IceWall SSO

Version 10.0

Configuration Manual for Automatic Form Authentication

August 2010

Printed in Japan

HP Part No. B1544-97009

Rev.111012A

Notice

The information contained in this document is subject to change without notice.

Meticulous care has been taken in the preparation of this document, however, if a questionable or erroneous item, or an omission of content is found, please contact us.

Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance or use of this document.

The copyright of this document is assigned to Hewlett-Packard Development Company, L.P. No part of this document may be photocopied or reproduced without prior written consent by Hewlett-Packard.

This manual and media, such as the CD-ROM supplied as a part of the product's package, are only to be used with this product.

IceWall is a trademark of Hewlett-Packard.

Adobe is a trademark of Adobe Systems Incorporated in the United States and/or other countries.
Intel, the Intel logo, Intel. Leap ahead., Intel. Leap ahead. logo, Itanium and Itanium Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

– Table of Contents –

1 Introduction

The Automatic Form Authentication function is used to perform automatic authentication on Forwarder for content on Backend Web Servers. This manual describes how to perform single sign on for various types of form authentication.

The descriptions in this manual are for administrators with some knowledge of Backend Web Server applications and basic knowledge of form authentication.

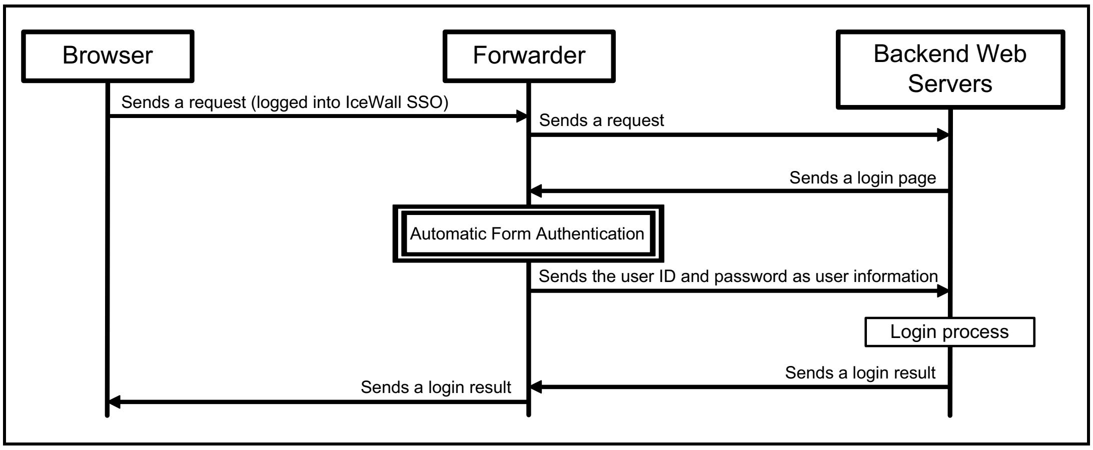
1.1 Version designations in the text

The table below gives the meaning of the version designation added to the text.

Designation	Meaning
10.0	An item added with the version enclosed in the square. In this case, the designation indicates the item was added with 10.0.

2 Automatic Form Authentication Overview

The Automatic Form Authentication function is to automatically send authentication data from IceWall SSO when form authentications exist on the Backend Web Servers.
Using this function, users can reference contents of a server simply by logging into IceWall SSO, without having to enter a user ID and password for form authentication on the Backend Web Server.



Automatic Form Authentication through IceWall SSO

2.1 Form authentication transmission methods supported by IceWall SSO Automatic Form Authentication

The following are descriptions of form authentication supported by the IceWall SSO Automatic Form Authentication function.

Item	Description
Request method	• GET • POST
Transmission data type	• Query String • POST data • Query String and POST data
Transmission data value	• Fixed string • Transmission information acquired from the INPUT tag • Information of the user logged into IceWall SSO
Session management method	• Session management using HTTP Cookie
Operations after authentication	• Transfer through redirection • Content display

For Automatic Form Authentication to work, all of the configuration details below must match.
• URL (prefix search)

- FORM_KEY parameter (multiple strings can be set)
- FORM_KEY_EXCEPTION parameter (multiple strings can be set) 10.0

2.2 Restrictions

There are several restrictions on the Automatic Form Authentication function.

- The user ID and password used with the Automatic Form Authentication function is assumed to match the user ID and password used with the Backend Web Server application. Form authentication always fails in environments where they do not match.

- The Automatic Form Authentication function can be used to automatically authenticate various types of form authentication, but some types of form authentication may not be automatically authenticated.
  Note that this function cannot be used depending on what session management method is used by the application of the Backend Web Server, how the system behaves after authentication, or other conditions.

  The following is an example of when the Automatic Form Authentication function cannot be used.
  (1) When a Java applet or ActiveX is downloaded and that downloaded module directly transmits data to the application of the Backend Web Server.
  (2) When the password changes with each login such as with one-time passwords.

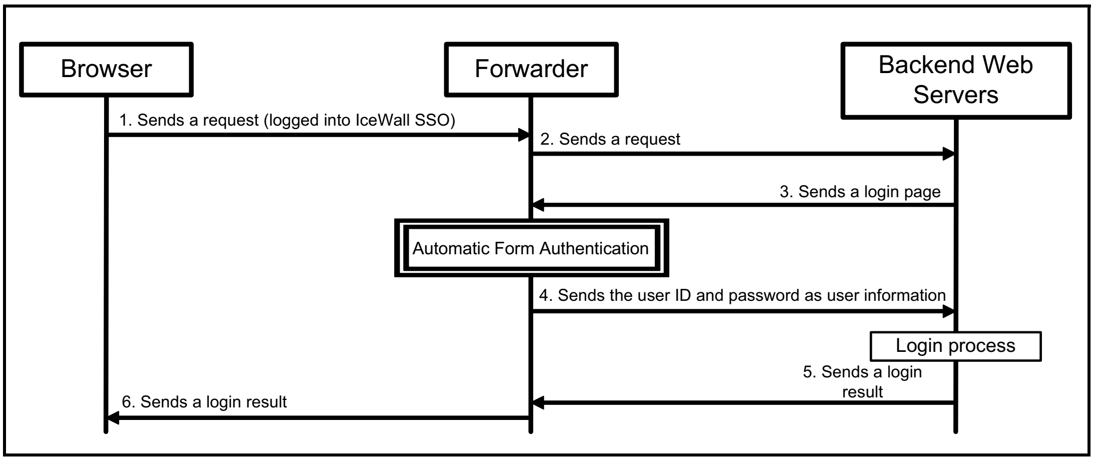
- In the indirect transmission procedure described later, this function cannot be used with clients that do not support JavaScript.

3 Transmission Procedures Usable with Automatic Form Authentication

The following two transmission procedures can be used for performing Automatic Form Authentication through IceWall SSO: the direct transmission procedure and the indirect transmission procedure. The direct transmission procedure is used for general form authentication, and the indirect transmission procedure is used when the direct transmission procedure cannot be used due to behaviors after authentication.

3.1 Direct transmission procedure

The direct transmission procedure is used to send and receive requests only between Forwarder and Backend Web Servers for content requiring form authentication. Because this procedure sends requests from Forwarder directly to the Backend Web Servers when form authentication is required, the number of requests for sending/ receiving is low and the requests are processed at a relatively high speed.

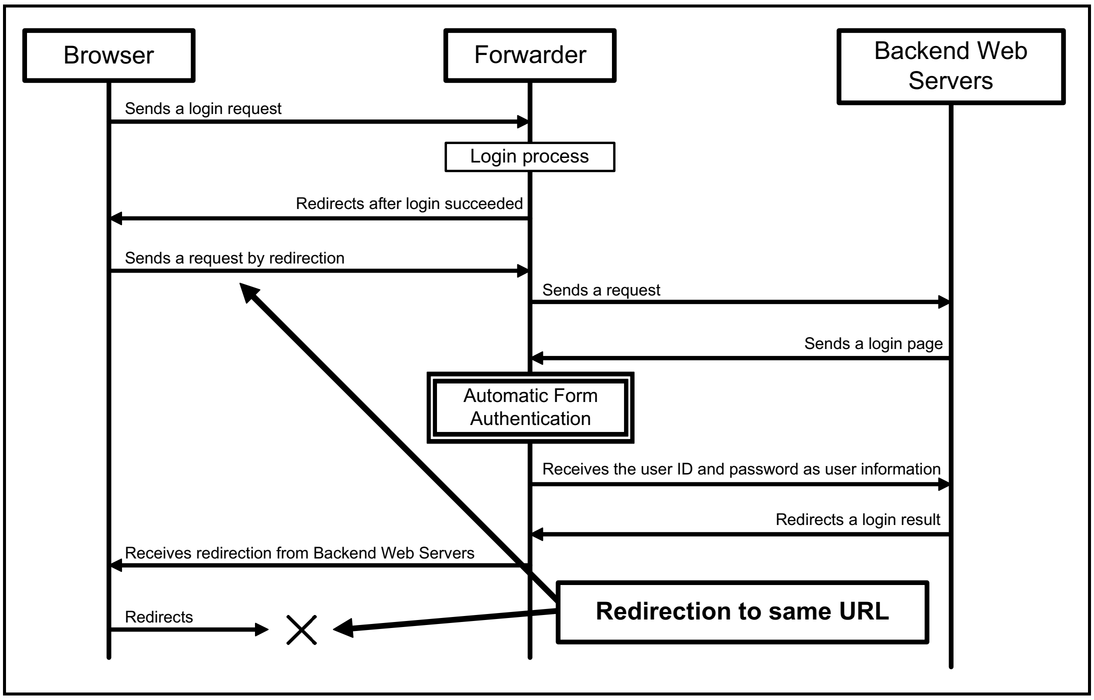


① A request is sent from the browser to Forwarder.
② Forwarder sends the request received from the client to a Backend Web Server.
③ When authentication is required for a request on the Backend Web Server, the login page for form authentication is sent to Forwarder.
④ Forwarder verifies the login page received from the Backend Web Server and the Automatic Form Authentication function is used to send the information necessary for authentication to the Backend Web Server.
⑤ The Backend Web Server performs authentication with the information received from Forwarder and sends the authentication result to Forwarder.
⑥ Forwarder sends the authentication result received from the Backend Web Server to the client.

The following are the form authentication conditions under which the direct transmission procedure cannot be used.

- When a redirection to the same URL is returned to the client twice in a row.

* This depends on browser specifications.


Browser
Forwarder
Backend Web Servers
Sends a login request
Login process
Redirects after login succeeded
Sends a request by redirection
Sends a request
Sends a login page
Automatic Form Authentication
Receives the user ID and password as user information
Redirects a login result
Receives redirection from Backend Web Servers
Redirects
Redirection to same URL

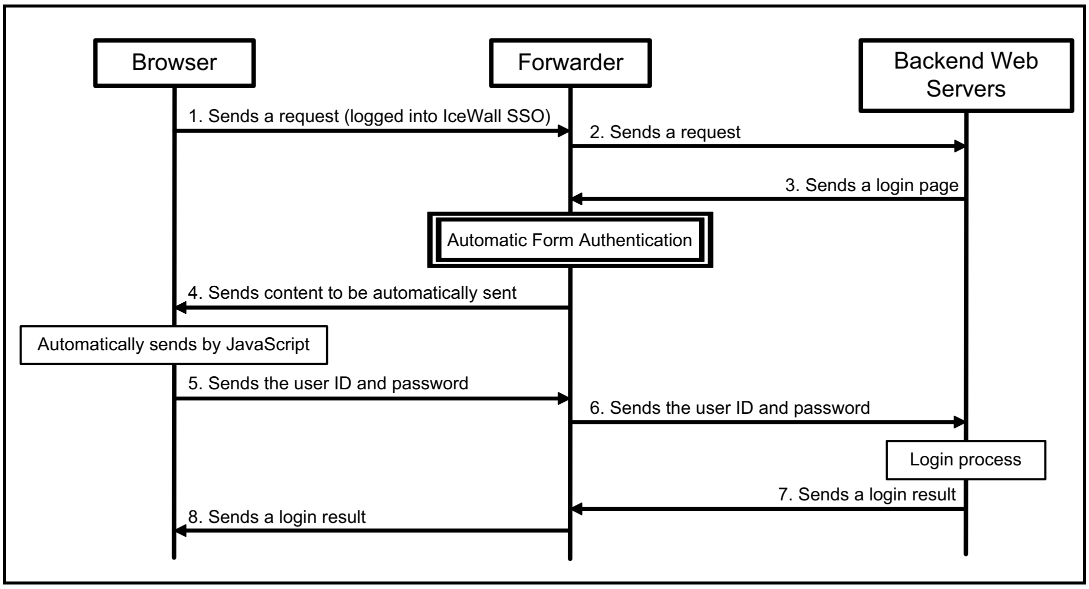
Apply the following workarounds to avoid the type of operation sequence shown in the figure above.

- Use the indirect transmission procedure for the transmission procedure instead.
- Configure the system to display some content and perform the form authentication before the second redirection.

3.2 Indirect transmission procedure

The indirect transmission procedure is used to send requests for form authentication of content from Forwarder to a Backend Web Server through the client.

Because this procedure returns the information necessary for form authentication on Backend Web Servers once to the browser, the response is delayed compared to the direct transmission procedure. The indirect transmission procedure, however, ensures successful authentication when it has been verified that authentication by user operations through IceWall SSO is possible.


Browser
Forwarder
Backend Web Servers
1. Sends a request (logged into IceWall SSO)
2. Sends a request
3. Sends a login page
Automatic Form Authentication
4. Sends content to be automatically sent
Automatically sends by JavaScript
5. Sends the user ID and password
6. Sends the user ID and password
Login process
7. Sends a login result
8. Sends a login result

① A request is sent from the browser to Forwarder.
② Forwarder sends the request received from the browser to a Backend Web Server.
③ When authentication is required for a request, the Backend Web Server sends a login page for form authentication to Forwarder.
④ Forwarder verifies the login page sent by the Backend Web Server and sends the template HTML with the information required for authentication to the browser using the Automatic Form Authentication function.
⑤ The browser automatically sends a request to Forwarder based on the template HTML received from Forwarder.
⑥ Forwarder sends the form authentication request sent from the browser to the Backend Web Server.
⑦ The Backend Web Server performs authentication with the information received from Forwarder and sends the authentication result to Forwarder.
⑧ Forwarder sends the authentication result received from the Backend Web Server to the browser.

The indirect transmission procedure can be used to perform automatic authentication. However, the indirect transmission procedure does not support the special authentication methods such as an authentication using Java applets or ActiveX where the module directly performs authentication to the web server.

With the Automatic Form Authentication function, the Backend Web Server form authentication page (login page) is determined by keywords, so Automatic Form Authentication repeats unlimited times in environments that correspond to all of the conditions below.

(1) The indirect transmission procedure is used
(2) The login page and login error page are the same
(3) The login retry count is unlimited
(4) Logging in fails

In this kind of situation, edit the template HTML used with the indirect transmission procedure as follows.

(1) Delete the onLoad event handler in the <BODY> tag.
(2) Add an <INPUT> tag for form authentication login use in between the <FORM> tag and the </FORM> tag.
Example: <INPUT TYPE="SUBMIT" VALUE="SUBMIT">

By editing the template HTML in this way, Automatic Form Authentication stops right before the step to log in to the Backend Web Server and the user must log in by themselves. Therefore, automatic login is no longer available.

* This is the absolute bare minimum of work to stop an infinite loop. Customize the indirect transmission procedure template HTML as necessary and take measures such as adding links to other pages.

When a section differs even slightly from the login page such as adding and displaying a portion of error messages on the login error page or displaying the state of a configured value entered in an <INPUT> tag, infinite loops can be avoided by setting the portion that differs from the login screen in the FORM_KEY_EXCEPTION parameter.

4 Information Necessary for Automatic Form Authentication

To use Automatic Form Authentication, two factors of target form authentication need to be collected. One is **how the form authentication works**, and the other is **what kind of information on content is necessary**.
This chapter describes how to collect the necessary values to configure the form authentication function.

4.1 Selecting a transmission procedure

Select from two transmission procedures for performing Automatic Form Authentication: the direct transmission procedure or the indirect transmission procedure.

The following two pieces of information are necessary for selecting the transmission procedure.

- The timing of login to IceWall SSO
- The behavior immediately after form authentication login

If the following condition is met, use the indirect transmission procedure instead of the direct transmission procedure.

> When the URL of the login page displayed during form authentication on a Backend Web Server and the URL of the content displayed after login are the same, and Automatic Form Authentication is performed immediately after login to IceWall SSO

Even if the above condition is met, the direct transmission procedure can be used if the following things are possible.

- Configure the REDIRECT parameter in the Forwarder configuration file.
- Configure the content that is displayed immediately after login to IceWall SSO so as to not allow it to be the target of Automatic Form Authentication.

The direct transmission procedure is used for general form authentication, but the indirect transmission procedure must be used in cases of conditions described above.

4.2 Collecting information on content for Automatic Form Authentication

This section describes how to collect information on content for Automatic Form Authentication.
The following two pieces of information are necessary.

- URL (path) for the login page for form authentication
- Unique keyword to identify the login page

4.2.1 URL for the login page

Only the Backend Web Server path portion of the URL for the target login page is used. The specified path differs depending on whether the login page is displayed only when a particular URL is accessed or when any path under a particular directory is accessed.

Example: http://www.xxxxxx.co.jp/fw/dfw/ALIAS/docs/index.html

When the target is only a particular URL:	**/docs/index.html**
When the target is under a particular directory:	**/docs/**
When the target path is not specified:	**/**

The path is compared using prefix search.

4.2.2 Unique keyword to identify the login page

The unique keywords included in the target login page are used to determine whether the login page was displayed. Select keywords that are not used in other content.

Example: **<TITLE>XXXXX LoginPage</TITLE>**

* Multiple keywords can be configured. To ensure the unique use of keywords, specifying multiple keywords is recommended.

4.3 Selecting a transmission method

Select either the GET method or POST method of transmission for Automatic Form Authentication.
Set the value described in the METHOD attribute of the FORM tag described in the login page as the transmission method.

Example: <FORM METHOD="**POST**" ACTION="/cgi-bin/login.cgi">
In this example, the transmission method is **POST**.

When using the GET method, only the argument (Query String) can be sent. When using the POST method, only the POST data or the set of both POST data and the argument (Query String) can be sent.

* Form authentication methods other than the GET and POST methods are not supported.

4.4 Transmission destination URL of authentication information

This section describes how to acquire a URL to send the authentication information using Automatic Form Authentication.
Normally, specify the value in the ACTION attribute of the FORM tag in the login page.

Example: <FORM METHOD="POST" ACTION="**/cgi-bin/login.cgi**">
In this example, the destination URL is **/cgi-bin/login.cgi**.

It is not necessary to set the transmission destination URL. If this parameter is not set, the value set in the ACTION attribute of the FORM tag of the IceWall SSO login page is acquired automatically. If the transmission destination URL is not fixed, for example different for each subsequent display of the login page, do not set this parameter, but instead, let it acquire the transmission destination URL automatically.

When you need to send a fixed argument (Query String) using the POST method, it can be included in the transmission destination URL in the following way:

Example: /cgi-bin/login.cgi**?name=value**

If the content of the argument (Query String) changes dynamically, then let it retrieve the transmission destination URL automatically.

4.5 Form transmission data information

This section describes how to collect all of the transmission data necessary for form authentication in the Backend Web Server used with Automatic Form Authentication.

The values set in the NAME and VALUE attributes of all INPUT tags in the login page are collected. (This does not include the “Submit” value in the TYPE attribute.)

The transmission data are divided into the following three categories:

(1) Values individually entered or selected by the user
This applies to parameters with an entered user ID or password, parameters that are stored as initial values allowed to be edited, or parameters serving as selection formulas.

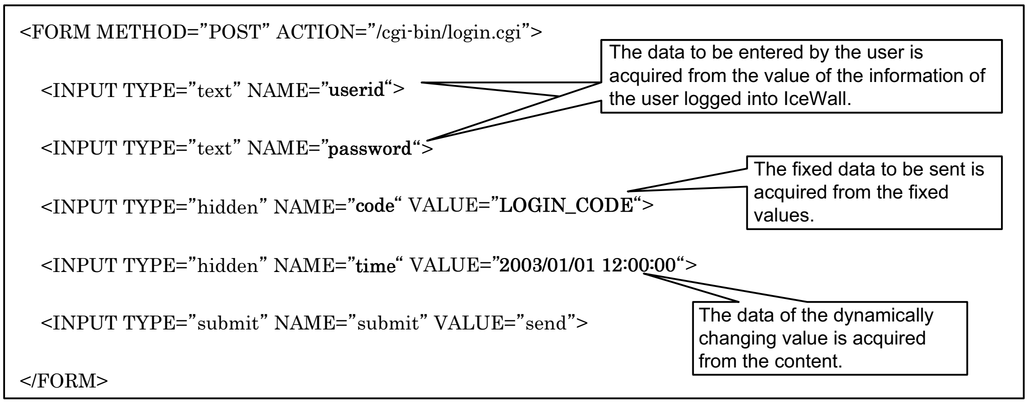
(2) Fixed values acquired from an application of Backend Web Server
These are parameters that do not have to be entered by the user, but are

necessary on the application side in the Backend Web Server. For these values, the TYPE attribute of the INPUT tag is normally set to “hidden.”

(3) Values dynamically stored on an application of Backend Web Server
The values are dynamically changed for each user on the application side in the Backend Web Server and the parameters do not have to be entered by the user. Just like (2), for these values, the TYPE attribute of the INPUT tag is normally set to “hidden.”

The following is an example of how the form transmission data is determined.

Example of form transmission data:



```
<FORM METHOD=”POST” ACTION=”/cgi-bin/login.cgi”>

  <INPUT TYPE=”text” NAME=”userid“>

  <INPUT TYPE=”text” NAME=”password“>

  <INPUT TYPE=”hidden” NAME=”code“ VALUE=”LOGIN_CODE“>

  <INPUT TYPE=”hidden” NAME=”time“ VALUE=”2003/01/01 12:00:00“>

  <INPUT TYPE=”submit” NAME=”submit” VALUE=”send”>

</FORM>
```

The data to be entered by the user is acquired from the value of the information of the user logged into IceWall.

The fixed data to be sent is acquired from the fixed values.

The data of the dynamically changing value is acquired from the content.

Values individually entered or selected by the user:

- the NAME attribute value “**userid**”
- the NAME attribute value “**password**”

Stored fixed values acquired from an application:

- the NAME attribute value “**code**” and VALUE attribute value “**LOGIN_CODE**”

Values dynamically stored from an application:

- the NAME attribute value “**time**”

In this way, the name of the transmitted data and the type of the transmitted value (where it is acquired from) can be determined.

With the Automatic Form Authentication function, fixed values for the VALUE attribute value, login user information, and values set on the login page can be used and sent.
To send dynamic values, use the user information values or the values acquired from the login page.

4.6 Researching other information

This section describes how to collect information on how the program behaves after login for the target of Automatic Form Authentication as well as information on the session management method.
The following are the two basic patterns for collecting information.

- Sending to a separate URL by redirection after form authentication
- Session management through issuing cookies

4.6.1 Redirection after form authentication

When the target of Automatic Form Authentication is redirected after login, check to see if the host of the redirect destination is the host in the HOST or SHOST parameter of the Forwarder configuration file.
If the host is unregistered, add it to the HOST or SHOST parameter.

4.6.2 Cookie session management

This section describes how to research the session management method of form authentication that is the target of Automatic Form Authentication.
The following points must be considered when using cookies for session management.

- Domain attribute for Set-Cookie header
  When the domain attribute is described and the domain is not that of the host in IceWall server, keyword conversion is used to delete the domain attribute.

- Secure attribute for Set-Cookie header
  When the secure attribute is described and SSL is not used between the client and Forwarder, keyword conversion is used to delete the secure attribute.

- Number of cookies
  If cookies are sent to the browser that exceed the maximum number of cookies the browser can retain, the IceWall SSO authentication cookie may be deleted.
  To use a large number of cookies, either go through content that deletes the unnecessary cookies, or set the COOKIEALWAYS parameter to 1 in the Forwarder configuration file.

5 Configuring the Automatic Form Authentication Function

This chapter describes the method for configuring the Automatic Form Authentication function.
To configure the values for the Automatic Form Authentication function described here, information on the target form authentication must be collected beforehand by referring to “4 Information Necessary for Automatic Form Authentication.”

Some of the configuration methods for the same parameters may differ between the direct transmission procedure and the indirect transmission procedure. The configuration of Automatic Form Authentication is described in the host configuration file or the form authentication configuration file.

For details on the configuration parameters, see the “IceWall SSO Reference Manual.”

5.1 Form group

With the Automatic Form Authentication function, when there are multiple form authentications for the target Backend Web Server, each of those form authentications can be individually configured. To make this kind of configuration possible, Automatic Form Authentication uses the concept of “groups.” A group configured for a single form authentication is called a “form group.”
The form group is configured as a single group for one form authentication.
Even if multiple form authentications exist within the same content, each form authentication can be configured separately.

Example of two form authentication configurations on the same Backend Web Server:

```
# FORM1 Configuration
FORM_URL=AAA,/docs/login.html
FORM_KEY=AAA,<TITLE>LoginPage</TITLE>
FORM_METHOD=AAA,POST
FORM_SEND=AAA,/cgi-bin/cert.cgi
FORM_DATA_STR=AAA,POSTDATA,LOGINUID,user001
FORM_DATA_USR=AAA,POSTDATA,PASSWORD,password
```

Configuration form group
for FORM1:AAA

```
# FORM2 Configuration
FORM_URL=BBB,/user.html
FORM_KEY=BBB,<TITLE>UserLogin</TITLE>
FORM_HTML=BBB,/bbb_login.html
FORM_METHOD=BBB,GET
FORM_SEND=BBB,/cgi-bin/login.cgi
FORM_DATA_STR=BBB,NOENCVAL,LOGINUID,user001
FORM_DATA_USR=BBB,NOENCVAL,PASSWORD,password
```

Configuration form group
for FORM2:BBB

5.2 Form authentication configuration file

The form authentication configuration file contains the configuration parameters for the Automatic Form Authentication function. The file name can be set to an arbitrary name.
The configuration of the Automatic Form Authentication function is usually described in the host configuration file. The form authentication configuration file is used when configuration files are managed separately according to the type of form authentication or when the files are configured to share a single form authentication selected from multiple host configuration files.

The setting of the form authentication configuration file is made in the host configuration file as follows:

```
FORM_FILE= (form group name), (name of form authentication configuration file)
```

Example of when the path of the form authentication configuration file is "/opt/icewall-sso/dfw/cgi-bin/form.conf:"
FORM_FILE=FGROUP,/opt/icewall-sso/dfw/cgi-bin/form.conf

When the FORM_FILE parameter is set in the host configuration file, the configuration parameters for the Automatic Form Authentication function are acquired from the form authentication configuration file. There are certain parameters that can have only one setting for each form group. If you specify the parameter, for which there can be only one setting for each form group, in both the host configuration file and the form authentication configuration file, only the setting in the form authentication configuration file will have effect.

Example of the form authentication configuration file:
[Host configuration file]

```
# FORM1 Configuration
FORM_FILE=AAA,./form.conf ←
```

Setting the form group name to AAA

[Form authentication configuration file (form.conf)]

```
# FORM1 Configuration
FORM URL=AAA,/docs/login.html
FORM KEY=AAA,<TITLE>LoginPage</TITLE>
FORM METHOD=AAA,POST
FORM SEND=AAA,/cgi-bin/cert.cgi
FORM DATA STR=AAA,POSTDATA,LOGINUID,user001
FORM_DATA_USR=AAA,POSTDATA,PASSWORD,password
```

Setting the form group name to AAA in the same way

In this case, even if you define “FORM_METHOD=AAA,GET” in the host configuration file, “FORM_METHOD=AAA,POST” is effective in the Form authentication configuration file.

5.3 Setting up the direct transmission procedure

The following describes the setup method when using the direct transmission procedure.

Templates HTML, used in the indirect transmission procedure, are not used in the direct transmission procedure.
The configuration settings described here can be made either in the host configuration file or in the form authentication configuration file. However, when using the form authentication configuration file, set the FORM_FILE parameter in the host configuration file.

In this example, the form group name is defined as “FGROUP.”

5.3.1 Automatic Form Authentication target path

This section describes how to configure the path of the content for performing Automatic Form Authentication. You can specify the information collected in “4.2.1 URL for the login page”.

■ FORM_URL parameter

```
FORM_URL= (form group name), (target path)
```

- Only one instance of this parameter can be configured in the form group.
- The path is checked using prefix search (can set to search under a certain directory).
- This is a mandatory parameter.

Configuration example:
When form authentication is requested on accessing /docs/loginpage.html

```
FORM_URL=FGROUP,/docs/loginpage.html
```

When form authentication is requested on accessing something under /docs/

```
FORM_URL=FGROUP,/docs/
```

When form authentication is requested on accessing a specific server, regardless of the target path

```
FORM_URL=FGROUP,/
```

5.3.2 Automatic Form Authentication determination keywords

This section describes how to set the keyword to identify the login page for Automatic Form Authentication. You can specify the information collected in “4.2.2 Unique keyword to identify the login page”.

■ FORM_KEY parameter

```
FORM_KEY= (form group name), (search keyword)
```

- More than one instance of this parameter can be configured in the form group.
- If multiple search keywords are set, form authentication is performed only when all the search keywords match.
- This is a mandatory parameter.

Configuration example:
When using the “<TITLE>Login Page</TITLE>” and the “UserLoginPage” as search keywords of the form authentication login page

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>
FORM_KEY=FGROUP,UserLoginPage
```

■ FORM_KEY_EXCEPTION parameter 10.0

```
FORM_KEY_EXCEPTION= (form group name), (search keyword)
```

- More than one instance of this parameter can be configured in the form group.
- Opposite of the FORM_KEY parameter, the page is subject to form authentication when the page does not include the search keywords.
- The FORM_KEY_EXCEPTION parameter cannot be used when the FORM_KEY parameter is not configured.
- If multiple search keywords are set, form authentication is not performed even when only one line of search keywords matches.

Configuration example:
When setting the form authentication target as the form authentication login page that contains “<TITLE>Login Page</TITLE>” and “UserLoginPage” and does not contained “UserID Error ReLogin”

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>
FORM_KEY=FGROUP,UserLoginPage
FORM_KEY_EXCEPTION=FGROUP,UserID Error ReLogin
```

5.3.3 Template HTML of the indirect transmission procedure

The template HTML for indirect transmission cannot be used with the direct transmission procedure. Therefore, this configuration is not required.

5.3.4 Request method

This section describes how to configure the request method used in Automatic Form Authentication. The information collected in “4.3 Selecting a transmission method” is used.

FORM_METHOD parameter

```
FORM_METHOD= (form group name), (method name)
```

- Only one instance of this parameter can be configured in the form group.
- This is a mandatory parameter.

Configuration example:
When performing form authentication by the POST method

```
FORM_METHOD=FGROUP,POST
```

5.3.5 Transmission destination

The following describes formats for configuring the transmission destination path of Automatic Form Authentication. The information collected in “4.4 Transmission destination URL of authentication information” is used.

■ FORM_SEND parameter

```
FORM_SEND= (form group name), (recipient path)
```

- Only one instance of this parameter can be configured in the form group.
- If this parameter is not set, the value set in the ACTION attribute of the FORM tag of the login page is acquired automatically. (If there is a dynamic Query String, etc., this setting must be omitted to acquire the value automatically.)
- “http”, “https”, “/”, and “.” can be used to start the path description.
- In the case of an absolute path starting from “http” or “https,” the host must be configured in the HOST or SHOST parameter of the Forwarder configuration file.
- When a Query String is added to the path, it is added, as is, to the end of the transmission destination path.

Configuration example:
When performing the form authentication to the file “/cgi-bin/cert.cgi” on the same

server as the server displaying the login page

```
FORM_SEND=FGROUP,/cgi-bin/cert.cgi
```

When performing the form authentication to the file "/cert.cgi" on the same server as the server displaying the login page

```
FORM_SEND=FGROUP,./cert.cgi
```

When performing the form authentication to the file "http://www.other.jp/cgi-bin/cert.cgi" on a server other than the server displaying the login page

```
FORM_SEND=FGROUP,http://www.other.jp/cgi-bin/cert.cgi
```

* "www.other.jp" must be configured in the HOST parameter.

When adding a fixed argument (Query String) "aaa=%2Fbbb" to the file "/cgi-bin/cert.cgi" on the same server as the server displaying the login page, and sending it

```
FORM_SEND=FGROUP,/cgi-bin/cert.cgi?aaa=%2Fbbb
```

* Describe the Query String with URL encoding.

5.3.6 Transmission data

The following describes formats for configuring the transmission data for Automatic Form Authentication. The information collected in "4.5 Form transmission data information" is used.
Fixed values, user information values, and values acquired from content can be used for the transmission data.

* The configuration of the transmission data differs from that for the indirect transmission procedure.

■ FORM_DATA_STR parameter
This parameter allows fixed values to be used as the transmission data.

```
FORM_DATA_STR= (form group name), (transmission data type), (attribute name), (attribute value)
```

- Specify either "POSTDATA" or "QUERY" for the transmission data type.
- More than one instance of this parameter can be configured in the form group.

Configuration example:
When sending the following tag information as is as POST data
<INPUT TYPE="text" NAME="userid" VALUE="user001">

```
FORM_DATA_STR=FGROUP,POSTDATA,userid,user001
```

When sending the following tag information as is as Query String
<INPUT TYPE="password" NAME="password" VALUE="pwd01">

```
FORM_DATA_STR=FGROUP,QUERY,password,pwd01
```

■ FORM_DATA_USR parameter
This uses user information values as the transmission data.

```
FORM_DATA_USR= (form group name), (transmission data type), (attribute
name), (authentication DB column name)
```

- Specify either “POSTDATA” or “QUERY” for the transmission data type.
- The user information sent from the authentication module is specified as the Authentication DB column name.
- The following words are reserved for Authentication DB column names:
  DEFAULTUID: uses the login user ID
  DEFAULTPWD: uses the login password*
- More than one instance of this parameter can be configured in the form group.

* Please note that when using IceWall Cert Protocol (ICP) 2.0, the request control configuration file (request.acl) must be configured to allow sending passwords.

Configuration example:
To send the following tag information as POST data with the value acquired from the Authentication DB column PWDCLM
<INPUT TYPE="password" NAME="password">

```
FORM_DATA_USR=FGROUP,POSTDATA,password,PWDCLM
```

To send the following tag information as a Query String with the value acquired from the Authentication DB column INFOCLM
<INPUT TYPE="text" NAME="info">

```
FORM_DATA_USR=FGROUP,QUERY,info,INFOCLM
```

■ FORM_DATA_PAGE parameter
The NAME attribute value and VALUE attribute value of the INPUT tag in the login page are used as transmission data.

```
FORM_DATA_PAGE= (form group name), (transmission data type),
(transmission attribute name), (search attribute name)
```

- Specify either “POSTDATA” or “QUERY” for the transmission data type.
- When there are multiple INPUT tags with the same attribute name in the content, the INPUT tag at the top becomes the target.
- More than one instance of this parameter can be configured in the form group.

Configuration example:
When sending the following tag value as is as POST data
<INPUT TYPE="hidden" NAME="data" VALUE="data-value">

```
FORM_DATA_PAGE=FGROUP,POSTDATA,data,data
```

When modifying the transmission attribute name of the following tag to “information,” and sending it as Query String
<INPUT TYPE="hidden" NAME="info" VALUE="info-value">

```
FORM_DATA_PAGE=FGROUP,QUERY,information,info
```

■ FORM_DATA_PAGE_REF parameter 10.0

This parameter sets whether or not to replace the entity references included in the values retrieved with the FORM_DATA_PAGE parameter with the original characters.

```
FORM_DATA_PAGE_REF= (form group name), (flag)
```

- Only one instance of this parameter can be configured in the form group.
- One of the following values can be set for the flag:

0 : Do not replace entity references
1 : Replace entity references

Configuration example:
To return the original characters when form information retrieved using the FORM_DATA_PAGE parameter contains entity references

```
FORM_DATA_PAGE_REF=FGROUP,1
```

The transmission data configures all the data required by the form authentication.
This completes the configuration of the direct transmission procedure.

5.4 Setting up the indirect transmission procedure

The following describes the configuration method for the indirect transmission procedure. The basic configuration procedure is the same as with the direct transmission procedure, but for the indirect transmission procedure, the indirect transmission procedure template HTML is configured.
The configuration settings described here can be made either in the host configuration file or in the form authentication configuration file. If you are going to use the form authentication configuration file, you will need to specify the FORM_FILE parameter in the host configuration file.

In this example, the form group is defined as “FGROUP.”

5.4.1 Automatic form target path

This section describes how to configure the path of the content for performing Automatic Form Authentication. The information collected in “4.2.1 URL for the login page” is used.

■ FORM_URL parameter

```
FORM_URL= (form group name), (target path)
```

- Only one instance of this parameter can be configured in the form group.
- The path is checked using prefix search (can set to search under a certain directory).
- This is a mandatory parameter.

Configuration example:
When form authentication is requested on accessing /docs/loginpage.html

```
FORM_URL=FGROUP,/docs/loginpage.html
```

When form authentication is requested on accessing something under /docs/

```
FORM_URL=FGROUP,/docs/
```

When form authentication is requested on accessing a specific server, regardless of the path

```
FORM_URL=FGROUP,/
```

5.4.2 Automatic form target keyword

This section describes how to set the keyword to identify the login page for Automatic Form Authentication. You can specify the information collected in “4.2.2 Unique keyword to identify the login page”.

■ FORM_KEY parameter

```
FORM_KEY= (form group name), (search keyword)
```

- More than one instance of this parameter can be configured in the form group.
- If multiple search keywords are set, form authentication is performed only when all the search keywords match.
- This is a mandatory parameter.

Configuration example:
When using "<TITLE>Login Page</TITLE>" and "UserLoginPage" as keywords of the form authentication login page

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>
FORM_KEY=FGROUP,UserLoginPage
```

■ FORM_KEY_EXCEPTION parameter 10.0

```
FORM_KEY_EXCEPTION= (form group name), (search keyword)
```

- More than one instance of this parameter can be configured in the form group.
- If multiple search keywords are set, form authentication is not performed even when only one line of search keywords matches.
- Opposite of the FORM_KEY parameter, the page is subject to form authentication when the page does not include the keywords.
- The FORM_KEY_EXCEPTION parameter cannot be used when the FORM_KEY parameter is not configured.

Configuration example:
When setting the form authentication target as the form authentication login page that contains "<TITLE>Login Page</TITLE>" and "UserLoginPage" and does not contained "UserID Error ReLogin"

```
FORM_KEY=FGROUP,<TITLE>Login Page</TITLE>
FORM_KEY=FGROUP,UserLoginPage
FORM_KEY_EXCEPTION=FGROUP,UserID Error ReLogin
```

5.4.3 Template HTML of the indirect transmission procedure

This section describes how to configure the indirect transmission procedure template HTML path to be sent for Automatic Form Authentication.
Unlike the direct transmission procedure that sends the requests between Forwarder and the Backend Web Server, the indirect transmission procedure sends the information required for the form authentication once to the browser. The information is sent to the browser as content, based on the indirect transmission procedure template HTML.
The indirect transmission procedure template HTML must contain all of the following information required for form authentication:

- Transmission destination URL (the ACTION attribute of the FORM tag)
- Transmission method (the METHOD attribute of the FORM tag)
- Transmission data (the NAME attribute and VALUE attribute of the INPUT tag)

This information is retrieved from the configuration file or the login page. The retrieved values are stored in the template HTML with “keyword conversion”. For this reason, the keyword for storing the above mentioned data must be described in the template HTML.
In addition, the JavaScript codes need to be specified in the indirect transmission procedure template HTML in order for form authentication to be performed automatically.

■ FORM_HTML parameter
This parameter specifies the template HTML file.

```
FORM_HTML= (form group name), (template HTML file name)
```

- Only one instance of this parameter can be configured in the form group.
- This is a mandatory parameter when using the indirect transmission procedure.

Configuration example:
When the indirect transmission template file is: /opt/icewall-sso/dfw/cgi-bin/autologin.html

```
FORM_HTML=FGROUP,/opt/icewall-sso/dfw/cgi-bin/autologin.html
```

The following is an example of indirect transmission template HTML.
You can specify replacement keywords; “$ACTION” for the transmission destination URL, “$METHOD” for the transmission method, “$UID” for the “USERID” attribute of the transmission data, and “$PWD” for the “PASSWD” attribute of the transmission data.

```
<HTML>
<HEAD>
<TITLE>AutoLogin Page</TITLE>
<SCRIPT LANGUAGE="JavaScript">
<!--
function LoadData()
{
  document.form.submit();
}
//-->
</SCRIPT>
</HEAD>
<BODY onLoad="LoadData();">

<FORM NAME="form" METHOD="$METHOD" ACTION="$ACTION">
   <INPUT TYPE="hidden" NAME="USERID" VALUE="$UID">
   <INPUT TYPE="hidden" NAME="PASSWD" VALUE="$PWD">
</FORM><P><BR>
<DIV ALIGN="center">Form authentication in progress</DIV>
</BODY>
</HTML>
```

JavaScript for automatic sending from the browser.

See “5.4.6 Transmission data” for detailed information about replacement keywords for transmission data.

5.4.4 Request method

The following describes formats for configuring the request method to send for Automatic Form Authentication. The information collected in “4.3 Selecting a transmission method” is used.

■ FORM_METHOD parameter

```
FORM_METHOD= (form group name), (method name)
```

- Only one instance of this parameter can be configured in the form group.
- This is a mandatory parameter.

Configuration example:
When performing form authentication by the POST method

```
FORM_METHOD=FGROUP,POST
```

5.4.5 Transmission destination

This section describes how to configure the transmission destination path of Automatic Form Authentication. The information collected in “4.4 Transmission destination URL of authentication information” is used.

■ FORM_SEND parameter

```
FORM_SEND= (form group name), (recipient path)
```

- Only one instance of this parameter can be configured in the form group.
- If this parameter is not set, the value set in the ACTION attribute of the FORM tag of the login page is acquired automatically. (If there is a dynamic Query String, etc., this setting must be omitted to acquire the value automatically.)
- “http”, “https”, “/”, and “.” can be used to start the path description.
- In the case of an absolute path starting from “http” or “https,” the host must be configured in the HOST or SHOST parameter of the Forwarder configuration file.
- When a Query String is added to the path, it is added, as is, to the end of the transmission destination path.

Configuration example:
When performing the form authentication to the file “/cgi-bin/cert.cgi” on the same server as the server displaying the login page

```
FORM_SEND=FGROUP,/cgi-bin/cert.cgi
```

When performing the form authentication to the file "/cert.cgi" on the same server as the server displaying the login page

```
FORM_SEND=FGROUP,./cert.cgi
```

When performing the form authentication to the file "http://www.other.jp/cgi-bin/cert.cgi" on a server other than the server displaying the login page

```
FORM_SEND=FGROUP,http://www.other.jp/cgi-bin/cert.cgi
```

* "www.other.jp" must be configured in the HOST parameter.

When adding a fixed argument (Query String) "aaa=%2Fbbb" to the file "/cgi-bin/cert.cgi" on the same server as the server displaying the login page, and sending it

```
FORM_SEND=FGROUP,/cgi-bin/cert.cgi?aaa=%2Fbbb
```

* Describe the Query String with URL encoding.

5.4.6 Transmission data

The following describes formats for configuring the transmission data for Automatic Form Authentication. The information collected in "4.5 Form transmission data information" is used.
Fixed values, user information values, and values acquired from content can be used for the transmission data.
IceWall SSO transmits data by replacing the keywords specified in the indirect transmission procedure template HTML with actual values and transmitting the data to clients.
URL encoding can be performed for the replaced values.
For the keywords described in the indirect transmission procedure template HTML, "$" prefixes the value configured in the keyword of each parameter.

■ FORM_DATA_STR parameter
This parameter uses fixed values as the transmission data.

```
FORM_DATA_STR= (form group name), (transmission data type), (attribute name), (attribute value)
```

- Specify either "ENCVAL" or "NOENCVAL" for the type of transmission.
- More than one instance of this parameter can be configured in the form group.

Configuration example:
When setting the following tag information value to "user001," storing it in the replacement keyword $PAGEKEY-UID of the indirect transmission template HTML without URL encoding, and sending it to the browser

<INPUT TYPE="text" NAME="userid">

```
FORM_DATA_STR=FGROUP,NOENCVAL,PAGEKEY-UID,user001
```

The indirect transmission procedure template is described as follows.

```
<INPUT TYPE="hidden" NAME="userid" VALUE="$PAGEKEY-UID">
```

When setting the following tag information value to “pwd01,” storing it as a URL-encoded argument in the replacement keyword $PAGEKEY-PWD of the indirect transmission template HTML, and sending it to the browser by the POST method
<INPUT TYPE="password" NAME="password">

```
FORM_DATA_STR=FGROUP,ENCVAL,PAGEKEY-PWD,pwd01
```

The indirect transmission procedure template is described as follows.

```
<FORM METHOD="POST" ACTION="/cgi-bin/cert.cgi?password=$PAGEKEY-PWD">
```

■ FORM_DATA_USR parameter
This parameter uses user information values as the transmission data.

```
FORM_DATA_USR= (form group name), (transmission data type), (attribute name), (authentication DB column name)
```

- Specify either “ENCVAL” or “NOENCVAL” for the transmission data type.
- The user information sent from the authentication module is used as the Authentication DB column name.
- The following words are reserved for Authentication DB column names:
  DEFAULTUID: uses the login user ID
  DEFAULTPWD: uses the login password*
- More than one instance of this parameter can be configured in the form group.

* Please note that when using IceWall Cert Protocol (ICP) 2.0, the request control configuration file (request.acl) must be configured to allow sending passwords.

Configuration example:
When acquiring the following tag information value from the PWDCLM of the Authentication DB column and sending it as POST data without URL encoding. The replacement keyword is $PAGEKEY-PWD.
<INPUT TYPE="password" NAME="password">

```
FORM_DATA_USR=FGROUP,NOENCVAL,PAGEKEY-PWD,PWDCLM
```

The indirect transmission procedure template HTML is described as follows.

```
<INPUT TYPE="hidden" NAME="password" VALUE="$PAGEKEY-PWD">
```

When acquiring the following tag information value from the INFOCLM of the Authentication DB column and sending it as a URL-encoded Query String by the POST method. The replacement keyword is $PAGEKEY-INFO.
<INPUT TYPE="text" NAME="info">

```
FORM_DATA_USR=FGROUP,ENCVAL,PAGEKEY-INFO,INFOCLM
```

The indirect transmission procedure template HTML is described as follows.

```
<FORM METHOD="POST" ACTION="/cgi-bin/cert.cgi?info=$PAGEKEY-INFO">
```

■ FORM_DATA_PAGE parameter
The VALUE attribute value and the NAME attribute name of the INPUT tag included in the login page are used as transmission data.

```
FORM_DATA_PAGE= (form group name), (transmission data type),
(transmission attribute name), (search attribute name)
```

- Specify either “ENCVAL” or “NOENCVAL” for the transmission data type.
- If there are multiple INPUT tags with the same attribute name in the content, the INPUT tag at the top becomes the target.
- More than one instance of this parameter can be configured in the form group.

Configuration example:
When acquiring the VALUE value “data-value” of the following tag using the NAME value “data” as the keyword, storing it in the replacement keyword “$PAGEKEY-DATA” of the indirect transmission template HTML without URL encoding, and sending it to the browser
<INPUT TYPE="hidden" NAME="data" VALUE="data-value">

```
FORM_DATA_PAGE=FGROUP,NOENCVAL,PAGEKEY-DATA,data
```

The indirect transmission procedure template HTML is described as follows.

```
<INPUT TYPE="hidden" NAME="data" VALUE="$PAGEKEY-DATA">
```

When acquiring the VALUE value “info-value” of the following tag using the NAME value “info” as the keyword, storing it as a URL-encoded argument in the replacement keyword “$PAGEKEY-INFO” of the indirect transmission template HTML, and sending it to the browser by the POST method

<INPUT TYPE="hidden" NAME="info" VALUE="info-value">

```
FORM_DATA_PAGE=FGROUP,ENCVAL,PAGEKEY-INFO,info
```

The indirect transmission procedure template is described as follows.

```
<FORM METHOD="POST" ACTION="/cgi-bin/cert.cgi?info=$PAGEKEY-
INFO">
```

5.5 Remarks about the configuration

When the target of Automatic Form Authentication uses cookies for redirection after login or for session management, you may add the settings in the Forwarder configuration file.

5.5.1 Redirection after login

If the target of the Automatic Form Authentication redirects after login but the host of the redirect destination is not specified in the HOST or SHOST parameters in the Forwarder configuration file, you will need to add these parameters.

Example of when the host of the redirect destination “www.yyyyyy.co.jp” is not set:

```
HOST=ALIAS=www,yyyyyy.co.jp
SVRFILE=ALIAS,./host.conf
```

5.5.2 Session management method

When cookies are used in session management and the following conditions are met, additional configuration is needed.

- Set-Cookie header domain attribute
  When the domain attribute is described and that domain is not the domain of the host in IceWall server, keyword conversion is specified in the host configuration file to delete the domain attribute.

  Example of Set-Cookie: [Name]=[Value]; domain=zzz.co.jp

  ```
  REPKEY=domain=zzz.co.jp,
  ```

- Set-Cookie header secure attribute
  When the secure attribute is described and the IceWall is not using SSL, keyword conversion is specified in the host configuration file to delete the secure attribute.

Example of Set-Cookie: [Name]=[Value]; secure

```
REPKEY=; secure,
```

5.5.3 Notes regarding the format of the Set-Cookie header

Note the following points when performing the direct transmission procedure:

- Only the semicolon character (;) can be used as separator in the Set-Cookie header.
- Multiple cookies cannot be described in a Set-Cookie header. Multiple cookies must be set in separate Set-Cookie header lines.

```
Incorrect descriptions:
Set-Cookie: [Name 1]=[Value 1]; [Name 2]=[Value 2]; expires=[Date and time];
path=[Send path]; domain=[Domain name]
Set-Cookie: [Name 1]=[Value 1]: expires=[Date and time]: path=[Send path]:
domain=[Domain name]

Correct descriptions:
Set-Cookie: [Name 1]=[Value 1]; expires=[Date and time]; path=[Send path];
domain=[Domain name]
Set-Cookie: [Name 2]=[Value 2]; expires=[Date and time]; path=[Send path];
domain=[Domain name]
```

5.5.4 Behavior when Automatic Form Authentication using the direct transfer procedure fails

When the Automatic Form Authentication fails due to defective transmission data (incorrect password, etc.), and the Backend Web Server resends the login page, the login page sent from the Backend Web Server is sent to the client as is.
This is because Automatic Form Authentication is not performed on the results of the initial Automatic Form Authentication.

Please note, however, that an Automatic Form Authentication loop may occur if the result of form authentication from the Backend Web Server returns a redirect response. It may occur when it is determined that the contents accessed by redirection are subject to Automatic Form Authentication.

5.5.5 Using the Domain Gateway Option for UNIX

The Domain Gateway Option for UNIX uses federation authentication, which authenticates a login with “user ID only” when a user logs into IceWall SSO. Note that “DEFAULTPWD” cannot be used with the Domain Gateway Option due to that reason.

6 Form Configuration Samples

This chapter introduces settings for automatic login to backend IceWall SSO in an IceWall SSO multi-tier architecture, as configuration samples of Automatic Form Authentication.

6.1 Sample of IceWall SSO multi-tier automatic form (direct transmission procedure)

This is an example of using the direct transmission procedure in an IceWall SSO multi-tier architecture.

■ Host configuration file
In this sample, the form authentication configuration file is used to configure form authentication for IceWall SSO login. The form group name is “IW.”

```
# IceWall SSO multi-tier form authentication
FORM_FILE=IW,./form_iw.conf
```

■ Form authentication configuration file (form_iw.conf)
In the case of IceWall SSO multi-tier architecture, it is necessary to ensure that the data required by the backend IceWall SSO at the time of login would not be recognized as a login request to the front-end IceWall SSO itself, which performs the configuration of the form authentication function. In this example, it is assumed that the backend IceWall SSO login information setting (POSTKEY_LOGIN) is modified. The user ID and password used for the backend IceWall SSO login is the same as the information used for the front-end IceWall SSO login.

Note that for the parameters dynamically set by IceWall SSO at the time of the login request, the transmission data is acquired from the transmitted login page, instead of specified as a fixed string or user information.

```
# IceWall multi-tier form authentication
FORM_METHOD=IW,POST
FORM_SEND=IW,/fw/dfw
FORM_URL=IW,/fw/dfw
FORM_KEY=IW,IceWall SSO - Login -
FORM_DATA_USR=IW,POSTDATA,ACCOUNTUID,DEFAULTUID
FORM_DATA_USR=IW,POSTDATA,PASSWORD,DEFAULTPWD
FORM_DATA_PAGE=IW,POSTDATA,HIDEURL,HIDEURL
FORM_DATA_PAGE=IW,POSTDATA,LOGIN,LOGIN
```

6.2 Sample of IceWall SSO multi-tier automatic form (indirect transmission procedure)

In the case of IceWall SSO multi-tier architecture, a backend IceWall SSO login may occur by accessing immediately after the front-end IceWall SSO login.
If a backend IceWall SSO login occurs immediately after the front-end IceWall SSO login, a redirect response for the same URL is sent twice to the browser. This is because the IceWall SSO sends a redirect response to the browser immediately after the login. In this case, the login sequence on the browser side will stop due to the restriction on the browser side that prevents executing two subsequent redirects. The indirect transmission procedure is used to avoid this problem.

■ Host configuration file
As with the direct transmission procedure, the form authentication configuration file is used to configure form authentication for IceWall SSO login. The form group name is “IW.”

```
# IceWall SSO multi-tier form authentication
FORM_FILE=IW,./form_iw.conf
```

■ Form authentication configuration file (form_iw.conf)
The configuration differs from the direct transmission procedure in terms of the indirect transmission template HTML configuration and the data transmission settings. The data transmission configuration contains a replacement keyword for storing the necessary information in the indirect transmission template HTML.

```
FORM_METHOD=IW,POST
FORM_SEND=IW,/fw/dfw
FORM_URL=IW,/fw/dfw
FORM_HTML=IW,./autologin_iw.html
FORM_KEY=IW,IceWall SSO - Login -
FORM_DATA_USR=IW,NOENCVAL,IW-USERID,BACKUID
FORM_DATA_USR=IW,NOENCVAL,IW-PASSWORD,BACKPWD
FORM_DATA_PAGE=IW,NOENCVAL,IW-HIDEURL,HIDEURL
FORM_DATA_PAGE=IW,NOENCVAL,IW-LOGINKEY,LOGIN
```

■ Indirect transmission template HTML (autologin.html)
Please note that the keyword to replace the transmission data configured in the form authentication configuration file should be included in the indirect transmission template HTML as “$replacement keyword.”

```
<HTML>
<HEAD>
<TITLE>Login Page</TITLE>
<SCRIPT LANGUAGE="JavaScript">
<!--
function LoadData()
{
  document.form.submit();
}
//-->
</SCRIPT>
</HEAD>
<BODY onLoad="LoadData();">
<FORM NAME="form" METHOD="$METHOD" ACTION="$ACTION">
    <INPUT TYPE="hidden" NAME="ACCOUNTUID" VALUE="$IW-USERID">
    <INPUT TYPE="hidden" NAME="PASSWORD" VALUE="$IW-PASSWORD">
    <INPUT TYPE="hidden" NAME="HIDEURL" VALUE="$IW-HIDEURL">
    <INPUT TYPE="hidden" NAME="LOGIN" VALUE="$IW-LOGINKEY">
</FORM><P><BR>
<DIV ALIGN="center">You are logged into the IceWall SSO.</DIV>
</BODY>
</HTML>
```