



# **IceWall SSO**

Version 10.0

## **Installation Guide of Domain Gateway Option for UNIX**

August 2010

**Printed in Japan**

**HP Part No. B1544-97006**

**Rev.111031A**

## 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 .....	1
1.1 Version designations in the text .....	1
2 Operating Environment .....	2
3 Overview .....	4
3.1 System configuration diagram .....	4
3.2 Transactions .....	5
3.2.1 Login transaction .....	5
3.2.2 Forced login transaction for duplicate login .....	9
3.3 Restrictions on the Domain Gateway Option .....	15
3.3.1 Remarks about authentication by the Domain Gateway Option .....	15
3.3.2 Restrictions on using the Authentication DB .....	15
3.3.3 Notes on proxy server .....	15
3.3.4 Authentication Module receive timeout .....	15
3.3.5 Combination with failover option <b>10.0</b> .....	15
3.3.6 Combining with Automatic Form Authentication of IceWall SSO .....	16
3.3.7 Transaction ID <b>10.0</b> .....	16
4 Installing the Domain Gateway Option .....	17
4.1 IceWall server configuration .....	17
4.2 Prerequisites for installing the Domain Gateway Option .....	17
4.3 Installing the Domain Gateway Option .....	18
4.3.1 Installing Linux edition .....	18
4.3.2 Installing HP-UX edition .....	19
4.4 Checking the installed files .....	20
4.5 Confirming the version information .....	21
4.5.1 Confirmation procedure of Linux edition .....	21
4.5.2 Confirmation procedure for HP-UX edition .....	21
4.6 Uninstallation .....	22
4.6.1 Linux edition .....	22
4.6.2 HP-UX edition .....	22
4.7 Configuring the Web server .....	22
4.8 Configuring Forwarder .....	25
4.9 Configuring the Authentication Module .....	25
4.9.1 Configuring federation authentication in the Authentication Module .....	26
4.9.2 Configuring LDAPBIND in the Authentication Module .....	26
5 Domain Gateway Option Reference .....	27
5.1 Domain Gateway Option configuration file (dgfw.conf) .....	28
5.1.1 Basic configuration .....	29
ALEVEL .....	30
ELEVEL .....	31
ACCESS .....	32
ERROR .....	33
TRACE .....	34
TRANSID <b>10.0</b> .....	35

TRANSID_STR (10.0)	37
DOCS	38
SERVICE_NAME	39
USERNAME_FRM	40
5.2 Domain Gateway Option HTML configuration file (dghtml.conf)	41
5.2.1 Login	42
DG_LOGIN_TKT	43
DG_LOGIN_FORCE	44
DG_LOGIN_ERR_ADDR	45
DG_LOGIN_ERR_UID	46
DG_LOGIN_ERR_TKT	47
DG_LOGIN_ERR_1STCERT	48
DG_LOGIN_ERR_LOCK	49
DG_LOGIN_ERR_NOGRP	50
DG_LOGIN_ERR_STOP	51
DG_LOGIN_ERR_LIMIT	52
5.2.2 System errors	53
DG_SYSTEM_ERR	54
DG_SYSTEM_DOWN_CERTD	55
DG_SYSTEM_DOWN_DB	56
DG_SYSTEM_TOUT_CERTD	57
DG_SYSTEM_BUSY_DB (10.0)	58
5.2.3 Page settings related to user-defined errors	59
DG_USREXT_ERR1	60
DG_USREXT_ERR2	61
DG_USREXT_ERR3	62
5.3 Forwarder configuration file (dfw.conf)	63
5.4 Authentication Module configuration file (cert.conf)	64
5.4.1 User authentication	65
FEDERATION (10.0)	66
6 Troubleshooting	68
6.1 When the ticket presentation request page is displayed	68
6.2 When HTTP_AUTHORIZATION is not inherited to the Domain Gateway Option	68
6.3 When the ticket verification error page is displayed	68
6.4 When the authentication dialog (pop-up) is displayed	70
7 Logs	71
7.1 Log format	71
7.1.1 Access log format	71
7.1.2 Error log format	71
7.2 Log Message List	72
7.2.1 Access log message list	72
7.2.2 Error log message list	72

## **1 Introduction**

The Domain Gateway Option for UNIX (hereafter referred to as “Domain Gateway Option”) is an optional product that links the authentication function of IceWall SSO with Integrated Windows Authentication implemented in the Microsoft Internet Explorer (hereafter referred to as “IE”) and domain controller as well as the authentication information using Kerberos v5.

Usually, when the IceWall SSO environment is built in the Windows domain environment, the authentication process occurs twice to log in to the Windows domain environment and then IceWall SSO. Using the Domain Gateway Option enables single sign-on that requires authentication for only the Windows domain environment and not for IceWall SSO.

This guide only describes the installation procedure for the Domain Gateway Option and reference items.

Configuration of the domain controller and generation procedure of the Kerberos key are not included in the IceWall SSO support. For questions concerning the environment or SE support, consult our sales personnel.

### **1.1 Version designations in the text**

The table below gives the meanings of the version designations added to the description.

<b>Designation</b>	<b>Meaning</b>
<b>10.0</b>	An item added to the version enclosed in the square. In this case, the designation indicates the item was added to 10.0.
<b>10.0</b>	An item where the specification was changed or function added to the version enclosed in the oval mark. In this case, the designation indicates a specification change or function addition to 10.0.

## **2 Operating Environment**

The following lists the operating environment of the Domain Gateway Option for UNIX.

- OS

HP-UX 11i v3 (Itanium) **10.0**

Red Hat Enterprise Linux 5.x (“x” is 4 or later) (x86 64-bit) **10.0**

- Web server

For HP-UX 11i v3 (Itanium)

HP-UX Apache-based Web server v2.2.8 or later (64-bit) (package supplied by the OS vendor only)

For Red Hat Enterprise Linux 5.x (“x” is 4 or later) (x86 64-bit) **10.0**

Apache HTTP Server 2.2.3(64bit)

- IceWall SSO

IceWall SSO Version 10.0 or higher **10.0**

IceWall SSO Version 8.0 Agent Option 2007 Update Release 2 or later **10.0**

- Domain controller

Microsoft Windows Server 2008

Microsoft Windows Server 2008 SP2 **10.0**

Microsoft Windows Server 2008 R2 **10.0**

- Client OS **10.0**

Microsoft Windows XP SP3 (32bit)

Microsoft Windows Vista SP1 (32bit)

Microsoft Windows Vista SP2 (32bit)

Microsoft Windows 7 (32bit)

- Browser **10.0**

For Microsoft Windows XP Professional SP3

Microsoft Internet Explorer 6

Microsoft Internet Explorer 7

Microsoft Internet Explorer 8

For Microsoft Windows Vista SP1, Microsoft Windows 7

Windows Internet Explorer 7

Windows Internet Explorer 8

For Microsoft Windows 7

Windows Internet Explorer 8

\* Operation on browsers other than the above (e.g., Netscape or Firefox) is not guaranteed.

- Remarks

1. For Red Hat Enterprise Linux 5.x (“x” is 4 or later), operation with the NSA Security-Enhanced Linux (SELinux) enabled is not guaranteed.

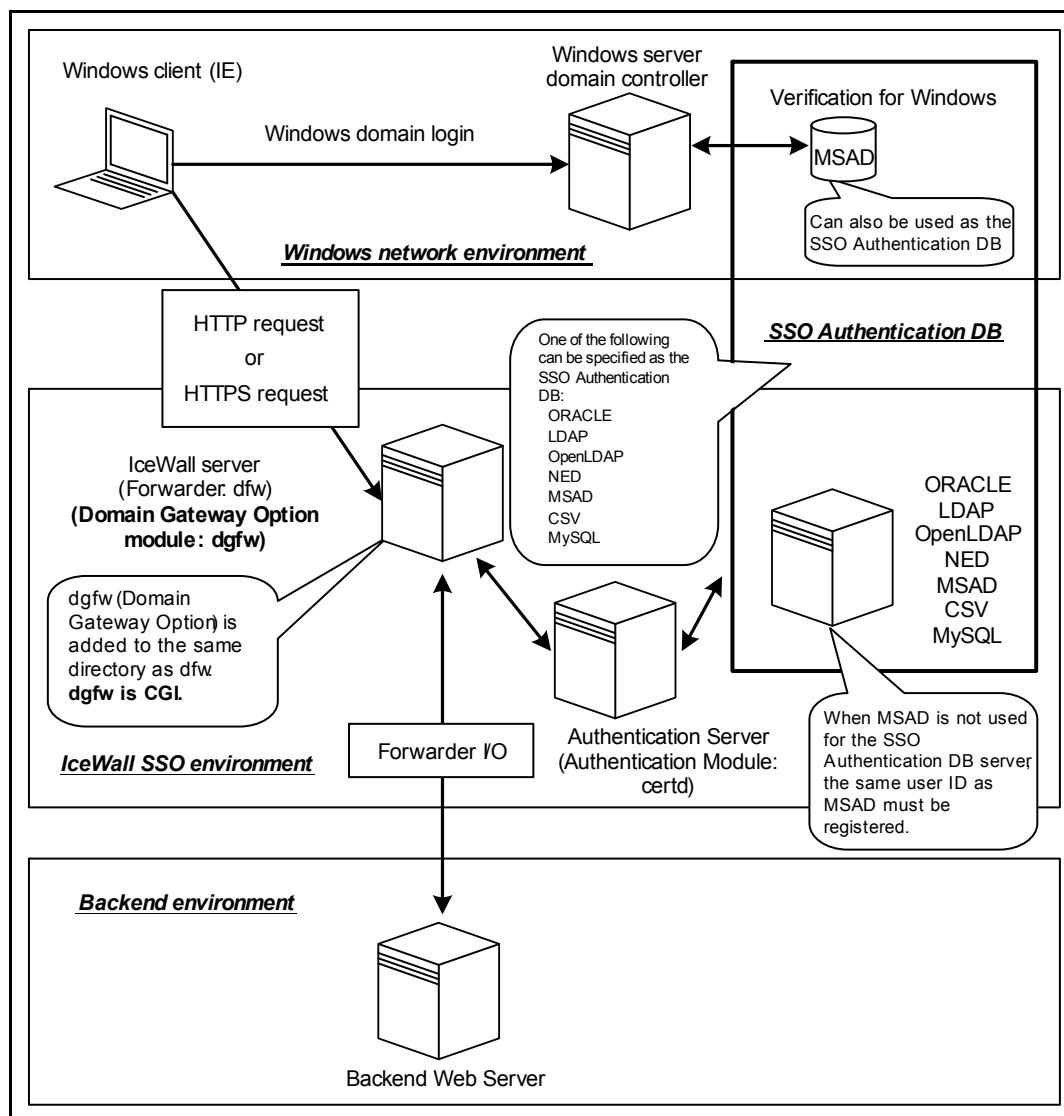
In explanations starting from the next chapter, the following terminology is used for the Web servers used by the Domain Gateway Option and databases supported by IceWall SSO.

Terminology	Corresponding products
Apache	HP-UX Apache-based Web Server Apache HTTP Server
ORACLE	Oracle Database 11g
LDAP	Sun Java System Directory Server Netscape Directory Server Red Hat Directory Server
OpenLDAP	OpenLDAP 2.4
NED	Novell eDirectory
MSAD	Microsoft Active Directory
CSV	Text Authentication DB file
MySQL	MySQL Server

### 3 Overview

This chapter gives an overview of the Domain Gateway Option for UNIX.

#### 3.1 System configuration diagram



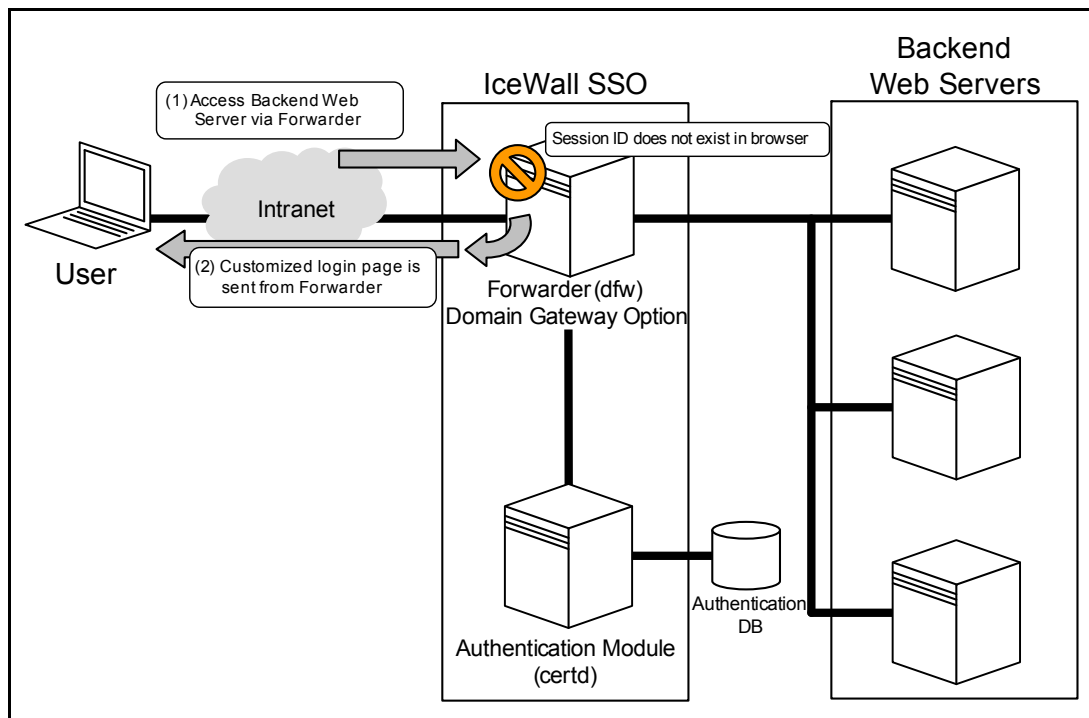


## 3.2 Transactions

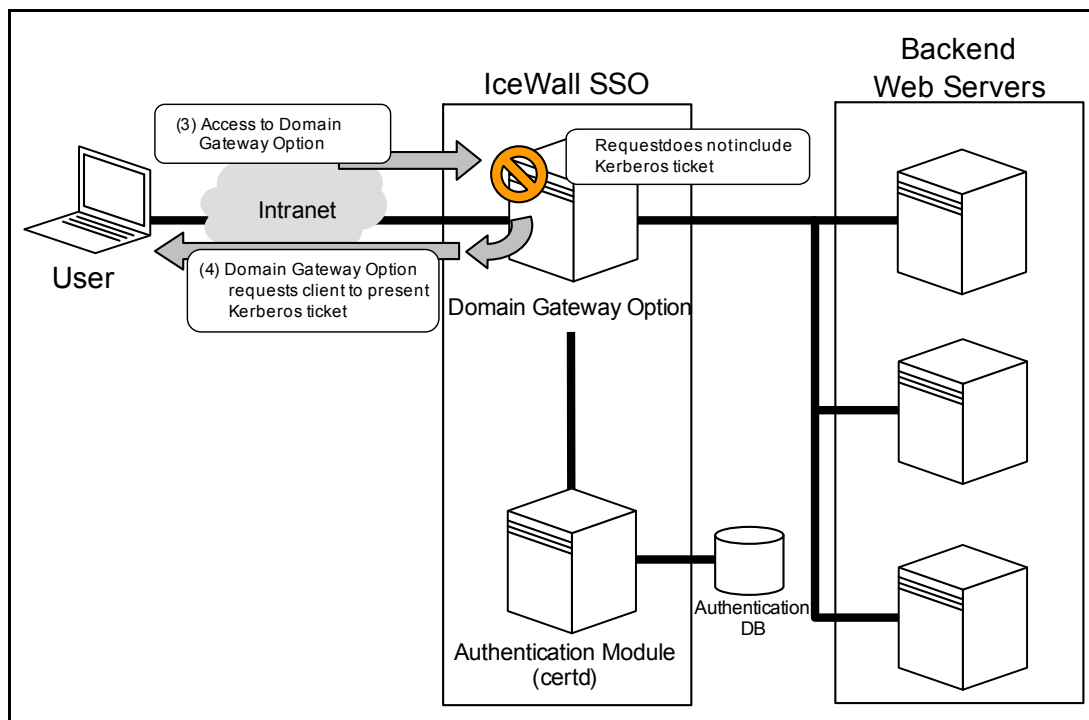
The following describes the transactions involved in the Domain Gateway Option for UNIX.

### 3.2.1 Login transaction

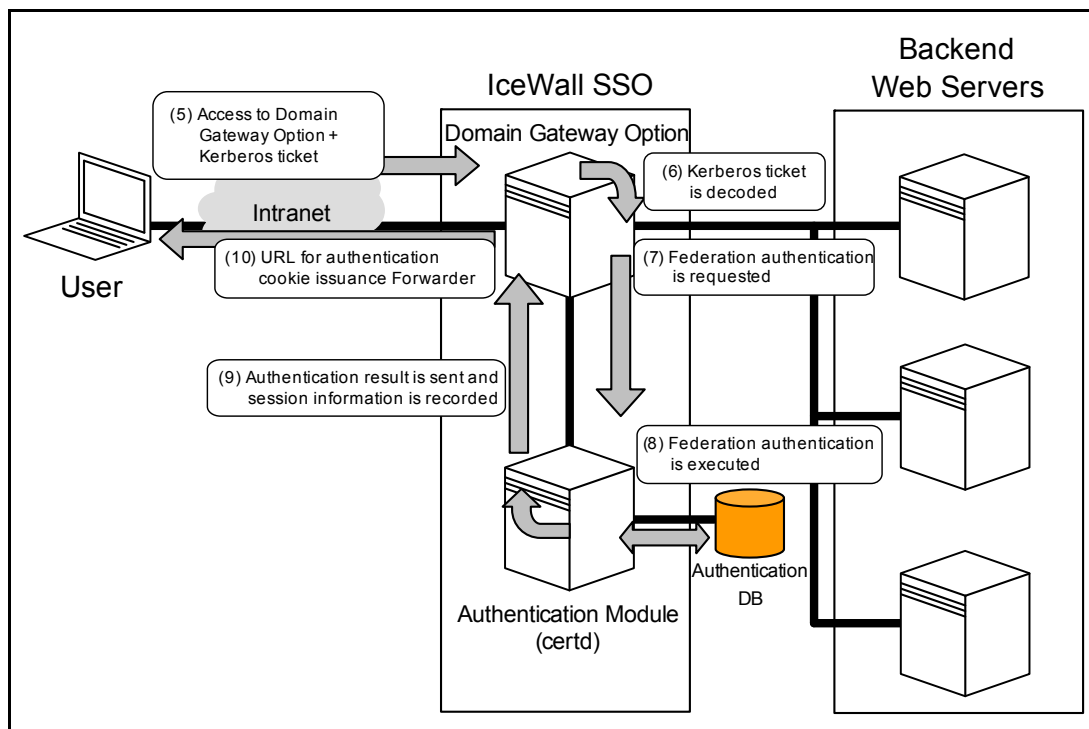
Assumption: The client has already logged in to the Windows domain.



- (1) The user enters the URL of the Backend Web Server accessed via Forwarder.
- (2) To verify the login status of the user, Forwarder verifies the HTTP request header sent by the browser to see if a session ID exists. As no session ID exists in the header for an initial access, Forwarder loads the login page and sends it to the user (if a session ID already exists, then the user is processed as a logged-in user and the process moves to the Backend Web Server screen display).



- (3) The user clicks the link to the Domain Gateway Option displayed on the login page.
- (4) Because the request header does not contain the [**Authorization: negotiate Kerberos ticket**], the Domain Gateway Option requests the client to present the Kerberos ticket. It sends the following HTTP header to request for the ticket presentation to the browser.
- Status: 401 Unauthorized**
- WWW-Authenticate: Negotiate**



(5) IE automatically browses to the URL of the Domain Gateway Option.

When IE receives the **Status: 401 Unauthorized** header, it adds [**Authorization: negotiate Kerberos ticket**] to the HTTP header and automatically browses to the last URL it accessed.

(6) The Domain Gateway Option decrypts the Kerberos ticket and acquires the user ID.

(7) The Domain Gateway Option uses the acquired user ID to request the Authentication Module for federation authentication. The federation authentication is a function to authenticate the user by the user ID only.

(8) The Authentication Module receives the request and performs federation authentication in connection with the Authentication DB.

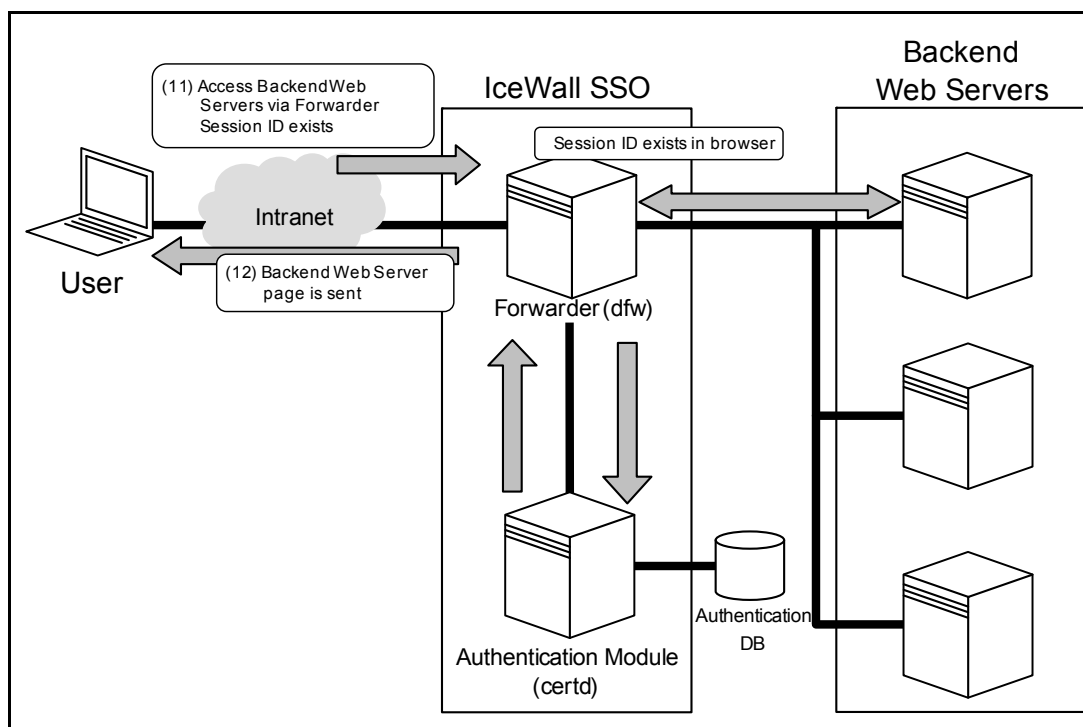
(9) The Authentication Module sends the authentication result to Domain Gateway Option and then creates and caches user session management information.

(10) If login fails, the Domain Gateway Option sends a page which shows the cause of the failure. If login is successful, the Domain Gateway Option sends the Cookie (IceWall SSO session) and the URL in (1). (Then the control returns to Forwarder.)

**Status: 302 Moved Temporarily**

**Location: URL in (1) URL of Backend Web Server accessed via Forwarder**

**Set-Cookie: IceWall SSO session ID**



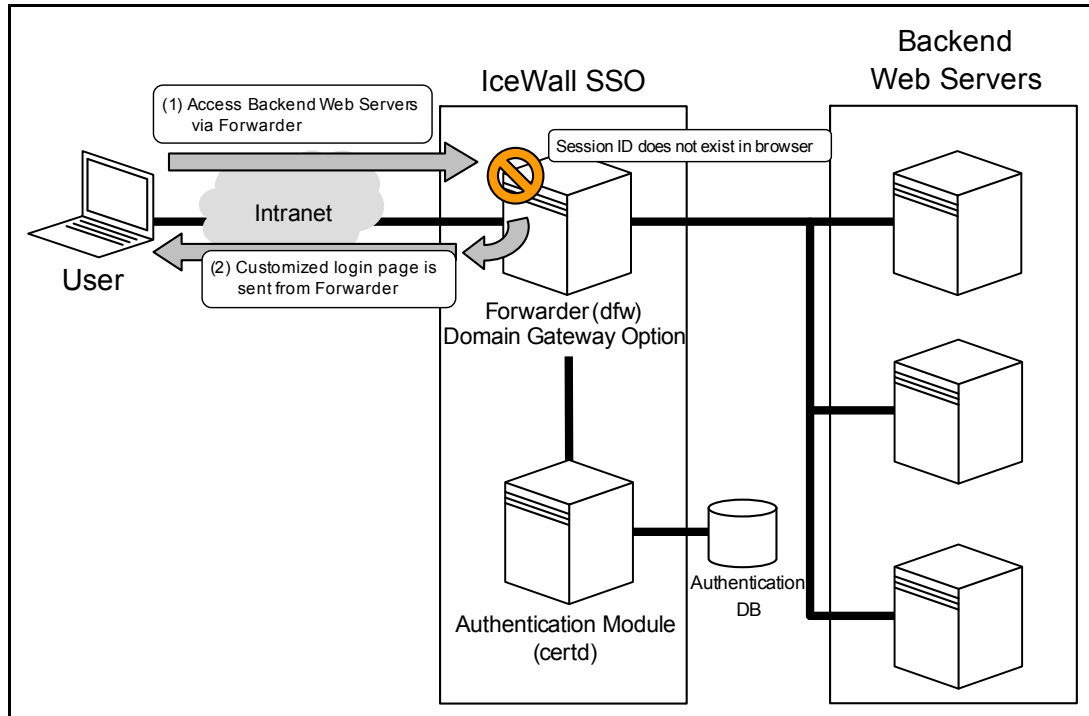
(11) IE automatically browses to the URL of Forwarder.

Forwarder normally processes the access using the session ID issued by the Domain Gateway Option.

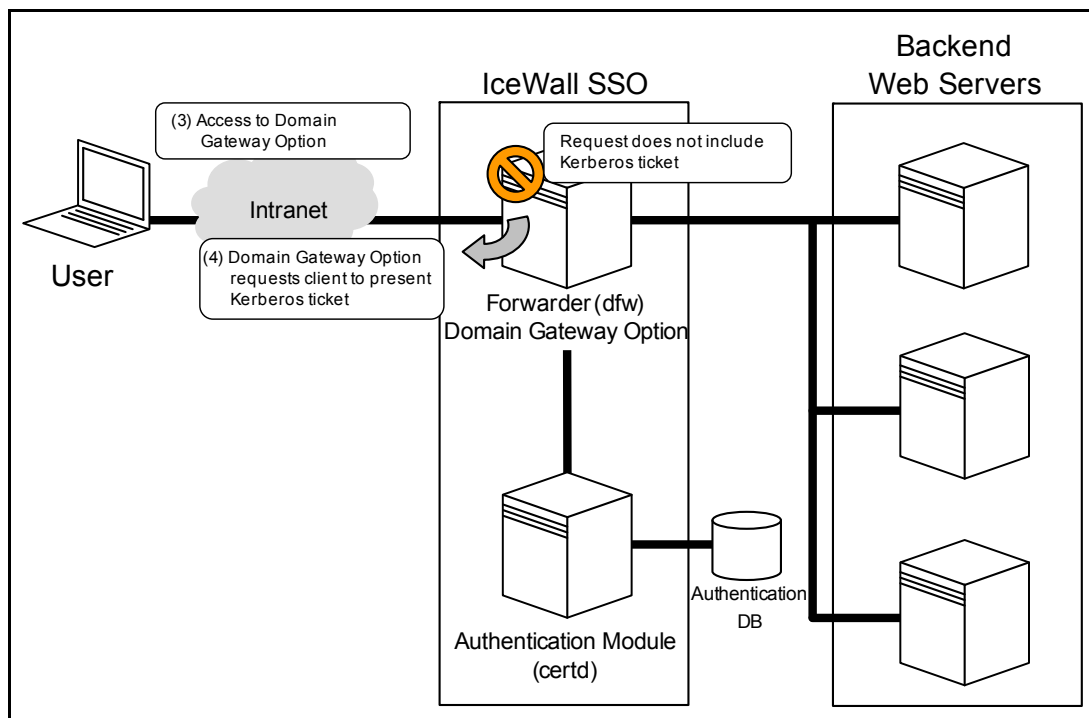
(12) The Backend Web Server screen is displayed.

### 3.2.2 Forced login transaction for duplicate login

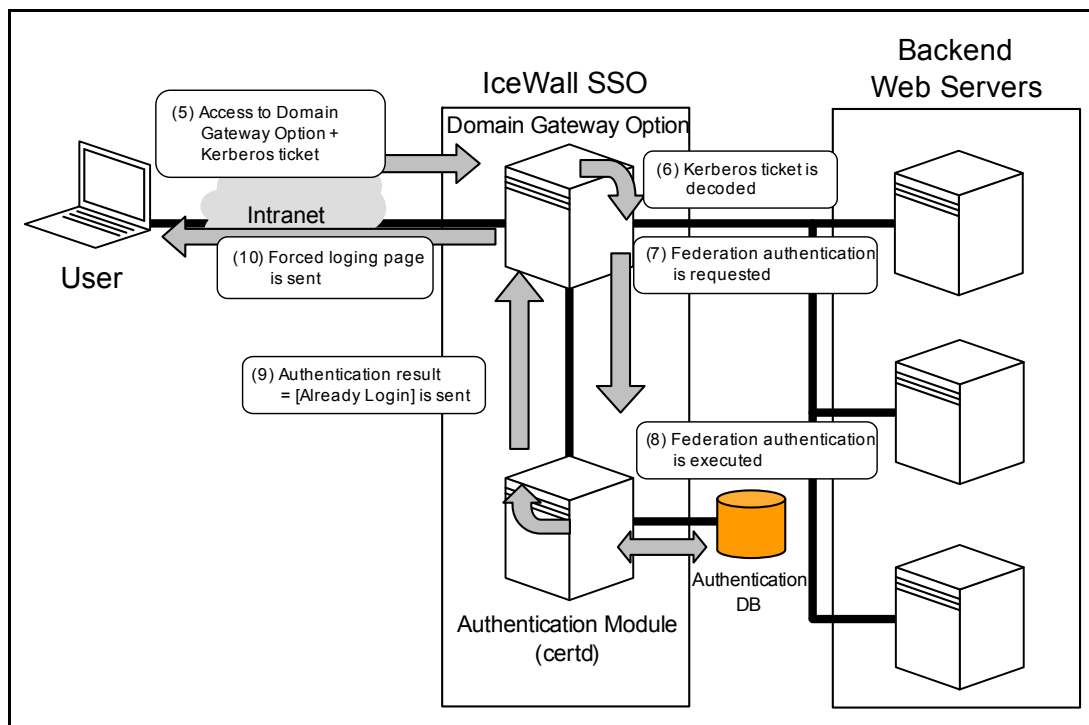
Assumption: The client has already logged in to the Windows domain.



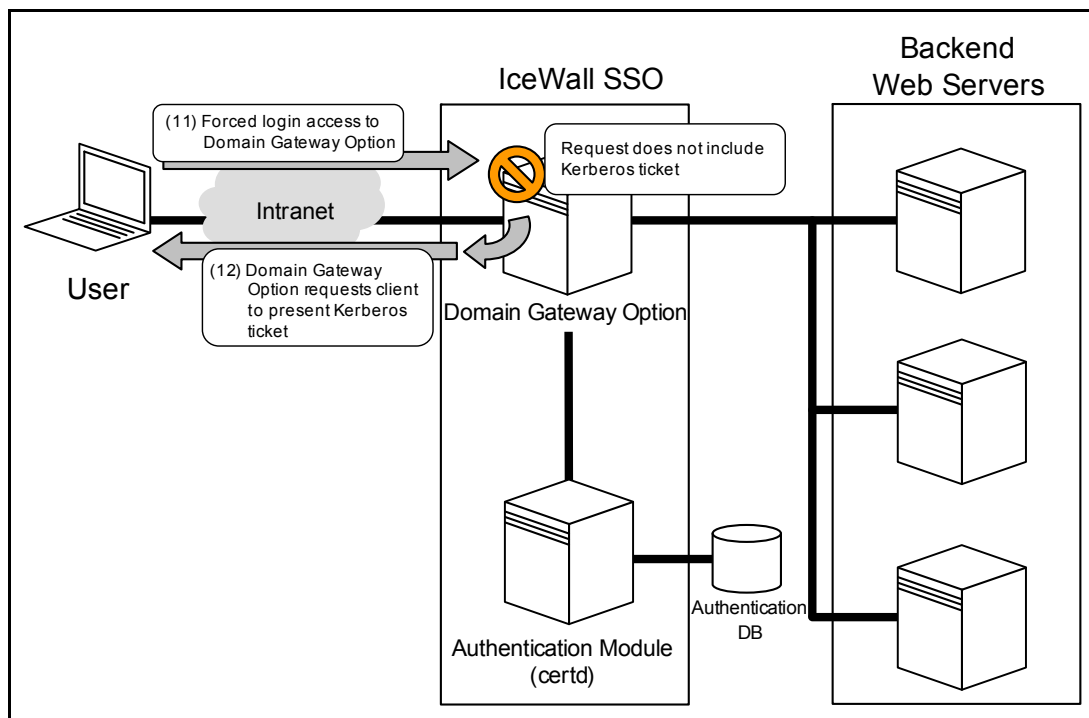
- (1) The user enters the URL of the Backend Web Server accessed via Forwarder.
- (2) To verify the login status of the user, Forwarder verifies the HTTP request header sent by the browser to see if a session ID exists. As no session ID exists in the request header for an initial access, Forwarder loads the login page and sends it to the user (if a session ID already exists, then the user is processed as a logged-in user and the process moves to the Backend Web Server screen display).



- (3) The user clicks the link to the Domain Gateway Option displayed on the login page.
- (4) Because the request header does not contain the [**Authorization: negotiate Kerberos ticket**], the Domain Gateway Option requests the client to present the Kerberos ticket. It sends the following HTTP header to request for the ticket presentation.
- Status: 401 Unauthorized**
- WWW-Authenticate: Negotiate**

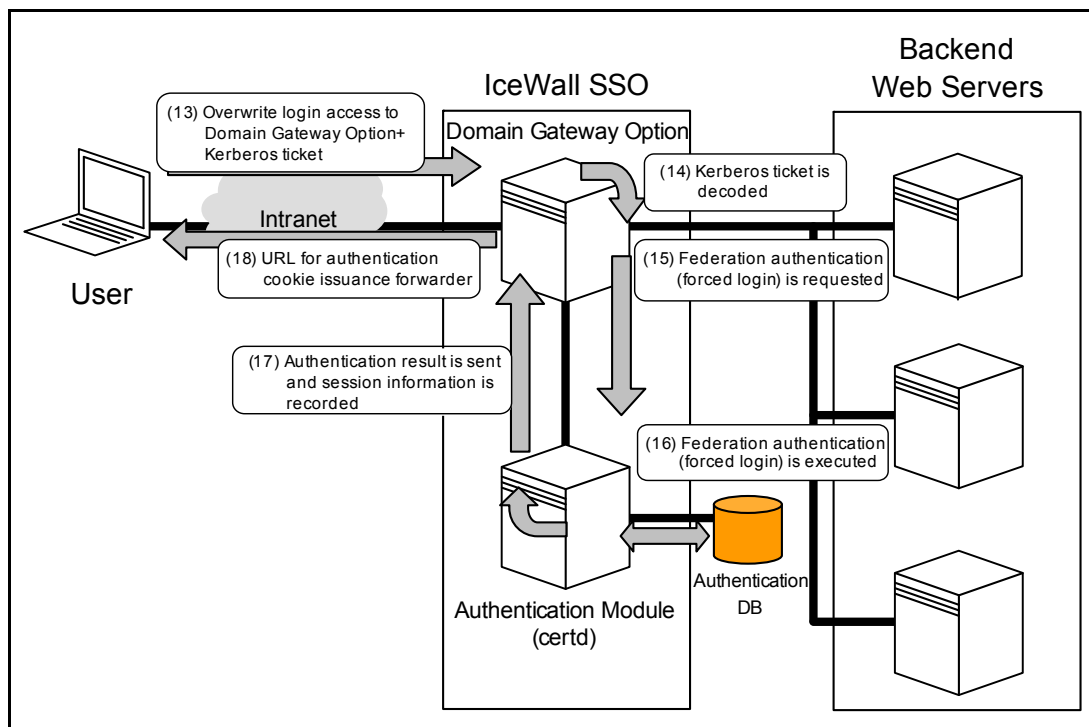


- (5) IE automatically browses to the URL of the Domain Gateway Option.  
When IE receives the **Status: 401 Unauthorized** header, it adds **[Authorization: negotiate Kerberos ticket]** to the HTTP header and automatically browses to the last URL it accessed.
- (6) The Domain Gateway Option decrypts the Kerberos ticket and acquires the user ID.
- (7) The Domain Gateway Option uses the acquired user ID to request the Authentication Module for federation authentication. The federation authentication is a function to authenticate the user by the user ID only.
- (8) The Authentication Module receives the request and performs federation authentication in connection with the Authentication DB.
- (9) The Authentication Module sends “Already Login” to the Domain Gateway Option.
- (10) Domain Gateway Option sends the Forced Login page for the “Already Login” from the Authentication Module.



- (11) IE browses to the URL of the Forced Login page for the Domain Gateway Option.
- (12) Because the request header does not contain the [**Authorization: negotiate Kerberos ticket**], the Domain Gateway Option requests the client to present the Kerberos ticket. It sends the following HTTP header to request for the ticket presentation.
- Status: 401 Unauthorized**
- WWW-Authenticate: Negotiate**





(13) IE automatically browses to the URL of the Domain Gateway Option.

When IE receives the **Status: 401 Unauthorized** header, it adds

[**Authorization: negotiate Kerberos ticket**] to the HTTP header and automatically browses to the last URL it accessed.

(14) The Domain Gateway Option decrypts the Kerberos ticket and acquires the user ID.

(15) The Domain Gateway Option uses the acquired user ID to request the Authentication Module for federation authentication (forced login).

(16) The Authentication Module receives the request and performs federation authentication (forced login) in connection with the Authentication DB.

(17) The Authentication Module sends the authentication result to Domain Gateway Option and then creates and caches user session management information.

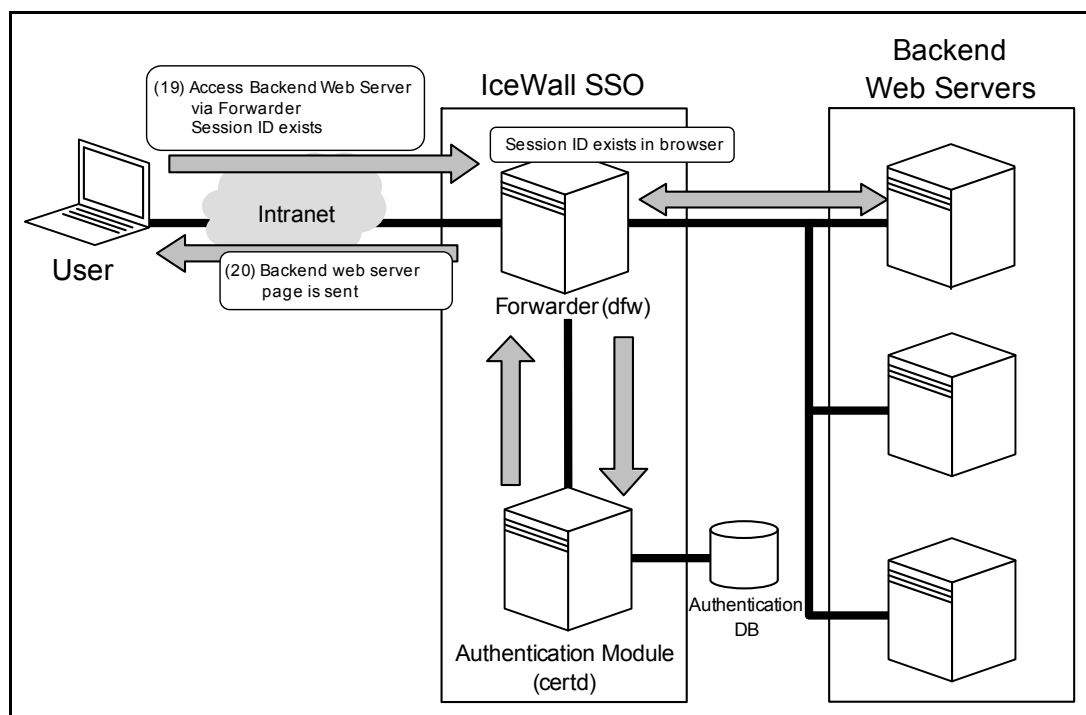
(18) If the login fails, the Domain Gateway Option sends a page which shows the cause of the failure.

If the login succeeds, the Domain Gateway Option sends the Cookie (IceWall SSO session) and the URL in (1). (Then the control returns to Forwarder.)

**Status: 302 Moved Temporarily**

**Location: URL in (1) URL of Backend Web Server accessed via Forwarder**

**Set-Cookie: IceWall SSO session ID**



(19) IE automatically browses to the URL of Forwarder.

Forwarder normally processes the access using the session ID issued by the Domain Gateway Option.

(20) The Backend Web Server screen is displayed.

### 3.3 Restrictions on the Domain Gateway Option

Some restrictions are applied to the Domain Gateway Option.

#### 3.3.1 Remarks about authentication by the Domain Gateway Option

- Because the Domain Gateway Option uses only the user ID for authentication, the password change function of IceWall SSO cannot be used.
- Because the Domain Gateway Option uses only the user ID for authentication, the SSO authentication password is blank.  
For the authentication information used when performing the basic and/or form authentication with the Backend Web Server, be sure to specify the column which contains a valid password.

#### 3.3.2 Restrictions on using the Authentication DB

When MSAD and NED process an authentication request from Forwarder, they use the BIND authentication (LDAPBIND=1) for accessing the Authentication DB of the Authentication Module. This setting must be changed so that BIND is not used (LDAPBIND=0) when processing an authentication request from the Domain Gateway Server.

For this reason, when a single Authentication Module is used to process user authentication from Forwarder as well as authentication requests from the Domain Gateway Option, MSAD and NED cannot be used as the Authentication DB.

#### 3.3.3 Notes on proxy server

When a proxy server is placed between the client and the Domain Gateway Option, be sure to use a proxy server which can pass a request header which contains the **Authorization: negotiate Kerberos ticket**.

#### 3.3.4 Authentication Module receive timeout

The Authentication Module receive timeout value for the Domain Gateway Option is **fixed to 600 seconds**.

#### 3.3.5 Combination with failover option ⑩

After the Domain Gateway Option has tried to connect to the Primary Authentication Module for the specified number of retries at the specified retry interval, it tries to connect to the Secondary Authentication Module. (It works similarly as Forwarder.)

When Forwarder succeeds in connecting to the Secondary Authentication Module, it changes the CERT parameter in the Forwarder configuration file (dfw.conf) as follows:

CERT=secondary authentication module,primary authentication module

If load balancing is used, Forwarder changes the CERTLB parameter in the Forwarder configuration file (dfw.conf) as follows:

CERTLB=authentication module identification key=secondary authentication module,primary authentication module

The Domain Gateway Option does not change the CERT and CERTLB parameters in the Forwarder configuration file. Therefore, failover may take a longer time than it does with the Forwarder alone.

### **3.3.6 Combining with Automatic Form Authentication of IceWall SSO**

While the user ID and password entered when the user logged in to IceWall SSO can be used during the execution of Automatic Form Authentication, the Domain Gateway Option uses federation authentication for the Authentication Module instead of using the user ID and password.

Because federation authentication uses only the user ID, the Authentication Module does not retain information equivalent to the login password. For this reason, note that you cannot set a login password (DEFAULTPWD) when using the Automatic Form Authentication.

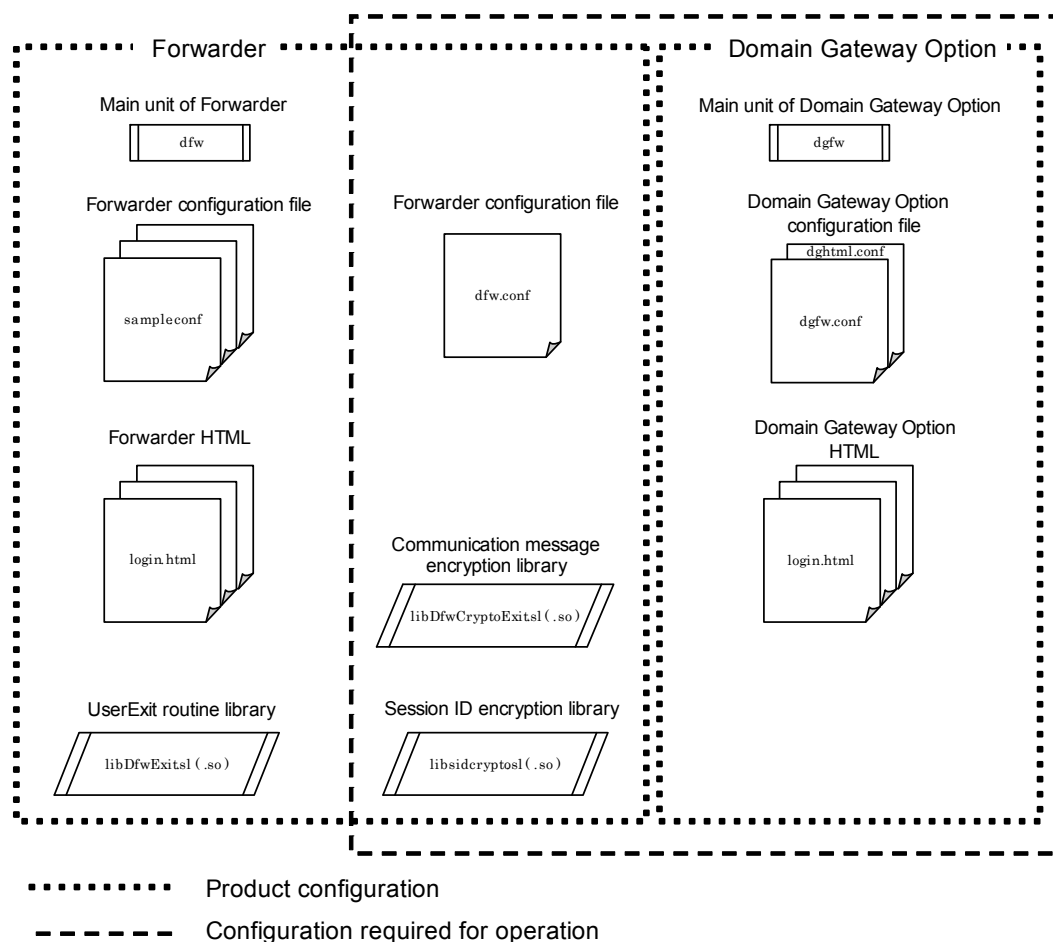
### **3.3.7 Transaction ID 10.0**

A transaction ID is a unique ID assigned to a request from the client. On ICP 2.0, because each transaction ID is notified to the Authentication Module, you can use the transaction ID from the output of the Authentication Module to identify the relationship among the log files.

## 4 Installing the Domain Gateway Option

### 4.1 IceWall server configuration

As an additional module of Forwarder, the Domain Gateway Option shares some of the configuration files and libraries with Forwarder. The IceWall server configuration after installing the Domain Gateway Option is described below.



### 4.2 Prerequisites for installing the Domain Gateway Option

Perform the following before installing the Domain Gateway Option:

- Install Forwarder.  
Ensure that the session encryption library bundled with Forwarder is installed.  
Ensure that the communication message encryption library bundled with Forwarder is installed.

OS	Library and link
Red Hat Enterprise Linux 5.x ("x" is 4 or later) (x86 64-bit) <b>10.0</b>	/opt/icewall-ss0/lib/dfw/libsidcrypto.so /libsidcrypto.sl /libCryptoExit.so <b>10.0</b> /libDfwCryptoExit.sl <b>10.0</b>
HP-UX 11i v3 (Itanium 64bit) <b>10.0</b>	/opt/icewall-ss0/lib/dfw/libsidcrypto.sl /libsidcrypto.sl /libCryptoExit.so <b>10.0</b> /libDfwCryptoExit.sl <b>10.0</b>

- Ensure that the GSS-API shared library bundled with the OS is installed.

OS	Library and link
Red Hat Enterprise Linux 5.x ("x" is 4 or later) (x86 64-bit) <b>10.0</b>	/usr/lib64/ libgssapi_krb5.so
HP-UX 11i v3 (Itanium 64bit) <b>10.0</b>	/usr/lib/hpux64/libgssapi_krb5.sl

### 4.3 Installing the Domain Gateway Option

The following describes how to install the Domain Gateway Option. The procedure depends on the type of OS.

#### 4.3.1 Installing Linux edition

Install the Domain Gateway Option with the following procedure:

- (1) Log in as root user to the server where the Domain Gateway Option is to be installed.
- (2) Insert the IceWall SSO CD-ROM into the CD-ROM drive.

- (3) Mount the CD-ROM using the following command.

- Red Hat Enterprise Linux 5.x ("x" is 4 or later) (x86 64-bit)

```
# mount -t iso9660 /dev/cdrom /mnt/cdrom
```

- (4) Enter the following command to install the option.

```
# rpm -ivh --nodeps /mnt/cdrom/SSO/linux/IceWall-SSO-dgfw_e-10.0-1.x86_64.rpm
```

- (5) Check if the option has been installed using the following command.

```
# rpm -qa | grep "IceWall-SSO-dgfw"
```

- (6) Change the owner of the directories and files related to the Domain Gateway Option and Forwarder to the user who is running the Web Server. This example assumes that the user running Apache is apache:apache.

```
# chown -R apache:apache /opt/icewall-ss0/dfw
```

#### **4.3.2 Installing HP-UX edition**

Install the Domain Gateway Option in the following procedure.

- (1) Log in as root to the server where the Domain Gateway Option is being installed.

- (2) Insert the IceWall SSO CD-ROM into the CD-ROM drive.

- (3) Check the CD-ROM drive's device file name using the following command:

```
# ioscan -fn | more
```

- (4) Mount the CD-ROM using the following command.

```
# mount [device file name] [mount point]
```

Example: When the device file name is “:/dev/dsk/c1t2d0” and the mount point is

```
“SD_CDROM” # mount -o rr /dev/dsk/c1t2d0 /SD_CDROM
```

```
# mount /dev/dsk/c1t2d0 /SD_CDROM
```

(If the SD\_CDROM directory does not exist, create it with the mkdir command.)

- (5) Specify the option name of each module to be installed and install them using the following command:

```
# swinstall -s /SD_CDROM/SSO/hpux/IceWall-SSO-ia64_e.sw dgfw
```

- (6) Check if the option has been installed using the following command.

```
# swlist dgfw
```

- (7) Change the owner of the directories and files related to the Domain Gateway Option and Forwarder to the user who is running the Web Server. This example assumes that the user

running Apache is apache:apache.

```
# chown -R apache:apache /opt/icewall-ssso/dfw
```

#### 4.4 Checking the installed files

The Domain Gateway Option is installed under the /opt/icewall-ssso directory. Check the file configuration under the /opt/icewall-ssso directory after installation.

Directory and file names (permission)			
/dfw(775)	/cgi-bin(775)	dgfw(755) dgfw.conf(644) dghtml.conf(644)	
	/dghtml(755)	/image(755)	arrow.gif(444) curve_b.gif(444) curve_r.gif(444) error.gif(444) footer.gif(444) header.gif(444) title_b.gif(444) title_r.gif(444)
		login.html(644) login_tkt.html (644) login_force_tkt.html (644) login_addr_error.html (644) login_userid_error.html (644) login_tkt_error.html (644) login_cert_error.html (644) login_lock_error.html (644) login_group_error.html (644) login_stop.html (644) login_limit_error.html (644) logout.html (644) system_busy_database.html (644) system_error.html (644) system_certd_error.html (644) system_ldap_error.html (644) system_timeout_certd.html (644) usr_ext1.html (644) usr_ext2.html (644) usr_ext3.html (644)	
		/js (755)	script.js (755)
/logs(777)			



## **4.5 Confirming the version information**

After installation, check the version information of each module to confirm that the binary for this version has been installed. This information is also necessary when you contact our customer support in the case of any problem.

### **4.5.1 Confirmation procedure of Linux edition**

The confirmation procedure is as follows:

- (1) Log in as root user to the server where the module has been installed.
- (2) Move to the directory where the binary exists.

```
# cd /opt/icewall-ssso/dfw/cgi-bin
```

- (3) Enter the following command:

```
# strings dgfw | grep '@(#)'
```

- (4) The following information is displayed:

```
@(#)IceWall SSO dgfw
@(#)Version: 10.00.00.xxxxxxxX
@(#)OS : Linux 2.6.18
@(#)CPU: x86_64
@(#)Bit: 64bit
@(#) (c) Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
```

### **4.5.2 Confirmation procedure for HP-UX edition**

The confirmation procedure is as follows:

- (1) Move to the directory where the binary exists.

```
# cd /opt/icewall-ssso/dfw/cgi-bin
```

- (2) Enter the following command:

```
# what dgfw
```

(3) The following information is displayed:

```
dgfw:
      Version: 10.00.00.xxxxxxxX
      OS : HP-UX B.11.23
      CPU: Itanium
      Bit: 64bit
      (c) Copyright 2001-2010 Hewlett-Packard Development
```

## **4.6 Uninstallation**

The following describes how to uninstall the Domain Gateway Option. The procedure depends on the type of OS.

### **4.6.1 Linux edition**

Uninstall the Domain Gateway Option with the following procedure:

- (1) Log in as root user to the server where the Domain Gateway Option is to be uninstalled.
- (2) Enter the following command:

```
# rpm -e IceWall-SSO-dgfw_e
```

### **4.6.2 HP-UX edition**

Uninstall the Domain Gateway Option with the following procedure:

- (1) Log in as root user to the server where the Domain Gateway Option is to be uninstalled.
- (2) Specify the option(s) specified upon installation and uninstall the module(s) using the following command:

```
# swremove dgfw
```

## **4.7 Configuring the Web server**

The following describes how to configure the Web server for the Domain Gateway Option to run.

Parameters	Overview
Authorization environment variable inheritance setting	With the default setting of Apache, the Authorization header in an HTTP request header is not inherited as an environment variable to CGI. Use the mod_rewrite (a standard module supplied with Apache) to inherit the Authorization header as <b>"HTTP_AUTHORIZATION"</b> environment variable.
Alias setting of image file directory	Define the path to the image file used by the template HTML supplied with the Domain Gateway Option using the Alias syntax. Describe the URL prefix in the template HTML image file using <b>/imgd</b> .
Shared library directory path environment variable setting	Use the SetEnv syntax to define the path to the directory where the shared libraries used by the Domain Gateway Option exist as an environment variable.
Domain Gateway Option CGI startup setting	Configure the Domain Gateway Option so that it can be started via CGI. Use the ScriptAlias syntax. Usually, use the setting configured when Forwarder was installed.

Use the following sample settings for these configuration parameters.

```
① LoadModule rewrite_module modules/mod_rewrite.so

User apache
Group apache

② RewriteEngine on
③ RewriteRule /fw/dgfw(.*) /fw/dgfw$1
[PT,E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

Alias /img/ "/opt/icewall-ssso/dfw/html/image/"
④ Alias /imgd/ "/opt/icewall-ssso/dfw/dghtml/image/"

⑤ SetEnv LD_LIBRARY_PATH "/opt/icewall-ssso/lib/dfw:/usr/lib64"

⑥ ScriptAlias /fw/ "/opt/icewall-ssso/dfw/cgi-bin/"
⑦ <Directory "/opt/icewall-ssso/dfw/cgi-bin">
    AllowOverride All
    Options ExecCGI
    SetHandler cgi-script
    Order allow,deny
    Allow from all
</Directory>
```

Parameters	Overview
Authorization environment variable inheritance setting	<p>① Load the mod_rewrite module. If ClearModule is set, describe this definition after ClearModule.</p> <p>② Enable the mod_rewrite module.</p> <p>③ Enable the acquisition of the Authorization header in each HTTP request as the HTTP_AUTHORIZATION environmental variable.</p>
Alias setting of image file directory	<p>④ Use the Alias syntax.</p> <p>* For HP-UX, the following definition is further necessary. (10.0)</p> <pre>&lt;Directory "/opt/icewall-ssso/dfw/dghtml/image/"&gt;     Order allow,deny     Allow from all &lt;/Directory&gt;</pre> <p>Without this setting, the target image file cannot be accessed.</p>
Shared library directory path environment variable setting (10.0)	<p>⑤ Check the path to the directory where the shared libraries used by the Domain Gateway Option exist.</p> <p>For HP-UX</p> <p>* In HP-UX, it is assumed that the SHLIB_PATH environment variable is set to "/opt/icewall-ssso/dfw/lib" and "/usr/lib/hpux64" when Forwarder was installed.</p> <p>For Linux</p> <p>* In Linux, it is assumed that the LD_LIBRARY_PATH environment variable is set to "/opt/icewall-ssso/dfw/lib" and "/usr/lib64" when Forwarder was installed.</p>
Domain Gateway Option CGI startup setting (10.0)	<p>⑥ Configure the Domain Gateway Option such that it can be started via CGI. This setting is common to the Domain Gateway Option and Forwarder.</p>

#### 4.8 Configuring Forwarder

Modify Forwarder html configuration file as follows to make the Domain Gateway Option perform authentication on behalf of Forwarder.

- (1) Move to the directory where the configuration file exists.

```
# cd /opt/icewall-ssso/dfw/cgi-bin
```

(2) Enter the following command:

```
# vi html.conf
```

(3) Perform the following modification. Change the bold part.

```
LOGIN_UID=file:///opt/icewall-ssso/dfw/dghtml/login.html
```

## **4.9 Configuring the Authentication Module**

Modify the Authentication Module configuration file such that authentication requests from the Domain Gateway Option can be processed by the Authentication Module.

### **4.9.1 Configuring federation authentication in the Authentication Module**

Define the IP address of the Domain Gateway Option server in the Authentication Module to process authentication requests from the Domain Gateway Option.

Sample configuration (when the IP address of the Domain Gateway Option is 192.168. 0.10)

```
FEDERATION=192.168.0.10
```

Restart the Authentication Module after modifying the configuration file to make modification effective .

### **4.9.2 Configuring LDAPBIND in the Authentication Module**

When the Authentication DB is other than Oracle or CSV, set the LDAPBIND parameter of the Authentication Module as follows:

```
LDAPBIND=0
```



## 5 Domain Gateway Option Reference

This chapter describes the parameters and their available settings in the configuration file used by the Domain Gateway Option.

- The following describes the format rules and restrictions common to all configuration files.
- Configuration files are text files.
- Lines beginning with “#” are comment lines.
- Lines with invalid parameter names are ignored.
- Indented lines are ignored (indentation is not allowed).
- Parts of the format enclosed by brackets “[ ]” can be omitted.
- Ellipses “...” in the format indicate that a series of items can be specified.
- Up to 4095 characters can be specified in a single line. This limit includes the parameter name.

**In the following description, a “default value” refers to a value of a parameter which is not defined in the configuration file.** Note that some of the initial values of the configuration file installed by default may be different from the default values.

## **5.1 Domain Gateway Option configuration file (dgfw.conf)**

**Overview** This configuration file configures the values needed to run the Domain Gateway Option, as well as the shared settings used by the entire system.  
The parameters available to the user are as follows:

Parameter group	Parameter name
Basic configuration	ALEVEL
	ELEVEL
	ACCESS
	ERROR
	TRACE
	TRANSID <b>10.0</b>
	TRANSID_STR <b>10.0</b>
	DOCS
	SERVICE_NAME
	USERNAME_FRM

**Storage location** The following is the default storage location:  
/opt/icewall-ssso/dfw/cgi-bin/dgfw.conf

**Remarks** To change the file name and location of the Domain Gateway Option configuration file, set the path to the required file using the environment variable IWDGFWCONFIG for the Web server where the Domain Gateway Option runs. **10.0**  
(Sample) To specify dgfw\_01.conf in the /opt/icewall-ssso/dfw/config directory as the Domain Gateway Option configuration file  
Set the environment variable IWDGFWCONFIG for the Web server where the Domain Gateway Option runs to “/opt/icewall-ssso/dfw/config/dgfw\_01.conf.”

The following pages describe these parameters.



### 5.1.1 Basic configuration

These parameters are used to configure the basic settings of the Domain Gateway Option.

Parameter name	Mandatory	Overview
ALEVEL	×	Sets the access log output level.
ELEVEL	×	Sets the error log output level.
ACCESS	×	Sets the access log file name.
ERROR	×	Sets the error log file name.
TRACE	×	Sets the trace log file name.
TRANSID <b>10.0</b>	×	Sets the transaction ID output.
TRANSID_STR <b>10.0</b>	×	Sets the module identification string contained in the transaction ID.
DOCS	×	Sets the template HTML file name.
SERVICE_NAME	×	Sets the service name.
USERNAME_FRM	×	Sets the user ID format in the ticket.

For details on these parameters, see the following pages.

## ALEVEL

Overview	Sets the access log output level.
Format	<b>ALEVEL=access log level</b> <ul style="list-style-type: none"><li>• One of the following values can be specified for this parameter:<ul style="list-style-type: none"><li>0 : No output</li><li>1 : Output basic information only</li><li>2 : Output basic information and client IP address</li></ul></li><li>• The default value in the execution binary is 1.</li><li>• The default value for the default configuration file is 2.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	1) To output only basic access log information in the access log: <b>ALEVEL=1</b>
Remarks	None.
See also	ACCESS (Domain Gateway Option configuration file)

## ELEVEL

Overview	Sets the error log output level.
Format	<b>ELEVEL=error log level</b> <ul style="list-style-type: none"><li>• One of the following values can be specified for this parameter:<ul style="list-style-type: none"><li>0 : No output</li><li>1 : Only fatal errors (Fatal)</li><li>2 : Fatal errors and warnings (Warning)</li></ul></li><li>• The default value in the execution binary is 1.</li><li>• The default value for the default configuration file is 2.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	1) To output fatal errors and warnings in the error log: <b>ELEVEL=2</b>
Remarks	None.
See also	ERROR (Domain Gateway Option configuration file)

## ACCESS

Overview	Sets the access log file name.
Format	<b>ACCESS=access log file name</b> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/logs/dgfw.log.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/logs/dgfw.log.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	1) To output to a standard access log file: <b>ACCESS=/opt/icewall-ssso/logs/dgfw.log</b>
Remarks	<ul style="list-style-type: none"><li>• If the file set by this parameter does not exist, a new file is created. If the file exists, the log is added to the end of that file.</li><li>• The owner and permission of the file specified with this parameter requires the Web Server user who runs the Domain Gateway Option to have the write permission for it.</li><li>• If this parameter is not set, the information is output to the file specified by the default value.</li></ul>
See also	ALEVEL (Domain Gateway Option configuration file)

## ERROR

Overview	Sets the error log file name.
Format	<b>ERROR=error log file name</b> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/logs/dgfwerr.log.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/logs/dgfwerr.log.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	1) To output to a standard error log file: <b>ERROR=/opt/icewall-ssso/logs/dgfwerr.log</b>
Remarks	<ul style="list-style-type: none"><li>• If the file set by this parameter does not exist, a new file is created. If the file exists, the log is added to the end of that file.</li><li>• The owner and permission of the file specified with this parameter requires the Web Server user who runs the Domain Gateway Option to have the write permission for it.</li><li>• If this parameter is not set, the information is output to the file specified by the default value.</li></ul>
See also	ELEVEL (Domain Gateway Option configuration file)

## TRACE

Overview	Sets the log file name for the trace log.
Format	<p><b>TRACE=trace log file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• If this parameter is not set, no trace log file is created.</li><li>• The default value for the default configuration file is not specified. (Comment line)</li></ul>
Configuration example	<p>1) To output to a standard trace log file:</p> <p><b>TRACE=/opt/icewall-ss0/logs/dgfwtrace.log</b></p>
Remarks	<ul style="list-style-type: none"><li>• If the file set by this parameter does not exist, a new file is created. If the file exists, the log is added to the end of that file.</li><li>• The owner and permission of the file specified with this parameter requires the Web Server user who runs the Domain Gateway Option to have the write permission for it.</li><li>• Setting this parameter causes a reduction in the performance of the Domain Gateway Option.</li><li>• Normally there is no need to set this parameter. It should be set only in situations such as confirming operation during installation or when providing information to technical support.</li><li>• Note that HP shall not be able to answer inquiries regarding the content of the trace log file.</li></ul>
See also	None

---

Domain Gateway Option configuration file (dgfw.conf)

---

## TRANSID 10.0

**Overview** Sets whether or not to output the transaction ID as additional information to each log file of Domain Gateway Option

This parameter is available with version 10.0 or later.

**Format** **TRANSID=flag**

- One of the following values can be specified for the flag:
  - 0 : Output no transaction ID to log (for backward compatibility)
  - 1 : Output transaction ID to log
- The default value in the execution binary is 0.
- The default value for the default configuration file is 1.
- The default value in the execution binary is used when the configuration file contains no line to set the value or a value outside the available range is specified.
- If multiple lines are set, only the last line is valid.

**Configuration example** 1) When the transaction ID is output as additional information to the Domain Gateway Option  
**TRANSID=1**

**Remarks**

- The transaction ID is used for comparison with log files output from the Authentication Module for a single client access.
- If this parameter is set to 1, the transaction ID is output as additional information to the error, access, and trace logs.  
(Example) For error log  
[2010/01/01 12:00:00] Fatal: Error Log Message. [userid] (pid)  
TID=xxxxxxxx [EG00000-00000]
- When this parameter is set to 1, the Domain Gateway Option notifies the Authentication Module of the transaction ID. The transaction ID is not output if the ICP\_VERSION parameter is not set to 2.0.
- If the TRANSID parameter is set to 1 in the Authentication Module configuration file, the transaction ID output to each log of the Domain Gateway Option is also output to each log of the Authentication Module.

**See also** TRANSID\_STR (Domain Gateway Option configuration file)  
ICP\_VERSION (Forwarder configuration file)

TRANSID (Authentication Module configuration file)



---

Domain Gateway Option configuration file (dgfw.conf)

---

## TRANSID\_STR 10.0

**Overview** Sets the string included in the generated transaction ID to identify which instance of the Domain Gateway Server issued the transaction ID.

This parameter is available with version 10.0 or later.

**Format** **TRANSID\_STR=identification string**

- The identification string can be specified within the range of 1 to 16 characters.
- a to z, A to Z, and 0 to 9 can be used.
- The default value in the execution binary is dgfw.
- The default value for the default configuration file is dgfw01.
- The default value in the execution binary is used when the configuration file contains no line to set the value.
- If multiple lines are set, only the last line is valid.

**Configuration example** 1) To set the identification string of Domain Gateway Option included in transaction ID

**TRANSID=1**  
**TRANSID\_STR=iwdgfw01**

**Remarks**

- When the TRANSID parameter is set to 0, this parameter is disabled.
- When multiple instances of the Domain Gateway Option are running, assign a unique identification string to each instance.

**See also** TRANSID (Domain Gateway Option configuration file)  
TRANSID (Authentication Module configuration file)

## DOCS

Overview	Specifies the Domain Gateway Option HTML configuration file name that defines the template HTML used by the Domain Gateway Option.
Format	<p><b>DOCS=HTML configuration file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ss0/dfw/cgi-bin/dghtml.conf.</li><li>• The default value in the default configuration file is //opt/icewall-ss0/dfw/cgi-bin/dghtml.conf.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) When using HTML configuration file installed by default <b>DOCS=/opt/icewall-ss0/dfw/cgi-bin/dghtml.conf</b></p>
Remarks	<ul style="list-style-type: none"><li>• If this parameter is not set, template HTML cannot be used, and the Domain Gateway Option outputs the following content. &lt;HTML&gt; &lt;HEAD&gt;&lt;TITLE&gt;SYSTEM ERROR [ICEWALL DOCUMENT DGFW]&lt;/TITLE&gt;&lt;/HEAD&gt; &lt;BODY&gt;&lt;P&gt; &lt;FONT SIZE=6&gt; System Error&lt;/FONT&gt;&lt;BR&gt; IceWall Document DGFW &lt;/BODY&gt; &lt;/HTML&gt;</li></ul>
See also	Domain Gateway Option HTML configuraiton file

---

Domain Gateway Option configuration file (dgfw.conf)

---

## SERVICE\_NAME

Overview	Specifies the service name used in Kerberos ticket analysis.
Format	<p><b>SERVICE_NAME=service name@host name.domain name</b></p> <ul style="list-style-type: none"><li>For “service name” and “host name.domain name”, specify the values at the following locations in the principal name used when you generated the Kerberos key using the Ktpass command: Principal name Ktpass -princ <u>HTTP</u>/<u>unix.jpn.hp.com</u>@JPN.HP.COM •• (1) (2) (1) service name HTTP (2) host name.domain name unix.jpn.hp.com</li><li>If this parameter is not set, the ticket passed from the client cannot be analyzed upon authentication and the user cannot log in to SSO.</li><li>The default value for the default configuration file is dgfw@jpn.hp.com.</li></ul>
Configuration example	<p>1) When the principal name of the Kerberos key is HTTP/ unix.jpn.hp.com@JPN.HP.COM <b>SERVICE_NAME=HTTP@unix.jpn.hp.com</b></p>
Remarks	<ul style="list-style-type: none"><li>Characters in “service name” and “host name.domain name” are case-sensitive. Use the same cases as specified in the principal name used when you generated the Kerberos key.</li></ul>
See also	None

## USERNAME\_FRM

Overview	Specifies the format of the user ID obtained from the ticket.
Format	<p><b>USERNAME_FRM=realm name flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be specified for the realm name flag:<ul style="list-style-type: none"><li>0 : Include realm name in user ID Example user0001@JPN.HP.COM</li><li>1 : Do not include realm name in user ID Example user0001</li></ul></li><li>• The default value in the execution binary is 1.</li><li>• The default value for the default configuration file is 1.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) When realm name is not included in user ID</p> <p><b>USERNAME_FRM=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• Note that when this parameter is set to 0, it is assumed that the realm name is also included in the user ID used for login with the basic and form authentication functions.</li><li>• When this parameter is set to 0, the realm name must be included in the user ID to be registered in the Authentication DB.</li></ul>
See also	None

## **5.2 Domain Gateway Option HTML configuration file (dghtml.conf)**

**Overview** This file is used to configure the storage location and file name of the page that is to be output to a client in each process by the Domain Gateway Option.  
The parameters available to the user are as follows:

<b>Parameter group</b>	<b>Parameter name</b>
Login	DG_LOGIN_TKT
	DG_LOGIN_FORCE
	DG_LOGIN_ERR_ADDR
	DG_LOGIN_ERR_UID
	DG_LOGIN_ERR_TKT
	DG_LOGIN_ERR_1STCERT
	DG_LOGIN_ERR_LOCK
	DG_LOGIN_ERR_NOGRP
	DG_LOGIN_ERR_STOP
	DG_LOGIN_ERR_LIMIT
System errors	DG_SYSTEM_ERR
	DG_SYSTEM_DOWN_CERTD
	DG_SYSTEM_DOWN_DB
	DG_SYSTEM_TOUT_CERTD
	DG_SYSTEM_BUSY_DB <b>10.0</b>
User-defined errors	DG_USREXT_ERR1
	DG_USREXT_ERR2
	DG_USREXT_ERR3

**Storage location** The following is the default storage location:  
/opt/icewall-ssso/dfw/cgi-bin/dghtml.conf

**Remarks** None

The following pages describe these parameters.

### 5.2.1 Login

These parameters are used to define the page used for login via the Domain Gateway Option.

Parameter name	Mandatory	Overview
DG_LOGIN_TKT	×	Sets the ticket authentication login page
DG_LOGIN_FORCE	×	Sets the forced login page
DG_LOGIN_ERR_ADDR	×	Sets the authentication execution permission error page
DG_LOGIN_ERR_UID	×	Sets the user ID error page
DG_LOGIN_ERR_TKT	×	Sets the ticket verification error page.
DG_LOGIN_ERR_1STCERT	×	Sets the pre-authenticated (concurrent usage) error page.
DG_LOGIN_ERR_LOCK	×	Sets the account lock error page.
DG_LOGIN_ERR_NOGRP	×	Sets the no group error page.
DG_LOGIN_ERR_STOP	×	Sets the login stop error page.
DG_LOGIN_ERR_LIMIT	×	Sets the maximum login counts error page.

For details on these parameters, see the following pages.

## DG\_LOGIN\_TKT

Overview	Body for requesting the client to issue a ticket.
Format	<p><b>DG_LOGIN_TKT=ticket authentication login page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_tkt.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_tkt.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_tkt.html as ticket authentication login page</p> <p><b>DG_LOGIN_TKT=/opt/icewall-ssso/dfw/dghtml/login_tkt.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_FORCE

Overview	Sets the forced login page that is displayed if a duplicate login is attempted when exclusive login forbidding duplicate logins is set.
Format	<p><b>DG_LOGIN_FORCE=forced login page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_force_tkt.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_force_tkt.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_force_tkt.html as forced login page</p> <p><b>DG_LOGIN_FORCE=/opt/icewall-ssso/dfw/dghtml/login_force_tkt.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>



## DG\_LOGIN\_ERR\_ADDR

Overview	Sets the error page output when the IP address of the Domain Gateway Option server is not defined in the FEDERATION parameter of the Authentication Module configuration file.
Format	<p><b>DG_LOGIN_ERR_ADDR=authentication execution permission error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_addr_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_addr_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_addr_error.html as authentication execution permission error page</p> <p><b>DG_LOGIN_ERR_ADDR=/opt/icewall-ssso/dfw/dghtml/login_addr_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_ERR\_UID

Overview	Sets the user ID error page that is displayed when a login is attempted with an unregistered user ID.
Format	<p><b>DG_LOGIN_ERR_UID=user ID error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_userid_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_userid_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_use-rid_error.html as user ID error page</p> <p><b>DG_LOGIN_ERR_UID=/opt/icewall-ssso/dfw/dghtml/login_userid_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_ERR\_TKT

Overview	Sets the error page output when the ticket received from the client causes a verification error.
Format	<p><b>DG_LOGIN_ERR_TKT=ticket verification error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_tkt_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_tkt_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_tkt_error.html as ticket verification error page</p> <p><b>DG_LOGIN_ERR_TKT=/opt/icewall-ssso/dfw/dghtml/login_tkt_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_ERR\_1STCERT

Overview	Sets the pre-authenticated error page that is displayed when a login with a ticket is attempted after an initial login using a client certificate.
Format	<p><b>DG_LOGIN_ERR_1STCERT=pre-authenticated (concurrent usage)error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_cert_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_cert_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_cert_error.html as pre-authenticated error page</p> <p><b>DG_LOGIN_ERR_1STCERT=/opt/icewall-ssso/dfw/dghtml/login_cert_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_ERR\_LOCK

Overview	<p>Sets the account lock error page that is displayed when a password error occurs more than the specified number of times.</p> <p>Because ticket authentication does not use a password, this error page is used for authentication of a user whose account is locked by another authentication method or on the Authentication DB.</p>
Format	<p><b>DG_LOGIN_ERR_LOCK=account lock error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_lock_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_lock_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_lock_error.html as account lock error page</p> <p><b>DG_LOGIN_ERR_LOCK=/opt/icewall-ssso/dfw/dghtml/login_lock_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_ERR\_NOGRP

Overview	Sets the no group error page that is displayed when a login is attempted with a user ID that does not have a group assigned to it.
Format	<p><b>DG_LOGIN_ERR_NOGRP=no group error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_nogrp_error.html.-</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_group_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_nogrp_error.html as no group error page</p> <p><b>DG_LOGIN_ERR_NOGRP=/opt/icewall-ssso/dfw/dghtml/login_nogrp_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_STOP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_ERR\_STOP

Overview	Sets the login stop error page that is displayed when a login is attempted with a user ID for which login has been stopped.
Format	<p><b>DG_LOGIN_ERR_STOP=login stop error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_stop_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_stop.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_stop_error.html as login stop error page</p> <p><b>DG_LOGIN_ERR_STOP=/opt/icewall-ssso/dfw/dghtml/login_stop_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_LIMIT</p>

## DG\_LOGIN\_ERR\_LIMIT

Overview	Sets the login limit error page that is displayed during a login attempt when the number of users currently logged in has already reached the maximum.
Format	<p><b>DG_LOGIN_ERR_LIMIT=maximum login count error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/login_limit_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/login_limit_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/login_limit_error.html as maximum login count error page</p> <p><b>DG_LOGIN_ERR_LIMIT=/opt/icewall-ssso/dfw/dghtml/login_limit_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_LOGIN_TKT DG_LOGIN_FORCE DG_LOGIN_ERR_ADDR DG_LOGIN_ERR_UID DG_LOGIN_ERR_TKT DG_LOGIN_ERR_1STCERT DG_LOGIN_ERR_LOCK DG_LOGIN_ERR_NOGRP DG_LOGIN_ERR_STOP</p>



### 5.2.2 System errors

These parameters are used to configure the HTML pages displayed when system errors occur in the Domain Gateway Option.

Parameter name	Mandatory	Overview
DG_SYSTEM_ERR	×	Sets the system error page
DG_SYSTEM_DOWN_CERTD	×	Sets the Authentication Module down error page
DG_SYSTEM_DOWN_DB	×	Sets the Authentication DB down error page.
DG_SYSTEM_TOUT_CERTD	×	Sets the Authentication Module timeout error page.
DG_SYSTEM_BUSY_DB <b>10.0</b>	×	Sets the number of Authentication DB connections.

For details on these parameters, see the following pages.

## DG\_SYSTEM\_ERR

Overview	Sets the system error page displayed when an error occurs in the Domain Gateway Option or the Authentication Module.
Format	<p><b>DG_SYSTEM_ERR=system error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/system_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/system_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/system_error.html as system error page</p> <p><b>DG_SYSTEM_ERR=/opt/icewall-ssso/dfw/dghtml/system_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_SYSTEM_DOWN_CERTD DG_SYSTEM_DOWN_DB DG_SYSTEM_TOUT_CERTD DG_SYSTEM_BUSY_DB <b>10.0</b></p>

## DG\_SYSTEM\_DOWN\_CERTD

Overview	Sets the Authentication Module down error page displayed when the Domain Gateway Option attempts to communicate with a non-operational Authentication Module.
Format	<p><b>DG_SYSTEM_DOWN_CERTD=authentication module down error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/system_certd_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/system_certd_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/system_certd_error.html as Authentication Module down error page</p> <p><b>DG_SYSTEM_DOWN_CERTD=/opt/icewall-ssso/dfw/dghtml/system_certd_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_SYSTEM_ERR DG_SYSTEM_DOWN_DB DG_SYSTEM_TOUT_CERTD DG_SYSTEM_BUSY_DB <b>10.0</b></p>

## DG\_SYSTEM\_DOWN\_DB

Overview	Sets the Authentication DB down error page displayed when the Authentication DB is non-operational when accessed by the Authentication Module.
Format	<p><b>DG_SYSTEM_DOWN_DB=authentication DB down error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/system_ldap_error.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/system_ldap_error.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/system_ldap_error.html as Authentication DB down error page</p> <p><b>DG_SYSTEM_DOWN_DB=/opt/icewall-ssso/dfw/dghtml/system_ldap_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_SYSTEM_ERR DG_SYSTEM_DOWN_CERTD DG_SYSTEM_TOUT_CERTD DG_SYSTEM_BUSY_DB <b>10.0</b></p>

## DG\_SYSTEM\_TOUT\_CERTD

Overview	Sets the Authentication Module timeout error page displayed if a timeout occurs when the Domain Gateway Option is communicating with the Authentication Module and waiting for a response message.
Format	<p><b>DG_SYSTEM_TOUT_CERTD=authentication module receive timeout error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/system_timeout_certd.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/system_timeout_certd.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/system_timeout_certd.html as Authentication Module receive timeout error page</p> <p><b>DG_SYSTEM_TOUT_CERTD=/opt/icewall-ssso/dfw/dghtml/system_timeout_certd.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	<p>DG_SYSTEM_ERR DG_SYSTEM_DOWN_CERTD DG_SYSTEM_DOWN_DB DG_SYSTEM_BUSY_DB <b>10.0</b></p>

## DG\_SYSTEM\_BUSY\_DB 10.0

Overview	<p>Sets the Authentication DB busy error page displayed when the Authentication Module cannot process the request due to congestion of database accesses.</p> <p>This parameter is available with version 10.0 or later.</p>
Format	<p><b>DG_SYSTEM_BUSY_DB=authentication DB busy error page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/system_busy_database.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/system_busy_database.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/system_busy_database.html as the Authentication DB busy error page</p> <p><b>DG_SYSTEM_BUSY_DB=/opt/icewall-ssso/dfw/dghtml/request_acl_error.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li><li>• This parameter is valid only when ICP 2.0 is used. To use ICP 2.0, you need to set the ICP_VERSION parameter in the Forwarder configuration file (dfw.conf) to use it.</li></ul>
See also	<p>ICP_VERSION (Forwarder configuration file)</p> <p>DG_SYSTEM_ERR</p> <p>DG_SYSTEM_DOWN_CERTD</p> <p>DG_SYSTEM_DOWN_DB</p> <p>DG_SYSTEM_TOUT_CERTD</p>

### **5.2.3 Page settings related to user-defined errors**

These parameters are used to configure the HTML pages defined by users, which contain external routines that can be used by the Authentication Module.

<b>Parameter name</b>	<b>Mandatory</b>	<b>Overview</b>
DG_USREXT_ERR1	×	Sets the user-defined error 1 page.
DG_USREXT_ERR2	×	Sets the user-defined error 2 page.
DG_USREXT_ERR3	×	Sets the user-defined error 3 page.

For details on these parameters, see the following pages.

## DG\_USREXT\_ERR1

Overview	Sets the user-defined error 1 page defined in the Authentication Module UserExit routine.
Format	<p><b>DG_USREXT_ERR1=user-defined error 1 page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/usr_ext1.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/usr_ext1.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/usr_ext1.html as user-defined error 1 page</p> <p><b>DG_USREXT_ERR1=/opt/icewall-ssso/dfw/dghtml/usr_ext1.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	DG_USREXT_ERR2 DG_USREXT_ERR3



## DG\_USREXT\_ERR2

Overview	Sets the user-defined error 2 page defined in the Authentication Module UserExit routine.
Format	<p><b>DG_USREXT_ERR2=user-defined error 2 page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/usr_ext2.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/usr_ext2.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/usr_ext1.thtml as user-defined error 2 page</p> <p><b>DG_USREXT_ERR2=/opt/icewall-ssso/dfw/dghtml/usr_ext2.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	DG_USREXT_ERR1 DG_USREXT_ERR3

## DG\_USREXT\_ERR3

Overview	Sets the user-defined error 3 page defined in the Authentication Module UserExit routine.
Format	<p><b>DG_USREXT_ERR3=user-defined error 3 page file name</b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value in the execution binary is /opt/icewall-ssso/dfw/dghtml/usr_ext3.html.</li><li>• The default value in the default configuration file is /opt/icewall-ssso/dfw/dghtml/usr_ext3.html.</li><li>• The default value in the execution binary is used when the configuration file contains no line to set the value.</li></ul>
Configuration example	<p>1) To specify /opt/icewall-ssso/dfw/dghtml/usr_ext1.thtml as user-defined error 3 page</p> <p><b>DG_USREXT_ERR3=/opt/icewall-ssso/dfw/dghtml/usr_ext3.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• A special keyword conversion function is implemented for the page content specified by this parameter. For this reason, the content of the output page must be in text format.</li></ul>
See also	DG_USREXT_ERR1 DG_USREXT_ERR2

### 5.3 Forwarder configuration file (dfw.conf)

**Overview** This file defines the settings necessary for the Domain Gateway Option to run, and some of the settings are shared with Forwarder. The parameters referenced are as follows.

Parameter group	Parameter name
Domain Gateway Option reference	CERT
	COOKIENAME
	COOKIEATTR
	POSTKEY_LOGIN
	RETRYCNTC
	RETRYTMC
	SESSION_ENC_KEY
	DFW_PROTOCOL
	ICP_VERSION
	ICP_AGENTSTR
	ICP_ENCSTR 10.0
	CERTLB 10.0
	CERTLB_TYPE 10.0

**Storage location** The following is the default storage location:  
/opt/icewall-ss0/dfw/cgi-bin/dfw.conf

**Remarks** The name of this file cannot be changed.  
This file must be stored in the same directory as Forwarder and Domain Gateway Option binary files.

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

## **5.4 Authentication Module configuration file (cert.conf)**

**Overview** This file defines the settings necessary for the Domain Gateway Option to perform IceWall SSO authentication. The following parameters are required to link with the Domain Gateway Option.

<b>Parameter group</b>	<b>Parameter name</b>
User authentication	FEDERATION ⑩.0


**Storage location** The following is the default storage location:  
/opt/icewall-ss0/certd/config/cert.conf

**Remarks** None

The following pages describe these parameters.

### 5.4.1 User authentication

These parameters are used to configure the settings related to user authentication by the Domain Gateway Option.

Parameter name	Mandatory	Overview
FEDERATION 	×	Sets the request source for authentication with user ID only.

For details on these parameters, see the following pages.

## FEDERATION 10.0

Overview	Sets the IP address of the IceWall (Domain Gateway Option) server which allows authentication with only the user ID.
Format	<p><b>FEDERATION=IP address(,IP address-IPaddress)</b></p> <ul style="list-style-type: none"><li>• Multiple IP addresses can be specified by separating them with a comma.</li><li>• IP addresses can be specified individually or as an address range.</li><li>• When specifying an IP address range, specify "lowest address-highest address."</li><li>• You cannot use the regular expression to specify the IP addresses.</li><li>• If you define multiple lines of IP address specification, only the last line takes effect.</li><li>• There is no default value in the execution binary.</li><li>• The default value for the default configuration file is not specified.</li></ul> <p><b>FEDERATION=[IP address](,[IP address]-[IP address])</b></p> <ul style="list-style-type: none"><li>• You can also specify the IPv6 IP addresses. When specifying an IPv6 IP address, enclose the IP address within square brackets ([ ]). <span style="border: 1px solid black; border-radius: 50%; padding: 0 2px;">10.0</span></li><li>• You cannot use both of the IPv4 and IPv6 IP addresses within single specification. <span style="border: 1px solid black; border-radius: 50%; padding: 0 2px;">10.0</span></li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) Single specification <b>FEDERATION=192.168.0.4</b></li><li>2) Multiple specification <b>FEDERATION=192.168.0.4,192.168.0.5</b></li><li>3) Range specification <b>FEDERATION=192.168.0.1-192.168.0.240</b></li><li>4) Multiple range specification <b>FEDERATION=192.168.0.1-192.168.0.50,192.168.0.100-192.168.0.150</b></li><li>5) Single and range specification <b>FEDERATION=192.168.0.5,192.168.0.50-192.168.0.100</b></li><li>6) Single and range specification of IPv6 IP addresses <b>FEDERATION=[1234:0000:5678:9abc:1234:::9a00],[1234:0000:5678:9abc:1234:::9a50]-[1234:0000:5678:9abc:1234:::9abc]</b></li></ol>

**Authentication Module configuration file (cert.conf)**

---

Remarks	<ul style="list-style-type: none"><li>• Note that this parameter is not required by the Authentication Module, but required for the Domain Gateway Option to operate.</li><li>• The new value for this parameter takes effect after restarting the Authentication Module.</li><li>• When using the IPv6 addresses, you can omit “0”s. <b>10.0</b></li></ul>
See also	IPV6LISTEN

## 6 Troubleshooting

### 6.1 When the ticket presentation request page is displayed

“Use Windows Integrated Authentication” is not enabled in the detailed settings of IE used for access.

Enable this option and try again.

### 6.2 When HTTP\_AUTHORIZATION is not inherited to the Domain Gateway Option

Check the configuration file of Apache to see if RewriteRule for mod\_rewrite is set correctly. When <VirtualHost> is used to define the port used for the Domain Gateway Option, describe the definition between the <VirtualHost> syntax.

Sample configuration of <VirtualHost XXXX:port>

```
<VirtualHost XXXX:port>
RewriteEngine on
RewriteRule /fw/dgfw(.*) /fw/dgfw$1
[PT,E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
</VirtualHost>
```

### 6.3 When the ticket verification error page is displayed

Refer to the error log of the Domain Gateway Option.

(1) When the following log message is output

```
Fatal: gss_acquire_cred() Error. MajorStatus=851968 [Miscellaneous failure] Minor
Status=13 [A later token has already been processed] [ ](4711) [EG16109-70077]
```

The Domain Gateway Option cannot refer to the /etc/krb5.keytab file of the IceWall server. Change the access permission of the /etc/krb5.keytab file such that it can be referenced by the chown and chmod commands.

(2) When the following log message is output

```
Fatal: gss_acquire_cred() Error. MajorStatus=851968 [Miscellaneous failure] Minor
Status=39756033 [Unknown supplementary info code (field =32768)] [ ] (4367) [EG1
6109-70077]
```

Check if the SERVICE\_NAME parameter is configured correctly in the Domain Gateway Option configuration file (dgfw.conf).

Also check if the correct host name is defined as the service name for the SERVICE\_NAME parameter in the /etc/hosts file of the IceWall server.



```
192.168.0.1 linux.jpn.hp.com linux ○
192.168.0.1 linux linux.jpn.hp.com ×
* This description causes an error in the name resolution process within GSS-API.
```

(3) When the following log message is output

```
Fatal: gss_accept_sec_context() Error. MajorStatus=851968[Miscellaneous failure]
MinorStatus=-1765328353 [Unknown supplementary info code?(field = 8192)] [ ] (20727) [EG16110-70078]
```

The Kerberos ticket cannot be decrypted because the key type does not match the registered type.

- Check if the Kerberos key is registered in the /etc/krb5.keytab file of the IceWall server.
- Check if the encryption method created by the Ktpass (Kerberos key generation command) of the domain controller matches the encryption method specified in the /etc/krb5.keytab file of the IceWall server.

If both settings are correct, restart the domain controller server.

(4) When the following log message is output (10.0)

```
Fatal: gss_accept_sec_context() Error. MajorStatus=851968[Miscellaneous failure]
MinorStatus=-1765328347 [Unknown supplementary info code (field = 8192)] [ ] (27518) [EG16110-70078]
```

The time between the client and the IceWall server is different by more than five minutes.

Adjust the time of the client and IceWall server such that the difference is less than five minutes.

(5) When the following log message is output (10.0)

```
Fatal: DGFWSpnegoInitFromBinary() Error. Errno=-1 [The supplied Token was invalid] [ ] (2837) [EG16103-70073]
Warning: DGFWSGetTktUidCtrl() Error. [ ] (2837) [EG00111-70007]
```

The request from the client does not contain a correct ticket.

Check the following IE settings.

1. Select [Tools (T)] - [Internet Options (O)] - [Security] in IE used for access.
2. Select the security zone the IceWall server is assigned to and click [Customize Level].
3. Select the following options:  
[User Authentication] - [Logon] - [Automatically log on using current user name and password] or [User Authentication] - [Logon] - [Automatic logon only in intranet zone]

If the problem persists, check the settings of the user who is experiencing the problem.

## **6.4 When the authentication dialog (pop-up) is displayed**

The current setting does not allow automatic login to the IceWall server.

Configure IE as follows:

1. Select [Tools (T)] - [Internet Options (O)] - [Security] in IE used for access.
2. Select the security zone the IceWall server is assigned to and click [Customize Level].
3. Select the following options:  
[User Authentication] - [Logon] - [Automatic logon with current user name and password]

## **7 Logs**

### **7.1 Log format**

#### **7.1.1 Access log format**

[date/time] △ [request analysis time △ authentication module processing time △ response processing time] △ log message △ [user ID] △ (processnumber) △ (IP address) △ transaction ID △ [message ID]

\* △ indicates a single-byte space.

\* The IP address is output only when ALEVEL=2.

Sample output

[2006/03/14 17:40:12] [000.000 000.000 000.000] Login Success.. [user024693] (3) (192.1.1.1) TID=TID20100102030405678901G0-dgfwsvr01 [AG00101-72004]
--

#### **7.1.2 Error log format**

[date/time] △ error level: △ log message △ [user ID] △ (process number) △ transaction ID △ [message ID]

\* △ indicates a single-byte space.

\* The error level if Fatal or Warning.

Sample output

[2006/03/14 16:50:27] Fatal: Can't Set Error Page. [user010992] (2) TID=TID20100102030405678901G0-dgfwsvr02 [EG00107-70003]
--

## 7.2 Log Message List

The following lists the log messages output from the Domain Gateway Option in the following order:

- Levels are sorted in the order of FATAL and WARNING.
- Code IDs are sorted in ascending order within each level.

### 7.2.1 Access log message list

Code ID	Message	Description
AG00101-72001	Return Status 401.	Returned a response to a ticket presentation request from the client.
AG00101-72002	Login Error.	Authentication failed.
AG00101-72003	Force Login Error.	Forced login failed.
AG00101-72004	Login Success.	Authentication succeeded.
AG00101-72005	Force Login Success.	Forced login succeeded.
AG00101-72006	Return Force Login Page.	Returned the forced login page.
AG00101-72007	Ticket Error.	A ticket verification error occurred.
AG00101-72008	System Error.	A system error occurred.

### 7.2.2 Error log message list

Code ID	Level	Message	Description
EG00101-71040	FATAL	DGFWLib_CreateSocketData() Error.	Could not allocate the buffer area.
EG00102-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.
EG00103-70004	FATAL	DGFW_CreateConfig() Error.	Failed to allocate the memory for the configuration file extension area.
EG00104-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.
EG00105-70005	FATAL	DGFW_ReadConfCtrl() Error.	Failed to load the configuration file.
EG00106-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.
EG00107-70003	FATAL	Can't Set Error Page.	Failed to build the ticket request page.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG00109-70003	FATAL	Can't Set Error Page.	Failed to create a page corresponding to the return value from DGFW_Login() Error.
EG00112-70003	FATAL	Can't Set Error Page.	Cannot build the ticket verification error page.
EG00113-70008	FATAL	DGFW_ClientRequest() Error.	An error occurred during the request analysis process.
EG00114-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.
EG00121-70083	FATAL	ICP_CreateComm() Error.	Failed to create ICP 2.0 communication information structure.
EG00122-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.
EG00125-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the transaction ID storage area. Output value: [Errno=error number output from OS]
EG00127-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.
EG02101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02201-70013	FATAL	Entry Create Error.	Failed to allocate the access log level area.
EG02202-70014	FATAL	Entry Add Error.	Failed to extend the default value of the access log level.
EG02203-70013	FATAL	Entry Create Error.	Failed to allocate the error log level area.
EG02204-70014	FATAL	Entry Add Error.	Failed to extend the default value of the error log level.
EG02205-70013	FATAL	Entry Create Error.	Failed to allocate the error log level area.
EG02206-70014	FATAL	Entry Add Error.	Failed to extend the default value of the access log file name.
EG02207-70013	FATAL	Entry Create Error.	Failed to allocate the error log file name.
EG02208-70014	FATAL	Entry Add Error.	Failed to extend the default value of the error log file name.
EG02209-70013	FATAL	Entry Create Error.	Failed to allocate the DOCS area.
EG02210-70014	FATAL	Entry Add Error.	Failed to extend the default value of DOCS.
EG02211-70013	FATAL	Entry Create Error.	Failed to allocate the user ID format area.
EG02212-70014	FATAL	Entry Add Error.	Failed to extend the default value of the user ID format.
EG02213-70013	FATAL	Entry Create Error.	Failed to allocate the retry count area.
EG02214-70014	FATAL	Entry Add Error.	Failed to extend the default value of the retry count.
EG02215-70013	FATAL	Entry Create Error.	Failed to allocate the retry interval area.
EG02216-70014	FATAL	Entry Add Error.	Failed to extend the default value of the retry interval.
EG02217-70013	FATAL	Entry Create Error.	Failed to allocate the cookie name area.
EG02218-70014	FATAL	Entry Add Error.	Failed to extend the default value of the cookie name.
EG02219-70013	FATAL	Entry Create Error.	Failed to allocate the login keyword area.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG02220-70014	FATAL	Entry Add Error.	Failed to extend the default value of the login keyword.
EG02221-70013	FATAL	Entry Create Error.	Failed to allocate the DFW_PROTOCOL area.
EG02222-70014	FATAL	Entry Add Error.	Failed to extend the default value of DFW_PROTOCOL.
EG02223-70013	FATAL	Entry Create Error.	Failed to allocate the ICP_VERSION area.
EG02224-70014	FATAL	Entry Add Error.	Failed to extend the default value of ICP_VERSION.
EG02225-70013	FATAL	Entry Create Error.	Failed to allocate the CONNECTCNTC area.
EG02226-70014	FATAL	Entry Add Error.	Failed to extend the default value of CONNECTCNTC.
EG02227-70013	FATAL	Entry Create Error.	Failed to extend CONNECTTMC area.
EG02228-70014	FATAL	Entry Add Error.	Failed to extend the default value of CONNECTTMC.
EG02229-70013	FATAL	Entry Create Error.	Failed to allocate the CERTLB_TYPE area.
EG02230-70014	FATAL	Entry Add Error.	Failed to extend the default value of CERTLB_TYPE.
EG02231-70013	FATAL	Entry Create Error.	Failed to allocate the TRANSID area.
EG02232-70014	FATAL	Entry Add Error.	Failed to extend the default value of TRANSID.
EG02233-70013	FATAL	Entry Create Error.	Failed to allocate the TRANSID_STR area.
EG02234-70014	FATAL	Entry Add Error.	Failed to extend the default value of TRANSID_STR.
EG02235-70013	FATAL	Entry Create Error.	Failed to allocate the ICP_ENCSTR area.
EG02236-70014	FATAL	Entry Add Error.	Failed to extend the default value of ICP_ENCSTR.
EG02301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02302-70015	FATAL	Can't Open Configuration File.[%s]	Cannot open the configuration file. Output value: [file path]
EG02303-70016	FATAL	File Lock Error. File=(%) errno=(%d) errmsg=(%).	Cannot lock the configuration file. Output value: [errno=error number output from OS errmsg=error message retrieved from OS]
EG02304-70017	FATAL	fdopen() Error.	Failed in fopen() of the configuration file.
EG02305-70018	FATAL	Configuration format error.[%s]", "fstat() error	Format is invalid. Output value: [configuration name]"
EG02306-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the area for loading a file. Output value: [Errno=error number output from OS]
EG02401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02402-70019	FATAL	DGFW_SetDGFWConf() Error.	An error occurred while splitting the dgfw.conf configuration file.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG02403-70020	FATAL	DGFW_SetDFWConf() Error.	An error occurred while splitting the dfw.conf configuration file.
EG02501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02601-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02701-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02702-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the alias name work area. Output value: [Errno=error number output from OS]
EG02703-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the value work area. Output value: [Errno=error number output from OS]
EG02705-70025	FATAL	KeyData Create Error.	Failed to create KeyData.
EG02706-70014	FATAL	Entry Add Error.	Failed to extend memory for value.
EG02801-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02901-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG02902-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the failover entry area. Output value: [Errno=error number output from OS]
EG02903-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the failover entry area. Output value: [Errno=error number output from OS]
EG02904-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the host area. Output value: [Errno=error number output from OS]
EG02905-70029	FATAL	Configuration Format Error.[failover]	CERT description format error.
EG03101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG03102-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the trace log file name. Output value: [Errno=error number output from OS]
EG03103-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the error log file name. Output value: [Errno=error number output from OS]
EG03104-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the error log level area. Output value: [Errno=error number output from OS]
EG03201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG04401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG04402-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the access log message work area. Output value: [Errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG04403-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the access log message ID work area. Output value: [Errno=error number output from OS]
EG06101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06102-70030	FATAL	Create SocketData Error.	Could not allocate the socket structure area.
EG06103-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the response message area. Output value: [Errno=error number output from OS]
EG06105-70001	FATAL	malloc() Error. Errno=%d	Failed to retrieve session information area. Output value: [Errno=error number output from OS]
EG06106-70001	FATAL	malloc() Error. Errno=%d	Failed to retrieve session information encryption area. Output value: [Errno=error number output from OS]
EG06107-70032	FATAL	SessionID Encrypt Failed.	Failed in session ID encryption.
EG06108-70033	FATAL	DGFW_ModifyStrings() Error.	Failed to register encryption session information.
EG06109-70001	FATAL	malloc() Error. Errno=%d	Failed to retrieve session information area. Output value: [Errno=error number output from OS]
EG06110-70034	FATAL	Can't Create Redirect URL.	Failed to create redirect URL.
EG06111-70003	FATAL	Can't Set Error Page.	Cannot build the authentication success page.
EG06112-70003	FATAL	Can't Set Error Page.	Cannot build the forced login page.
EG06113-70003	FATAL	Can't Set Error Page.	Cannot build the certificate execution permission error page.
EG06114-70003	FATAL	Can't Set Error Page.	Cannot build the user ID error page.
EG06115-70003	FATAL	Can't Set Error Page.	Cannot build the user ID error page.
EG06116-70003	FATAL	Can't Set Error Page.	Cannot build the account lock error page.
EG06117-70003	FATAL	Can't Set Error Page.	Cannot build the no group error page.
EG06118-70003	FATAL	Can't Set Error Page.	Cannot build the login stop error page.
EG06119-70003	FATAL	Can't Set Error Page.	Cannot build the user count exceeded error page.
EG06120-70003	FATAL	Can't Set Error Page.	Cannot build the Authentication DB down error page.
EG06121-70003	FATAL	Can't Set Error Page.	Cannot build the page for external interface error 1.
EG06122-70003	FATAL	Can't Set Error Page.	Cannot build the page for external interface error 2.
EG06123-70003	FATAL	Can't Set Error Page.	Cannot build the page for external interface error 3.
EG06124-70003	FATAL	Can't Set Error Page.	Cannot build the concurrent usage error page.
EG06125-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.



## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG06126-70003	FATAL	Can't Set Error Page.	Cannot build the DB connection busy error page.
EG06127-70003	FATAL	Can't Set Error Page.	Cannot build the system error page.
EG06201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06204-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the SSO session work area. Output value: [Errno=error number output from OS]
EG06205-70085	FATAL	Can't Find.[%s]	Failed to retrieve the User-Agent header. Output value: [unretrievable data]
EG06207-70087	FATAL	DGFWL_GetCertAlias() Error.	Failed to retrieve the Authentication Module identification key.
EG06211-70088	FATAL	Format Error.[%s]", "ICP Sid Error	Session ID received from the Authentication Module is invalid. Output value: [session ID]
EG06208-70089	FATAL	sessionid length error. (certd) sid=[%s]	Length of the session ID received from the Authentication Module is invalid. Output value: [session ID]
EG06301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06502-70037	FATAL	DGFWLib_FindFailover() Error.	Cannot find the certd failover entry.
EG06503-70038	FATAL	Certification Server Down.[%s:%d]	Authentication Server or module is down. Output value: host name:port number]
EG06504-70039	FATAL	Data Send Failed.	Failed to send data.
EG06505-70040	FATAL	Data Receive Failed.	Failed to receive data.
EG06506-70041	FATAL	Connection Timeout.	Connection timed out.
EG06507-70042	FATAL	DGFWLib_MessageExchange() Error.	An error occurred during data communication with the Authentication Module.
EG06508-70043	FATAL	All Certification Server Down.	Authentication Servers and/or modules are all down.
EG06509-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06510-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06511-71050	FATAL	Can't get CertdLBAlias.	Could not retrieve Authentication Module information from the Authentication Module identification key.
EG06601-70001	FATAL	malloc() Error. Errno=%d	Cannot allocate the receive buffer structure creation area. Output value: [Errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG06602-70044	FATAL	DGFWLib_CreateBuf() Error.	An error occurred during creation of the receive buffer structure.
EG06603-70044	FATAL	DGFWLib_CreateBuf() Error.	An error occurred during creation of the send buffer structure.
EG06801-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06802-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the session ID keyword work area. Output value: [Errno=error number output from OS]
EG06803-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the session ID work area. Output value: [Errno=error number output from OS]
EG06901-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG06902-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the keyword work area. Output value: [Errno=error number output from OS]
EG06903-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the value work area. Output value: [Errno=error number output from OS]
EG06904-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the value work area. Output value: [Errno=error number output from OS]
EG07001-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG07002-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the Authentication Module information storage area. - Output value: [Errno=error number output from OS]
EG07004-71050	FATAL	Can't get CertdLBAlias.	Could not retrieve Authentication Module information from the Authentication Module identification key.
EG07005-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the Authentication Module information storage area. - Output value: [Errno=error number output from OS]
EG07101-70001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG07102-71050	FATAL	ICP_JoinBuffer() Error.	Failed in operation to link the ICP 2.0 body.
EG07103-71052	FATAL	IW_ExEncrypto IW_EXCRYPTO is NULL.	Failed to encrypt an ICP 2.0 request.
EG07104-71053	FATAL	IW_ExEncrypto ErrNo[%d] ErrMsg[%s]	An ICP 2.0 encryption library error. Output value: [return value][error message]
EG07105-71054	FATAL	ICP_SetWriteBuf() Error.	Failed in creation of an ICP 2.0 request message.
EG07201-70001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG07202-71055	FATAL	ICP_GetBodyLength() Error.	Failed to retrieve encrypted body information.
EG07203-71056	FATAL	IW_ExDecrypto IW_EXCRYPTO is NULL.	Failed to decrypt an ICP 2.0 request.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG07204-71057	FATAL	IW_ExDecrypto ErrNo[%d] ErrMsg[%s]	An ICP 2.0 encryption library decryption error. Output value: [return value][error message]
EG07205-71058	FATAL	ICP_GetReadBuf() Error.	Failed to split an ICP 2.0 response message.
EG07301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG07302-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the session ID storage area. Output value: [Errno=error number output from OS]
EG07303-71059	FATAL	CMN_FindConfEntry() Error	Failed to create the entry.
EG07304-71060	FATAL	CMN_AddConfEntry() Error	Failed to add entry.
EG07305-71061	FATAL	CMN_ModifyConfValue() Error	Failed to replace the Description value.
EG07306-71062	FATAL	Invalid Response type.	Invalid response data.
EG08101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG08102-70045	FATAL	DGFWLib_FindConfigValue(): Not Found.[DOCS]	Cannot retrieve DOCS.
EG08103-70046	FATAL	DOCSPATH Not Found.[%s]	Cannot find the DOCS path. Output value: [DOCS directory name]
EG08104-70047	FATAL	DGFWLib_CreateConfig() Error.	Failed to create the DGFW_CONF-type HTML path structure.
EG08105-70048	FATAL	DGFW_ReadHTMLConfig() Error.	An error occurred during loading of HTML file information when DOCS is a file.
EG08106-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the ticket request page.
EG08107-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the forced login page.
EG08108-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the authentication execution permission error page.
EG08109-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the user ID error page.
EG08110-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the ticket verification error page.
EG08111-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the authentication concurrent usage error page.
EG08112-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the authentication user lock error page.
EG08113-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the no group error page.
EG08114-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the login stop error page.
EG08115-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the maximum user count exceeded error page.
EG08116-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the system error page.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG08117-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the Authentication Module down error page.
EG08118-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the Authentication DB down error page.
EG08119-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the Authentication Module response timeout error page.
EG08120-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the external interface error 1 page.
EG08121-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the external interface error 2 page.
EG08122-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the external interface error 3 page.
EG08123-70050	FATAL	DGFW Page Select Error.	Corresponding page does not exist.
EG08126-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the file path to the DB connection busy error page.
EG08201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG08202-70053	FATAL	DGFWLib_ClearBuff() Error.	Failed to initialize the area for loading the template HTML.
EG08203-70054	FATAL	DGFWLib_CreateHTML(): Error	Failed to load the template HTML.
EG08301-70055	FATAL	Can't Set Keyword.	Failed to allocate the keyword area.
EG08401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG08402-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the ticket request page.
EG08403-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the ticket request page.
EG08404-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the forced login page.
EG08405-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the forced login page.
EG08406-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the authentication execution permission error page.
EG08407-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the authentication execution permission error page.
EG08408-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the user ID error page.
EG08409-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the user ID error page.
EG08410-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the ticket verification error page.
EG08411-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the ticket verification error page.
EG08412-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the concurrent usage error page.
EG08413-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the concurrent usage error page.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG08414-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the user ID lock error page.
EG08415-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the user ID lock error page.
EG08416-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the no group error page.
EG08417-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the no group error page.
EG08418-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the login stop error page.
EG08419-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the login stop error page.
EG08420-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the maximum user count exceeded error page.
EG08421-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the maximum user count exceeded error page.
EG08422-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the system error page.
EG08423-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the system error page.
EG08424-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the Authentication Module down error page.
EG08425-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the Authentication Module down error page.
EG08426-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the Authentication DB down error page.
EG08427-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the Authentication DB down error page.
EG08428-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the Authentication Module timeout error page.
EG08429-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the Authentication Module timeout error page.
EG08430-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the external interface error 1 page.
EG08431-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the external interface error 1 page.
EG08432-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the external interface error 2 page.
EG08433-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the external interface error 2 page.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG08434-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the external interface error 3 page.
EG08435-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the external interface error 3 page.
EG08436-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Cannot find the DOCS value.
EG08437-70058	FATAL	Can't Open HTML Configuration File.[%s]	Cannot open the dghtml.conf configuration file. Output value: [configuration file name]
EG08438-70017	FATAL	fdopen() Error.	An fd open error occurred.
EG08440-70056	FATAL	Entry Create Error.	Failed to allocate the file path area for the DB connection busy error page.
EG08441-70057	FATAL	Entry Add Error.	Failed to register the default file path value for the DB connection busy error page.
EG08601-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG08602-70053	FATAL	DGFWLib_ClearBuf() Error.	Failed to initialize the ticket presentation request buffer.
EG08603-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set status.
EG08604-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set a status comment.
EG08605-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG08606-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set WWW-Authorization.
EG08607-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG08608-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG08609-70059	FATAL	DGFWLib_FileToBuf() Error.	Failed to link the ticket request HTML in the body data.
EG08701-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG08702-70060	FATAL	DGFWLib_CreateConfig() Error.	Failed to allocate the specific keyword area.
EG10101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG10102-70044	FATAL	DGFWLib_ClearBuf() Error.	Failed to initialize the redirect buffer.
EG10103-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set status.
EG10104-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set MIME.
EG10105-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set Set-Cookie.
EG10106-70063	FATAL	IW_INFO format Error.	Cookie format is invalid.
EG10107-70064	FATAL	Can't Find COOKIENAME.	No cookie name.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG10108-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the cookie edit work area. Output value: [Errno=error number output from OS]
EG10109-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the cookie.
EG10110-70065	FATAL	RedirectURL is NULL.	URL buffer attached to Location is NULL.
EG10111-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the Location line.
EG10201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG10202-70066	FATAL	DGFW_ReplaceFilterChar() Error.	An error occurred during redirect URL filtering.
EG12101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG12102-70067	FATAL	DGFW_GetClientInfo() Error.	Failed to retrieve the request environmental variable.
EG12103-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Failed to retrieve the POSTKEYLOGIN value.
EG12104-70068	FATAL	QueryString Format Error.	QueryString format is invalid.
EG12105-70068	FATAL	QueryString Format Error.	QueryString format is invalid.
EG12106-70069	FATAL	DGFW_SetHideURLRequest() Error.	Failed to retrieve the HIDEURL value from QueryString.
EG12107-70068	FATAL	QueryString Format Error.	QueryString format is invalid.
EG12201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG12202-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the method work area. Output value: [Errno=error number output from OS]
EG12203-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the method work area. Output value: [Errno=error number output from OS]
EG12204-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the REMOTE_ADDR work area. Output value: [Errno=error number output from OS]
EG12205-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the REMOTE_ADDR work area. Output value: [Errno=error number output from OS]
EG12206-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the CONTENT_TYPE work area. Output value: [Errno=error number output from OS]
EG12207-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the POST data work area. Output value: [Errno=error number output from OS]
EG12208-71006	FATAL	fread() Error.	Failed to load the POST data.
EG12209-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the QUERY_STRING work area. Output value: [Errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG12210-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the HTTP_AUTHORIZATION work area. Output value: [Errno=error number output from OS]
EG12211-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the HTTP_HOST work area. Output value: [Errno=error number output from OS]
EG12212-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the SERVER_PORT work area. Output value: [Errno=error number output from OS]
EG12213-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the SCRIPT_URI work area. Output value: [Errno=error number output from OS]
EG12214-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the SCRIPT_URI SCRIPT_NAME work area. Output value: [Errno=error number output from OS]
EG12215-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the REQUEST_URI work area. Output value: [Errno=error number output from OS]
EG12216-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the SCRIPT_URI work area. Output value: [Errno=error number output from OS]
EG12217-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the SERVER_NAME work area. Output value: [Errno=error number output from OS]
EG12301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG12302-70047	FATAL	DGFWLib_CreateConfig() Error.	Failed to allocate the QueryString data area.
EG12303-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the QueryString split data area. Output value: [Errno=error number output from OS]
EG12304-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the QueryString split data area. Output value: [Errno=error number output from OS]
EG12305-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the QueryString split record area.
EG12306-70024	FATAL	DGFWLib_AddConfigEntry() Error.	Failed to register the QueryString split record.
EG12307-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the QueryString split data area. Output value: [Errno=error number output from OS]
EG12308-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the QueryString split record area.
EG12309-70024	FATAL	DGFWLib_AddConfigEntry() Error.	Failed to register the QueryString split record.
EG12401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG12402-70070	FATAL	DGFW_FWC_EncodeData() Error.	An error occurred during the encoding process..
EG12501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.



---

**IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX**

---

Code ID	Level	Message	Description
EG12601-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate keyword work area. Output value: [Errno=error number output from OS]
EG12602-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the value work area. Output value: [Errno=error number output from OS]
EG12701-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG12801-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Could not retrieve the DFW_PROTOCOL value.
EG12802-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the redirect URL area. Output value: [Errno=error number output from OS]
EG14101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG14102-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the replacement area. Output value: [Errno=error number output from OS]
EG14201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG14202-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the encode buffer area. Output value: [Errno=error number output from OS]
EG16102-70072	FATAL	DGFW_Base64Decode() Error.	Failed to decode the Authorization value.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG16103-70073	FATAL	DGFW_spnegoInitFromBinary() Error. Errno=-1 [The supplied Token was invalid]	Failed to initialize SPNEGO. The format of the Kerberos ticket passed from the client is invalid.
		DGFW_spnegoInitFromBinary() Error. Errno=-2 [An invalid length was encountered]	Failed to initialize SPNEGO. The format (length) of the Kerberos ticket passed from the client is invalid.
		DGFW_spnegoInitFromBinary() Error. Errno=-3 [The Token Parse failed]	Failed to initialize SPNEGO. An SPNEGO format analysis error.
		DGFW_spnegoInitFromBinary() Error. Errno=-4 [The requested value was not found]	Failed to initialize SPNEGO. No value was found during SPNEGO analysis.
		DGFW_spnegoInitFromBinary() Error. Errno=-5 [The requested element is not available]	Failed to initialize SPNEGO. Field configuration was invalid during SPNEGO analysis.
		DGFW_spnegoInitFromBinary() Error. Errno=-6 [Out of Memory]	Failed to initialize SPNEGO. Failed to allocate the memory area during the SPNEGO process.
		DGFW_spnegoInitFromBinary() Error. Errno=-7 [Not Implemented]	Failed to initialize SPNEGO. SPNEGO process execution error.
		DGFW_spnegoInitFromBinary() Error. Errno=-8 [Invalid Parameter]	Failed to initialize SPNEGO. SPNEGO function parameter is invalid.
		DGFW_spnegoInitFromBinary() Error. Errno=-9 [Token Handler encountered an unexpected OID]	Failed to initialize SPNEGO. Invalid OID was used for the SPNEGO function parameter.
		DGFW_spnegoInitFromBinary() Error. Errno=-10 [The requested token was not found]	Failed to initialize SPNEGO. SPNEGO function parameter does not contain the Kerberos ticket.
		DGFW_spnegoInitFromBinary() Error. Errno=-11 [An unexpected type was encountered in the encoding]	Failed to initialize SPNEGO. SPNEGO process cannot be done due to unexpected data.
		DGFW_spnegoInitFromBinary() Error. Errno=-12 [The buffer was too small]	Failed to initialize SPNEGO. Extend the work buffer size for the SPNEGO process.
		DGFW_spnegoInitFromBinary() Error. Errno=-13 [A Token Element was invalid (e.g. improper length or value)]	Failed to initialize SPNEGO. Field data was invalid during SPNEGO analysis.
		DGFW_spnegoInitFromBinary() Error. Errno=%d [Error Code Not Found]	Failed to initialize SPNEGO. Returned value from the SPNEGO API is a known code.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG16104-70074	FATAL	DGFW_spnegoGetTokenType() Error. Errno=-1 [The supplied Token was invalid]	An error occurred during retrieval of the SPNEGO Token type. The format of the Kerberos ticket passed from the client is invalid.
		DGFW_spnegoGetTokenType() Error. Errno=-2 [An invalid length was encountered]	An error occurred during retrieval of the SPNEGO Token type. The format (length) of the Kerberos ticket passed from the client is invalid.
		DGFW_spnegoGetTokenType() Error. Errno=-3 [The Token Parsefailed]	An error occurred during retrieval of the SPNEGO Token type. An SPNEGO format analysis error.
		DGFW_spnegoGetTokenType() Error. Errno=-4 [The requested value was not found]	An error occurred during retrieval of the SPNEGO Token type. No value was found during SPNEGO analysis.
		DGFW_spnegoGetTokenType() Error. Errno=-5 [The requested element is not available]	An error occurred during retrieval of the SPNEGO Token type. Field configuration was invalid during SPNEGO analysis.
		DGFW_spnegoGetTokenType() Error. Errno=-6 [Out of Memory]	An error occurred during retrieval of the SPNEGO Token type. Failed to allocate the memory area during the SPNEGO process.
		DGFW_spnegoGetTokenType() Error. Errno=-7 [Not Implemented]	An error occurred during retrieval of the SPNEGO Token type. SPNEGO process execution error.
		DGFW_spnegoGetTokenType() Error. Errno=-8 [Invalid Parameter]	An error occurred during retrieval of the SPNEGO Token type. SPNEGO function parameter is invalid.
		DGFW_spnegoGetTokenType() Error. Errno=-9 [Token Handler encountered an unexpected OID]	An error occurred during retrieval of the SPNEGO Token type. Invalid OID was used for the SPNEGO function parameter.
		DGFW_spnegoGetTokenType() Error. Errno=-10 [The requested token was not found]	An error occurred during retrieval of the SPNEGO Token type. SPNEGO function parameter does not contain the Kerberos ticket.
		DGFW_spnegoGetTokenType() Error. Errno=-11 [An unexpected type was encountered in the encoding]	An error occurred during retrieval of the SPNEGO Token type. SPNEGO process cannot be done due to unexpected data.
		DGFW_spnegoGetTokenType() Error. Errno=-12 [The buffer was too small]	An error occurred during retrieval of the SPNEGO Token type. Extend the work buffer size for the SPNEGO process.
		DGFW_spnegoGetTokenType() Error. Errno=-13 [A Token Element was invalid (e.g. improper length or value)]	An error occurred during retrieval of the SPNEGO Token type. Field data was invalid during SPNEGO analysis.
		DGFW_spnegoGetTokenType() Error. Errno=%d [Error Code Not Found]	An error occurred during retrieval of the SPNEGO Token type. Returned value from the SPNEGO API is a known code.
EG16105-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the token work area. Output value: [Errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG16106-70075	FATAL	DGFW_spnegoGetMechToken() Error. Errno=-1 [The supplied Token was invalid]	Failed to retrieve SPNEGO MechToken. The format of the Kerberos ticket passed from the client is invalid.
		DGFW_spnegoGetMechToken() Error. Errno=-2 [An invalid length was encountered]	Failed to retrieve SPNEGO MechToken. The format (length) of the Kerberos ticket passed from the client is invalid.
		DGFW_spnegoGetMechToken() Error. Errno=-3 [The Token Parse failed]	Failed to retrieve SPNEGO MechToken. An SPNEGO format analysis error.
		DGFW_spnegoGetMechToken() Error. Errno=-4 [The requested value was not found]	Failed to retrieve SPNEGO MechToken. No value was found during SPNEGO analysis.
		DGFW_spnegoGetMechToken() Error. Errno=-5 [The requested element is not available]	Failed to retrieve SPNEGO MechToken. Field configuration was invalid during SPNEGO analysis.
		DGFW_spnegoGetMechToken() Error. Errno=-6 [Out of Memory]	Failed to retrieve SPNEGO MechToken. Failed to allocate the memory area during the SPNEGO process.
		DGFW_spnegoGetMechToken() Error. Errno=-7 [Not Implemented]	Failed to retrieve SPNEGO MechToken. SPNEGO process execution error.
		DGFW_spnegoGetMechToken() Error. Errno=-8 [Invalid Parameter]	Failed to retrieve SPNEGO MechToken. SPNEGO function parameter is invalid.
		DGFW_spnegoGetMechToken() Error. Errno=-9 [Token Handler encountered an unexpected OID]	Failed to retrieve SPNEGO MechToken. Invalid OID was used for the SPNEGO function parameter.
		DGFW_spnegoGetMechToken() Error. Errno=-10 [The requested token was not found]	Failed to retrieve SPNEGO MechToken. SPNEGO function parameter does not contain the Kerberos ticket.
		DGFW_spnegoGetMechToken() Error. Errno=-11 [An unexpected type was encountered in the encoding]	Failed to retrieve SPNEGO MechToken. SPNEGO process cannot be done due to unexpected data.
		DGFW_spnegoGetMechToken() Error. Errno=-12 [The buffer was too small]	Failed to retrieve SPNEGO MechToken. Extend the work buffer size for the SPNEGO process.
		DGFW_spnegoGetMechToken() Error. Errno=-13 [A Token Element was invalid (e.g. improper length or value)]	Failed to retrieve SPNEGO MechToken. Field data was invalid during SPNEGO analysis.
EG16107-70049	FATAL	DGFWLib_FindConfigValue(): Not Found	Failed to retrieve the SERVICE_NAME value.
EG16108-70076	FATAL	gss_import_name() Error. MajorStatus=%d [%s] MinorStatus=%d [%s]	Failed to generate the principal name. Output value: [GSS-API error code, GSS-API error message]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG16109-70077	FATAL	gss_acquire_cred() Error. MajorStatus=%d [%s] MinorStatus=%d [%s]	GSS certificate handle processing error. Output value: [GSS-API error code, GSS-API error message]
EG16110-70078	FATAL	gss_accept_sec_context() Error. MajorStatus=%d [%s] MinorStatus=%d [%s]	GSS security context establishment error. Output value: [GSS-API error code, GSS-API error message]
EG16111-70079	FATAL	gss_inquire_context() Error. MajorStatus=%d [%s] MinorStatus=%d [%s]	Security context information retrieval error. Output value: [GSS-API error code, GSS-API error message]
EG16112-70079	FATAL	gss_inquire_context() Error. MajorStatus=%d [%s] MinorStatus=%d [%s]	Security context information retrieval error. Output value: [GSS-API error code, GSS-API error message]
EG16113-70080	FATAL	gss_display_name() Error. MajorStatus=%d [%s] MinorStatus=%d [%s]	Client information retrieval error. Output value: [GSS-API error code, GSS-API error message]
EG16114-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the area for retrieving the user ID. Output value: [Errno=error number output from OS]
EG16115-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the area for retrieving the user ID. Output value: [Errno=error number output from OS]
EG16201-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the Authorization value work area. Output value: [Errno=error number output from OS]
EG16202-70081	FATAL	Authorization is not Negotiate. client value is %s	Authorization format error Output value: [%s=format error details]
EG16203-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the Authorization value work area. Output value: [Errno=error number output from OS]
EG40101-71001	FATAL	alloc Size is 0.	Cannot allocate the area because the parameter area allocation size is 0.
EG40102-70001	FATAL	malloc() Error. Errno=%d	Failed to extend the area. Output value: [Errno=error number output from OS]
EG40201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG40301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG40302-71002	FATAL	DGFWLib_ExtendBuf() Error.	Failed to extend the buffer.
EG40501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG40502-71003	FATAL	DGFWLib_ReplaceBuf() Error.	Failed to replace the string in the buffer.
EG40601-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG40603-71002	FATAL	DGFWLib_ExtendBuf() Error.	Failed to change the buffer size after replacement.
EG40604-71002	FATAL	DGFWLib_ExtendBuf() Error.	Failed to change the buffer size after replacement.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG40701-71005	FATAL	fopen() Error. File=%s	Cannot open file. Output value: [File=file name]
EG40702-71006	FATAL	fread() Error.	Cannot load file.
EG40703-71007	FATAL	DGFWLib_SetBuf() Error.	An error occurred during buffer storage.
EG40801-71005	FATAL	fopen() Error. File=%s	File open error occurred. Output value: [File=file name]
EG40802-71008	FATAL	fwrite() Error.	A file write error occurred.
EG40901-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG40903-70001	FATAL	malloc() Error. Errno=%d	Cannot allocate area for creating the extended buffer. Output value: [Errno=error number output from OS]
EG41101-71002	FATAL	DGFWLib_ExtendBuf() Error.	An error occurred during buffer extension.
EG42101-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the memory area. Output value: [Errno=error number output from OS]
EG42301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG42302-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the CHAINENTRY area. Output value: [Errno=error number output from OS]
EG42303-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the value work area. Output value: [Errno=error number output from OS]
EG42401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG42501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG44101-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the CONF area. Output value: [Errno=error number output from OS]
EG44301-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the CONF_ENTRY area. Output value: [Errno=error number output from OS]
EG44302-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the alias area. Output value: [Errno=error number output from OS]
EG44303-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the area. Output value: [Errno=error number output from OS]
EG44501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG44601-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG44701-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG44801-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG44802-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the search key area. Output value: [Errno=error number output from OS]
EG44901-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45001-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45102-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the area. Output value: [Errno=error number output from OS]
EG45201-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45202-71005	FATAL	fopen() Error. File=%s	A file open error. Output value: [File=file name]
EG45205-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the entry addition area.
EG45301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45302-71005	FATAL	fopen() Error. File=%s	A file open error. Output value: [File=file name]
EG45305-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the entry addition area.
EG45401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45402-71005	FATAL	fopen() Error. File=%s	A file open error. Output value: [File=file name]
EG45403-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the memory for the configuration file information registration area.
EG45404-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the memory for the configuration file information registration area.
EG45405-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the memory for the configuration file information registration area.
EG45406-71012	FATAL	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the memory for the configuration file information registration area.
EG45501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45502-71005	FATAL	fopen() Error. File=%s	A file open error. Output value: [File=file name]
EG45503-71013	FATAL	Entry struct doesn't exist.	Configuration file record information is NULL.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG45504-71014	FATAL	fprintf() Error.	Failed to edit the record.
EG45505-71014	FATAL	fprintf() Error.	Failed to edit the record.
EG45506-71014	FATAL	fprintf() Error.	Failed to edit the record.
EG45601-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG45602-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG46101-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the failover area. Output value: [Errno=error number output from OS]
EG46301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG46302-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the failover entry. Output value: [Errno=error number output from OS]
EG46303-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the failover list. Output value: [Errno=error number output from OS]
EG46304-70001	FATAL	malloc() Error. Errno=%d	Failed to allocate the failover entry. Output value: [Errno=error number output from OS]
EG46305-71015	FATAL	Configuration Format Error.[failover]	Failover registration data format is invalid.
EG46501-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG46601-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG46701-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG46801-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG46802-71016	FATAL	Can't Search host.	Failed to find the Authentication Server.
EG46901-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG48101-71017	FATAL	Buffer Struct Error.	Argument parameter buffer is NULL.
EG48201-71017	FATAL	Buffer Struct Error.	Argument parameter buffer is NULL.
EG48202-71018	FATAL	DGFWLib_ClearBuf() Error.	Failed to clear the buffer.
EG48203-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the status entry.
EG48204-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the status header data.
EG48205-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48206-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the MIME entry.
EG48207-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48208-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the Pragma.



## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG48209-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48210-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG48302-71018	FATAL	DGFWLib_ClearBuf() Error.	Failed to clear the buffer.
EG48303-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the status entry.
EG48304-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the status header data.
EG48305-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48306-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the MIME entry.
EG48307-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48308-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set SetCookie.
EG48309-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the session.
EG48310-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48311-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the Pragma.
EG48312-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48313-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG48314-71007	FATAL	DGFWLib_SetBuf() Error.	Failed to set the line feed code.
EG50101-71019	FATAL	Create Socket Failed.	Failed to create the client socket.
EG50102-71020	FATAL	Send Data Failed.	Failed to send data.
EG50103-71021	FATAL	Recv Data Failed.	Failed to receive data.
EG50104-71022	FATAL	Close Socket Failed.	Failed to close the socket.
EG50201-71019	FATAL	Create Socket Failed.	Failed to create the client socket.
EG50202-71020	FATAL	Send Data Failed.	Failed to send data.
EG50203-71021	FATAL	Recv Data Failed.	Failed to receive data.
EG50204-71022	FATAL	Close Socket Failed.	Failed to close the socket.
EG50301-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EG50302-71023	FATAL	Make Header Failed.	Could not perform operation for creating response header and adding to buffer.
EG50303-71024	FATAL	Get HTML Failed.	Failed to retrieve HTML.
EG50304-71025	FATAL	Replace Keyword Failed.	Failed to convert a specific keyword.
EG50401-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG50402-71023	FATAL	Make Header Failed.	Could not perform operation for creating response header and adding to buffer.
EG50403-71024	FATAL	Get HTML Failed.	Failed to retrieve HTML.
EG50404-71025	FATAL	Replace Keyword Failed.	Failed to convert a specific keyword.
EG52301-71026	FATAL	socket() Error: %s	Socket error occurred. Output value: [Error: message corresponding to error number output from OS]
EG52501-71026	FATAL	socket() Error: %s	Socket error occurred. Output value: [Error: message corresponding to error number output from OS]
EG52504-71030	FATAL	select() Error: %s	An error occurred during socket asynchronous judgment. Output value: [Error: message corresponding to error number output from OS]
EG54101-70002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI25001-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI25002-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the buffer area. Output value: [Errno=error number output from OS]
EI25003-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the buffer area. Output value: [Errno=error number output from OS]
EI25201-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI25301-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI25302-11044	FATAL	CMN_ExtendBuf() Error.	Failed to extend the buffer.
EI25501-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI25502-11044	FATAL	CMN_ExtendBuf() Error.	Failed to extend the buffer.
EI25601-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI25603-00001	FATAL	malloc() Error. Errno=%d	Failed to extend the buffer. Output value: [Errno=error number output from OS]
EI25701-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the communication information structure area. Output value: [Errno=error number output from OS]
EI25702-11004	FATAL	CMN_ClearBuf() Error.	An error occurred during creation of the receive buffer structure.
EI25703-11004	FATAL	CMN_ClearBuf() Error.	An error occurred during creation of the send buffer structure.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EI25901-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the configuration structure area. Output value: [Errno=error number output from OS]
EI26101-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI26102-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the configuration structure entry area. Output value: [Errno=error number output from OS]
EI26103-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the entry structure member area. Output value: [Errno=error number output from OS]
EI26104-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the entry structure member area. Output value: [Errno=error number output from OS]
EI26301-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI26501-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI26601-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI26701-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI26702-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the changed entry structure member area. Output value: [Errno=error number output from OS]
EI27401-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the failover structure area. Output value: [Errno=error number output from OS]
EI32001-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI32101-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI32701-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI32901-00002	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI32902-11075	FATAL	CMN_GetTimeNow() Error.	Failed to retrieve the current time.
EI32903-11073	FATAL	localtime_r() Error.	Failed to retrieve the time element.
EI32904-11068	FATAL	Module type Format Error [%s].	Module type format in the transaction ID is invalid. Output value: [configuration value]
EI32905-11069	FATAL	Transid_str Format Error [%s].	Identification string format in the transaction ID is invalid. Output value: [configuration value]
EI32906-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the memory area required for creating the transaction ID. Output value: [Errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EI90001-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the buffer area for URL encoding. Output value: [Errno=error number output from OS]
EI90101-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the buffer area for URL decoding. Output value: [Errno=error number output from OS]
EI90201-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90202-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90203-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the buffer disassembly work area. Output value: [Errno=error number output from OS]
EI90205-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate entry area. Output value: [Errno=error number output from OS]
EI90301-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90303-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate buffer for concatenating work area. Output value: [Errno=error number output from OS]
EI90401-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90402-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90403-11005	FATAL	CMN_SetBuf() Error.	Failed to set the fixed format to the encryption data buffer.
EI90404-11005	FATAL	CMN_SetBuf() Error.	Failed to set the fixed format to the encryption data buffer.
EI90405-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90406-11005	FATAL	CMN_SetBuf() Error.	Failed to set the fixed format to the encryption data buffer.
EI90407-11005	FATAL	CMN_SetBuf() Error.	Failed to set the fixed format to the encryption data buffer.
EI90408-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90409-11005	FATAL	CMN_SetBuf() Error.	Failed to set the fixed format to the encryption data buffer.
EI90410-11005	FATAL	CMN_SetBuf() Error.	Failed to set the fixed format to the encryption data buffer.
EI90411-11005	FATAL	CMN_SetBuf() Error.	Failed to set the fixed format to the encryption data buffer.
EI90413-11005	FATAL	CMN_SetBuf() Error.	Failed to set the send data buffer header and arbitrary header separator.
EI90414-11005	FATAL	CMN_SetBuf() Error.	Failed to set the send data buffer header and arbitrary header.
EI90415-11005	FATAL	CMN_SetBuf() Error.	Failed to set the separator character for the send data buffer.
EI90416-11005	FATAL	CMN_SetBuf() Error.	Failed to set the encrypted body section for the send data buffer.
EI90417-11005	FATAL	CMN_SetBuf() Error.	Could not add the transaction ID to the header.
EI90418-11005	FATAL	CMN_SetBuf() Error.	Could not store [m] in the buffer.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EI90419-11005	FATAL	CMN_SetBuf() Error.	Could not store [m] in the buffer.
EI90420-11005	FATAL	CMN_SetBuf() Error.	Could not add the ICP encryption method to the header.
EI90501-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90502-19015	FATAL	ICP Format Error.	ICP communication data format is invalid. [Failed to retrieve fixed header information. ]
EI90503-19015	FATAL	ICP Format Error.	ICP communication data format is invalid. [Failed to retrieve fixed header information. ]
EI90504-19015	FATAL	ICP Format Error.	ICP communication data format is invalid. [Failed to retrieve fixed header information. ]
EI90505-19015	FATAL	ICP Format Error.	ICP communication data format is invalid. [Failed to retrieve separator for header suffix.]
EI90601-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI90602-19015	FATAL	ICP Format Error.	ICP communication data format is invalid. [Failed to retrieve body.]
EI90603-19015	FATAL	ICP Format Error.	ICP communication data format is invalid. [Body is 0 bytes.]
EI90604-19020	FATAL	Content-length Error. [%d] Body=[%d]	Content-length value and received body length do not match.
EI92001-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the ICP communication structure area. Output value: [Errno=error number output from OS]
EI92002-11008	FATAL	CMN_CreateComData() Error.	Failed to create send/receive data structure.
EI92101-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate splitting data structure area. Output value: [Errno=error number output from OS]
EI92601-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI92602-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the method area in the header structure. Output value: [Errno=error number output from OS]
EI92603-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the path area in the header structure. Output value: [Errno=error number output from OS]
EI92604-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate ICP version area in the header structure. Output value: [Errno=error number output from OS]
EI92605-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate ICP version area in the header structure. Output value: [Errno=error number output from OS]
EI92606-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the message area in the header structure. Output value: [Errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EI92701-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI92702-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI92703-19003	FATAL	Create Socket Failed.	Failed to create the client socket.
EI92704-19006	FATAL	Send Data Failed.	Failed to send ICP 1.0 encryption data.
EI92705-19005	FATAL	Recv Data Failed.	Failed to receive ICP 1.0 decryption data.
EI92706-19006	FATAL	Send Data Failed.	Failed to send ICP 2.0 encryption data.
EI92707-19005	FATAL	Recv Data Failed.	Failed to receive ICP 2.0 encryption data.
EI92708-19004	FATAL	Close Socket Failed.	Failed to close socket.
EI94101-19007	FATAL	Bad Response Data.	Response data is invalid.
EI94201-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI94202-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI94203-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI94204-19002	FATAL	malloc() Error. Errno=%d	Failed to create area for AGENT_ID message. Output value: [Errno=error number output from OS]
EI95701-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI95801-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI95802-19018	FATAL	Not Found. [%s]	User ID not found. Output value: [unretrievable data]
EI95804-19018	FATAL	Not Found. [%s]	Remote address not found. Output value: [unretrievable data]
EI95901-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI95902-19016	FATAL	No Match ICP Version. Send[%s] -> Recv[%s]	ICP version does not match. Output value: [Send[sent ICP version] - Recv[received ICP version]]
EI95903-19007	FATAL	Bad Response Data.	Response data is invalid.
EI96001-19003	FATAL	Create Socket Failed.	Failed to create the socket.
EI96002-19006	FATAL	Send Data Failed.	Failed to send data.
EI96003-19005	FATAL	Recv Data Failed.	Failed to receive data.
EI96004-19004	FATAL	Close Socket Failed.	Failed to close socket.
EI96005-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI96006-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.

---

**IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX**

---

Code ID	Level	Message	Description
EI96101-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI96201-19022	FATAL	socket() Error: %s	Socket error occurred. Output value: [error message output from OS]
EI96208-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI96209-00001	FATAL	malloc() Error. Errno=%d	Failed to allocate the connection target host information storage area. Output value: [Errno=error number output from OS]
EI96403-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI96906-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI96705-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI97003-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI97201-19001	FATAL	Parameter is NULL.	Argument parameter is NULL.
EI97202-19002	FATAL	malloc() Error. Errno=%d	Failed to allocate the memory area. Output value: [Errno=error number output from OS]
EG00108-70006	WARNING	DGFW_Login() Error. [11][ Duplicate Login Detected.]	An authentication error occurred. Already logged in.
		DGFW_Login() Error. [12][ Unregistered Domain Gateway OptionServer IP Address.]	An authentication error occurred. IP address of the server where the Domain Gateway Option is running is not defined in FEDERATION of the Authentication Module.
		DGFW_Login() Error. [13] [ UserID Not Found]	An authentication error occurred. User is not registered in the Authentication DB.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
		DGFW_Login() Error. [14][ Invalid Ticket.]	An authentication error occurred. Failed to analyze the Kerberos ticket.
		DGFW_Login() Error. [15][ Client Certificate Required.]	An authentication error occurred. Pre-authentication performed with the client certificate.
		DGFW_Login() Error. [16][ Account Suspended By Failed Login Attempts.]	An authentication error occurred. User is not allowed for login.
		DGFW_Login() Error. [17][ No Group Assigned.]	An authentication error occurred. No group.
		DGFW_Login() Error. [18][ Account Suspended.]	An authentication error occurred. User ID is locked.
		DGFW_Login() Error. [19][ Login Limit Reached.]	An authentication error occurred. Maximum login count has been reached.
		DGFW_Login() Error. [20][ System Error]	An authentication error occurred. A known problem occurred with the Domain Gateway Option or Authentication Module.
		DGFW_Login() Error. [21][ Certification Module Down.]	An authentication error occurred. Authentication Module is down.
		DGFW_Login() Error. [22][ Database Down.]	An authentication error occurred. Authentication DB is down.
		DGFW_Login() Error. [23][ Certification Module Timed-out.]	An authentication error occurred. No response from the Authentication Module.
		DGFW_Login() Error. [24][ UserExit 1 Returned.]	An authentication error occurred. Return value from the Authentication Module was the user-defined error 1.
		DGFW_Login() Error. [25][ UserExit 2 Returned.]	An authentication error occurred. Return value from the Authentication Module was the user-defined error 2.
		DGFW_Login() Error. [26][ UserExit 3 Returned.]	An authentication error occurred. Return value from the Authentication Module was the user-defined error 3.
EG00110-70006	WARNING	DGFW_Login() Error. [11][ Duplicate Login Detected.]	An authentication error occurred. Already logged in.
		DGFW_Login() Error. [12][ Unregistered Domain Gateway OptionServer IP Address.]	An authentication error occurred. IP address of the server where the Domain Gateway Option is running is not defined in FEDERATION of the Authentication Module.
		DGFW_Login() Error. [13][ UserID Not Found]	An authentication error occurred. User is not registered in the Authentication DB.
		DGFW_Login() Error. [14][ Invalid Ticket.]	An authentication error occurred. Failed to analyze the Kerberos ticket.



## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
		DGFW_Login() Error. [15][ Client Certificate Required.]	An authentication error occurred. Pre-authentication performed with the client certificate.
		DGFW_Login() Error. [16][ Account Suspended By Failed Login Attempts.]	An authentication error occurred. User is not allowed for login.
		DGFW_Login() Error. [17][ No Group Assigned.]	An authentication error occurred. No group.
		DGFW_Login() Error. [18][ Account Suspended.]	An authentication error occurred. User ID is locked.
		DGFW_Login() Error. [19][ Login Limit Reached.]	An authentication error occurred. Maximum login count has been reached.
		DGFW_Login() Error. [20][ System Error]	An authentication error occurred. A known problem occurred with the Domain Gateway Option or Authentication Module.
		DGFW_Login() Error. [21][ Certification Module Down.]	An authentication error occurred. Authentication Module is down.
		DGFW_Login() Error. [22][ Database Down.]	An authentication error occurred. Authentication DB is down.
		DGFW_Login() Error. [23][ Certification Module Timed-out.]	An authentication error occurred. No response from the Authentication Module.
		DGFW_Login() Error. [24][ UserExit 1 Returned.]	An authentication error occurred. Return value from the Authentication Module was the user-defined error 1.
		DGFW_Login() Error. [25][ UserExit 2 Returned.]	An authentication error occurred. Return value from the Authentication Module was the user-defined error 2.
		DGFW_Login() Error. [26][ UserExit 3 Returned.]	An authentication error occurred. Return value from the Authentication Module was the user-defined error 3.
EG00111-70007	WARNING	DGFW_GetTktUidCtrl() Error.	An error occurred during the ticket verification process.
EG00115-70082	WARNING	gettimeofday() Error. Errno=%d	Failed to retrieve the time. Output value: [Errno=error number output from OS]
EG00116-70082	WARNING	gettimeofday() Error. Errno=%d	Failed to retrieve the time. Output value: [Errno=error number output from OS]
EG00117-70082	WARNING	gettimeofday() Error. Errno=%d	Failed to retrieve the time. Output value: [Errno=error number output from OS]
EG00118-70082	WARNING	gettimeofday() Error. Errno=%d	Failed to retrieve the time. Output value: [Errno=error number output from OS]
EG00119-70082	WARNING	gettimeofday() Error. Errno=%d	Failed to retrieve the time. Output value: [Errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG00120-70082	WARNING	gettimeofday() Error. Errno=%d	Failed to retrieve the time. Output value: [Errno=error number output from OS]
EG00123-71040	WARNING	Configuration format error.[%s]	Set value for the TRANSID_STR parameter is invalid. Output value: [TRANSID_STR]
EG00124-71040	WARNING	Configuration format error.[%s]	Set value for the TRANSID_STR parameter is invalid. Output value: [TRANSID_STR]
EG00126-70084	WARNING	CMN_CreateTIDString() Error.	Failed to generate the transaction ID.
EG02102-70009	WARNING	Can't Set Default Data.	Failed to extend the default value of the set value.
EG02103-70010	WARNING	DGFW_ReadFile() Error.	Failed to load dgfw.conf.
EG02104-70011	WARNING	DGFW_SplitConf() Error.	Failed to load data read from dgfw.conf into memory.
EG02105-70010	WARNING	DGFW_ReadFile() Error.	Failed to load dfw.conf.
EG02106-70011	WARNING	DGFW_SplitConf() Error.	Failed to load data read from dfw.conf into memory.
EG02107-70012	WARNING	DGFW_Conf_Add() Error.	Failed to load data read from the configuration file into memory.
EG02502-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02602-70022	WARNING	DGFW_SetCertInfo() Error.	Could not store CERT information in the structure.
EG02603-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02604-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02605-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02606-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02607-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02608-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02609-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02610-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02611-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02612-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02613-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02614-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02615-70022	WARNING	DGFW_SetCertInfo() Error.	Could not store CERT information in the structure.
EG02616-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.
EG02617-70021	WARNING	DGFW_SetBasicInfo() Error.	An error occurred during storage of the basic information structure.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG02704-70023	WARNING	DGFWLib_ModifyConfigValue() Error.	Failed to extend memory for the set value.
EG02802-70026	WARNING	Not Include '='.	Cannot find “=”.
EG02803-70027	WARNING	DGFW_CreateFailoverEntry() Error.	Failed to create the failover entry.
EG02804-70028	WARNING	DGFWLib_ModifyFailoverEntry() Error.	Failed to create the failover entry.
EG02805-70027	WARNING	DGFW_CreateFailoverEntry() Error.	Failed to create the failover entry.
EG02806-70023	WARNING	DGFWLib_ModifyConfigValue() Error.	Failed to set the value.
EG02807-71012	WARNING	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the area.
EG02808-70024	WARNING	DGFWLib_AddConfigEntry() Error.	Failed to set the value.
EG02809-70023	WARNING	DGFWLib_ModifyConfigValue() Error.	Failed to set the value.
EG02810-71012	WARNING	DGFWLib_CreateConfigEntry() Error.	Failed to allocate the area.
EG02811-70024	WARNING	DGFWLib_AddConfigEntry() Error.	Failed to set the value.
EG06104-70031	WARNING	DGFW_LoginConnection() Error.	Error occurred during communication with the Authentication Module.
EG06202-70035	WARNING	DGFW_SetLoginRequest() Error.	Failed to create the authentication request message.
EG06203-70036	WARNING	Can't Divide Login Response.	Failed to analyze the authentication response message.
EG06206-70086	WARNING	ICP_SetFederationLoginRequest() Error.	Failed in creation of the ICP 2.0 login request message.
EG06209-70090	WARNING	DGFW_OptimizeResponse() Error.	Failed to optimize the ICP 2.0 response message.
EG06210-70036	WARNING	Can't Divide Login Response.	Failed to analyze the authentication response message.
EG06302-71048	WARNING	CMN_SetBuf() Error.	An error occurred during buffer storage.
EG06402-70002	WARNING	Bad Response Data.	Format of the response message from the Authentication Module is invalid.
EG07003-71049	WARNING	CMN_DistributesFromStr() Error.	Selection of the Authentication Module failed.
EG08124-70051	WARNING	DGFW_AuthenticateHTML() Error.	Failed to load ticket presentation request HTML.
EG08125-70052	WARNING	DGFW_GetIcewallHTML() Error.	Failed to create the response message for authentication success.
EG08439-70021	WARNING	DGFW_SetBasicInfo() Error.	Failed to set the template HTML file path.
EG08703-70061	WARNING	DGFW_SetKeyword() Error.	Failed to register the keyword entry.
EG08704-70061	WARNING	DGFW_SetKeyword() Error.	Failed to register the keyword entry.
EG08705-70061	WARNING	DGFW_SetKeyword() Error.	Failed to register the keyword entry.
EG08706-70061	WARNING	DGFW_SetKeyword() Error.	Failed to register the keyword entry.
EG08707-70061	WARNING	DGFW_SetKeyword() Error.	Failed to register the keyword entry.
EG08708-70062	WARNING	DGFWLib_ChangeKeyword() Error.	Failed to convert a specific keyword.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG08709-70061	WARNING	DGFW_SetKeyword() Error.	Failed to register the keyword entry.
EG16101-70071	WARNING	DGFW_GetAuthStr() Error.	Authorization value format was invalid.
EG45203-71010	WARNING	Configuration Invalid Entry.	Entry format error.
EG45204-71011	WARNING	Configuration Invalid Entry. Entry=%s	Entry format error.
EG45303-71010	WARNING	Configuration Invalid Entry.	Argument parameter is NULL.
EG45304-71011	WARNING	Configuration Invalid Entry. Entry=%s	Entry format error.
EG52302-71027	WARNING	gethostbyname() Error: %s	Failed to resolve the name. Output value: [host name]
EG52303-71028	WARNING	connect() Error: %s	A connection error occurred. Output value: [Error: message corresponding to error number output from OS]
EG52502-71029	WARNING	DGFWLib_SockNonblock() Error.	Cannot set socket to the non-blocking mode.
EG52503-71027	WARNING	gethostbyname() Error: %s	Failed to resolve the name. Output value: [host name]
EG52505-71031	WARNING	connect() Error: %s(errno=%d)	A connection error occurred. Output value: [error message output from OS], [error number output from OS]
EG52506-71032	WARNING	fcntl() Error: %s	An error occurred in executing operation to return to state before non-blocking. Output value: message corresponding to error number output from OS]
EG52507-71033	WARNING	ioctl() Error: %s	An error occurred in executing operation to return to blocking. Output value: message corresponding to error number output from OS]
EG52508-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]
EG52509-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]
EG52510-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG52602-71035	WARNING	close() Error: %s(errno=%d)	Failed to close the socket. Output value: [error message output from OS], [errno=error number output from OS]
EG52701-71033	WARNING	ioctl() Error: %s	Cannot set socket to the non-blocking mode. Output value: message corresponding to error number output from OS]
EG52702-71032	WARNING	fcntl() Error: %s	Cannot set socket to the non-blocking mode. Output value: message corresponding to error number output from OS]
EG53001-71036	WARNING	Send Data is NULL.	Send buffer is NULL.
EG53002-71037	WARNING	send timeout.	Send timeout occurred.
EG53003-71038	WARNING	send Error.	A send error occurred.
EG53004-71039	WARNING	send() Error: %s(%d)	Send error. Output value: [error message output from OS], [errno=error number output from OS]
EG53005-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]
EG53101-71036	WARNING	Send Data is NULL.	Send data is NULL.
EG53102-71040	WARNING	DGFWLib_CreateSocketData() Error.	Could not allocate the buffer area.
EG53103-71007	WARNING	DGFWLib_SetBuf() Error.	An error occurred during buffer storage.
EG53104-71041	WARNING	DGFWLib_CryptoBuf() Error.	An error occurred during data encryption.
EG53105-71042	WARNING	DGFWLib_Send() Error.	An error occurred during data send.
EG53106-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]
EG53107-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]
EG53108-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EG53109-71034	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]
EG53201-71029	WARNING	DGFWLib_SockNonblock() Error.	Cannot set socket to the non-blocking mode.
EG53202-71043	WARNING	DGFWLib_RecvSelect() Error.	An error occurred during data receive.
EG53203-71044	WARNING	DGFWLib_RecvSelect() Timeout.	The data receive operation timed out.
EG53204-71045	WARNING	recv() Error: %s	Receive error. Output value: [Errno=error number output from OS]
EG53205-71007	WARNING	DGFWLib_SetBuf() Error.	An error occurred during buffer storage.
EG53301-71046	WARNING	DGFWLib_Recv() Error.	An error occurred during data receive.
EG53302-71041	WARNING	DGFWLib_CryptoBuf() Error.	An error occurred during data encryption.
EG53401-71047	WARNING	DGFWLib_CloseSocket() Error.	An error occurred during socket close.
EI32102-11063	WARNING	gettimeofday() Error. Errno=%d	Failed to retrieve the time. Output value: [Errno=error number output from OS]
EI90412-19017	WARNING	ICP_JoinBuffer() Error.	Failed to concatenate the send data body.
EI90506-19014	WARNING	ICP_CutBuffer() Error.	Failed to split the receive data header.
EI90507-19014	WARNING	ICP_CutBuffer() Error.	Failed to split receive the data body.
EI92003-19013	WARNING	ICP_CreateParseData() Error.	Failed to create the structure for parsed receive data of response mode.
EI92004-19013	WARNING	ICP_CreateParseData() Error.	Failed to create the structure for parsed send data of request mode.
EI92102-11010	WARNING	CMN_CreateConf() Error.	Cannot create the header structure.
EI92103-11010	WARNING	CMN_CreateConf() Error.	Cannot create the body structure.
EI94102-11016	WARNING	CMN_ModifyConfValue() Error.	Failed to convert error number.
EI94103-11011	WARNING	CMN_CreateConfEntry() Error.	An error occurred when adding entry.
EI94104-11011	WARNING	CMN_CreateConfEntry() Error.	An error occurred when adding entry.
EI95702-11016	WARNING	CMN_ModifyConfValue() Error.	Failed to convert error number.
EI95703-11003	WARNING	CMN_CreateBuf() Error.	Failed to allocate work area for Description information.
EI95704-11005	WARNING	CMN_SetBuf() Error.	Failed to create Description information.
EI95705-11005	WARNING	CMN_SetBuf() Error.	Failed to create Description information.
EI95706-11005	WARNING	CMN_SetBuf() Error.	Failed to create Description information.
EI95707-11005	WARNING	CMN_SetBuf() Error.	Failed to create Description information.

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EI95708-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to allocate the Description information entry.
EI95709-11012	WARNING	CMN_AddConfEntry() Error.	Failed to add the Description information entry.
EI95710-11016	WARNING	CMN_ModifyConfValue() Error.	Failed to change Description information.
EI95711-19007	WARNING	Bad Response Data.	Response type is invalid.
EI95712-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the user ID information entry.
EI95713-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the password information entry.
EI95805-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the entry.
EI95806-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the entry.
EI95807-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the entry.
EI95809-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the entry.
EI95810-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the entry.
EI95812-11011	WARNING	CMN_CreateConfEntry() Error.	Failed to create the entry.
EI96202-19023	WARNING	ICP_SockNonblock() Error.	Cannot set socket to the non-blocking mode.
EI96205-19026	WARNING	connect() Error: %s(errno=%d)	A connection error occurred. Output value: [error message output from OS], [errno=error number output from OS]
EI96206-19027	WARNING	fcntl() Error: %s	An error occurred in executing operation to return to state before non-blocking. Output value: [error message output from OS]
EI96207-19028	WARNING	ioctl() Error: %s	An error occurred in executing operation to return to blocking. Output value: [error message output from OS]
EI96210-19046	WARNING	getaddrinfo() error. Can't get network address. errno=[%d] errmsg=[%s] host=[%s:%d]	Failed to retrieve the network address Output value: [errno=error number output from OS], [errmsg=error message retrieved from OS], [host=host name:port]
EI96211-19047	WARNING	Priority IPVerInfo was not able to be acquired. host=[%s:%d]	Could not retrieve the network address of the prioritized version. Output value: host name:port number]
EI96212-19047	WARNING	Priority IPVerInfo was not able to be acquired. host=[%s:%d]	Could not retrieve the network address of the prioritized version. Output value: host name:port number]
EI96213-19048	WARNING	All IPVerInfo was not able to be acquired. host=[%s:%d]	Could not retrieve the network address of all versions. Output value: host name:port number]

## IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX

Code ID	Level	Message	Description
EI96214-19049	WARNING	getnameinfo() error. errno=[%d] errmsg=[%s]	Failed to convert the network address. Output value: [errno=error number output from OS errmsg=error message retrieved from OS]
EI96215-19050	WARNING	if_nametoindex() error. errno=[%d] errmsg=[%s]	Failed to convert the interface. Output value: [errno=error number output from OS errmsg=error message retrieved from OS]
EI96301-19029	WARNING	shutdown() Error: %s(errno=%d)	Failed to shut down the socket. Output value: [error message output from OS], [errno=error number output from OS]
EI96302-19030	WARNING	close() Error: %s(errno=%d)	Failed to close the socket. Output value: [error message output from OS], [errno=error number output from OS]
EI96401-19027	WARNING	fcntl() Error: %s	Cannot set socket to the non-blocking mode. Output value: [error message output from OS]
EI96402-19028	WARNING	ioctl() Error: %s	Cannot set socket to the non-blocking mode. Output value: [error message output from OS]
EI96701-19031	WARNING	Send Data is NULL.	Send data is NULL.
EI96702-19032	WARNING	send timeout.	Send operation timed out.
EI96703-19033	WARNING	send Error.	Send error.
EI96704-19034	WARNING	send() Error: %s(%d)	Send error. Output value: [error message output from OS], [error number output from OS]
EI96801-19031	WARNING	Send Data is NULL.	Send data is NULL.
EI96802-11008	WARNING	CMN_CreateComData() Error.	Failed to create the socket data structure.
EI96803-11005	WARNING	CMN_SetBuf() Error.	An error occurred during buffer storage.
EI96804-19036	WARNING	ICP_CryptoBuf() Error.	An error occurred during data encryption.
EI96805-19037	WARNING	ICP_Send() Error.	An error occurred during data send.
EI96901-19023	WARNING	ICP_SockNonblock() Error.	Cannot set socket to the non-blocking mode.
EI96902-19038	WARNING	ICP_RecvSelect() Error.	An error occurred during data receive.
EI96903-19039	WARNING	ICP_RecvSelect() Timeout.	The data receive operation timed out.



---

**IceWall SSO Version 10.0 / Installation Guide of Domain Gateway Option for UNIX**

---

Code ID	Level	Message	Description
EI96904-19040	WARNING	recv() Error: %s	Receive error. Output value: [Errno=error number output from OS]
EI96905-11005	WARNING	CMN_SetBuf() Error.	An error occurred during buffer storage.
EI97001-19041	WARNING	ICP_Recv() Error.	An error occurred during data receive.
EI97002-19036	WARNING	ICP_CryptoBuf() Error.	An error occurred during data encryption.
EI97203-11007	WARNING	CMN_StrInsertBuf() Error.	Failed in inserting data to the buffer.
EI97301-19031	WARNING	Send Data is NULL.	Send data is NULL.
EI97302-11008	WARNING	CMN_CreateComData() Error.	Failed in creating the socket structure.
EI97303-11005	WARNING	CMN_SetBuf() Error.	An error occurred during buffer storage.
EI97304-19036	WARNING	ICP_CryptoBuf() Error.	An error occurred during data encryption.
EI97305-19044	WARNING	ICP_AddICPHeader() Error.	An error occurred during ICP header processing.
EI97306-19037	WARNING	ICP_Send() Error.	An error occurred during data send.
EI90204-19015	INFO	ICP Format Error.	ICP communication data fixed format is invalid. [Line separator is not a line feed code.
EI90206-19015	INFO	ICP Format Error.	ICP communication data format is invalid. [Name is NULL.]
EI90302-19001	INFO	Parameter is NULL.	Argument parameter is NULL.
EI95811-19018	INFO	Not Found. [%s]	No User-Agent found. Output value: [unretrievable data]

