Windows Authentication, the Integrated Windows Authentication application must be running.

For details on starting the Interstage Management Console, refer to the Operator's Guide. For details on using the Interstage Management Console window, refer to the Operator's Guide.

Starting an Authentication Server

Starting Interstage HTTP Server starts the authentication server. Use the Interstage Management Console to select [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Name: Status], and then start Interstage HTTP Server. Select the Web server that is integrated with the authentication server for "Web Server name". If the authentication server starts normally, information is output to the system log.

If the authentication server and repository server are installed on the same server, both the authentication server and repository server will start when the Interstage HTTP Server starts.

Starting an Integrated Windows Authentication application

Use the Interstage Management Console to select [System] > [WorkUnit] > [IJServer Name] > [Operation]. Click [Start] to start the WorkUnit that the Integrated Windows Authentication application has been deployed to.

WorkUnit start user Solaris32/64 Linux32/64

To start a WorkUnit, the WorkUnit start user and effective user or effective group authority of the Web server used by the authentication server must match.

Start the WorkUnit according to the Interstage HTTP Server environment definition file (httpd.conf) User directive or Group directive settings with either of the following users:

- The user specified in the User directive
- The user that belongs to the group specified in the Group directive

Example

To start the WorkUnit using the settings shown below, configure the OS user authority settings so that the 'operator' user belongs to the 'nobody' group.

Table 4.1 Starting the WorkUnit

Interstage HTTP Server Environment Definition File (httpd.conf) Group Settings	WorkUnit Start User
nobody	operator

For details about changing the Web server effective user or effective group, refer to "Changing the Effective User for the Web Server" or "Changing the Effective Group for the Web Server" in "Operation and Maintenance" of the "Single Sign-on Operator's Guide".

4.1.3 Starting a Business Server

The method for starting a business server depends on the Web server where the business server runs. The following examples show how to start a business server for each Web server being used as the business server.

If the business server is started normally, information is output to the system log. The repository server and authentication server must be running correctly in order for the business server to operate.

- If Interstage HTTP Server is used

  To start a business server, use the Interstage Management Console on the server where the business server has been installed. Starting Interstage HTTP Server starts the business server. Use the Interstage Management Console to select [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Name: Status]. Click [Start] to start the business server. Select the Web server that is integrated with the business server for "Web Server name".

  For details on starting the Interstage Management Console, refer to the Operator's Guide. For details on using the Interstage Management Console window, refer to the Operator's Guide.

Windows32/64

- If Microsoft Internet Information Services 6.0 or later is used

  To start a business server, start Microsoft Internet Information Services, and then access the Web server from a Web browser. To start Microsoft Internet Information Services, select 'Start' in 'World Wide Web Publishing Service' in Service.

  For details on starting Microsoft Internet Information Services 6.0 or later, refer to the online help in the Microsoft Internet Information Services.

Solaris32

- If Sun Java System Web Server is used

  Starting Sun Java System Web Server automatically starts a business server. To start Sun Java System Web Server, execute the 'start' shell.

  For details on starting Sun Java System Web Server, refer to the Sun Java System Web Server manual.

Notes

- If the access log file for a business server cannot be initialized, the Web server where the business server is operated has not been started. If the Web server does not start, check the contents of the message starting with SSO output in the system log, and then remove the cause of the problem. For details about the messages, refer to "Messages with Message Number Beginning 'sso'" in Messages.
- If the setting "update the access control information in starting a business server" is selected, start a repository server before starting a business server. For access control information, refer to "Updating Access Control Information".
- After a business server has started, access the protection resource and ensure that authentication and authorization are performed. If authentication and authorization are not performed, the business server environment may be invalid. Check the contents of the message output to the system log, and then remove the cause of the problem. For details about the message, refer to 'Messages Beginning with 'sso'" in Messages.

4.2 Stopping Single Sign-on

This section explains how to stop the servers.

- 4.2.1 Stopping a Repository Server
- 4.2.2 Stopping an Authentication Server
- 4.2.3 Stopping a Business Server

4.2.1 Stopping a Repository Server

To stop a repository server, use the Interstage Management Console on the server where the repository server has been set up. If a repository server is stopped, an authentication server and business server cannot operate. Extreme care must be taken when stopping repository servers.

Before stopping an SSO repository, ensure that the repository server has been stopped.

For details on starting the Interstage Management Console, refer to the Operator's Guide. For details on using the Interstage Management Console window, refer to the Operator's Guide.

Stopping a Repository Server

Stopping Interstage HTTP Server automatically stops a repository server. Use the Interstage Management Console to select [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Name: Status]. Click [Stop] to stop the repository server. Select the Web server that is integrated with the repository server for "Web Server name". If the repository server stops normally, information is output to the system log.

If the Authentication server and Repository server are set up on one server, they are both stopped by stopping Interstage HTTP Server.

Stopping an SSO Repository

Use the Interstage Management Console to select [System] > [Services] > [Repository] > [Repository: View Status] and then stop the SSO repository.

For details on stopping the SSO repository, refer to the Directory Service Operator's Guide.

4.2.2 Stopping an Authentication Server

To stop an authentication server, use the Interstage Management Console on the server where the authentication server has been installed. If an authentication server is stopped, a business server cannot operate. Extreme care must be taken when stopping authentication servers.

To use Integrated Windows Authentication, the Integrated Windows Authentication application must be stopped.

Stopping an Authentication Server

For details on starting the Interstage Management Console and using the Interstage Management Console window, refer to the Operator's Guide.

Stopping Interstage HTTP Server stops an authentication server. Use the Interstage Management Console to select [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Name: Status]. Click [Stop] to stop the authentication server. Select the Web server that is integrated with the authentication server for "Web Server name". If the authentication server stops normally, information is output to the system log.

If the Authentication server and Repository server are set up on one server, they are both stopped by stopping Interstage HTTP Server.

Stopping an Integrated Windows Authentication Application

To stop the WorkUnit, in the Interstage Management Console select [System] > [WorkUnit] > [IJServer Name] > [Operation]. Click [Stop] to stop the WorkUnit that the Integrated Windows Authentication application has been deployed to

4.2.3 Stopping a Business Server

The method for stopping a business server is dependent on the Web server where the business server operates. The following examples show how to stop a business server for each type of Web server on which a business server may operate. If the business server stops normally, information is output to the system log. Stopping the Web server may take several minutes depending on the load status.

- If Interstage HTTP Server is used

  To stop a business server, use the Interstage Management Console on the server where the business server has been installed. Stopping Interstage HTTP Server automatically stops the business server. Use the Interstage Management Console to select [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Name: Status]. Click [Stop] to stop the business server. Select the Web server that is integrated with the business server for "Web Server name".

  For details on starting the Interstage Management Console and using the Interstage Management Console window, refer to the Operator's Guide.

Windows32/64

- If Microsoft Internet Information Services is used

  Stopping Microsoft Internet Information Services automatically stops a business server. To stop Microsoft Internet Information Services, select 'Stop' in 'World Wide Web Publishing Service' in Service.

  For details on stopping Microsoft Internet Information Services, refer to the online help in the Microsoft Internet Information Services.

Solaris32

- If Sun Java System Web Server is used

  Stopping Sun Java System Web Server automatically stops a business server. To stop Sun Java System Web Server, execute the 'stop' shell.

  For details on stopping Sun Java System Web Server, refer to the Sun Java System Web Server manual.

4.3 Changing Environment Settings

This section explains how to change the operating environments of the repository server, authentication server, and business server after environment setup.

- 4.3.1 Changing the Environment Settings of Repository Server, Authentication Server and Business Server
- 4.3.2 Changing the Effective User for the Web Server
- 4.3.3 Changing the Effective Group for the Web Server

4.3.1 Changing the Environment Settings of Repository Server, Authentication Server and Business Server

To change the environment settings of the repository server, authentication server, or business server, use the following tabs on the Interstage Management Console. Select the server whose environment setting requires changing in the bold portion.

The following settings are changed by the SSO administrator:

- Repository server

  [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab

- Authentication server

  [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab

The following settings are changed by the Business server administrator:

- Business server

  `[System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab

If the environment settings of the repository server, authentication server, and business server have been changed, stop and then restart the servers. (*1)

Solaris32/64 Linux32/64

*1 If the settings are changed in an environment in which multiple business servers are built on one machine, then stop/start them.

If the Java application using JavaAPI provided by Single Sign-on has been used to change the setting of [Notify User Information?] in [Linkage with Web applications] during environment setup of business server, the Java application must be restarted to enable the change.

Notes

- If the SSL environment setting used by an authentication server has been changed, stop and then restart the authentication server. To change the SSL environment setting, use the following tab on the Interstage Management Console:

  [System] > [Security] > [SSL] > [Configuration Name] > [SSL Settings] tab

- If the following settings of the repository server (update system) have been changed using the Interstage Management Console, take action according to the repository server structure.

  - User information registration entry
  - Role configuration registration entry
  - Protection resource registration entry

- Extended user information

    - Structure in which repository servers (update system) is increased for load balancing

      Modify the settings of all the repository servers (update system) that are being used for load balancing in the same way.

    - Structure in which load balancing is used for repository server (update system) and repository server (reference system)

      Create the repository server (reference system) again.

      For details on creating the repository server (reference system), refer to "Adding a Repository Server (Reference System)".

4.3.2 Changing the Effective User for the Web Server

Solaris32/64 Linux32/64

This section provides notes on changing the effective user for the Web server.

Change the Web server effective user according to the following procedure.

To Change the Effective User for the Repository Server

1. Set the name of the Interstage HTTP Server effective user to be changed in the User directive of the Interstage HTTP Server environment definition file (httpd.conf).
2. After the effective user of the Web server is changed, use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and then click the [Update] button.

To Change the Effective User for the Authentication Server

1. Set the name of the Interstage HTTP Server effective user to be changed in the User directive of the Interstage HTTP Server environment definition file (httpd.conf).
2. After the effective user of the Web server is changed, use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab, and then click the [Update] button.

To Change the Effective User for the Business Server

If Interstage HTTP Server is used

1. The effective user name of the Web server (Interstage HTTP Server) can be set using the User directive in the environment definition file (httpd.conf) for the Interstage HTTP Server.
2. After the effective user of the Web server is changed, use the Interstage Management Console to select the [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab, and then click the [Update] button.

If Sun Java System Web Server is used Solaris32

1. The effective user name of the Sun Java System Web Server can be set using the User Directive in the configuration file (magnus.conf) for the Sun Java System Web Server.
2. After the effective user of the Web server is changed, use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab, and then click [Detailed Settings [Show]]. Specify the effective user name set in the Web server configuration file for [Effective user name] in [Web Server used] of [Web Server Settings], and then click the [Update] button.

Notes

If multiple business servers operate on one server, specify as follows:

- Specify the same effective user as for the Interstage HTTP Server of the Sun Java System Web Server.

For example, the relationship between effective users set in the configuration files of Web servers and effective users set on the Interstage Management Console is shown in the following table.

Table 4.2 Relationship Between Effective Users

Web server	Effective user of Web server	Setting on Interstage Management Console
Interstage HTTP Server	nobody	Setting disabled (the value in the left column is automatically set)
Sun Java System Web Server	nobody	nobody

4.3.3 Changing the Effective Group for the Web Server

Solaris32/64 Linux32/64

Change the Web server effective group according to the following procedure.

To Change the Effective Group for the Authentication Server

1. Set the name of the Interstage HTTP Server effective group to be changed in the Group directive of the Interstage HTTP Server environment definition file (httpd.conf).
2. After the effective user of the Web server is changed, use the Interstage Management Console to select the [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab, and then click the [Update] button.

4.4 Deleting Single Sign-on

This section explains how to delete the servers:

- 4.4.1 Deleting the Repository Server
- 4.4.2 Deleting the Authentication Server
- 4.4.3 Deleting the Business Server

4.4.1 Deleting the Repository Server

The Repository server is deleted according to the procedure described below.

After the Repository server is deleted, the Authentication server and Business server can no longer be operated. For this reason, take care when deleting the Repository server.

Deleting the Repository Server (Update System)

1. Stop the Repository server (update system).

   For details about stopping the Repository server (update system), refer to 4.2.1 Stopping a Repository Server.
2. In the Interstage Management Console of the machine used to set up the Repository server (update system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [List], and select the Repository server (update system) to be deleted.
3. Click [Delete].
4. Delete the SSO repository information used by the Repository server (update system) if necessary.

Deleting the Repository Server (Reference System)

1. Stop the Repository server (reference system).

   For details about stopping the Repository server (reference system), refer to 4.2.1 Stopping a Repository Server.
2. In the Interstage Management Console of the machine used to set up the Repository server (reference system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [List], and select the Repository server (reference system) to be deleted.
3. Click [Delete].

4. Delete the SSO repository information used by the Repository server (reference system) if necessary.

5. In the Interstage Management Console of the machine used to set up the Authentication server, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]].

6. If the URL of the deleted Repository server (reference system) is set in [Communication Settings with Repository server (reference system)] > [Repository server (reference system) URL], delete all of the URLs and then click [Update].

7. Restart the Authentication server.

4.4.2 Deleting the Authentication Server

The Authentication server is deleted according to the procedure described below.

After the Authentication server is deleted, the Business server can no longer be operated. For this reason, take care when deleting the Authentication server.

To use Integrated Windows Authentication, the Integrated Windows Authentication application must be deleted.

Deleting the Authentication Server

1. Stop the Authentication server.

   For details about stopping the Authentication server, refer to 4.2.2 Stopping an Authentication Server.

2. In the Interstage Management Console of the machine used to set up the Authentication server, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [List], and select the Authentication server to be deleted.

3. Click [Delete].

Deleting an Integrated Windows Authentication Application

Use the Interstage Management Console to select [System] > [WorkUnit] > [IJServer Name] > [Operation]. Click [Delete] to delete the WorkUnit that the Integrated Windows Authentication application has been deployed to.

4.4.3 Deleting the Business Server

The Business server administrator deletes the Business server according to the following procedure:

1. Stop the Business server to be deleted. The method for stopping the Business server depends on the Web server used to integrate the Business server.

   For details about stopping the Business server, refer to 4.2.3 Stopping a Business Server.

2. In the Interstage Management Console of the machine used to set up the Business server, click [System] > [Security] > [Single Sign-on] > [Business system] > [List], and select the Business system to be deleted.

3. Click [Delete].

   Solaris32/64 Linux32/64

4. If there are other business servers built on the machine, then restart them.

If the Business server is operated in the following Web servers after completing the above tasks, delete the settings made for integration with the Web server and then delete the integration.

- Interstage HTTP Server 2.2
- Microsoft(R) Internet Information Services 6.0
- Microsoft(R) Internet Information Services 7.0
- Microsoft(R) Internet Information Services 7.5
- Microsoft(R) Internet Information Services 8.0

- Sun Java System Web Server 6.1

Next, the SSO administrator deletes the Business server Site definition according to the following procedure:

1. In the Interstage Management Console of the machine used to set up the Repository server (update system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository Server] > [Protection Resource] > [Protection Resource:List], and select the Site definition of the deleted Business server.
2. Click [Delete].

Note

If session management is not used, delete Site definition and protection path information set in the Authentication server definition file for the deleted Business server.

For details about the Authentication server definition file settings, refer to Appendix E, "Settings for Protection Resource in Authentication server".

4.5 User Related Operation

This section explains how to manage user-related operations. Single Sign-on users are managed in the SSO repository. To add a user, add the user entry to the user information in the SSO repository and specify the user ID, password, and role name.

The user session can be managed to reduce the risk of illegal access by another user by "spoofing".

4.5.1 Adding a User

To add a user entry to the user information managed in the SSO repository, use the user program. For details about the user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

When adding a user entry, note the following points:

- If the authentication method is "certificate authentication" or "password authentication and certificate authentication," a certificate must be distributed to the user.
- If the authentication method is "password authentication or certificate authentication," a certificate must also be distributed to a certificate authenticated user.
- The addition of new users is effective immediately. The repository server, authentication server, and business server need not be running.

For details on adding a user to the SSO repository, refer to "Registering User Information and Role Configuration in the SSO Repository".

4.5.2 Deleting a User

To delete a user entry from the user information managed in the SSO repository, use the user program. For details about the user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

Deletion of users is effective immediately. The repository server, authentication server, and business server need not be running.

4.5.3 Amending the Role of a User

If the section or title of a user changes, the accessible resources can be amended by changing or adding a user role.

To change or add a user role use the user program. For details about user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

4.5.4 Changing User Passwords

To change a user password managed in the SSO repository, use the user program. For details about user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

Note

When changing user passwords managed in the SSO repository, pay careful attention to password security.

For details on password security refer to "Security Risks" - "Interstage Single Sign-on" - "Security Measures" in the Security System Guide.

4.5.5 Taking Corrective Action if the User Password is Forgotten

If a user password managed in the SSO repository is forgotten, a new password must be set. To set a new password, use the user program. For details about user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

Note

When setting new user passwords managed in the SSO repository, pay careful attention to password security.

For details on password security refer to "Security Risks" - "Interstage Single Sign-on" - "Security Measures" in the Security System Guide.

4.5.6 User Lock

To lock a user by force, use the user program. For details about the user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

4.5.7 Canceling Lockout

The Interstage Management Console is used to release lockout as follows:

1. Select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Release User Lock] tab, and then specify the ID of the user whose lockout is to be released.
2. Clicking the [Search] button displays information about the specified user.
3. Check the user information, and then click the [Apply] button.

If the user is locked out because the password is forgotten, the user password can be reset by setting a new password.

To reset a password, use the user program. For details about user program refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

Notes

- When resetting a password, pay careful attention to password security.

  For details on password security refer to "Security Risks" - "Interstage Single Sign-on" - "Security Measures" in the Security System Guide.

- If the Interstage Management Console has been used to release user lockout, the consecutive failure count will also be cleared.

4.5.8 Checking User Lock Status

To check the user lock status, use the user program. For details about user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

To release a user lockout refer to "Canceling Lockout".

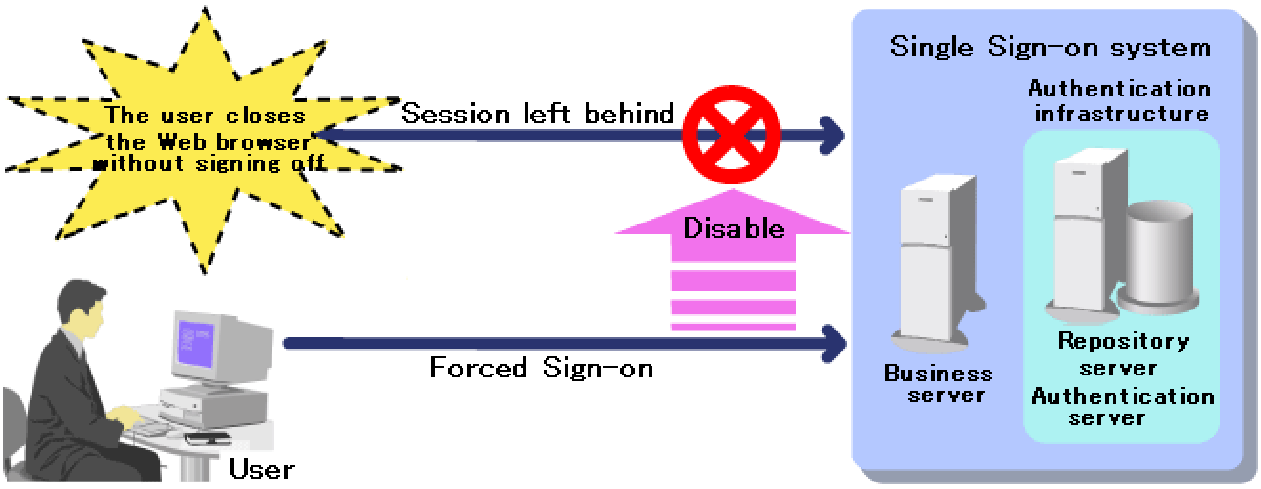
4.5.9 Checking and Changing User Validity Period

To check and change the user validity period, use the user program. For details about user program, refer to "Preparation for a User Program" in the chapter "Environment Setup (SSO Administrators)".

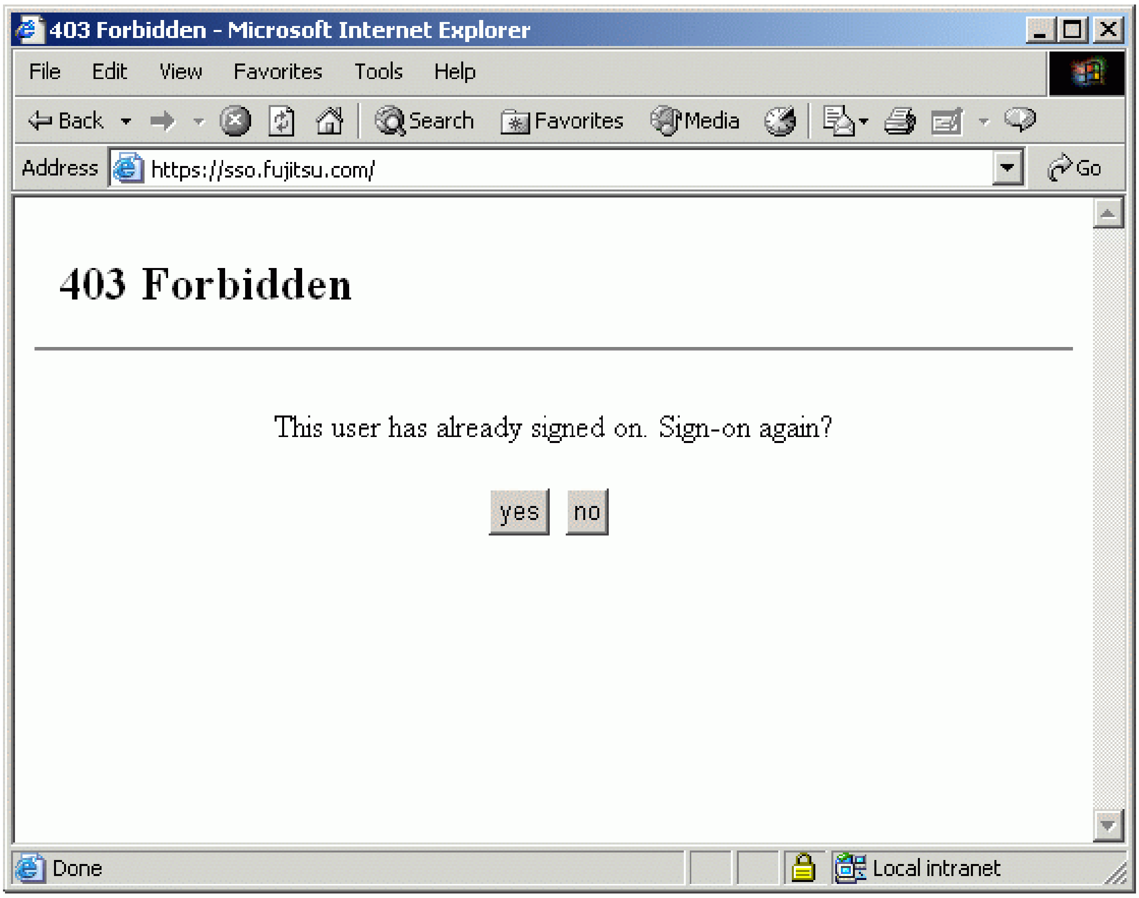
4.5.10 Forced Sign-on

While using Business server contents, if the user closes the Web browser without signing off, an unneeded session may be left open. This makes it impossible to sign on again with the same user ID.

Using Forced Sign-on, the user can sign on again with the same user ID without needing to wait for the session to be automatically disabled or needing to ask the SSO administrator to disable the session. In this situation, a session that is not needed is automatically disabled.



If a user signs on with the user ID of an already signed-on user, the Forced Sign-on confirmation page, shown below, opens.



403 Forbidden

This user has already signed on. Sign-on again?

The options provided by the buttons on the Forced Sign-on confirmation page are described below:

- "Yes" is clicked

  Forced Sign-on is performed.

  The session already in use with the same user is disabled.

  If the Business server contents are accessed, they are displayed in the user Web browser. If the Authentication infrastructure is accessed directly, and the authentication was successful, the page opens.

- "No" is clicked

  Forced Sign-on is cancelled.

  A Sign-off cancellation message is output in the user Web browser.

The Forced Sign-on confirmation page message can be customized by editing the following message file that is stored on the Authentication server:

- 200queryforcedsignon_en.template

For details about the customization method for messages on the Forced Sign-on confirmation page, refer to "Customizing messages Displayed on a Web browser" in "Single Sign-on Customization".

To use Forced Sign-on, in the Interstage Management Console of the machine used to set up the Repository server (update system) click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Session management detailed settings [Show]] > [Sign-on] > [Use Forced Sign-on?], and set "Yes".

For details about options and the method settings, refer to the Operator's Guide.

4.5.11 Forced Sign-off

If illegal access (a session) from another user by "spoofing" is detected when a user query is received, the SSO administrator can sign off the illegal sessions by force and block access from Single Sign-on systems without stopping the Business server. It is possible to perform Forced Sign-off for a specific user as well as a specific session.

"Spoofing" can be detected from the Business server or Authentication server access log information in the cases shown below:

For details about access log reference, refer to "Maintenance Using Access Logs".

- Access to the Single Sign-on system from a non-network IP address.
- Access from an unused IP address.

In Interstage Single Sign-on, the "ssosignoff" Forced Sign-off command is offered to sign off illegal sessions by force.

For details about the Forced Sign-off command, refer to "Single sign-on Operation Commands" in the "Reference Manual (Command Edition)".

Notes

- After Forced Sign-off is performed, ask the user to change his/her password.

  Take care to avoid password attacks when the password is changed. For details about the measures that can be taken to avoid password attacks, refer to "Security Risks" - "Interstage Single Sign-on" - "Security Measures" in the "Security System Guide".

- To use load balancing when more than one repository server (update system) is deployed, execute the ssosignoff command in the repository server (update system) used to manage the session. This repository server (update system) can be checked using the following:

  - The "Server" output in the business server access log
  - The "Session ID" output in the session management log

  When the repository server (update system) that manages the session cannot be checked in the business server access log, execute the ssosignoff command in all the repository servers (update system).

4.5.12 Checking the Time of the Previous Sign-on

The user can check the time of the previous Sign-on according to the methods shown below.

- Accessing the authentication infrastructure URL.

  If a user that is already signed on uses the Web browser to access the following authentication infrastructure URL, the Notice window for the time of the previous Sign-on opens.

  ```
  Authentication infrastructure URL/ssoatcag?fj-is-sso-request=last-signon-time (*1)(*2)
  ```

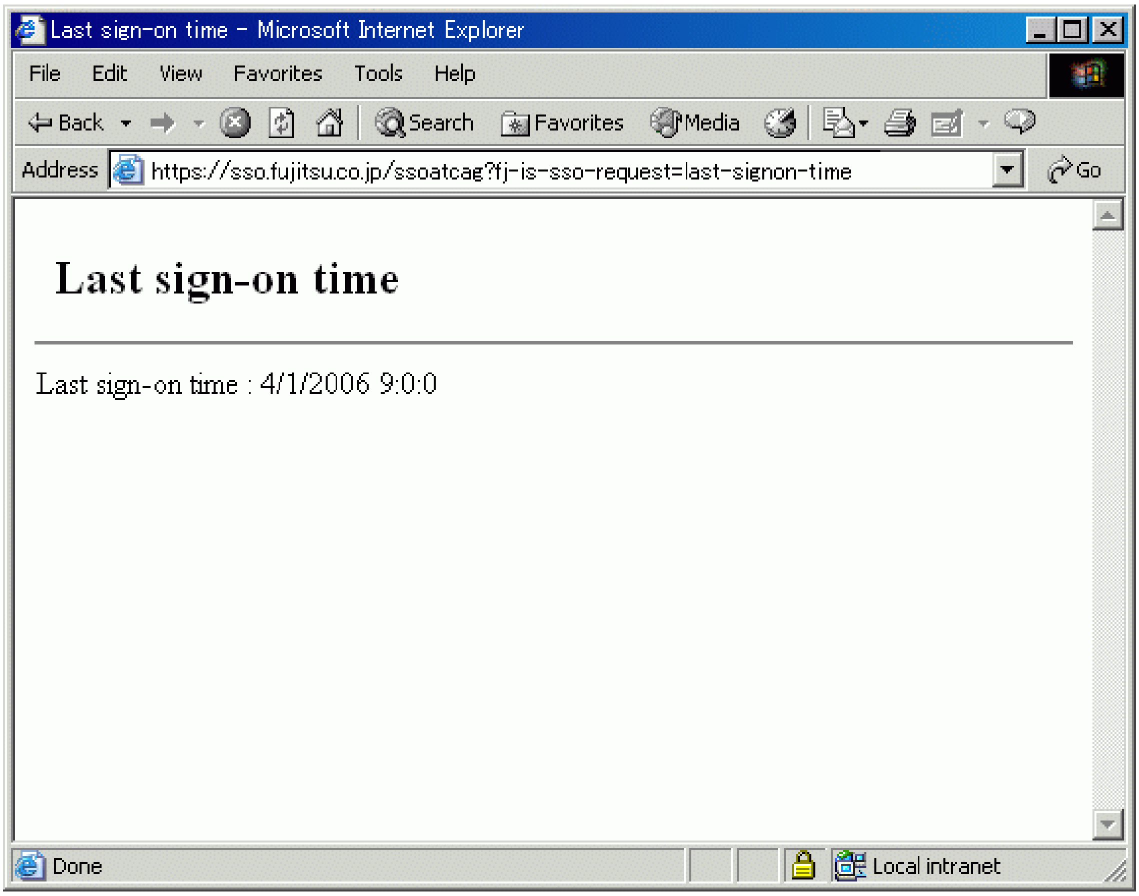
  *1 Specify the port number of Authentication infrastructure URL even if 443 is specified.

  *2 If the Authentication infrastructure URL is confirmed after setting the business server, on the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]], and then check the setting for [Authentication infrastructure URL] under [Authentication Infrastructure Information Settings].

  The SSO administrator can customize the Notice window for the time of the previous Sign-on by editing the following message file that is stored on the Authentication server:

  - 200lastsignontime_en.template

For details about the customization method, refer to "Customizing Messages Displayed on a Web browser", in "Single Sign-on Customization".


Last sign-on time - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.co.jp/ssoatcag?fj-is-sso-request=last-signon-time
Go
Done
Local intranet

Last sign-on time

Last sign-on time : 4/1/2006 9:0:0

- Checking the Business system window.

  The Business server administrator embeds the time of the previous Sign-on that was obtained in the Business system contents. This means that, for example, the time of the previous Sign-on can always be displayed in the Business system window.

  The user can find out the time of the previous Sign-on just by checking the Business system window.

  For details about the Web applications for which time of the previous Sign-on can be obtained, refer to "Setting User Information Report with Environment Variables" in "Developing Applications".

4.6 Authorization-related Operation

This section explains changing role configurations and protection resources.

- 4.6.1 Amending Role Configurations
- 4.6.2 Amending Protection Resource

4.6.1 Amending Role Configurations

Role configuration amendments may be required due to organization change.

The role configuration is changed or added as follows:

The SSO administrator uses the SSO repository and repository server as follows:

1. Change or add the role configuration in the SSO repository.
2. Change or add the role to set in the path configuration of the protection resource as required.
3. Change or add the role to set in the user information entry as required.

4. Use the repository server to retrieve role information and update the cache.

   Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Update Role information] tab, and then click the [Update] button.

   If more than one repository server is used for load balancing, update the cache on all the repository servers.

5. Request the business server administrator to update the access control information.

The business server administrator then operates the business server as follows: (*1).

1. Update access control information on the business server.

   Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Update access control information] tab, and then click the [Update] button to update the access control information.

*1 If "Execute when business server is started" is selected in [Update access control information] in the business server environment setup, this operation is required only when the business server is running. If "Execute manually as needed" is selected, this operation is required regardless of whether the business server is running or stopped.

For details about the setting [Update access control information], refer to "Updating Access Control Information".

For details about the role of the SSO repository, refer to "Role Configuration Entry"'.

Notes

- If more than one repository server is used for load balancing, change or add roles during off-peak hours (e.g. night hours) when only a few users are accessing the servers.
- Changing the role configuration in the SSO repository and then updating the role information in the repository server will not reflect the changes in the authorization operation of the business server. After role information in the repository server is updated, the access control information must be updated on the business server.
- If access control information is updated and an error message is output, the business server remains in the state where it performs authorization according to the previous access control information. Correct the error, and then stop the business server as required until the access control information is updated normally.

4.6.2 Amending Protection Resource

If the user issues a request to access resources such as a Web application in a business server, the business server determines whether the resource is an authentication or authorization target based on the protection resource. If the business server determines that the resource is an authentication or authorization target, it performs authentication and determines whether the user can access the resource based on the user information and role managed in the SSO repository.

The SSO administrator amends protection resources in the SSO repository as follows:

1. Change the protection resource in the SSO repository.

   For details on how to change the resource, refer to 'Registering Site Configuration of Business System' and 'Registering Protection Path' under Environment Setup (SSO Administrators)

2. Request the business server administrator to update access control information.

The business server administrator then operates the business server as follows: (*1)

1. On the business server, use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Update access control information] tab, and then click the [Update] button to update the access control information.

*1 If [Update access control information] in the business server environment setup is set to "Execute when business server is started," this operation is required only when the business server is running. If it is set to "Execute manually as needed"," this operation is required regardless of whether the business server is running or stopped.

For details about setting for [Update access control information], refer to "Updating Access Control Information".

For details about the protection resource in the SSO repository, refer to "Protection resource" in "Information Required for Authorization Using Roles".

Remark

If session management is not used, the Business server protection resource information set in the Authentication server definition file must be changed after the SSO repository protection resources are changed. For details about the Authentication server definition file settings, refer to "Authentication server protection resource settings".

Notes

- If more than one repository server is used for load balancing, amend the role during the off-peak hours (for example, night hours) when only a few users are accessing the servers.
- Amendments to protection resource information in the SSO repository will not reflect in the authorization operation of the business server without updating access control information. On the business server, update access control information.
- If an error message is output when access control information is updated, the business server remains in the state where the server performs authorization according to the previous access control information. Correct the error by stopping and restarting the business server as required until access control information is updated normally.

4.7 Maintenance Using Access Logs

Interstage Single Sign-on records authentication and authorization processing performed by the repository server, authentication server, and business server as access logs. An access log (containing authentication and authorization results, date and time, access source identification information and user identification information) is recorded for each server. Each access log is output as a text file with one record per line.

For details on access logs, refer to Messages Logged and Output in Single Sign-on in the Messages manual. Use the Interstage Management Console of each server to specify the access log output destination file name, maximum file size, and preferred saving method. These methods are described below;

For details about the configuration of the Interstage Management Console, refer to the Operator's Guide.

- Repository Server

  [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab > [Access Log Settings]

- Authentication Server

  System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Access Log Settings]

- Business Server

  [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab > [Access Log Settings]

4.8 Maintenance Using Session Management Logs

In Interstage Single Sign-on, update of the session is recorded as a session management log. The session management log is recorded in the session management server and outputs the update of the session as a text file with one record per line.

For details on access logs, refer to "Messages Logged and Output in Single Sign-on" in the Messages manual. Use the Interstage Management Console of the repository server (update system) to specify the session management log output destination file name, maximum file size, and preferred saving method. These methods are described below;

- [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings].tab > [Session management Log Settings]

For details about the configuration of the Interstage Management Console, refer to the Operator's Guide.

4.9 Operating Notes for Large Systems

For operation using large systems, note the following points:

- To update the SSO repository information in the repository server (update system), check whether operation stopped because of a problem such as the SSO repository being down in the repository server (reference system). If the SSO repository is stopped, start it immediately.

- If the repository server (reference system) stays down for an extensive period of time, the data integrity of the SSO repository may not be guaranteed. If irep15071 is output to the system log of the repository server (update system), check the message contents and recover SSO repository data. For details about messages output to the system log, refer to "Messages with Message Number Beginning 'irep'" in Messages.

  If irep15071 is not output, restore the repository server (reference system). The update of the SSO repository of the repository server (update system) is reflected in the SSO repository of the repository server (reference system). The reflection is completed when the last update information output to the access log of the SSO repository of the repository server (update system) is output to the access log of the SSO repository of the repository server (reference system).

Chapter 5 Single Sign-on Customization

This chapter explains Interstage Single Sign-on Customization and includes the following sections:

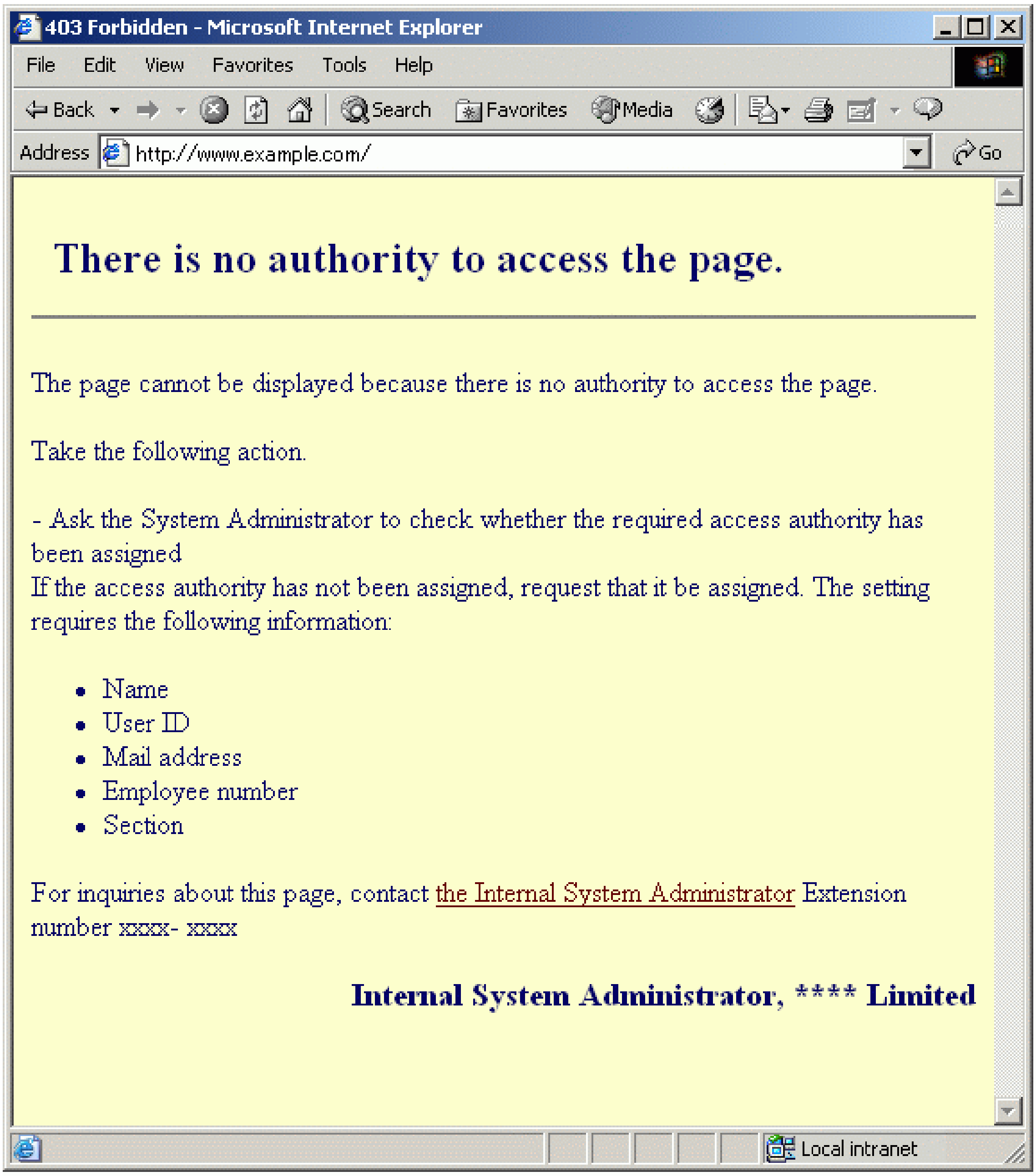
5.1 Customizing Messages Displayed on a Web Browser

Interstage Single Sign-on provides a function that customizes messages to be displayed on a Web browser. Specifically, the messages displayed on a Web browser can be changed as required by editing the message file in HTML format.

For example, this function enables messages displayed on the Web browser to include the destination specific information) and also mail used for direct inquiries. Using this function, the contents of a message can be modified to include more detailed information.

The following figure shows an example of a customized message:

Figure 5.1 Error Message Example


403 Forbidden - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.example.com/ Go
Local intranet

There is no authority to access the page.

The page cannot be displayed because there is no authority to access the page.

Take the following action.

- Ask the System Administrator to check whether the required access authority has been assigned
If the access authority has not been assigned, request that it be assigned. The setting requires the following information:

- Name
- User ID
- Mail address
- Employee number
- Section

For inquiries about this page, contact the Internal System Administrator Extension number xxxx- xxxx

Internal System Administrator, ** Limited**

5.1.1 Messages that can be Customized

Interstage Single Sign-on enables the customization of the following messages.

- Messages Displayed for Form Authentication
- Authentication Error Messages
- Messages Displayed for Integrated Windows Authentication
- Authorization Error Messages

Messages are customized by editing the message file in HTML format.

Messages Displayed for Form Authentication

Messages displayed for form authentication can be customized. Customize the messages on the machine on which the authentication server was built while the authentication server is stopped.

If an authentication server has already been added for load balancing, also customize the messages for the added authentication server. When customizing the messages for the added authentication server, copy them from the export machine to the import machine (added authentication server).

The message file is stored in the directory shown below. When editing messages, refer to "5.1.9 Setting Access Authority for a Message File" to confirm message file access authorization.

Message file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\pub\template\
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/pub/template/
```

If the message file is corrupted because of an incorrect action, copy the original file shown below to the message file storage directory and use the copied version.

Original file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\pub\original\template\
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/pub/original/template/
```

Table 5.1 Form Authentication Messages

No.	Cause of the message to be displayed	Message Contents	Message File Name
1	Sign-on has been performed directly from the form authentication page with no protection resource accessed.	Welcome to Single Sign-on.	200auth_succeeded_en.template (*2)
2	The sign off it did.	The sign off it did.	200signoff_en.template (*2)
3	The time of the previous Sign-on was notified.	Last sign-on time : MM/DD/ YYYY hh:mm:ss	200lastsignontime_en.template (*2)(*3)
4	Form authentication was performed.	Enter your user name and password.	200auth_form_en.template (*4)
5	The user name or password is incorrect, or user information corresponding to the certificate could not be found.	User name or password is incorrect.	200passwderr_form_en.template (*4)
6	Authentication needs to be re-started because the authentication information is invalid, possibly due to term expiration.	Authentication has been expired.	200authexpired_en_template (*4)
7	Confirm whether or not you want to sign off.	Sign off?	200querysignoff_en.template (*2)(*5)
8	There was a timeout because Idle Monitoring Time was exceeded. For this reason, the authentication procedure must be performed again.	Timed out, session is unavailable.	200timedout_en.template (*4)
9	The user is already signed on. Confirm whether or not you want to sign on again.	This user has already signed-on. Sign-on again?	200queryforcedsignon_en. template (*2) (*6)

No.	Cause of the message to be displayed	Message Contents	Message File Name
10	Authentication was performed on more than one page at the same time. Alternatively, another protection resource was accessed during authentication.	Waiting for authentication from another window or page... If authentication is not already in progress, click the following button to continue authentication processing.	200check_duplication_auth_en.template (*2)(*7)
11	The form authentication page was accessed when authentication had already taken place.	User was already authenticated.	403alreadyauth_en_template (*2)
12	Integrated Windows Authentication failed.	Authentication failed.	403auth_failed_en.template (*2)
13	The correct certificate was not used for authentication or the relevant user information is not contained in the certificate.(*1)	Certificate authentication is needed.	403requestcert_en.template (*2)
14	The specified certificate is damaged or user identification information is not contained in the certificate.	Certificate is invalid.	403certinvalid_en.template (*2)
15	The certificate has expired.	Certificate has expired.	403certexpired_en.template (*2)
16	The specified certificate has been revoked.	Certificate has been revoked.	403certrevoke_en.template (*2)
17	The user was locked out because the password was re-entered more than the allowed number of times. (*1)	User was locked out.	403locked_en.template (*2)
18	Resources managed by Interstage Single Sign-on could not be accessed because the user was locked out. (*1)	User has been locked.	403alreadylocked_en.template (*2)
19	The specified resource could not be accessed because a user identification was registered delicately (*1).	User is duplicated.	403notspecified_en.template (*2)
20	The user cannot access the resource managed by Interstage Single Sign-on because the validity period has not started or has expired. (*1).	User is not available.	403notavailable_en.template (*2)
21	The user information is not contained in the SSO repository (*1).	User has not been found.	403noentry_en.template (*2)
22	A request was made for a service by a user that is already signed on, but Sign-on was not completed.	Sign-on is not done.	403notsignon_en.template (*2)
23	Sign-off was canceled in the Sign-off confirmation window.	Sign-off was canceled.	403cancelesignoff_en.template (*2)
24	Forced Sign-on was canceled in the Forced Sign-on confirmation window.	Sign-on was canceled.	403cancelforcedsignon_en. template (*2)
25	An attempt was made to sign on even though the user is already signed on. The Sign-on attempt was not successful because multiple Sign-on is prohibited.	Failed to Sign-on. This user has already signed-on.	403session_already_exist_en. template (*2)

No.	Cause of the message to be displayed	Message Contents	Message File Name
26	Could not sign off because information required for sign off has been lost.	Failed to Sign-off. Please close web browser.	403signoff_failed_en.template (*2)
27	An internal error occurred during the Single Sign-on operation.	An internal error has occurred.	500internalerr_en.template (*2)

*1 If [No] is specified for [Notify Cause of Authentication Failure to user?], when the authentication server environment is set up this message is incorporated into the message: "User name or password is incorrect."

To specify [Notify Cause of Authentication Failure to user?], use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]], and then set [Communication Settings with Business system].

*2 This message file must not contain the authentication form tag, otherwise authentication may not be executed correctly

*3 The time of the previous Sign-on is automatically embedded in this message file.

*4 A form tag for authentication must already exist in this message file. For details on how to specify the authentication form tag, refer to 5.1.3 Authentication Form Tag Specifications

*5 A form tag for sign-off confirmation must already exist in this message file. For details on how to specify the authentication form tag, refer to 5.1.5 Sign-off Confirmation Window Form Tag Specifications.

*6 A form tag for forced Sign-on confirmation must already exist in this message file. For details on how to specify the authentication form tag, refer to 5.1.4 Forced Sign-on Confirmation Window Form Tag Specifications.

*7 A tag for simultaneous authentication confirmation is already contained in this message file. For details on simultaneous authentication confirmation tag specifications, refer to "Simultaneous Authentication Confirmation Window Tag Specifications".

Authentication Error Messages

Messages that are displayed when authentication errors occur can be customized. The types of error messages are displayed in the following table. Customize the messages on the server where the authentication server is set up and stopped.

If an authentication server has been added for load balancing purposes, also customize the messages for the additional authentication server. To customize error messages for the additional authentication server, copy the error messages from the export machine to the import machine (the additional authentication server).

The message file is stored in the directory shown below. When editing messages, refer to "5.1.9 Setting Access Authority for a Message File" to confirm message file access authorization.

Message file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\pub\template\
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/pub/template/
```

If the message file is corrupted because of an incorrect action, copy the original file shown below to the message file storage directory and use the copied version.

Original file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\pub\original\template\
```

Solaris32/64 Linux32/64

```
/opt/FJSVssoac/pub/original/template/
```

Table 5.2 Authentication Error Messages

No.	Cause of Error	Message Contents	Message File Name
1	Authentication was performed on more than one page at the same time. Alternatively, another protection resource was accessed during authentication.	Waiting for authentication from another window or page... If authentication is not already in progress, click the following button to continue authentication processing.	200check_duplication_auth_en.template (*2)
2	The user name or password is invalid or the relevant user information is not contained in the certificate.	User name or password is incorrect.	401passwderr_en.template
3	Integrated Windows Authentication failed.	Authentication failed.	403auth_failed_en.template
4	The correct certificate was not used for authentication or the relevant user information is not contained in the certificate. (*1)	Certificate authentication is needed.	403requestcert_en.template
5	The specified certificate is damaged or user identification information is not contained in the certificate.	Certificate is invalid.	403certinvalid_en.template
6	The certificate has expired.	Certificate has expired.	403certexpired_en.template
7	The specified certificate has been revoked.	Certificate has been revoked.	403certrevoke_en.template
8	The user was locked out because the password was re-entered more than the allowed number of times. (*1)	User was locked out.	403locked_en.template
9	Resources managed by Interstage Single Sign-on could not be accessed because the user was locked out. (*1)	User has been locked.	403alreadylocked_en.template
10	The specified resource could not be accessed because a user identification was registered delicately (*1).	User is duplicated.	403notspecified_en.template
11	The user cannot access the resource managed by Interstage Single Sign-on because the validity period has not started or has expired. (*1).	User is not available.	403notavailable_en.template
12	The user information is not contained in the SSO repository (*1).	User has not been found.	403noentry_en.template
13	Sign-off failed because necessary information was not found.	Failed to Sign-off. Please close web browser.	403signoff_failed_en.template
14	An internal error occurred during the Single Sign-on operation.	An internal error has occurred.	500internalerr_en.template

*1 When the authentication server environment is set up, if [No] is specified for [Notify Cause of Authentication Failure to user?], this message is incorporated into the message: "User name or password is incorrect".

To specify [Notify Cause of Authentication Failure to user?], use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] > [Detailed Settings [Show]], and then set [Communication Settings with Business system].When editing the messages, refer to "Setting Access Authority for Message Files" to check the access authority for message files. The relevant message files are contained in the following directories.

*2 A tag for simultaneous authentication confirmation is already contained in this message file. For details on simultaneous authentication confirmation tag specifications, refer to "Simultaneous Authentication Confirmation Window Tag Specifications".

Messages Displayed for Integrated Windows Authentication

Messages displayed for Integrated Windows Authentication can be customized. Customize the messages on the machine on which the authentication server was built while the authentication server is stopped.

If an authentication server has already been added for load balancing, also customize the messages for the added authentication server. To do this, copy them from the export machine to the import machine (added authentication server).

The message file is stored in the directory shown below. When editing messages, refer to "5.1.9 Setting Access Authority for a Message File" to confirm message file access authorization.

Message file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\webapps\winauth\custom\page\
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/webapps/winauth/custom/page/
```

If the message file is corrupted because of an incorrect action, copy the original file shown below to the message file storage directory and use the copied version.

Original file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\webapps\winauth\original\page\
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/webapps/winauth/original/page/
```

Table 5.3 Errors and Corresponding Message Information

No.	Cause of Error	Message Contents	Message File Name
1	For the first authentication, confirm whether or not you want to sign on using Integrated Windows Authentication.	Do you want to sign on using Integrated Windows Authentication?	200_confirm_winauth_en.html(*1)
2	Since the idle monitoring time has been exceeded and a timeout has occurred, confirm whether or not you want to sign on using Integrated Windows Authentication.	Timed out, session is unavailable. Do you want to sign on again using Integrated Windows Authentication?	200_confirm_timeout_en.html(*1)
3	Since the authentication validity period has expired, confirm whether or not you want to sign on using Integrated Windows Authentication.	Authentication has been expired. Do you want to sign on again using Integrated Windows Authentication?	200_confirm_expired_en.html(*1)
4	Sign-on using Integrated Windows Authentication was canceled.	Sign-on using Integrated Windows Authentication was canceled.	200_winauth_cancel_en.html
5	The browser has not been configured to use Integrated Windows Authentication.	User authentication is required.	401_request_winauth_en.html
6	Integrated Windows Authentication failed.	Integrated Windows Authentication failed.	403_winauth_failed_en.html
7	Authentication requests cannot be received	Invalid operation.	403_winauth_invalid_en.html
8	An internal error occurred during the Single Sign-on operation.	An internal error has occurred.	500_internal_error_en.html (*2)

*1 Tags for the messages displayed for Integrated Windows Authentication are already embedded in this message file. For details about specifying tags for messages displayed for Integrated Windows Authentication, refer to '5.1.8 Specifying Tags for Messages Displayed for Integrated Windows Authentication'.

*2 Customize this message file so that the file size is at least 512 bytes. It if is less than 512 bytes, the customized message file may not display correctly.

Authorization Error Messages

Messages that are displayed when authorization errors occur can be customized. The types of error messages are displayed in the following table. The messages can be customized for each operation server. Customize the messages on the server where the business server is set up and stopped.

If a business server has been added for load balancing purposes, also customize the messages for the additional business server. To customize error messages for the additional business server, copy the error messages from the export machine to the import machine (the additional business server).

The message files are saved in the following directories. When editing the messages, refer to "Setting Access Authority for Message files" to check the access authority for message files.

Message file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatzag\pub\template\
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoaz/pub/template/
```

If the message file is corrupted because of an incorrect action, copy the original file shown below to the message file storage directory and use the copied version.

Original file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatzag\pub\original\template\
```

Solaris32/64 Linux32/64

```
/opt/FJSVssoaz/pub/original/template/
```

Table 5.4 Authorization Error Messages

No.	Cause of Error	Message Contents	Message File Name
1	The POST request was authenticated.	Click the link below to open the Authentication window. Check that the authentication server is correct, and then complete the authentication procedure.	200postauth_en.template (*1)
	There was an Idle Monitoring timeout when the POST request was made.		
	The validity for the authentication had already expired when the POST request was made.		
	The POST request is sent the first time the Business system is accessed.		
2	The authentication operation for the POST request is stopped and then restarted.	Authentication was successful.	200closeerr_en.template
3	The information cannot be displayed because the user has not been assigned to the required role.	Access is not allowed.	403roleerr_en.template (*3)
4	The browser is not set to accept cookies.	Browser does not accept cookies.	403cookieerr_en.template (*3)

No.	Cause of Error	Message Contents	Message File Name
5	The authentication operation must be retried because the authentication information has expired.	Authentication has been expired.	403postdecodeerr_en.template (*3)
6	Authentication information could not be found.	Authentication is needed. Try again after authentication.	403postrequesterr_en.template (*3)
7	Authentication information is not correct. The IP address for accessing the authentication server and the IP address for accessing the business server may be different.	Authentication information is invalid.	403ipcheckerr_en.template (*3)
8	The system does not support generation of an 8.3-format file name from a long file name or URLs that include folders or filenames ending with a period.	Requested path is invalid form.	403patherr_en.template (*2) (*3)
9	An internal error occurred during the Single Sign-on operation.	An internal error has occurred.	500internalerr_en.template (*3)

*1 A tag for the unauthenticated window must already exist in this message file. For details on the unauthenticated window tag specifications, refer to "5.1.7 Unauthenticated Window Tag Specifications"

*2 "403patherr_en.template" is message file used only for Windows.

*3 In Microsoft(R) Internet Information Services 7.0 or later, the Microsoft(R) Internet Information Services error page shown below will display instead of this message file. Customize the Microsoft(R) Internet Information Services error page according to the application.

- Messages for which the message file name starts with 403

  The Microsoft(R) Internet Information Services status code 403 error page

- Messages for which the message file name starts with 500

  The Microsoft(R) Internet Information Services status code 500 error page

5.1.2 Customizing a Message

The following explains how to customize a message file.

1. Edit the message file. Refer to the example below for more information about editing message files.

   - When editing the authentication form tag, refer to 5.1.3 Authentication Form Tag Specifications.
   - When editing the Forced Sign-on confirmation window, refer to 5.1.4 Forced Sign-on Confirmation Window Form Tag Specifications.
   - When editing the Sign-off confirmation window, refer to 5.1.5 Sign-off Confirmation Window Form Tag Specifications.
   - When editing the Simultaneous Authentication Confirmation window, refer to 5.1.6 Simultaneous Authentication Confirmation Window Tag Specifications.
   - When editing the Unauthenticated window, refer to 5.1.7 Unauthenticated Window Tag Specifications.
   - For details on editing the message displayed when an error is detected in the Integrated Windows Authentication application, refer to 5.1.8 Specifying Tags for Messages Displayed for Integrated Windows Authentication.

2. Display the edited message file to confirm that the message file displays correctly. If the message file displays correctly, start the authentication server or business server. After the application starts, the message that was edited is displayed.

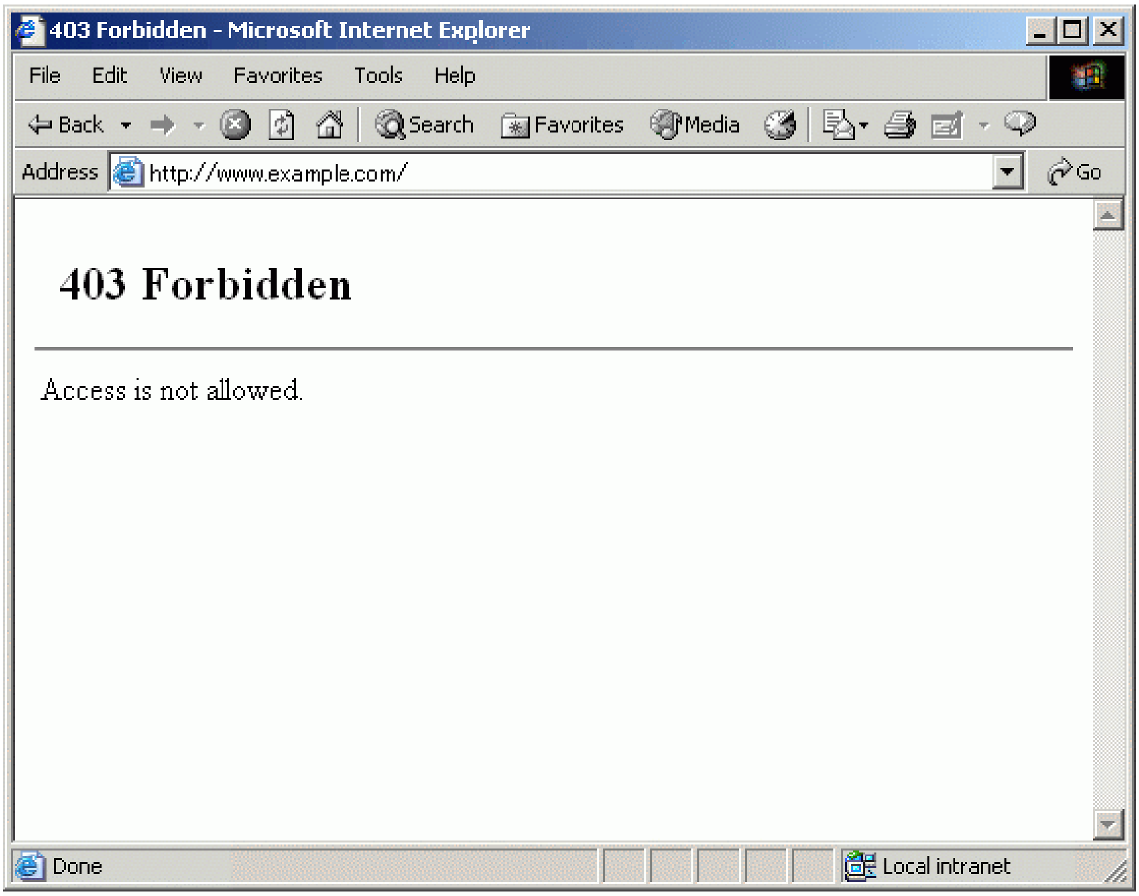
Example

An example of editing message file "403roleerr_en.template" is shown below.

Unedited Message Output

The following figure shows an unedited example of message file "403roleerr_en.template."

Figure 5.2 Unedited Example of the Message File



403 Forbidden

Access is not allowed.

Edited Message File

Open and edit the 403roleerr_en.template file.

In the following example, bold text indicates a change:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title> 403 Forbidden </title>
</head>

<body TEXT="#000066" BGCOLOR="#FFFFCC" LINK="#660000" VLINK="#660000" ALINK="#FFCC33">
<table border="0" cellpadding="10" width="100%">
<tr><td>
<b><font size="+2"> There is no authority to access the page.</font></b>
</td></tr>
</table>
<hr size="2" noshade>
<P>
  The page cannot be displayed because there is no authority to access the
page.</P>
<P> Take the following action.<BR><BR>
- Ask the System Administrator to check whether the required access
authority has been assigned<BR>
  If the access authority has not been assigned, request that it be assigned.
```

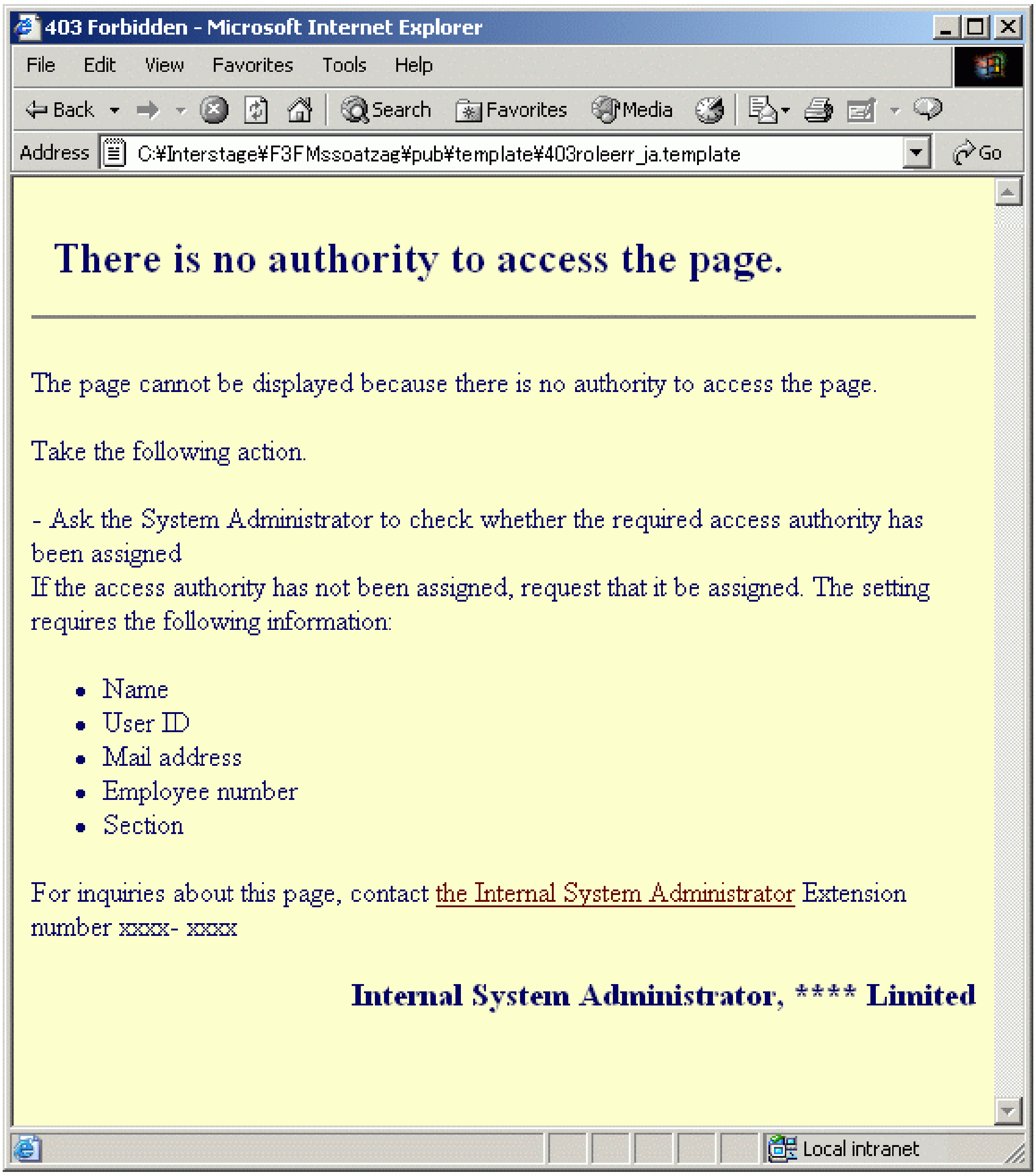
```
The setting requires the following information:
<UL>
<LI> Name
<LI> User ID
<LI> Mail address
<LI> Employee number
<LI> Section </UL>
  For inquiries about this page, contact <a href="mailto:admin@syanai-system.fujitsu.com">the
Internal System Administrator</a> Extension number xxxx-xxxx</P>
<h3 align="right"> Internal System Administrator, **** Limited </h3>
</body>
</html>
```

Edited Message Output

In the following example, the error message file has been edited using Windows(R) Internet Explorer(R) as the Web browser.

Ensure that the edited message file can be displayed using any Web browser.

Figure 5.3 Edited Error Message Example


403 Forbidden - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:¥Interstage¥F3FMssoatzag¥pub¥template¥403roleerr_ja.template
Go
Local intranet

There is no authority to access the page.

The page cannot be displayed because there is no authority to access the page.

Take the following action.

- Ask the System Administrator to check whether the required access authority has been assigned
If the access authority has not been assigned, request that it be assigned. The setting requires the following information:

- Name
- User ID
- Mail address
- Employee number
- Section

For inquiries about this page, contact the Internal System Administrator Extension number xxxx- xxxx

Internal System Administrator, ** Limited**

Notes

- Be extremely careful when changing a message. Changes to an error message may prevent the user from referencing the Messages and checking the details of the error that has occurred.
- Do not use special HTML tags that are only effective on the server and specific Web browsers.
- If a message file is deleted or there is no authority to access a message file, the system log of Interstage Single Sign-on is output and the non-edited English message will be displayed on the Web browser. Do not delete message files or change their access authority. For details on the messages output to the system log, refer to "Messages Beginning with 'sso'" in Messages.
- The time of the previous Sign-on is displayed in the "<!--SSO_LAST_SIGNON_TIME-->" portion of the 200lastsignontime_en.template message file. Note that the time of the previous Sign-on is not displayed if "<!--SSO_LAST_SIGNON_TIME-->" is deleted.
- The error detail code is displayed in the "<!--SSO_DETAIL_CODE-->" portion of the 500internalerr_en.template message file. Note that the error detail code is not displayed if "<!--SSO_DETAIL_CODE-->" is deleted.

- In the 200closeerr_en.template message files, do not edit the JavaScript in the <script> tag described in the <head> tag, or the [onload="close_sso_window()"] JavaScript event handler part in the <body> tag. If these are changed, authentication for the POST request may not be performed correctly.
- When specifying images to be displayed or hyperlinks to other pages, note the following points:
  - Use the URL or the absolute path from the root path ("/") to specify the location of the content.
  - To read the content from an active business server, do not specify files that are under a protection path.
- Information to be displayed as a message may pose a security risk. When editing a message, be extremely careful not to display information that could threaten security.

5.1.3 Authentication Form Tag Specifications

The following explains the specifications for the password authentication form tags to be inserted into the messages displayed at form authentication:

Example

The authentication form tags already inserted into the message file "200auth_form_en.template" are shown below.

The bold portions are required.

```
<form action="/ssoatcag" method="post" autocomplete="off">
<table border="0">
  <tr>
    <td nowrap align="right">user name</td>
    <td><input name="fj_is_sso_user_name" type="text" maxlength="255"></td>
  </tr>
  <tr>
    <td nowrap align="right">password</td>
    <td><input name="fj_is_sso_password" type="password"
maxlength="255"></td>
  </tr>
  <tr><td colspan="2">&nbsp;</td></tr>
  <tr><td colspan="2" nowrap align="center"><input type="submit"
value="sign-on">&nbsp;<input type="reset" value="reset"></td></tr>
</table>
</form>
```

The following explains the specification of each tag:

Form definition

```
<form action="/ssoatcag" method="post">
```

- Set "/ssoatcag" for the action attribute value. (*1)
- Set "post" for the method attribute value.
- Omit the enctype attribute

User ID

```
<input name="fj_is_sso_user_name" type="text">
```

- This text area is used for user ID input and is required.
- Set "fj_is_sso_user_name" for the name attribute value.
- Set "text" for the type attribute value.

Password

```
<input name="fj_is_sso_password" type="password">
```

- This password input area is used for password input and is required.

    - Set "fj_is_sso_password" for the name attribute value.
    - Set "password" for the type attribute value.

*1 If the incorrect URL is specified, the following error occurs and authentication may fail.

- The following message may output on the Web browser.
    - "403 Not Found"
    - "The requested page is not available"
- The message sso02012 or sso12003 may output to the system log.
- If client authentication is processed through SSL communication, the request window for the client certificate is displayed several times.
- Content may be displayed without authentication.

5.1.4 Forced Sign-on Confirmation Window Form Tag Specifications

The following section explains how to specify the form tags to be inserted into the messages displayed at forced Sign-on confirmation:

Example

The form tags already inserted into the message file "200queryforcedsignon_en.template" are shown below.

```
<form action="/ssoatcag" method="post">
<input name="fj_is_sso_forced_sign_on_continue" type="submit" value="yes">&nbsp;
<input name="fj_is_sso_forced_sign_on_cancel" type="submit" value="no">&nbsp;
<input name="fj_is_sso_forced_sign_on_id" type="hidden" value="<!--SSO_FORCED_SIGNON_ID-->">
</form>
```

The parts shown above in bold must not be changed.

Setting invalid values may cause any of the following problems and make it impossible to use Forced Sign-on correctly:

- Output of the following messages in the Web browser:
    - "404 Not Found"
    - The page cannot be displayed
- Output of sso02012 or sso12003 in the system log.
- Multiple output of the client certificate request window if client authentication is used for SSL.

5.1.5 Sign-off Confirmation Window Form Tag Specifications

The following section explains how to specify the form tags to be inserted into the messages displayed at Sign-off confirmation:

Example

The form tags already inserted into the message file "200querysignoff_en.template" are shown below.

```
<form action="/ssoatcag" method="post">
<input name="fj_is_sso_sign_off_continue" type="submit" value="yes">&nbsp;
<input name="fj_is_sso_sign_off_cancel" type="submit" value="no">&nbsp;
<input name="fj_is_sso_sign_off_id" type="hidden" value="<!--SSO_SIGNOFF_ID-->">
</form>
```

The parts shown above in bold must not be changed.

Setting invalid values may cause any of the following problems and make it impossible to use Sign-off correctly:

- Output of the following messages in the Web browser:
    - "404 Not Found"
    - The page cannot be displayed

    - Sign-on was not performed.
- Output of sso02012 or sso12003 in the system log.
- Multiple output of the client certificate request window if client authentication is used for SSL.

5.1.6 Simultaneous Authentication Confirmation Window Tag Specifications

The following section explains how to specify the tags to be inserted into the Simultaneous Authentication Confirmation window displayed when authentication was performed on more than one page at the same time or when another protection resource was accessed during authentication.

Example

The tags already inserted into the message file "200check_duplication_auth_en.template" are shown below.

The numbers at the start of each line in the following example are only there to identify each line for editing purposes. They are not included in the actual message file.

```
  1:<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
  2:<html lang="ja">
  3:<head>
  4:<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  5:<title> </title>
  6:<meta http-equiv="Content-Style-Type" content="text/css">
  7:<meta http-equiv="Content-Script-Type" content="text/javascript">
  8:<script type="text/javascript">
  9:<!--
 10:// Message
 11:var docTitle = "Waiting";
 12:var retryMsg = "Executing the authentication page while another window or page has already opened
an authentication page may result in the incorrect authentication page transition.  Continue?";
 13:
 14:// Initialize
 ~:  ~Omitted~
185:// -->
186:</script>
187:</head>
188:<body onload="autosend()">
189:
190:<!-- Waiting start -->
191:<layer id="layerProcessing" visibility="hidden">
192:<div id="divProcessing" style="visibility: hidden">
193:<div style="position: absolute">
194:<table border="0" cellpadding="10" width="100%">
195:<tr><td>
196:<b><font size="+2"> Waiting </font></b>
197:</td></tr>
198:</table>
199:<hr size="2" noshade>
200:<div align="center">
201:<table border="0">
202:<tr><td>
203:Waiting for authentication from another window or page...<br>
204:If authentication is not already in progress, click the following button to continue
authentication processing.<br>
205:</td></tr>
206:</table>
207:<br>
208:<form action="#">
209:<input type="button" value="Continue" onClick="javascript:retry();">
```

```
210:</form>
211:</div>
212:<h3 align="right">Interstage Single Sign-on</h3>
213:</div>
214:</div>
215:</layer>
216:<!-- Waiting end -->
217:
218:<layer id="layerNocookie" visibility="hidden">
219:<div id="divNocookie" style="visibility: hidden">
220:<div style="position: absolute">
221:Please enable COOKIE on your browser.
222:</div>
223:</div>
224:</layer>
225:
226:<form action="/ssoatcag" name="postdata" method="{SSO_FORM_METHOD}">
227:{SSO_FORM_PARAMETER}
228:<input type="hidden" name="fj-is-sso-req-check" value="1">
229:</form>
230:
231:<form action="/ssoatcag" name="postdata_org" method="{SSO_FORM_METHOD}">
232:{SSO_FORM_PARAMETER}
233:</form>
234:
235:<noscript>
236:Please enable JavaScript on your browser.
237:</noscript>
238:
239:</body>
240:</html>
```

Note the following points when editing the message file:

- The parts in bold must not be changed.
- For 'retryMsg' in line 12, specify the message that is displayed when the [Continue] button in line 209 is clicked.
- For lines 194 to 212, specify the message that is displayed when authentication was performed on more than one page at the same time, or another protection resource was accessed during authentication. Also specify the title used when this message is displayed (this is equivalent to the 'title' tag) for docTitle in line 11.
- In line 221, specify a message for Web browsers in which cookies are not enabled.
- In line 236, specify a message for Web browsers in which JavaScript is not enabled.

5.1.7 Unauthenticated Window Tag Specifications

The following section explains how to specify the form tags to be inserted into the unauthenticated window displayed when a POST request is authenticated.

Example

The form tags already inserted into the message file "200postauth_en.template" are shown below.

The numbers at the beginning of each line in the following example have been added only to identify each line for editing, and are not included in an actual message file.

```
1:<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
2:<html>
3:<head>
4:<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
5:<title> POST authentication </title>
6:<script language=JavaScript>
```

```
 7:<!--
 8:var winObj;
 9:var target = "<!--SSO_POST_REQUEST_AUTH_TARGET-->";
10:var winName = "_blank";
11:var options = "width=480,height=360,menubar=no,toolbar=no,status=yes,location=yes";
12:function popup_open(){
13:  if( (!winObj) || (true==winObj.closed) ){
14:    winObj = window.open(target, winName, options);
15:  }
16:}
17:function popup_close(){
18:  if( (winObj) && (false==winObj.closed) ){
19:    winObj.close();
20:  }
21:}
22:function popup_check(){
23:  if( (winObj) && (false==winObj.closed) ){
24:    winObj.focus();
25:  }
26:}
27:// -->
28:</script>
29:</head>
30:
31:<body onunload="popup_close()" onfocus="popup_check()" >
32:<!--SSO_POST_REQUEST_AUTH_NEED-->
33:<table border="0" cellpadding="10" width="100%">
34:<tr><td>
35:<b><font size="+2"> POST authentication </font></b>
36:</td></tr>
37:</table>
38:<hr size="2" noshade>
39:Click the link below to open the Authentication window.<br>
40:Check that the authentication server is correct, and then complete the authentication
procedure.<br><br>
41:<div id="fj_is_sso" style="position: absolute"><a href="javascript:void(0)"
onClick="popup_open()">Authentication window</a></div>
42:<br>
43:</body>
44:</html>
```

Note the following points when editing the message file:

- The parts in bold must not be changed.
- Ensure that the character code set for the "charset" attribute described in the <meta> tag in line 4 is the same as the character code for the Web contents.
- Do not change or delete <!--SSO_POST_REQUEST_AUTH_TARGET--> and <!--SSO_POST_REQUEST_AUTH_NEED--> in lines 9 and 32.
- If the size of the Authentication window shown in the link in line 39 is changed, change the "options" variable in line 11.
- The <div> and <a> tags in line 41 are required to open the Authentication window. For this reason, the part after <!--SSO_POST_REQUEST_AUTH_NEED--> in the <body> tag must be included. Do not change the <div> and <a> tag attributes.

Note

If the following conditions apply, then the message file must be changed.

- There is a link to a reverse proxy.
- The reverse proxy to be linked to cannot convert the URL in the <script> tags.

For details on the changes, refer to "Production Notes", section "Notes on Interstage Operation" > "Notes on Interstage Single Sign-on" > "Notes on Reverse Proxy Linkage".

5.1.8 Specifying Tags for Messages Displayed for Integrated Windows Authentication

This section describes the specifications for tags embedded in messages displayed for Integrated Windows Authentication.

General specifications for tags for message files displayed for Integrated Windows Authentication

"Content-Type" must be set for the "http-equiv" attribute in the <meta> tag described in the message file. The character code used in the message file must also be set for the value in the "content" attribute.

In the <meta> tag, only change the value set for the "charset" attribute. Do not change the parts in bold.

Example

```
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
```

Tag Specifications for the Sign-on Confirmation Page

The examples in this section illustrate how to specify tags embedded in the following message files that are displayed during Sign-on confirmation when Integrated Windows Authentication is used:

- 200_confirm_winauth_en.html
- 200_confirm_timeout_en.html
- 200_confirm_expired_en.html

Example

The form tag that is already embedded in the "200_confirm_winauth_en.html" message file is shown below.

Do not change the parts in bold.

```
<form action="/winauth/SSOPreSignOn" method="post">
<input name="fj_is_sso_winauth_continue" type="submit" value="yes">&nbsp;
<input name="fj_is_sso_winauth_cancel" type="submit" value="no">&nbsp;
<input name="fj_is_sso_winauth_id" type="hidden" value="<!--FJ_IS_SSO_REQ_ID-->">
</form>
```

5.1.9 Setting Access Authority for a Message File

This section explains how to set the access authority for a message file.

The following access authority is set immediately after the installation, so there is no need to configure these settings.

Windows32/64

To set the access authority, use Explorer to change the access permissions for the user and group. Users require administrator authority to change user and group permissions.

Solaris32/64 Linux32/64

To set the access authority, use the chmod or chown command. Set the access authority to superuser (root).

Access Authorization for the Message File Output at Form Authentication

Windows32/64

Table 5.5 Windows Access Authorization

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to administrators and SYSTEM.

Solaris32/64 Linux32/64

Table 5.6 Solaris and Linux Setting Authority

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to the user, such as nobody, that has been specified for user name (User) in the environment configuration file (httpd.conf) of the Interstage HTTP Server.

Access Authority for the Authentication Error Message File

Windows32/64

Table 5.7 Windows Authentication Authority

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to administrators and SYSTEM.

Solaris32/64 Linux32/64

Table 5.8 Solaris and Linux Authentication Authority

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to the user, such as nobody, that has been specified for user name (User) in the environment configuration file (httpd.conf) of the Interstage HTTP Server.

Access Authority for the Message File displayed for Integrated Windows Authentication

Windows32/64

Table 5.9 Windows Authentication Authority

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to administrators and SYSTEM.

Solaris32/64 Linux32/64

Table 5.10 Solaris and Linux Authentication Authority

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Allow "read" for the start user of the WorkUnit used to deploy the Integrated Windows Authentication application.

Access Authority for the Authorization Error Message File

Windows32/64

The setting contents vary depending on the types of Web servers being used.

Table 5.11 Configuring Microsoft Internet Information Services 6.0 or later

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to administrators, SYSTEM, and the account or user specified for the application pool ID of the application pool.

The application pool ID is different from the user name/group name with access permission to the message file. Refer to the correspondence table below before setting the access permission:

Application Pool Identity	User name or group name
ApplicationPoolIdentity (*1)	IIS_IUSRS group
NetworkService	NETWORK SERVICE
LocalSystem	SYSTEM

*1 This can be selected in Windows Server (R) 2008 Service Pack2 or later, and Windows Server (R) 2008 R2 or later.

For details on setting Microsoft Internet Information Services, refer to Microsoft(R) Internet Information Services Help.

Table 5.12 Configuring Services Other than Microsoft Internet Information Services 6.0 or later

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to administrators and SYSTEM.

Solaris32/64

The configuration settings vary depending on the types of Web servers being used.

[Interstage HTTP Server]

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to the effective user, such as nobody, that has been specified for user name (User) in the environment configuration file (httpd.conf) of Interstage HTTP Server.

Solaris32

[Sun Java System Web Server]

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to the effective user, such as nobody, that has been specified for user account (User) in the configuration file (magnus.conf) of Sun Java System Web Server.

Notes

If multiple Web servers are operating on one server, set the effective user as follows:

- Grant read permission to the effective user:
    - Set the same effective user for the Interstage HTTP Server and Sun Java System Web Server.

For details on setting the effective user, refer to 'To Change Effective User for the Business Server' in 'Changing the Effective User for the Web Server' in the Operation and Maintenance chapter.

Linux32/64

Interstage HTTP Server

Resource	Setting Authority to Access Content
Message file to be displayed on a Web browser	Grant read permission to the effective user, such as nobody, that has been specified for user name (User) in the environment configuration file (httpd.conf) of Interstage HTTP Server.

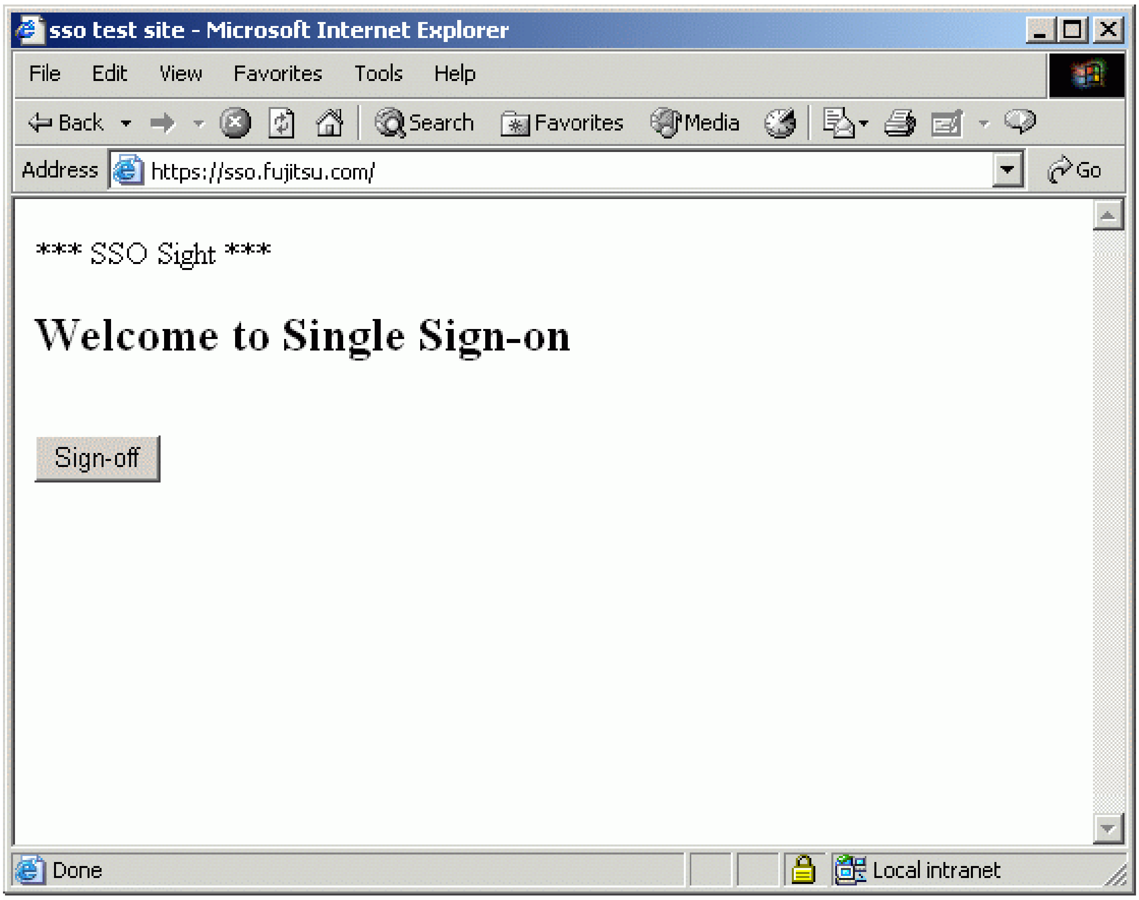
5.2 Customizing Web Pages for Sign-off

To enable users to easily sign off from the Single Sign-on system, Web pages on the existing Business system can be edited by adding a Sign-off button and link to the application.

The user can sign off from the Single Sign-on system using the Sign-off button and link on the Business server contents.

In the example below, a Sign-off button has been added to a Web page on the Business system.

The user can sign off by clicking the [Sign-off] button.


sso test site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.com/
Go
Done
Local intranet

*** SSO Sight ***

Welcome to Single Sign-on

5.2.1 Customizing Web Pages

The method for customizing Web pages for Sign-off is described below.

A Web page of an existing Business system can be customized by adding a Sign-off button and link so that a user can access a Sign-off URL when he or she signs off.

Make the following settings for the Sign-off URL:

```
Authentication infrastructure URL/ssoatcag?fj-is-sso-request=sign-off (*1)(*2)
```

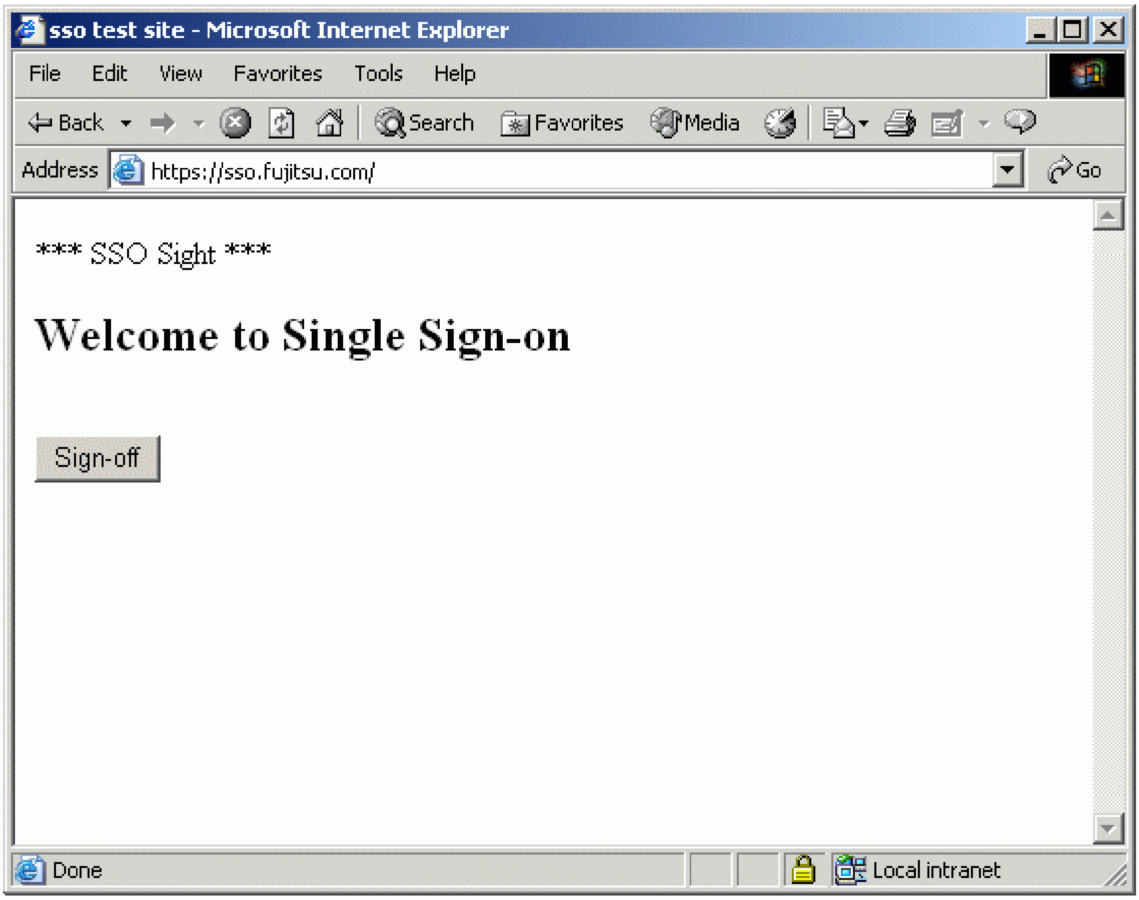
*1 Specify the port number of Authentication infrastructure URL even if 443 is specified.

*2 If the Authentication infrastructure URL is confirmed after setting the business server, on the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]], and then check the setting for [Authentication infrastructure URL] under [Authentication Infrastructure Information Settings].

An example of the [Sign-off] button settings is described below

Example

Customized Web page



sso test site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://sso.fujitsu.com/
Go
Done
Local intranet

*** SSO Sight ***

Welcome to Single Sign-on

Sign-off

The part shown in bold has been added for the [Sign-off] button settings.

The Authentication infrastructure URL set as the Sign-off URL is 'https://sso.fujitsu.co.jp'.

The user can sign off by clicking the [Sign-off] button.

```
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=iso-8859-1">
<title>sso test site</title>
</head>
<body>
  *** SSO Sight ***
  <h2>  Welcome to Single Sign-on</h2>
  <br>
    <form action="https://sso.fujitsu.co.jp:443/ssoatcag" method="GET">
    <input type="hidden" name="fj-is-sso-request" value="sign-off">
    <input type="submit" value="Sign-off">
    </form>
  </body>
  </html>
```

5.3 Service Linkage with SSO Repository

Windows32/64

Before the repository server of the Interstage Single Sign-on is started, the SSO repository must be started.

When starting a service on system startup, if the repository server starts up before the SSO repository is started, the sso01041 error is output and the repository server startup fails.

If a service dependency between the SSO repository and repository server is set, the repository server can be started after the SSO repository, and the repository can start up automatically when the system starts up.

Interstage Single Sign-on provides the command that sets and cancels the service dependency. This command enables setting and cancellation of the service dependency between the SSO repository and repository server.

The following explains how to set and cancel the service dependency.

Setting the Service Dependency

1. Check the repository name of the SSO repository.

   Use the Interstage Management Console on the repository server to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and then click [Repository server detailed settings [Show]] or [Detailed Settings [Show]] to check [Repository Name] in [Repository Settings].

2. Specify the repository name checked in Step 1 for the option of the ssosetsvc command and execute the command to set the service dependency.

For details on the ssosetsvc command, refer to "Single Sign-on Operation Commands" in the Reference Manual (Command Edition).

Example

Setting the service dependency between the "web001" Web server of the Interstage HTTP Server on which the repository server was built and the "ssorep" SSO repository

```
C:\>ssosetsvc ssorep web001
```

Notes

- When the cluster service is to be used, the service dependency should not be set using this command.
- If the repository name of the SSO repository has changed, ensure that the service dependency has been set for the changed repository name. The service dependency for the unchanged repository name does not need to be canceled.
- If a relational database (RDB) is used as the SSO repository, dependency must be set for the SSO repository and the RDB services. For details about service dependency settings, refer to 'Starting/stopping a Repository' in the chapter 'Operation and Maintenance' of the 'Directory Service Operator's Guide'.

Canceling the Service Dependency

Use the ssounsetsvc command to cancel the service dependency.

For details on the ssounsetsvc command, refer to "Single Sign-on Operation Commands" in the Reference Manual (Command Edition).

Example

Removing the service dependency of the "web001" Web server of the Interstage HTTP Server on which the repository server was built

```
C:\>ssounsetsvc web001
```

Note

To delete the SSO repository or to stop the SSO repository, cancel the service dependency.

Chapter 6 Troubleshooting

This chapter explains the action to be taken if an error occurs during operation of the Interstage Single Sign-on system.

6.1 Error Handling

This section explains how to respond to abnormalities that may occur during operation.

6.1.1 Error Investigation and Corrective Action

User

The user needs to respond to any messages displayed on the Web browser. When an error occurs that the user cannot correct (for example a "500 Internal Server Error") they contact the Business Server Administrator. In this case, the user must supply the following information:

- Error-detected date and time
- User ID or certificate used for authentication
- Message and status code displayed on the Web browser.

Business Server Administrator

The Business Server Administrator must do the following:

- Investigate the business server status
- Request changes to the SSO repository, repository server, and authentication server

When receiving an inquiry from a user, investigate the cause of the error in the following sequence:

1. Check the message and status code displayed on the Web-browser that are reported by the user. Remove the cause of the trouble.

   Refer to "Status Codes Reported from the Browser" in Messages for details of the message or status code displayed on the Web browser.

   When [Business Server Administrator Action] in "Status Codes Reported from the Browser" describes user actions for the SSO repository, repository server, or authentication server errors, post the user-reported information to the SSO administrator for investigation and any necessary modification of settings.

2. Check the "Trouble detection date and time" and "User ID or certificate used for authentication" reported by the user. Also check the access log of the business server and remove the cause of the error.

   Refer to "Access Log In Single Sign-on Mode" of "Messages Logged and Output in Single Sign-on" of Messages for details of the access log of the business server.

3. If you cannot identify the cause of the trouble from the access log of the business server, use the system log of the business server to remove the cause.

   Refer to "Messages Beginning with 'sso'" in Messages for details of the system log of the business server.

4. If you cannot identify the cause of the trouble from the system log of the business server, post the user-reported information to the SSO administrator, and request the investigation.

SSO Administrator

The SSO administrator must perform the following steps as necessary:

- Change the SSO repository settings
- Investigate and change the authentication server settings
- Investigate and change the repository server settings.

When receiving an investigation request or a request to change settings from the business server administrator, the SSO administrator must investigate the cause of the error or change settings in the following order:

1. When receiving a request to change settings from the business server administrator, check the status code displayed on the Web browser, and change the settings according to [SSO Administrator Action] in "Status Codes Reported from the Browser" of Messages.

2. When receiving an investigation request from the business server administrator, check the "Trouble detection date and time" and "User ID or certificate used for authentication" that were posted by the business server administrator. Then refer to the authentication server access log to remove the cause of the error.

   Refer to "Access Log In Single Sign-on Mode" of "Messages Logged and Output in Single Sign-on" of Messages for details of the access log of the authentication server.

3. If the cause of the error cannot be identified from the authentication server access log, refer to the authentication server system log and remove the cause of the error.

   Refer to "Messages Beginning with 'sso'" of Messages for details of the system log of the authentication server.

4. If the cause of the error cannot be identified from the authentication server system log, check the "Trouble detection date and time" and "User ID or certificate used in authentication" that were reported by the business server administrator. Then refer to the repository server access log and remove the cause of the error.

   Refer to "Access Log In Single Sign-on Mode" of "Messages Logged and Output in Single Sign-on" of Messages for details of the access log of the repository server.

   If session management is used, refer to the session management log to check the session status.

   For details about the session management log, refer to in "Log messages output in Single Sign-on" - "Single Sign-on session management log" in "Messages".

5. If the cause of the error cannot be identified from the repository server access log refer to the repository server system log and remove the cause of the error.

   Refer to "Messages Beginning with 'sso'" of Messages for details of the system log of the repository server.

6.1.2 Log Output Destination

The logs of the Single Sign-on system are output to the following destinations:

- Output destination of system log

  Windows32/64

  ```
  Event viewer (application log)
  ```

  Solaris32/64

  ```
  /var/adm/messages
  ```

  Linux32/64

  ```
  /var/log/messages
  ```

- Output destination of access log of business server

  The access log is output to the file that is set using the Interstage Management Console. Select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab and click [Access Log Settings] > [File name].

  Storage destination of access log file

  Windows32/64

  ```
  C:\Interstage\F3FMsso\ssoatzag\log
  ```

  Solaris32/64 Linux32/64

  ```
  /var/opt/FJSVssoaz/log
  ```

- Output destination of access log of authentication server

  The access log is output to the file that is set using the Interstage Management Console. Select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab and click [Access Log Settings] > [File name].

  Storage destination of access log file

  Windows32/64

  ```
  C:\Interstage\F3FMsso\ssoatcag\log
  ```

  Solaris32/64 Linux32/64

  ```
  /var/opt/FJSVssoac/log
  ```

- Output destination of access log of repository server

  The access log is output to the file that is set using the Interstage Management Console. Select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab and click [Access Log Setting] > [File name].

  Storage destination of access log file

  Windows32/64

  ```
  C:\Interstage\F3FMsso\ssoatcsv\log
  ```

  Solaris32/64 Linux32/64

  ```
  /var/opt/FJSVssosv/log
  ```

- Output destination of session management log

  The access log is output to the file set using the Interstage Management Console. Select the [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab and click [Session management Log Settings] > [File name].

  Storage destination of session management log

  Windows32/64

  ```
  C:\Interstage\F3FMsso\ssoatcsv\log
  ```

  Solaris32/64 Linux32/64

  ```
  /var/opt/FJSVssosv/log
  ```

6.2 Examples of Errors

Errors are generally classified into the following items:

- 6.2.1 Errors in Authentication
- 6.2.2 Errors in POST Request Authentication
- 6.2.3 Errors in Integrated Windows Authentication
- 6.2.4 Errors in Business Server Authorization
- 6.2.5 Errors in the Repository Server
- 6.2.6 Errors when using Active Directory in the user Directory Service where the User Information is Registered
- 6.2.7 Errors in Microsoft(R) Internet Information Services
- 6.2.8 Errors in the Web Browser
- 6.2.9 Errors in the Interstage Management Console
- 6.2.10 Errors that may be Encountered while using the Interstage Directory Service Replication Function
- 6.2.11 Errors in Upgrading from a Previous Version

6.2.1 Errors in Authentication

Although a business system protection resource is accessed, the content is displayed without authentication.

- Confirm the following:
- Confirm that the [Web Server used] value in the [Web Server Settings] of the business-server environment setup is the same as the port number of the Web server on which the business server operates. (*1)
- Check the access log of the Web server that integrates the business server to see whether the request has been received or not. If the request is not received, it is possible that it is accessing another Web server.
- Check if the Web server that integrates the business server has been restarted, and if it hasn't then restart it.

Although a business system protection resource is accessed, unexpected content is displayed.

Confirm that the [Public URL] of [Business system Information] or the [Authentication infrastructure URL] of [Authentication Infrastructure Information Settings] of the business-server environment setup is correctly set. (*2)

The business system protection resource is accessed, but the response takes at least 1 minute.

Check whether name resolution for the business server FQDN included in the business system protection resource URL can be performed in the authentication server.

Although a business system protection resource is accessed, no response is returned.

Confirm the following:

- The business server and authentication server are operating.
- The [Public URL] of [Business system Information] or the [URL] of [Authentication Infrastructure Information Settings] of the business-server environment is setup correctly. (*2)
- On machines on which the repository server or authentication server has been set up, check whether there is a Web server or virtual host blocking communication.
- Check the following points before linking a business system with Interstage Portalworks.
  - The business system setup file used to configure the business server was created for linking the business system with Interstage Portalworks. (*3)
  - In the business server environment settings, [Authentication Information Setting] > [Enable Client IP Address Check?] is set to "No". (*1)
- If the SSL accelerator, load balancer, or Application Gateway is placed before the authentication server, check that the settings are correct. (*4)

Launching reauthentication before the user information validity period expires

Check that the system time on the repository server, authentication server, and business server is the same. (*5)

User information expired so re-authentication does not occur.

Confirm the following:

- If any re-authentication request is not issued to the user, the cache information of the Web browser may be displayed.
- Check that the system time for the repository server, authentication server, and business server is the same. (*5)

Protected resources are displayed after sign-off

If Firefox is used as the client web browser and content that uses frames is accessed, the web browser cache information may sometimes be displayed. Check whether the frame page protected resource settings have been executed correctly.

For details on the frame page protected resource settings, refer to "Designing a Business System", "Notes on Creating the Contents", "Note on Using the Frame Page" in the "Environment Setup (Business Server Administrators)" chapter.

Authentication page does not appear even after accessing the business system protection resource or the authentication infrastructure URL.

After "Waiting for authentication from another window or page..." is displayed on the web browser, the user pressed the [Continue] button, but it did not function properly.

Message file customization displayed on the Web browser may not be done properly. Check the message file (*6) of the following simultaneous authentication confirmation window and customize it again correctly (*7)

- 200check_duplication_auth_en.template

Certificate authentication using an IC card cannot be switched for password authentication

If the browser settings have been configured so that the certificate is sent automatically, password authentication cannot be performed for a user using the authentication method "Certificate or password authentication". Check the browser settings.

The protection path is accessed and authentication performed, but the protection path is not displayed

The protection path is accessed and authentication performed, but the Authentication window is still displayed

The protection path is accessed and authentication performed, but the Authentication window is still displayed as empty contents

In the Windows(R) Internet Explorer(R) 7.0 or later Internet Options Security settings, the "Protected Mode" settings registered for each zone, such as the Internet and Local intranet zones, for the Interstage Single Sign-on business server and the Interstage Single Sign-on authentication server may be different. Make the "Protected Mode" settings for the business server and the authentication server the same.

"Please enable COOKIE on your browser" message is displayed in the Web browser where COOKIE is valid.

The user accessed the authentication server with non-SSL communication via Web browser.

Communicate with the authentication server with SSL. When SSL accelerator is installed, access to the authentication server via SSL accelerator.

Errors Using Repository Server (Update System) Load Balancing

The protection path is accessed and authentication performed, but the protection path URL and Authentication infrastructure URL are displayed repeatedly without the protection path being displayed.

The protection path is accessed and authentication performed using the correct user ID/password, but the authentication fails.

The authentication page is displayed even if the [Yes] button is pressed on the Forced Sign-on confirmation window.

Check that the load balancer settings have been configured correctly.

For details about the load balancer settings, refer to "Repository Server Setup" - "Adding the repository server (update system) for load balancing" in the chapter "Environment Setup (SSO Administrators)".

*1 To check or modify [Web Server used] in [Web Server Settings], and [Enable Client IP Address Check?] in [Authentication Information Settings], in the Interstage Management Console, click the [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tabs, and then click [Detailed Settings [Show]].

*2 For the [Public URL] of [Business system Information] or the [URL] of [Authentication Infrastructure Information Settings], use the Interstage Management Console to select the [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab, and check [Detailed Settings [Show]] in the tab.

To change the value, set up the business server again.

To set up the business server again, use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] window > [List] tab to delete the current business server from [List] tab. Then, add a new business server by using the [Addition of Business server] tab.

*3 To create a business system configuration file for linkage with the Interstage Portalworks business system, use the Interstage Management Console for the repository server (update system). Click [Security] > [Single Sign-on] > [Authentication infrastructure] > [Business system setup file], and in [Linkage with Interstage Portalworks?] select "Yes". Specify the validity range for authentication in the domain name.

*4 Refer to "Linkage with SSL Accelerator" for details of the SSL accelerator settings. Refer to "Load Balancing" for details of the load balancer. Refer to "Linkage with Application Gateway" for details of the Application Gateway settings.

*5 When setting a system time for each server, take care with the time zone settings.

*6 For details of the simultaneous authentication confirmation window message, refer to "Single Sign-on Customization" - "Customizing Messages Displayed on Web Browser" - "Customizing a Message" in the "Single Sign-on Operator's Guide."

*7 For details of the specifications of the tag for the simultaneous authentication confirmation window, refer to " Single Sign-on Customization" - "Customizing Messages Displayed on Web Browser" - "Simultaneous authentication confirmation window Tag Specifications" in the "Single Sign-on Operator's Guide."

6.2.2 Errors in POST Request Authentication

The Unauthenticated window is displayed, but the Authentication window is not

Confirm the following:

- Are the browser JavaScript settings enabled? If they are disabled, enable them and re-execute authentication.
- The [var target = "<!--SSO_POST_REQUEST_AUTH_TARGET-->";] part in the following Unauthenticated window message files (*1) may have been deleted. If it was deleted, re-enter it. (*2)
    - 200postauth_en.template or 403postauth_en.template

Nothing is displayed in the Authentication window

The [var target = "<!--SSO_POST_REQUEST_AUTH_TARGET-->";] in the following Unauthenticated window message files (*1) may have been changed. If it was changed, correct it. (*2)

- 200postauth_en.template or 403postauth_en.template

"Waiting" is displayed in the Authentication window

If different types of contents (such as images used for display or hyperlinks to other pages) are specified in the following Unauthenticated window message files, the files stored under the protection path of the Business server that is running may be specified. Check that the message file does not allow files stored under the protection path to be specified.

- 200postauth_en.template or 403postauth_en.template

The Authentication window closes automatically, but focus is returned to the original window (Unauthenticated window)

After authentication, the Authentication window does not close automatically and the contents are displayed in the Authentication window, or "Authentication was successful." is displayed

Confirm the following:

- The hostname and port number entered in the destination for the sent POST request (the "action" attribute of the <FORM> tag) in the Web contents may be different to the Business system public URL hostname and port number. If they are not the same, correct them to be the same.
- If the scheme of the destination for the sent POST request is "http" and the port number is "80", or the scheme is "https" and the port number is "443", the port number may be entered in the destination for the sent POST request (the "action" attribute of the <FORM> tag). In this case, delete the port number as follows:
- (Incorrect): https://business_server.fujitsu.co.jp:443/post
- (Correct): https://business_server.fujitsu.co.jp/post
- The [<!--SSO_POST_REQUEST_AUTH_NEED-->] part in the following Unauthenticated window message files (*1) may have been deleted or changed. If it was deleted, re-enter it. If it was changed, correct it. (*2)
    - 200postauth_en.template or 403postauth_en.template

POST data is not sent correctly

If after authentication the Japanese in the window is garbled and the POST data is not sent correctly, the character codes specified in the "charset" attribute of the <meta> tag of the following Unauthenticated window message files (*1) may be different to the character codes used in the Web contents. If they are not the same, change the settings so that they are the same.

- 200postauth_en.template or 403postauth_en.template

The link for the Authentication window is not displayed in the Unauthenticated window

The user may have interrupted the authentication operation for the POST request. If the authentication operation is complete, use of the Business system can be continued.

To stop using the Business system, perform Sign-off in the Business system that is using session management. If the Business system does not use session management, close the Web browser.

"Authentication was successful." is displayed in the window following authentication

Confirm the following:

- The authentication operation for the POST request may have been interrupted, and the re-authentication operation performed. If the authentication operation is complete, use of the Business system can be continued.
- There is a possibility that the following message files were customized incorrectly:
    - 200closeerr_en.template or 403closeerr_en.template

  Check whether the JavaScript entered in the <script> tag of the <head> tag and the [onload="close_sso_window()"] JavaScript event handler part set in the <body> tag were changed or deleted. If they were, return them to their original state.
- The request ring used in the URL for the request to the Business server may start with "fj-is-sso". Change the settings so that the request ring does not start with "fj-is-sso".
- In the Windows(R) Internet Explorer(R) 7.0 or later Internet Options Security settings, the "Protected Mode" settings registered for each zone, such as the Internet and Local intranet zones, for the Interstage Single Sign-on business server and the Interstage Single Sign-on authentication server may be different. Make the "Protected Mode" settings for the business server and the authentication server the same.

*1 For details about Unauthenticated window message files, refer to "Single Sign-on Customization" - "Customizing Messages Displayed on a Web Browser" - "Messages that Can be Customized" in the "Single Sign-on Operator's Guide".

*2 For details about customizing Unauthenticated window message files, refer to "Single Sign-on Customization" - "Customizing Messages Displayed on a Web Browser" - "Unauthenticated Window Tag Specifications" in the "Single Sign-on Operator's Guide".

6.2.3 Errors in Integrated Windows Authentication

When the business system protection resource or Authentication infrastructure URL is accessed, the Authentication window is not displayed and nothing is displayed in the Web browser

A FORM tag that is required for the message file (*1) displayed in Integrated Windows Authentication may not have been set. Check the following message and make sure that the FORM tag is correct. (*2)

- 200_confirm_winauth_en.html
- 200_confirm_timeout_en.html
- 200_confirm_expired_en.html

The basic authentication dialog is output even though Integrated Windows Authentication is used

Check the Web browser settings. For details about the Web browser settings, refer to "Active Directory Linkage Settings".

The 'Integrated Windows Authentication failed' is displayed when Sign-on using Integrated Windows Authentication is canceled

Close all the Web browsers windows that were displayed as a result of the authentication operation and re-execute the authentication operation.

After changing the Active Directory settings and performing the Integrated Windows authentication, "Integrated Windows Authentication failed" is displayed.

Logoff the domain once, and login again, and then perform the Integrated Windows Authentication.

The Integrated Windows Authentication failed even if logged on to the federated Active Directory domain.

Check that the ticket permission ticket is correctly issued from the Kerberos authentication key distribution center when logged on the Windows with the user ID in which the Integrated Windows Authentication failed.

"The page cannot be displayed" is displayed on Web browser, and a message number beginning with sso07000 is output in the system log.

The following message file size displayed on Web browser is less than 512 bytes. Customize the file size to 512 bites or more (*1)

- 500_internal_error_en.html

*1 For details about message files displayed when Integrated Windows Authentication is used, refer to "Customizing Messages Displayed on a Web Browser" - "Messages that can be Customized" in the chapter "Single Sign-on Customization".

*2 For details about customizing message files displayed when Integrated Windows Authentication is used, refer to "Customizing Messages Displayed on a Web Browser" - "Specifying tags for messages displayed for Integrated Windows Authentication" in the chapter "Single Sign-on Customization".

6.2.4 Errors in Business Server Authorization

Although a protection resource or path configuration for the SSO repository has been added, changed, or deleted, it is not correctly authorized

When a protection resource or path configuration for the SSO repository has been added, changed, or deleted, be sure to update the access control information. (*1)

When the role configuration has been changed, always update the role information and then update the access control information. (*1)(*2)

The extended user information is not notified to the Web application

Confirm the following:

- The version of the server that constructs the Single Sign-on system may be out of date. Check that the version of each server to be constructed matches with the system that notifies the extended user information to the web application (*3)
- The extended user information may not be set in the protection path. Check that the extended user information to be notified is set in the protection path (*4)
- The access control information may not be updated. Update the access control information (*1)
- If the repository server (update system) is run in a system configuration in which more than one server is set up so that the load is distributed, the [Extended User Information] setting may not match the environment settings in all load distribution servers. Make all repository server environment settings the same, and then restart the repository server (update system). (*5)
- If the repository server (update system) and repository server (reference system) are run using a load distribution system configuration, [Extended User Information] in the environment settings may have been changed after the repository server (reference system) was set up. If [Extended User Information] has been changed, create the repository server (reference system) again. (*6)

Failed to update the access control information

When the access control information is updated using the business server Interstage management console, sso04139 error message may be displayed.

Check that an error is output in the repository server system log. If an error is output, take action according to the response measure for the repository server system log.

The access control information file was updated, however the authorization was incorrect

Solaris32/64 Linux32/64

- If one of the following operations was executed, restart all the business servers which are built on one machine.
  - The business server configuration was updated using the Interstage Management Console.
  - The business server configuration file was updated.
  - A business server was added.
  - A business server was deleted.
  - The *ssoimpaz* command was executed (for details, refer to "Single sign-on Operation Commands" in the "Reference Manual (Command Edition)".).

The business system protection resource is accessed, but the response is extremely slow

A path that does not need to be a target of access control might have been set as protection path. Set paths that do not need to be targets of access control so that they do not become protection paths. (*7)

The displayed protection resource is different from the one accessed before authentication

When the authentication fails or is cancelled, the protection resource is accessed instead of the Web browser closing, therefore the previously obtained information about the protection resource may still remain. In this case, close and then restart the Web browser, and then access the protection resource again.

*1 To update the access control information, in the Interstage management console of the business server, press the [Update] button in [System] > [Security] > [Single sign-on] > [Business system] > [Business system name] > [Update access control information] tab,

*2 To update the role information, in the repository server (Update system) of the Interstage management console, click the [Update] button in [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Repository server] > [Update Role information] tab.

*3 For details on possible matching with the system that notifies the extended user information to the Web application, refer to "Notes on Interstage Operation" - "Notes on Interstage Single Sign-on " - "Notes about Setting up Single Sign-on Systems Containing Mixed Versions and Editions" in the "Product Notes".

*4 For details of the extended user information to be notified, in the repository server (Updated system) of the Interstage management console, click [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Repository server] > [Protection resource] > [Site configuration] > [Protection path] > [Path configuration], and check [Notify extended user information] in [Path Configuration Settings].

*5 For details on stopping the repository server, refer to "4.2.1 Stopping a Repository Server". For details on starting the repository server, refer to "4.1.1 Starting a Repository Server".

*6 For details on creating a repository server (reference system), refer to "2.3.6 Adding a Repository Server (Reference System)".

*7 For details on how to set protection paths, refer to "2.6.3.2 Registering Protection Path".

6.2.5 Errors in the Repository Server

Time taken to start the repository server

The time taken to start Interstage HTTP Server depends on the number of role configuration and site configuration entries registered in the SSO repository.

In particular, if role sets are used heavily in the role definition, and the role set name is specified as the role contained in the role set (the role set nest), the Interstage HTTP Server startup time doubles for each registered role set and nest layer as shown below.

The repository server start time can be reduced by changing the role definition so that the role set nests are reduced.

Example

Table 6.1 Interstage HHTP Server Startup Time

No.	Role definition registration type	Interstage HTTP Server startup time
1	Only if 1000 roles are registered	1 second + α（*1）
2	In addition to No.1, if 100 rolesets containing 10 roles have been registered	101 seconds + α（*1）
3	In addition to No.2, if 10 rolesets containing 10 roles have been registered	1101 seconds + α（*1）

*1 This is the time (a few seconds) required for Interstage HTTP Server to start, regardless of the role definition.

6.2.6 Errors when using Active Directory in the user Directory Service where the User Information is Registered

ihs01027 message is output at the start of the repository server, and the start failed. Solaris32/64 Linux32/64

Check if the Directory Service URL is correct. (*1)

Without using the Single sign-on extended schema

Integrated Windows authentication is performed by accessing to the protection path, but the authentication failed.

Confirm the following:

- Check that the connection information (DN for connection, DN password for connection) bears the reference authority for all user information. (*2) (*3)
- Check that the target user information exists under the user information registration destination entry. (*3) (*4)
- Check that necessary attributes exist in the target user information under the user information registration destination entry. (*3) (*5)
- Make sure that Active Directory is not using the referral function, since it cannot be used for linkage.

Protection path is not displayed even if Integrated Windows authentication is performed by accessing to the protection path

Confirm the following:

- Check that the value specified in the [Attribute name to use for a role] specified in the [Active Directory Settings] in the environment settings of the repository server is correct. (*6)
- Check that the value specified in the [Attribute name to use for a role] specified in the [Active Directory Settings] in the environment settings of the repository server is registered with the user information.
  - If it is not registered with the user information, register the value in the [Attribute name to use for a role]
  - If it is registered with the user information, check that the value registered in the user information exists in [Attribute name to use for a role] that is set for either the role or role set that is set in the protection path that was accessed.
  - If the role/role set which is set in the accessed protection path is registered with a multi-level layer, check all roles and role sets that are set in the role set content. (*7)
- If no errors are found in the above, check the link to the role configuration (*8)

Using the Single Sign-on Extended Schema

Even if Integrated Windows authentication or password authentication is performed by accessing to the protection path, the authentication failed.

Even if the user lock is released, the user could not be identified and the lock release failed.

Confirm the following:

- Check that the connection information (DN for connection, DN password for connection) contains the reference authority for all user information and the update authorization. (*2) (*3)
- Check that the target user information exists under the user information registration destination entry (*3) (*4)
- Check that necessary attributes exist in the target user information under the user information registration destination entry (*3) (*5)
- Check that "inetOrgPerson" object class is included in the user information (*3)
- Check that the correct value ("good" or "locked") is set in the user information "ssoUserStatus" attribute (*3)
- Check the following to determine if the Single sign-on extended schema is correctly set.
  - Check that "inetOrgPerson" object class exists in the Active Directory schema (*9)
  - Check that "ssoUser" object class exists in the Active Directory schema (*9)
  - Check that all attributes of the Single sign-on exist in the Active Directory schema (*9) (*10)
  - Check that all attributes of the Single sign-on exist in the "ssoUser" object class option attributes of the Active Directory schema (*9) (*10)
  - Check that the "ssoUser" object class is set in the supplementary type class of the "inetOrgPerson" object class of the Active Directory schema (*9)
- Make sure that Active Directory is not using the referral function, since it cannot be used for linkage.

Even if Integrated Windows authentication or password authentication is performed by accessing to the protection path, the protection path is not displayed.

Check that the role name or the role set name (ssoRoleName) that can access to the protection path is set in the user information (*3)

*1 In the Interstage management console, click [Repository server detailed settings [Show]] in [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and check with [Directory service URL] in [Repository Settings] > [Active Directory Settings].

*2 In the Interstage management console, click [Repository server detailed settings [Show]] in [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and check with [Connection DN] in [Active Directory Settings] or with [Connection DN password].

*3 Check with the ADSI Edit tool provided by Microsoft

*4 In the Interstage management console, click [Repository server detailed settings [Show]] in [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and check with [Repository Settings] > [User Information Registration Entry].

*5 For details about necessary attributes for user information, refer to "Setting the user information of the Active Directory".

*6 In the Interstage management console, click [Repository server detailed settings [Show]] in [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and check with [Attribute names to use for a role] in [Repository Settings] > [Active Directory Settings].

*7 For details on how to confirm the role/role set which is set in the accessed protection path, in the Interstage management console, click [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Protection resource] > [Site configuration] > [Protection path], and click the protection path which was accessed from the path definition list. Then check the role/role set, role set contents, and the attribute values to be used for the role.

*8 For details on how to associate with the role configuration, refer to "SSO repository settings (Associating the role configuration)".

*9 For details on how to confirm the Active Directory, refer to the Active Directory manual.

*10 There are nine attributes for the single sign-on as shown below:

- ssoAuthType
- ssoCredentialTTL
- ssoFailureCount
- ssoLockTimeStamp
- ssoNotAfter
- ssoNotBefore
- ssoRoleName
- ssoSessionInfo
- ssoUserStatus

6.2.7 Errors in Microsoft(R) Internet Information Services

Failure of the attempt to read business server programs in Microsoft(R) Internet Information Services

If the following event log is output, restart the system.

```
The HTTP filter DLL C:\Interstage\F3FMsso\ssoatzag\lib\F3FMssoatziis.dll failed to load. The data is
the error.
```

Non-business server programs are set up in an ISAPI filter, and not correctly authorized

If non-business server programs are set up in an ISAPI filter, change the order so that business server programs display first in the [ISAPI filter] tab of the property sheet in Microsoft(R) Internet Information Services.

For details on ISAPI filter settings, refer to "Integrating into the Web server" in the "Environment Setup (Business Server Administrators)" chapter.

The sso00202 message is output to the system log during an operation

Check whether the application pool settings are correct. For details on the application pool settings, refer to "Integrating with Microsoft(R) Internet Information Services 7.0 or 7.5" under "Setting up Business Servers" in the "Environment Setup (Business Server Administrators)" chapter.

6.2.8 Errors in the Web Browser

When accessing a business system through multiple windows the message "The page cannot be displayed" is displayed.

Check if the "Show friendly HTTP error messages" check box is selected on the Advanced page of the Internet Options window. If it is selected, clear it, click **OK**, and then refresh the browser window.

If you are using an IC card for authentication, check that the card is correctly inserted then refresh the browser window.

6.2.9 Errors in the Interstage Management Console

When a business server was added, warning message sso04604 or sso04608 is displayed.

The access control information was not updated successfully because the authentication infrastructure was not ready. Take action according to the error message. After that action, always select the [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Update access control information] tab to click [Update] to confirm that the access control information is updated successfully.

The setting procedure of the authentication infrastructure needs to be confirmed.

To confirm the authentication infrastructure setting procedure using the Interstage Management Console, refer to the Operator's Guide.

The site configuration or path configuration created in the SSO repository is not displayed on the List of Site configuration Setting, Path configuration Setting, or Download Business-System Setup File.

The site configuration or path configuration in the SSO repository may have been modified to an invalid state using the entry management tool or ldapmodify command of the Interstage Directory Service. Refer to "Entry Attributes To Be Registered in SSO Repository" and correct the site or path configuration using the entry management tool or ldapmodify command of the Interstage Directory Service. For further information regarding entry operation of SSO repository, refer to the "Entry Management" section of the Directory Service Operator's Guide.

Message "ihs81364: A timeout occurred. " is displayed on the Interstage Management Console at repository server start. Solaris32/64 Linux32/64

It may take a while to start the Interstage HTTP Server if many role-configuration entries or site-configuration entries have been defined in the SSO repository. In this case, message "ihs81364: A timeout occurred." is displayed on the Interstage Management Console of the server on which the repository server was set up. Check the system log. When the system is running normally, wait for a while and select [System] > [Services] > [Web Server] > [Web Server Name]. On [Web Server Name: Status], confirm that the Interstage HTTP Server is operating.

Fail to connect to the Active Directory or cannot connect correctly.

Connection to the Active Directory failed due to the changes made in the machine network settings. Restart the Interstage management console and then perform the same operation again.

Display of site or path definition is extremely slow

The number of entries (user information, role configurations, protection resources) registered in the SSO repository is large, so it takes a long time to search site and path configurations.

To obtain this information (which is registered under "Protection Resource Registration Entry" (*1)), you can use the Interstage Directory Service Entry Management Tool or the *ldapsearch* command.

*1 In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Repository server detailed settings [Show]] > [Repository] > [Protection Resource Registration Entry].

6.2.10 Errors that may be Encountered while using the Interstage Directory Service Replication Function

The role information has been updated from the Interstage Management Console, but these modifications or additions are not successful.

If the SSO repository has been synchronized using the Interstage Directory Service replication function, synchronization may take several seconds in certain conditions; for example under heavy network load.

If role information is updated before being it can be synchronized, updates to a role configuration will not be reflected correctly.

In this case, update the role information, but ensure that the modifications made to the SSO repository (on the repository server (update system)) have first been reflected in the SSO repository (on the repository server (reference system)).

For information on how to make modifications or additions to the role configuration, see "Amending Role Configurations" in the "Authorization-related Operation" section of the Single Sign-on Operator's Guide.

The Entry Administration Tool can be used to identify entries in the SSO repository. For more information, refer to the "Entry Management" section of the Directory Service Operator's Guide.

For further information regarding the replication function, refer to the "Overview "section of the Directory Service Operator's Guide.

6.2.11 Errors in Upgrading from a Previous Version

After upgrading from a previous version, the Interstage Management Console operation or startup of the Repository server, Authentication server, and Business server fails

The upgrade procedure may have been incorrect for the following systems. Check that the upgrade procedure was correct.

- The "Broken environment." error message (sso04000, sso04304, sso04504, sso04704) is output while the Interstage Management Console is running.
- Startup of the Repository server, Authentication server, and Business server fails.
- Connection to the Repository server, Authentication server, and Business server fails.

After upgrading from a previous version, the access log is not generated

When upgrading from a previous version, the access log configuration may not have been set correctly. Check the access log settings in the environment configuration file.

If an application is used in an environment in which the repository server (reference system) is not used after the upgrade, the repository server (reference system) access log will not be generated.

For details on applications in which the repository server (reference system) is not used, refer to "Load Balancing".

Chapter 7 Developing Applications

Interstage SSO (single sign-on) supports authentication to Interstage single sign-on authentication servers and to develop applications with the use of reported user information.

This functionality can be used in Java EE and J2EE. When using J2EE, "IJServer cluster" will be referred to as "IJServer" throughout this document.

This chapter explains the provided application interface and describes how to develop applications.

From this point onwards, single sign-on authentication executed via a Web browser when accessing a protection resource in a business server is referred to as 'SSO authentication'. Authentication using a provided Java application interface is referred to as 'JAAS authentication'.

For details on application security, refer to "Security Risks and Measures" of "Security Risks" in "Application Programming" of the Security System Guide.

Windows32/64

Java EE common directory

The Java EE common directory can be specified at the time of installation. In the manual descriptions throughout this document, the Java EE common directory in the explanations is the default directory "C:\Interstage\F3FMisjee\var". If the Java common directory was changed during installation, this should be read as the directory that was changed from the default directory.

J2EE common directory

The J2EE common directory can be specified in implementation. In the following sections, it is assumed that the default J2EE common directory (C:\Interstage\J2EE\var\deployment) is used. If a directory other than the default is specified, replace the default value with the specified directory name in the following sections.

7.1 Developing Java Applications

This section explains how to develop Java applications using the Java application interface (hereafter referred to as "single sign-on JavaAPI") supported by Interstage single sign-on. The single sign-on JavaAPI class library is contained in the business server function.

The single sign-on JavaAPI uses the Java(TM) Authentication and Authorization Service (hereafter referred to as "JAAS") framework. Knowledge of JAAS application development is therefore required. For details on Java application development using JAAS, refer to the JAAS documents provided by Oracle.

To enable the use of JAAS authentication from a Java application, Interstage single sign-on supports the JAAS functions listed in the table below. For the API specifications for classes supported by the single sign-on JavaAPI (classes in packages under "com.fujitsu.interstage.sso"), refer to JavaDoc (javadocs_sso), which can be found in the "ApplicationServer\javadocs" folder on the Manual package.

Table 7.1 Functions Supported by Interstage Single Sign-on

Packaged Function	Explanation
Callback	Class for transferring information to be used for JAAS authentication (SSO authentication confirmation) to LoginModule
CallbackHandler	Class for setting information to be used for JAAS authentication (SSO authentication confirmation) in Callback. The application creator can implement this class separately.
LoginModule	Class with interface for JAAS authentication implemented
Credential	Class for storing credentials information set when JAAS authentication is successful
Principal	Class indicating an actor (such as user and role) set when JAAS authentication is successful

The following Java applications can be developed using the single sign-on JavaAPI:

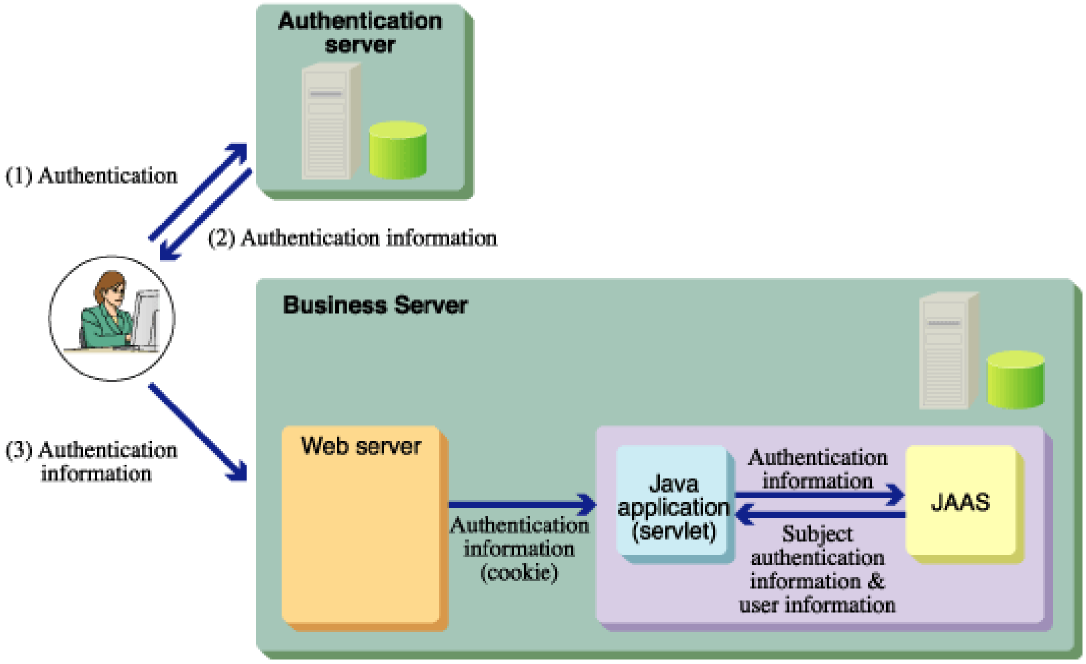
- Servlet application that receives authentication information from a client.

  After SSO authentication in a client (Web browser), this application uses a Servlet to receive authentication success information (confirming successful execution of SSO authentication) from the client. It then uses the received information to perform JAAS authentication and reference user information.

7.1.1 Program Development Flow

Servlet Application that Receives Authentication Information from a Client

Figure 7.1 Servlet Application That Receives Authentication Information from a Client


Authentication server
(1) Authentication
(2) Authentication information
Business Server
(3) Authentication information
Web server
Authentication information (cookie)
Java application (servlet)
Authentication information
JAAS
Subject authentication information & user information

After SSO authentication in a client (Web browser), a Servlet application receive authentication success information (confirming successful execution of SSO authentication) from the client via a Cookie. An application can be created that uses the Cookie value for JAAS authentication and uses user information.

Processing Flow

The following table provides processing flow information.

Table 7.2 Process Flow Information

Processing Flow	Required?	Explanation
1. Converting CallbackHandler to instance	Required	Set login information for JAAS authentication. Use the Cookie information set when SSO authentication succeeded for conversion.
2. Converting LoginContext to instance	Required	To prepare for JAAS authentication, specify the LoginModule and CallbackHandler to be used for JAAS authentication.
3. Calling LoginContext login method	Required	Perform JAAS authentication processing. Since JAAS authentication succeeded in SSO authentication, actual authentication is not executed for the authentication server.
4. Obtaining user information	Required to obtain authentication information on an authenticated user	Obtain user information (Credential object, Principal object).

Environment Setup

The following table lists the environment setup items required for application execution.

Table 7.3 Process Flow Information for Application Execution

Setup Item	Required?	Explanation
Setting environment variable	Required	Set the environment variables required for operation.
Creating login configuration file	Required	Create a login configuration file corresponding to the entry name specified when converting LoginContext to an instance.
Setting access permission for operated resources	Required	Set the access permission for the login configuration file. For security reasons, it is recommended that the permission settings be minimized.
Registering protection resources	Required	Register the Servlet as a protection resource.
Settings for using JavaAPI	Required to use session management	Configure the settings to use JAAS authentication.
Executing application	Required	Set the JavaVM options.

Obtaining User Information Without Using the JAAS Framework

Information on a user can be obtained as a character string from the HTTP header without using the JAAS framework. For information on obtaining the HTTP header value with a Servlet application, refer to the Servlet documents provided by Oracle. For details of the header names reported from a business server, refer to 7.2 Setting User Information Report with Environment Variables.

Note

The JAAS authorization function cannot be used with Servlet.

7.1.2 Developing Programs

This section explains how to develop a program that uses the single sign-on JavaAPI. The single sign-on JavaAPI uses the JAAS framework.

An example with sample code SampleServlet.java is shown below. This sample code is a Servlet application that receives information from the client confirming that authentication is already completed. It then displays authenticated user information.

Example

```
import java.io.IOException;
import java.io.PrintWriter;
import java.io.OutputStreamWriter;
import java.security.Principal;
import java.util.Iterator;
import java.util.Map;
import java.util.Set;
import javax.security.auth.Subject;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.login.LoginContext;
import javax.security.auth.login.LoginException;
import javax.servlet.ServletException;
import javax.servlet.http.Cookie;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import com.fujitsu.interstage.sso.auth.ISAuthorizationCredential;
import com.fujitsu.interstage.sso.auth.callback.ISCallbackHandler;

public class SampleServlet extends HttpServlet {
    public void doGet(HttpServletRequest request, HttpServletResponse response)
            throws ServletException, IOException
    {
        PrintWriter out = response.getWriter();
        response.setContentType("text/html; charset=Shift_JIS");
        Cookie cookie = null;
        Cookie[] cookies = request.getCookies();
        if (cookies != null){
            for (int i=0; i< cookies.length;i++){
                if (cookies[i].getName().equals(
                    ISAuthorizationCredential.COOKIE_KEY)){
                    cookie = cookies[i];
                }
            }
        }
        if (cookie == null ){
            out.println("<html>");
            out.println("<body>");
            out.println("No cookie information");
            out.println("</body>");
            out.println("</html>");
            return;
        }
        String credentialStr = cookie.getValue();
        LoginContext context = null;
        try{
            // Converting CallbackHandler to an Instance
            CallbackHandler myHandler = new ISCallbackHandler(credentialStr);
            // Converting LoginContext to an Instance
            context = new LoginContext(
                "com.fujitsu.interstage.sso",myHandler);
            // Calling LoginContext Login Method
            context.login();
        }
        catch(Exception ex){
            out.println("<html>");
            out.println("<body>");
            out.println("Exception : " + ex.getMessage());
            out.println("</body>");
            out.println("</html>");
            return;
        }
        // Obtaining User Information
        Subject subject = context.getSubject();
        Set principals = subject.getPrincipals();
        // display principal information
        out.println("<html>");
        out.println("<body>");
        out.println("<table>");
        Iterator p_iterator = principals.iterator();
        while (p_iterator.hasNext()) {
            Principal principal = (Principal)p_iterator.next();
            out.println("<tr>");
            out.println("<td>" + principal.getClass().getName() + "</td>");
            out.println("<td>" + principal.getName() + "</td>");
            out.println("</tr>");
        }
        out.println("</table>");
        out.println("</body>");
        out.println("</html>");
    }
}
```

7.1.2.1 Converting CallbackHandler to an Instance

To use JAAS, CallbackHandler must be converted to an instance. The single sign-on JavaAPI supports a CallbackHandler implementation class with the class name:

- com.fujitsu.interstage.sso.auth.callback.ISCallbackHandler.

The information required for authentication is passed from CallbackHandler to LoginModule via Callback.

Convert ISCallbackHandler to an instance with information indicating SSO authentication success obtained from the client. The target information is stored in a Cookie with the key name fj-is-sso-credential. The key name is defined in variable COOKIE_KEY of class com.fujitsu.interstage.sso.auth.ISAuthorizationCredential. The code is shown below.

```
Cookie cookie = null;
Cookie[] cookies = request.getCookies();
if (cookies != null){
  for (int i=0; i< cookies.length;i++){
    if (cookies[i].getName().equals(
      ISAuthorizationCredential.COOKIE_KEY)){
      cookie = cookies[i];
    }
  }
}
String credentialStr = cookie.getValue();
CallbackHandler myHandler = new ISCallbackHandler(credentialStr);
```

7.1.2.2 Converting LoginContext to an Instance

Convert the LoginContext to an instance. The code is shown below.

```
LoginContext Context = new LoginContext("com.fujitsu.interstage.sso",
                                               myHandler);
```

Use the following arguments for conversion:

- First argument

  Login configuration file entry name. For the login configuration file details, refer to "7.1.3.2 Creating Login Configuration File".

- Second argument

  Instances that were instantiated in "Converting CallbackHandler to an Instance".

7.1.2.3 Calling LoginContext Login Method

Authentication processing is executed by calling the LoginContext login method. LoginException or its subclass is thrown in the login method. Catch a thrown LoginException or its subclass. This is shown in the following example:

```
try{
  loginContext.login();
}
catch(FailedLoginException ex){
  System.out.println("Authenticate failed");
  continue;
}
```

7.1.2.4 Obtaining User Information

When JAAS authentication is executed successfully, the objects listed below are associated with the Subject object of the return value.

- Principal object that indicates the user ID of the authenticated user

- Principal object that indicates the name of the role to which the user belongs

- Principal object that indicates the unique distinguished name in the SSO repository.

Principal objects can be obtained with the following Subject object methods:

- public Set getPrincipals();
- public Set getPrincipals(Class c);

The difference between these methods is the same as the difference between the getPrivateCredentials methods.

The following table lists the classes of objects that can be associated with the Subject object.

Table 7.4 Object Classes Associated with the Subject Object

Class Name	Explanation
com.fujitsu.interstage.sso.auth.ISUserPrincipal	Indicates the user ID of an authenticated user.
com.fujitsu.interstage.sso.auth.ISRolePrincipal	Indicates the name of the role to which the user belongs. If the user belongs to a role set, roles in the role set are associated as ISRolePrincipal objects. No object is set unless the user belongs to a role.
javax.security.auth.x500.X500Principal	Indicates the unique distinguished name (DN) of the user in the SSO repository. Note the following points for development using the getName method of the java.security.Principal interface: - No space is inserted immediately after a DN delimiter (comma). Example: Value returned with getName method CN= user001,OU=User,OU=interstage,O=fujitsu,DC=com

The code is shown below.

```
Set principals = subject.getPrincipals();
iterator = principals.iterator();
while (iterator.hasNext()) {
  Principal principal = (Principal)iterator.next();
  System.out.println("Principal=" + principal.getClass().getName());
  System.out.println(principal.getName());
}
```

Reported User Information

When a business server configuration is used to specify an authentication server of the authentication destination, the following information (which is retained in the object ISAuthorizationCredential) is reported when "Yes" is selected for [Notify User Information?] on the Interstage Management Console.

- User DN
- Role name
- Authentication method
- User UID
- Client IP address
- Authentication time
- Re-authentication time
- Extended User Information

On the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name]. Select the [Settings] tab and click [Detailed Settings [Show]] then check [Notify User Information?] in [Linkage with Web applications]. For details, refer to the Operator's Guide.

IJServer cluster must be restarted to reflect the [Notify User Information?] settings. Restart IJServer cluster. For login configuration details, refer to "7.1.3.2 Creating Login Configuration File".

To check [Extended User Information], click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository Server] > [Settings] tab > [Repository server detailed settings[Show]] > [Information notified to the Business System] > [Extended user information] of the Interstage Management Console. For details on these settings, refer to the Interstage Management Console Help.

Reporting User Information at Indefinite Re-authentication Intervals

The re-authentication interval can be obtained using the ISAuthorizationCredential object getExpiration method. If the re-authentication interval is indefinite, the time obtained with the getAuthTime method is the same as that obtained with the getExpiration method.

7.1.3 Setting the Application Execution Environment

This section explains how the administrator for the operating application should set the environments required for application execution.

Java EE and J2EE can both be used as the application runtime environment.

7.1.3.1 Setting Environment Variables

Set the following paths (directory names/file names) in the environment variables CLASSPATH required for application operation:

Windows32/64

Table 7.5 Setting CLASSPATH Environment Variables for Windows

Definition	Values
CLASSPATH	Specify the following Java Archive (jar) file: - [Interstage install directory] \F3FMsso\ssoatzag\lib\isssomod14.jar

The environment variables are set as system environment variables. If a system environment variable is changed, restart the system.

Solaris32/64 Linux32/64

Table 7.6 Setting CLASSPATH Environment Variables for Solaris and Linux

Definition	Values
CLASSPATH	Specify the following Java Archive (jar) file: - /opt/FJSVssoaz/lib/isssomod14.jar

Using Java EE

Using the Interstage Java EE Admin Console, perform the following procedure to set the CLASSPATH environment variable:

1. Select [Clusters], then in the [Configuration] column, select [<IJServer-cluster>-config].
2. Select [JVM Settings].
3. In the [Path Settings] tab, set [Classpath Suffix].

Using J2EE

To configure the CLASSPATH environment variable settings, in the Interstage Management Console click [System] > [WorkUnit] > [IJServer] > [Settings], and set the classpath in [WorkUnit].

7.1.3.2 Creating Login Configuration File

The application operation administrator creates a login configuration file required for application execution. Any file name can be specified for system property java.security.auth.login.config at application execution time. In the login configuration file, write the login configuration in which a LoginModule provided by single sign-on JavaAPI is set. For login configuration file details, refer to the J2SDK and JAAS documents provided by Oracle.

Write the login configuration in the following format:

```
<entry-name> {
    <loginmodule-class-name> <flag> <module-option>;
};
```

Write the name specified when LoginContext is converted to an instance in entry-name. All symbols can be used if the entry name is enclosed with double or single quotation marks. Guidelines on the symbols that can be used if the entry name is not enclosed with double or single quotation marks are as follows.

Symbols that can be used without enclosing the entry name with double or single quotation marks:

- Dollar sign ($)
- Hyphen (-)
- Period (.)
- Underscore (_)

Set the following LoginModules provided by the single sign-on JavaAPI in loginmodule-class-name.

- com.fujitsu.interstage.sso.auth.module.ISCredentialLoginModule

Generally, "required" should be set in the flag. "requisite", "sufficient", and "optional" can also be set. For details, refer to the J2SDK and JAAS documents provided by Oracle.

In module-option, write the information used by LoginModule such as authentication infrastructure information of the authentication destination in list format where a blank character is used as a delimiter. Insert an equals sign between an option name and a value and enclose the value with double quotation marks. Use only lowercase letters to specify an option name to be used by LoginModule provided by the single sign-on JavaAPI. If an uppercase letter is used in an option name (or if an option name is specified incorrectly), it is assumed that the option name is omitted. Insert a semicolon at the end of LoginModule specification items.

Use the options shown in the table below in com.fujitsu.interstage.sso.auth.module.ISCredentialLoginModule.

Table 7.7 Option for module ISCredentialLoginModule

Option	Explanation
business-system-name	This is used to set the name of the business system for the business server used to run Java applications. To check the name of the business system, in the Interstage Management Console of the business server click [System] > [Security] > [Single Sign-on] > [Business System] > [List]. For details about the Interstage Management Console definition, refer to the Interstage Management Console Help.

File Encoding Mode for Login Configuration File

When characters other than alphanumeric characters and symbols are used in a login configuration file, store the login configuration using the following file encoding mode:

- UTF-8 encoding mode

Login configuration file examples are provided below. In the examples, the login configuration entry name com.fujitsu.interstage.sso is used.

Examples

Name of the business system for the business server: Business001

```
com.fujitsu.interstage.sso {
com.fujitsu.interstage.sso.auth.module.ISCredentialLoginModule required
    business-system-name="Business001"
    ;
};
```

Note

After switching from a previous version/level, if you are using a Java application that uses JAAS offered in Interstage Single Sign-on in an environment with more than one Interstage HTTP Server Web server or virtual host, check the module option of the login configuration file. If "serverport" is used for the module option, change it to "business-system-name".

7.1.3.3 Setting Access Permission for Operation Resources

Resources (such as the configuration file) are required for Java application operation and must be securely protected. This section explains how to set access permission to protect these resources.

The actual setting methods are shown below.

When Servlet Application Uses Business Server Configuration for Specifying an Authentication Server of the Authentication Destination

Windows32/64

Execute a Java application that uses a business server configuration as a user belonging to the Administrators group.

Solaris32/64 Linux32/64

So that it is possible even for an IJServer cluster service operator user to read the business server definition, make sure that the IJServer cluster service operator user and the user specified for the "User" directive in the Interstage HTTP Server environment definition file (httpd.conf) match.

If the IJServer cluster service operator user is set to a value other than "nobody", use the following procedure to configure the environment settings:

1. Execute the *useradd* command, for example, to create the new IJServer cluster service operator user. Ensure that the user is granted user privileges that are equal to the file access privileges of the user that was specified for the "User" directive in httpd.conf.
2. Set access permission for the created user as explained below.
3. Specify the user in the httpd.conf User directive.
4. Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab and click [Update].(*1)

*1 For further details, refer to "Changing Effective User for Web Server" in "Operation and Maintenance".

Setting Access Permission for Files

Windows32/64

Use Windows explorer to change user and group access permission. Set access permission as a user with Administrator authority.

Table 7.8 Setting Access Permissions for Files (Windows)

Resource	Explanation
Login configuration file	Permit only a Java application execution user (in the case of the servlet, this is the IJServer cluster service operator user) to read the file.

Solaris32/64 Linux32/64

Use a chmod or chown command. Set access permission with super user (root) authority.

Table 7.9 Setting Access Permissions for Files (Solaris and Linux)

Resource	Explanation
Login configuration file	Permit only a Java application execution user (in the case of the servlet, this is the IJServer cluster service operator user) to read the file.

7.1.3.4 Registering Protection Resources

The SSO administrator must register the servlet application path in the SSO repository as a protection resource and set its role name or role set name to enable its use.

For details, refer to "Registering Protection Resources" and "Using an LDIF File."

Information about the registered resource must then be stored in the business server. The business server administrator must use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Update access control information] tab and click [Update]. For details on Interstage Management Console definition, refer to the Operator's Guide.

For information on updating access control information, refer to "Amending Role Configuration" and "Amending Protection Resource" in "Operation and Maintenance".

Protection resource to be registered:

```
Business-server-name:port-number/servlet-application-path
```

7.1.3.5 Settings for Using JavaAPI

If session management is used, log in as the Business server administrator, and in the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]] > [Single Sign-on JavaAPI]. Change the [Use Single Sign-on JavaAPI?] settings to "Yes", and then click [Update].

7.1.3.6 Exceptions and Exception Handling

When an exception occurs in a single sign-on JavaAPI, check the exception object type and detailed message obtained with the exception object getMessage method and take the required action after referring to the Messages manual.

Example

Message displayed when authentication fails

```
Error: Authentication failed
```

If the OutOfMemoryError exception occurs, then take action according to "JDK/JRE Tuning" - "Identifying the Causes of Errors" - "When java.lang.OutOfMemoryError is Thrown" in the "Tuning Guide".

7.1.4 Executing Applications

This section explains how to execute a Java application that uses the single sign-on JavaAPI.

(1) Setting System Property

To execute a Java application that uses the single sign-on JavaAPI, the following system property must be set on JavaVM activation.

Table 7.10 Setting System Properties (JavaAPI)

System Property	Value to be Set
java.security.auth.login.config	Login configuration file absolute path name

Using Java EE

Using the Interstage Java EE Admin Console, perform the following procedure to set the system property:

1. Select [Clusters], then in the [Configuration] column, select [<IJServer>-config].
2. Select [JVM Settings].
3. In the [JVM Options] tab, change "java.security.auth.login.config".

Using J2EE

Set the system properties in the JavaVM option of the IJServer WorkUnit environment settings in the Interstage Management Console.

Note

The same system property value is used by all applications that operate within the same VM.

(2) Activating Application

Using Java EE

Start the IJServer cluster.

Using J2EE

Start the IJServer WorkUnit.

When Reactivation of an Application is Required

An application must be reactivated if a login configuration is updated; settings are changed in [Report User Information] in [Linkage with Web Application] in the business server environment setup; or the business system is re-set up. If the application is a servlet application, stop IJServer cluster before reactivating it.

7.1.5 Sample Code

This section explains how to use single sign-on JavaAPI sample codes.

Executing these samples requires single sign-on environments set up according to "Environment Setup (SSO Administrators)" and "Environment Setup (SSO Business Server Administrators)."

Outline

A servlet application sample receives authentication information confirming successful authentication from a client and displays information on the authenticated user. To use a sample, a Web server linked to the servlet must be set up as a business server.

Table 7.11 Business Server setup

URL	Application	Registration of Protection Resource
http(s)://Business server name:port number/jaassample/SampleServlet	Servlet application that receives authentication success confirmation from a client	Required

Sample Code Storage Location

Sample codes are stored in the following directories (hereafter referred to as sample directories).

Windows32/64

Interstage install directory: C:\Interstage

C:\Interstage\F3FMsso\ssoatzag\sample\javaapi

Solaris32/64 Linux32/64

/opt/FJSVssoaz/sample/javaapi

The following table lists the files required to execute the sample code.

Table 7.12 Sample Code

File	Explanation
jaassample.war	War file
webapp/jaassample/WEB-INF/isssojaaslogin.conf	Servlet login configuration file
webapp/jaassample/WEB-INF/web.xml	Web application environment configuration file (Deployment Descriptor)
SampleServlet.java	Servlet java source file

7.1.5.1 Procedure used to Execute the Sample Code in Java EE

Execution Procedure

(1) Servlet Service Environment Setup

Solaris32/64 Linux32/64

To enable the IJServer cluster user to read the business server configuration, set up the environment as follows.

1. Use the useradd command to create an IJServer cluster user.

2. Grant the created user authority equivalent to the file access permission of the user specified in the User directive in the Interstage HTTP Server environment configuration file (httpd.conf).

3. Specify the name of the created user in the User directive in the httpd.conf file.

4. Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab and click [Update]. (*1)

*1 For details, refer to "Changing Effective User for Web Server" in "Operation and Maintenance".

(2) Deploying Servlet Application

Deploy the servlet application to the Servlet container. The Interstage Java EE Admin Console is used for the deployment. The example here explains the deployment to the IJServer cluster called "IJServer". For details on the IJServer cluster, refer to "Functionality provided in the Java EE application" - "IJServer Cluster" in the "Java EE Operator's Guide".

If the "IJServer" IJServer cluster has not been created, create a new IJServer cluster with this name.

Use the following procedure to deploy a servlet application:

1. Using the Interstage Java EE Admin Console, select [Clusters], and click [New].

2. In the [New Cluster] window, set the following values:

   [Name]: "IJServer"

   [Configuration]: Select "default-config".

3. Select [Make a copy of the selected Configuration].

4. Create the server instance.

   In [Server Instances to be Created], click [New].

   In [Instance Name], type "instance".

   Click [OK].

5. Set the Web server connector that will link to the "IJServer" created.

   Select [Clusters] > [IJServer].

   In the [Web Server Connector] tab, select "the Web server that integrates with the business server", and then click [Save].

6. Deploy the servlet application.

   Select [Clusters] > [IJServer].

   In the [Applications] tab, click [Deploy].

   In the [Deploy Enterprise Applications/Modules] page, set [Type] to [Web Application (.war)], select [Packaged file to be uploaded to the server] and enter the jaassample.war file stored in the sample directory.

   Note that, when the machine on which the Interstage Java EE Admin Console has been installed is different from the machine using the Console, select [Local packaged file or directory that is accessible from the Application Server], and enter the path of the jaassample.war file stored in the machine on which the Interstage Java EE Admin Console has been installed:

   Windows32/64

   Interstage install directory: C:\Interstage

   ```
   C:\Interstage\F3FMsso\ssoatzag\sample\javaapi\jaassample.war
   ```

   Solaris32/64 Linux32/64

   ```
   /opt/FJSVssoaz/sample/javaapi/jaassample.war
   ```

7. Click [OK].

   The sample application is deployed to the following directory:

   Windows32/64

   Interstage install directory: C:\Interstage

```
C:\Interstage\F3FMisjee\var\domains\interstage\applications\j2ee-modules\jaassample
```

Solaris32/64 Linux32/64

```
/var/opt/FJSVisjee/domains/interstage/applications/j2ee-modules/jaassample
```

(3) Setting the IJServer cluster

Using the Interstage Java EE Admin Console, set the class path and JavaVM options:

1. Select [Clusters], then in the [Configuration] column, select [<IJServer-cluster>-config].
2. Select [JVM Settings].
3. In the [Path Settings] tab, set [Classpath Suffix].

   Windows32/64

   Interstage install directory: C:\Interstage

   ```
   C:\Interstage\F3FMsso\ssoatzag\lib\isssomod14.jar
   ```

   Solaris32/64 Linux32/64

   ```
   /opt/FJSVssoaz/lib/isssomod14.jar
   ```

4. Click [Save].
5. In the [JVM Options] tab, change "-Djava.security.auth.login.config".

   Windows32/64

   ```
   -Djava.security.auth.login.config=C:\Interstage\F3FMisjee\var\domains\
   interstage\applications\j2ee-modules\jaassample\WEB-INF\isssojaaslogin.conf
   ```

   Solaris32/64 Linux32/64

   ```
   -Djava.security.auth.login.config=/var/opt/FJSVisjee/domains/interstage/
   applications/j2ee-modules/jaassample/WEB-INF/isssojaaslogin.conf
   ```

6. Click [Save].

(4) Editing the Login Configuration File

Set the name of the name of the business system for the business server used to run Servlet applications.

Using a text editor, edit the value set for business-system-name in the isssojaaslogin.conf login configuration file stored in the Servlet application deployed in (2) above.

Path name in which the login configuration file is deployed by default:

Windows32/64

Interstage install directory: C:\Interstage

```
C:\Interstage\F3FMisjee\var\domains\interstage\applications\j2ee-modules\jaassample\WEB-INF
\isssojaaslogin.conf
```

Solaris32/64 Linux32/64

```
/var/opt/FJSVisjee/domains/interstage/applications/j2ee-modules/jaassample/WEB-INF/
isssojaaslogin.conf
```

Example

A login configuration file where the business system for the business server used to run the Servlet application is "Business001"

Entry "com.fujitsu.interstage.sso" is used by a Servlet application that receives authentication information from a client.

```
/**
*  sample login config file
```

```
*/

com.fujitsu.interstage.sso{
  com.fujitsu.interstage.sso.auth.module.ISCredentialLoginModule Required
  business-system-name="Business001" <- Edit here.
  ;
};
```

(5) Registering Certificate

Obtain both the authentication server site certificate and the CA certificate from the site certificate issuer and register them in the business server Interstage certificate environment. If a load balancer is used, use a site certificate issued with the load balancer FQDN.

(6) Defining Servlet Application as a Protection Resource

The SSO administrator should register the Servlet application URL in the SSO repository as a protection resource.

1. Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] tab and click [Protection resource]. When [Protection resource] is displayed, a list of sites is displayed under the [Protection resource] tree.
2. Click the site configuration of the business server to which the sample application is deployed.
3. Click [Protection path] to display the path configuration list window and then select the [Create a New Path configuration] tab.
4. Enter /jaassample/SampleServlet in [Path] as the access control target path then select the check box for a role name with which the protection resource can be used.
5. Click [Create] to display and check the specified path and role information.

Servlet application URL

```
http(s)://Business server name:port number/jaassample/SampleServlet
```

Protection resource to be registered

```
Business server name:port number/jaassample/SampleServlet
```

Example

Protection resource to be registered: "www.fujitsu.com:80/jaassample/SampleServlet"

Name of role name that can use protection resources: "Admin"

The business server site configuration (www.fujitsu.com:80) and role configuration need be registered in the SSO repository before registering a protection resource. If these configurations are not registered in the SSO repository, refer to "Using an LDIF File" and "Registering Protection Resources" to register them.

(7) Updating Business Server Access Control Information

The business server administrator stores information on a protection resource registered in the business server in Step (6). Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Update access control information] tab and click [Update]. For details on Interstage Management Console definition, refer to the Operator's Guide. For information on updating access control information, refer to "Amending Role Configuration" and "Amending Protection Resource" in "Operation and Maintenance".

(8) Changing Setting for Business Server Linkage to Web Application

Log in as the Business Server administrator, and in the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab. Click [Detailed Settings [Show]] then select [Linkage with Web applications] > [Notify User Information?] to select the setting to "Yes" and click [Update].

(9) Changing the Business Server Single Sign-on JavaAPI settings

If session management is used, Log in as the Business Server administrator, and in the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]] > [Single Sign-on JavaAPI]. Select the [Use Single Sign-on JavaAPI?] setting to "Yes", and then click [Update].

(10) Activating Business Server

Activate the business server. For Web server activation details, refer to "Starting Business Server."

(11) Activating Servlet Service

In the Interstage Java EE Admin Console, select [Clusters] > [IJServer]. In the [General] tab, click [Start].

(12) Calling Servlet Application from Web Browser

Specify the URL in the business server by using the Web browser as shown below.

Example

Using SSL communication when the business server is "www.fujitsu.com:80"

```
https://www.fujitsu.com:80/jaassample/
```

Using non-SSL communication when the business server is "www.fujitsu.com:80"

```
http://www.fujitsu.com:80/jaassample/
```

(13) Execution Result

"SSO Authentication" is displayed in the Web browser.

Click "SSO Authentication" to display the certificate selection window, the form authentication page, and basic authentication window. Select the certificate of a user belonging to the role with which the protection resource was registered in Step (6) or enter the user ID/ password. When the authentication is successful, authentication information on the authenticated user is displayed in the Web browser window.

An execution example is shown below.

Example

When user "user001" belonging to role "Admin" is authenticated successfully.

```
com.fujitsu.interstage.sso.auth.ISUserPrincipal user001
javax.security.auth.x500.X500Principal CN=user001,OU=User,OU=interstage,O=fujitsu,DC=com
com.fujitsu.interstage.sso.auth.ISRolePrincipal Admin
```

Note

If "No cookie information" is output in the Web browser window, it means that the Business Server Single Sign-on JavaAPI settings are not changed. Check the execution procedure and change the settings.

7.1.5.2 Procedure used to Execute the Sample Code in J2EE

Execution Procedure

(1) Servlet Service Environment Setup

Solaris32/64 Linux32/64

To enable the IJServer user to read the business server configuration, set up the environment as follows.

1. Use the *useradd* command to create an IJServer user.
2. Grant the created user authority equivalent to the file access permissions of the user specified in the User directive in the Interstage HTTP Server environment configuration file (httpd.conf).
3. Specify the name of the created user in the User directive in the httpd.conf file.
4. Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab and click [Update]. (*1)

*1 For details, refer to "Changing Effective User for Web Server" in "Operation and Maintenance".

(2) Deploying the Servlet Application

Use the Interstage Management Console to deploy the servlet application in a servlet container. The example below shows how to deploy an application in the IJServer WorkUnit "IJServer". For IJServer details, refer to "Design of J2EE Application" in "Environment Where J2EE Applications are Operated (IJServer)" in the "J2EE User's Guide".

If the IJServer WorkUnit "IJServer" has not been created, create a new IJServer with the name "IJServer" of either of the following types:

- Run Web/EJB applications on a single JavaVM
- Run Web/EJB applications on separate JavaVMs
- Web Application Only

Use the following procedure to deploy a servlet application:

1. Use the Interstage Management Console to select [System] > [WorkUnit] > [IJServer] tab and click [Deploy].
2. Clear the check box specifying not to start IJServer automatically after completing deployment.
3. Click [Reference] in [Deployment File] to select jaassample.war stored in the sample directory.

   The Interstage Management Console may be installed on a server different from the Web browser execution server on which the console is operated. If so, specify the jaassample.war path in the server containing the console directly in the deployment file text box as shown below, after choosing the radio button "Deploys files stored on the server".

   Windows32/64

   Interstage install directory: C:\Interstage

   C:\Interstage\F3FMsso\ssoatzag\sample\javaapi\jaassample.war

   Solaris32/64 Linux32/64

   /opt/FJSVssoaz/sample/javaapi/jaassample.war

4. Click [Deploy] to deploy the file after specifying the jaassample.war path.

The sample application is deployed in the following directories:

Windows32/64

Interstage install directory: C:\Interstage

```
C:\Interstage\J2EE\var\deployment\ijserver\IJServer\apps\jaassample.war
```

Solaris32/64 Linux32/64

```
/opt/FJSVj2ee/var/deployment/ijserver/IJServer/apps/jaassample.war
```

(3) Setting the IJServer WorkUnit

Use the Interstage Management Console to select the [System] > [WorkUnit] > [IJServer] tab and click [Settings]. Set a class path and JavaVM options with [WorkUnit] as shown below.

Windows32/64

Interstage install directory: C:\Interstage

Class path

```
C:\Interstage\F3FMsso\ssoatzag\lib\isssomod14.jar
```

JavaVM option

```
-Djava.security.auth.login.config=C:\Interstage\J2EE\var\deployment\ijserver
\IJServer\apps\jaassample.war\WEB-INF\isssojaaslogin.conf
-Djavax.net.ssl.trustStore=C:\Interstage\etc\security\env\keystore\.keystore
```

Solaris32/64 Linux32/64

Class path

```
/opt/FJSVssoaz/lib/isssomod14.jar
```

JavaVM option

```
-Djava.security.auth.login.config=/opt/FJSVj2ee/var/deployment/ijserver/IJServer/apps/
jaassample.war/WEB-INF/isssojaaslogin.conf
-Djavax.net.ssl.trustStore=/etc/opt/FJSVisscs/security/env/keystore/.keystore
```

(4) Editing the Login Configuration File

Set the name of the name of the business system for the business server used to run Servlet applications.

Using a text editor, edit the value set for business-system-name in the isssojaaslogin.conf login configuration file stored in the Servlet application deployed in (2) above.

The path name in which the login configuration file is deployed by default:

Windows32/64

Interstage install directory: C:\Interstage

```
C:\Interstage\J2EE\var\deployment\ijserver\IJServer\apps\jaassample.war\WEB-INF
\isssojaaslogin.conf
```

Solaris32/64 Linux32/64

```
/opt/FJSVj2ee/var/deployment/ijserver/IJServer/apps/jaassample.war/WEB-INF/isssojaaslogin.conf
```

Example

A login configuration file where the business system for the business server used to run the Servlet application is "Business001"

Entry "com.fujitsu.interstage.sso" is used by a Servlet application that receives authentication information from a client.

```
/**
*  sample login config file
*/

com.fujitsu.interstage.sso{
  com.fujitsu.interstage.sso.auth.module.ISCredentialLoginModule Required
  business-system-name="Business001" <- Edit here.
  ;
};
```

(5) Registering Certificates

Obtain both the authentication server site certificate and the CA certificate from the site certificate issuer and register them in the business server Interstage certificate environment. If a load balancer is used, use a site certificate issued with the load balancer FQDN.

(6) Defining the Servlet Application as a Protection Resource

The SSO administrator should register the Servlet application URL in the SSO repository as a protection resource.

1. Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] tab and click [Protection resource]. When [Protection resource] is displayed, a list of sites is displayed under the [Protection resource] tree.
2. Click the business server site configuration to which the sample application is deployed.
3. Click [Protection path] to display the path configuration list window and then select the [Create a New Path configuration] tab.
4. Enter /jaassample/SampleServlet in [Path] as the access control target path then select the check box for a role name with which the protection resource can be used.
5. Click [Create] to display and check the specified path and role information.

Servlet application URL

```
http(s)://Business server name:port number/jaassample/SampleServlet
```

Protection resource to be registered

```
Business server name:port number/jaassample/SampleServlet
```

Example

Protection resource to be registered: "www.fujitsu.com:80/jaassample/SampleServlet"

Name of role name that can use protection resources: "Admin"

The business server site configuration (www.fujitsu.com:80) and role configuration need be registered in the SSO repository before registering a protection resource. If these configurations are not registered in the SSO repository, refer to "Using an LDIF File" and "Registering Protection Resources" to register them.

(7) Updating the Business Server Access Control Information

The business server administrator stores information on a protection resource registered in the business server in Step (6). Use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Update access control information] tab and click [Update]. For details on Interstage Management Console definition, refer to the "Operator's Guide". For information on updating access control information, refer to "Amending Role Configuration" and "Amending Protection Resource" in "Operation and Maintenance".

(8) Changing the Setting for Business Server Linkage to Web Applications

Log in as the Business Server administrator, and in the Interstage Management Console select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab. Click [Detailed Settings [Show]] then select [Linkage with Web applications] > [Notify User Information?] to change the setting to "Yes" and click [Update].

(9) Changing the Business Server Single Sign-on JavaAPI settings

If session management is used, log in as the Business Server administrator, and in the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]] > [Single Sign-on JavaAPI]. Change the [Use Single Sign-on JavaAPI?] setting to "Yes", and click [Update].

(10) Activating the Business Server

Activate the business server. For Web server activation details, refer to "Starting Business Server."

(11) Activating the Servlet Service

Use the Interstage Management Console to select [System] > [WorkUnit] > [IJServer] tab. Click [Status] then click [Start] to activate the WorkUnit.

(12) Calling the Servlet Application from a Web Browser

Specify the URL in the business server by using the Web browser as shown below.

Example

Using SSL communication when the business server is "www.fujitsu.com:80"

```
https://www.fujitsu.com:80/jaassample/
```

Using non-SSL communication when the business server is "www.fujitsu.com:80"

```
http://www.fujitsu.com:80/jaassample/
```

(13) Execution Result

"SSO Authentication" is displayed in the Web browser.

Click "SSO Authentication" to display the certificate selection window, the form authentication page, and the basic authentication window. Select the certificate for a user belonging to the role with which the protection resource was registered in Step (6) or enter the user ID/password. When the authentication is successful, authentication information on the authenticated user is displayed in the Web browser window.

An execution example is shown below.

Example

When user "user001" belonging to the role "Admin" is authenticated successfully.

```
com.fujitsu.interstage.sso.auth.ISUserPrincipal user001
javax.security.auth.x500.X500Principal CN=user001,OU=User,OU=interstage,O=fujitsu,DC=com
com.fujitsu.interstage.sso.auth.ISRolePrincipal Admin
```

Note

If "No cookie information" is output in the Web browser window, it means that the Business Server Single Sign-on JavaAPI settings are not changed. Check the execution procedure and change the settings.

7.2 Setting User Information Report with Environment Variables

Information on an authenticated user can be used in a Web application such as a CGI operating on a business server. A business server reports information to a Web application by attaching it to an HTTP request header. The Web application can obtain the information by referencing the HTTP request header through the corresponding interface. For example, a CGI can obtain information from an environment variable.

The table below lists the information that can be obtained by a Web application.

Table 7.13 Information that can be Obtained by a Web Application

User Information	Explanation	Example
User DN	The user entry stored in user information in the SSO repository is reported using DN.	cn=user001,ou=interstage,o=fujitsu,dc=com
Role name	The role name set in the user entry stored in user information in the SSO repository is reported. If two or more role names are set, they are reported by inserting commas between them. If a role set is set, the role name(s) set in it are reported. If a role name is not set, a space is reported.	Admin,General,Leader
Number of role names	The number of reported role names is reported.	3
Authentication method	The authentication method (basicAuth, certAuth, or basicAuthAndCertAuth) of the authenticated user is reported. When the authentication method "password authentication or certificate authentication" is set, basicAuth is reported for success in password authentication or certAuth is reported for success in certificate authentication.	basicAuth
User ID	The user ID presented by the user for password authentication is reported.	user001
Client IP address	The client IP address used for authentication is reported in IPv4 or IPv6 format.	xxx.xxx.xxx.xxx
Authentication time	The time at which the user was authenticated is reported in Greenwich time (YYYYMMDDHHMMSSZ).	20030901151118Z
Re-authentication time	The time at which re-authentication was required is reported in Greenwich time (YYYYMMDDHHMMSSZ).	20030901154118Z
Valid range for authentication information	The valid range for the authentication information is reported.	www.fujitsu.com
Time of the previous Sign-on (*1)	The time of the previous Sign-on is reported in Greenwich time (YYYYMMDDHHMMSSZ). The first time a user signs on to the Single Sign-on system, a space is reported.	20050713000000Z

User Information	Explanation	Example
Extended User Information (*2)	Optional information about the authenticated user is reported.	For mail: tarou@fujitsu.com

*1 This can only be notified if session management is used.

*2 This is notified if the following conditions apply:

- Session management is used.
- The attribute name was set by clicking [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Repository server detailed settings [Show]] > [Information notified to the Business System] of the Interstage Management Console, then setting it in [Extended User Information].
- In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Protected resource] > [Site definition] > [Protected path] > [Path definition] > [Settings] > [Path definition] > [Notify Extended User Information], then select the attribute name set above.

To report user information to a Web application, use the Interstage Management Console to select [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab. Click [Detailed Settings [Show]] then select [Linkage with Web applications] > [Notify User Information?] and click "Yes."

Usage in Web Application

User information is reported with the environment variable names and HTTP request headers listed below. Values to be reported are encoded in UTF-8 format.

Table 7.14 User Information in Web Applications

User Information	Environment Variable Names	HTTP Request Header
User DN	HTTP_X_FJ_SSO_CREDENTIAL_DN	X-FJ-SSO-CREDENTIAL-DN: Value
Role name	HTTP_X_FJ_SSO_CREDENTIAL_ROLELIST	X-FJ-SSO-CREDENTIAL-ROLELIST: Value
Number of role names	HTTP_X_FJ_SSO_CREDENTIAL_ROLECOUNT	X-FJ-SSO-CREDENTIAL-ROLECOUNT: Value
Authentication method	HTTP_X_FJ_SSO_CREDENTIAL_AUTHMETHOD AUTH_TYPE (*1)(*2)	X-FJ-SSO-CREDENTIAL-AUTHMETHOD: Value
User UID	HTTP_X_FJ_SSO_CREDENTIAL_UID REMOTE_USER (*1)(*2)	X-FJ-SSO-CREDENTIAL-UID: Value
Client IP address	HTTP_X_FJ_SSO_CREDENTIAL_IPADDRESS	X-FJ-SSO-CREDENTIAL-IPADDRESS: Value
Authentication time	HTTP_X_FJ_SSO_CREDENTIAL_FIRSTACCESS	X-FJ-SSO-CREDENTIAL-FIRSTACCESS: Value
Re-authentication time	HTTP_X_FJ_SSO_CREDENTIAL_EXPIRATION	X-FJ-SSO-CREDENTIAL-EXPIRATION: Value
Valid range for authentication information	HTTP_X_FJ_SSO_CREDENTIAL_DOMAIN	X-FJ-SSO-CREDENTIAL-DOMAIN: Value
Time of the previous Sign-on (*3)	HTTP_X_FJ_SSO_SSOLASTSIGNONTIME	X-FJ-SSO-SSOLASTSIGNONTIME:Value
Extended User Information (*4)	HTTP_X_FJ_SSO_EXT_xxxx(*5)	X-FJ-SSO-EXT-xxxx: Value (*5)

*1 This is only reported when Interstage HTTP Server is used as the Web server. The reporting method for user information can be changed by adding the following definition items to the business server environment definition file as shown below.

Environment definition file

Windows32/64

```
C:\Interstage\F3FMsso\ssoatzag\conf\ssoatzag.conf
```

Solaris32/64 Linux32/64

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

Additional definitions

The following definition items can be added:

- header-auth-type-default="string"

  The value specified for "string" is reported with AUTH_TYPE regardless of the authentication method.

  To report "SSO_AUTH", define it as follows:

  header-auth-type-default=SSO_AUTH

- set-http-header-auth-type=NO

  The authentication method is not reported with AUTH_TYPE.

- set-http-header-uid=NO

  The user ID of the user is not reported with REMOTE_USER.

Note

- If "set-http-header-uid=NO" is added, the user ID of the user is not recorded in Audit Trail. If you are using Audit Trail, do not define "set-http-header-uid=NO".

- If the strings shown below are specified for header-auth-type-default, they are reported using AUTH_TYPE. However, if you are also using one of these strings in a web application of a previous version, you should confirm that operation continues normally when the same string is also reported using AUTH_TYPE in that version.

  - Basic
  - Digest
  - BASIC
  - DIGEST
  - FORM
  - CLIENT_CERT

*2 If this is used together with the Interstage HTTP Server authentication function, the authentication method and user ID for the user authenticated using the Interstage HTTP Server authentication function are stored in this environment variable.

*3 This can only be notified if session management is used.

*4 This is notified if the following conditions apply:

- Session management is used.

- The attribute name was set by clicking [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Repository server detailed settings [Show]] > [Information notified to the Business System] of the Interstage Management Console, then setting it in [Extended User information].

- In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Protection resource] > [Site] configuration> [Protection path] > [Path configuration] > [Settings] > [Path configuration] > [Extended User Information], then select the attribute name set above.

*5 'xxxx' is the attribute name set for [Extended user information]. These are all upper case characters.

Example

When "mail" is set for [Extended user information]

Environment Variable Names	HTTP Request Header
HTTP_X_FJ_SSO_EXT_MAIL	X-FJ-SSO-EXT-MAIL:Value

Notes

- In applications in which session management is not used, the information reported to a Web application must be within the size specified below. If it exceeds the maximum size, authentication fails.

  2048 bytes less than or equal to ((128 bytes + DN character string length) + user ID character string length + 8 bytes * number of roles + sum of role name character string lengths) * 1.5 + character string length of business server URL accessed by the user at authentication

  * Each character string length is represented in units of bytes.

- Only alphanumeric characters and symbols can be used in the user information reported to a Web application. If other characters are used in information reported to a Web application, the Web application may not obtain the correct value.
- The URL of the attribute value reported is encoded, decode it in the application.
- If the attribute value is binary data, this can be obtained by decoding the URL and then decoding the Base64 string.
- If the attribute value is not binary data, the UTF8 character code can be obtained by decoding the URL.
- If there is more than one attribute value, each value should be separated using a comma (,). For this reason, separate the values using a comma (,) and then decode to obtain the value.
- If the binary data is reported in Extended User Information exceeds dozens of KBytes, authorization performance may deteriorate, therefore only report information that is required for the business application. When more than one business application is run on one server and user information required for each application is different, authorization performance can be improved by using a separate server for each application and reducing the size of user information that is reported.

7.3 Setting the Sign-off URL Report with Environment Variables

The Sign-off URL can be used in a Web application, such as a CGI operating on a Business Server. A Business Server reports a Sign-off URL to a Web application by attaching it to an HTTP request header. The Web application can obtain the Sign-off URL by referencing the HTTP request header through the corresponding interface. For example, a CGI can obtain information from an environment variable.

To notify the Web application of the Sign-off URL, in the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] > [Detailed Settings [Show]] > [Linkage with Web applications]. Set "Yes" for [Notify Sign-off URL?].

The Sign-off URL can only be notified if session management is used.

Usage in Web Application

The Sign-off URL is reported with the environment variable names and HTTP request headers listed below. Values to be reported are encoded in UTF-8 format.

Table 7.15 the Sign-off URL in Web Applications

Environment Variable Names	HTTP Request Header	Example
HTTP_X_FJ_SSO_SIGN_OFF_URL	X-FJ-SSO-SIGN-OFF-URL: Value	https://authserver.fujitsu.com:443/ssoatcag?fj-is-sso-request=sign-off

Appendix A Notes on Previous Versions

A.1 Using Commands of Previous Versions

The following table explains how the commands of previous versions can be used in this version.

Table A.1 Using Commands from Previous Versions

Command	Treatment of the command in this version	How the command is executed in the Interstage Management Console
ssomksid	Cannot be used if session management is used.	The command cannot be executed in the Interstage Management Console.
ssocloneac	Cannot be used. Use the *ssobackup* and *ssorestore* commands. (*1)	The command cannot be executed in the Interstage Management Console.
ssocloneaz	Use the *ssobackup* and *ssorestore* commands. (*1)	The command cannot be executed in the Interstage Management Console.

*1 For details about the *ssobackup* and *ssorestore* commands, refer to the "Backup Commands" chapter of the Reference Manual (Command Edition).

A.2 Service ID File

What is the service ID file?

The authentication information on a user registered in the SSO repository, such as mail address and employee number is fetched from the repository server on the basis of the certificate, user ID, and password the user used for authentication. The authentication information is posted to the business server through the authentication server. The service ID file is required to securely communicate the authentication information.

Creating the service ID file

In this version, the Interstage Management Console and commands are used to make the Interstage Single Sign-on environment settings and set up the system. For this reason, there is no need to be aware of the service ID file.

However, the service ID file is required in the following cases:

- Using JAAS authentication

If session management is not used, use the *ssomksid* command to create the service ID file.

A.3 Setting up a System Containing Mixed Previous Versions

For notes about setting up Interstage Single Sign-on systems containing mixed versions and editions, refer to "Notes about Setting up Single Sign-on Systems Containing Mixed Versions and Editions" in the "Notes on Interstage Single Sign-on" section of the Product Notes.

A.4 Improved Messages

Due to improvements made to messages and status codes, the output may be different to previous versions.

The following table explains messages and status codes improved from previous versions.

Messages improved in 8.0 from V7.0

Messages Beginning with 'sso'

Table A.2 Comparison of Message Text in 8.0 and V7.0

Previous message	New message
SSO: ERROR: sso01012: Internal error.	SSO: ERROR: sso01012: Internal error. Detail=(%s1) Code=(%s2)
SSO: WARNING: sso01032: Initialization of maintenance log failed.	SSO: ERROR: sso01032: Initialization of maintenance log failed.
SSO: ERROR: sso02009: Reading service ID file failed. Filename=(%s1)	SSO: ERROR: sso02009: Reading service ID file failed. Filename=(%s1) Reason=(%s2) Code=(%s3)
SSO: ERROR: sso02012: Invalid request was received. IPAddr=(%s1)	SSO: ERROR: sso02012: Invalid request was received. IPAddr=(%s1) Detail=(%s2) Code=(%s3)
SSO: ERROR: sso02017: Internal error.	SSO: ERROR: sso02017: Internal error. Code=(%s1)
SSO: ERROR: sso02018: Allocation of memory failed.	SSO: ERROR: sso02018: Allocation of memory failed. Size=(%s1) Code=(%s2)
SSO: ERROR: sso02020: Invalid environment of validity check of certificate. EnvDir=(%s1)	SSO: ERROR: sso02020: Invalid environment of validity check of certificate. EnvDir=(%s1) Detail=(%s2)
SSO: WARNING: sso02036: Initialization of maintenance log failed.	SSO: ERROR: sso02036: Initialization of maintenance log failed.
SSO: WARNING: sso03024: Initialization of maintenance log failed.	SSO: ERROR: sso03024: Initialization of maintenance log failed.
SSO: INFO: sso04203: The environmental configuration of the Repository server was updated. The Web Server (Interstage HTTP Server) is required to reboot ([System] > [Services] > [Web Server]).	SSO: INFO: sso04203: The environmental configuration of the Repository server was updated. The Web Server (Interstage HTTP Server) is required to reboot ([System] > [Services] > [Web Server]). (%s1)
SSO: INFO: sso04253: The environmental configuration of the Repository server was updated. The Web Server (Interstage HTTP Server) is required to read configuration and reboot by using Interstage Management Console of the Admin Server.	SSO: INFO: sso04253: The environmental configuration of the Repository server was updated. The Web Server (Interstage HTTP Server) is required to read configuration and reboot by using Interstage Management Console of the Admin Server. (%s1)
SSO: INFO: sso04401: The environmental configuration of the Authentication server was updated. The Web Server (Interstage HTTP Server) is required to reboot ([System] > [Services] > [Web Server]).	SSO: INFO: sso04401: The environmental configuration of the Authentication server was updated. The Web Server (Interstage HTTP Server) is required to reboot ([System] > [Services] > [Web Server]). (%s1)
SSO: INFO: sso04451: The environmental configuration of the Authentication server was updated. The Web Server (Interstage HTTP Server) is required to read configuration and reboot by using Interstage Management Console of the Admin Server.	SSO: INFO: sso04451: The environmental configuration of the Authentication server was updated. The Web Server (Interstage HTTP Server) is required to read configuration and reboot by using Interstage Management Console of the Admin Server. (%s1)
SSO: INFO: sso04601: The environmental configuration of the Business server was updated. The Web Server (Interstage HTTP Server) is required to reboot ([System] > [Services] > [Web Server]). Business server=(%s1)	SSO: INFO: sso04601: The environmental configuration of the Business server was updated. The Web Server (Interstage HTTP Server) is required to reboot ([System] > [Services] > [Web Server]). (%s2) Business server=(%s1)
SSO: INFO: sso04606: The environmental configuration of the Business server was updated. The Web Server is required to reboot. Business server=(%s1)	SSO: INFO: sso04606: The environmental configuration of the Business server was updated. The Web Server is required to reboot. (%s2) Business server=(%s1)
SSO: INFO: sso04651: The environmental configuration of the Business server was updated.	SSO: INFO: sso04651: The environmental configuration of the Business server was updated. The Web Server (Interstage HTTP

Previous message	New message
The Web Server (Interstage HTTP Server) is required to read configuration and reboot by using Interstage Management Console of the Admin Server. Business server=(%s1)	Server) is required to read configuration and reboot by using Interstage Management Console of the Admin Server. (%s2) Business server=(%s1)

Log Messages Output by Single Sign-on

The supplementary information for the access logs of the business servers shown below has been changed.

Previous message	New message
Attachment to a shared memory failed	Server error
Failed to allocate memory	Server error
Get cookie credential error	Violation request. or Server error
Get url Credential error	Violation request. or Server error
Server error[%s]	Server error.[%s]
Set up cookie failed	Violation request. or Server error

Messages improved in V9.0 from 8.0

Messages Beginning with 'sso'

Table A.3 Comparison of Message Text in 8.0 and V9.0

Previous message	New message
SSO: INFO: sso03015: Access control information was updated.	SSO: INFO: sso03015: Access control information was updated. Name=(%s1)
SSO: ERROR: sso03018: The length of URL is too long. (Location URL:%d1)	SSO: ERROR: sso03018: The length of URL is too long. Name=(%s1) (Location URL:%d2)
SSO: ERROR: sso03026: Acquisition of access control information failed. Code=(%x1)	SSO: ERROR: sso03026: Acquisition of access control information failed. Name=(%s1) Code=(%x2)
SSO: ERROR: sso03047: Invalid role setting in access control information.	SSO: ERROR: sso03047: Invalid role setting in access control information. Name=(%s1)
SSO: ERROR: sso03048: Updating of access control information failed. Filename=(%s1) Code=(%d2)	SSO: ERROR: sso03048: Updating of access control information failed. Name=(%s1) Filename=(%s2) Code=(%d3)
SSO: ERROR: sso04122: Smart Repository package is not installed.	SSO: ERROR: sso04122: Interstage Directory Service package is not installed.
SSO: ERROR: sso04362: Repository server environment is broken. Detail=(%d1,%s2)	SSO: ERROR: sso04362: The Repository server environment is broken. Detail=(%s1,%s2)
SSO: ERROR: sso04635: The Business server could not be added because there are already 32 Business servers on the same machine.	SSO: ERROR: sso04635: The Business server could not be added because there are already 256 Business servers on the same machine.
SSO: ERROR: sso04735: The Business server could not be added because there are already 32 Business servers on the same machine	SSO: ERROR: sso04735: The Business server could not be added because there are already 256 Business servers on the same machine
SSO: ERROR: sso04736: The environmental configuration of the Business server could not be updated because there are already 33 Business servers on the same machine	SSO: ERROR: sso04736: The environmental configuration of the Business server could not be updated because there are already 257 Business servers on the same machine.
SSO: ERROR: sso04742: Business server environment is broken. Detail=(%d1,%s2)	SSO: ERROR: sso04742: The Business server environment is broken. Detail=(%s1,%s2)

Previous message	New message
SSO: ERROR: sso13001: Invalid request was received. IPAddr=(%s1) Detail=(%s2) Code=(%s3)	SSO: ERROR: sso13001: Invalid request was received. Name=(%s1) IPAddr=(%s2) Detail=(%s3) Code=(%s4)
SSO: ERROR: sso13002: An invalid response was received. There is an inconsistency in the environment settings of the server from which the response originated. Host=(%s1) Detail=(%s2) Code=(%s3)	SSO: ERROR: sso13002: An invalid response was received. There is an inconsistency in the environment settings of the server from which the response originated. Name=(%s1) Host=(%s2) Detail=(%s3) Code=(%s4)
SSO: ERROR: sso13005: Request data is broken. IPAddr=(%s1) Detail=(%s2) Code=(%s3)	SSO: ERROR: sso13005: Request data is broken. Name=(%s1) IPAddr=(%s2) Detail=(%s3) Code=(%s4)
SSO: ERROR: sso13006: Response data is broken. Host=(%s1) Detail=(%s2) Code=(%s3)	SSO: ERROR: sso13006: Response data is broken. Name=(%s1) Host=(%s2) Detail=(%s3) Code=(%s4)
SSO: ERROR: sso13007: Analysis of request data failed. IPAddr=(%s1) Detail=(%s2) Code=(%s3)	SSO: ERROR: sso13007: Analysis of request data failed. Name=(%s1) IPAddr=(%s2) Detail=(%s3) Code=(%s4)
SSO: ERROR: sso13008: Analysis of response data failed. Host=(%s1) Detail=(%s2) Code=(%s3)	SSO: ERROR: sso13008: Analysis of response data failed. Name=(%s1) Host=(%s2) Detail=(%s3) Code=(%s4)

Messages output by Single Sign-on

ssosetsvc command

Previous message	New message
[0071]Abnormality occurred by Smart Repository	[0071]Abnormality occurred by Interstage Directory Service
[0072]Smart Repository package is not installed	[0072]Interstage Directory Service package is not installed

ssosignoff command

Previous message	New message
[0078]Specified session or user ID was not found : <session | user ID>	[0078]Specified session or user ID was not found : <session | user ID | global-session >

Messages output when an exception occurs in JavaAPI

Previous message	New message
Error: No definition found in Business server configuration file : ConfFile=%s1 ServerPort=%s2	Error: No definition found in Business server configuration file : ConfFile=%s1 %s2=%s3

Messages improved in V9.1 from V9.0

Status Codes Reported from the Browser

Table A.4 Client Error 403

Previous message	New message
Authentication is processing.	Waiting for authentication from another window or page... If authentication is not already in progress, click the following button to continue authentication processing.

Log Messages Output by Single Sign-on

The supplementary information for the access logs of the business servers shown below has been improved.

Previous message	New message
IPAddress check error	IPAddress check error.IPAddr=[%s]

IP address is not the same	IP address is not the same.IPAddr=[%s]

Settings for the output of messages from previous versions

If the following definition option is added to the environment configuration file, messages from previous versions can be output.

Repository server

Environment configuration file name

ssoatcsv.conf

Environment configuration file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcsv\conf
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssosv/conf
```

Addition definition option

```
use-old-syslog-sso01050=YES
use-old-syslog-sso01051=YES
```

Authentication server

Environment configuration file name

ssoatcag.conf

Environment configuration file storage directory

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\conf
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/conf
```

Addition definition option

```
use-old-syslog-sso02012=YES
use-old-syslog-sso02013=YES
use-old-syslog-sso02015=YES
use-old-syslog-sso02031=YES
use-old-syslog-sso02050=YES
```

Note

In environments upgraded from previous versions, the above definition is set automatically when the upgrade is performed. To output new messages, delete the above definition.

Change in the status code of the message output in the Web browser

The messages shown in the table below are output in the Web browser in versions/levels of Interstage Application Server 8.0 and earlier. The HTTP status code returned to the Web browser has changed from "403" to "200". The file names have also changed.

Note

- In environments that have been upgraded from a previous version/level, the existing "403" status code is returned. To change the status code that is returned from "403" to "200", perform the following steps:
    - Delete the new message files. (These will have a different name to the old message files, as shown in the table below.)

  - Keep the old message files, but rename them with the same name as the new message files (as shown in the table below). The new name will contain the new status code.

- When Microsoft(R) Internet Information Services 7.0 is used for the Web server in a business server that has been upgraded from 8.0, perform the following steps:

  - Delete the new message files. (These will have a different name to the old message files, as shown in the table below.)

  - Keep the old message files, but rename them with the same name as the new message files (as shown in the table below). The new name will contain the new status code.

Authentication server

Old message	New message	Contents that have changed
403auth_form_en.template	200auth_form_en.template	These are returned using status code 200.
403passwderr_form_en.template	200passwderr_form_en.template	
403authexpired_en.template	200authexpired_en.template	
403timedout_en.template	200timedout_en.template	
403queryforcedsignon_en.template	200queryforcedsignon_en.template	
403querysignoff_en.template	200querysignoff_en.template	

Business server

Old message	New message	Contents that have changed
403postauth_en.template	200postauth_en.template	These are returned using status code 200.
403closeerr_en.template	200closeerr_en.template	

A.5 Switching to an Application to Perform Session Management

To switch from a system that does not use session management to one that does, the environment must be changed. Note the points below:

Notes

- The environment settings that are changed must also be changed for all the servers in the Interstage Single Sign-on system.

- Before changing the environment settings, back up the Interstage Single Sign-on resources for all the servers. For details, refer to the "Maintenance (Resource Backup)" chapter of the Operator's Guide.

- If "certAuth" is set for the authentication method (ssoAuthType) for user information managed in the SSO repository, user authentication fails. Either change the user authentication format, or configure the settings so that certificate authentication is performed. (*1)(*2)

- In systems that use session management, the user ID must be set in the user information managed in the SSO repository. (*1)

- If load distribution is being used, check the settings for the load balancer. (*3)

*1 For details about the authentication method and user information, refer to "User Information Entry" in the "Environment Setup (SSO Administrators)" chapter.

*2 Refer to the "Settings for Performing Certificate Authentication in a System that Performs Session Management" chapter for more details.

*3 Refer to the "Load Balancer Settings" appendix for more details.

Procedure to change to Session Management

This is described separately for the following system configurations:

- A system that does not use repository server load balancing

- A system in which a repository server (update system) is installed on more than one server to perform load balancing

- A system in which the repository server and the authentication server are set up on one machine, and more than one server is used to perform load balancing
- A system in which load balancing is used in the repository server (update system) and the repository server (reference system)

A system that does not use repository server load balancing

Perform the following steps:

1. Change the Repository server
2. Change the Authentication server
3. Change the Business server
4. Change the Java application (*1)

*1 This should be performed for Interstage Single Sign-on JAAS Java applications.

The following tasks are performed by the SSO administrator.

1. Changing the Repository server

The procedure for changing the Repository server using the Interstage Management Console is described below:

1. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Session management detailed settings [Show]].
2. Check that "Yes" is set for [Use Session management?] in [Session management Setting], and then click [Update]. (*1) (*2)
3. Restart the Repository server.
4. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication infrastructure setup file].
5. Click [Detailed Settings [Show]], and check that "Yes" is set for [Use Session management?] in [Authentication Infrastructure Information Settings].
6. Set [Password], and click [Download] to download the Authentication infrastructure setup file to the machine used to start the Web browser.
7. To run the Authentication server, forward the Authentication infrastructure setup file to the Authentication server, and then delete the Authentication infrastructure setup file.
8. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Business system setup file].
9. Click [Detailed Settings [Show]], and check that "Yes" is set for [Use Session management] in [Authentication Infrastructure Information Settings]. (*3)
10. If you are running more than one business system, in Steps 11 and 12, perform the procedure for all Business systems.
11. Set the required options, and click [Download] to download the Business system setup file to the machine used to start the Web browser.
12. Send the Business system setup file to the Business server administrator, and then delete it.

*1 For details about using SSL communication in the Repository server, refer to "Procedure for changing a Repository Server to use SSL Communication" in the "Preparations for SSL Communication" chapter and configure the environment settings.

*2 To run the repository server on a cluster system, change the encryption information (service ID) file on the shared disk and change the environment configuration file. Change the standby node environment settings at the same time. For details, refer to the High Availability System Guide "Using Interstage Single Sign-on", "1) Setup in the operation node (node 1)" section, Steps 3 and 4.

Register the Interstage Single Sign-on status transition procedure. For details about the status transition procedure, refer to "Setting Cluster Service" in the "Environment Setup Procedure for Cluster Service" chapter of the High Availability System Guide.

*3 To link with Application Gateway and use non-SSL for communication between the Application Gateway and the Authentication server, the Authentication server URL referenced by the Business server must be changed before the Business server is restarted. Specify the Authentication server URL in [Authentication server URL] of [Authentication Infrastructure Information Settings]. For details on the Authentication server URLs referenced by Business systems, refer to "Choosing URLs", "URL Used by the Business System to Reference the Authentication Server" in the "Overview" chapter.

2. Changing the Authentication server

The procedure for changing the authentication server is described below. If you are using authentication server load balancing, perform the procedure for all authentication servers.

1. Forward to the authentication server the Authentication infrastructure setup file downloaded from the repository server (update system) for which the settings were changed to use session management.

2. Specify the Authentication infrastructure setup file forwarded in Step 1, and execute the *ssoimpac* command. For details about the *ssoimpac* command, refer to the "Single Sign-on Operation Commands" chapter of the Reference Manual (Command Edition).

3. In the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab.

4. Click [Detailed Settings [Show]], and check that "Yes" is set for [Use Session management?] in [Authentication Infrastructure Information Setting]. If "Yes" is not set, specify the invalid Authentication infrastructure setup file in Step 2 and execute the command. Repeat Step 1.

5. Restart the authentication server.

6. Delete the Authentication infrastructure setup file.

The following tasks are performed by the Business server administrator.

3. Changing the Business server

The procedure for changing the Business server is described below. If you are using business server load balancing, or using more than one business system, perform the procedure for all Business systems.

1. Create the Interstage certificate environment required for using SSL with the Authentication server. If the Interstage certificate environment has already been created, there is no need to perform this task. For details about creating the Interstage certificate environment, refer to "Creating the Interstage Certificate Environment" in the "Preparations for SSL Communication" appendix.

2. Obtain the Business system setup file downloaded from the Repository server (update system) for which the settings were changed to use session management from the SSO administrator.

3. Specify the Business system setup file obtained in Step 2 and execute the *ssoimpaz* command. To use Single Sign-on JavaAPI in the Business server, specify the -j option. For details about the *ssoimpaz* command, refer to the "Single Sign-on Operation Commands" chapter of the Reference Manual (Command Edition).

4. In the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Business system] > [Business system Name] > [Settings] tab.

5. Click [Detailed Settings [Show]], and check that "Yes" is set for [Use Session management?] in [Authentication Infrastructure Information Settings]. If "Yes" is not set, specify the invalid Authentication infrastructure setup file in Step 3 and execute the command. Repeat Step 2.

6. Add the following settings for the Business server integrated with the Web server if they have not already been configured:

   - Microsoft(R) Internet Information Services 6.0

     Perform Steps 5 to 12 and Step 16 in "Integrating with Microsoft(R) Internet Information Service 6.0" in the chapter "Environment Setup (Business Server Administrators)".

   - Microsoft(R) Internet Information Services 7.0,7.5

     Perform Steps 6 to 12 and Step 16 in "Integrating with Microsoft(R) Internet Information Service 6.0" in the chapter "Environment Setup (Business Server Administrators)".

   - Sun Java System Web Server 6.1

     Refer to "Integrating into Sun Java System Web Server 6.1" in the "Environment Setup (Business Server Administrators)" chapter, and add the required options to the environment configuration file.

7. Restart the business server.

8. Delete the Business system setup file.

4. Changing the Java application

If the application is an Interstage Single Sign-on JAAS Java application, change the application according to the following procedure. If the application uses a Business server configuration (the "serverport" option is specified in the login configuration file), change the Business server as well.

1. Obtain the Business system setup file downloaded from the Repository server (update system) for which the settings were changed to use session management from the SSO administrator.
2. Specify the Business system setup file obtained in Step 1 and execute the *ssoimpaz* command. For details about the *ssoimpaz* command, refer to the "Single Sign-on Operation Commands" chapter of the Reference Manual (Command Edition).
3. Restart the Java application.
4. Delete the Business system setup file.

A system in which a repository server (update system) is installed on more than one server to perform load balancing

Perform the following steps:

In this kind of system, first of all change the single repository server (update system) and then change all the remaining repository servers (update system) that are used for load balancing.

1. Change the Repository server (update system)
    - Change the repository server (update system)
    - Change the repository servers (update system) that are used for load balancing
2. Change the Authentication server
3. Change the Business server
4. Change the Java application (*1)

*1 This should be performed for Interstage Single Sign-on JAAS Java applications.

The following tasks are performed by the SSO administrator.

1. Changing the Repository server (update system)

1. Change the repository server (update system)
    - Change the single repository server (update system) using the same procedure as described in 'Changing the Repository server' in a system that does not use repository server load balancing.
    - To export the repository server resources to the resource storage file, execute the *ssobackup* command in the -sv option on the repository server (update system) machine on which the settings were changed so that session management can be used.
    - For details about the *ssobackup* command, refer to the "Backup Commands" chapter of the Reference Manual (Command Edition).
2. Change the repository servers (update system) that are used for load balancing

    Perform the procedure for all the remaining repository servers (update system) that are used for load balancing.

    - Forward the resource storage file that was exported in 'Change the repository server (update system)' to the repository servers (update system) that are used for load balancing.
    - Execute the *ssorestore* command to import the repository server resources.
    - For details about the *ssorestore* command, refer to the "Backup Commands" chapter of the Reference Manual (Command Edition).
    - In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab.
    - Click [Session management detailed settings [Show]], and check whether "Yes" is selected for [Use Session management?] in [Session management Setting]. If "Yes" is not selected, the command in Step 2 was executed after an incorrect resource storage file was specified. In this case, re-execute the procedure from Step 1.

When the above tasks are complete, start all the repository servers (update system) and delete the resource storage file that was exported.

2. Changing the Authentication server

Change the authentication server using the same procedure as for the 'Changing the Authentication server' in a system that does not use repository server load balancing.

The following tasks are performed by the Business server administrator.

3. Changing the Business server

Change the business server using the same procedure as for the 'Changing the Business server' in a system that does not use repository server load balancing.

4. Changing the Java application

Change the Java application using the same procedure as for the 'Changing the Java application' in a system that does not use repository server load balancing.

A system in which the repository server and the authentication server are set up on one machine, and more than one server is used to perform load balancing

Perform the following steps:

In this kind of system, first of all change the repository server and the authentication server that have been set up on one machine and then change all the remaining repository servers and authentication servers that are used for load balancing.

1. Change the Repository server
2. Change the Authentication server
3. Change the repository server and the authentication server that are used for load balancing
4. Change the Business server
5. Change the Java application (*1)

*1 This should be performed for Interstage Single Sign-on JAAS Java applications.

The following tasks are performed by the SSO administrator.

1. Changing the Repository server

Change the single repository server using the same procedure described in 'Changing the Repository server' in a system that does not use repository server load balancing.

2. Changing the Authentication server

1. Change the single authentication server using the same procedure described in'Changing the Authentication server' in a system that does not use repository server load balancing.

2. To export the repository server and authentication server resources to the resource storage file, execute the *ssobackup* command in the -sv and -ac options on the authentication server machine on which the settings were changed so that session management can be used.

For details about the *ssobackup* command, refer to the "Backup Commands" chapter of the Reference Manual (Command Edition).

3. Change the repository server and the authentication server that are used for load balancing

Change all the remaining repository servers and authentication servers that are used for load balancing according to the following procedure:

1. Forward the resource storage file that was exported in 'Changing the Authentication server' to the repository server and authentication server that are used for load balancing.

2. Execute the *ssorestore* command to import the repository server and authentication server resources.

   For details about the *ssorestore* command, refer to the "Backup Commands" chapter of the Reference Manual (Command Edition).

3. In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab.

4. Click [Session management detailed settings [Show]], and check whether "Yes" is selected for [Use Session management?] in [Session management Setting]. If "Yes" is not selected, the command in Step 2 was executed after an incorrect resource storage file was specified. In this case, re-execute the procedure from Step 1.

5. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab.

6. Click [Detailed Settings[Show]], and check whether "Yes" is selected for [Use Session management?] in [Authentication infrastructure Information]. If "Yes" is not selected, the command in Step 2 was executed after an incorrect resource storage file was specified. In this case, re-execute the procedure from Step 1.

When the above tasks are complete, start all the repository servers and authentication servers and delete the resource storage file that was exported.

The following tasks are performed by the Business server administrator.

4. Changing the Business server

Change the business server using the same procedure described in 'Changing the Business server' in a system that does not use repository server load balancing.

5. Changing the Java application

Change the Java application using the same procedure described in 'Changing the Java application' in a system that does not use repository server load balancing.

A system in which load balancing is used in the repository server (update system) and the repository server (reference system)

Perform the following steps:

1. Change the Repository server (update system)
2. Change the Repository server (reference system)
3. Change the Authentication server
4. Change the Business server
5. Change the Java application (*1)

*1 This should be performed for Interstage Single Sign-on JAAS Java applications.

The following tasks are performed by the SSO administrator.

1. Changing the Repository server (update system)

The procedure for changing the Repository server (if this is running on more than one machine, this is the Repository server (update system)) using the Interstage Management Console is described below:

1. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Session management detailed settings [Show]].

2. Check that "Yes" is set for [Use Session management?] in [Session management Setting], and then click [Update]. (*1) (*2)

3. Restart the Repository server (update system).

4. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication infrastructure setup file].

5. Click [Detailed Settings [Show]], and check that "Yes" is set for [Use Session management?] in [Authentication Infrastructure Information Settings].

6. Set [Password], and click [Download] to download the Authentication infrastructure setup file to the machine used to start the Web browser.

7. To run the Authentication server or Repository server on more than one machine, forward the Authentication infrastructure setup file to the Authentication server or Repository server (reference system), and then delete the Authentication infrastructure setup file.

8. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Business system setup file].
9. Click [Detailed Settings [Show]], and check that "Yes" is set for [Use Session management] in [Authentication Infrastructure Information Settings]. (*3)
10. In Steps 11 and 12, perform the procedure for all Business systems.
11. Set the required options, and click [Download] to download the Business system setup file to the machine used to start the Web browser.
12. Send the Business system setup file to the Business server administrator, and then delete it.

*1 For details about using SSL communication in the Repository server (update system), refer to "Procedure for changing a Repository Server to use SSL Communication" in the "Preparations for SSL Communication" chapter and configure the environment settings.

*2 To run the repository server on a cluster system, change the encryption information (service ID) file on the shared disk and change the environment configuration file. Change the standby node environment settings at the same time. For details, refer to the High Availability System Guide "Using Interstage Single Sign-on", "1) Setup in the operation node (node 1)" section, Steps 3 and 4.

Register the Interstage Single Sign-on status transition procedure. For details about the status transition procedure, refer to "Setting Cluster Service" in the "Environment Setup Procedure for Cluster Service" chapter of the High Availability System Guide.

*3 To link with Application Gateway and use non-SSL for communication between Application Gateway and the Authentication server, the Authentication server URL referenced by the Business server must be changed before the Business server is restarted. Specify the Authentication server URL in [Authentication server URL] of [Authentication Infrastructure Information Settings]. For details about Authentication server URLs referenced by Business systems, refer to "URL Used by the Business System to Reference the Authentication Server" in the "Overview" chapter.

2. Changing the Repository server (reference system)

The procedure for changing the repository server (reference system) if the repository server is running on more than one machine is described below: If you are running more than one repository server (reference system), perform the procedure for all repository servers (reference system).

1. Forward to the repository server (reference system) the Authentication infrastructure setup file downloaded from the repository server (update system) for which the settings were changed to use session management.
2. Specify the Authentication infrastructure setup file forwarded in Step 1, and execute the *ssoimpsv* command. For details about the *ssoimpsv* command, refer to the "Single Sign-on Operation Commands" chapter of the Reference Manual (Command Edition).
3. In the Interstage Management Console click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server (reference system)] > [Settings].
4. Click [Detailed Settings [Show]], and check that "Yes" is set for [Use Session management?] in [Authentication Infrastructure Information Settings]. If "Yes" is not set, specify the invalid Authentication infrastructure setup file in Step 2 and execute the command. Repeat Step 1.(*1)
5. Restart the repository server (reference system).
6. Delete the Authentication infrastructure setup file.

*1 For details about using SSL communication in the repository server (reference system), refer to "Procedure for changing a Repository Server to use SSL Communication" in the "Preparations for SSL Communication" chapter and configure the environment settings.

3. Changing the Authentication server

Change the authentication server using the same procedure as described in 'Changing the Authentication server' in a system that does not use repository server load balancing.

The following tasks are performed by the Business server administrator.

4. Changing the Business server

Change the business server using the same procedure as described in 'Changing the Business server' in a system that does not use repository server load balancing.

5. Changing the Java application

Change the Java application using the same procedure as described in 'Changing the Java application' in a system that does not use repository server load balancing.

A.6 Upgrading to a System that Performs Repository Server (update system) Load Balancing

To upgrade from a system that does not use repository server (update system) load balancing to a system that does, note the points shown in the table below and change the environment.

Upgrading an environment that does not use session management

Setting up the authentication server and the repository server on more than one machine

Change the server environment as shown in the table below.

Server	Changes
Repository server (update system)	- If you are using a previous version of the server, upgrade to this version. - Change the existing SSO repository to an SSO repository that uses the Directory Service database sharing function. For details about the database sharing function, refer to the Directory Service Operator's Guide.
Repository server (reference system)	- Delete this server.
Authentication server	- If a load balancer is placed between the authentication server and the repository server, and the load balancer URL is different to the repository server (update system) before the upgrade, set up the authentication server again.
Business server	- No changes are required for this server.

Setting up the authentication server and the repository server on one machine

Change the server environment as shown in the table below.

Server	Changes
Repository server	- If you are using a previous version of the server, upgrade to this version. - Change the existing SSO repository to an SSO repository that uses the Directory Service database sharing function. For details about the database sharing function, refer to the Directory Service Operator's Guide.
Authentication server	- If a load balancer is placed between the authentication server and the repository server, and the load balancer URL is different to the repository server (update system) before the upgrade, set up the authentication server again.
Business server	- No changes are required for this server.

Upgrading an environment that uses session management

Setting up the authentication server and the repository server on more than one machine

Change the server environment as shown in the table below.

Server	Changes
Repository server (update system)	If you are using a previous version of the server, upgrade to this version. Change the existing SSO repository to an SSO repository that uses the Directory Service database sharing function. For details about the database sharing function, refer to the Directory Service Operator's Guide.
- Repository server (reference system)	- Delete this server.
- Authentication server	- If you are using a previous version of the server, upgrade to this version.
- Business server	- If you are using a previous version of the server, upgrade to this version.

Setting up the authentication server and the repository server on one machine

Change the server environment as shown in the table below.

Server	Changes
Repository server	- If you are using a previous version of the server, upgrade to this version. - Refer to "Load Distribution of the Repository Server and the Authentication Server that are Built on the Same Machine" in the "Settings of the Load Balancer" appendix and check if [Repository server (Update system) URL] is correctly set in the Interstage management console. - Change the existing SSO repository to an SSO repository that uses the Directory Service database sharing function. For details about the database sharing function, refer to the Directory Service Operator's Guide.
Authentication server	- If you are using a previous version of the server, upgrade to this version. - Refer to "Load Distribution of the Repository Server and the Authentication Server that are Built on the Same Machine" in the "Settings of the Load Balancer" appendix and check if [Repository server (Update system) URL] is correctly set in the Interstage management console.
Business server	- If you are using a previous version of the server, upgrade to this version.

The actions mentioned above should also be done if repository server load balancing is carried out when the repository server and the authentication server are set up separately on one machine.

A.7 Switching to a System which Uses Active Directory

When switching from a system that uses Interstage directory services as the directory service for registering the user information, to a system that uses Active Directory, the following must be noted and the environment changed.

Refer to "Linking to Active Directory" in the Overview chapter for more information on systems that use Active Directory as the directory service used for registering user information.

Note

- Changes made to environment settings for changing to Active Directory as the directory service for registering user information must be made for all repository servers as well as authentication servers built with the Interstage Single Sign-on system.

- Before changing environment settings, backup all Interstage Single Sign-on resource files of all repository and authentication servers. Refer to the "Maintenance (Resource Backup)" chapter of the Operator's Guide for more information on backing up.

Procedure for switching

The following system configuration options are explained:

- A system in which a repository server is set up on one server
- A system in which a repository server (update system) is set up on more than one server to perform load balancing

A system in which a repository server is set up on one server

Perform the following steps:

1. Set up a Single Sign-on extended schema

   This is performed for use of the Single Sign-on extended schema.

2. Set user information in Active Directory
3. Set up the SSO repository
4. Set up the SSL communication environment

   Configure the settings to communicate with Active Directory using SSL.

5. Change the repository server
6. Change the authentication server
7. Set up Integrated Windows authentication

1. Set up a Single Sign-on extended schema

The Single Sign-on schema is extended in ActiveDirectory.

Refer to "Set up an Extended schema for Single Sign-on" in the "Settings for Active Directory Linkage" appendix for details on extending the Single Sign-on schema in Active Directory.

2. Set user information in Active Directory

The user information is set in Active Directory.

Refer to "Setting up User Information for Active Directory" in the "Settings for Active Directory Linkage" appendix for information regarding the settings of user information in Active Directory.

3. Set up the SSO repository

Register the role configuration in the SSO repository

- Without using the Single Sign-on extended schema

  Associate any attribute value of the user information managed in Active Directory, with the role configuration in Interstage Single Sign-on, and then register the role configuration in the SSO repository.

  Refer to "Setting up the SSO Repository (Associating Role Configurations)" in the "Settings for Active Directory Linkage" appendix for information about this procedure.

- Using the Single Sign-on extended schema

  When a role configuration other than the role configuration already registered in the SSO repository is required, or when a role configuration needs to be changed, add or change the role configuration according to what is required.

  Refer to "Amending Role Configurations" in the "Operation and Maintenance" chapter for more information.

4. Set up the SSL communication environment

Configure the settings to communicate with Active Directory using SSL.

Refer to "Creating an Environment for SSL Communication" in the "Settings for Active Directory Linkage" appendix for information on this procedure.

5. Change the repository server

   Use the Interstage Management Console of the repository server, take the following steps:

   1. Select [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and click [Repository server detailed settings [Show]].
   2. Change [Directory service for the user information registration entry] in [Repository Settings] to [Active Directory], and check [Use a Single Sign-on extended schema] according to the application.
   3. Set the connection information for Active Directory in [Active Directory Settings], change [User Information Registration Entry] to the user information registration entry in Active Directory, and then click the [Update] button.
   4. Restart the Repository server.
   5. Select [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Authentication infrastructure setup file] tab
   6. Click [Detailed Settings [Show]] and check that [User Information Registration Entry] in [Repository Settings] has been changed to the user information registration in Active Directory.
   7. Set [Password], click the [Download] button, to download the authentication infrastructure setup file from the repository server to the machine on which the Web browser is operating.
   8. After transferring the authentication infrastructure setup file to the authentication server, delete the downloaded authentication infrastructure setup file from the machine on which the Web browser is operating.

6. Change the authentication server

   Change the authentication server as follows:

   If the load of the authentication server is distributed, perform this procedure on all authentication servers. Refer to "Load Distribution of the Authentication Server" in the "Settings of the Load Balancer" appendix for information about setting the load balance.

   1. Confirm that the authentication infrastructure setup file has been transferred to the authentication server. The file is downloaded from the repository server in which the Directory Service has been changed to Active Directory.
   2. Execute the ssoimpac command specifying the file downloaded and confirmed in Step 1 above.
   3. In the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab.
   4. Click [Detailed settings [Show]], confirm that [Attribute used for authentication] in [Integrated Windows Authentication Setting] is [Not used], and then click the [Update] button. If [Not used] has not been set an incorrect authentication infrastructure setup file will be executed with the command in Step 2. In this case, re-execute the procedure again from Step 1.
   5. Restart the authentication server
   6. Delete the authentication infrastructure setup file

7. Set up integrated Windows authentication

   Configure the settings for Integrated Windows Authentication.

   Refer to "Configure Integrated Windows Authentication" in the "Settings for Active Directory Linkage" appendix for information on this procedure.

   There would be no need to perform this procedure if it is already set up.

A system in which a repository server (update system) is set up on more than one server to perform load balancing

Perform the following steps:

Change one repository server first, and then change the remaining servers to be included in the load distribution.

1. Set up a Single Sign-on extended schema

   This is performed for use of the Single Sign-on extended schema.

2. Set user information in Active Directory
3. Set up the SSO repository

4. Set up the SSL communication environment

   Configure the settings to communicate with Active Directory using SSL.

5. Change the repository server (update system)

   1. Change a repository server (update system)

   2. Change any remaining repository servers (update system) included in the load distribution.

6. Change the authentication server

7. Set up Integrated Windows authentication

1. Set up a Single Sign-on extended schema

Use the corresponding procedure, as outlined in "A system in which a repository server is set up on one server" above.

2. Set user information in Active Directory

Use the corresponding procedure, as outlined in "A system in which a repository server is set up on one server" above.

3. Set up the SSO repository

Use the corresponding procedure, as outlined in "A system in which a repository server is set up on one server" above.

4. Set up the SSL communication environment

Use the corresponding procedure, as outlined in "A system in which a repository server is set up on one server" above.

5. Change the repository servers (update system)

Change a repository server (update system)

1. Use the same procedures as outlined in "A system in which a repository server is set up on one server" above.

2. The repository server on which the Directory service has been changed to Active Directory, will be used as the export machine. Execute the *ssobackup* command with the -sv option on this machine, to export the repository server resources to the resource storage file.

   Refer to the "Backup Commands" chapter in the Reference Manual (Command Edition) for more information about this command.

Change the remaining repository servers (update system) included in load distribution

Perform this on all remaining repository servers (update system) in which the load is distributed.

1. Use each subsequent repository server as an import machine and transfer the resource storage file that was created above.

2. Execute the *ssorestore* command to the import the repository server resource.

   Refer to the "Backup Commands" chapter in the Reference Manual (Command Edition) for more information about this command.

3. In the Interstage Management Console, select [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab.

4. Click [Repository server detailed settings [Show]], and check that [Active Directory Settings] is displayed in [Repository Settings], and then press the [Update] button. If [Active Directory Settings] is not displayed, an incorrect resource storage file may have been set in Step 2b above, in which case you must do all of Step 2 again.

Upon completing the above procedure on all repository servers, restart them all and then delete all the exported resource storage files.

6. Change the authentication server

Use the corresponding procedure as outlined in "A system in which a repository server is set up on one server" above.

7. Set up Integrated Windows authentication

Use the corresponding procedure as outlined in "A system in which a repository server is set up on one server" above.

A.8 Notes on Upgrading from Previous Versions

The Interstage backup and restore functions are used to upgrade Interstage from a previous version.

For details, refer to the "Maintenance (Resource Backup)" chapter of the Operator's Guide.

Note

In this version, a maximum of 256 Business servers can be created on the same server machine. If 257 or more servers are defined, check that the server configuration is for a maximum of 256 Business servers before upgrading.

Appendix B Samples of User Program Descriptions

This appendix provides examples of user programs developed with Java that are used to operate the SSO repository.

When other user programs to operate the SSO repository are required, create the required user programs based on the description examples below.

All the above processing requires common preprocessing and postprocessing. Each user processing must be inserted between the pre-processing and post processing programs.

The common processing programs are explained below.

Pre-processing (opening the connection with the repository)

Example

Connect the sample program below to the host named "ssohost" using port number "389" in the security level "simple."

Specify the administrator DN and password as Java strings in the "bindDn" and "password" parameters, respectively.

```
java.util.Hashtable env = new java.util.Hashtable();
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldap://ssohost:389");
env.put(Context.SECURITY_AUTHENTICATION, "simple");
env.put(Context.SECURITY_PRINCIPAL, bindDn);
env.put(Context.SECURITY_CREDENTIALS, password);

DirContext ctx = new InitialDirContext(env);
```

Note

Carefully handle the administrator DN and password to protect the password from attack.

For measures that can be taken against password attack, refer to "Security Measures" under "Interstage Single Sign-on" of "Security Risks" of "Security Risks and Measures" in the Security System Guide.

Postprocessing (closing the connection with the repository)

Example

Close the connection between the sample program and the repository made by the pre-processing.

Use the result obtained by the common pre-processing as the value of "ctx".

```
ctx.close();
```

A user program to operate the SSO repository must be based on a correct design of the SSO repository and created very carefully to prevent invalid SSO repository data from being created.

For details about the design of the SSO repository, see "Designing a SSO Repository".

Remarks

- Knowledge of LDAP and the Java programming language are necessary prerequisites. If you are using the Java API, refer to Java API specifications and other JAVA resources.

  For details about the environment properties required for the pre-processing and other details on application programming using the Java language, refer to "Creating an Application (JNDI)" in the Interstage Directory Service Operator's Guide. The sample programs shown here exclude the package notation of classes to be used and the handling of exceptions. The actual user programs must include the following import declarations and exception processing:

  - Add the import declarations below.

    import javax.naming.*;

    import javax.naming.directory.*;

  - Add the exception processing below.

    javax.naming.NamingException

- Arrange the user program in the location that satisfies the operation, while fully considering security. In addition, add any error-handling descriptions when it is needed.

B.1 Registering a Role Configuration in the SSO Repository

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory at creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of role information is "ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com".
- The relevant role name is specified for "roleName" in java.lang.String.
- The result of common preprocessing is used as the value of "ctx".

Description of User Program

Example

Close the connection between the sample program and the repository made by the pre-processing.

Use the result obtained by the common pre-processing as the value of "ctx".

```
          Pre-processing
              :

Attributes attrs = new BasicAttributes();

Attribute objectClass = new BasicAttribute("objectClass");
objectClass.add("top");
objectClass.add("ssoRole");
attrs.put(objectClass);
attrs.put("cn", roleName);

String dn = "cn=" + roleName + ",ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com";

ctx.createSubcontext(dn, attrs);

              :
           Postprocessing
```

B.2 Registering User Information in the SSO Repository

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory at creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".

- RDN of user information is expressed by "cn".
- The result of common preprocessing is used as the value of "ctx".
- User information is read from the CSV file named "sample.csv" to be processed.

Note

Since the CSV file includes passwords, the file must be handled carefully to protect the password from attack.

For details about the measures that can be taken against password attack, refer to "Security Measures" under "Interstage Single Sign-on" of "Security Risks" of "Security Risks and Measures" of the Security System Guide.

Description of CSV File

Example

The CSV format uses the comma (,) as the delimiter. In this sample file, user attributes are described in the following order:

1. cn 2. sn 3. uid 4. userPassword
5. employeeNumber 6. mail 7. ssoAuthType 8. ssoCredentialTTL
9. ssoNotBefore (*1) 10. ssoNotAfter 11. ssoUserStatus 12. ssoRoleName

The numbers shown at the top of the sample file below indicate the correspondence between user information and the above attributes. Do not describe the numbers in the actual CSV file.

*1 In the following example, the date is specified in the format YYYYMMDDHHMMSS+XXXX. "+XXXX" refers to the time difference from UTC (Universal Time Coordinate). In cases where "-XXXX" is used, it means the same as above.

```
1         2        3        4      5             6              7
8           9         10  11   12
user001, user001, user001, user001,100001,
 user001@interstage.fujitsu.com,basicAuthOrCertAuth,60,20010101090000+0900,,
good,Admin
user002, user002, user002, user002,100002,
user002@interstage.fujitsu.com,basicAuthOrCertAuth,60,20010101090000+0900,,
good,Admin
user003, user003, user003, user003,100003,
user003@interstage.fujitsu.com,basicAuthOrCertAuth,60,20010101090000+0900,,
good,Leader
                                        :
```

Description of User Program

Example

```
// Associating the values in CSV file with attributes
private static final int INDEX_CN = 0;
private static final int INDEX_SN = 1;
private static final int INDEX_UID = 2;
private static final int INDEX_USERPASSWORD = 3;
private static final int INDEX_EMPLOYEENUMBER = 4;
private static final int INDEX_MAIL = 5;
private static final int INDEX_SSOAUTHTYPE = 6;
private static final int INDEX_SSOCREDENTIALTTL = 7;
private static final int INDEX_SSONOTBEFORE = 8;
private static final int INDEX_SSONOTAFTER = 9;
private static final int INDEX_USERSTATUS = 10;
private static final int INDEX_SSOROLENAME = 11;
private static final int INDEX_RDN = 0;
private static final String [] attributeNames = {
    "cn",
    "sn",
    "uid",
    "userPassword",
    "employeeNumber",
    "mail",
    "ssoAuthType",
    "ssoCredentialTTL",
    "ssoNotBefore",
    "ssoNotAfter",
    "ssoUserStatus",
    "ssoRoleName"
};

              :
          Pre-processing
              :

// Opening the CSV file (current simple.csv)
java.io.FileInputStream fis = new java.io.FileInputStream("sample.csv");
java.io.InputStreamReader isr = new java.io.InputStreamReader(fis);
java.io.BufferedReader br = new java.io.BufferedReader(isr);

// Processing the CSV file by reading it line by line
String line;
String [] data;
while((line = br.readLine()) != null) {
        java.util.StringTokenizer st = new java.util.StringTokenizer(line, ",", true);
        int index = 0;
        java.util.ArrayList al = new java.util.ArrayList(64);

        al.add(0, null);
        String s;
        while(st.hasMoreTokens()) {
               s = st.nextToken();
               if(s.equals(",")) {
                       index++;
                       al.add(index, null);
               } else {
                       al.set(index, s);
               }
        }

        data = (String[])al.toArray(new String[0]);

        if( data == null || data.length == 0 ) {
               continue;
        }

        Attributes attrs = new BasicAttributes();

        Attribute objectClass = new BasicAttribute("objectClass");
        objectClass.add("top");
        objectClass.add("person");
        objectClass.add("organizationalPerson");
        objectClass.add("inetOrgPerson");
        objectClass.add("ssoUser");
        attrs.put(objectClass);

        // Setting the values before ssoRoleName
        for(int i = 0; i < INDEX_SSOROLENAME; i++ ) {
               if( data[ i ] != null ) {
                       attrs.put( attributeNames[ i ], data[ i ] );
               }
        }

        // Setting the value of ssoRoleName
        Attribute ssoRoleName = new BasicAttribute( "ssoRoleName" );
        for(int i = INDEX_SSOROLENAME; i < data.length; i++ ) {
               if( data[ i ] != null ) {
```

```
                        ssoRoleName.add( data[ i ] );
                }
        }
        if( ssoRoleName.size() > 0 ) {
                attrs.put( ssoRoleName );
        }

        String dn = "cn=" + data[INDEX_RDN] + ",ou=User,ou=interstage,o=fujitsu,dc=com";

        ctx.createSubcontext( dn, attrs );
}

              :
          Postprocessing
```

B.3 Deleting User Information from the SSO Repository

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory for creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- The user name to be deleted is specified for "user" in java.lang.String.
- The result of common preprocessing is used as the value of "ctx".

Description of User Program

Example

```
          Pre-processing
              :

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";
ctx.destroySubcontext(dn);

              :
          Postprocessing
```

B.4 Adding a User Role

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory for creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- The name of the user whose role is to be added is specified for "user" in java.lang.String.
- The role to be added is specified for "role" in java.lang.String.
- The result of common pre-processing is used as the value of "ctx".

Description of User Program

Example

```
          Pre-processing
              :

String [] retAttributes = new String[1];
```

```
retAttributes[0] = "ssoRoleName";

SearchControls sc = new SearchControls();
sc.setSearchScope(SearchControls.OBJECT_SCOPE);
sc.setReturningAttributes(retAttributes);
sc.setCountLimit(1);
sc.setTimeLimit(5*1000); // 5 seconds

String filter = "(cn=" + user + ")";

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";

NamingEnumeration ne = ctx.search(dn, filter, sc);

Attribute roleAttr = null;
while(ne.hasMore()) {
          SearchResult sr = (SearchResult)ne.next();
          Attributes attrs = sr.getAttributes();
          if(attrs != null) {
                    roleAttr = attrs.get("ssoRoleName");
                    if(roleAttr != null) {
                              break;
                    }
          }
}
if(roleAttr == null) {
          roleAttr = new BasicAttribute("ssoRoleName", role);
} else {
          // No processing if the role already exists
          for(int i = 0; i < roleAttr.size(); i++) {
                    if(role.compareToIgnoreCase((String)roleAttr.get(i)) == 0) {
                              ctx.close();
                              return;
                    }
          }
          roleAttr.add(role);
}
ModificationItem[] mods = new ModificationItem[1];
mods[0] = new ModificationItem(DirContext.REPLACE_ATTRIBUTE, roleAttr);
ctx.modifyAttributes(dn, mods);

              :
          Postprocessing
```

B.5 Deleting a User Role

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory for creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- The name of the user whose role is to be deleted is specified for "user" in java.lang.String.
- The role to be deleted is specified for "role" in java.lang.String.
- The result of common preprocessing is used as "ctx".

Description of User Program

Example

```
          Pre-processing
              :

String [] retAttributes = new String[1];
retAttributes[0] = "ssoRoleName";

SearchControls  sc = new SearchControls();
sc.setSearchScope(SearchControls.OBJECT_SCOPE);
sc.setReturningAttributes(retAttributes);
sc.setCountLimit(1);
sc.setTimeLimit(5*1000); // 5 seconds

String filter = "(cn=" + user + ")";

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";

NamingEnumeration ne = ctx.search(dn, filter, sc);

Attribute roleAttr = null;
while(ne.hasMore()) {
          SearchResult sr = (SearchResult)ne.next();
          Attributes attrs = sr.getAttributes();
          if(attrs != null) {
                    roleAttr = attrs.get("ssoRoleName");
                    if(roleAttr != null) {
                              break;
                    }
          }
}

if(roleAttr != null) {
          if(roleAttr.remove(role)) {
                    ModificationItem[] mods = new ModificationItem[1];
                    mods[0] = new ModificationItem( DirContext.REPLACE_ATTRIBUTE, roleAttr );

                    ctx.modifyAttributes(dn, mods);
          }
}

              :
          Postprocessing
```

B.6 Displaying the User Lock Status

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory at creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- The name of the user whose lock status is to be displayed is specified for "user" in java.lang.String.
- The result of common preprocessing is used as the value of "ctx".

Description of User Program

Example

```
          Pre-processing
              :

String [] retAttributes = new String [1];
```

```
retAttributes[0] = "ssoUserStatus";

SearchControls  sc = new SearchControls();
sc.setSearchScope(SearchControls.OBJECT_SCOPE);
sc.setReturningAttributes(retAttributes);
sc.setCountLimit(1);
sc.setTimeLimit(5 * 1000); // 5 seconds

String filter = "(cn=" + user + ")";

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";

NamingEnumeration ne = ctx.search(dn, filter, sc);

while(ne.hasMore()) {
        SearchResult sr = (SearchResult)ne.next();
        Attributes attrs = sr.getAttributes();
        if(attrs != null) {
               Attribute a = attrs.get("ssoUserStatus");
               if(a == null) {
                       System.out.println("Not locked");
                       return;
               } else {
                       String value = (String)a.get();
                       if(value.compareToIgnoreCase("locked") == 0) {
                               System.out.println("Locked");
                               return;
                       } else {
                               System.out.println("Not locked");
                               return;
                       }
               }
        }
}

              :
          Postprocessing
```

B.7 Locking a User

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory for creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- Specify the name of the user to be locked in "user" in java.lang.String.
- Specify the locked time (the current time) in "time" in java.lang.String.
- The result of common pre-processing is used as the value of "ctx".

Description of User Program

Example

```
          Pre-processing
              :

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";

ModificationItem[] mods = new ModificationItem[1];
mods[0] = new ModificationItem(DirContext.REPLACE_ATTRIBUTE,
                               new BasicAttribute("ssoUserStatus", "locked"));
mods[1] = new ModificationItem(DirContext.REPLACE_ATTRIBUTE,
                               new BasicAttribute("ssoLockTimeStamp", time));

ctx. modifyAttributes(dn, mods);

              :
          Postprocessing
```

B.8 Displaying the User Validity Period

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory for creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- The name of the user whose validity period is to be displayed is specified for "user" in java.lang.String.
- The result of common pre-processing is used as the value of "ctx".

Description of User Program

Example

```
          Pre-processing
              :

String [] ret = new String[2];
String [] retAttributes = { "ssoNotBefore", "ssoNotAfter" };

SearchControls  sc = new SearchControls();
sc.setSearchScope(SearchControls.OBJECT_SCOPE);
sc.setReturningAttributes(retAttributes);
sc.setCountLimit(1);
sc.setTimeLimit(5 * 1000); // 5 seconds

String filter = "(cn=" + user + ")";

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";

NamingEnumeration ne = ctx.search(dn, filter, sc);

ret[0] = ret[1] = null;
while(ne.hasMore()) {
          SearchResult sr = (SearchResult)ne.next();
          Attributes attrs = sr.getAttributes();
          if(attrs != null) {
                    Attribute ba = attrs.get("ssoNotBefore");
                    if(ba != null) {
                              ret[0] = (String)ba.get();
                    }

                    Attribute aa = attrs.get("ssoNotAfter");
                    if(aa != null) {
                              ret[1] = (String)aa.get();
                    }
                    break;
          }
}
if(ret[0] != null) {
          System.out.println("Validity period start time = " + ret[0]);
} else {
          System.out.println("Validity period start time not specified");
}
if(ret[1] != null) {
          System.out.println("Validity period end time = " + ret[1]);
} else {
          System.out.println("Validity period end time not specified");
}

              :
          Postprocessing
```

B.9 Changing the User Validity Period

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory for creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- The name of the user whose validity period is to be changed is specified for "user" in java.lang.String.
- The validity period start time is specified for "before" in java.lang.String.
- The validity period end time is specified for "after" in java.lang.String.
- The result of common pre-processing is used as the value of "ctx".

Description of User Program

Example

```
          Pre-processing
              :

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";

ModificationItem[] mods = new ModificationItem[2];
mods[0] = new ModificationItem(DirContext.REPLACE_ATTRIBUTE,
                                      new BasicAttribute("ssoNotBefore",
before));
mods[1] = new ModificationItem(DirContext.REPLACE_ATTRIBUTE,
                                      new BasicAttribute("ssoNotAfter",
after));

ctx.modifyAttributes(dn, mods);

              :
          Postprocessing
```

B.10 Changing the User Password

This sample program assumes the environment setup below. Change the setup according to the actual environment used.

- The public directory for creation of the repository is "ou=interstage,o=fujitsu,dc=com".
- The storage location of user information is "ou=User,ou=interstage,o=fujitsu,dc=com".
- RDN of user information is expressed by "cn".
- The new user password is specified for "newPassword" in java.lang.String.
- The name of the user whose password is to be changed is specified for "user" in java.lang.String.

- The result of common preprocessing is used as the value of "ctx".

Note

When a password is changed to new one, the new password must be handled carefully to protect the password from attack.

For details about measures that can be used against password attack, refer to "Security Measures" under "Interstage Single Sign-on" of "Security Risks" of "Security Risks and Measures" of the Security System Guide.

Description of User Program

Example

```
          Pre-processing
              :

ModificationItem[] mods = new ModificationItem[1];
mods[ 0 ] = new ModificationItem(DirContext.REPLACE_ATTRIBUTE,
                    new BasicAttribute("userPassword", newPassword));

String dn = "cn=" + user + ",ou=User,ou=interstage,o=fujitsu,dc=com";

ctx.modifyAttributes(dn, mods);

              :
          Postprocessing
```

Appendix C Entry Attributes to be Registered in SSO Repository

This appendix describes the user information, role configurations and protection resources required by Interstage Single Sign-on for authentication and authorization, and that must be registered in the SSO repository.

- User Information

  This section describes the user information managed by Interstage Single Sign-on such as user ID, password, and authentication method.

- Role Configuration

  This section describes the role information required by Interstage Single Sign-on for authorization.

- Protection Resources

  This section describes the target domain information required by Interstage Single Sign-on for access control.

C.1 User Information

This section describes the user information managed by Interstage Single Sign-on such as user ID, password, and authentication method.

The user information definition consists of general definitions that target a person, and special definitions that target network devices such as printers.

General Definitions

Table C.1 User Information Object Class and Description for General Definitions

User information Object class	Description
top	Basic LDAP object class
person	User information
inetOrgPerson	
organizationalPerson	
ssoUser	SSO user information

Table C.2 User Information for General Definitions

Attribute name	Explanation	Description	Example of registration
cn	Name	Specifies the user's full name. (*1)(*2)	user001
sn	Second name	Specifies the user's second name.	Fujitsu
uid	User ID	Specifies the user ID that identifies the user and is used for password authentication. (*1) (*2) (*3)	user001
userPassword	Password	Specifies the password to be used for password authentication. (*4)	user001
Other information required for authentication (Attributes that must be specified depending on operation.)			
employeeNumber	Employee number	Specifies the number, such as employee number, assigned to the user. (*1) (*2)	000001
mail	E-mail address	Specifies the e-mail address. (*1) (*2)	user001@interstage.fujitsu.com
dnQualifier	DN qualifier	Specifies the DN qualifier of the user. (*1) (*2)	000001

Special Definitions

Table C.3 User Information Object Class and Description for Special Definitions

User information Object class	Description
Top	Basic LDAP object class
device	Network device information for devices such as printers
uidObject	User ID information
ssoUser	SSO user information

Table C.4 User Information for Special Definitions

Attribute name	Explanation	Description	Example of registration
cn	Name	Specifies the device. (*1) (*2)	Device10000
uid	User ID	Specifies the user ID that identifies the user and is used for password authentication. (*1) (*2) (*3)	1234-1234-AB
serialNumber	Serial number	Specifies the serial number of the user. (*1) (*2)	1234-1234-AB

General Definitions and Special Definitions

Table C.5 User Information for General Definitions and Special Definitions

Attribute name	Explanation	Description	Example of registration
Other information required for authentication (Attributes that must be specified depending on operation.)			
ssoRoleName	Role name	Specifies the name of the role assigned to the user. (*1) (*5)	Admin
ssoAuthType	Authentication method	Specifies the user authentication method from one of the following values: (*1) basicAuth: Password authentication certAuth :Certificate authentication (*6) basicAuthAndCertAuth : Password authentication and certificate authentication basicAuthOrCertAuth : Password authentication or certificate authentication When this attribute is omitted, specification of "basicAuthOrCertAuth" is assumed.	basicAuthOrCertAuth
ssoCredentialTTL	Re-authentication interval	Specifies the interval of time (in unit of minutes) from user authentication to re-authentication. Specify the re-authentication interval as 0 or a value (in minutes) between 30 and 1440. When 0 is specified and session management is used, this setting is treated as "1440" minutes (24 hours).	60

Attribute name	Explanation	Description	Example of registration
		When 0 is specified and session management is not used, the interval is unlimited, and re-authentication is not necessary. When a value less than 30 is specified, specification of 30 minutes is assumed. When a value over 1440 is specified, specification of 1440 minutes (24 hours) is assumed. If this attribute is omitted, its value defaults to the configuration value in [Re-authentication Interval] of [Operation after Authentication] in the environment setup of the authentication server.	
ssoUserStatus	User status	Specifies whether the user is locked. The repository server sets one of the following values: (*7)(*12) good: The user is not locked. locked: The user is locked.	good
ssoNotBefore	Validity period start time	Specifies the date and time from when the user can use Single Sign-on. (*8)(*9) (*11) Specify a date between "20000101000000" and "20371231235959" in ssoNotBefore If the user attempts to use Single Sign-on before the specified time, authentication will fail. Use the format "YYYYMMDDHHMMSS+XXXX". To specify a Greenwich Mean Time, use the format "YYYYMMDDHHMMSSZ".(*14) When this attribute is omitted, the user can use Single Sign-on immediately.	20030101000000+0900
ssoNotAfter	Validity period end time	Specifies the date and time from when the user ends to access Single Sign-on. (*8) (*9) (*11) Specify a date between "20000101000000" and "20371231235959" in ssoNotBefore. If the user attempts to use Single Sign-on after the specified time, the authentication will fail. Use the format "YYYYMMDDHHMMSS+XXXX". To specify a Greenwich Mean Time, use the format "YYYYMMDDHHMMSSZ".(*14)	20030102000000+0900

Attribute name	Explanation	Description	Example of registration
		When this attribute is omitted, the user can use Single Sign-on for an indefinite period.	
ssoFailureCount	Count of failures in authentication with user name/ password	Specifies the number of times the user failed in password authentication due to incorrect password. When the user succeeds in authentication by entering the correct password, the count is reset to 0. The repository server sets this value. (*10)	0
ssoLockTimeStamp	Lockout time	Specifies the date and time the user was locked in the Greenwich Mean Time (YYYYMMDDHHMMSSZ). The repository server sets this value. (*12) (*13)	20020101090000Z
ssoSessionInfo	SSO Session Information	Internal information required for using session management is set from the Repository server. (*10) Character strings of up to 32 bytes are stored (*15)	00:20020101090000Z

*1 Set values are not case sensitive.

*2 Consecutive spaces ( ) must not be set in this attribute.

*3 Alphanumeric characters and symbols except the colon (:) can be used for this attribute. If any other character is used for this attribute, user authentication will fail. Do not set this attribute more than once. If it is set more than once, user authentication fails.

*4 Alphanumeric characters and symbols can be set in this attribute. If any other character is set in this attribute, user authentication fails. Do not set this attribute more than once. If it is set more than once, user authentication may not be executed correctly.

*5 If a deleted or unregistered role or role set name is set in this attribute, the role or role name will be ignored. When a role set name is specified, it is assumed that the user belongs to only the registered roles in the role set. If the user does not belong to a specified role or role set name, they will be prevented from accessing the site protected by Single Sign-on.

*6 When session management is used in a system in which certificate authentication is not permitted,, do not set "certAuth" for this attribute. If "certAuth" is set, user authentication will fail. If "certAuth" is set, the settings must be configured so that certificate authentication is used in systems in which session management is used. For details on the settings to use certificate authentication, refer to "Settings for Performing Certificate Authentication in a System that performs Session Management"

*7 [Release User Lock] of the Interstage Management Console is used to unlock the user account.

*8 Do not set the same date and time in "ssoNotBefore" and "ssoNotAfter" or user authentication will fail. User authentication will also fail if the date and time set in "ssoNotBefore" is later than the date and time set in "ssoNotAfter". If a date and time outside of this range is set, user authentication will fail.

*9 This attribute represents Daylight Savings Time.

*10 Do not change the setting of this attribute

*11 "+XXXX" refers to the time difference from UTC (Universal Time Coordinate). In cases where "-XXXX" is used, it has the same meaning.

*12 The user can be locked by force if this attribute is set from the user program.

*13 Configure the settings for the value in the user program using the format "YYYYMMDDHHMMSSZ" or "YYYYMMDDHHMMSS+XXXX". Set a time from "20000101000000" to "20371231235959", regardless of the value set for Japan Time or Greenwich Mean Time. If a time outside this range is set, the user authentication will fail.

*14 To use Active Directory as the directory service that is used for registering user information and extend the Single Sign-on schema in ActiveDirectory, configure the settings using the format "YYYYMMDDHHMMSS.0+XXXX". If Greenwich Mean Time is used, configure the settings using the format "YYYYMMDDHHMMSS.0Z".

*15 If the environment was transferred from before Interstage Application Server V9.0, calculate using the following formula:

256 + ((512 + (length of local host name (FQDN) of the repository server (update system)) / 3 * 4)

If the repository server (update system) is installed on multiple machines, specify the longest size within each repository server (update system).

C.2 Role Configuration

This section describes the role information required by Interstage Single Sign-on for authorization.

Role

Table C.6 Object class and Description

Object class	Description
top	Basic LDAP object class
ssoRole	SSO role information

Table C.7 Role configuration

Attribute	Explanation	Description	Example of registration
cn	Name	Specifies a role name. (*1) (*2) (*3)	Admin
ssoAuthType	Authentication method	Specifies the authentication method. This attribute is not used in this version. (*4)	-
ssoSessionInfo	Information used in Interstage Single Sign-on	Set the value used as the Active Directory role/role set attribute. (*1)	05:CN=SALES DEPT.I,CN=Users,DC=ad,DC=local

*1 Set values are not case sensitive.

*2 The role name must not include a comma (,).

*3 This attribute must always be unique.

*4 This attribute must not be set or changed.

The role configuration can also be a role set that contains multiple roles. An example of role set configuration is shown below.

Role set

Table C.8 Object class and Description

Object class	Description
top	Basic LDAP object class
ssoRoleSet	SSO role set information

Table C.9 Role set configuration

Attribute	**Explanation**	**Description**	**Example of registration**
cn	Name	Specifies a role set name. (*1) (*2) (*3)	AdminSet
ssoRoleName	Role name	Specifies the names of the roles contained in the role set. Another role set can be specified as a role included in the specified role set. (*1) (*4) (*5) (*6)	Admin

ssoSessionInfo	Information used in Interstage Single Sign-on	Set the value used as the Active Directory role/role set attribute. (*1)	05:CN=SALES DEPT.I,CN=Users,DC=ad,DC=local

*1 Set values are not case sensitive.

*2 The role name must not include a comma (,).

*3 This attribute must always be unique.

*4 Duplicated roles or role sets are invalid.

*5 If a role set that causes a loop of configurations is set, the looped portion of configuration is invalid.

*6 Non-existent roles or role sets must not be specified.

C.3 Protection Resources

This section describes the target domain information required by Interstage Single Sign-on for access control.

Table C.10 Object class and Description

Object class	Description
Top	Basic LDAP object class
domain	Domain information

Table C.11 Protection resources

Attribute	Explanation	Description	Example of registration
dc	Domain component	Specifies a domain component name. (*1) (*2)	com or fujitsu

*1 Set values are not case sensitive.

*2 The domain component name must not include a period (.).

C.3.1 Site Configuration

This section describes the target site information required by Interstage Single Sign-on for access control.

Table C.12 Object class and Description

Object class	Description
top	Basic LDAP object class
domain	Domain
ssoSite	SSO site information

Table C.13 Site configuration

Attribute	Explanation	Description	Example of registration
dc	Domain component	Specifies a site name. (*1) (*2)	www
ssoPortNumber	Port number	Specifies a port number.	443
ssoSessionInfo	Information used in Interstage Single Sign-on	Internal information required for using session management is set from the Interstage Management Console. (*3) Character strings of up to 256 bytes are stored.	04:xxxx

*1 Set values are not case sensitive.

*2 The domain component name must not include a period (.).

*3 Do not set or change this attribute.

C.3.2 Path Configuration

This section describes the target path information required by Interstage Single Sign-on for access control.

Table C.14 Object class and Description

Object class	Description
top	Basic LDAP object class
ssoResource	SSO path information

Table C.15 Path configuration

Attribute	Explanation	Description	Example of registration
cn	Name	Specifies a path. (*1) (*2) (*3)	/admin/
ssoRoleName	Role name	Specifies the name of the role or role set that can use the relevant resource. (*2) (*4) (*5)	AdminSet
ssoUserAttribute	User attribute	Specifies the attribute name to be notified as the extended user information. (*1)(*2)	mail

*1 Alphanumeric characters and symbols can be set in this attribute.

*2 Set values are not case sensitive.

*3 This attribute must always be unique.

*4 Do not set a role name that includes a comma (,) in this attribute.

*5 Multiple role names can be specified. When multiple role names are specified, the user is allowed to access the protection resource when the user's role and any of the specified roles match.

Appendix D Preparations for SSL Communication

D.1 Setting up an SSL Communication Environment for a Repository Server

To use SSL communication on the repository server, the SSL communication environment must be set up on the repository server machine. However, If SSL communication is used on SSL Accelerator, there is no need to set up the SSL communication environment.

Preparations for SSL communication (acquiring the SSL site certificate and registering it in the Interstage certificate environment)

If the SSL environment is already set up on the Repository server machine, there is no need to perform this task. For details, refer to "Preparations for SSL Communication", in the "Environment Setup (SSO Administrators)" chapter.

Setup for SSL communication (creation of SSL configuration for the Repository server)

On the Interstage Management Console, select [Security] and then [SSL] from the [System] menu. From the [Create a new SSL Configuration] tab, perform setup for SSL communication as follows:

- Configuration Name

  Set the name identifying the SSL configuration.

- Site Certificate Nickname

  Set the nickname of the SSL Site certificate used for SSL communication. The SSL site certificate can be accessed in the Interstage Management Console by selecting [Security] and then [Certificates] on the [System] menu. Click [Site Certificate] to access the SSL site certificate.

- Protocol Version

  Select 'SSL 3.0' and 'TLS 1.0'.

- Client certificate

  Select 'No'.

- Encryption Method

  Change the encryption method when necessary.

- Nickname of Certificate of Certificate Authority

  Change the nickname when necessary.

For details of the above items, refer to the Operator's Guide.

D.2 Procedure for changing a Repository Server to use SSL Communication

In systems in which session management is used, the repository server can use SSL communication.

The procedure for changing a repository server to use SSL communication is described below.

Modify the environment settings in each server according to the following procedure:

1. Set up the SSL environment in the Repository server
2. Change the Repository server environment settings
3. Create the Authentication server Interstage certificate environment
4. Change the Authentication server environment settings

Notes

After all of these tasks are completed, access the contents under the protected path for the business server, perform user authentication, and then start the application.

Changing the Repository Server Environment Settings

Using SSL communication on the Repository server (update system)

1. In the Interstage Management Console of the Repository server (update system), click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] > [Session management detailed settings [Show]].
2. Check that "Yes" is set for [Use Session management?] in [Session management setting].

   If "No" is set, SSL communication cannot be used. This must be changed to use session management. For details on how to change the settings to use session management, refer to "Switching to an application to perform session management".
3. If SSL communication is performed on SSL Accelerator, and the repository server (update system) FQDN or port number made public in the authentication server have been changed, [Repository server (update system) URL] in [Authentication Infrastructure Information Settings] must also be changed.
4. If SSL communication is performed on the repository server, configure the SSL settings for the Web server (Interstage HTTP Server) used by the repository server. To configure the settings, click [System] > [Services] > [Web Server] > [Web Server Name] > [Settings] > [Detailed Settings [Show]]. Select the SSL definition for the repository server created in "Setup for SSL communication".
5. Restart the repository server (update system).
6. Click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication infrastructure setup file].
7. Set [Password], and click [Download] to download the authentication infrastructure setup file to the machine used to start the Web browser.
8. Forward the authentication infrastructure setup file to the authentication server, and then delete the authentication infrastructure setup file.

Using SSL communication on the Repository server (reference system)

1. In the repository server (reference system) Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Repository server (reference system)] > [Settings] > [Session management detailed settings [Show]].
2. Check that "Yes" is set for [Use Session management?] in [Session management setting].

   If "No" is set, SSL communication cannot be used. This must be changed to use session management. For details about the procedure for changing the settings to use session management, refer to "Switching to an application to perform session management".
3. If SSL communication is performed on the repository server, configure the SSL settings for the Web server (Interstage HTTP Server) used by the repository server. To configure the settings, click [System] > [Services] > [Web Server] > [Web Server Name] > [Settings] > [Detailed Settings [Show]]. Select the SSL definition for the repository server created in "Setup for SSL communication".
4. Click [Update].
5. Restart the repository server (reference system).

Creating the Interstage Certificate Environment for the Authentication Server

If SSL communication for the Authentication server is used on SSL Accelerator or Application Gateway, the Interstage certificate environment is created using the "scsmakeenv" command. If the Interstage certificate environment has already been created, there is no need to perform this task.

For details about creating the Interstage certificate environment, refer to D.5 Creating the Interstage Certificate Environment

Changing the Authentication Server Environment Settings

1. Perform the following steps to run the repository server (update system) using SSL communication:

    1. Forward to the authentication server the Authentication infrastructure setup file that was downloaded from the repository server (update system) and changed so that SSL communication can be used on it.

    2. Specify the Authentication infrastructure setup file forwarded in step 1, and execute the "ssoimpac" command.(*1) For details about the "ssoimpac" command, refer to "Single Sign-on Operation Commands" in the "Reference Manual (Command Edition)".

    3. In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings].

    4. Click [Detailed Settings [Show]], and check that the scheme for [Repository server (update system) URL] in [Communication Settings with Repository server] is "https". If the repository server (update system) has been set to use SSL communication and the FQDN or port number have been changed, check that these are set.

        If the repository server (update system) URL is not changed correctly, it will mean that the Authentication infrastructure setup file specified in step 2 (before execution of the "ssoimpac" command) is invalid. In this case, repeat step 1.

2. Perform the following steps to run the repository server (reference system) using SSL communication:

    1. In the Interstage Management Console, click [System] > [Security] > [Single Sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings].

    2. Click [Detailed Settings [Show]], and change the scheme for [Repository server (reference system) URL] in [Communication Settings with Repository server (reference system)] to "https".

        Change the settings "Same as the scheme of Repository server (update system)" according to the application.

3. Then restart the authentication server.

4. If the Authentication infrastructure setup file was used, delete it.

*1 Back up the authentication server resources before executing the "ssoimpac" command. For details about backing up the Authentication server, refer to the "Operator's Guide".

D.3 Creating the Interstage Certificate Environment and Certificate Signing Request (CSR) for SSL Certificates

The "scsmakeenv" command is used to create a certificate signing request (CSR) for signing and requesting the certificate for the SSL communication. It also creates the Interstage certificate environment at the same time.

Use the scsmakeenv command to create the certificate signing request (CSR). Send the CSR to a certificate authority to request to issue the certificate.

Executing the scsmakeenv command prompts the operator to enter distinguished names. In response to the message, 'What is your first and last name?' specify the Fully Qualified Domain Name (FQDN) of the server used to apply for the certificate as the Web server host name. If the load of the Web server is distributed using a load balancer, specify the FQDN of the load balancer. FQDN is a host name including a domain name. To request the certificate of a Web server, FQDN must be specified as the owner name of the certificate. (For example: ssoserver.fujitsu.com)

In the scsmakeenv command, specify the password and private-key nickname for access to the Interstage certificate environment. The password is required to access the Interstage certificate environment.

Note

Make sure you remember the private-key nickname specified in the *scsmakeenv* command, which is required to register the site certificate acquired from the certificate authority.

Refer to 'SSL Commands' in Reference Manual (Command Edition) for details of the scsmakeenv command for CSR creation.

Example

Windows32/64

The following is an example in which the name of the CSR output destination file is 'C:\WINNT\temp\ssocert.txt'. When necessary, change the name of the CSR output destination file.

When password entry is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

When you are requested to enter distinguished names, enter them in the bold as shown below.

- Site Certificate Nickname: 'SERVERCERT'
- CSR output destination file name : 'C:\WINNT\temp\ssocert.txt'
- Country code: jp
- Alphanumeric first and last name: ssoserver.fujitsu.com
- Alphanumeric organization name: FUJITSU
- Alphanumeric organizational unit name: FUJITSU TOKYO
- Prefecture name: Tokyo
- Municipality name: Shinjuku

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

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

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

Solaris32/64 Linux32/64

The following is an example in which the Interstage certificate environment with the access permission by 'iscertg' is newly created and a CSR is created. When the Interstage certificate environment is already created, set the access permission in the Interstage certificate environment when necessary.

In this example, iscertg is created as the owner group permitted access to the Interstage certificate environment. The effective user 'nobody' is added to the owner group iscertg. 'Nobody' is set as the initial value in the User directive of the environment configuration file (httpd.conf) of the Interstage HTTP server. The name of the CSR output destination file is '/tmp/ssocert.txt'. Change the CSR output destination file when necessary.

Before requesting the CSR, set the JDK or JRE installation path in environment variable JAVA_HOME.

The following example uses the Bourne shell. When password input is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

When you are requested to enter distinguished names, enter them in bold as shown below.

- Site Certificate Nickname: 'SERVERCERT'
- CSR output destination file name: '/tmp/ssocert.txt'

- Country code: jp
- Alphanumeric first and last name: ssoserver.fujitsu.com
- Alphanumeric organization name: FUJITSU
- Alphanumeric organizational unit name: FUJITSU TOKYO
- Prefecture name: Tokyo
- Municipality name: Shinjuku
- Group which is permitted to access to Interstage certificate environment: iscertg

```
# JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
# scsmakeenv -n SERVERCERT -f /tmp/ssocert.txt -g iscertg
New Password:
Retype:

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

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

D.4 Registering the Certificates for SSL Communication

The site certificate issued by a certificate authority and the CA certificate of the certificate authority that issued the site certificate must be acquired and registered.

Depending on the CA, the intermediate CA certificate may need to be registered. For details, refer to "Setting and Use of the Interstage Certificate Environment" - "Configuring the Interstage Certificate Environment with CSR" - "Registering Certificates and CRL" in the "Security System Guide".

Use the certificate and CRL registration command (scsenter) to register these certificates.

In the scsenter command, specify the passwords and certificate nicknames that are specified in the scsmakeenv command for access to the Interstage certificate environment. To register the site certificate that was acquired from the certificate authority, use the scsmakeenv command to specify the nickname specified in the private-key. Be sure to specify the -o option for registering the site certificate.

Refer to 'SSL Commands' in Reference Manual (Command Edition) for details of the scsenter command.

Example

Windows32/64

CA certificate: 'C:\WINNT\temp\ca-cert.cer'

CA Certificate Nickname: 'CACERT'

Site certificate: 'C:\WINNT\temp\server-cert.cer'

Site Certificate Nickname: 'SERVERCERT'

The following shows an example of the scsenter command in which C:\WINNT\temp\ca-cert.cer is specified as the CA certificate and C:\WINNT\temp\server-cert.cer is specified as the site certificate. Change the file path of each certificate when necessary.

When password entry is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

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

Solaris32/64 Linux32/64

CA certificate: '/tmp/ca-cert.cer'

CA Certificate Nickname: 'CACERT'

Site certificate: '/tmp/server-cert.cer'

Site Certificate Nickname: 'SERVERCERT'

The following shows an example of the scsenter command in which /tmp/ca-cert.cer is specified as the CA certificate and /tmp/server-cert.cer is specified as the site certificate. Change the file path of each certificate when necessary.

Before requesting the certificates, set the JDK or JRE installation path in environment variable JAVA_HOME.

The following example uses the Bourne shell. When password input is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

```
# JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
# scsenter -n CACERT -f /tmp/ca-cert.cer
Password:
Certificate was added to keystore
UX:SCS: INFO: scs0104: Certificate was imported
# scsenter -n SERVERCERT -f /tmp/server-cert.cer -o
Password:
Certificate reply was installed in keystore
UX:SCS: INFO: scs0104: Certificate was imported
#
```

D.5 Creating the Interstage Certificate Environment

The Interstage certificate environment is created using the "scsmakeenv" command.

For details about the "scsmakeenv" command, refer to "SSL Environment Setting Commands" in the "Reference Manual (Command Edition)".

Example

Windows32/64

In the example below, a new Interstage certificate environment is created using the "scsmakeenv" command.

When you are prompted to enter your password, enter the password for access to the Interstage certificate environment. The password that you enter will not be displayed.

```
C:\> scsmakeenv -e
New Password:
Retype:
SCS: INFO: scs0100: Interstage certificate environment was created
C:\>
```

Solaris32/64 Linux32/64

The following example shows how the Interstage certificate environment access permission is granted to the user 'iscertg' when it is created for the first time using the scsmakeenv command.

In this example, iscertg is created as the owner group permitted access to the Interstage certificate environment. The effective user 'nobody' is added to the owner group iscertg. 'Nobody' is set as the initial value in the User directive of the environment configuration file (httpd.conf) of the Interstage HTTP server.

Before requesting the certificates, set the JDK or JRE installation path in environment variable JAVA_HOME.

The following example uses the Bourne shell. When the password input is requested, enter the password for access to the Interstage certificate environment. The entered password will not be displayed.

```
# JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
# scsmakeenv -e -g iscertg
New Password:
Retype:
UX:SCS: INFO: scs0100: Interstage certificate environment was created
UX:SCS: INFO: scs0180: The owners group of Interstage certificate environment was set
#
```

D.6 Registering the Certificate of the CRL-issuing Authority

The certificate of the authority that issued the CRL must be acquired and registered before registering the CRL. If the certificate of the CRL-issuing authority has not been registered, register the certificate of the CRL-issuing authority.

Depending on the CA, the intermediate CA certificate may need to be registered. For details, refer to "Setting and Use of the Interstage Certificate Environment" - "Configuring the Interstage Certificate Environment with CSR" - "Registering Certificates and CRL" in the "Security System Guide".

To register the certificate of the CRL-issuing authority, use the certificate and CRL registration command (scsenter).

In the scsenter command, specify the password and certificate nickname that were specified in the scsmakeenv command for access to the security environment.

Refer to 'SSL Commands' in the Reference Manual (Command Edition)the Reference Manual (Command Edition) for details of the scsenter command.

Example

Windows32/64

Certificate of CRL-issuing authority: 'C:\WINNT\temp\crlca-cert.cer'

Nickname of certificate of CRL-issuing authority: 'CRLCACERT'

The following shows an example of the scsenter command in which C:\WINNT\temp\crlca-cert.cer is specified as the certificate of the CRL-issuing authority. Change the file path of the certificate when necessary.

When password entry is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

```
C:\>scsenter -n CRLCACERT -f C:\WINNT\temp\crlca-cert.cer
Password:
Certificate was added to keystore
SCS: INFO: scs0104: Certificate was imported
C:\>
```

Solaris32/64 Linux32/64

Certificate of CRL-issuing authority: '/tmp/crlca-cert.cer'

Nickname of certificate of CRL-issuing authority: 'CRLCACERT'

The following shows an example of the scsenter command in which /tmp/crlca-cert.cer is specified as the certificate of the CRL-issuing authority. Change the file path of the certificate when necessary.

Before requesting the certificates, set the JDK or JRE installation path in environment variable JAVA_HOME.

The following example uses the Bourne shell. When password input is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

```
# JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
# scsenter -n CRLCACERT -f /tmp/crlca-cert.cer
Password:
Certificate was added to keystore
UX:SCS: INFO: scs0104: Certificate was imported
#
```

D.7 Registering CRL

To confirm the validity of a certificate, the CRL that was acquired from the certificate authority must be registered using the certificate and CRL registration command (scsenter).

In the scsenter command, specify the password that was specified in the scsmakeenv command to access the security environment.

The -o option must always be specified to register the CRL.

Refer to 'SSL Commands' in the Reference Manual (Command Edition) for details of the scsenter command.

The validity of a user's certificate can be confirmed by setting [Yes] in [Enable Certificate Revocation Check?] of [Certificate Authentication Settings] in authentication server settings after CRL registration.

Example

Windows32/64

CRL that was acquired from certificate authority: 'C:\WINNT\temp\crl.crl'

The following is an example of the scsenter command in which C:\WINNT\temp\crl.crl is specified as the acquired CRL. Change the CRL file path when necessary.

When password input is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

```
C:\>scsenter -c -f C:\WINNT\temp\crl.crl
Password:
SCS: INFO: scs0105: CRL was imported
C:\>
```

Solaris32/64 Linux32/64

CRL that was acquired from certificate authority: '/tmp/crl.crl'

The following shows an example of the scsenter command in which /tmp/crl.crl is specified as the acquired CRL. Change the CRL file path when necessary.

Before registering the CRL, set the JDK or JRE installation path in environment variable JAVA_HOME.

The following example uses the Bourne shell. When password input is requested, enter the password for access to the Interstage certificate environment. The entered password is not displayed.

```
# JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
# scsenter -c -f /tmp/crl.crl
Password:
UX:SCS: INFO: scs0105: CRL was imported
#
```

Appendix E Settings of the Load Balancer

In the Interstage single sign-on, the server load can be distributed by setting the load balancer before setting up the repository server and the authentication server.

However, the load balancer will need to be set up differently depending on the operation, such as according to the system configuration or the functions required. The load will not be correctly distributed unless the correct settings are used.

This appendix explains how to set the load balancer for the following system configurations:

- E.1 Load Distribution of the Repository Server (Update System)
- E.2 Load Distribution of the Authentication Server
- E.3 Load Distribution of the Repository Server and the Authentication Server that are Built on the Same Machine

E.1 Load Distribution of the Repository Server (Update System)

When the load balancer is newly added and the load is distributed by adding the repository server (update system), set the load balancer in accordance with the operations required.

To perform session management, set up as follows:

Session uniqueness guarantee function (session maintenance function)

Table E.1 Load Balancer Guarantee Method Settings

Configuration item	Value set
Guarantee method	Use cookies or URL embedded parameters (other) to identify sessions.
Guarantee duration	Set a value that is larger than the idle surveillance time (*1)
Keyword	fj-is-sso-disperse=

Fault monitoring function

Use one of the following methods to set the fault monitoring function:

- Use a monitoring tool such as Systemwalker to monitor and detect load balancer faults, and configure a repository server to restart if a fault is detected on that repository server.
- For the load balancer fault monitoring interval, set a value that is longer than the idle monitoring time (*1).

*1 To check the idle monitoring time, use the Interstage Management Console on the repository server (update system). Under the [System] menu, click the [Security] > [Single sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, then click [Session management detailed settings [Show]]. Check the [Idle surveillance time] shown for [Idle surveillance].

Note

Note the following if a new load balancer has been added to the repository server in operation:

- Set the host name of the repository server that is already set up to the load balancer.
- Do not change the repository server (update system) URL. For details about the repository server URL, refer to "Repository Server URL".

E.2 Load Distribution of the Authentication Server

When one or more authentication servers are set up to balance the load, the load balancer is set up differently depending on the functions to be used.

Set the load balancer in accordance with the operations, as outlined below.

Table E.2 Functions used in load balancing

Integrated Windows authentication	Directory service that registers the user information	
	Interstage directory service	Active Directory
Do not perform	- (*1)	- (*1)
Perform	Settings 1	Settings 2

*1 The special setup mentioned in the next section is not required.

Settings 1

Distribution method

Set up so that access to the authentication infrastructure URL is distributed to all authentication servers.

Table E.3 Load Balancer Distribution Method Settings

Configuration item	Value set
Distribution method	Set a method other than the round robin method

Session uniqueness guarantee function (session maintenance function)

Table E.4 Load Balancer Guarantee Method Settings

Configuration item	Value set
Guarantee method	Use cookies or URL embedded parameters (other) to identify sessions.
Guarantee duration	Set a value that is larger than the idle surveillance time (*1)
Keyword	fj-is-sso-disperse=

Settings 2

Session uniqueness guarantee function (session maintenance function)

Table E.5 Load Balancer Guarantee Method Settings

Configuration item	Value set
Guarantee method	Identify the session by Cookie or URL embedded parameter ((ServletAPI2.2).
Guarantee duration	Value larger than the Integrated Windows authentication application session timeout (session-timeout). (*2)(*3)

*1 For idle monitoring time, in the repository server (update system) Interstage management console, click [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, then click [Session management detailed settings [Show]], and check [Idle surveillance time] in [Idle surveillance].

*2 The session timeout value is set in the environment configuration file of the Integrated Windows Authentication application stored in the following locations. The default value for session timeout is one minute. When you change the session timeout, change the guarantee time if necessary.

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\webapps\winauth\WEB-INF\web.xml
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/webapps/winauth/WEB-INF/web.xml
```

*3 For details about the session timeout, refer to "Web Application Development" - "Web Application Environment Definition File (Deployment Descriptor)" in the "J2EE User's Guide".

Note

- Note the following if a new load balancer is added to the repository server in operation:
    - Set the host name of the authentication server that is already set in the load balancer.
    - Do not change the authentication infrastructure URL. For details about the authentication infrastructure URL, refer to "Authentication infrastructure URL".
- If the Load Balancer has the unique guarantee keyword duplication un-checked, then make sure it is not configured to check it.
- To install the load balancer and use the session uniqueness guarantee feature (session maintenance feature), disable the Web server HTTP Keep-Alive feature in the Interstage Management Console. The HTTP Keep-Alive feature settings are configured by clicking [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Settings] tab, [Detailed Settings[Show]], then [Detailed Settings], [Enable HTTP Keep-Alive?].

E.3 Load Distribution of the Repository Server and the Authentication Server that are Built on the Same Machine

When the repository server and the authentication server are built on the same machine, and are extended, the load balancer is set differently depending on the functions to be used.

Also, check in the Interstage management console, that the [Repository server (update system) URL] is correctly set.

When performing the session management, use the following settings:

Integrated Windows authentication	Directory service that registers user information	
	Interstage directory service	Active Directory
Do not perform	Settings1,Confirmation1	Settings2,Confirmation2
Perform	Settings1,Confirmation1	Settings2,Settings3,Confirmation2

When not performing the session management, use the following settings:

Integrated Windows authentication	Directory service that registers user information	
	Interstage directory service	Active Directory
Do not perform	- (*1)	- (*1)
Perform	Settings1	Settings3

*1 The special setup mentioned in the next section is not required.

Settings 1

Distribution method

Set so that access to the authentication infrastructure URL is distributed to all repository servers.

Table E.6 Load Balancer Distribution Method Settings

Configuration item	Value set
Distribution method	Set a method other than the round robin method

Session uniqueness guarantee function (session maintenance function)

Table E.7 Load Balancer Guarantee Method Settings

Configuration item	Value set
Guarantee method	Use cookies or URL embedded parameters (other) to identify sessions.
Guarantee duration	Set a value that is larger than the idle surveillance time (*1)
Keyword	fj-is-sso-disperse=

Fault monitoring function

Use one of the following methods to set the fault monitoring function:

- Use a monitoring tool such as Systemwalker to monitor and detect load balancer faults, and configure a repository server to restart if a fault is detected on that repository server.
- For the load balancer fault monitoring interval, set a value that is longer than the idle monitoring time (*1).

Settings 2

Settings to define that access to the Repository server (update system) URL is distributed

Session uniqueness guarantee function (session maintenance function)

Table E.8 Load Balancer Guarantee Method Settings

Configuration item	Value set
Guarantee method	Use cookies or URL embedded parameters (other) to identify sessions.
Guarantee duration	Set a value that is larger than the idle surveillance time (*1)
Keyword	fj-is-sso-disperse=

Fault monitoring function

Use one of the following methods to set the fault monitoring function:

- Use a monitoring tool such as Systemwalker to monitor and detect load balancer faults, and configure a repository server to restart if a fault is detected on that repository server.
- For the load balancer fault monitoring interval, set a value that is longer than the idle monitoring time (*1).

Settings 3

Settings to define that access to the Authentication infrastructure URL is distributed

Session uniqueness guarantee function (session maintenance function)

Table E.9 Load Balancer Guarantee Method Settings

Configuration item	Value set
Guarantee method	Identify the session by Cookie or URL embedded parameter ((ServletAPI2.2)
Guarantee duration	Value larger than the Integrated Windows authentication application session timeout (session-timeout) (*2)(*3)

Confirmation 1

Confirming [Repository server (update system) URL]

In the Interstage management console, select [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab, and check that "localhost" is set in [Repository server (update system) URL] of [Detailed settings[Show]].

When something other than "localhost" is set, change the settings of the [Repository server (update system) URL] of the repository server and the authentication server according to the following procedures.

- For the Repository server

  Change [Repository server (update system) URL] to "localhost" in [System] > [Security] > [Single sign-on]> [Authentication infrastructure] > [Repository server] > [Settings] tab > [Repository server detailed settings[Show]].

  If the load is distributed to the repository server, perform this on all repository servers that have a load distributed to them.

- For the Authentication server

  Follow these steps:

  1. Click [System] > [Security] > [Single sign-on]> [Authentication infrastructure] > [Authentication infrastructure setup file] tab, and download the Authentication infrastructure setup file.

2. In [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab, check the details of the environment settings of the authentication server. These same settings will need to be reconstructed in the authentication server.

3. Delete the authentication server once.

4. Select the Web server (Interstage HTTP Server) that creates the authentication server. If there is no Web server for creating an authentication server, create a new Web server exclusively for the Interstage single sign-on.

5. If the authentication server is to use SSL communication, set the SSL settings in the Web server that was selected or created in Step 4 according to the operation.

6. Use the Authentication infrastructure setup file downloaded in Step 1 to set up the authentication server.

7. Click [System] > [Security] > [Single sign-on]> [Authentication infrastructure] > [Authentication server] > [Settings] tab, and set the details of the environment settings of the authentication server which were obtained in Step 2.

8. Click [Detailed settings[Show]], and check whether "localhost" is set in the [Repository server (update system) URL] of the [Communication Settings with Repository server].

If the load of the Authentication server is distributed, export the environment of the authentication server which was changed in the above procedure, using the ssobackup command, and import the environment in to the remaining authentication servers with the ssorestore command.

If the load balancer has just been newly added to the Authentication infrastructure server in operation:

- Set the host name of the authentication server which is already set up to the load balancer, and do not change the Authentication infrastructure URL (*4).

Confirmation 2

Confirming [Repository server (update system) URL]

In the Interstage management console, select [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab, and check if the host name of the repository server, which is set in the load balancer, is set in [Repository server (update system) URL] of [Detailed settings [Show]].

If something other than the host name of the repository server is set in the load balancer, change the settings of the [Repository server (update system) URL] of the repository server and the authentication server in according to the following procedure:

For the Repository server

Change [Repository server (update system) URL] of [System] > [Security] > [Single sign-on]> [Authentication infrastructure] > [Repository server] > [Settings] tab > [Repository server detailed settings[Show]] to the host name of the repository server set in the load balancer.

If the load of the repository server is distributed, perform this to all repository servers.

For the Authentication server

Follow these steps:

1. Click [System] > [Security] > [Single sign-on]> [Authentication infrastructure] > [Authentication infrastructure setup file] tab, and download the Authentication infrastructure setup file.

2. In [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Authentication server] > [Settings] tab, check the details of the environment settings of the authentication server. These same settings need to be reconstructed in the authentication server.

3. Delete the authentication server once.

4. Select the Web server (Interstage HTTP Server) that creates the authentication server. If there is no Web server for creating an authentication server, create a new Web server exclusively for the Interstage single sign-on.

5. If the authentication server is to use SSL communication, set the SSL settings in the Web server that was selected or created in Step 4 according to the operation.

6. Use the Authentication infrastructure setup file downloaded in Step 1 to set up the authentication server.

7. Click [System] > [Security] > [Single sign-on]> [Authentication infrastructure] > [Authentication server] > [Settings] tab, and set the details of the environment settings of the authentication server which was confirmed in Step 2.

8. Click [Detailed settings [Show]], and check if the host name of the repository server set in the load balancer is set in the [Repository server (update system) URL] of [Communication Settings with Repository server].

If the load of the authentication server is distributed, export the environment of the authentication server, which was changed in the above procedure, with the ssobackup command and import the environment in the remaining authentication server with the ssorestore command.

Note the following when the load balancer is newly added to the Authentication infrastructure in operation.

- Set the host name of the repository server which has already been set to the load balancer, and do not change repository server (update system) URL (*5)

- Set the host name of the authentication server which is already setup to the load balancer, and do not change the Authentication infrastructure URL (*4).

*1 For idle monitoring time, in Interstage management console of the repository server (update system), click [Session management detailed settings[Show]] of [System] > [Security] > [Single sign-on] > [Authentication infrastructure] > [Repository server] > [Settings] tab, and check [Idle surveillance time] of [Idle surveillance].

*2 The session timeout value is set in the environment configuration file of the Integrated Windows authentication application stored in the following. The default value of the session timeout is set at one minute. When the session timeout is changed, change the guarantee time if necessary.

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\webapps\winauth\WEB-INF\web.xml
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/webapps/winauth/WEB-INF/web.xml
```

*3 For details about the session timeout, refer to "Web Application Development" - "Web Application Environment Definition File (Deployment Descriptor)" in the "J2EE User's Guide".

*4 For details about the Authentication infrastructure URL, refer to "Authentication infrastructure URL".

*5 For details about the Repository server (update system) URL, refer to "Repository server URL".

- If the Load Balancer has the unique guarantee keyword duplication un-checked, then make sure it is not configured to check it.

- To install the load balancer and use the session uniqueness guarantee feature (session maintenance feature), disable the Web server HTTP Keep-Alive feature in the Interstage Management Console. The HTTP Keep-Alive feature settings are configured by clicking [System] > [Services] > [Web Server] > [Web Server Name] > [Web Server Settings] tab, [Detailed Settings[Show]], then [Detailed Settings], [Enable HTTP Keep-Alive?].

Appendix F Settings for Active Directory Linkage

This appendix describes the settings that must be configured to use Active Directory.

The setup procedure for linking to Active Directory is different depending on which of the following directory services is used to register user information:

- Active Directory
- Interstage Directory Service

F.1 Using Active Directory as the Directory Service for Registering User Information

To use Active Directory as the Directory Service for registering user information, configure the basic stages outlined below. Details for configuring each stage are provided later in this chapter.

1. Set up an extended schema for Single Sign-on
2. Set up user information for Active Directory
3. Create an SSO repository

   Refer to "Creating an SSO Repository"
4. Set up an SSO repository
   - If an extended schema for Single Sign-on is not used:

     Register role configuration and make associations configuration by referring to "Creating and Setting up the SSO Repository (Associating Role Configuration)".
   - If an extended schema for Single Sign-on is used:

     Register role configuration by referring to "Registering User Information and Role Configuration in the SSO Repository". (*1)
5. Create an environment for SSL communications, if necessary
6. Create a repository server
7. Create an authentication server, if using a separate machine to the repository server
8. Configure Integrated Windows Authentication:
   1. Active Directory Setup
   2. Integrated Windows Authentication Application Deployment
   3. WorkUnit Start User Setup
   4. Web Browser Setup

*1 User information is registered with Active Directory, therefore there is no need to register user information in the SSO repository.

Note

Before starting the operation, be sure to check that the user has authority to access the protection path.

F.1.1 Set up an Extended Schema for Single Sign-on

An extended schema for single sign-on means that users can sign on using password or certificate authentication, without having to sign on with Integrated Windows authentication.

In Interstage Single Sign-on, the extended schema sample file shown below is provided. A Single Sign-on schema can be extended using this file.

Sample File Names and Storage Directory for Single Sign-on Extended Schemas

Sample file for attribute schemas:

sso_attribute_for_ad.ldf

Sample file for object class schemas: (*1)

sso_class_for_ad.ldf

Sample storage directory:

Windows32/64

C:\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad

Solaris32/64 Linux32/64

/opt/FJSVssosv/sample/OtherDirectory/ad

Perform the following procedure on the machine where Active Directory is running. Refer to the Active Directory manuals for more information about the *ldifde* command used in this example.

*1 In this sample file, Single Sign-on schema extension is performed for the inetOrgPerson object class. If you want to perform it for the user object class instead, then replace "inetOrgPerson" in this sample file to "user".

Example

File for the Single Sign-on extended attribute schema: C:\Temp\sso_attribute_for_ad.ldf

File for the Single Sign-on extended object class schema: C:\Temp\sso_class_for_ad.ldf

Active Directory domain name: ad.local

```
C:\>ldifde -i -f C:\Temp\sso_attribute_for_ad.ldf -s localhost -t 389 -k -c
"CN=Schema,CN=Configuration,DC=X" "CN=Schema,CN=Configuration,DC=ad,DC=local"
Connecting to "localhost"
Logging in as current user using SSPI
Importing directory from file "C:\Temp\sso_attribute_for_ad.ldf"
Loading entries...........
10 entries modified successfully.

The command has completed successfully

C:\>ldifde -i -f C:\Temp\sso_class_for_ad.ldf -s localhost -t 389 -k -c
"CN=Schema,CN=Configuration,DC=X" "CN=Schema,CN=Configuration,DC=ad,DC=local"
Connecting to "localhost"
Logging in as current user using SSPI
Importing directory from file "C:\Temp\sso_class_for_ad.ldf"
Loading entries.....
4 entries modified successfully.

This command has completed successfully

C:\>
```

F.1.2 Setting up User Information for Active Directory

This section explains points that should be noted when setting up user information in Active Directory.

Object Classes

The user registered in Active Directory is managed by the following object classes:

If not using an extended schema for single sign-on

Table F.1 Not using an extended schema

User information object class	Description
top	Basic LDAP object class
person	User information
organizationalPerson	
user	

If using an extended schema for single sign-on

Table F.2 Using an extended schema

User information object class	Description
top	Basic LDAP object class
person	User information
organizationalPerson	
user	
inetOrgPerson (*1)	
ssoUser (*2)	SSO user information

*1 There is no need to register this in the user information if the Single Sign-on extended object class schema sample file is edited and Single Sign-on schema extension performed for the user object class when the Single Sign-on extended schema is set.

*2 The ssoUser object class is set up as an auxiliary class for inetOrgPerson when setting up the extended schema for single sign-on. This means that the ssoUser object class does not need to be registered in the user information.

Attributes

Set each attribute that can be set to the entry of each user configuration according to operation as follows.

Note that the size of each attribute is determined by Active Directory.

	If not using an extended schema for Single Sign-on	If using an extended schema for Single Sign-on
Attributes that must always be specified	cn	cn ssoUserStatus
Attributes that must be set for executing Integrated Windows Authentication (*1)	userPrincipalName	userPrincipalName sAMAccountName (*2)
Attributes that must be set for executing password authentication	No setting required	sAMAccountName (*2)
Attributes that must be set for executing certificate authentication (*3)	No setting required	mail employeeNumber uid serialNumber dnQualifier cn
Attributes that must be specified depending on operation	None	ssoAuthType ssoRoleName

	If not using an extended schema for Single Sign-on	If using an extended schema for Single Sign-on
		ssoCredentialTTL ssoNotBefore ssoNotAfter
Attributes that must be specified depending on operation	None	ssoFailureCount ssoLockTimeStamp ssoSessionInfo

*1 These attributes are not included in user accounts (such as "Administrator") that already exist immediately after Active Directory has been created. To perform Integrated Windows Authentication using these user accounts, set up these attributes and then perform an authentication operation.

*2 Interstage Single Sign-on regards this attribute as a user ID for uniquely identifying users.

*3 These attributes uniquely identify users based on the owner name information in the user certificate. Set up one of these attributes.

This section explains the attributes used with Interstage Single Sign-on.

Refer to Active Directory manuals, for more information about Active Directory attributes.

(1) ssoRoleName

This attribute is the same as the user information registered with the SSO repository. Refer to "User Information Entry".

(2) ssoAuthType

This attribute is the same as the user information registered with the SSO repository. Refer to "User Information Entry".

(3) ssoCredentialTTL

This attribute is the same as the user information registered with the SSO repository. Refer to "User Information Entry".

(4) ssoUserStatus

Description

This attribute specifies the lock status of the user account as follows:

- good: Not locked

- locked: Locked

Example of Specification

good

Note

Be sure to set up values for user information. If values are not set up, authentication will fail.

[Release User Lock] on the Interstage Management Console is used to unlock the user account. Refer to "Canceling Lockout" for details of how to unlock the user account.

This attribute can operate in user programs to lock out users. Refer to "Locking a user" in the Appendix "Samples of User Program Descriptions".

(5) ssoNotBefore

Description

This attribute specifies the date when single sign-on is started for a user.

If the user attempts to use single sign-on before the specified date, authentication will fails.

If this attribute is omitted, the user can use single sign-on immediately.

Specify the date in the format YYYYMMDDHHMMSS.0+XXXX. (*1) For Greenwich Mean Time, specify the date in the format YYYYMMDDHHMMSS.0Z.

Note that this attribute adjusts automatically to Daylight Saving Time.

- YYYY: Year (four digits of the year)
- MM: Month (two digits)
- DD: Day (two digits)
- HH: Hour (two digits for 24 hours)
- MM: Minute (two digits)
- SS: Second (two digits)

*1 "+XXXX" (or "-XXXX") refers to the time difference from UTC (Universal Time Coordinate).

Character Types that can be Specified

Numbers

Example of Specification

20030101000000.0+0900

Note

Set a different date and time for ssoNotBefore and ssoNotAfter. If the same date and time is specified for both these attributes, user authentication will fail.

Set a date and time for ssoNotBefore that is earlier than the date and time set for ssoNotAfter. If the date and time set for 'ssoNotBefore' is later than the date and time set for 'ssoNotAfter', user authentication will fail.

Specify a date between '20000101000000' and '20371231235959' in ssoNotBefore and ssoNotAfter regardless of what time zone you are using. If a date and time outside this range is set, user authentication will fail.

(6) ssoNotAfter

Description

Specify the date after which single sign-on will not be available to users. If the user attempts single sign-on after the specified date, authentication will fail.

If this attribute is omitted, the user can use single sign-on for an indefinite period.

Specify the date in the format YYYYMMDDHHMMSS.0+XXXX. (*1)

For Greenwich Mean Time, specify the date in the format YYYYMMDDHHMMSS.0Z.

Note that this attribute adjusts automatically to Daylight Saving Time.

- YYYY: Year (four digits of the year)
- MM: Month (two digits)
- DD: Day (two digits)
- HH: Hour (two digits for 24 hours)
- MM: Minute (two digits)
- SS: Second (two digits)

*1 '+XXXX' (or '-XXXX) refers to the time difference from UTC (Universal Time Coordinate).

Character Types that can be Specified

Numbers

Example of Specification

20030102000000.0+0900

Note

Set a different date and time for ssoNotBefore and ssoNotAfter. If the same date and time is specified, user authentication will fail.

Set a date and time for 'ssoNotAfter' that is later than the date and time set for 'ssoNotBefore'. If the date and time set for 'ssoNotAfter' is earlier than the date and time set for 'ssoNotBefore', user authentication will fail.

Specify a date between '20000101000000' and '20371231235959' in ssoNotBefore and ssoNotAfter regardless of which time zone you are using. User authentication will fail, if a date and time outside this range is set.

(7) ssoFailureCount

This attribute is the same as the user information registered with the SSO repository. Refer to 'User Information Entry'.

(8) ssoLockTimeStamp

Description

This attribute specifies the date when the user was locked by the repository server in Greenwich Mean Time (YYYYMMDDHHMMSSZ.0Z).

Note

This attribute can operate in user programs to lock out users. Refer to "Locking a user" in the Appendix "Samples of User Program Descriptions".

To set values in user programs, enter settings in either the "YYYYMMDDHHMMSS.0Z" or "YYYYMMDDHHMMSS.0+XXXX" format. Set a date and time between "20000101000000" and "20371231235959", regardless of what time zone the time is set in. If a date and time outside of this range is set, user authentication will fail.

(9) ssoSessionInfo

This attribute is the same as the user information registered with the SSO repository. Refer to 'User Information Entry'.

F.1.3 Setting up the SSO Repository (Associating Role Configurations)

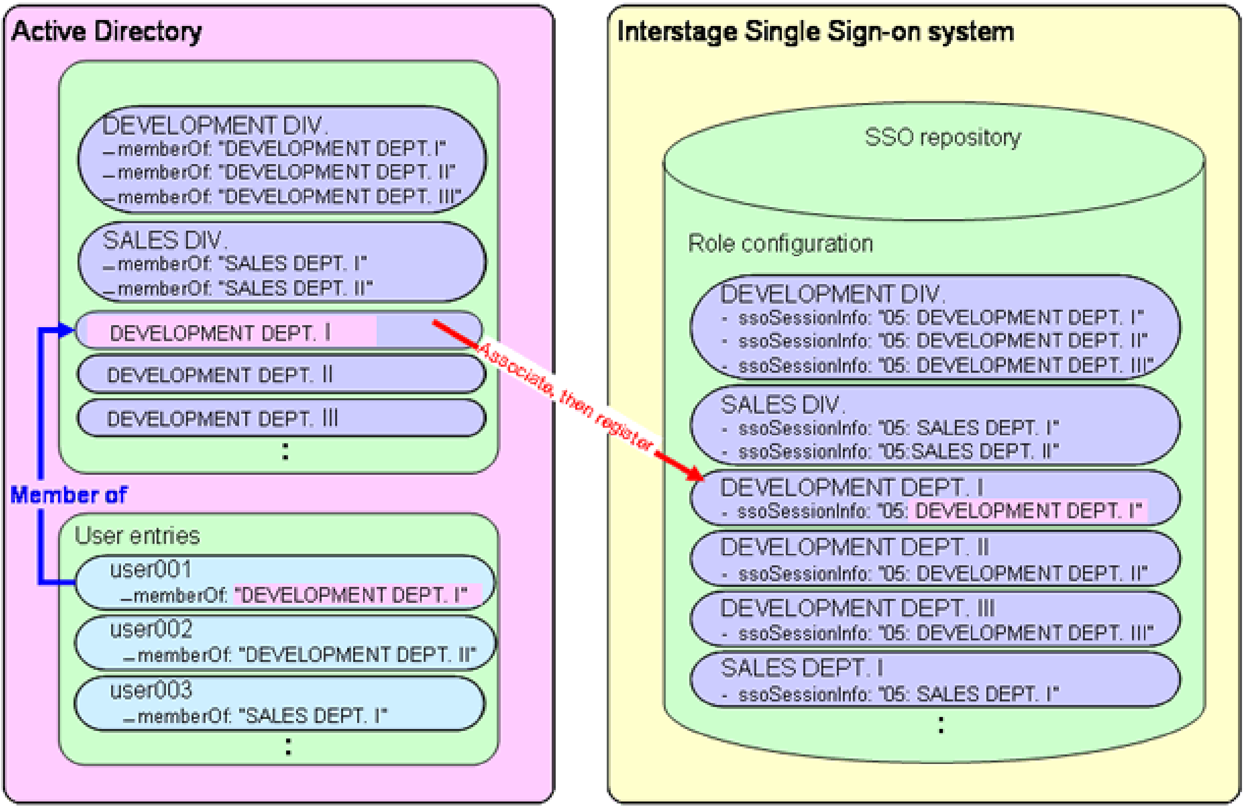
This section outlines how to:

Make associations between the arbitrary attribute values in the user information managed by Active Directory, and the role configuration for Interstage Single Sign-on

Register these associated role configurations in the SSO repository.

In the following example, a group name "DEVELOPMENT DEPT.I" that user entry "user001" registered with Active Directory is associated with the SSO repository role configuration "DEVELOPMENT DEPT.I", and is newly registered.

It is also possible to make associations with role configurations that are already registered in the SSO repository.


Active Directory
DEVELOPMENT DIV.
–memberOf: "DEVELOPMENT DEPT. I"
–memberOf: "DEVELOPMENT DEPT. II"
–memberOf: "DEVELOPMENT DEPT. III"
SALES DIV.
–memberOf: "SALES DEPT. I"
–memberOf: "SALES DEPT. II"
DEVELOPMENT DEPT. I
DEVELOPMENT DEPT. II
DEVELOPMENT DEPT. III
Member of
User entries
user001
–memberOf: "DEVELOPMENT DEPT. I"
user002
–memberOf: "DEVELOPMENT DEPT. II"
user003
–memberOf: "SALES DEPT. I"
Associate, then register
Interstage Single Sign-on system
SSO repository
Role configuration
DEVELOPMENT DIV.
- ssoSessionInfo: "05: DEVELOPMENT DEPT. I"
- ssoSessionInfo: "05: DEVELOPMENT DEPT. II"
- ssoSessionInfo: "05: DEVELOPMENT DEPT. III"
SALES DIV.
- ssoSessionInfo: "05: SALES DEPT. I"
- ssoSessionInfo: "05:SALES DEPT. II"
DEVELOPMENT DEPT. I
- ssoSessionInfo: "05: DEVELOPMENT DEPT. I"
DEVELOPMENT DEPT. II
- ssoSessionInfo: "05: DEVELOPMENT DEPT. II"
DEVELOPMENT DEPT. III
- ssoSessionInfo: "05: DEVELOPMENT DEPT. III"
SALES DEPT. I
- ssoSessionInfo: "05: SALES DEPT. I"

Interstage Single Sign-on provides sample CSV data files.

Role configurations are registered by using the follow sample CSV data files in Interstage Single Sign-on.

Sample File Names and Storage Directory

Sample CSV file for adding roles:

sample_ad_role_mapping_add_en.csv

Sample rule file for adding roles:

sample_ad_role_mapping_rule.xml

Sample CSV file for adding role sets:

sample_ad_roleset_mapping_add_en.csv

Sample rule file for adding role sets:

sample_ad_roleset_mapping_rule.xml

Sample storage directory:

Windows32/64

C:\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad

Solaris32/64 Linux32/64

/opt/FJSVssosv/sample/OtherDirectory/ad

To register role configuration using a CSV data file, execute the *irepmodifyent* command. Refer to "Interstage Directory Service Operation Commands" in the Reference Manual (Command Edition), for more information about this command.

Information can be deleted and updated using CSV data files. Refer to the Directory Service Operator's Guide for more information.

The procedure for registering role configuration using a CSV data file is explained below using the sample CSV data file provided by Interstage Single Sign-on.

In the following example, the values for the groups that include users managed by Active Directory are registered as role configurations. Note that it is also possible to register objects other than groups as role configurations.

1. Get the group list
2. Register roles:
    1. Create a CSV file
    2. Create a rule file
    3. Execute the *irepmodifyent* command
3. Register role sets:
    1. Create a CSV file
    2. Create a rule file
    3. Execute the *irepmodifyent* command

Note

When you create the repository server, if values for groups that include users managed by Active Directory are registered as role configuration, you will need to specify "memberOf" in [Attribute name to use for a role] in [Active Directory Settings]

Getting the Group List

Get the group list from Active Directory via LDAP.

Note

The group that has been set as the primary group with Active Directory cannot be acquired via LDAP with the "memberOf" attribute. When setting the primary group, do not specify a group for which role or role set associations will be made.

Example

Windows32/64

The following example shows how to use the *ldapsearch* command to get the following attributes (belonging to groups) on the repository server machine. The host name of the machine on which Active Directory is running is "ADserver.fujitsu.com", and the Active Directory domain name is "ad.local".

- cn
- distinguishedName
- memberOf

```
C:\> C:\Interstage\bin\ldapsearch -h ADserver.fujitsu.com -p 389 -D
"CN=Administrator,CN=Users,DC=ad,DC=local" -w password -b "DC=ad,DC=local"
"objectClass=group" cn distinguishedName memberOf

dn: CN=DEVELOPMENT DIV.,CN=Builtin,DC=ad,DC=local
cn: DEVELOPMENT DIV.
distinguishedName: CN=DEVELOPMENT DIV.,CN=Builtin,DC=ad,DC=local
memberOf: CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local
memberOf: CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local
memberOf: CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local

dn: CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local
cn: DEVELOPMENT DEPT.I
distinguishedName: CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local

dn: CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local
cn: DEVELOPMENT DEPT.II
distinguishedName: CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local

dn: CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local
cn: DEVELOPMENT DEPT.III
distinguishedName: CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local
```

```
dn: CN=SALES DIV.,CN=Builtin,DC=ad,DC=local
cn: SALES DIV.
distinguishedName: CN=SALES DIV.,CN=Builtin,DC=ad,DC=local
memberOf: CN=SALES DEPT.II,CN=Users,DC=ad,DC=local
memberOf: CN=SALES DEPT.I,CN=Users,DC=ad,DC=local

dn: CN=SALES DEPT.I,CN=Users,DC=ad,DC=local
cn: SALES DEPT.I
distinguishedName: CN=SALES DEPT.I,CN=Users,DC=ad,DC=local

dn: CN=SALES DEPT.II,CN=Users,DC=ad,DC=local
cn: SALES DEPT.II
distinguishedName: CN=SALES DEPT.II,CN=Users,DC=ad,DC=local

dn: CN=GENERAL AFFAIRS DEPT.,CN=Users,DC=ad,DC=local
cn: GENERAL AFFAIRS DEPT.
distinguishedName: CN=GENERAL AFFAIRS DEPT.,CN=Users,DC=ad,DC=local
```

Example

Solaris32/64 Linux32/64

The following example shows how to use the *ldapsearch* command to get the following attributes (belonging to groups) on the repository server machine. The host name of the machine on which Active Directory is running is "ADserver.fujitsu.com", and the Active Directory domain name is "ad.local".

- cn
- distinguishedName
- memberOf

```
#/opt/FJSVirepc/bin/ldapsearch -h ADserver.fujitsu.com -p 389 -D
"CN=Administrator,CN=Users,DC=ad,DC=local" -w password -b "DC=ad,DC=local"
"objectClass=group" cn distinguishedName memberOf

dn: CN=DEVELOPMENT DIV.,CN=Builtin,DC=ad,DC=local
cn: DEVELOPMENT DIV.
distinguishedName: CN=DEVELOPMENT DIV.,CN=Builtin,DC=ad,DC=local
memberOf: CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local
memberOf: CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local
memberOf: CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local

dn: CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local
cn: DEVELOPMENT DEPT.I
distinguishedName: CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local

dn: CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local
cn: DEVELOPMENT DEPT.II
distinguishedName: CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local

dn: CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local
cn: DEVELOPMENT DEPT.III
distinguishedName: CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local

dn: CN=SALES DIV.,CN=Builtin,DC=ad,DC=local
cn: SALES DIV.
distinguishedName: CN=SALES DIV.,CN=Builtin,DC=ad,DC=local
memberOf: CN=SALES DEPT.II,CN=Users,DC=ad,DC=local
memberOf: CN=SALES DEPT.I,CN=Users,DC=ad,DC=local

dn: CN=SALES DEPT.I,CN=Users,DC=ad,DC=local
cn: SALES DEPT.I
distinguishedName: CN=SALES DEPT.I,CN=Users,DC=ad,DC=local
```

```
dn: CN=SALES DEPT.II,CN=Users,DC=ad,DC=local
cn: SALES DEPT.II
distinguishedName: CN=SALES DEPT.II,CN=Users,DC=ad,DC=local

dn: CN=GENERAL AFFAIRS DEPT.,CN=Users,DC=ad,DC=local
cn: GENERAL AFFAIRS DEPT.
distinguishedName: CN=GENERAL AFFAIRS DEPT.,CN=Users,DC=ad,DC=local
```

Note

For the results above, you will need to register the groups as follows:

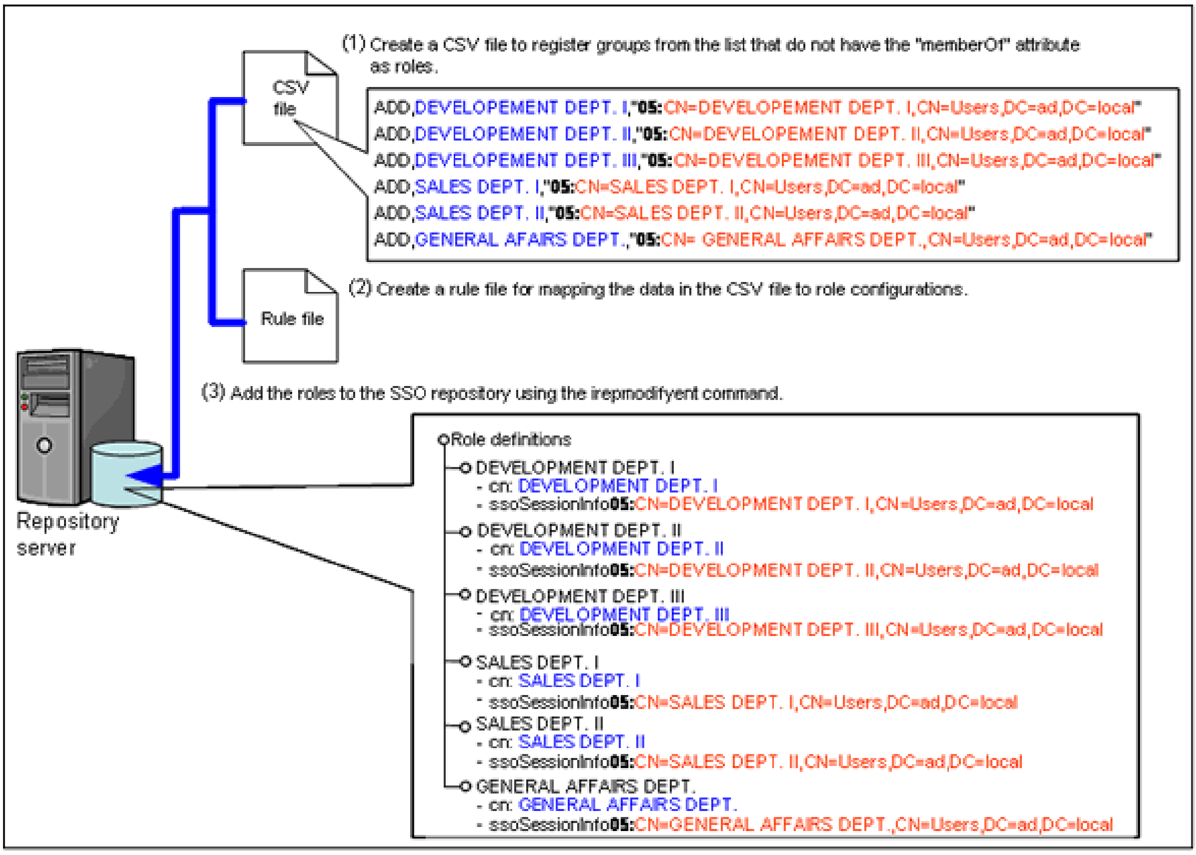
groups that contain "memberOf" attributes should be registered as role sets

groups that do not contain "memberOf" attributes should be registered as roles.

Registering Roles

To register roles (that is, to register groups in the group list that do not contain "memberOf" attributes), use the following procedure:

1. Create a CSV file
2. Create a rule file
3. Execute the *irepmodifyent* command



(1) Create a CSV file to register groups from the list that do not have the "memberOf" attribute as roles.

```
ADD,DEVELOPEMENT DEPT. I,"05:CN=DEVELOPEMENT DEPT. I,CN=Users,DC=ad,DC=local"
ADD,DEVELOPEMENT DEPT. II,"05:CN=DEVELOPEMENT DEPT. II,CN=Users,DC=ad,DC=local"
ADD,DEVELOPEMENT DEPT. III,"05:CN=DEVELOPEMENT DEPT. III,CN=Users,DC=ad,DC=local"
ADD,SALES DEPT. I,"05:CN=SALES DEPT. I,CN=Users,DC=ad,DC=local"
ADD,SALES DEPT. II,"05:CN=SALES DEPT. II,CN=Users,DC=ad,DC=local"
ADD,GENERAL AFAIRS DEPT.,"05:CN= GENERAL AFFAIRS DEPT.,CN=Users,DC=ad,DC=local"
```

(2) Create a rule file for mapping the data in the CSV file to role configurations.

(3) Add the roles to the SSO repository using the irepmodifyent command.

```
Role definitions
 DEVELOPMENT DEPT. I
  - cn: DEVELOPMENT DEPT. I
  - ssoSessionInfo05:CN=DEVELOPMENT DEPT. I,CN=Users,DC=ad,DC=local
 DEVELOPMENT DEPT. II
  - cn: DEVELOPMENT DEPT. II
  - ssoSessionInfo05:CN=DEVELOPMENT DEPT. II,CN=Users,DC=ad,DC=local
 DEVELOPMENT DEPT. III
  - cn: DEVELOPMENT DEPT. III
  - ssoSessionInfo05:CN=DEVELOPMENT DEPT. III,CN=Users,DC=ad,DC=local
 SALES DEPT. I
  - cn: SALES DEPT. I
  - ssoSessionInfo05:CN=SALES DEPT. I,CN=Users,DC=ad,DC=local
 SALES DEPT. II
  - cn: SALES DEPT. II
  - ssoSessionInfo05:CN=SALES DEPT. II,CN=Users,DC=ad,DC=local
 GENERAL AFFAIRS DEPT.
  - cn: GENERAL AFFAIRS DEPT.
  - ssoSessionInfo05:CN=GENERAL AFFAIRS DEPT.,CN=Users,DC=ad,DC=local
```

Creating CSV Files

Extract information for the groups in the group list that do not contain a "memberOf" attribute as CSV data, as shown below.

Column	Item	Content extracted
0th column	The operation to be performed on the SSO repository	To add roles, specify "ADD". (*1)
Ist column	The group	Specify the "cn" value. (*2)

Column	Item	Content extracted
2nd column	The attribute value to be used for the role or role set	Specify the "distinguishedName" value. (*3)(*4)

*1 Refer to the Directory Service Operator's Guide for more information.

*2 If associated role configurations are already registered in the SSO repository, set up the cn value for the role configuration you want to associate.

*3 Add "05:" at the start of the "distinguishedName" value, otherwise the value will not be treated as an attribute value to be used for a role or role set.

*4 When specifying a value that includes commas (","), enclose the value with double quotes ("").

The CSV data corresponding to the data above is as follows:

Example

The following example shows how to set up groups that do not contain "memberOf" attributes.

- cn: DEVELOPMENT DEPT.I
- cn: DEVELOPMENT DEPT.II
- cn: DEVELOPMENT DEPT.III
- cn: SALES DEPT.I
- cn: SALES DEPT.II
- cn: GENERAL AFFAIRS DEPT.

```
ADD,DEVELOPMENT DEPT.I,"05:CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local"
ADD,DEVELOPMENT DEPT.II,"05:CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local"
ADD,DEVELOPMENT DEPT.III,"05:CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local"
ADD,SALES DEPT.I,"05:CN=SALES DEPT.I,CN=Users,DC=ad,DC=local"
ADD,SALES DEPT.II,"05:CN=SALES DEPT.II,CN=Users,DC=ad,DC=local"
ADD,GENERAL AFFAIRS DEPT.,"05:CN=GENERAL AFFAIRS DEPT.,CN=Users,DC=ad,DC=local"
```

Creating Rule Files

Create a rule file to make associations between the CSV data and the role configuration for Interstage Single Sign-on.

Make associations between the CSV data and the attributes for the entries in the role configuration as follows:

Column	Item	Attribute for the entries in the role configuration
0th column	The operation to be performed on the SSO repository	None required.
1st column	The group	cn
2nd column	The attribute value to be used for the role or role set	ssoSessionInfo

The following example explains the rule files for making associations between role configuration and the CSV data shown above.

Example

This example rule file configures the following settings:

Rule Name

sso ad role mapping rule

Public Directory

ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

Entry attribute that uniquely identifies role configuration

cn

Operation

ADD (addition)

Attributes to be set According to CSV Data

cn, ssoSessionInfo

```
<?xml version="1.0" encoding="UTF-8" ?>

<!-- Do not change it.  -->
<!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)>

]>
<!-- Do not change it.  -->

<Csv2Directory>

        <Rule>
                <name>sso ad role mapping rule</name>

<!-- baseDn is defined.  (Required) -->
                <baseDn>ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com</baseDn>

<!-- The one added in front of baseDn is defined.  (Optional) -->
<!-- It is unnecessary for SSO.
                <midDn>ou=3,ou=4,ou=5</midDn>
-->

<!-- RDN is defined.  (Required : RDN can be specified in duplicate : Value
of RDN cannot be specified in duplicate) -->
<!-- Specify the one which becomes unique by either of the number or the attribute name.  -->
                <Rdn>cn</Rdn>

<!-- Is the change of DN considered to be a movement? (Optional) -->
<!-- Specify 1 when considering it.  -->
                <DnChange>1</DnChange>

<!-- objectClass is defined.  -->
                <objectClass>top</objectClass>
                <objectClass>ssoRole</objectClass>

<!-- Character of delimitation when attribute value is made from two or more
CSV items (Optional) -->
<!-- One blank character is used when not specifying it.  -->
<!-- Blank character cannot be specified.  -->
                <attributeSeparator>-</attributeSeparator>

<!-- Specify the attribute in which repetition is not permitted under baseDn.  -->
<!-- Specify the one which becomes unique by either of the number or the attribute name.  -->
<!-- (Optional : It can be specified in duplicate : Value of it cannot be
specified in duplicate) -->
                <unique>cn</unique>

                <CSV>
                        <!-- Operation (Add, Delete, and Modify) to
repository and Position in CSV (Optional) -->
                        <!-- Which position of CSV defines the operation (Add,
Delete, and Modify).  -->
                        <ldapop>
                                <op>0</op>
                                <ldapadd>ADD</ldapadd>
                                <ldapdelete>DEL</ldapdelete>
                                <ldapmodify>MOD</ldapmodify>
                                <ldapmove>MOV</ldapmove>
                        </ldapop>

<!-- Associating of every particular item of CSV and attribute of entry (Optional) -->
                        <Attribute>
                                <cn>1</cn>
                                <ssoSessionInfo>2</ssoSessionInfo>
                        </Attribute>
                </CSV>
        </Rule>
</Csv2Directory>
```

Executing the *irepmodifyent* command

Add entry data according to the association rules by executing the *irepmodifyent* command provided by Interstage Directory Service on the machine where the repository server is to be created.

After executing the *irepmodifyent* command, check whether the entry data has been added correctly (by extracting entry information, for example). Refer to 'Entry Management' in the Directory Service Operator's Guide for information about how to manipulate entries.

Example

Windows32/64

For the administrator DN and Bind password, specify the administrator DN and password for the administrator DN that were specified when the SSO repository was created from the [Repository] window of the Interstage Management Console, which is displayed by selecting [System] > [Service] and then [Repository].

In the example below, the port number for the SSO repository is 389, and the administrator DN is specified as "cn=manager,ou=interstage,o=fujitsu,dc=com".

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

Rule file: C:\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_role_mapping_rule.xml

CSV file: C:\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_role_mapping_add_en.csv

When prompted for the Bind password, enter the password for the administrator DN. Note that the password entered will not be displayed.

```
C:\>irepmodifyent -h localhost -p 389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -r C:
\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_role_mapping_rule.xml -i C:
\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_role_mapping_add_en.csv
Enter Bind password:
IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DEPT.I,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DEPT.II,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DEPT.III,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry cn=SALES DEPT.I,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry cn=SALES DEPT.II,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
```

```
IREP: INFO: irep13570: adding new entry cn=GENERAL AFFAIRS DEPT.,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
C:\>
```

Example

Solaris32/64 Linux32/64

For the administrator DN and Bind password, specify the administrator DN and password for the administrator DN that were specified when the SSO repository was created from the [Repository] window of the Interstage Management Console, which is displayed by selecting [System] > [Service] and then [Repository].

In the example below, the port number for the SSO repository is 389, and the administrator DN is specified by "cn=manager,ou=interstage,o=fujitsu,dc=com".

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

Rule file: /opt/FJSVssosv/sample/OtherDirectory/ad/sample_ad_role_mapping_rule.xml

CSV file: /opt/FJSVssosv/sample/OtherDirectory/ad/sample_ad_role_mapping_add_en.csv

When prompted for the Bind password, enter the password for the administrator DN. Note that the password entered will not be displayed.

```
# irepmodifyent -h localhost -p 389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -r /opt/
FJSVssosv/sample/OtherDirectory/ad/sample_ad_role_mapping_rule.xml -i /opt/FJSVssosv/sample/
OtherDirectory/ad/sample_ad_role_mapping_add_en.csv
Enter Bind password:
UX:IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DEPT.I,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DEPT.II,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DEPT.III,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=SALES DEPT.I,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=SALES DEPT.II,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=GENERAL AFFAIRS DEPT.,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
#
```

Note

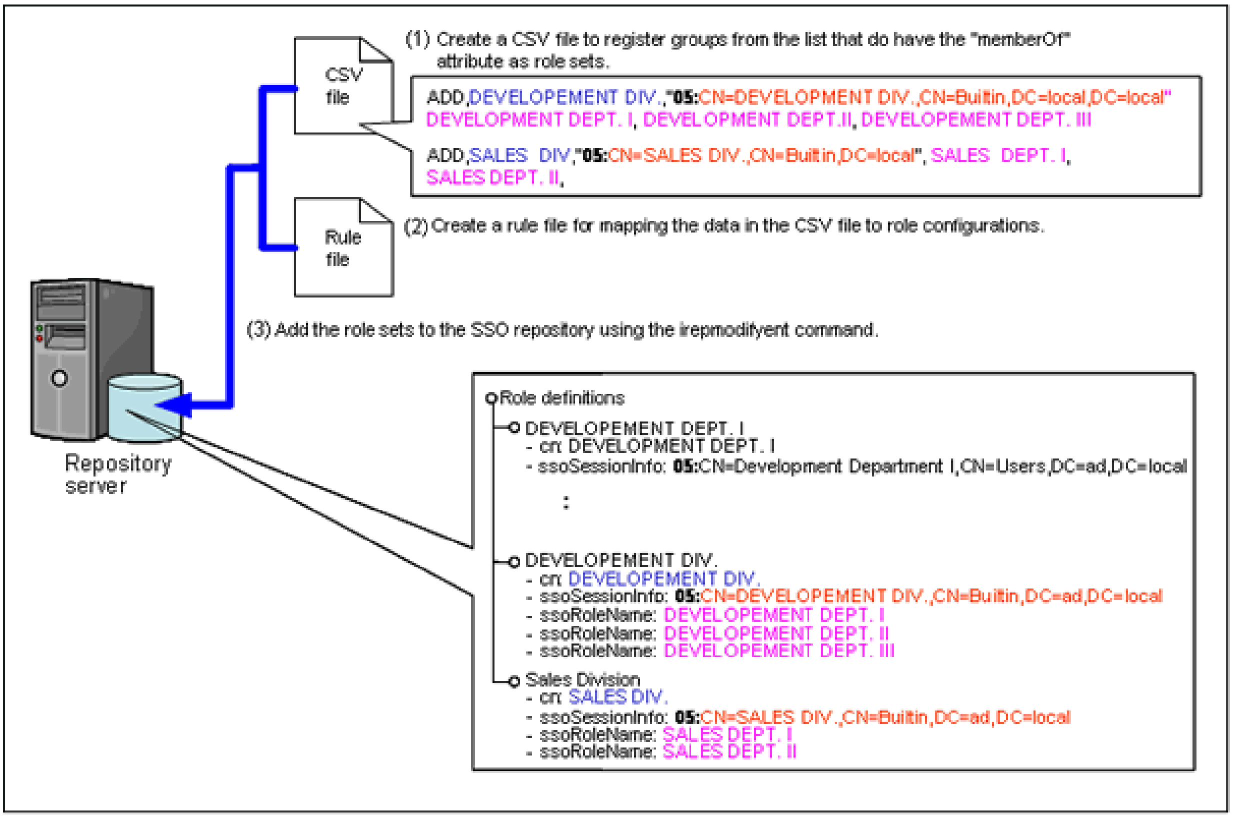
Take special care to protect the password for the administrator DN, and ensure security measures are in place to protect it. Refer to 'Security Measures' under 'Interstage Single Sign-on' in the 'Security Risks' section of the Security System Guide, for more information on protecting passwords.

Registering Role Sets

To register groups as role sets (that is, for the groups in the group list that do contain a "memberOf" attribute), use the following procedure:

1. Create a CSV file
2. Create a rule file

3. Execute the *irepmodifyent* command



(1) Create a CSV file to register groups from the list that do have the "memberOf" attribute as role sets.

```
ADD,DEVELOPEMENT DIV.,"05:CN=DEVELOPMENT DIV.,CN=Builtin,DC=local,DC=local"
DEVELOPMENT DEPT. I, DEVELOPMENT DEPT.II, DEVELOPEMENT DEPT. III

ADD,SALES  DIV,"05:CN=SALES DIV.,CN=Builtin,DC=local", SALES  DEPT. I,
SALES DEPT. II,
```

(2) Create a rule file for mapping the data in the CSV file to role configurations.

(3) Add the role sets to the SSO repository using the irepmodifyent command.

```
Role definitions
 ├ DEVELOPEMENT DEPT. I
 │  - cn: DEVELOPMENT DEPT. I
 │  - ssoSessionInfo: 05:CN=Development Department I,CN=Users,DC=ad,DC=local
 │
 │       :
 │
 ├ DEVELOPEMENT DIV.
 │  - cn: DEVELOPEMENT DIV.
 │  - ssoSessionInfo: 05:CN=DEVELOPEMENT DIV.,CN=Builtin,DC=ad,DC=local
 │  - ssoRoleName: DEVELOPEMENT DEPT. I
 │  - ssoRoleName: DEVELOPEMENT DEPT. II
 │  - ssoRoleName: DEVELOPEMENT DEPT. III
 └ Sales Division
    - cn: SALES DIV.
    - ssoSessionInfo: 05:CN=SALES DIV.,CN=Builtin,DC=ad,DC=local
    - ssoRoleName: SALES DEPT. I
    - ssoRoleName: SALES DEPT. II
```

Creating CSV Files

Extract information for the groups in the group list that do contain a "memberOf" attribute as CSV data, as shown below.

Column	Item	Content extracted
0th column	The operation on the SSO repository	To add a role set, specify "ADD". (*1)
1st column	The group	Specify the "cn" value. (*2)
2nd column	The attribute value to be used for the role or role set	Specify the "distinguishedName" value. (*3)(*4)
3rd column	The content of the role set	Specify the role name ("cn" value) registered during the role registration. (*5)
4th column		
5th column		

*1 Refer to the Directory Service Operator's Guide for more information.

*2 If associated role configurations are already registered in the SSO repository, set up the cn value for the role configuration you want to associate.

*3 Add "05:" at the start of the "distinguishedName" value, otherwise the value will not be treated as an attribute value to be used for a role or role set.

*4 When specifying a value that includes commas (","), enclose the value in double quotes.

*5 Specify columns containing the content of the role set, with a separate column for each role name to be set.

CSV data corresponding to the data above is as follows:

Example

For the following groups that contain "memberOf" attributes, roles are set up so that the value of the "memberOf" attribute is associated with ssoSessionInfo.

- cn: DEVELOPMENT DIV.
    - memberOf: CN=DEVELOPMENT DEPT.I,CN=Users,DC=ad,DC=local
    - memberOf: CN=DEVELOPMENT DEPT.II,CN=Users,DC=ad,DC=local
    - memberOf: CN=DEVELOPMENT DEPT.III,CN=Users,DC=ad,DC=local
- cn: SALES DIV.
    - memberOf: CN=SALES DEPT.I,CN=Users,DC=ad,DC=local
    - memberOf: CN=SALES DEPT.II,CN=Users,DC=ad,DC=local

```
ADD,DEVELOPMENT DIV.,"05:CN=DEVELOPMENT DIV.,CN=Builtin,DC=ad,DC=local",DEVELOPMENT
DEPT.I,DEVELOPMENT DEPT.II,DEVELOPMENT DEPT.III
ADD,SALES DIV.,"05:CN=SALES DIV.,CN=Builtin,DC=ad,DC=local",SALES DEPT.I,SALES DEPT.II
```

Creating Rule Files

Create a rule file to make associations between the CSV data and the role configuration for Interstage Single Sign-on.

Make associations between the CSV data and the attributes for the entries in the role configuration as follows:

Column	Item	Attribute for the entries in the role configuration
0th column	The operation to be performed on the SSO repository	None required.
1st column	The group	cn
2nd column	The attribute value to be used for the role or role set	ssoSessionInfo
3rd column	The content of the role set	ssoRoleName
4th column		
5th column		

The following example explains the rule files for making associations between role configuration and the CSV data shown above.

Example

This example rule file configures the following settings.

Rule Name

sso ad roleset mapping rule

Public Directory

ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com

Entry attribute that uniquely identifies role configuration

cn

Operation

ADD (addition)

Attributes to be set According to CSV Data

cn, ssoSessionInfo, ssoRoleName

```
<?xml version="1.0" encoding="UTF-8" ?>

<!-- Do not change it.  -->
<!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)>

]>
<!-- Do not change it.  -->

<Csv2Directory>

        <Rule>
                <name>sso ad roleset mapping rule</name>

<!-- baseDn is defined.  (Required) -->
                <baseDn>ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com</baseDn>

<!-- The one added in front of baseDn is defined.  (Optional) -->
<!-- It is unnecessary for SSO.
                <midDn>ou=3,ou=4,ou=5</midDn>
-->

<!-- RDN is defined.  (Required : RDN can be specified in duplicate : Value
of RDN cannot be specified in duplicate) -->
<!-- Specify the one which becomes unique by either of the number or the attribute name.  -->
                <Rdn>cn</Rdn>

<!-- Is the change of DN considered to be a movement? (Optional) -->
<!-- Specify 1 when considering it.  -->
                <DnChange>1</DnChange>

<!-- objectClass is defined.  -->
                <objectClass>top</objectClass>
                <objectClass>ssoRoleSet</objectClass>

<!-- Character of delimitation when attribute value is made from two or more
CSV items (Optional) -->
<!-- One blank character is used when not specifying it.  -->
<!-- Blank character cannot be specified.  -->
                <attributeSeparator>-</attributeSeparator>

<!-- Specify the attribute in which repetition is not permitted under baseDn.  -->
<!-- Specify the one which becomes unique by either of the number or the attribute name.  -->
<!-- (Optional : It can be specified in duplicate : Value of it cannot be
specified in duplicate) -->
                <unique>cn</unique>

                <CSV>
                        <!-- Operation (Add, Delete, and Modify) to
repository and Position in CSV (Optional) -->
                        <!-- Which position of CSV defines the operation (Add,
Delete, and Modify).  -->
                        <ldapop>
                                <op>0</op>
                                <ldapadd>ADD</ldapadd>
                                <ldapdelete>DEL</ldapdelete>
                                <ldapmodify>MOD</ldapmodify>
                                <ldapmove>MOV</ldapmove>
                        </ldapop>

<!-- Associating of every particular item of CSV and attribute of entry (Optional) -->
                        <Attribute>
                                <cn>1</cn>
                                <ssoSessionInfo>2</ssoSessionInfo>
                                <ssoRoleName>3</ssoRoleName>
                                <ssoRoleName>4</ssoRoleName>
                                <ssoRoleName>5</ssoRoleName>
                        </Attribute>
                </CSV>
        </Rule>
</Csv2Directory>
```

Executing the *irepmodifyent* command

Add entry data according to the association rules by executing the *irepmodifyent* command provided by Interstage Directory Service on the machine where the repository server is to be created.

After executing the *irepmodifyent* command, check whether the entry data has been added correctly (by extracting entry information, for example). Refer to 'Entry Management' in the Directory Service Operator's Guide for information about how to manipulate entries.

Example

Windows32/64

For the administrator DN and Bind password, specify the administrator DN and password for the administrator DN that were specified when the SSO repository was created.

In the example below, the port number for the SSO repository is 389, and the administrator DN is specified by "cn=manager,ou=interstage,o=fujitsu,dc=com".

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

Rule file: C:\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_roleset_mapping_rule.xml

CSV file: C:\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_roleset_mapping_add_en.csv

When prompted for the Bind password, enter the password for the administrator DN. Note that the password entered will not be displayed.

```
C:\>irepmodifyent -h localhost -p 389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -r C:
\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_roleset_mapping_rule.xml -i C:
\Interstage\F3FMsso\ssoatcsv\sample\OtherDirectory\ad\sample_ad_roleset_mapping_add_en.csv
Enter Bind password:
IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DIV.,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
IREP: INFO: irep13570: adding new entry cn=SALES DIV.,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
C:\>
```

Example

Solaris32/64 Linux32/64

For the administrator DN and Bind password, specify the administrator DN and password for the administrator DN that were specified when the SSO repository was created.

In the example below, the port number for the SSO repository is 389, and "cn=manager,ou=interstage,o=fujitsu,dc=com" has been specified for the administrator DN.

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

Rule file: /opt/FJSVssosv/sample/OtherDirectory/ad/sample_ad_roleset_mapping_rule.xml

CSV file: /opt/FJSVssosv/sample/OtherDirectory/ad/sample_ad_roleset_mapping_add_en.csv

When prompted for the Bind password, enter the password for the administrator DN. Note that the password entered will not be displayed.

```
# irepmodifyent -h localhost -p 389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -r /opt/
FJSVssosv/sample/OtherDirectory/ad/sample_ad_roleset_mapping_rule.xml -i /opt/FJSVssosv/sample/
OtherDirectory/ad/sample_ad_roleset_mapping_add_en.csv
Enter Bind password:
UX:IREP: INFO: irep13570: adding new entry cn=DEVELOPMENT DIV.,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
UX:IREP: INFO: irep13570: adding new entry cn=SALES DIV.,ou=Role,ou=SSO
ACI,ou=interstage,o=fujitsu,dc=com
#
```

Note

Take special care to protect the password for the administrator DN, and ensure security measures are in place to protect it. Refer to 'Security Measures' under 'Interstage Single Sign-on' in the 'Security Risks' section of the Security System Guide, for more information on protecting passwords.

F.1.4 Creating an Environment for SSL Communication

To use SSL for communications with Active Directory, an SSL environment must be created before the repository server is created.

The procedure for creating an SSL environment is as follows:

1. Create the Interstage Certificate Environment

   If it has not already been created, create the Interstage certificate environment required for using SSL communication with Active Directory. (*1)

2. Register a CA certificate for Active Directory

   Register the CA certificate that has been acquired from Active Directory with the Interstage certificate environment. (*2)

   Example

   Windows32/64

   CA certificate: C:\temp\ad-ca-cert.cer

   Nickname for the CA certificate: ADCACERT

   In this example, the CA certificate that has been acquired from Active Directory is "C:\temp\ad-ca-cert.cer". If necessary, change the file paths for each certificate.

   When prompted for a password, enter the password for accessing the Interstage certificate environment. Note that the password that is entered will not be displayed.

   ```
   C:\> scsenter -n ADCACERT -f C:\temp\ad-ca-cert.cer
   Password:
   Certificate was added to keystore
   SCS: INFO: scs0104: Certificate was imported
   C:\>
   ```

   Example

   Solaris32/64 Linux32/64

   CA certificate: /tmp/ad-ca-cert.cer

   Nickname for the CA certificate: ADCACERT

   In this example, the CA certificate that has been acquired from Active Directory is "/tmp/ad-ca-cert.cer". If necessary, change the file paths for each certificate.

   Before registering the certificate, set the JAVA_HOME environment variable to the installation path for the JDK or JRE.

   The following execution example uses a Bourne shell. When prompted for a password, enter the password for accessing the Interstage certificate environment. Note that the password that is entered will not be displayed.

   ```
   # JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
   # scsenter -n ADCACERT -f /tmp/ad-ca-cert.cer
   Password:
   ```

```
Certificate was added to keystore
UX: SCS: INFO: scs0104: Certificate was imported
#
```

3. Register a test certificate

   To use SSL for communications with Active Directory, create a test certificate (rather than CSR) using the *scsmakeenv* command, since the system only uses server authentication. (*3)

4. Create an SSL configuration

   Create an SSL configuration using the Interstage Management Console.

   To create an SSL configuration, select the [New] tab of the [SSL] window displayed by selecting [System] and then [Security] from the Interstage Management Console, and then make the settings under [General Settings]. Select the nickname for the site certificate specified when the test certificate was registered, and then create the SSL configuration by selecting the [Authenticate (Always authenticate a client certificate)] checkbox for [Client authentication].

*1 For details about creating the Interstage certificate environment, refer to "Creating the Interstage certificate environment".

*2 Refer to the Active Directory manuals for information about acquiring CA certificates for Active Directory.

*3 Refer to the Reference Manual (Command Edition) for information about the *scsmakeenv* command.

Note

If the [Authenticate (Always authenticate a client certificate)] checkbox for [client authentication] is not selected when the SSL configuration is created, then connections will be allowed unconditionally without verifying the CA certificates for Active Directory.

F.1.5 Creating a Repository Server

This section explains how to create a repository server for each system configuration.

Creating a repository server on a single machine

Create a repository server:

Refer to "Constructing a Repository Server (One Server or update System)".

Creating a repository server over multiple machines

Create a repository server (update system):

Create the repository server (update system) on the first machine.

Refer to "Constructing a Repository Server (One Server or update System)".

Add repository server (update system):

Export the environment for the first repository server (update system) and then import it as the environment for the other (load balancing) repository server (update system).

- Set up a load balancer:

  If session management is used, set up a load balancer.

  Refer to "Load distribution of the repository server (update system)" for information about the setting up a load balancer.

- Extract resources for the export machine:

  1. Extract repository server resources to a resource storage file by executing the ssobackup command with the "-sv" option on the export machine.

     Export resources for Interstage HTTP Server at the same time. (*1)

  2. If either the repository server or the Interstage Directory Service is using SSL for communication, export Interstage certificate environment resources as well. (*1)

3. Transfer the resources extracted in steps 1 and 2 to the import machine. Take care to avoid eavesdropping by third parties when transferring these resources.

   Also, do not change the access rights for the resource storage file that was extracted in step 1 when transferring it to the import machine.

- Import resources to the import machine, as follows:

  1. Import repository server resources by executing the *ssorestore* command on the import machine. No Interstage Management Console operations are required for the import machine after the resources have been imported.

     Import resources for Interstage HTTP Server at the same time. (*1)

  2. If either the repository server or the Interstage Directory Service is using SSL for communication, import the Interstage certificate environment resources that were extracted from the export machine as well. (*1)

Create a load balancing environment for the SSO repository:

Create a load balancing environment for the SSO repository to suit the operation. (*2)

Set up repository servers (update system):

Make the following settings on all of the repository servers (update system) that are subject to load balancing.

1. Select [System] > [Security] > [Single Sign-on] > [Authentication Infrastructure] > [Repository Server] from the Interstage Management Console, and then click [Repository server detailed settings [Show]] in the [Settings] tab. Make sure that the SSO repository that was created above has been set as the [Repository Name], and then click [Update].

2. Start the repository server.

   Refer to "Starting a Repository Server" for information about how to start the repository server.

3. Delete the resource storage file that was extracted from the export machine.

Creating the repository server and the authentication server on the same machine

Create a repository server and an authentication server

Create a repository server and an authentication server on the same machine.

Refer to "Setting up a Repository Server and Authentication Server on a Single Machine".

*1 For information on exporting and importing resources, refer to 'Moving Resources to Another Server' under 'Maintenance (Resource Backup)' in the Operator's Guide.

*2 For information on creating a load balancing environment for the SSO repository, refer to 'Creating a Load Distribution Environment' or 'Creating a Load Distribution Environment (Replication Mode)' in the Directory Service Operator's Guide.

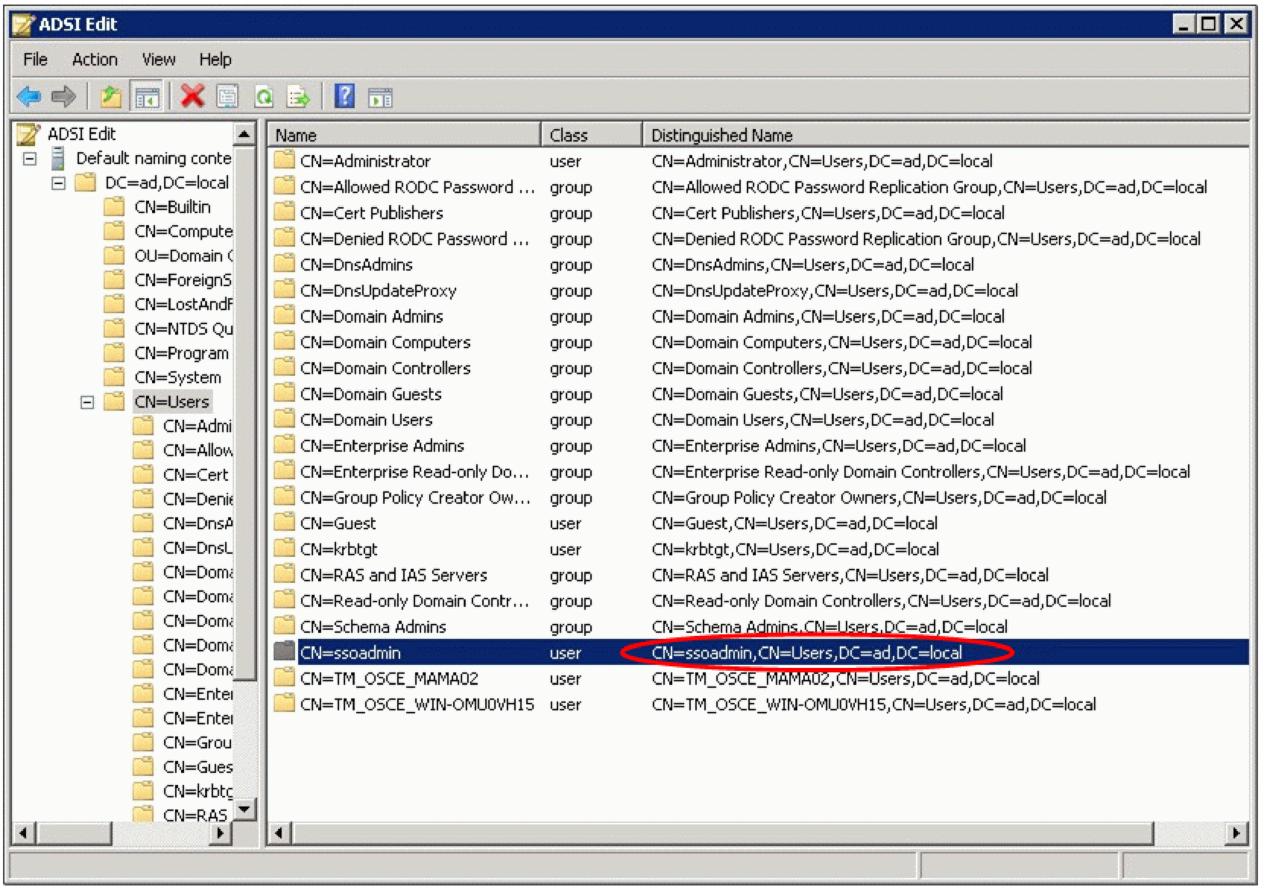
Note

The following information, which is set up in the [Active Directory Settings], can be checked using the ADSI Edit tool provided by Microsoft. The ADSI Edit tool is stored on the Windows installation media.

- [connection DN]

  To connect using the "ssoadmin" user account, open the ADSI Edit tool window and specify "CN=ssoadmin, CN=Users, DC=ad, DC=local", which has been set as the Distinguished Name for "CN=ssoadmin", as shown below.

For the password for the connection DN, specify the password for the "ssoadmin" user account.

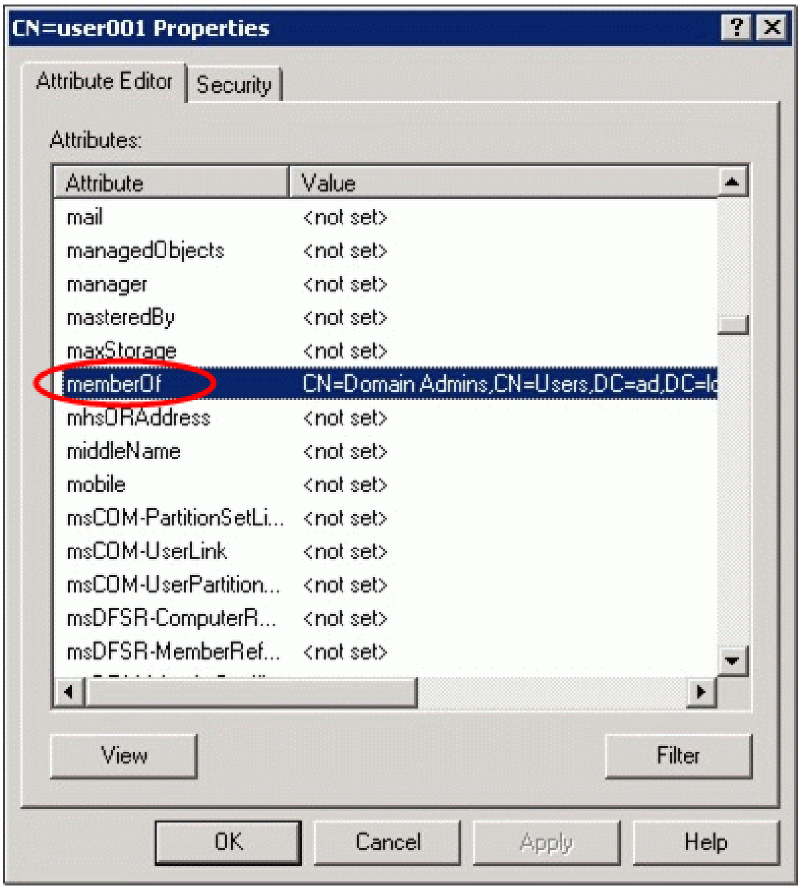


Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=ad,DC=local
CN=Allowed RODC Password ...	group	CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=local
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=ad,DC=local
CN=Denied RODC Password ...	group	CN=Denied RODC Password Replication Group,CN=Users,DC=ad,DC=local
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=ad,DC=local
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=ad,DC=local
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=ad,DC=local
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=ad,DC=local
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=ad,DC=local
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=ad,DC=local
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=ad,DC=local
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=ad,DC=local
CN=Enterprise Read-only Do...	group	CN=Enterprise Read-only Domain Controllers,CN=Users,DC=ad,DC=local
CN=Group Policy Creator Ow...	group	CN=Group Policy Creator Owners,CN=Users,DC=ad,DC=local
CN=Guest	user	CN=Guest,CN=Users,DC=ad,DC=local
CN=krbtgt	user	CN=krbtgt,CN=Users,DC=ad,DC=local
CN=RAS and IAS Servers	group	CN=RAS and IAS Servers,CN=Users,DC=ad,DC=local
CN=Read-only Domain Contr...	group	CN=Read-only Domain Controllers,CN=Users,DC=ad,DC=local
CN=Schema Admins	group	CN=Schema Admins,CN=Users,DC=ad,DC=local
CN=ssoadmin	user	CN=ssoadmin,CN=Users,DC=ad,DC=local
CN=TM_OSCE_MAMA02	user	CN=TM_OSCE_MAMA02,CN=Users,DC=ad,DC=local
CN=TM_OSCE_WIN-OMU0VH15	user	CN=TM_OSCE_WIN-OMU0VH15,CN=Users,DC=ad,DC=local

- [Attribute name to use for a role]

  If an extended schema for Single Sign-on is not used, open the window for the ADSI Edit tool as shown below, and then specify the "Attribute" attribute name included in the user information for Active Directory.

To register the values of groups (to which the users managed by Active Directory belong) as a role configuration, specify a "memberOf" attribute.



Attribute	Value
mail	<not set>
managedObjects	<not set>
manager	<not set>
masteredBy	<not set>
maxStorage	<not set>
memberOf	CN=Domain Admins,CN=Users,DC=ad,DC=lo
mhsORAddress	<not set>
middleName	<not set>
mobile	<not set>
msCOM-PartitionSetLi...	<not set>
msCOM-UserLink	<not set>
msCOM-UserPartition...	<not set>
msDFSR-ComputerR...	<not set>
msDFSR-MemberRef...	<not set>

F.1.6 Configure Integrated Windows Authentication

Configure settings using the following procedure:

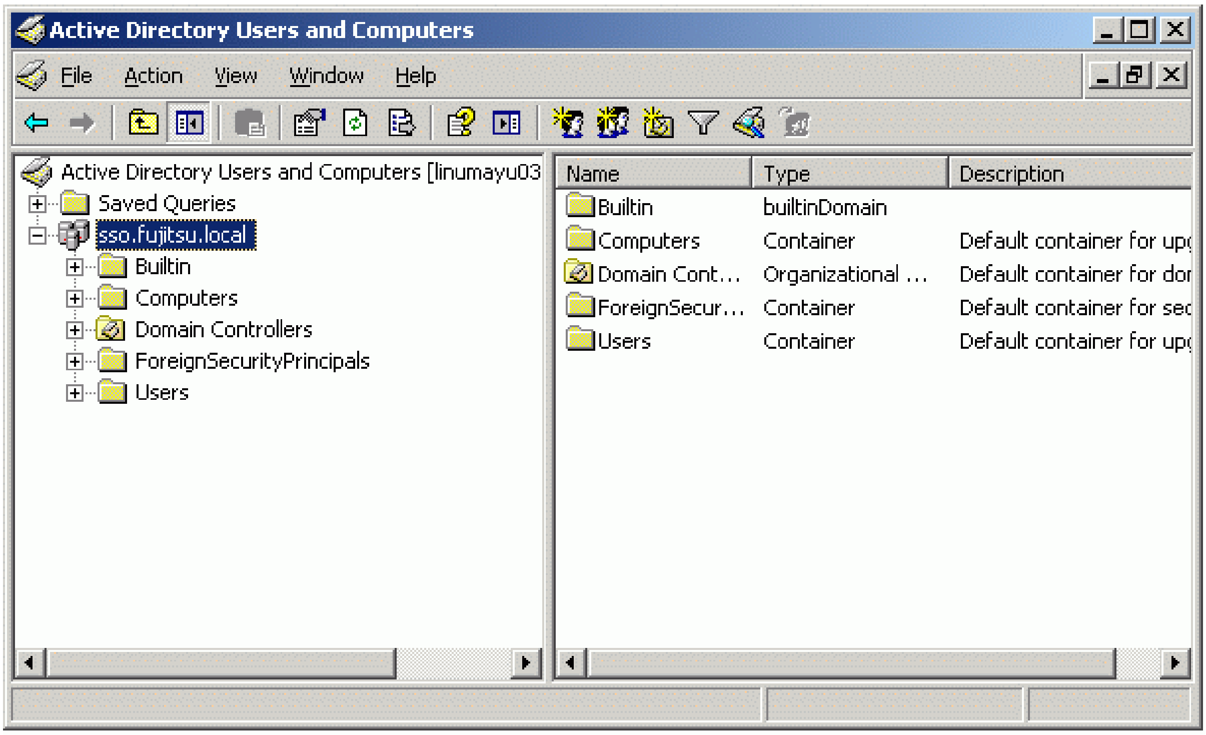
1. Active Directory Setup
2. Integrated Windows Authentication Application Deployment
3. WorkUnit Start User Setup
4. Web Browser Setup

Active Directory Setup

Perform the following tasks on the machine used to run Active Directory.

(1) Register the authentication server in Active Directory

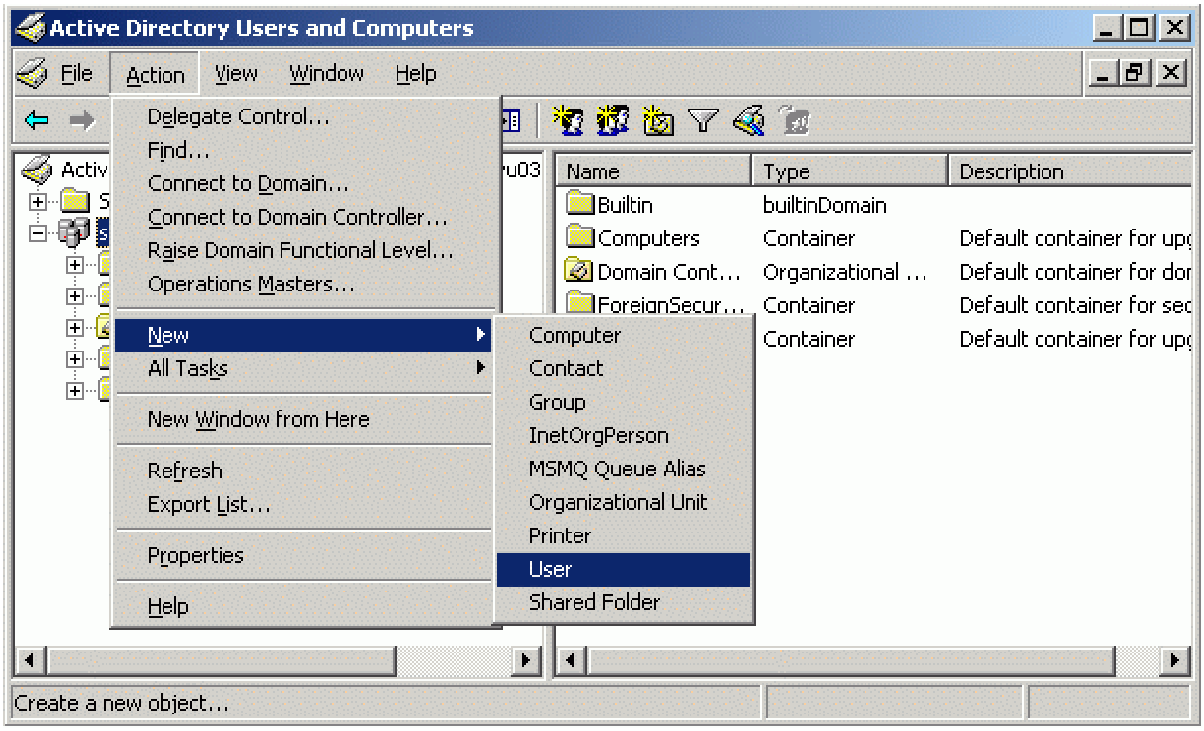
1. In the [Start] menu, click [Programs] - [Administrative Tools], and then click [Active Directory Users and Computers].


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers [linumayu03
Saved Queries
sso.fujitsu.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upg
Domain Cont…	Organizational …	Default container for dor
ForeignSecur…	Container	Default container for sec
Users	Container	Default container for upg

2. Select the domain name, and then select [Action] - [New] - [User].

Do not select [Computer].

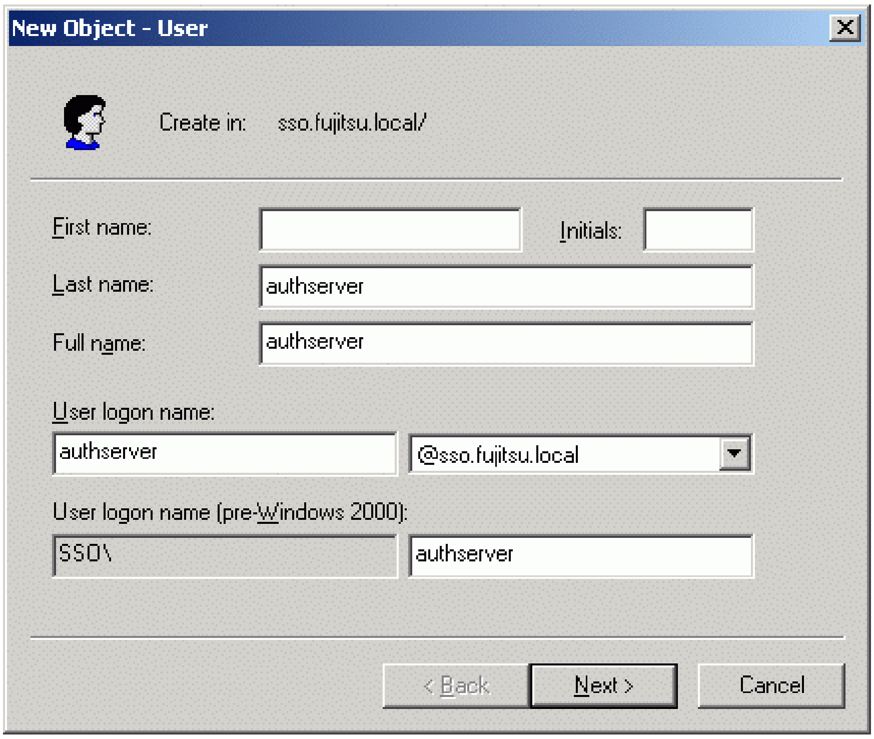


Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upg
Domain Cont…	Organizational …	Default container for dor
ForeignSecur…	Container	Default container for sec
	Container	Default container for upg

3. Enter the authentication server host name in the Last name and User logon name fields.

If the load balancer is used for authentication server load balancing, enter the load balancer host name.

In the following example, the name used is "authserver".


New Object - User

Create in: sso.fujitsu.local/

First name:

Initials:

Last name: authserver

Full name: authserver

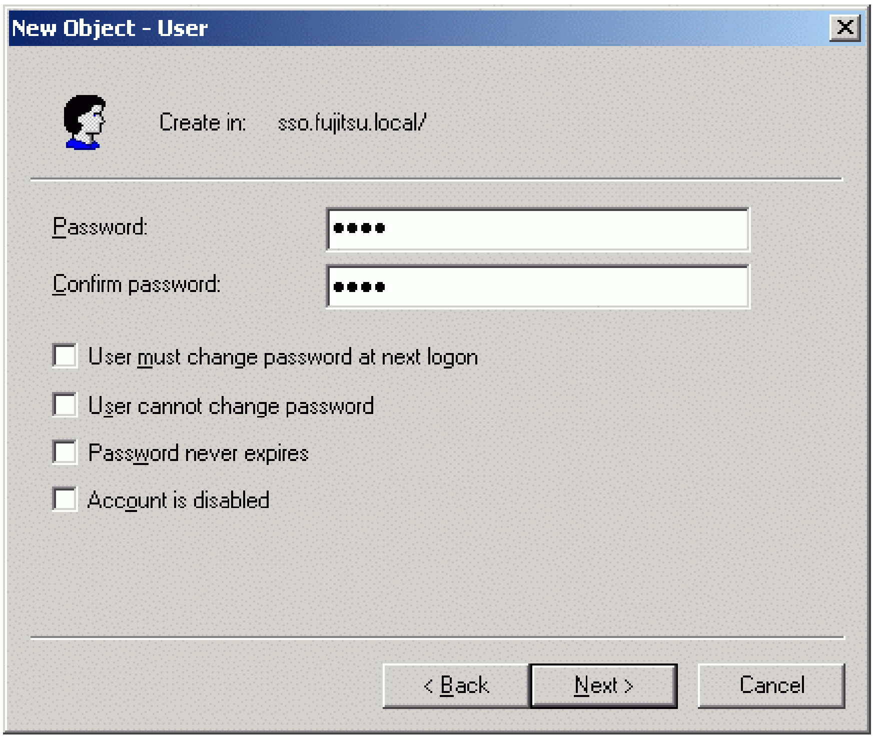
User logon name: authserver @sso.fujitsu.local

User logon name (pre-Windows 2000): SSO\ authserver

4. Click [Next], and enter the password set for the authentication server account entered in Step 3 above.

   Do not select "User must change password at next logon".

   Do not forget that the password that is set here will be required in future.


New Object - User

Create in: sso.fujitsu.local/

Password: ●●●●

Confirm password: ●●●●

□ User must change password at next logon

□ User cannot change password

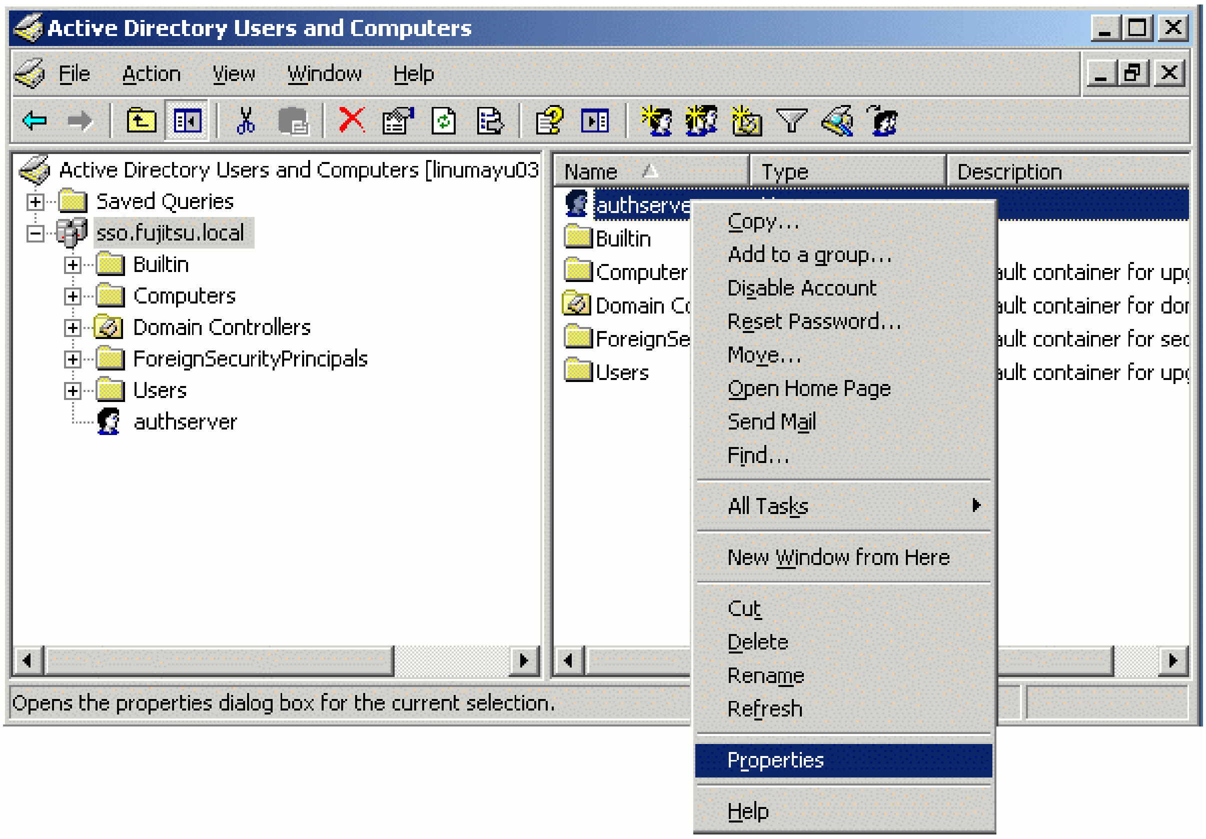
□ Password never expires

□ Account is disabled

5. Click [Next], and then click [Finish].

   Creation of the authentication server account is complete.

6. Right click on the user that was created, and then click [Properties].



7. Click the [Account] tab, and from [Account options], select the following items according to the encryption cipher used (*1):

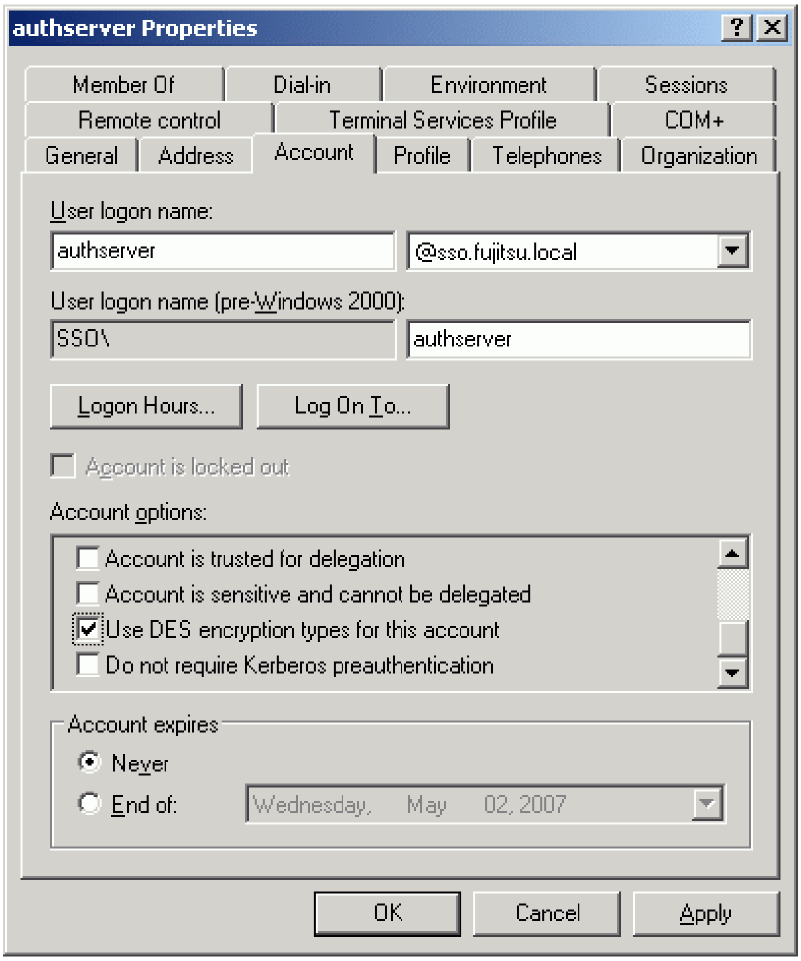
Encryption cipher used in Integrated Windows Authentication	Name of [Account options] item
AES128-CTS-HMAC-SHA1-96	This account supports Kerberos AES 128 bit encryption
RC4-HMAC	None (selection not required)
DES-CBC-CRC	If Windows Server(R) 2003 is used, "Use DES encryption types for this account". If Windows Server(R) 2008 is used (*2), "Use Kerberos DES encryption types for this account".

*1 For details on which encryption ciphers are used with Integrated Windows Authentication, refer to. "Encryption ciphers used in Integrated Windows Authentication"

*2 Except Windows Server(R) 2008 R2.

Windows Server(R) 2003 window

If "DES-CBC-CRC" is selected as the encryption cipher used in Integrated Windows Authentication:



User logon name:
authserver @sso.fujitsu.local

User logon name (pre-Windows 2000):
SSO\ authserver

□ Account is locked out

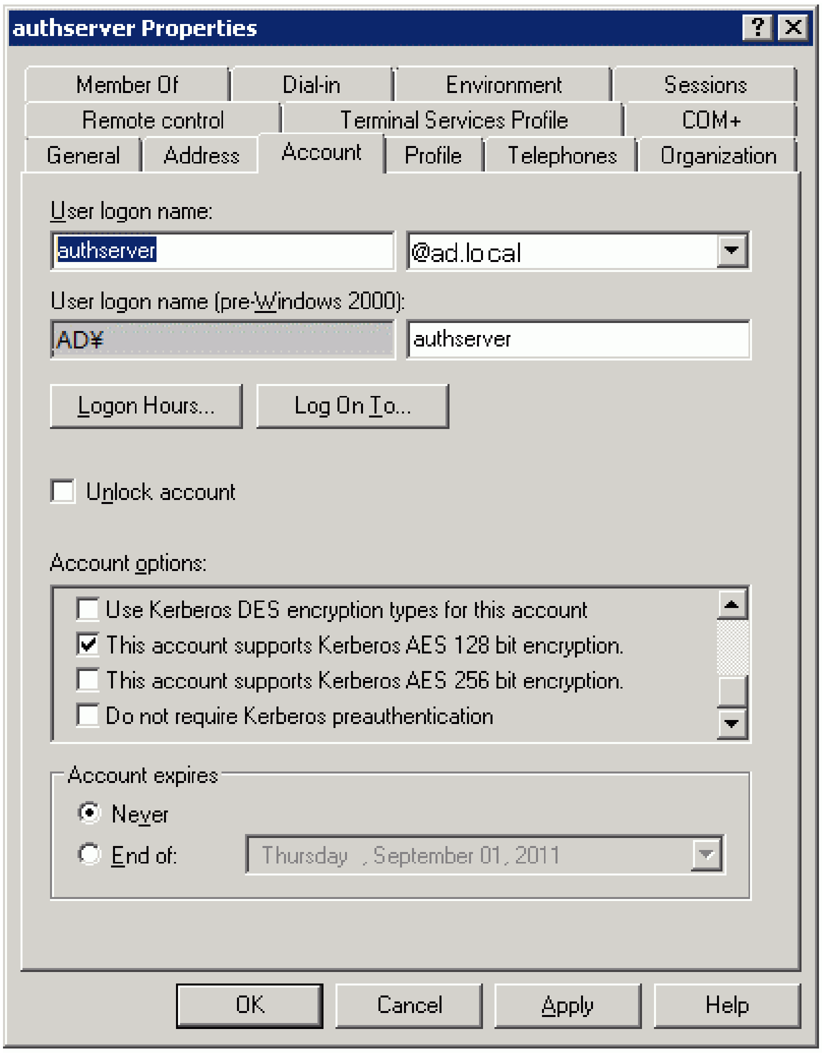
Account options:

□ Account is trusted for delegation
□ Account is sensitive and cannot be delegated
☑ Use DES encryption types for this account
□ Do not require Kerberos preauthentication

Account expires
● Never
○ End of: Wednesday, May 02, 2007

Windows Server(R) 2008 window

If "AES128-CTS-HMAC-SHA1-96" is selected as the encryption cipher used in Integrated Windows Authentication:



User logon name: authserver @ad.local

User logon name (pre-Windows 2000): AD¥ authserver

□ Unlock account

Account options:

□ Use Kerberos DES encryption types for this account

☑ This account supports Kerberos AES 128 bit encryption.

□ This account supports Kerberos AES 256 bit encryption.

□ Do not require Kerberos preauthentication

Account expires

● Never

○ End of: Thursday , September 01, 2011

Note

Multiple items should not be selected at the same time in [Account options]. Additionally, when RC4-HMAC is used, check that items have not been selected unnecessarily.

8. Click [OK].

(2) Assign the service principal name to the authentication server

Execute ktpass.exe in the command prompt, specifying the following for each option: (*1)

-princ :Authentication infrastructure URL FQDN, and Active Directory Kerberos domain (using the "host/ *<authentication_URL_FQDN>@<Active_Dir_Kerberos_domain>*" format)

-pass : Password for the account created in step 1

-mapuser: Account created in step 1

-ptype : Principal type (the literal "KRB5_NT_PRINCIPAL" must be specified)

-crypto : Encryption method

-out : Full path to the keytab file created

*1 If ktpass.exe does not exist, install Windows Support Tools from the Windows installation media. Note that, if Service Pack is applied in the operating system, download from the Microsoft(R) website the Windows Support Tools corresponding to the Service Pack, and then install it

Specify the following for the encryption cipher:

Encryption cipher used in Integrated Windows Authentication (*1)(*2)	Encryption cipher specified in ktpass.exe
AES128-CTS-HMAC-SHA1-96	AES128-SHA1
RC4-HMAC	RC4-HMAC-NT (*3)
DES-CBC-CRC	DES-CBC-CRC

*1 For details on which encryption ciphers are used with Integrated Windows Authentication, refer to "Overview" - "Authentication" - "Integrated Windows Authentication" in the "Single Sign-on Operator's Guide".

*2 The encryption cipher used in Integrated Windows Authentication should match step 1.

*3 Service Pack 1 or later Support Tools must be installed if using Microsoft(R) Windows Server(R) 2003 (except R2).

Example

An example of executing in Microsoft(R) Windows Server(R) 2003 R2 is shown below.

Authentication infrastructure URL FQDN : authserver.fujitsu.com

Active Directory Kerberos domain: AD.LOCAL

Password for the account : authpass01

Account : authserver

Principal type : KRB5_NT_PRINCIPAL

Encryption method : RC4-HMAC

Full path of the keytab file : C: \Temp\sso-winauth.keytab

```
C:\>ktpass -princ host/authserver.fujitsu.com@AD.LOCAL -pass authpass01 -mapuser authserver -ptype
KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT -out C:\Temp\sso-winauth.keytab
Targeting domain controller: ADserver.ad.local
Using legacy password setting method
Successfully mapped host/authserver.fujitsu.com to authserver.
Key created.
Output keytab to C:\Temp\sso-winauth.keytab:
Keytab version: 0x502
keysize 94 host/authserver.fujitsu.com@AD.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-
HMAC) keylength 16 (0x0fd4babdb68dfe59421fb690b0485bbf)
```

(3) Transfer the keytab file

Transfer the keytab file created in step 2 to the machine used for running the authentication server. After the transfer is complete, delete the keytab file from the machine used for running Active Directory.

Integrated Windows Authentication Application Deployment

In the machine used for running the authentication server, the Integrated Windows Authentication application is deployed to the servlet container as a servlet application. To deploy the application, specify the winauth subcommand in the ssodeploy command.

After the deployment is complete, delete the transferred keytab file.

If Integrated Windows Authentication is used in a system in which authentication server load balancing has already been performed, deploy the Integrated Windows Authentication application in all authentication servers for which the load has been balanced.

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

Note

After executing the ssodeploy command, check the message that was output, and take action if the output contents shown in the table below are incorrect.

Contents that are output	Action
FQDN of SSO Authentication server	Delete the authentication server account registered in Active Directory, and reconfigure the Active Directory settings.

Contents that are output	Action
Kerberos domain area	
Host name of Active Directory	The name of the machine used for running Active Directory that was specified in the "kdc" argument of the ssodeploy command is incorrect. Specify the correct machine name.

Example

Windows32/64

Name of the machine used for running Active Directory: ADserver.fujitsu.com

Full path name of the keytab file : C:\Temp\sso-winauth.keytab

Name of new IJServer : SSO_WINDOWS_AUTH

A confirmation message asking if you want to deploy the Integrated Windows Authentication application is displayed, so enter "yes".

```
C:\>ssodeploy winauth ADserver.fujitsu.com C:\Temp\sso-winauth.keytab
[Deployment information]
 FQDN of SSO Authentication server :  authserver.fujitsu.com
 Host name of Active Directory :  ADserver.fujitsu.com
 Kerberos domain area :  AD.LOCAL
 IJServer name :  SSO_WINDOWS_AUTH
 Application name :  winauth
Are you sure you want to deploy the Integrated Windows Authentication application? (yes/no) yes

isj2eeadmin ijserver -a -f "C: \Interstage\F3FMsso\ssoatcag\webapps\winauth\WEB-INF\ijserver.xml"
isj2eeadmin: INFO: isj2ee2100:IJServer has been registered.  NAME=SSO_WINDOWS_AUTH

ijsdeployment -n SSO_WINDOWS_AUTH -d "C: \Interstage\F3FMsso\ssoatcag\webapps\winauth"
DEPLOY: INFO: DEP5050:Deployment processing has been completed.  File name=C:\Interstage\F3FMsso
\ssoatcag\webapps\winauth
```

Solaris32/64 Linux32/64

Name of the machine used for running Active Directory: ADserver.fujitsu.com

Full path name of the keytab file: /tmp/authserver.keytab

Name of new IJServer: SSO_WINDOWS_AUTH

Before executing the ssodeploy command, set the JDK or JRE installation path in environment variable JAVA_HOME

A confirmation message asking you if you want to deploy the Integrated Windows Authentication application is displayed, so enter "yes".

```
#JAVA_HOME=/opt/FJSVawjbk/jdk6;export JAVA_HOME
#/opt/FJSVssoac/bin/ssodeploy winauth ADserver.fujitsu.com /tmp/authserver.keytab
[Deployment information]
 FQDN of SSO Authentication server :  authserver.fujitsu.com
 Host name of Active Directory :  ADserver.fujitsu.com
 Kerberos domain area :  AD.LOCAL
 IJServer name :  SSO_WINDOWS_AUTH
 Application name :  winauth
Are you sure you want to deploy the Integrated Windows Authentication application? (yes/no) yes

isj2eeadmin ijserver -a -f /etc/opt/FJSVssoac/webapps/winauth/WEB-INF/ijserver.xml
UX:isj2eeadmin: INFO: isj2ee2100:IJServer has been registered.  NAME=SSO_WINDOWS_AUTH

ijsdeployment -n SSO_WINDOWS_AUTH -d /etc/opt/FJSVssoac/webapps/winauth
UX:DEPLOY: INFO: DEP5050:Deployment processing has been completed.  File name=/etc/opt/FJSVssoac/
webapps/winauth
```

WorkUnit Start User Setup

Solaris32/64 Linux32/64

If an Integrated Windows Authentication application is deployed, the administrator user is set for the WorkUnit start user name.

Change the name of the active user of the WorkUnit in line with the authority of the effective user or the effective group of the Web server that the authentication server is using.

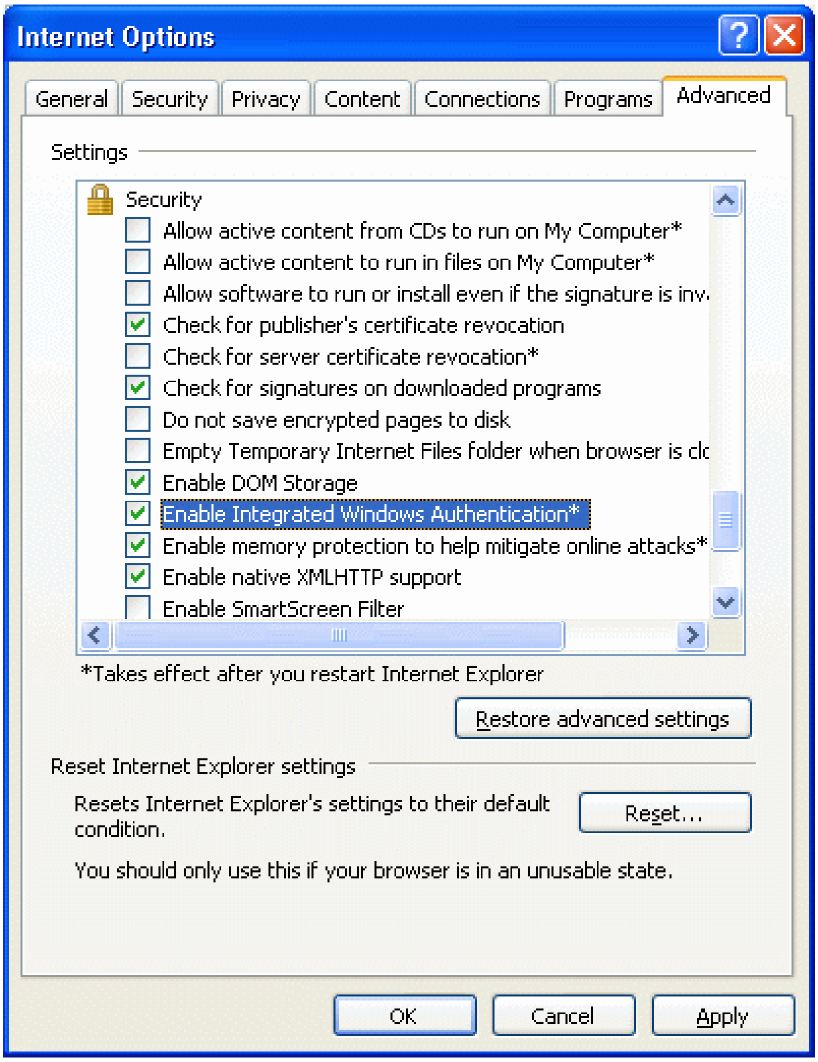
For details about the WorkUnit start user, refer to "Starting an Authentication Server" - "WorkUnit start user" in "Operation and Maintenance".

Web Browser Setup

Configure the Web browser settings.

In the following example, Windows(R) Internet Explorer is used.

1. Click [Tools] - [Internet Options] - [Advanced], and select "Enable Integrated Windows Authentication".



Settings

Security

☐ Allow active content from CDs to run on My Computer*
☐ Allow active content to run in files on My Computer*
☐ Allow software to run or install even if the signature is inv
☑ Check for publisher's certificate revocation
☐ Check for server certificate revocation*
☑ Check for signatures on downloaded programs
☐ Do not save encrypted pages to disk
☐ Empty Temporary Internet Files folder when browser is clo
☑ Enable DOM Storage
☑ Enable Integrated Windows Authentication*
☑ Enable memory protection to help mitigate online attacks*
☑ Enable native XMLHTTP support
☐ Enable SmartScreen Filter

*Takes effect after you restart Internet Explorer

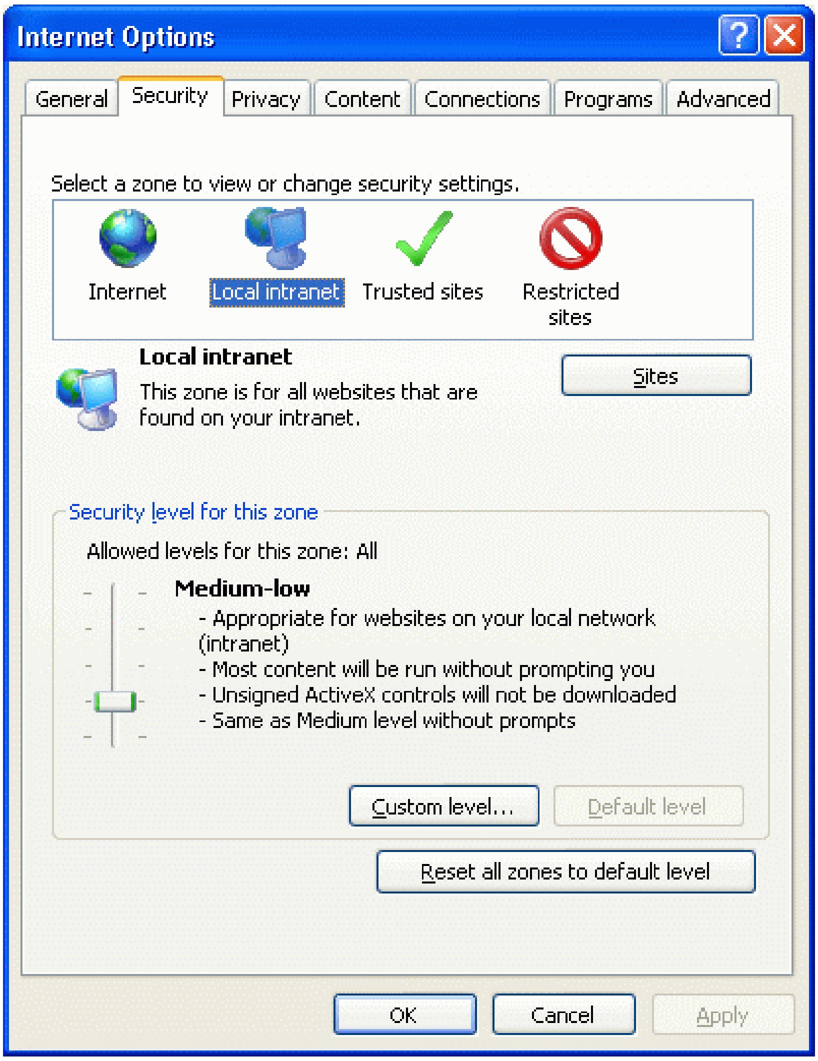
Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

2. Click the [Security] tab, and then click [Local intranet].

   Click [Sites].



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

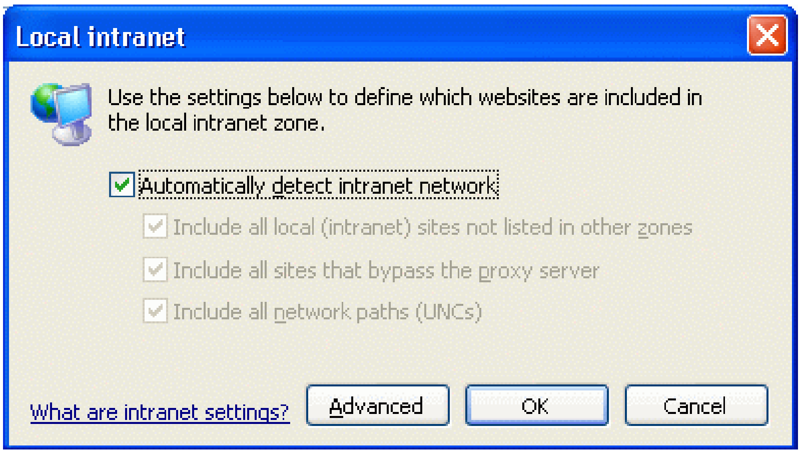
Security level for this zone

Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

3. If the following window is displayed, click on the [Advanced...] button. If this window is not displayed, go to the next step.



Use the settings below to define which websites are included in the local intranet zone.

☑ Automatically detect intranet network

☑ Include all local (intranet) sites not listed in other zones

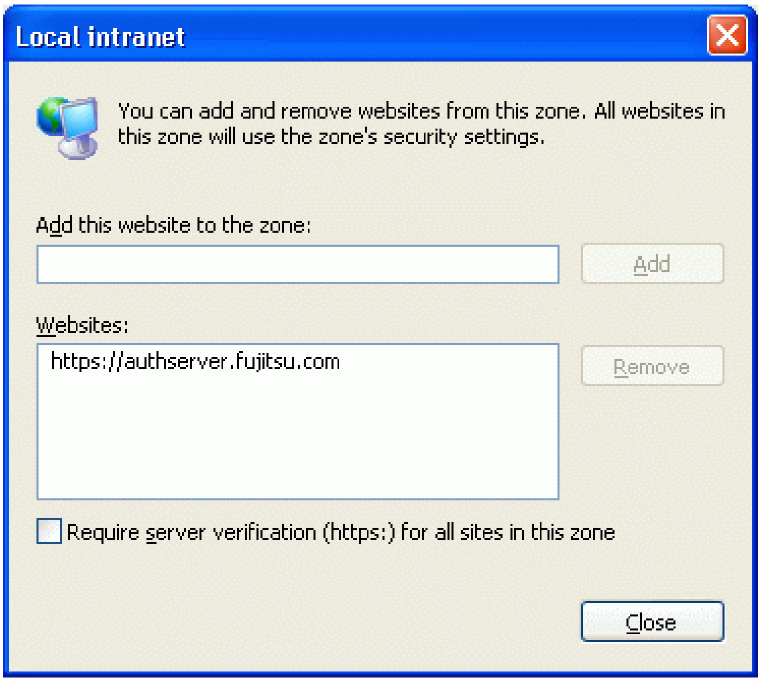
☑ Include all sites that bypass the proxy server

☑ Include all network paths (UNCs)

4. Add the authentication infrastructure URL to the Web site.

   In the following example, https://authserver.fujitsu.com is added to the Web site.

After the Web site has been added, click [Close].



Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

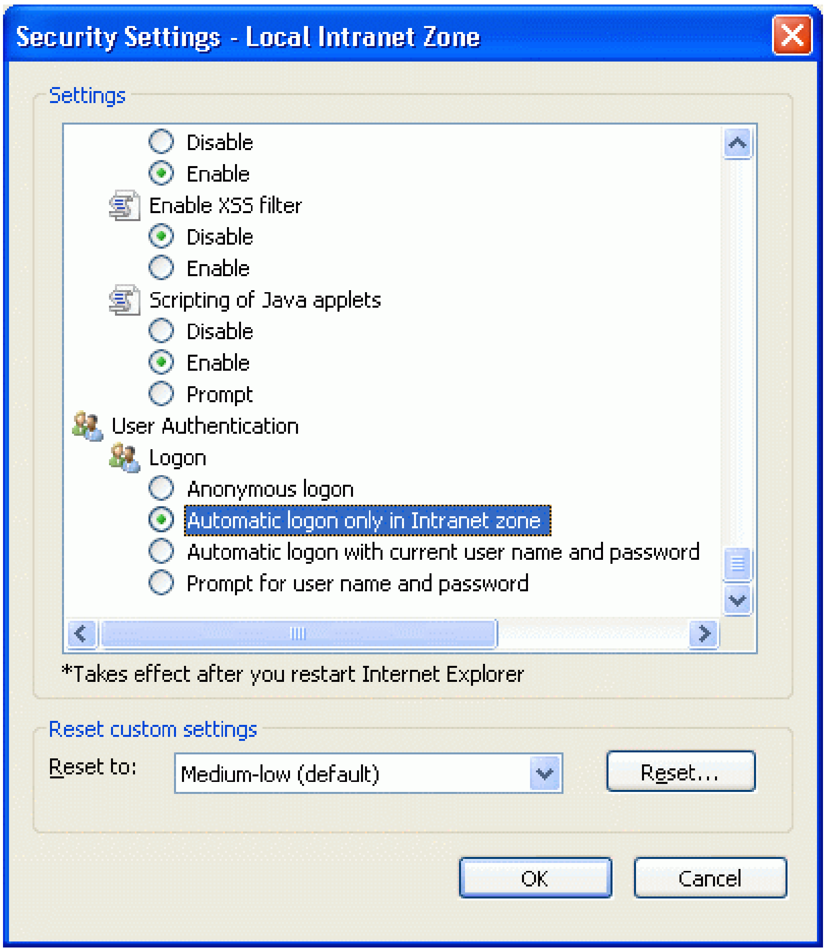
Add this website to the zone:

Websites:
https://authserver.fujitsu.com

□ Require server verification (https:) for all sites in this zone

5. If a window was displayed in step 3, click the [OK] button to return to the window in step 2. If this window is not displayed, go to the next step.

6. Click [Custom Level], and in [User Authentication] - [Logon] select "Automatic logon only in Intranet zone".



Security Settings - Local Intranet Zone

Settings

○ Disable
● Enable
Enable XSS filter
● Disable
○ Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
● Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
○ Prompt for user name and password

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-low (default)

7. Click [OK].

F.2 Using Interstage Directory Service as the Directory Service for Registering User Information

After setting up the authentication server, the following must be performed:

1. SSO Repository Setup (making associations for user information)
2. Configure Integrated Windows Authentication
    1. Active Directory Setup
    2. Integrated Windows Authentication Application Deployment
    3. WorkUnit Start User Setup
    4. Web Browser Setup

F.2.1 SSO Repository Setup (Making Associations for User Information)

Associate users managed in the SSO repository and users registered in Active Directory.

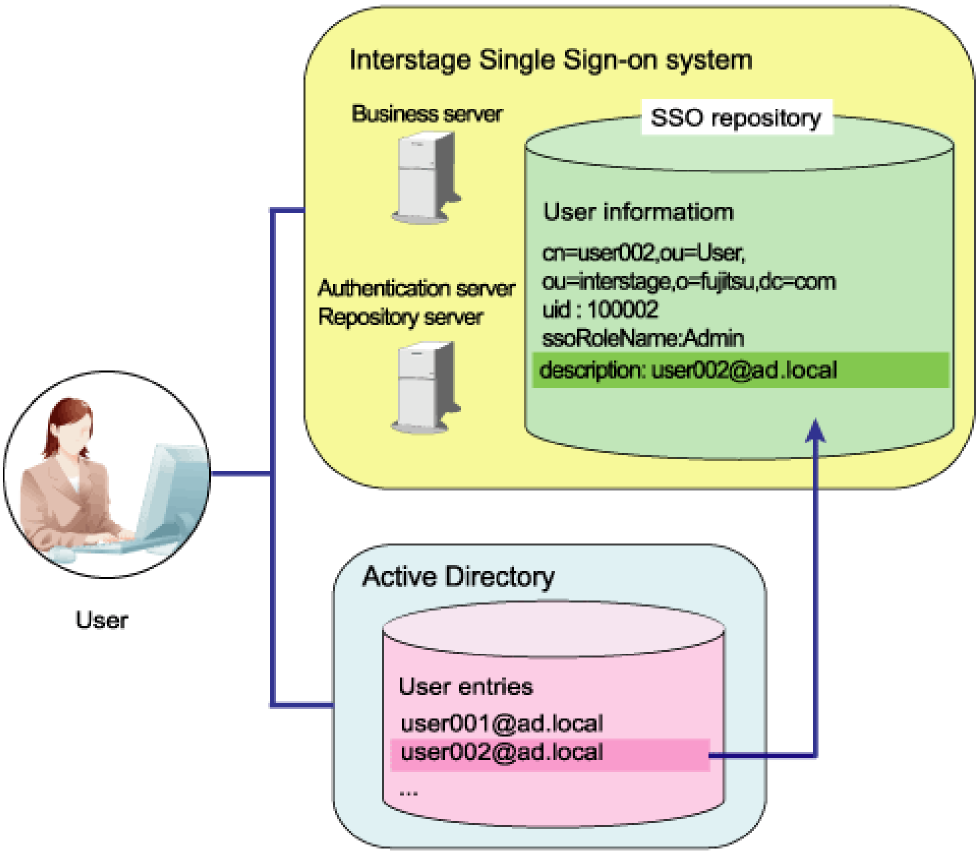
The [user logon name] value for the user entry registered in Active Directory can be registered as any attribute value for the user information managed in the SSO repository using the *ldapmodify* command.

There is no need for the user ID managed in the SSO repository and the user logon name registered in Active Directory to match.

Specify the attribute name used to register the user logon name in "SSO Repository Settings" in [Integrated Windows Authentication Setting] > [Attribute used for authentication] using the Interstage Management Console of the authentication server.

In the following example, the user logon name "user002@ad.local" that is registered in Active Directory is registered as the "description" attribute in the SSO repository.

Example



Appendix G Settings for Performing Certificate Authentication in a System that Performs Session Management

This appendix explains the environment configuration settings to enable Certificate Authentication in the system that is performing Session Management.

To perform certificate authentication in a system that performs session management, settings to allow certification authentication must be configured in the authentication server environment configuration file.

Notes

- When certificate authentication is performed in a system that performs session management, continued use of a service is possible without having to re-authenticate, even when the functions shown below are used. Provide the user with sufficient instruction in order to reduce the threat of interference by a third party while a user is away from his or her desk.
  - The following functions can be disabled:
    - - Idle surveillance
    - - Sign-off
    - - Forced Sign-off
  - User instruction
    - - Use protection functionality such as a screen saver password so that idle monitoring is performed.
    - - Be sure to close the Web browser when signing off.
    - - Use the certificate stored in the IC card, instead of registering the certificate in the Web browser.
- The settings for performing certificate authentication in a system that performs session management can only be configured by editing the environment configuration file directly. As with individual server environment configurations in the normal Single Sign-on system, the Interstage Management Console cannot be used to configure these settings.

Work Procedure

Update the authentication server environment configuration file according to the following procedure:

1. Stop the Authentication server.
2. Change the Authentication server environment configuration file.
3. Start the Authentication server.

For details on how to start and stop the authentication server, refer to 'Starting an Authentication Server' and 'Stopping an Authentication Server' in "Operation and Maintenance".

Changing the Authentication Server Environment Configuration File

Set the item shown in the table in the environment configuration file that is stored on the authentication server by using a text editor.

Notes

- Do not edit options that are not shown in the table below. If these options are edited, it may not be possible to operate the Authentication server correctly.
- Set the item in the environment configuration file by using the "configuration name=value that is set" format. Start from the beginning of the line. There must not be a space either before or after "=".

File Name and File Path of the Authentication Server Configuration File

Configuration file name:

ssoatcag.conf

Configuration file path (directory)

Windows32/64

```
C:\Interstage\F3FMsso\ssoatcag\conf
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoac/conf
```

Configuration Items to Add

Table G.1 Configuration Items to Add

Item	Configuration Name	Setting Contents	Omissible or Required
Allowing certificate authentication in a system that performs session management	allow-sm-cert-auth	Select whether to allow certificate authentication in a Single Sign-on system that performs session management. YES: Certificate authentication is allowed NO: Certificate authentication is not allowed Omitting this setting is the same as specifying "NO". If values other than those above are set, sso02040 is output to system log, and "NO" is considered to have been set.	Omissible.

The following example shows how to set a configuration file.

Example

In the example, the performing of certificate authentication is allowed in a Single Sign-on system that performs session management.

```
allow-sm-cert-auth=YES
```

Appendix H Prevention of Caching of Contents

In Interstage Single Sign-on, for security reasons the use of the cache in the Web browser is prevented so that contents that are set as protection resources do not remain in the user PC.

To prevent use of the Web browser cache, the "Cache-Control" and "Pragma" headers for cache control are set in the HTTP response header.

However, if the Web browser cache is disabled in Windows(R) Internet Explorer(R), file download may fail in the contents that perform the file download.

To create the contents that perform the file download, the settings that the use of the Web browser cache is enabled must be configured.

Configure the settings so that the use of the Web browser cache is enabled according to the following procedure:

Windows32/64

1. Stop the Business server.
2. Change the Business server environment configuration file.
3. Start the Business server.

Solaris32/64 Linux32/64

1. Stop all Business servers built on the same machine.
2. Change the Business server configuration file.
3. Start the Business servers built on the same machine.

For details on how to start and stop the Business server, refer to "Starting a Business Server" and 'Stopping a Business Server' in "Operation and Maintenance".

Note

If configuring the settings so that the use of the Web browser cache is not prevented, consider to the security implications as mentioned above by, for example, preventing the use of the cache in the Web application.

Changing the Authentication Server Environment Configuration File

Use a text editor to set the item shown in the table in the environment configuration file that is stored on the business server.

Notes

- Do not edit options that are not shown in the table below. If these options are edited, it may not be possible to operate the Business server correctly.
- Set the item in the environment configuration file by using the "configuration name=value that is set" format. Start from the beginning of the line. There must not be a space either before or after "=".
- If more than one business server is set up in one machine, more than one business server configuration is set in the environment configuration file. Edit the target business server configuration based on the settings example below.

File Name and File Path of the Authentication Server Configuration File

Configuration file name:

ssoatzag.conf

Configuration file path (directory)

Windows32/64

```
C:\Interstage\F3FMsso\ssoatzag\conf
```

Solaris32/64 Linux32/64

```
/etc/opt/FJSVssoaz/conf
```

Configuration Items to Add

Table H.1 Configuration Items to Add

Item	Configuration Name	Setting Contents	Omissible or Required
Web browser cache control	http-cache-cntl	Select whether the contents that are set as protection resources are cached in the Web browser. YES: They are not cached NO: They are cached If "YES" is set, the following values are set in the HTTP response header, and Web browser cache is prevented. Cache-Control:no-cache,no-store Pragma:no-cache Omitting this setting is the same as specifying "YES". If values other than those above are set, sso03006 is output to system log, and "YES" is considered to have been set.	Omissible.

The following example shows how to set a configuration file.

Example

In the example, two business servers, with business system names "Business001" and "Business002", are set up in one machine (*1). The environment configuration file settings are shown in the example.

To configure the settings so that the contents set as protection resources are cached in the Web browser for the business server that has business system name "Business001", search for the line in which **"Business001"** is set in business-system-name, and then add **"http-cache-cntl=NO"** to the next line.

```
ServerPort=80
FQDN=http://sso.fujitsu.co.jp:80
   ~ Omitted ~
business-system-name=Business001
http-cache-cntl=NO
   ~ Omitted ~

ServerPort=81
FQDN=http://sso.fujitsu.co.jp:81
   ~ Omitted ~
business-system-name=Business002
   ~ Omitted ~
```

*1 The business system name can be checked by clicking the [System] > [Security] > [Single Sign-on] > [Business system] > [List] tabs in the Interstage Management Console.

Appendix I Settings for Protection Resource in Authentication Server

The environment definitions required for setting protection resource information in the authentication server are described below.

To reject authentication requests from non-protection resources in Business systems, in the authentication server environment definition file, you must set the site configuration of the business system and the protection path information registered in the SSO repository.

Update the Authentication server environment definition file by performing the following steps:

1. Stop the Authentication server.
2. Change the Authentication server environment definition file.
3. Start the Authentication server.

For details on how to start and stop the authentication server, refer to "Starting an Authentication Server" and 'Stopping an Authentication Server' in "Operation and Maintenance".

Notes

- The environment definition for rejecting authentication requests from non-protection resources in Business systems can only be set by editing the environment definition file directly. It cannot be edited using Interstage Management Console.
- If session management is used, there is no need to make these settings.

Notes on Setting the Environment Definition File

Note the following points about setting the environment definition file:

- The error messages output when invalid settings are configured are registered in the system log. At this time, the same message may be recorded in the system log more than once.
- Set the configuration file items using the "<configuration name>=<set value>" form from the head of line. Do not include blanks in front of or behind "=".
- If the configuration item does not allow multiple lines, when multiple lines are entered only the top line is valid, and other lines will be ignored.
- Set the items of configuration file without unnecessary blanks.

  For example, "<configuration name>=123 " (with a blank behind 123) and "<configuration name>= NO" (with a blank in front of NO) are incorrect. Such entries will be ignored.
- If an option that does not exist (is invalid) is set in the environment definition file, it is ignored.
- If more than one option is set, use commas (,) to separate them.
- Lines starting with "#" are regarded as comment lines.

Example

The following example shows a configuration file which includes invalid settings.

```
Repository-port= 389
#repository-bind-dn=cn=admin
repository-user-search-base=ou=User,o=Interstage,c=jp
repository-user-search-base=ou=User1,o=Interstage,c=jp
accesslog-save-all=NO
repository-role-search-base=
```

- In line 1, there is a space after "=" for "repository-port". For this reason, this setting is treated as " 389".
- In line 2, there is a "#" at the start". The line is treated as a comment.
- "repository-user-search-base" is described in both lines 3 and 4. If the same definition is set more than once, the first settings (in this case, in line 3) are valid, and all other settings (in this case, in line 4) are invalid.

- In line 5, "accesslog-save-all" has been set by mistake. The correct definition is "accesslog-save-all-log". In this case, the setting is treated as if nothing at all was set. If the option can be omitted, the default value is used. If the option cannot be omitted, an error occurs.
- In line 6, there is a space in "repository-role-search-base". In this case, the setting is invalid. If the option can be omitted, the default value is used. If the option cannot be omitted, an error occurs.

Changing the Authentication Server Environment Definition File

In the environment definition file stored in the Authentication server, define the Business system Site definition registered in the SSO repository and the protected path information.

Use a text editor to set the options shown in the table below.

Notes

Do not edit options that are not shown in the table below. If these options are edited, it may not be possible to operate the Authentication server correctly.

File Name and File Path of the Authentication Server Configuration File

Configuration file name:

ssoatcag.conf

Configuration file path (directory)

Windows32/64

C:\Interstage\F3FMsso\ssoatcag\conf

Solaris32/64 Linux32/64

/etc/opt/FJSVssoac/conf

Configuration Items to Add

Table I.1 Configuration Items to Add

Item	Configuration Name	Setting Contents	Omissible or Required
Restraint of authentication requests (except from the protection resource)	reject-incorrect-protection-resource-url	Set whether authentication requests (except those from the business system protection resource) are restrained. YES : restrained NO : unrestrained Omitting this setting is the same as specifying "NO". If values other than those above are set, sso02040 is output to system log, and "NO" is considered to have been set. If users operate form authentication, and directly access authentication Infrastructure for authentication, the restraint of the authentication request is invalid.	Omissible.
The protection resource URL which accepts authentication requests	protection-resource-url	If authentication requests, except those from the business system protection resource are restrained, set the protection resource URL which accepts authentication requests. This configuration is valid only when "YES" is set to "reject-incorrect-protection-resource-url". In the protection resource URL, set the site configuration and path configuration registered in the SSO repository using the following URL forms.	Omissible. If "YES" is specified for "reject-incorrect-protection-resource-url", this setting is required.

<table>
<tr><th>Item</th><th>Configuration Name</th><th>Setting Contents</th><th>Omissible or Required</th></tr>
<tr><td></td><td></td><td><URL form>
[Protocol Scheme][Host Name][: Port number][Path]
[Protocol Scheme]:
Set "http://" or "https://"
[Host Name]:
Set the host name defined in the protection resource site configuration using FQDN. In the host name, "@", "?" and "&" are invalid.
[: Port number]:
Set the port number defined in the protection resource site configuration. The Port number can be omitted. If it is omitted, the port number is considered to have been set as the following:
- If protocol scheme is "https://"
Port number: ":443"
- If protocol scheme is "http://"
Port number: ":80"
[Path]:
Set the path configuration of the protection resource. The Path cannot be omitted. Set carefully with the following:
The path must start with "/".
Relative paths ("/./", "/../"), continued "/" ("//") and ";" are invalid.
The path cannot end with the characters "/." or "/..".
Set the above URL form carefully as the following:
Only alphanumeric characters and symbols can be used. However, the following symbols cannot be used.
"<", ">", """, "{", "}", "|", "\", "^", "[", "]", "`", " ", "%", "#'
Multi-bytes string (for example kanji code) cannot be used.
Specify the length of string within 2048 bytes.
In URL form, query strings are invalid.
Example of setting the protection resource URL:
Specifying the protection path "/protect/" of the protection site "bus.example.com" of operated port number 443 on https:
protection-resource-url=https://bus.example.com:443/protect/</td><td></td></tr>
</table>

Item	Configuration Name	Setting Contents	Omissible or Required
		If the set protection resource URL ends with "/", it will be handled as a directory. In order for the protection resource to be authenticated, when authentication is requested, the characters of the set value and the URL must match from the first character forward. If the URL ends with a character other than "/", it will be handled as a file. In order for the protection resource to be authenticated, when authentication is requested, the characters of the set value and the URL must match completely from the first character forward. If setting more than one protection resource URL, set the first protection resource URL on one line, and subsequent URLs on separate lines. If multiple URLs are set, decide whether the set URL corresponds to the protection resource URL which accepts the authentication request from the head in order. Setting example: Setting two protection resource URLs. protection-resource-url=https://bus.example.com:443/protect/ protection-resource-url=https://bus.example.com:443/bussystem/ If these details are omitted when "reject-incorrect-protection-resource-url" is set to "YES", sso02008 error message is output to the system log when the authentication server starts and stops. If the value set for the protection resource URL is incorrect, sso02007 error message is output to the system log when the authentication server starts and stops.	

The following example shows how to set a configuration file.

Example

The following is an example of a protection resource URL which accepts the authentication request and restrains all authentication requests except those from the protection resource:

Protection resource URL:

https://bus.example.com:443/protect/

https://bus.example.com:443/bussystem/

```
Reject-incorrect-protection-resource-url=YES
protection-resource-url=https://bus.example.com:443/protect/
protection-resource-url=https://bus.example.com:443/bussystem/
```

Notes on the Set Value of Configuration Item "protection-resource-url"

Set all protection resource information registered in the SSO repository in the configuration item "protection-resource-url" of the authentication server correctly.

If the set value does not correspond to the protection resource information, restraint of authentication requests, except those from the protection resource, cannot be performed correctly.

Addition, Modification or Deletion of Protection Resource Information

If adding, modifying or deleting protection resource information of the SSO repository, modify the configuration item "protection-resource-url" of the authentication server, and then restart the authentication server.

Moreover, ask the business server administrator for access to real protection resources, or to confirm that the authentication server is functioning with the configuration correctly.