



# **IceWall SSO**

Version 10.0

## **Reference Manual**

August 2010

**Printed in Japan**

**HP Part No. B1544-94000**

**Rev.111020B**

## 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 Japan, Ltd. 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 Japan, Ltd.

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 Japan, Ltd.

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	Configuration file format .....	1
1.2	Version designations in the text .....	1
2	Forwarder .....	2
2.1	Forwarder configuration file (dfw.conf) .....	3
2.1.1	Basic configuration parameters .....	6
	ALEVEL .....	7
	ELEVEL .....	8
	ACCESS .....	9
	ERROR .....	10
	ERRORINFO .....	11
	TRACE .....	12
	CATALOG <small>(10.0)</small> .....	13
	SECURITY .....	14
	SECINFO <small>(10.0)</small> .....	15
	SECLEVEL .....	16
	SECEXCPAGE .....	17
	SPKEY_TOPPAGE_URL <small>(10.0)</small> .....	18
	TRANSID <small>(10.0)</small> .....	20
	TRANSID_STR <small>(10.0)</small> .....	22
	TRACETIME <small>(10.0)</small> .....	23
	DFW_PROTOCOL .....	24
	REQUEST_URI .....	25
	VIRTUALPATH_ENV .....	26
	VIRTUALURL_ALIAS .....	27
2.1.2	User authentication parameters .....	28
	CERT <small>overwrite (10.0)</small> .....	30
	CERTLB <small>overwrite (10.0)</small> .....	32
	CERTLB_TYPE <small>(10.0)</small> .....	34
	CERTFAILBACK <small>(10.0)</small> .....	36
	CERTLBFAILBACK <small>(10.0)</small> .....	38
	COOKIENAME .....	40
	COOKIEATTR .....	42
	COOKIEALWAYS .....	44
	POSTLIMIT_PAGE .....	46
	POSTLIMIT_TIME .....	47
	POSTLIMIT_ENC .....	48
	FORCELOGIN_ENC .....	49
	SESSION .....	50
	POSTKEY_LOGIN .....	51
	POSTKEY_LOGOUT .....	52
	POSTKEY_PWDCHG .....	53
	REDIRECT <small>(10.0)</small> .....	54
	LOALIAS .....	56
	ICP_VERSION <small>(10.0)</small> .....	57
	ICP_AGENTSTR .....	58
	ICP_ENCSTR <small>(10.0)</small> .....	60
2.1.3	Template HTML parameters .....	61

DOCS .....	62
LOCATIONURL <sup>(10.0)</sup> .....	63
LOCATIONRETRY .....	64
HTML_CHARSET .....	65
2.1.4 Backend Web Server parameters .....	66
HOST <sup>overwrite</sup> <sup>(10.0)</sup> .....	67
SHOST <sup>overwrite</sup> <sup>(10.0)</sup> .....	70
SVRFILE .....	72
2.1.5 Password change parameters .....	73
PWDALIAS .....	74
MINLEN <sup>(10.0)</sup> .....	75
MAXLEN <sup>(10.0)</sup> .....	76
EXPIRE <sup>(10.0)</sup> .....	77
SAMEPASS <sup>(10.0)</sup> .....	79
ALPHANUM <sup>(10.0)</sup> .....	80
2.1.6 Performance tuning parameters .....	82
RETRYCNTC .....	83
RETRYTMC <sup>(10.0)</sup> .....	84
CERT_TOUT .....	86
ALLOC .....	87
SET_CONTENT_LENGTH .....	88
POSTWAITTIME .....	89
2.1.7 Security parameters .....	90
MAXURL .....	91
MAXQUERY .....	92
REV_PATH <sup>(10.0)</sup> .....	93
SESSION_ENC_KEY .....	95
DFWFILTER .....	96
NOCHK_EXT_ALIAS .....	98
REQUESTFILTER <sup>(10.0)</sup> .....	101
2.1.8 Client certificate parameters .....	103
CC_UID .....	104
CC_UIDKEYS .....	105
CC_UIDKEYE .....	106
CC_ENVNAME .....	108
CC_DECODE_FLG .....	109
CC_ENVUID .....	110
CC_ENVSERIAL .....	111
CC_ENVEXPIRE .....	112
CC_ENVISSUER .....	113
2.1.9 POST data inheritance parameters .....	114
POST_INHERIT .....	115
MAXPOST .....	116
POSTNAME .....	117
POST_HTML .....	118
POST_ENC .....	119
2.1.10 Agent parameters .....	120
AGENT_KEY .....	121
AGENT_PERMIT <sup>(10.0)</sup> .....	122
QUERY_ENC .....	124
QUERY_ENC_NAME .....	125

QUERY_ENC_KIND .....	126
RELOGIN_KEY .....	127
2.2 Host configuration file <u>[arbitrary file name]</u> .....	128
2.2.1 Parameters for content conversion .....	131
CTYPE .....	132
URLKEY .....	133
REPKEY .....	135
REPKEY_EXT <sup>(10.0)</sup> .....	137
URLCONV_FLG .....	139
URLCONV_ATTR_FLG <sup>(10.0)</sup> .....	141
ATTRQUOT_FLG .....	143
2.2.2 Error page parameters .....	144
SYSERR <sup>(10.0)</sup> .....	145
SYSTOUT <sup>(10.0)</sup> .....	147
ERRKEY <sup>(10.0)</sup> .....	149
2.2.3 Basic authentication parameters .....	151
BASICAUTH .....	152
BA_UID .....	153
BA_PWD .....	154
2.2.4 Parameters for information inheritance .....	155
HTTPDATA .....	156
HEADER .....	158
HEADER_FILTER <sup>(10.0)</sup> .....	160
COOKIE_FILTER .....	162
HEADER_NAME_TID <sup>(10.0)</sup> .....	163
HEADER_NAME_UID <sup>(10.0)</sup> .....	164
HEADER_NAME_SID <sup>(10.0)</sup> .....	165
RES_HEADER <sup>(10.0)</sup> .....	166
UNCONV_HEADER .....	168
CTRL_SPKEY <sup>(10.0)</sup> .....	169
2.2.5 Parameters for handling cross site scripting .....	171
GETFILTER .....	172
GETEXCEPTION .....	173
GETFILTERERR <sup>(10.0)</sup> .....	174
GETFILTER_LOG_FLG .....	176
POSTFILTER .....	177
POSTEXCEPTION .....	178
POSTFILTERERR <sup>(10.0)</sup> .....	179
POSTFILTER_LOG_FLG .....	181
HTMLFILTER .....	182
HTMLFILTERERR <sup>(10.0)</sup> .....	183
SVRFILTER .....	185
SVREXCEPTION .....	187
SVRFILTERERR <sup>(10.0)</sup> .....	188
SVRFILTERSTR .....	190
2.2.6 System tuning configuration parameters .....	192
RETRYCNTW .....	193
RETRYTMW <sup>(10.0)</sup> .....	194
TIMEOUT .....	196
CLOSETIME <sup>(10.0)</sup> .....	198
BUFFER .....	200

LASTMOD_HEADER .....	201
CENCODE .....	202
URL_SCOLON .....	204
FO_SEND .....	205
FO_RECV .....	206
FO_NODATA .....	207
RECV_ZERO_FLG .....	208
2.2.7 Form authentication configuration parameters .....	209
FORM_FILE .....	210
2.2.8 Security parameters .....	211
SSL_CIPHER_SUITE .....	212
2.3 Form authentication configuration file (arbitrary file) .....	213
2.3.1 Form authentication configuration parameters .....	214
FORM_METHOD .....	215
FORM_SEND .....	216
FORM_URL .....	217
FORM_KEY .....	218
FORM_KEY_EXCEPTION <sup>(10.0)</sup> .....	220
FORM_HTML .....	222
FORM_DATA_STR .....	224
FORM_DATA_USR .....	226
FORM_DATA_PAGE <sup>(10.0)</sup> .....	228
FORM_DATA_PAGE_REF <sup>(10.0)</sup> .....	230
2.4 HTML configuration file (html.conf) .....	232
2.4.1 Login related page parameters .....	234
LOGIN_UID <sup>(10.0)</sup> .....	235
LOGIN_CERT <sup>(10.0)</sup> .....	237
LOGIN_FORCE <sup>(10.0)</sup> .....	239
LOGIN_ERR_UID <sup>(10.0)</sup> .....	241
LOGIN_ERR_PWD <sup>(10.0)</sup> .....	243
LOGIN_ERR_LOCK <sup>(10.0)</sup> .....	245
LOGIN_ERR_1STCERT <sup>(10.0)</sup> .....	247
LOGIN_ERR_SERIAL <sup>(10.0)</sup> .....	249
LOGIN_ERR_NOGRP <sup>(10.0)</sup> .....	251
LOGIN_ERR_STOP <sup>(10.0)</sup> .....	253
LOGIN_ERR_LIMIT <sup>(10.0)</sup> .....	255
LOGIN_ERR_POSTLIMIT <sup>(10.0)</sup> .....	257
2.4.2 Access control related page parameters .....	259
ACCESS_DENY <sup>(10.0)</sup> .....	260
DATA_SEND_ERR <sup>(10.0)</sup> .....	262
REQUEST_ACL_ERR <sup>(10.0)</sup> .....	264
FILTER_REQUEST <sup>(10.0)</sup> .....	266
2.4.3 POST data inheritance related page parameters .....	268
MAXPOST_ERR <sup>(10.0)</sup> .....	269
2.4.4 Logout related page parameters .....	271
LOGOUT <sup>(10.0)</sup> .....	272
LOGOUT_SUCCESS <sup>(10.0)</sup> .....	274
LOGOUT_EXPIRE <sup>(10.0)</sup> .....	276
LOGOUT_FAILURE <sup>(10.0)</sup> .....	278
2.4.5 Password change related page parameters .....	280
PWDCHG <sup>(10.0)</sup> .....	281

PWDCHG_SUCCESS 10.0	283
PWDCHG_ERR_OLD 10.0	285
PWDCHG_ERR_REENT 10.0	287
PWDCHG_ERR_POLICY 10.0	289
PWDCHG_ERR_LOGNG 10.0	291
PWDCHG_ERR_VIO 10.0	293
PWDCHG_FAILURE 10.0	295
PWDCHG_WARNING 10.0	297
PWDCHG_ERR_POSTLIMIT 10.0	299
2.4.6 Cross site scripting error related page parameters	301
FILTER_GET 10.0	302
FILTER_POST 10.0	304
FILTER_HTML 10.0	306
FILTER_SVR 10.0	308
2.4.7 System error related page parameters	310
SYSTEM_ERR 10.0	311
SYSTEM_ERR_NOALIAS 10.0	313
SYSTEM_ERR_BADALIAS 10.0	315
SYSTEM_DOWN_CERTD 10.0	317
SYSTEM_DOWN_DB 10.0	319
SYSTEM_DOWN_HTTP 10.0	321
SYSTEM_TOUT_CERTD 10.0	323
SYSTEM_TOUT_HTTP 10.0	325
SYSTEM_BUSY_DB 10.0	327
2.4.8 User defined error related page parameters	329
USREXT_ERR1 10.0	330
USREXT_ERR2 10.0	332
USREXT_ERR3 10.0	334
USREXT_ERR4 10.0	336
USREXT_ERR5 10.0	338
USREXT_ERR6 10.0	340
3 Authentication Module	342
3.1 Authentication Module configuration file (cert.conf)	344
3.1.1 Basic configuration parameters	347
ALEVEL	348
ELEVEL	349
ACCESS	350
ERROR	351
TRACE	352
CATALOG 10.0	353
LOGINFO	354
LOGPERF	356
TRANSID 10.0	357
PERFORMANCE	359
INFORMATION	361
PORT	363
IPV6LISTEN 10.0	365
HTTPPORT 10.0	367
HTTPECHOHEADER 10.0	368
3.1.2 Access control related parameters	369
GROUP	370

ACL .....	371
ACLREQUEST .....	372
ADGROUP .....	373
ADGROUPDN .....	374
ADGROUPINTERVAL .....	375
ADGROUPPRINAME .....	376
ADGROUPPREFIX .....	377
ADGROUPMAXMEMBER .....	378
3.1.3 Session policy related parameters .....	379
COOKIERETRY .....	380
COOKIE TIME .....	381
COOKIEEXP .....	382
LOMETHOD .....	384
DUPLOGIN .....	386
DUPKIND .....	387
PARALOGIN .....	389
ACCCTRLFLG .....	390
SESSIONIDLEN <small>(10.0)</small> .....	392
CERTUNIQUEKEY <small>(10.0)</small> .....	394
3.1.4 Password policy related parameters .....	395
PWDLOGINHASH <small>(10.0)</small> .....	396
PWDCHGHASH <small>(10.0)</small> .....	398
PWDMINLEN <small>(10.0)</small> .....	400
PWDMAXLEN <small>(10.0)</small> .....	401
PWDALPHANUM <small>(10.0)</small> .....	402
PWDEXPIRE <small>(10.0)</small> .....	404
PWDSAMEPASS <small>(10.0)</small> .....	406
LOCKCOUNT .....	407
PWDEXPCHK .....	408
PWDHISCHK .....	409
PWDHISCNT <small>(10.0)</small> .....	410
PWDFORBID .....	411
PWDEXPWARN .....	412
3.1.5 Authentication DB related parameters .....	414
DBHOST <small>(10.0)</small> .....	416
DBUID <small>Overwrite</small> .....	419
DBPWD <small>Overwrite</small> .....	421
DBTBL .....	422
DBATTR .....	424
DBEXATTR .....	425
DBCRYPTOTYPE <small>(10.0)</small> .....	427
DBIWCRYPTOSEED <small>(10.0)</small> .....	428
DBCRYPTOATTR <small>(10.0)</small> .....	429
LDAPBIND .....	430
LDAPPCHG .....	432
LDAPLANG .....	434
LDAPSSL .....	436
LDAPCACERT .....	437
LDAPVERIFYSVRCERT .....	438
LDAPCIPHERSUITE .....	439
LDAPSSLBIND .....	440
ADPCHG .....	441



LDAPMULTIVAL .....	443
LDAPREFERRAL .....	444
ADDGFWBIND .....	445
3.1.6 Audit log table related parameters .....	446
LOGDBTBL .....	447
LOGDBATTR .....	448
LOGDBSEQNAME .....	449
3.1.7 Reference table related parameters .....	450
REFTBL .....	451
REFATTR .....	453
REFUID .....	454
3.1.8 System tuning related parameters .....	455
MAXREQTHREAD .....	456
ACCTHREAD <sup>(10.0)</sup> .....	458
REQQESIZE .....	460
MAXDBCONNECT .....	461
DBQESIZE <sup>(10.0)</sup> .....	463
LOGDBQESIZE <sup>(10.0)</sup> .....	464
LOGBUFSIZE .....	465
CACHE .....	467
MAXLOGINUSER <sup>(10.0)</sup> .....	468
RECVWAITTIME .....	470
THREADSTACKSIZE .....	471
LOGMULTITHREAD <sup>(10.0)</sup> .....	472
DOWNLOADCONFFLG <sup>(10.0)</sup> .....	474
3.1.9 Replication parameters .....	476
CERT <sup>(10.0)</sup> .....	477
CERTREPTYPE .....	480
RETRYCNTC .....	482
RETRYTMC <sup>(10.0)</sup> .....	483
LIVETIMER .....	484
HEALTHTIMER .....	486
HEALTHCNT .....	488
FAILBACK <sup>(10.0)</sup> .....	490
MAXREPTHREAD .....	492
REPQESIZE .....	494
3.2 Group configuration file (cert.grp) .....	495
Group settings <sup>(10.0)</sup> .....	496
3.3 Access control file (cert.acl) .....	499
Access control settings <sup>(10.0)</sup> .....	500
3.4 Authentication DB column information file (dbattr.conf) .....	503
3.4.1 Basic user information parameters .....	504
UID .....	505
PASSWORD .....	506
PWDEXPDATE .....	507
PWDHISTORY .....	508
PCHGOK .....	510
PCHGDATE .....	511
LLOGINDATE .....	512
PLOGINDATE .....	513
FLOGINDATE .....	515

PWDRETRY .....	517
PWDLOCK .....	518
LOGINOK .....	519
LOCKDATE .....	520
LOGINSTAT .....	521
3.4.2 Client certificate information parameters .....	522
RASERIALNO .....	523
IWSERIALNO .....	524
CERTEXPDATE .....	525
GETCERT .....	526
ONLINE .....	527
3.5 Log column information file (logdbattr.conf) .....	528
3.5.1 Basic information parameters .....	529
NO .....	530
TIME .....	531
UID .....	532
KIND .....	533
RESULT .....	534
MSG .....	535
CLIP .....	536
3.5.2 Client certificate information parameters .....	537
SERIAL .....	538
3.6 Forbidden password configuration file (pwdforbid.conf) .....	539
Forbidden password configuration <small>override 10.0</small> .....	540
3.7 Request control configuration file (request.acl) .....	542
3.7.1 Basic configuration parameters .....	545
TARGET <small>10.0</small> .....	546
VERSION .....	549
REJECT .....	551
SEND .....	553
NOTSEND .....	556
ACCCTRL .....	558
3.8 Authentication Module commands .....	559
3.8.1 Script command options .....	560
-c .....	561
-F .....	562
-H <small>10.0</small> .....	563
-K .....	564
-P .....	565
-R .....	566
-U .....	567
--dump-config <small>10.0</small> .....	568
--silent <small>10.0</small> .....	569
--wait-response <small>10.0</small> .....	570
--logout-alluser <small>10.0</small> .....	571

## 1 Introduction

This manual describes the configurable parameters and their meaning for each IceWall SSO configuration file.

### 1.1 Configuration file format

The following describes the format rules and restrictions common to all configuration files.

- Configuration files are text files.
- Lines that start with “#” are comment lines.
- Lines with parameter names that are ineffective 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 this manual, “default value” and “initial value” are defined as follows.



**Default value** : Refers to the value used when the parameter is not specified in the configuration file.

**Initial value** : Refers to the value that is preset for the parameter in the standard installed configuration file. Some parameters are preset with initial values that are different from the default values.

Please note that the values shown in the parameter setting examples are not always the same as the default values or initial values.

### 1.2 Version designations in the text

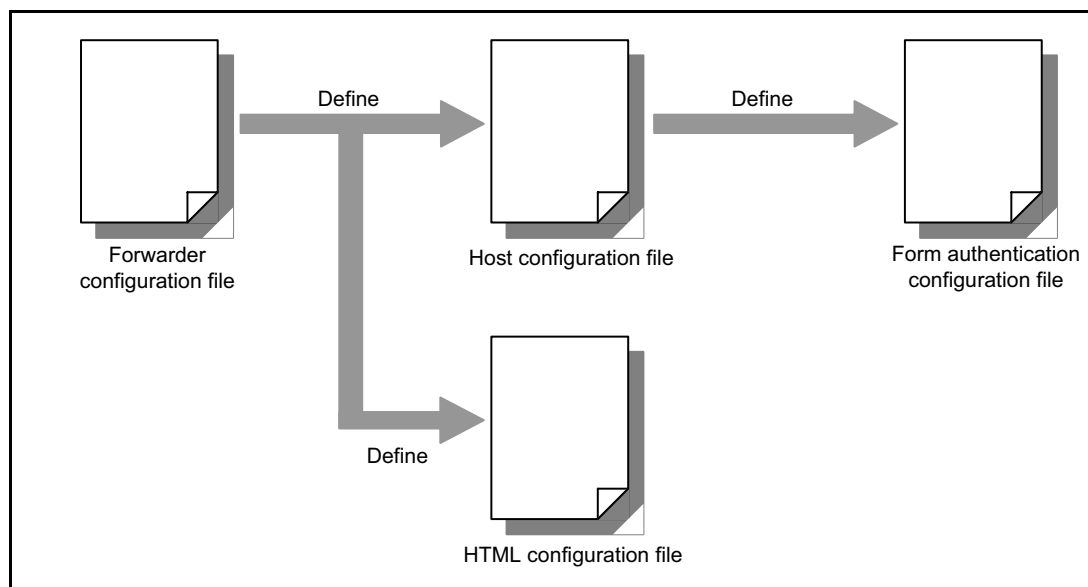
The table below gives the meanings of the symbols used in the manual and placed next to the parameter names.

Designation	Meaning
	An item added with the version enclosed in the square. In this case, the designation indicates the item was added with 10.0.
	An item where the specification was changed or function added with the version enclosed in the oval. In this case, the designation indicates a specification change or added function with 10.0.
<i>Overwrite</i>	This symbol indicates the item will be rewritten.

## 2 Forwarder

Forwarder uses the following four configuration files.

- Forwarder configuration file
- Host configuration file
- HTML configuration file
- Form authentication configuration file



Configuration file association chart

This chapter describes each of the parameters in these configuration files.

## 2.1 Forwarder configuration file (dfw.conf)

### Overview

This configuration file contains the numeric settings necessary for the operation of Forwarder, as well as some common settings used for the entire system.

Parameters available to the user are as follows:

Parameter group	Parameter name
Basic configuration parameters	ALEVEL
	ELEVEL
	ACCESS
	ERROR
	ERRORINFO
	TRACE
	CATALOG (10.0)
	SECURITY
	SECINFO (10.0)
	SECLEVEL
	SECEXCPAGE
	SPKEY_TOPPAGE_URL (10.0)
	TRANSID (10.0)
	TRANSID_STR (10.0)
	TRACETIME (10.0)
	DFW_PROTOCOL
	REQUEST_URI
	VIRTUALPATH_ENV
	VIRTUALURL_ALIAS
User authentication parameters	CERT (10.0)
	CERTLB <small>overwrite</small> (10.0)
	CERTLB_TYPE (10.0)
	CERTFAILBACK (10.0)
	CERTLBFAILBACK (10.0)
	COOKIENAME
	COOKIEATTR
	COOKIEALWAYS
	POSTLIMIT_PAGE
	POSTLIMIT_TIME
	POSTLIMIT_ENC
	FORCELOGIN_ENC
	SESSION
	POSTKEY_LOGIN
	POSTKEY_LOGOUT
	POSTKEY_PWDCHG
	REDIRECT (10.0)

Parameter group	Parameter name
User authentication parameters	LOALIAS
	ICP_VERSION
	ICP_AGENTSTR
	ICP_ENCSTR (10.0)
Template HTML parameters	DOCS
	LOCATIONURL (10.0)
	LOCATIONRETRY
	HTML_CHARSET
Backend Web Server parameters	HOST (10.0)
	SHOST (10.0)
	SVRFILE
Password change parameters	PWDALIAS
	MINLEN (10.0)
	MAXLEN (10.0)
	EXPIRE (10.0)
	SAMEPASS (10.0)
	ALPHANUM (10.0)
Performance tuning parameters	RETRYCNTC
	RETRYTMC (10.0)
	CERT_TOUT
	ALLOC
	SET_CONTENT_LENGTH
	POSTWAITTIME
Security parameters	MAXURL
	MAXQUERY
	REV_PATH (10.0)
	SESSION_ENC_KEY
	DFWFILTER
	NOCHK_EXT_ALIAS
Client certificate parameters	REQUESTFILTER (10.0)
	CC_UID
	CC_UIDKEYS
	CC_UIDKEYE
	CC_ENVNAME
	CC_DECODE_FLG
	CC_ENVUID
	CC_ENVSERIAL
	CC_ENVEXPIRE
	CC_ENVISSUER

Parameter group	Parameter name
POST data inheritance parameters	POST_INHERIT
	MAXPOST
	POSTNAME
	POST_HTML
	POST_ENC
Agent parameters	AGENT_KEY
	AGENT_PERMIT (10.0)
	QUERY_ENC
	QUERY_ENC_NAME
	QUERY_ENC_KIND (10.0)
	RELOGIN_KEY

**Storage  
location**

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

**Remarks**

To change the file name and storage location for the Forwarder configuration file, define the path for the file you want to specify in the value for IWDFWCONFIG, an environment variable for the web server executing Forwarder.

This file must be stored in the same directory as the Forwarder binary file.

Example: If you want to specify dfw\_01.conf in /opt/icewall-ssso/dfw/config as the Forwarder configuration file

Set the value for IWDFWCONFIG, an environment variable for the web server executing Forwarder, to:

/opt/icewall-ssso/dfw/config/dfw\_01.conf

These parameters are described on the following pages.

### 2.1.1 Basic configuration parameters

These are the common, system-wide parameters used during Forwarder operation.

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
ERRORINFO	×	Sets the error log additional information
TRACE	×	Sets the trace log file name
CATALOG <small>10.0</small>	×	Sets the message catalog
SECURITY	×	Sets the security log file name
SECINFO <small>10.0</small>	×	Sets the security log output information
SECLEVEL	×	Sets the security log information level
SECEXCPAGE	×	Sets the page names to be excluded in the Forwarder page output log, which is output to the security log
SPKEY_TOPPAGE_URL <small>10.0</small>	×	Sets top-page URL in the entire system that will be replaced by the specific keyword
TRANSID <small>10.0</small>	×	Sets whether to output the transaction ID in Forwarder's log files as additional information
TRANSID_STR <small>10.0</small>	×	Sets the character string included in the transaction ID when generated to determine which Forwarder issued the transaction ID
TRACETIME <small>10.0</small>	×	Sets the log file name for the trace time log
DFW_PROTOCOL	×	Sets the operating protocol of Forwarder
REQUEST_URI	×	Sets the path information acquisition method
VIRTUALPATH_ENV	×	Sets the name of the environment variable used to set the path added to REQUEST_URI
VIRTUALURL_ALIAS	×	Sets the character string included in the URL when connecting to Forwarder that supports original URLs and the supporting Backend Web Server alias name

For details on these parameters, see the following pages.



# ALEVEL

Overview                Sets the access log output level.

Format                 **ALEVEL=access log level**

- Set one of the following values for the access log level:
  - 0 : No output
  - 1 : Output basic information only
  - 2 : Output basic information + content size + client IP address + Backend Web Server status
- The default value set in the executable binary file is 1.
- The initial value set in the standard configuration file is 1.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

Configuration example    1) To output only basic access log information in the access log:  
**ALEVEL=1**

Remarks                • This parameter can be set in the host configuration file, and the access log output level can be set to each Backend Web Server. If this parameter is not set in the host configuration file, the access log is output at the level set in the Forwarder configuration file, as in earlier versions.

See also                ACCESS (Forwarder configuration file)

Forwarder configuration file (dfw.conf)

---

## ELEVEL

Overview                Sets the error log output level.

Format                 **ELEVEL=error log level**

- Set one of the following values for the error log level:
  - 0 : No output
  - 1 : Only fatal errors (Fatal)
  - 2 : Fatal errors and warnings (Warning)
  - 3 : All information (Information)
- The default value set in the executable binary file is 1.
- The initial value set in the standard configuration file is 1.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

Configuration example    1) To output fatal errors and warnings in the error log:  
**ELEVEL=2**

Remarks                • This parameter can be set in the host configuration file, and the error log output level can be set to each Backend Web Server. If this parameter is not set in the host configuration file, the access log is output at the level set in the Forwarder configuration file, as in earlier versions. The level of output may be determined by the Forwarder configuration file, depending on the process timing.

See also                ERROR (Forwarder configuration file)

# ACCESS

Overview	Sets the access log file name.
Format	<b>ACCESS=<u>access log file name</u></b> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value set in the executable binary file is /opt/icewall-ss/logs/dfw.log.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ss/logs/dfw.log.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	1) To output to a standard access log file: <b>ACCESS=/opt/icewall-ss/logs/dfw.log</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter can be set in the host configuration file, and the access log file can be set to each Backend Web Server. If this parameter is not set in the host configuration file, the access log is output to the file set in the Forwarder configuration file.</li><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 for the file specified by this parameter require write permission for the user of the web server executing Forwarder.</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 (Forwarder configuration file)

Forwarder configuration file (dfw.conf)

---

# ERROR

Overview                Sets the error log file name.

Format                 **ERROR=error log file name**

- The file name has a maximum length of 255 bytes.
- The default value set in the executable binary file is /opt/icewall-ss/logs/dfwerr.log.
- The initial value set in the standard configuration file is /opt/icewall-ss/logs/dfwerr.log.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

Configuration example    1) To output to a standard error log file:  
**ERROR=/opt/icewall-ss/logs/dfwerr.log**

Remarks

- This parameter can be set in the host configuration file, and the error log file can be set to each Backend Web Server. If this parameter is not set in the host configuration file, the access log is output to the file set in the Forwarder configuration file. The level of output may be determined by the Forwarder configuration file, depending on the process timing.
- 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.
- The owner and permission for the file specified by this parameter require write permission for the user of the web server executing Forwarder.
- If this parameter is not set, the information is output to the file specified by the default value.

See also                ELEVEL (Forwarder configuration file)  
                          ERRORINFO (Forwarder configuration file)

# ERRORINFO

Overview	Sets additional information to be output to the error log.
Format	<b>ERRORINFO=<u>output entry name</u>[<u>output entry name</u>,...]</b> <ul style="list-style-type: none"><li>• One of the following values can be set to the output entry name:<ul style="list-style-type: none"><li>UID : Outputs the user ID of the requested user.</li><li>URL : Outputs the requested URL.</li><li>IP : Outputs the requested IP address.</li><li>AGENT : Outputs the requested browser type.</li></ul></li><li>• The configuration of these output entry names is not order-sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	1) To output the user ID and browser type to the error log: <b>ERRORINFO=UID,AGENT</b>
Remarks	<ul style="list-style-type: none"><li>• When this parameter is set, the additional information generated by the specified output entries is added to the end of the normal error log message.</li><li>• The entry information is output regardless of the error log level.</li><li>• Entry information is output as follows. The output order for each entry is fixed. <i>uid=userid url=url IP=ip address agent=browser agent</i></li><li>• If an output entry name is specified even though the entry information that is to be output is missing, the output data will be "[output entry name]=."</li></ul>
See also	ELEVEL (Forwarder configuration file) ERROR (Forwarder configuration file)

---

**Forwarder configuration file (dfw.conf)**

---

# TRACE

Overview	Sets the log file name for the trace log.
Format	<b>TRACE=<u>trace log file name</u></b> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• If this parameter is not set, no trace log file is created.</li></ul>
Configuration example	1) To output to a standard trace log file: <b>TRACE=/opt/icewall-ss0/logs/dfwtrace.log</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter can be set in the host configuration file, and the trace log file can be set to each Backend Web Server. If this parameter is not set in the host configuration file, the access log is output to the file set in the Forwarder configuration file. The level of output may be determined by the Forwarder configuration file, depending on the process timing.</li><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 for the file specified by this parameter require write permission for the user of the web server executing Forwarder.</li><li>• Setting this parameter causes a reduction in the performance of Forwarder.</li><li>• Normally there is no need to set this parameter. It should be set only in situations such as when providing information to technical support.</li><li>• HP is not able to answer inquiries regarding the content of the trace log file.</li></ul>
See also	None

# CATALOG 10.0

Overview	<p>Sets the file name and path for the Forwarder message catalog file.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b>CATALOG=<u>message catalog file name</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is /opt/icewall-sso/messages/C/icewall_dfw.cat. <small>10.0</small></li><li>• Although there is no default value in the executable binary file, the message catalog file specified by the environment variable NLSPATH will be used if no value is set to this parameter.</li></ul>
Configuration example	<p>1) To set the standard Forwarder message catalog file name:</p> <p><b>CATALOG=/opt/icewall-sso/messages/C/icewall_dfw.cat</b></p>
Remarks	<ul style="list-style-type: none"><li>• “Message Nothing” will be output instead of the message that is normally output to the error log when there is an error with the message catalog, such as when this parameter has not been set, or the file name is incorrect.</li></ul>
See also	<p>CATALOG (Authentication Module configuration file)</p>

Forwarder configuration file (dfw.conf)

---

## SECURITY

Overview	Sets the name of the security log file used for such operations as login, logout, password changes, and agent link processes.
Format	<b>SECURITY=<u>security log file name</u></b> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• If this parameter is not set, no security log file is created.</li></ul>
Configuration example	1) To output the security log to /opt/icewall-ss0/logs/dfwsecurity.log: <b>SECURITY=/opt/icewall-ss0/logs/dfwsecurity.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 for the file specified by this parameter require write permission for the user of the web server executing Forwarder.</li><li>• Setting this parameter causes a slight reduction in the performance of Forwarder.</li></ul>
See also	SECINFO SECLEVEL



## SECINFO 10.0

Overview	<p>Sets the information which is output to the security log.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b>SECINFO=<u>output information</u>[,<u>output information</u>, ...]</b></p> <ul style="list-style-type: none"><li>• The information output can be set as follows:<ul style="list-style-type: none"><li>LOGIN : Outputs the login successful log.</li><li>LOGOUT : Outputs the logout successful log.</li><li>PWDCHG : Outputs the password change successful log.</li><li>AGENT : Outputs the agent link process successful log.</li><li>PAGE : Outputs the template HTML display log.</li><li>REQUEST: Outputs the access stopped log. <small>10.0</small></li></ul></li><li>• The configuration of these output entry names is not order-sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To output the login successful and logout successful logs: <b>SECINFO=LOGIN,LOGOUT</b></p>
Remarks	<ul style="list-style-type: none"><li>• In the security log, the log messages are output regardless of the CATALOG parameter setting.</li><li>• Note that if this parameter is not set, the security log is not output even if the SECURITY parameter is set.</li><li>• Output information REQUEST can only be controlled when the REQUESTFILTER parameter is effective. <small>10.0</small></li></ul>
See also	<p>SECURITY SECLEVEL REQUESTFILTER (Forwarder configuration file)</p>

## SECLEVEL

Overview	Defines the security log information level.
Format	<b>SECLEVEL=level</b> <ul style="list-style-type: none"><li>• One of the following values can be set to this parameter:<ul style="list-style-type: none"><li>0 : Outputs the host name of the agent server.</li><li>1 : Outputs the agent server host name, client IP address, and login user ID.</li><li>2 : Outputs the agent server host name, client IP address, login user ID, and AGENT_KEY of the requesting agent.</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To output the agent server host name, client IP address, and login user ID to the security log: <b>SECLEVEL=1</b>
Remarks	<ul style="list-style-type: none"><li>• The Agent server host name and the AGENT_KEY for the requesting agent are only output during agent link operation. Even when Agent is set in the SECINFO parameter, the Agent server host name and the AGENT_KEY for the requesting agent are not output to the security log except during agent link operation.</li></ul>
See also	SECURITY SECINFO

# SECEXCPAGE

Overview	Sets the page names excluded in the template HTML display log that is output to the security log.
Format	<b>SECEXCPAGE=page name[,page name,...]</b> <ul style="list-style-type: none"><li>• The page names represent template HTML parameter names configured in the HTML configuration file and host configuration file, and the “DFWERROR” parameter.</li><li>• Several lines may be used to set as many values as necessary.</li><li>• The configuration of these output entry names is not order-sensitive.</li><li>• This parameter is effective only when the SECURITY parameter is set and PAGE is set in the SECINFO parameter.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To prevent login, logout, and password change pages from being generated with the Forwarder page logs that are output to the security log:</p> <pre>SECURITY=/opt/icewall-ssso/logs/dfwsecurity.log SECINFO=PAGE SECEXCPAGE=LOGIN_UID,LOGIN_ERR_UID,LOGIN_ERR_PWD SECEXCPAGE=LOGOUT,LOGOUT_SUCCESS SECEXCPAGE=PWDCHG,PWDCHG_SUCCESS</pre>
Remarks	<ul style="list-style-type: none"><li>• One of the possible page name settings, “DFWERROR,” represents the fixed error page Forwarder displays when the template HTML cannot be retrieved (including the system error page).</li><li>• Note that the page names that are output to the log are the final page names created.</li><li>• The local (file://) determines the page names to be output, even when the template HTML is installed to an external server (http://, https://).</li></ul>
See also	SECURITY SECINFO

Forwarder configuration file (dfw.conf)

---

## SPKEY\_TOPPAGE\_URL 10.0

**Overview**                Sets top-page URL in the entire system that will be replaced by the specific keyword \$TOPPAGE\_URL.

This parameter is available since version 10.0.

**Format**                **SPKEY\_TOPPAGE\_URL=top page URL**

- The URL must be an absolute path.
- The URL has a maximum length of 255 bytes.
- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is http://www.hp.com/.
- If a value is not set, the specific keyword \$TOPPAGE\_URL has no value.

**Configuration example**        1) To set the system top page to http://www.hp.com/:  
**SPKEY\_TOPPAGE\_URL=http://www.hp.com/**

**Remarks**

- Be aware that the host name contained in the URL set to this parameter must also be set in either the HOST or SHOST parameters, or the URL will connect to the Internet outside of IceWall SSO protection.  
SPKEY\_TOPPAGE\_URL=http://www.hp.com/  
HOST=XXX=www.hp.com  
The URL that is replaced by the specific keyword \$TOPPAGE\_URL in this situation is www.hp.com via IceWall SSO.
- Set this parameter when using the specific keyword \$TOPPAGE\_URL.
- If this parameter is set when using the password change function, the URL set to this parameter can be used as the link to return to the top page after changing the password.
- When the REDIRECT parameter is set, HP recommends setting the REDIRECT parameter to the same setting.
- When changing a password linked with Agent Option, the value set to this parameter is not replaced by the specific keyword

\$TOPPAGE\_URL on the password change-related pages, it is a URL that returns to Agent Option.

- When changing a password linked with Agent Option, the agent module must support changing passwords linked with Agent Option.

See also           None

---

Forwarder configuration file (dfw.conf)

---

## TRANSID 10.0

Overview	<p>Sets whether to output the transaction ID in Forwarder's log files as additional information.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>TRANSID=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Do not output transaction ID to the log (backward compatibility)</li><li>1 : Output transaction ID to the log</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To output the transaction ID in Forwarder's log files as additional information:</p> <p><b>TRANSID=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• The transaction ID is used when matching log files output by IceWall modules that connect and communicate when accessed from a client once.</li><li>• Fundamentally, the transaction ID is generated by the module first accessed from the client. If this parameter is set to 1 and Forwarder is not accessed first, Forwarder generates a transaction ID and notifies other modules of it, even when a transaction ID is not passed from another module.</li><li>• If this parameter is set to 1, the transaction ID is output in the error log, access log, and security log as additional information. Example: For the error log [2010/01/01 12:00:00] Fatal: Error Message. TID=xxxxxxxxxx [ED00000-00000]</li></ul>

- If this parameter is set to 1, Forwarder notifies the Authentication Module of the transaction ID. If 2.0 is not set to the ICP\_VERSION parameter, there is no notification.
- If this parameter is set to 1, Agent Option is notified of the transaction ID when linking with Agent Option.
- If this parameter is set to 1, Forwarder can receive the transaction ID from Agent Option. If the transaction ID function is not implemented in Agent Option, Forwarder cannot receive the transaction ID.
- If this parameter is set to 1, the transaction ID is sent to the Backend Web Server in the HTTP headers. The transaction ID can be configured not to be sent with the HEADER\_FILTER parameter. The transaction ID HTTP header name can be changed with the HEADER\_NAME\_TID parameter.

See also

TRANSID\_STR

HEADER\_FILTER (host configuration file)

HEADER\_NAME\_TID (host configuration file)

ICP\_VERSION

TRANSID (Authentication Module configuration file)

Forwarder configuration file (dfw.conf)

---

## TRANSID\_STR 10.0

**Overview** Sets the character string included in the transaction ID when generated to determine which Forwarder issued the transaction ID.

This parameter is available since version 10.0.

**Format** **TRANSID\_STR=identifier character string**

- Set the identifier character string in a range between 1 byte and 16 bytes.
- The identifier character string can be set with the characters a through z, A through Z, and 0 through 9.
- The default value set in the executable binary file is dfw.
- The initial value set in the standard configuration file is dfw01.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**

1) To set the character string to identify Forwarder that includes the transaction ID to iwdfw01:  
**TRANSID=1**  
**TRANSID\_STR=iwdfw01**

**Remarks**

- This parameter is ineffective when the TRANSID parameter is set to 0.
- In environments running multiple Forwarders, set each Forwarder to a different identifier character string.

**See also** TRANSID (Forwarder configuration file)  
TRANSID (Authentication Module configuration file)



# TRACETIME 10.0

Overview	<p>Sets the log file name for the trace time log.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>TRACETIME=<u>trace time log file name</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• If this parameter is not set, no trace time log file is created.</li></ul>
Configuration example	<p>1) To output to a standard trace time log file:</p> <p><b>TRACETIME=/opt/icewall-ss0/logs/dfwtracetime.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 for the file specified by this parameter require write permission for the user of the web server running Forwarder.</li><li>• Normally there is no need to set this parameter. It should be set only in situations such as when providing information to technical support.</li><li>• HP is not able to answer inquiries regarding the content of the trace time log file.</li></ul>
See also	None

Forwarder configuration file (dfw.conf)

---

## DFW\_PROTOCOL

Overview	Sets the protocol Forwarder should use when load balancing products are used that cannot perform protocol changes to the URL information contained within the HTTP header.
Format	<p><b>DFW_PROTOCOL=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Does not change protocol</li><li>1 : Changes protocol to SSL (https)</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To allow Forwarder to operate correctly when the browser and load balancer are connected via SSL, and the load balancer and Forwarder are connected via HTTP:</p> <p><b>DFW_PROTOCOL=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• It is not guaranteed that Forwarder will work as expected in environments without load-balancing if this parameter is set to 1.</li><li>• HTTP connections cannot be used to run Forwarder when this parameter is configured to use SSL.</li></ul>
See also	None

# REQUEST\_URI

Overview	Sets the type of retrieval method to be used to retrieve the path information requested by the client.
Format	<p><b>REQUEST_URI=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be specified for the flag:<ul style="list-style-type: none"><li>0 : Conventional method (Retrieve path information from the environment variable PATH_INFO)</li><li>1 : New method (Retrieve path information from the environment variable REQUEST_URI)</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To retrieve path information using the new method: <b>REQUEST_URI=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• Use the new method for this parameter under the following conditions: the requested path contains an equal sign "=", the "%3d" encoding has been used, and the application is not running properly.</li><li>• The URL_SCOLON parameter value will be disabled when using the new method for this parameter. Set to 0 to enable the URL_SCOLON parameter.</li><li>• This parameter has effect to enable new retrieval method only if the type of web server for the IceWall server is an Apache HTTP server.</li></ul>
See also	URL_SCOLON (host configuration file)

## VIRTUALPATH\_ENV

Overview	Sets the name of the environment variable containing the path added to REQUEST_URI.
Format	<p><b>VIRTUALPATH_ENV=<u>environment variable name</u></b></p> <ul style="list-style-type: none"><li>• The environment variable has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set the environment variable name, which acquires the Forwarder operation path and alias, to “MOD_PATH”:</p> <p><b>VIRTUALPATH_ENV=MOD_PATH</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when the REQUEST_URI parameter is set to 1.</li><li>• This parameter cannot be used when implementing session management using URL-Cookie.</li><li>• The path retrieved from the set environment variable must match (prefix search) the environment variable SCRIPT_NAME, which defines the Forwarder operation path.</li><li>• This parameter is effective only when the web server is an Apache HTTP server.</li></ul>
See also	REQUEST_URI

# VIRTUALURL\_ALIAS

Overview	Sets the character string included in the URL when connecting to Forwarder that supports original URLs and the supporting Backend Web Server alias name.
Format	<b><u>VIRTUALURL_ALIAS=alias name=character string included in URL</u></b> <ul style="list-style-type: none"><li>• The alias name has a maximum length of 64 bytes.</li><li>• The slash character “/” cannot be used in alias names.</li><li>• The alias name is case sensitive.</li><li>• Define the alias name as the alias name set in the HOST and SHOST parameters.</li><li>• Define the character string included in the URL within 128 bytes.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) When connecting to the Backend Web Server with the alias “ALIAS1,” if the request from the client includes “www.orgurl1.com” in the URL: <b>HOST=ALIAS1=www.hp.com</b> <b>VIRTUALURL_ALIAS=ALIAS1=www.orgurl1.com</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter cannot be used when implementing session management using URL-Cookie.</li><li>• Even when connected to Forwarder with the original URL handled by this parameter, the requested header URL can undergo conversion.</li><li>• If this parameter is not set when supporting original URLs, the request header URL is not converted.</li><li>• When the request header URL may contain a relative path, the character string containing the relative path must be set.</li><li>• Set this parameter only when using original URL support. Request header URL conversion will not operate correctly when original URL support is not used.</li></ul>
See also	None

### 2.1.2 User authentication parameters

These parameters are used for settings such as user authentication and logout.

Parameter name	Mandatory	Overview
CERT <sub>Overwrite</sub> (10.0)	×	Sets the host name and port number for the Authentication Module
CERTLB <sub>Overwrite</sub> (10.0)	×	Sets the connection information for the Authentication Module performing load balancing
CERTLB_TYPE (10.0)	×	Sets the assignment method for the Authentication Module performing load balancing
CERTFAILBACK (10.0)	×	Sets the original connection order when performing a failback in the Authentication Module connection settings configured for failover
CERTLBFAILBACK (10.0)	×	Sets the original connection order when performing a failback in the Authentication Module connection settings for load balancing configured for failover
COOKIE_NAME	×	Sets the name for the authentication cookie
COOKIE_ATTR	×	Sets the attribute for the authentication cookie
COOKIE_ALWAYS	×	Sets the renotification for the authentication cookie
POSTLIMIT_PAGE	×	Sets the template HTML page imposing restrictions on the time until POST data is sent to Forwarder
POSTLIMIT_TIME	×	Sets the time limit when restricting the time until POST data is sent to Forwarder
POSTLIMIT_ENC	×	Sets the key for encrypting and decrypting data set for the template HTML page when restricting the time until POST data is sent to Forwarder
FORCELOGIN_ENC	×	Sets the key for encrypting and decrypting user information included on the forced login page
SESSION	×	Sets the transmission format for the session ID
POSTKEY_LOGIN	×	Sets the login keyword
POSTKEY_LOGOUT	×	Sets the logout keyword
POSTKEY_PWDCHG	×	Sets the password change keyword

Parameter name	Mandatory	Overview
REDIRECT <b>10.0</b>	×	Sets the redirect location
LOALIAS	×	Sets the alias for logout
ICP_VERSION	×	Sets the communication protocol
ICP_AGENTSTR	×	Sets the text string added to AGENT_ID
ICP_ENCSTR <b>10.0</b>	×	Sets the character string indicating the encryption method that is announced to the Authentication Module when using an original encryption method in the ICP 2.0 communication message encryption library

For details on these parameters, see the following pages.

---

Forwarder configuration file (dfw.conf)

---

**CERT** overwrite **10.0**

Overview	<p>Sets the host name (or IP address) and port number of the Authentication Module.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>CERT=host name (or IP address)[:port number][,host name:port number]</u></b></p> <ul style="list-style-type: none"><li>• The host name has a maximum length of 64 bytes.</li><li>• The port number defaults to 14142 if omitted.</li><li>• Failover settings are enabled by setting multiple host names separated by commas.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is localhost:14142.</li><li>• If this parameter and CERTLB parameter are not set, the product runs in <b>Reverse Proxy mode</b> with no authentication.</li><li>• When connecting to the Authentication Module in the IPv6 format, enclose the host name or IP address in square brackets ([ ]). <b>10.0</b></li></ul>
Configuration example	<p>1) To connect to an Authentication Module using the default port number: <b>CERT=certsvr.com</b></p> <p>2) To connect to an Authentication Module with a changed port number: <b>CERT=certsvr.com:14144</b></p> <p>3) To create a failover setup for a duplex-configuration Authentication Module: <b>CERT=certsvr.com1,certscr.com2</b></p>
Remarks	<ul style="list-style-type: none"><li>• If a failover has occurred, the Authentication Module does not return to the state before the failover occurred unless the Forwarder configuration file is overwritten or a failover occurs again. However, it is possible to return to the original connection order when using the failover recovery function. <b>10.0</b></li><li>• This parameter is ineffective when the CERTLB parameter is set.</li></ul>



- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
- The “IceWall SSO FailOver Option” is required to implement a failover setup.
- In March 2006, ICANN\* assigned port number 14142 to IceWall SSO. This is the official port number for the “IceWall Cert Protocol,” which is the IceWall SSO communication protocol. It is therefore recommended to use this port number.  
No need to change the existing systems that are already using a different port number.
  - \* ICANN (Internet Corporation for Assigned Names and Numbers) is an international nonprofit corporation that assigns and manages Internet address resources.

See also      PORT (Authentication Module configuration file)  
                 CERTLB  
                 CERTFAILBACK

---

Forwarder configuration file (dfw.conf)

---

## CERTLB Override 10.0

Overview	<p>Sets the connection information for the Authentication Module performing load balancing.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>CERTLB=authentication module identifier key=host name (or IP address)[:port number][,host name:port number]</b></p> <ul style="list-style-type: none"><li>• Define the Authentication Module identifier key as 1 character.</li><li>• Set the Authentication Module identifier key to the CERTUNIQUEKEY parameter value for the Authentication Module configured by “host name (or IP address)[:port number]”.</li><li>• The host name has a maximum length of 64 bytes.</li><li>• The port number defaults to 14142 if omitted.</li><li>• Failover settings are enabled by setting multiple host names separated by commas.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• If this parameter and CERT parameter are not set, the product runs in <b>Reverse Proxy mode</b> with no authentication.</li><li>• When connecting to the Authentication Module in the IPv6 format, enclose the host name or IP address in square brackets ([ ]).</li></ul>
Configuration example	<p>1) When connecting to two Authentication Module groups with the load balancing function:</p> <p><b>CERTLB=a=certsrv1.com</b> <b>CERTLB=b=certsrv2.com</b></p> <p>2) When connecting to two Authentication Module groups configured for failover with the load balancing function:</p> <p><b>CERTLB=a=certsrv1.com,certsrv1.com2</b> <b>CERTLB=b=certsrv2.com,certsrv2.com2</b></p>
Remarks	<ul style="list-style-type: none"><li>• Authentication Modules set on the same line for this parameter are treated as an Authentication Module group.</li></ul>

- If this parameter is set on multiple lines, the load balancing function is enabled. The Authentication Module group that the user connects to during login is automatically determined and the destination Authentication Module group is assigned.
  - If this parameter is set on multiple lines, always set different Authentication Module identifier keys.
  - If this parameter is set, the CERT parameter becomes ineffective.
  - If a failover has occurred, the Authentication Module does not return to the state before the failover occurred unless the Forwarder configuration file is overwritten or a failover occurs again. However, it is possible to return to the original connection order when using the failover recovery function.
  - For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual.
  - The “IceWall SSO FailOver Option” is required to implement a failover setup.
  - In March 2006, ICANN\* assigned port number 14142 to IceWall SSO. This is the official port number for the “IceWall Cert Protocol,” which is the IceWall SSO communication protocol. It is therefore recommended to use this port number.  
No need to change the existing systems that are already using a different port number.
  - When this parameter is set and when linking to the agent module, the agent module must support the load balancing function for Authentication Module connections.
- \* ICANN (Internet Corporation for Assigned Names and Numbers) is an international nonprofit corporation that assigns and manages Internet address resources.

See also

CERT (Forwarder configuration file)  
CERTLB\_TYPE  
CERTLBFAILBACK  
PORT (Authentication Module configuration file)  
CERTUNIQUEKEY (Authentication Module configuration file)

## CERTLB\_TYPE 10.0

Overview	<p>Sets the assignment method for the Authentication Module performing load balancing.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>CERTLB_TYPE=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Assignment method by random numbers</li><li>1 : Assignment method by user ID</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To set the assignment method for Authentication Modules performing load balancing to the assignment method by user ID:</p> <p><b>CERTLB_TYPE=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is ineffective when the CERTLB parameter is set to 1 line or less.</li><li>• If this parameter is set to 0, the user cannot tell which Authentication Module group they will be assigned to.</li><li>• If this parameter is set to 1, the same user ID is always assigned to the same Authentication Module group.</li><li>• Users cannot be assigned to the Authentication Module group set to each user ID with this function.</li><li>• If the Authentication Module is set to allow exclusive logins (DUPLOGIN=0, DUPKIND=1), the forced login function can be used. When performing forced logins, the destination login Authentication Module is assigned twice before logging in. When using assignment by random numbers, both assignment destinations are indeterminate, so use assignment by user ID.</li></ul>
See also	CERTLB

DUPLOGIN (Authentication Module configuration file)

DUPKIND (Authentication Module configuration file)

## CERTFAILBACK 10.0

Overview	<p>Sets the original connection order when performing a failback in the Authentication Module connection settings configured for failover.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>CERTFAILBACK=<u>original connection order</u></b></p> <ul style="list-style-type: none"><li>• Define the original connection order in the same format below as the CERT parameter. <b><u>host name (or IP address):port number[,host name:port number]</u></b></li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• When connecting to the Authentication Module in the IPv6 format, enclose the host name or IP address in square brackets ([ ]).</li></ul>
Configuration example	<p>1) To perform failback with the CERT parameter configured for failovers: <b>CERT=iwcertsvr1.com:14142,iwcertsvr2.com:14142</b> <b>CERTFAILBACK=iwcertsvr1.com:14142,iwcertsvr2.com:14142</b></p>
Remarks	<ul style="list-style-type: none"><li>• By setting this parameter, failback is performed from the CERT parameter configured for failovers.</li><li>• This parameter is only effective when the ICP_VERSION parameter is set to 2.0 (when using ICP 2.0).</li><li>• Always use this parameter in combination with the CERT parameter.</li><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual.</li><li>• When performing a failback operation, the Authentication Module connection settings in the Forwarder configuration file CERT parameter are overwritten with the original connection order set by this parameter.</li><li>• Set the original connection order to the same value as the host information for the initial state of the CERT parameter. If the host information is defined in different formats such as omitting the</li></ul>

default port, the host information will be overwritten with information different than the initial state when a failback operation occurs.

- This parameter is only effective when configured to announce that the Primary Authentication Module is live with the FAILBACK parameter in the Secondary Authentication Module configuration file.

See also

CERT (Forwarder configuration file)

CERTLBFAILBACK

FAILBACK (Authentication Module configuration file)

## CERTLBFAILBACK 10.0

**Overview** Sets the original connection order when performing a failback in the Authentication Module connection settings for load balancing configured for failover.

This parameter is available since version 10.0.

**Format** **CERTLBFAILBACK=authentication module identifier key=original connection order**

- Define the Authentication Module identifier key as 1 character.
- Set the Authentication Module identifier key to the same value as the Authentication Module identifier key set in the corresponding CERTLB parameter.
- Define the original connection order in the same format below as the CERTLB parameter.  
**host name (or IP address):port number][,host name:port number]**
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- When connecting to the Authentication Module in the IPv6 format, enclose the host name or IP address in square brackets ([ ]).

**Configuration example**

1) To perform failback operations with the CERTLB parameter configured for failovers using the load balancing function:  
**CERTLB=a=iwcertsvr1.com:14142,iwcertsvr2.com:14142**  
**CERTLB=b=iwcertsvr3.com:14142,iwcertsvr4.com:14142**  
**CERTLBFAILACK=a=iwcertsvr1.com:14142,iwcertsvr2.com:14142**  
**CERTLBFAILACK=b=iwcertsvr3.com:14142,iwcertsvr4.com:14142**

**Remarks**

- By setting this parameter, failback operations are performed from the CERTLB parameter for load balancing configured for failovers
- This parameter is only effective when the ICP\_VERSION parameter is set to 2.0 (when using ICP 2.0)
- Always use this parameter in combination with the CERTLB parameter.



- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual.
- When performing a failback operation, the Authentication Module connection settings in the Forwarder configuration file CERTLB parameter are overwritten with the original connection order set by this parameter.
- Set the original connection order to the same value as the host information for the initial state of the CERTLB parameter. If the host information is defined in different formats such as omitting the default port, the host information will be overwritten with information different than the initial state when a failback operation occurs.
- This parameter is only effective when configured to announce the Primary Authentication Module is live with the FAILBACK parameter in the Secondary Authentication Module configuration file.

See also

CERTLB (Forwarder configuration file)

CERTFAILBACK (Forwarder configuration file)

FAILBACK (Authentication Module configuration file)

CERTUNIQUEKEY (Authentication Module configuration file)

Forwarder configuration file (dfw.conf)

---

# COOKIE\_NAME

Overview	Sets the session ID to be used when the IceWall SSO session ID information is sent to the client in a Set-cookie header.
Format	<p><b>COOKIE_NAME=<u>session ID name</u></b></p> <ul style="list-style-type: none"><li>• The set session ID is sent to the client as an HTTP-cookie, as shown below. Set-Cookie: Session ID name="xxxx-xxxx" * "xxxx-xxxx" is the session ID.</li><li>• The session ID name must contain at least one byte, with a maximum length of 64 bytes.</li><li>• The characters used in the session ID name are based on general cookie specifications.</li><li>• The default value set in the executable binary file is IW_INFO.</li><li>• The initial value set in the standard configuration file is IW_INFO.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To notify the client of the standard session ID name: <b>COOKIE_NAME=IW_INFO</b></p>
Remarks	<ul style="list-style-type: none"><li>• If cookies are used in a Backend Web Server application, use different session IDs when setting this parameter.</li><li>• When IceWall SSO is being used as an IceWall SSO Backend Web Server (IceWall SSO multi-tier architecture), the session ID name must be changed on either the front-end IceWall SSO connected to the client, or on the backend IceWall SSO connected to the front-end IceWall SSO. It does not matter if the session ID name is changed from the default value on both the front-end and the backend server.</li><li>• Besides this parameter, the following parameters must be set when using IceWall SSO multi-tier architecture: POSTKEY_LOGIN POSTKEY_LOGOUT POSTKEY_PWDCHG</li></ul>
See also	POSTKEY_LOGIN POSTKEY_LOGOUT

POSTKEY\_PWDCHG

# COOKIEATTR

Overview	Sets the cookie attributes when using an HTTP-Cookie to notify a client of the IceWall SSO session ID.
Format	<p><b>COOKIEATTR=<u>cookie attribute</u></b></p> <ul style="list-style-type: none"><li>• Sets the required attribute in the cookie attributes. The content set here is sent directly to the client without modification.</li><li>• Separate multiple attributes by using a semicolon “;.”</li><li>• A cookie attribute has a minimum length of one byte and a maximum of 256 bytes.</li><li>• The attributes that can be set are based on general cookie specifications.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set www.hp.com as the domain attribute: <b>COOKIEATTR=domain=www.hp.com</b></p> <p>2) To set / as the path attribute: <b>COOKIEATTR=path=</b></p> <p>3) To set secure as the attribute in an SSL connection environment: <b>COOKIEATTR=secure</b></p> <p>4) To set www.hp.com as the domain attribute and to set / as the path attribute: <b>COOKIEATTR=domain=www.hp.com; path=</b></p>
Remarks	<ul style="list-style-type: none"><li>• When this parameter is set, operations using these attributes run according to general cookie specifications.</li><li>• Operations may not work properly if these attributes are not set correctly.</li><li>• Another cookie attribute, Expires, can be set only when the login expiration time setting on the Authentication Module is set to “a fixed period after login” (LOMETHOD=0). In this case, the client will be notified of the two Expires attributes. The actual operational behavior</li></ul>

will depend on the browser specifications.

- If session management using URL-Cookie (SESSION=1) is used, the path attribute, which contains the Forwarder path, is added to the authentication cookie when issued. Note that default attributes are deleted when any of these attributes are set manually with this parameter.

See also

SESSION  
LOMETHOD (Authentication Module configuration file)

# COOKIEALWAYS

**Overview**                Sets the client notification timing of the IceWall SSO session ID.

**Format**                **COOKIEALWAYS=flag**

- One of the following values can be set to the flag:
  - 0 : Session ID is notified at time of login only
  - 1 : Session ID is notified each time that the conversion target content is accessed
  - 2 : Session ID is notified each time any content is accessed
- The default value set in the executable binary file is 0.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**        1) To notify the client of the session ID each time the conversion target content is accessed:  
**COOKIEALWAYS=1**

**Remarks**

- Using this parameter prevents the IceWall SSO session ID from being deleted by the browser in the event that the number of cookies used by all connected Backend Web Servers exceeds the maximum number of cookies the browser can sustain. When this happens, some cookies required by Backend Web Server applications will be deleted. The cookies that are deleted depend on the browser specifications.
- If this parameter is set to 1 or 2, a path attribute is always added because of problems in cookie properties.
- If a path attribute is set with the COOKIEATTR parameter, that value is given priority. The path attribute set with this parameter is only effective when the COOKIEATTR parameter is not set.
- When session ID expiration settings are made on the Authentication Module (COOKIEEXP=1 and LOMETHOD=0), the expiration time is no longer added to the session ID, which is sent when a user browses content. Be aware that this causes the expiration time of the session

ID itself to be deleted.

- With session management using URL-Cookie (SESSION=1), notification of the session ID with the cookie is not made every time that the content is accessed even if this parameter is set to 1 or 2.
  - This parameter can also be defined in the host configuration file. However, be aware that setting this parameter to 0 in the Forwarder configuration file, and either 1 or 2 in the host configuration file will result in two different session IDs and two different cookies. One will be created at login, and the other will be created when content is accessed. To have a client notified of the session ID when accessing content from specific Backend Web Servers only, set the configuration files as below:
    - Forwarder configuration file : COOKIEALWAYS=1
    - Host configuration file (target server) : COOKIEALWAYS=1
    - Host configuration file (non-target server) : COOKIEALWAYS=0
- \* Set to 2 to send the authentication cookie again for all content.

See also

COOKIEATTR

SESSION

COOKIEEXP (Authentication Module configuration file)

LOMETHOD (Authentication Module configuration file)

Forwarder configuration file (dfw.conf)

---

## POSTLIMIT\_PAGE

Overview	Sets the template HTML page imposing restrictions on the time until POST data is sent to Forwarder.
Format	<p><b>POSTLIMIT_PAGE=<u>target page</u>[,<u>target page</u>][...]</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag: LOGIN: User ID login page Certificate login page FORCELOGIN: Forced login page PWDCHG: Password change page</li><li>• The configuration of these target pages is not order-sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To restrict the time until POST data is sent from the login page and the password change page: <b>POSTLIMIT_PAGE=LOGIN,PWDCHG</b></p>
Remarks	<ul style="list-style-type: none"><li>• If this parameter is not set, there is no limit on the time until POST data is sent.</li><li>• Does not operate correctly when the form tag in the target template HTML pages does not have the input tag below. &lt;input type="hidden" name="LIMIT" value="\$POST_LIMIT"&gt;</li><li>• Ignored when the target page is set to a value other than LOGIN, FORCELOGIN, PWDCHG.</li></ul>
See also	POSTLIMIT_TIME POSTLIMIT_ENC



# POSTLIMIT\_TIME

Overview	Sets the time limit when restricting the time until POST data is sent to Forwarder.
Format	<p><b>POSTLIMIT_TIME=<u>time limit</u></b> (minutes)</p> <ul style="list-style-type: none"><li>• The time limit is specified in minutes.</li><li>• The time limit can be set between 1 and 3600.</li><li>• The default value set in the executable binary file is 3.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To impose a restriction of 3 minutes to send data from the login page:</p> <p><b>POSTLIMIT_PAGE=LOGIN</b> <b>POSTLIMIT_TIME=3</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when the POSTLIMIT_PAGE parameter is set.</li><li>• Calculated in second increments. Maximum margin of error is 1 second.</li></ul>
See also	POSTLIMIT_PAGE POSTLIMIT_ENC

Forwarder configuration file (dfw.conf)

---

## POSTLIMIT\_ENC

Overview	Sets the key for encrypting and decrypting data set for the template HTML page when restricting the time until POST data is sent to Forwarder.
Format	<p><b>POSTLIMIT_ENC=<u>encryption/decryption key</u></b></p> <ul style="list-style-type: none"><li>• Encryption/decryption keys may contain the following types of characters. Numbers (0-9) Alphabetical characters (a-z, A-Z) Symbols (“-”   “_”   “.”   “!”   “~”   “*”   “!”   “(”   “)”) </li><li>• The encryption/decryption key has a maximum length of 256 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To encrypt the data set in the template HTML with “abc123ABC-!”, <b>POSTLIMIT_ENC=abc123ABC-!</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when the POSTLIMIT_PAGE parameter is set.</li><li>• When POSTLIMIT_PAGE is set and this parameter is not set, an error will occur.</li><li>• The system is not guaranteed to work as expected if characters other than those that are permitted to be set are used in the key.</li></ul>
See also	POSTLIMIT_PAGE POSTLIMIT_TIME

# FORCELOGIN\_ENC

Overview	Sets the key for encrypting and decrypting user information included on the forced login page.
Format	<p><b>FORCELOGIN_ENC=<u>encryption/decryption key</u></b></p> <ul style="list-style-type: none"><li>• Encryption/decryption keys may contain the following types of characters. Numbers (0-9) Alphabetical characters (a-z, A-Z) Symbols (“-”   “_”   “.”   “!”   “~”   “*”   “”   “(”   “)”) </li><li>• The encryption/decryption key has a maximum length of 256 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To use “abc123ABC-_!” as the key for encrypting and decrypting user information included on the forced login page: <b>FORCELOGIN_ENC=abc123ABC-_!</b></p>
Remarks	<ul style="list-style-type: none"><li>• When performing an operation that references POST data using the UserExit routine, be aware that the user ID and password sent from the forced login page are encrypted when encrypting with this function.</li><li>• The system is not guaranteed to work as expected if characters other than those that are permitted to be set are used in the key.</li></ul>
See also	None

# SESSION

Overview	Sets the client notification method for session IDs.
Format	<b>SESSION=<u>flag</u></b> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Session management using HTTP-Cookie</li><li>1 : Session management using URL-Cookie</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To use session management using URL-Cookie: <b>SESSION=1</b>
Remarks	<ul style="list-style-type: none"><li>• Session management using HTTP-Cookie is a method for maintaining the session using cookies.</li><li>• Session management using URL-Cookie is a method for maintaining the session by embedding the session ID in the URL. This method has lower security than session management using HTTP-Cookie and is useful for browsers that do not support cookies.</li></ul>
See also	None

# POSTKEY\_LOGIN

Overview	Sets a keyword used for identifying Forwarder login information. Setting this parameter is essential when using IceWall SSO in a multi-tier architecture.
Format	<b>POSTKEY_LOGIN=<u>identification keyword</u></b> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is ICEWALL_LOGIN.</li><li>• The initial value set in the standard configuration file is ICEWALL_LOGIN.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	1) To run IceWall with the default identification keyword: <b>POSTKEY_LOGIN=ICEWALL_LOGIN</b>
Remarks	<ul style="list-style-type: none"><li>• When IceWall SSO is being used in a multi-tier architecture, the identification keyword must be set in either front-end or backend IceWall SSO.</li><li>• Please use a keyword different from the default value when setting this parameter.</li></ul>
See also	POSTKEY_LOGOUT POSTKEY_PWDCHG

## POSTKEY\_LOGOUT

Overview	Sets a keyword used for identifying Forwarder logout information. Setting this parameter is essential when using IceWall SSO in a multi-tier architecture.
Format	<b>POSTKEY_LOGOUT=<u>identification keyword</u></b> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is ICEWALL_LOGOUT.</li><li>• The initial value set in the standard configuration file is ICEWALL_LOGOUT.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	1) To run IceWall with the default identification keyword: <b>POSTKEY_LOGOUT=ICEWALL_LOGOUT</b>
Remarks	<ul style="list-style-type: none"><li>• When IceWall SSO is being used in a multi-tier architecture, the identification keyword must be set in either front-end or backend IceWall SSO.</li><li>• Please use a keyword different from the default value when setting this parameter.</li><li>• It is recommended to set this parameter with a unique keyword and not use the default value when the user does not control logouts.</li></ul>
See also	POSTKEY_LOGIN POSTKEY_PWDCHG

# POSTKEY\_PWDCHG

Overview	Sets a keyword used for identifying Forwarder password change information. Setting this parameter is essential when using IceWall SSO in a multi-tier architecture.
Format	<b>POSTKEY_PWDCHG=<u>identification keyword</u></b> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is ICEWALL_PWDCHG.</li><li>• The initial value set in the standard configuration file is ICEWALL_PWDCHG.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	1) To run IceWall with the default identification keyword: <b>POSTKEY_PWDCHG=ICEWALL_PWDCHG</b>
Remarks	<ul style="list-style-type: none"><li>• When IceWall SSO is being used in a multi-tier architecture, the identification keyword must be set in either front-end or backend IceWall SSO.</li><li>• Please use a keyword different from the default value when setting this parameter.</li><li>• It is recommended to set this parameter with a unique keyword and not use the default value when the user does not control logouts.</li></ul>
See also	POSTKEY_LOGIN POSTKEY_LOGOUT

---

Forwarder configuration file (dfw.conf)

---

## REDIRECT <sup>(10.0)</sup>

**Overview** Sets the target URL when it is desired to redirect all users to a particular page after user authentication.

Additional functionality of this parameter is available since version 10.0.

**Format** **REDIRECT=**redirect location URL

- The URL must be an absolute path.
- The URL has a maximum length of 255 bytes.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- If this parameter is omitted, the URL entered in the browser at user authentication (or linked from another page) is displayed.
- When connecting to the Backend Web Server in the IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) Typical setting method:  
**REDIRECT=http://www.hp.com/**
- 2) To set an argument and redirect:  
**REDIRECT=http://www.hp.com/welcome.cgi?msg=Hello**
- 3) To redirect using an SSL connection for the target URL:  
**REDIRECT=https://www.hp.com/**

**Remarks**

- Be aware that the host name contained in the redirect URL must also be set in either the HOST or SHOST parameters, or the connection to the redirect's target URL will be unprotected by IceWall SSO.

```
REDIRECT=http://www.hp.com/  
HOST=XXX=www.hp.com
```

With this example configuration, after user authentication, the user will be redirected to www.hp.com through IceWall SSO.

- Be aware that because this runs through a general redirect command, URLs that receive requests through the POST method connect via the GET method.



- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. [10.0](#)

See also       HOST  
                  SHOST

# LOALIAS

Overview	Sets an alias name used to display the logout page.
Format	<b>LOALIAS=<u>logout alias name</u></b> <ul style="list-style-type: none"><li>• The alias name has a minimum length of one byte, and a maximum length of 64 bytes.</li><li>• The slash character “/” cannot be used in alias names.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is IW-LOGOUT.</li></ul>
Configuration example	1) To run IceWall with the standard logout alias name: <b>LOALIAS=IW-LOGOUT</b>
Remarks	<ul style="list-style-type: none"><li>• A logout page will not be displayed if this parameter is not set.</li><li>• Display of a logout page is not necessary. Logouts can be performed by sending the required information to IceWall SSO.</li><li>• It is recommended that this parameter not be set or be commented out in cases where users do not logout manually.</li></ul>
See also	PWDALIAS

## ICP\_VERSION <sup>(10.0)</sup>

Overview	<p>Sets the communication protocol between Forwarder and the Authentication Module.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b>ICP_VERSION=<u>version</u></b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the version:<ul style="list-style-type: none"><li>1.1 : Communication by ICP 1.0 expansion</li><li>2.0 : Communication by ICP 2.0</li></ul></li><li>• The default value set in the executable binary file is 1.1. <sup>(10.0)</sup></li><li>• The initial value set in the standard configuration file is 2.0. <sup>(10.0)</sup></li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To use ICP 2.0 for communication with the Authentication Module: <b>ICP_VERSION=2.0</b></p>
Remarks	<ul style="list-style-type: none"><li>• Multiple ICP versions cannot be used together.</li></ul>
See also	<p>CERTFAILBACK CERTLBFAILBACK ICP_AGENTSTR ICP_ENCSTR HTTPECHOHEADER (Authentication Module configuration file) LOGINFO (Authentication Module configuration file) TRANSID (Authentication Module configuration file) SESSIONIDLEN (Authentication Module configuration file) FAILBACK (Authentication Module configuration file) SEND (request control configuration file) NOTSEND (request control configuration file)</p>

Forwarder configuration file (dfw.conf)

---

## ICP\_AGENTSTR

Overview	Sets a user-defined text string that is added to the AGENT_ID in ICP 2.0 requests. Setting this parameter gives a unique ID to the sender of the request.
Format	<p><b>ICP_AGENTSTR=<u>user-defined character string</u></b></p> <ul style="list-style-type: none"><li>• The user-defined character string may contain uppercase and lowercase alphanumeric characters.</li><li>• The user-defined character string should have a maximum length of 35 bytes.</li><li>• If this is not set, nothing is added to AGENT_ID.</li><li>• The system may not run properly if characters other than uppercase and lowercase alphanumeric characters are used for the user-defined text string.</li><li>• If multiple lines are set, only the final line is effective.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• This parameter is ineffective when the ICP_VERSION parameter is set to 1.1.</li></ul>
Configuration example	<p>1) To perform communication with the Authentication Module using ICP 2.0 and add DFW to the AGENT_ID:</p> <p><b>ICP_VERSION=2.0</b> <b>ICP_AGENTSTR=DFW</b></p>
Remarks	<ul style="list-style-type: none"><li>• When the LOGINFO parameter of the Authentication Module configuration file is set to 2, the AGENT_ID is output to the Authentication Module error logs and access logs. In this case, the log output from the Authentication Module may be cut off if the user-defined character string is over 35 bytes.</li><li>• The standard setting for the AGENT_ID is shown below. [platform information];[web server name];[Forwarder version information]</li></ul> <p>Example: HP-UX B.11.31;Apache;10.00.00.xxxxxxX</p>
See also	ICP_VERSION

LOGINFO (Authentication Module configuration file)

## ICP\_ENCSTR 10.0

Overview	Sets the character string indicating the encryption method that is announced to the Authentication Module when using an original encryption method in the ICP 2.0 communication message encryption library.
Format	<p><b>ICP_ENCSTR=<u>user-defined character string</u></b></p> <ul style="list-style-type: none"><li>• The user-defined character string may contain uppercase and lowercase alphanumeric characters.</li><li>• The user-defined character string should have a maximum length of 32 bytes.</li><li>• The system may not run properly if characters other than uppercase and lowercase alphanumeric characters are used for the user-defined text string.</li><li>• If multiple lines are set, only the final line is effective.</li><li>• This parameter is ineffective when the ICP_VERSION parameter is set to 2.0.</li><li>• The default value set in the executable binary file is icewall.</li><li>• The initial value in the standard configuration file is originalenc in a comment.</li></ul>
Configuration example	<p>1) To announce to the Authentication Module the use of the original code “encrypto1” in ICP 2.0:</p> <p><b>ICP_ENCSTR=encrypto1</b></p>
Remarks	<ul style="list-style-type: none"><li>• When using an originally developed ICP 2.0 communication message encryption library, this parameter must always be set.</li><li>• When using the standard ICP 2.0 communication message encryption library, do not set this parameter or it must be set to “icewall.”</li><li>• The value set by this parameter is sent to the Authentication Module as the value for the “X-iw-encrypted” header. Example: X-iw-encrypted: icewall</li><li>• When using ICP 2.0, the “X-iw-encrypted” header is always sent to the Authentication Module.</li></ul>
See also	ICP_VERSION

### 2.1.3 Template HTML parameters

These parameters are used to configure the IceWall SSO-specific HTML that Forwarder displays to the client.

Parameter name	Mandatory	Overview
DOCS	×	Sets the HTML configuration file
LOCATIONURL <sup>(10.0)</sup>	×	Sets the redirect location for template HTML
LOCATIONRETRY	×	Sets the maximum redirect retries for template HTML
HTML_CHARSET	×	Sets the charset for template HTML

For details on these parameters, see the following pages.

---

**Forwarder configuration file (dfw.conf)**

---

## DOCS

Overview	Specifies the HTML configuration file name that defines the template HTML used by Forwarder.
Format	<p><b><u>DOCS=HTML configuration file name</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value set in the executable binary file is /opt/icewall-ss0/dfw/cgi-bin/html.conf.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ss0/dfw/cgi-bin/html.conf.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To use the HTML configuration file for i-mode content that is included in the standard installation:</p> <p><b>DOCS=/opt/icewall-ss0/dfw/cgi-bin/chtml.conf</b></p>
Remarks	<ul style="list-style-type: none"><li>• If the file set by this parameter cannot be read, the template HTML cannot be used, and Forwarder outputs the following content. &lt;HTML&gt; &lt;HEAD&gt;&lt;TITLE&gt;SYSTEM ERROR [ICEWALL DOCUMENT FORWARDER]&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 DocumentForwarder &lt;/BODY&gt; &lt;/HTML&gt;</li></ul>
See also	HTML configuration file



## LOCATIONURL 10.0

Overview	<p>Defines the redirect URLs allowed when template HTML is acquired remotely.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b>LOCATIONURL=<u>redirect permitted URL</u></b></p> <ul style="list-style-type: none"><li>• The URL must be an absolute path.</li><li>• The URL has a maximum length of 255 bytes.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• Without this parameter, template HTML will not be reacquired due to a redirect.</li><li>• When connecting to the template HTML redirect location in the IPv6 format, enclose the host name or IP address in square brackets ([ ]).</li></ul> <p><small>10.0</small></p>
Configuration example	<p>1) To permit the following address, www.hp.com/template, to be used as a template HTML redirect location:</p> <p><b>LOCATIONURL=http://www.hp.com/template</b></p>
Remarks	<ul style="list-style-type: none"><li>• Do not set URLs that pass through the IceWall SSO for the permissible template location. This may result in operability errors.</li><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. <small>10.0</small></li></ul>
See also	LOCATIONRETRY

## LOCATIONRETRY

Overview	Sets the maximum number of times a single template HTML file can be reacquired remotely due to redirects.
Format	<p><b>LOCATIONRETRY=<u>maximum redirect attempts</u></b></p> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is 1.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• This parameter cannot be set for every template HTML file.</li><li>• This parameter cannot be set for every URL defined in LOCATIONURL.</li></ul>
Configuration example	<p>1) To permit a maximum of two reacquires due to redirects: <b>LOCATIONRETRY=2</b></p>
Remarks	<ul style="list-style-type: none"><li>• Be aware that the first redirect received when acquiring content is not included in the maximum redirect count.</li></ul>
See also	LOCATIONURL

# HTML\_CHARSET

**Overview** Sets the charset value that is added to the Content-type header of the template HTML generated by Forwarder.

**Format** **HTML\_CHARSET=character code**

- The character string must include characters that can be recognized by browsers using “Shift\_JIS” or other encoding.
- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is Shift\_JIS.
- If this parameter is not set, no character set is added.

**Configuration example** 1) To set the character encoding for content output by Forwarder to “Shift\_JIS”:

**HTML\_CHARSET=Shift\_JIS**

Original Content-type header

**Content-type:text/html**

Content-type header that is set by HTML\_CHARSET

**Content-type:text/html;charset=SHIFT\_JIS**

**Remarks**

- Setting this parameter to a value not recognized by browsers may result in operational errors.
- Because this parameter is used to configure content output by Forwarder, this parameter does not apply to content sent from Backend Web Servers.
- This parameter does not apply to the post-authentication redirect response, which directs the user to the IceWall SSO.
- This parameter may cause content display problems in Netscape Navigator 4.x if the redirect and the actual redirect location have different character codes configured.  
(Example: HTML\_CHARSET of Shift\_JIS changes to UTF-8 after redirecting)

**See also** None

#### 2.1.4 Backend Web Server parameters

These parameters are used to configure the Backend Web Servers, which the user connects to through Forwarder.

Parameter name	Mandatory	Overview
HOST <small>10.0</small>	×	Sets an alias name for Backend Web Servers
SHOST <small>10.0</small>	×	Sets an alias name for Backend Web Servers (SSL)
SVRFILE	×	Sets the relationship between the alias and the host configuration file

For details on these parameters, see the following pages.

# HOST Overwrite (10.0)

Overview	<p>Sets an alias for the host name of a Backend Web Server. This allows clients to recognize Backend Web Servers as part of the IceWall SSO server directory.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b>HOST=alias name=host name[:port number](proxy server name[:proxy port number])</b></p> <ul style="list-style-type: none"><li>• The port number defaults to 80 if omitted.</li><li>• The host name has a maximum length of 64 bytes. (Excluding the port number)</li><li>• The alias name has a maximum length of 64 bytes.</li><li>• The slash character “/” cannot be used in alias names.</li><li>• The alias name is case sensitive, except for failovers.</li><li>• The proxy server name has a maximum length of 64 bytes (excluding the port number).</li><li>• The proxy port number defaults to 8080 if omitted.</li><li>• This parameter can span multiple lines.</li><li>• Failover settings can be made with this parameter.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: SCC=www.scc-kk.co.jp:80 HPJP=welcome.hp.com:80 LOCALHOST=localhost:80</li><li>• When connecting to the Backend Web Server in the IPv6 format, enclose the host name or IP address in square brackets ([ ]). (10.0)</li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) To set Backend Web Server: www.hp.com: <b>HOST=HP=www.hp.com</b></li><li>2) To set Backend Web Server: local.hp.com, and proxy server: proxy.hp.com:8088: <b>HOST=HP=local.hp.com(proxy.hp.com:8088)</b></li><li>3) To configure failover settings for the Backend Web Server: <b>HOST=HP=www.hp.com,local.hp.com</b></li><li>4) To configure failover settings when a proxy server is used: <b>HOST=HP=www.hp.com(proxy.hp.com),www.hp.com(proxy2.hp.com)</b></li></ol>

---

**Forwarder configuration file (dfw.conf)**

---

**Remarks**

- Failover host names are also changed for Backend Web Server content conversion.
- The following example shows how to configure this parameter on multiple lines.  
Configuration example: HOST=HP=www.hp.com  
HOST=HP=www.hp.co.jp
  - 1) Request from client  
When searching for a host name from an alias name, the content set first is always used.  
In the example above, the alias name included in the client request will always be translated to www.hp.com.
  - 2) Content conversion from a Backend Web Server  
When www.hp.com and www.hp.co.jp are part of any link, they will both be converted to the alias name “HP” as configured in the above example.
- Aliases used for both normal and failover settings are handled as follows:
  - 1) When the normal configuration occurs before the failover configuration:  
Client request processing will only use the normal configuration.  
Backend Web Server content conversion will use all lines of the configuration.
  - 2) When the failover configuration occurs before the normal configuration:  
Client request processing will only use the failover configuration, and this is how to configure the failover properly. Backend Web Server content conversion will use all lines of the configuration.
- Content conversion will use the first alias name found in the configuration for any Backend Web Server with multiple alias names.
- After a failover, the Authentication Module will not return to its previous state unless the Forwarder configuration file is overwritten.
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)

- The “IceWall SSO FailOver Option” is required to enable failover settings.
- Too many entries in this parameter could cause a reduction in performance.

See also

SHOST

SVRFILE

URLKEY (host configuration file)

SVRFILTER (host configuration file)

---

Forwarder configuration file (dfw.conf)

---

# SHOST overwrite (10.0)

Overview	<p>Sets an alias name for a host that is connecting through SSL.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b>SHOST=<u>alias name</u>=<u>host name</u>[:<u>port number</u>]</b></p> <ul style="list-style-type: none"><li>• The port number defaults to 443 if omitted.</li><li>• The host name has a maximum length of 64 bytes. (Excluding the port number)</li><li>• The alias has a maximum length of 64 bytes.</li><li>• The slash character “/” cannot be used in alias names.</li><li>• This parameter can span multiple lines.</li><li>• Failover settings can be made with this parameter.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• When connecting to the Backend Web Server in the IPv6 format, enclose the host name or IP address in square brackets ([ ]). (10.0)</li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) To set a host with host name that can be resolved: <b>SHOST=HP=www.hp.com</b></li><li>2) To set the host as an IP address: <b>SHOST=HP=192.168.0.1</b></li><li>3) To set up the host with a port number specified: <b>SHOST=HP=www.hp.com:444</b></li><li>4) To make failover settings: <b>SHOST=HP=www.hp.com,www1.hp.com</b></li></ol>
Remarks	<ul style="list-style-type: none"><li>• Failover configurations cannot include hosts that are both defined in the SSL configuration and normal HTTP configuration.</li><li>• After a failover, the Authentication Module will not return to its previous state unless the Forwarder configuration file is overwritten.</li></ul>



- Proxy servers cannot be set with this parameter, which can be done using the HOST parameter.
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
- The “IceWall SSO SSL Option” is required to use this parameter.
- The “IceWall SSO FailOver Option” is required to enable failover settings.
- Too many entries in this parameter could cause a reduction in performance.

See also

HOST  
SVRFILE  
URLKEY (host configuration file)  
SVRFILTER (host configuration file)

Forwarder configuration file (dfw.conf)

---

## SVRFILE

Overview	Allows the use of separate host configuration files that contain the alias names configured with the HOST and SHOST parameters. This enables each Backend Web Server to have a different configuration.
Format	<p><b>SVRFILE=<u>alias name,host configuration file name</u></b></p> <ul style="list-style-type: none"><li>• The alias name and host configuration file name cannot be omitted.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: SCC,./sample.conf HPJP,./sample.conf LOCALHOST,./sample.conf</li></ul>
Configuration example	<p>1) To use sample.conf as the host configuration file for the alias name “sys”:</p> <p><b>SVRFILE=sys,/opt/icewall-ss0/dfw/cgi-bin/sample.conf</b></p>
Remarks	<ul style="list-style-type: none"><li>• A system error will result if this parameter is used and the client request contains an alias name not associated with the host configuration file.</li><li>• The host configuration file does not necessarily need to have a one-to-one correspondence with an alias name. A single host configuration file may be associated with multiple alias names, and the settings can be shared.</li><li>• Absolute paths are not necessary when configuring the host configuration file.</li></ul>
See also	HOST SHOST

### 2.1.5 Password change parameters

These parameters are used for password changes, and they apply to the entire system.

Parameter name	Mandatory	Overview
PWDALIAS	×	Sets the alias for password changes
MINLEN <sup>(10.0)</sup>	×	Sets the minimum password length
MAXLEN <sup>(10.0)</sup>	×	Sets the maximum password length
EXPIRE <sup>(10.0)</sup>	×	Sets the password expiration date
SAMEPASS <sup>(10.0)</sup>	×	Allows setting a password that is the same as the user ID
ALPHANUM <sup>(10.0)</sup>	×	Sets the character types for passwords

For details on these parameters, see the following pages.

Forwarder configuration file (dfw.conf)

---

## PWDALIAS

Overview	Sets an alias name used to display the password change page when changing passwords.
Format	<p><b>PWDALIAS=<u>password change alias name</u></b></p> <ul style="list-style-type: none"><li>• The alias has a maximum length of 64 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is IW-PWDCHG.</li></ul>
Configuration example	<p>1) To use the standard password change alias name: <b>PWDALIAS=IW-PWDCHG</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is required to display the password change page, except when a user's password has expired and is prompted to change their password at login.</li><li>• Display of a password change page is not necessary. Password changes can be performed by sending the required information to IceWall SSO.</li><li>• It is recommended that this parameter be disabled or commented out in cases where users are not allowed to change their passwords. In this case, please set the Authentication Module to not check for password expiration dates.</li></ul>
See also	<p>LOALIAS PWDCHG (HTML configuration file) PWDEXPCHK (Authentication Module configuration file)</p>

## MINLEN 10.0

Overview	<p>Sets the minimum password length for new passwords.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b><u>MINLEN=password minimum characters</u></b></p> <ul style="list-style-type: none"><li>• The minimum password length can be a maximum of 128 bytes.</li><li>• There is no default value in the executable binary file. <small>10.0</small></li><li>• The initial value is not set in the standard configuration file.</li></ul>
Configuration example	<p>1) To set a minimum number of password length to 5 characters:</p> <p><b>MINLEN=5</b></p>
Remarks	<ul style="list-style-type: none"><li>• Password changes will result in error if this parameter is set to a value larger than the value set to the MAXLEN parameter.</li><li>• Setting this parameter to 0 does not result in a “no password” setting.</li><li>• Since this parameter will be removed in future releases, set PWDMILEN of the Authentication Module instead of this parameter. <small>10.0</small></li><li>• Do not set different values for this parameter and PWDMILEN of the Authentication Module at the same time. The same value can be set to these parameters. <small>10.0</small></li></ul>
See also	<p>PWDMILEN (Authentication Module configuration file)</p> <p>MAXLEN</p>

---

Forwarder configuration file (dfw.conf)

---

## MAXLEN 10.0

Overview	<p>Sets the maximum password length for new passwords.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b>MAXLEN=password maximum length</b></p> <ul style="list-style-type: none"><li>• The maximum password length can be a maximum of 128 bytes.</li><li>• There is no default value in the executable binary file. <small>10.0</small></li><li>• The initial value is not set in the standard configuration file.</li></ul>
Configuration example	<p>1) To set a maximum number of password length to 6 characters:</p> <p><b>MAXLEN=6</b></p>
Remarks	<ul style="list-style-type: none"><li>• Password changes will result in error if this parameter is set to a value smaller than the value set to the MINLEN parameter.</li><li>• Since this parameter will be removed in future releases, set PWDMAXLEN of the Authentication Module instead of this parameter. <small>10.0</small></li><li>• Do not set different values for this parameter and PWDMAXLEN of the Authentication Module at the same time. The same value can be set to these parameters. <small>10.0</small></li></ul>
See also	<p>PWDMAXLEN (Authentication Module configuration file)</p> <p>MINLEN</p>

## EXPIRE 10.0

Overview	<p>Sets the number of days a new password change is effective.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b>EXPIRE=password expiration days</b></p> <ul style="list-style-type: none"><li>• The unit for setting this value is in days.</li><li>• If 0 is set, the password will not expire (no expiration date).</li><li>• There is no default value in the executable binary file. <small>10.0</small></li><li>• The initial value is not set in the standard configuration file.</li></ul>
Configuration example	<p>1) To set new passwords to expire after 72 days:</p> <p><b>EXPIRE=72</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter can only have one setting, which applies to the entire system.</li><li>• Individual users cannot have different expiration times.</li><li>• The value of the PWDEXPCHK parameter in the Authentication Module configuration file has priority over this parameter, which means this parameter will be ineffective regardless of its setting if the PWDEXPCHK parameter is set to 0 (will not check password expiration values).</li><li>• Users will be asked to change their password when logging in after the password has expired. (Authentication Module must be set to check for expiration data.)</li><li>• Since this parameter will be removed in future releases, set PWDEXPIRE of the Authentication Module instead of this parameter. <small>10.0</small></li><li>• Do not set different values for this parameter and PWDEXPIRE of the Authentication Module at the same time. The same value can be set to these parameters. <small>10.0</small></li></ul>
See also	<p>PWDEXPIRE (Authentication Module configuration file)</p>

**Forwarder configuration file (dfw.conf)**

---

PWDEXPCHK (Authentication Module configuration file)



## SAMEPASS <sup>(10.0)</sup>

Overview	<p>Sets whether to allow or disallow passwords identical to the user ID.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b>SAMEPASS=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Allows passwords identical to the user ID</li><li>1 : Prohibits passwords identical to the user ID</li></ul></li><li>• There is no default value in the executable binary file. <sup>(10.0)</sup></li><li>• The initial value is not set in the standard configuration file.</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To prohibit passwords that are identical to the user ID:</p> <p><b>SAMEPASS=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• It is recommended to set this parameter to 1 (prohibit) to help ensure good security measures.</li><li>• Since this parameter will be removed in future releases, set PWDSAMEPASS of the Authentication Module instead of this parameter. <sup>(10.0)</sup></li><li>• Do not set different values for this parameter and PWDSAMEPASS of the Authentication Module at the same time. The same value can be set to these parameters. <sup>(10.0)</sup></li></ul>
See also	<p>PWDSAMEPASS (Authentication Module configuration file)</p>

## ALPHANUM <sup>10.0</sup>

**Overview**                Sets the type of characters that are available for use in passwords.

Some specifications of this parameter have been modified since version 10.0.

**Format**                **ALPHANUM=combination flag**

- One of the following values can be set to the combination flag:
  - 0 : All character types allowed, including alphabetical, numerical, and special characters.
  - 1 : Password must contain both alphabetical and numerical characters; no special characters allowed.
  - 2 : Numerical characters only
  - 3 : Alphabetical characters only
  - 4 : Special characters only
  - 5 : Password must contain both numerical and special characters; no alphabetical characters allowed.
  - 6 : Password must contain both alphabetical and special characters; no numerical characters allowed.
  - 7 : Password must contain all character types, including alphabetical, numerical, and special characters.
  - 8 : Password must contain both alphabetical and numerical characters; special characters allowed.
  - 9 : Password must contain numerical characters; alphabetical and special characters allowed.
  - 10 : Password must contain alphabetical characters; numerical and special characters allowed.
  - 11 : Password must contain special characters; alphabetical and numerical characters allowed.
  - 12 : Password must contain both numerical and special characters; alphabetical characters allowed.
  - 13 : Password must contain both alphabetical and special characters; numerical characters allowed.
- The following special characters are supported. Blank spaces may not be used. Single quotes are no longer supported from version 8.0 R2 and up.  
!"#\$%&()\*+,-./:;<=>?@[\\]^\_`{|}~
- There is no default value in the executable binary file. <sup>10.0</sup>
- The initial value is not set in the standard configuration file.
- The system is not guaranteed to work as expected if the value for this parameter is out of range.

Configuration example	<p>1) To configure passwords to require both alphabetical and numerical characters: <b>ALPHANUM=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• It is recommended to enforce a password policy that requires multiple character types to help ensure good security measures.</li><li>• Double-byte characters and single-byte katakana cannot be used.</li><li>• Since this parameter will be removed in future releases, set PWDALPHANUM of the Authentication Module instead of this parameter. (10.0)</li><li>• Do not set different values for this parameter and PWDALPHANUM of the Authentication Module at the same time. The same value can be set to these parameters. (10.0)</li></ul>
See also	<p>PWDALPHANUM (Authentication Module configuration file)</p>

### 2.1.6 Performance tuning parameters

The following parameters are used to enhance performance of the entire system while Forwarder is running.

Parameter name	Mandatory	Overview
RETRYCNTC	×	Sets the number of retries for connecting to the Authentication Module
RETRYTMC ⑩.0	×	Sets the retry interval for connecting to the Authentication Module
CERT_TOUT	×	Sets the receive timeout value with the Authentication Module
ALLOC	×	Sets the transfer buffer size
SET_CONTENT_LENGTH	×	Adds/removes the content-length information to the header
POSTWAITTIME	×	Sets the POST data read waiting time

For details on these parameters, see the following pages.

# RETRYCNTC

**Overview** Sets the number of retries allowed when connection to the Authentication Module fails.

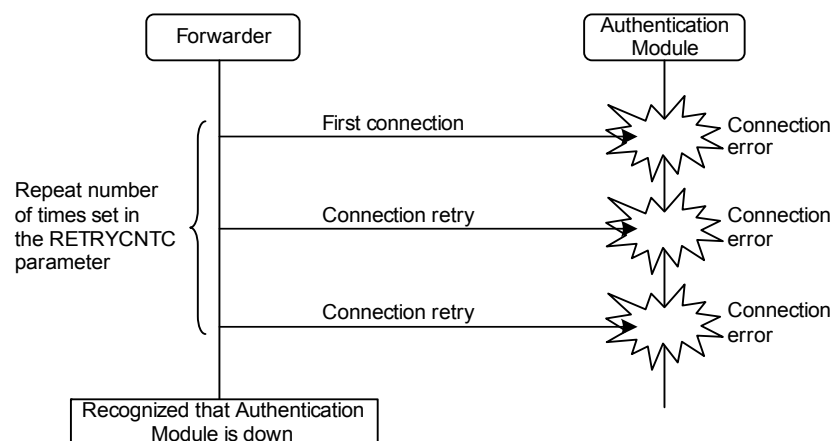
**Format** **RETRYCNTC=number of retries**

- The default value set in the executable binary file is 10.
- The initial value set in the standard configuration file is 10.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

**Configuration example** 1) To set the number of retries to the Authentication Module to 10:  
**RETRYCNTC=10**

**Remarks**

- The initial connection attempt is included in the retry count.
- The value set to this parameter is the number of retries allowed to connect to the Authentication Module. It is not the number of retries allowed for requesting a response after connecting to the module.



**See also**

- RETRYCNTC (Authentication Module configuration file)
- RETRYTMC (Forwarder configuration file)
- RETRYTMC (Authentication Module configuration file)

---

**Forwarder configuration file (dfw.conf)**


---

## RETRYTMC 10.0

Overview	<p>Sets the retry interval when connection to the Authentication Module fails.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b>RETRYTMC=<u>retry interval</u></b></p> <ul style="list-style-type: none"> <li>• The unit for setting the retry interval is seconds.</li> <li>• The default value set in the executable binary file is 3 seconds.</li> <li>• The initial value set in the standard configuration file is 3 seconds.</li> <li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li> </ul>
Configuration example	<p>1) To retry connecting to the Authentication Module at three-second intervals:</p> <p><b>RETRYTMC=3</b></p>
Remarks	<ul style="list-style-type: none"> <li>• The value set with this parameter is the wait time until the next attempt when retrying connection to the Authentication Module.</li> <li>• The detection of a connection error to the Authentication Module can take up to 12 seconds if no Authentication Server is found. If an Authentication Server is detected, but the Authentication Module is down, the error is detected virtually instantly. The actual time for the error detection to occur is dependant on the network status and cannot be configured.</li> <li>• The total time to determine an offline Authentication Module is calculated by:  “(RETRYCNTC parameter setting value × maximum of 12 seconds) + (RETRYCNTC parameter setting value × (RETRYTMC parameter setting value -1).” <span style="border: 1px solid black; border-radius: 50%; padding: 0 2px;">10.0</span></li> </ul> <p>Example: RETRYCNTC=5  RETRYTMC=2</p> <p>The total time until the Authentication Module is determined to be down is:  <math>(5 \times 12) + (2 \times (5-1)) = 68</math> seconds.</p>

The value calculated with the formula above is the maximum value. Use caution as Forwarder may not always wait until the calculated value depending on factors such as the network settings and environment.

See also      RETRYCNTC (Forwarder configuration file)  
                 RETRYCNTC (Authentication Module configuration file)  
                 RETRYTMC (Authentication Module configuration file)

Forwarder configuration file (dfw.conf)

---

# CERT\_TOUT

Overview	Sets the receive timeout counter for Authentication Module communication.
Format	<b>CERT_TOUT=<u>timeout value</u> (seconds)</b> <ul style="list-style-type: none"><li>• The unit for setting the timeout value is seconds.</li><li>• The default value set in the executable binary file is 600 seconds.</li><li>• The initial value set in the standard configuration file is 600 seconds.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	1) To set the receive timeout value for Authentication Module communication to 30 seconds: <b>CERT_TOUT=30</b>
Remarks	<ul style="list-style-type: none"><li>• Once connectivity to the Authentication Module has been established, this parameter specifies the timeout counter for receiving a response message after a request has been sent. It is not a timeout counter for general Authentication Module communication.</li><li>• This parameter also functions as the timeout counter when the response message is disrupted during transmission from the Authentication Module.</li><li>• The Authentication Module timeout error page will be displayed when a timeout occurs.</li></ul>
See also	RETRYCNTC RETRYTMC SYSTOUT (host configuration file) SYSTEM_TOUT_CERTD (HTML configuration file)



# ALLOC

Overview	Sets the initial buffer size to be used when receiving content from a Backend Web Server.
Format	<p><b>ALLOC=<u>allocate size</u> (bytes)</b></p> <ul style="list-style-type: none"><li>• The allocate size is specified in bytes.</li><li>• The default value set in the executable binary file is 65536 bytes.</li><li>• The initial value set in the standard configuration file is 65536 bytes.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To set the authentication buffer size to 20 kilobytes (one kilobyte = 1024 bytes):</p> <p><b>ALLOC=20480</b></p>
Remarks	<ul style="list-style-type: none"><li>• The content refers to both the header and body.</li><li>• If the content is larger than the buffer size specified by this parameter, another buffer of the specified size is added. Example: ALLOC=1000 If 1500 bytes of content are received, the buffer is increased as follows: 1000 bytes (initial buffer) + 1000 bytes (added buffer) = 2000 bytes</li><li>• This parameter can also be set in the host configuration file. If different values are set in the Forwarder configuration file and host configuration file, the value in the host configuration file is given priority.</li><li>• Specifying a large value (more than one megabyte) for this parameter will result in reduced performance.</li></ul>
See also	None

## SET\_CONTENT\_LENGTH

Overview	Specifies the addition or removal of the body size information to the HTTP header for content received from a Backend Web Server (Content-length header).
Format	<p><b>SET_CONTENT_LENGTH=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Do not add to HTTP header</li><li>1 : Add to HTTP header</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To add a Content-length header to the content received from a Backend Web Server:</p> <p><b>SET_CONTENT_LENGTH=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• If the client is an i-mode terminal, the Content-length header is required.</li><li>• If 1 is set to this parameter and a Content-length header already exists, the content length is recalculated and replaced by the new number.</li><li>• This function will not operate when non-buffering mode is enabled (BUFFER=0), except for conversion content.</li></ul>
See also	<p>CTYPE (host configuration file) BUFFER (host configuration file)</p>

# POSTWAITTIME

Overview	Sets the wait time for reading POST data sent from the client.
Format	<b>POSTWAITTIME=<u>wait time</u> (seconds)</b> <ul style="list-style-type: none"><li>• The unit for setting the timeout value is seconds.</li><li>• The default value set in the executable binary file is 180 seconds.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	1) To set the POST data reading wait time to 60 seconds: <b>POSTWAITTIME=60</b>
Remarks	<ul style="list-style-type: none"><li>• This counter becomes active once the POST data can no longer be read, resulting in a timeout error after the number of seconds set in this parameter have elapsed.</li><li>• If a timeout occurs during the reading of POST data, the system error page is displayed.</li><li>• If the POST data length is short relative to the Content-length sent from the client, a timeout occurs after the number of seconds set in this parameter have elapsed.</li><li>• Please note that if the web server CGI timeout value is smaller than the value set to this parameter, the web server kills (CGI timeout) the Forwarder process before a POST data reading timeout occurs.</li></ul>
See also	None

### 2.1.7 Security parameters

These security parameters are used to prevent attacks from clients.

Parameter name	Mandatory	Overview
MAXURL	×	Sets the maximum length of requests
MAXQUERY	×	Sets the maximum length of arguments
REV_PATH <small>(10.0)</small>	×	Sets specific URLs for referencing
SESSION_ENC_KEY	×	Sets the character strings used as keys for encryption and decryption of session IDs
DFWFILTER	×	Sets a filter for specific keywords
NOCHK_EXT_ALIAS	×	Permits/prohibits authentication for extensions
REQUESTFILTER <small>(10.0)</small>	×	Sets types of requests that will not accept access from clients

For details on these parameters, see the following pages.

# MAXURL

**Overview** Sets the maximum length of requests forwarded to a Backend Web Server.

**Format** **MAXURL=maximum request length (bytes)**

- The maximum length is specified in bytes.
- The argument (QueryString) is not included in this length.
- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is 512 bytes.

**Configuration example** 1) To limit requests to a Backend Web Server to 512 bytes:  
**MAXURL=512**

**Remarks**

- The maximum request length is measured starting from the alias name in the URL (including the “/” immediately before the alias name).
- A system error occurs when a request to the Backend Web Server contains a URL longer than the length specified in this parameter.
- If this parameter is not set, the maximum request length depends on the restrictions in the browser and Backend Web Server.
- This parameter can also be set in the host configuration file. The table below shows how the system will operate if the Forwarder configuration file and host configuration file contain different values for this parameter.

Setting value	Value that is used
Forwarder configuration file $\leq$ Host configuration file	Value in the Forwarder configuration file is used
Forwarder configuration file $>$ Host configuration file	Value in the host configuration file is used *1

\*1 After a check is performed using the setting value in the Forwarder configuration file, another check is performed using the setting value in the host configuration file.

**See also** MAXQUERY

# MAXQUERY

Overview	Sets the maximum length for arguments within requests that are forwarded to a Backend Web Server.						
Format	<b>MAXQUERY=<u>maximum argument length</u> (bytes)</b> <ul style="list-style-type: none"><li>• The maximum length is specified in bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is 512 bytes.</li></ul>						
Configuration example	1) To limit the length of arguments to a Backend Web Server to 64 bytes: <b>MAXQUERY=64</b>						
Remarks	<ul style="list-style-type: none"><li>• Backend Web Server attacks using long requests can be prevented by combining this parameter with the MAXURL parameter.</li><li>• If this parameter is not set, the maximum argument length in a request depends on the restrictions on the browser and Backend Web Server.</li><li>• This parameter can also be set in the host configuration file. The table below shows how the system will operate if the Forwarder configuration file and host configuration file contain different values for this parameter.</li></ul> <table><tr><th>Setting value</th><th>Value that is used</th></tr><tr><td>Forwarder configuration file <math>\leq</math> Host configuration file</td><td>Value in the Forwarder configuration file is used</td></tr><tr><td>Forwarder configuration file <math>&gt;</math> Host configuration file</td><td>Value in the host configuration file is used *1</td></tr></table> <p>*1 After a check is performed using the setting value in the Forwarder configuration file, another check is performed using the setting value in the host configuration file.</p>	Setting value	Value that is used	Forwarder configuration file $\leq$ Host configuration file	Value in the Forwarder configuration file is used	Forwarder configuration file $>$ Host configuration file	Value in the host configuration file is used *1
Setting value	Value that is used						
Forwarder configuration file $\leq$ Host configuration file	Value in the Forwarder configuration file is used						
Forwarder configuration file $>$ Host configuration file	Value in the host configuration file is used *1						
See also	MAXURL						

## REV\_PATH 10.0

Overview	<p>Configures URLs that bypass normal access control for requests forwarded to Backend Web Servers.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b>REV_PATH=</b><u>URL of the backend web server for authentication control</u></p> <ul style="list-style-type: none"><li>• The absolute path must be used to set the URL.</li><li>• The URL has a maximum length of 255 bytes.</li><li>• The URL host must be set in the HOST parameter or the SHOST parameter.</li><li>• This parameter can span multiple lines.</li><li>• This parameter operates differently for SSO mode and Reverse Proxy mode. See below:</li></ul> <p><b>SSO Mode</b></p> <p>Authentication is not required for the preset URL only.</p> <p><b>Reverse Proxy mode</b></p> <p>Only the preset URL is forwarded. Access will be denied to URLs that are not set in this parameter.</p> <ul style="list-style-type: none"><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• When connecting to the Backend Web Server in the IPv6 format, enclose the host name or IP address in square brackets ([ ]). <span style="border: 1px solid black; border-radius: 50%; padding: 0 2px;">10.0</span></li></ul>
Configuration example	<p>1) To set http://www.hp.com/ as a URL not requiring authentication in SSO mode:</p> <p><b>CERT=[host name]</b> <b>REV_PATH=http://www.hp.com/</b></p> <p>2) To set content that can be browsed in Reverse Proxy mode to /home or lower level of the Backend Web Server:</p> <p><b>REV_PATH=http://www.hp.com/home</b></p>
Remarks	<ul style="list-style-type: none"><li>• If the URL set in this parameter is accessed in SSO mode, the operation is the same as in Reverse Proxy mode. As a result, user data for logged-in users is not sent to the Backend Web Server.</li></ul>

**Forwarder configuration file (dfw.conf)**

---

- The cookie header sent from the client is sent to the back end that was set by this parameter. However, the IceWall SSO authentication cookie (IW\_INFO in the initial value) is not sent.
- Prefix searches are used to identify URLs. For example, assume that we have the two URLs below available.  
http://www.hp.com/index1.html  
http://www.hp.com/index2.html  
To enable both URLs in this parameter:  
REV\_PATH=http://www.hp.com/index
- SSO mode and Reverse Proxy mode can be distinguished by checking if the user ID is output to the Forwarder access log. If user IDs are in the log output, the system is in SSO mode.
- For details on the setup procedure for Reverse Proxy mode, see the CERT parameter.
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)

See also

CERT  
HOST  
SHOST  
CERTLB



## SESSION\_ENC\_KEY

**Overview** Specifies key strings used in encrypting and decrypting session IDs that are communicated between the Authentication Module and a client.

**Format** **SESSION\_ENC\_KEY=encryption/decryption key**

- Encryption/decryption keys may contain the following types of characters.
  - Numbers (0-9)
  - Alphabetical characters (a-z, A-Z)
  - Symbols (“-” | “\_” | “.” | “!” | “~” | “\*” | “” | “(” | “)”
- The encryption/decryption key has a maximum length of 256 bytes.
- Encryption and decryption will not occur unless this setting is configured.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)

**Configuration example** 1) To set the key to the character string “abc123ABC-\_!”:  
**SESSION\_ENC\_KEY=abc123ABC-\_!**

**Remarks**

- The generated session ID is a character string that is useful for a cookie or URL, and has a maximum size of 128 bytes.
- Session IDs encrypted by Forwarder have no effect on session IDs transferred to the agent or session IDs sent to the Authentication Module.
- If session management using URL-Cookie (SESSION=1) is implemented, be sure to consider the session ID length so that the entire URL does not exceed the URL length restriction (which varies depending on the web server).
- The system is not guaranteed to work as expected if characters other than those that are permitted to be set are used in the key.

**See also** None

# DFWFILTER

Overview	Sets the HTML tag filter for specific keywords. This setting enables the prevention of cross site scripting attacks on the login error page.												
Format	<p><b>DFWFILTER=flag</b></p> <ul style="list-style-type: none"><li>• The possible values for this flag are shown below.<ul style="list-style-type: none"><li>0 : No filtering</li><li>1 : Filtering is performed (all content except for that displayed by the Backend Web Server)</li><li>2 : Filtering is performed (all display content)</li></ul></li><li>• The flag value determines the filtering timing, as detailed below.<p><b>When DFWFILTER=1</b></p><p>The filter is applied to all template HTML specific keywords other than content being displayed by the Backend Web Server.</p><p><b>When DFWFILTER=2</b></p><p>The filter is applied at all times whenever a specific keyword is converted, including content being displayed by the Backend Web Server.</p></li></ul> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is 1.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>												
Configuration example	1) To disable filtering: <b>DFWFILTER=0</b>												
Remarks	<ul style="list-style-type: none"><li>• Filtering is also performed on the redirect URL at the time of login.</li><li>• Filtering causes the following characters changed to entity references.<table><tr><td>"&lt;"</td><td>→ "&amp;lt;"</td></tr><tr><td>"&gt;"</td><td>→ "&amp;gt;"</td></tr><tr><td>"&amp;"</td><td>→ "&amp;amp;"</td></tr><tr><td>" " "</td><td>→ "&amp;quot;"</td></tr><tr><td>" ' "</td><td>→ "&amp;#39;"</td></tr><tr><td>"\r"</td><td>→ "&amp;#13;"</td></tr></table></li></ul>	"<"	→ "&lt;"	">"	→ "&gt;"	"&"	→ "&amp;"	" " "	→ "&quot;"	" ' "	→ "&#39;"	"\r"	→ "&#13;"
"<"	→ "&lt;"												
">"	→ "&gt;"												
"&"	→ "&amp;"												
" " "	→ "&quot;"												
" ' "	→ "&#39;"												
"\r"	→ "&#13;"												

“\n” → “&#10;”

- If the IceWall SSO specific keyword is used for a special purpose, such as in the Backend Web Server and UserExit routine, filtering can cause this process to operate improperly. In this case, disable filtering (DFWFILTER=0).
- Setting this parameter does not change the order of priority for content conversion. The content conversion process order remains the same as previous versions.

See also

GETFILTER (host configuration file)  
POSTFILTER (host configuration file)  
HTMLFILTER (host configuration file)  
SVRFILTER (host configuration file)

## NOCHK\_EXT\_ALIAS

Overview	Configures authentication authorization attributes for extensions. If the conditions set here are met, operation is performed in Reverse Proxy mode.
Format	<p><b>NOCHK_EXT_ALIAS=<u>alias name</u>,<u>case-sensitive flag</u>,<u>[extension]</u>[, ...]</b></p> <ul style="list-style-type: none"><li>• The alias name is defined by the alias name set in the HOST parameter or SHOST parameter, or by “*” (system-wide setting).</li><li>• One of the following values can be set to the case-sensitive flag:<ul style="list-style-type: none"><li>0 : Extension is not case-sensitive</li><li>1 : Extension is case-sensitive</li></ul></li><li>• The extensions are input without dots.</li><li>• Omitting the extension from the configuration will result in making authentication authorization necessary for all requests.</li><li>• Separate extensions by commas to configure multiple items on a single line.</li><li>• Extensions with different numbers of characters are considered unique.</li><li>• The range of allowable settings for each item is shown below.<ul style="list-style-type: none"><li>Alias name : 1 to 64 characters</li><li>Case-sensitive flag : 0 or 1</li><li>Extension : 0 to 16 characters</li><li>Entire setting : 256 characters</li></ul></li><li>• When the same alias name is used for multiple lines, only the last line for that alias name will be effective.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set the extensions gif and jpeg to bypass authentication authorization for the entire system, with the case-sensitive flag turned on: <b>NOCHK_EXT_ALIAS=*,1,gif,jpeg</b></p> <p>* As the case-sensitive flag is turned on in this example, authentication authorization will occur if the request extension is such as “GIF.”</p> <p>2) To set the extensions gif and jpeg to bypass authentication authorization for the entire system, with the case-sensitive flag turned off:</p>

**NOCHK\_EXT\_ALIAS=\*,0,gif,jpeg**

- \* As the case-sensitive flag is turned off in this example, authentication authorization will not occur even if the request extension is such as "GIF."

- 3) To set the extensions gif and jpeg to bypass authentication authorization for the entire system, with the case-sensitive flag turned on; and to set only gif to bypass authentication authorization for a specific alias (ALIAS1):

**NOCHK\_EXT\_ALIAS=\*,1,gif,jpeg****NOCHK\_EXT\_ALIAS=ALIAS1,1,gif**

- \* As the case-sensitive flag is turned on in this example, authentication authorization will occur if the request extension is such as "GIF."

- 4) To set all extensions to require authentication authorization for the entire system, with the case-sensitive flag turned on; and to set gif and jpeg to bypass authentication authorization for only a specific alias (ALIAS1):

**NOCHK\_EXT\_ALIAS=\*,1,****NOCHK\_EXT\_ALIAS=ALIAS1,1,gif,jpeg**

- \* As the case-sensitive flag is turned on in this example, authentication authorization will occur if the request extension is such as "GIF."
- \* NOCHK\_EXT\_ALIAS=\*,1, can be omitted.

- 5) To set the extensions gif and jpeg to bypass authentication authorization for the entire system, with the case-sensitive flag turned on; and to require authentication authorization on all extensions for only a specific alias (ALIAS1):

**NOCHK\_EXT\_ALIAS=\*,1,gif,jpeg****NOCHK\_EXT\_ALIAS=ALIAS1,1,**

- \* As the case-sensitive flag is turned on in this example, authentication authorization will occur if the request extension is such as "GIF."

**Remarks**

- The alias name and case-sensitive flag cannot be omitted.
- Specific alias name settings always have priority over the general system-wide setting using the "\*" character. This line of code is used only when there is no alias name match.
- Regular expressions cannot be used to set this parameter.

**Forwarder configuration file (dfw.conf)**

---

- The alias name is case-sensitive regardless of the case-sensitive flag setting.
- If the extension is omitted, authentication authorization is required for all requests to the Backend Web Server.
- This parameter's configuration is processed in the order it was input, except for the general system-wide settings.
- If multiple extensions are specified in this parameter, the system will check extensions in the order in which they are listed in this parameter. Thus, placing an extension that is frequently requested lower down on the list will reduce the efficiency of checking. It is recommended to organize the configuration in the order of most-often used extensions to least-often used extensions.

See also      HOST  
              SHOST  
              REV\_PATH

# REQUESTFILTER 10.0

Overview	<p>Sets types of requests that will not accept access from clients.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>REQUESTFILTER=<u>request type</u>[,<u>request type</u>,...]</b></p> <ul style="list-style-type: none"><li>• The following values can be specified for the request type: LOGIN: Login, display login page LOGOUT: Logout, display logout page ACCESS: Access control (forward) PWDCHG: Password change, display password change page AGTLOGIN: Login, display login page when linking with Agent Option AGTPWDCHG: Password change, display password change page when linking with Agent Option</li><li>• The configuration of the request types is not order-sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To not accept requests for login-related functions by Forwarder: <b>REQUESTFILTER=LOGIN</b></p> <p>2) To not accept requests for login-related functions and logout-related functions by Forwarder: <b>REQUESTFILTER=LOGIN,LOGOUT</b></p>
Remarks	<ul style="list-style-type: none"><li>• Use this parameter when there are types of requests for unprovided services or when access has been temporarily stopped for maintenance.</li><li>• When the types of requests set to this parameter are requested from the client, the request filter error page is displayed. The request filter error page can be configured by the FILTER_REQUEST parameter.</li><li>• When the types of requests set to this parameter are requested from the client, the type of request that access was stopped for is output in</li></ul>

**Forwarder configuration file (dfw.conf)**

---

the security log. The log is not output if the security log is not configured with the SECURITY parameter or if output is not configured with the SECINFO parameter.

- For Reverse Proxy mode, all connections are access control (forward) request types.

See also

SECURITY

SECINFO

FILTER\_REQUEST (HTML configuration file)



### 2.1.8 Client certificate parameters

These parameters establish client certificates for user authentication.

Parameter name	Mandatory	Overview
CC_UID	×	Sets a client certificate user ID area
CC_UIDKEYS	×	Sets the start position for acquiring user IDs
CC_UIDKEYE	×	Sets the end position for acquiring user IDs
CC_ENVNAME	×	Sets the environment variable name for acquiring client certificates
CC_DECODE_FLG	×	Turns on/off Forwarder decoding of the client certificate
CC_ENVUID	×	Sets the name of the environment variable that includes the user ID from the client certificate information
CC_ENVSERIAL	×	Sets the environment variable that includes the serial number from the client certificate information.
CC_ENVEXPIRE	×	Sets the environment variable that includes the certificate expiration date from the client certificate information
CC_ENVISSUER	×	Sets the environment variable name that includes the issuer information from the client certificate information

For details on these parameters, see the following pages.

Forwarder configuration file (dfw.conf)

---

## CC\_UID

Overview	Sets an area to store the user ID, which is taken from the client certificate.
Format	<p><b>CC_UID=<u>area name</u></b></p> <ul style="list-style-type: none"><li>• The following values can be set to the area name: CN EMAIL OU</li><li>• When multiple OUs are set in the subject area of the certificate, all of the OUs are targeted.</li><li>• Not specifying the area name will result in an error.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To acquire the user ID from the OU area: <b>CC_UID=OU</b></p>
Remarks	<ul style="list-style-type: none"><li>• If this parameter is not set, IceWall SSO does not use certificates even though the one is selected at the client side.</li><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	<p>CC_UIDKEYS CC_UIDKEYE</p>

## CC\_UIDKEYS

Overview	Specifies the character string which acts as the start position for extracting the user ID from the area of the client certificate specified with the CC_UID parameter.
Format	<p><b>CC_UIDKEYS=<u>reference start character string</u></b></p> <ul style="list-style-type: none"><li>• Refers to the character string defined by this parameter in the area set with the CC_UID parameter. If a reference start character string exists, the text immediately following the detected character string is used as the user ID.</li><li>• If no reference start character string is set, the characters from the start of the area specified by the CC_UID parameter is used as the user ID.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>Example: when the Certificate is as follows:</p> <pre>Serial      : 0d1000aef9caf635bc4ed7603121030e Not Befor   : 20010227000000 Not After   : 20010425235959 Subject     : /O=xxx Corporation/OU=Client Certificate Service CA/               OU=OP1 - user001/OU=OP2 - client certificate/               OU=OP3 - 0/CN=user001 Issuer      : /O=xxx Corporation/CN= Client Certificate Service CA</pre> <p>1) To acquire “user001” as the user ID from the OU area: <b>CC_UID=OU</b> <b>CC_UIDKEYS=OP1 -</b> * For “OP1 - ” the space after the hyphen “-” is also set.</p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when the CC_UID parameter is set.</li><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	CC_UID CC_UIDKEYE

---

Forwarder configuration file (dfw.conf)

---

## CC\_UIDKEYE

**Overview** Specifies the character string which acts as the end position for extracting the user ID from the area of the client certificate specified with the CC\_UID parameter.

**Format** **CC\_UIDKEYE=reference end character string**

- Refers to the character string defined by this parameter in the area set with the CC\_UID parameter. If a reference end character string exists, the user ID is extracted from the start of the area specified with the CC\_UID parameter to the last character immediately before the character defined by this parameter.
- If the CC\_UIDKEYS parameter has been set, the user ID is extracted starting from the character following the character string detected with that parameter to the last character immediately before the character string defined by this parameter.
- If this parameter is not specified, the user ID is extracted from the start of the area specified with the CC\_UID parameter or from the character string starting from the position specified by the CC\_UIDKEYS parameter to the end of the string.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)

**Configuration example**

Example: when the certificate is as follows:

```
Serial      : 0d1000aef9caf635bc4ed7603121030e
Not Befor   : 200102270000000
Not After   : 20010425235959
Subject     : /O=xxx Corporation/OU=Client Certificate Service CA/
              OU=OP1 - user001/OU=OP2 - client certificate/
              OU=OP3 - 0/CN=user001
Issuer      : /O=xxx Corporation/CN= Client Certificate Service CA
```

- 1) To acquire “user001” as the user ID from the CN area:

```
CC_UID=CN
CC_UIDKEYS=
CC_UIDKEYE=
```

- 2) To acquire “user001” as the user ID from the OU(OPT1) area:

```
CC_UID=OU
CC_UIDKEYS=OP1 -
```

**CC\_UIDKEYE=**

- 3) To acquire “client cert” as the user ID from the OU(OPT2) area:

**CC\_UID=OU**

**CC\_UIDKEYS=OP2 -**

**CC\_UIDKEYE=ificate**

\* Be sure to input the space at the end of the CC\_UIDKEYS line.

- 4) To acquire “user0” as the user ID from the CN area:

**CC\_UID=OU**

**CC\_UIDKEYS=**

**CC\_UIDKEYE=01**

Remarks

- This parameter is effective only when the CC\_UID parameter is set.
- When using this parameter, the “IceWall SSO Client Certificates Option” is required.

See also

CC\_UID

CC\_UIDKEYS

Forwarder configuration file (dfw.conf)

---

## CC\_ENVNAME

Overview	Sets the name of the environment variable for acquiring client certificates.
Format	<p><b>CC_ENVNAME=<u>environment variable name</u></b></p> <ul style="list-style-type: none"><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set “CLIENT_CERT” as the environment variable name, which will store client certificate data:</p> <p><b>CC_ENVNAME=CLIENT_CERT</b></p>
Remarks	<ul style="list-style-type: none"><li>• The system will attempt to acquire the client certificate from the following environment variables if this parameter is not set, or if the configured environment variable does not exist. This function is provided for backward compatibility. CLIENT_CERT SSL_CLIENT_CERT</li><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	<p>CC_UID CC_UIDKEYS CC_UIDKEYE CC_DECODE_FLG</p>

# CC\_DECODE\_FLG

**Overview** Turns on/off Forwarder decoding of client certificates.

**Format** **CC\_DECODE\_FLG=flag**

- One of the following values can be set to the flag:
  - 0 : Forwarder does not decode the certificate
  - 1 : Forwarder decodes the certificate
- The default value set in the executable binary file is 1.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**

1) To acquire the client certificate from the environment variable HTTP\_IW\_CLIENT\_CERT, configure Forwarder to decode the certificate, and acquire various information:

**CC\_DECODE\_FLG=1**  
**CC\_ENVNAME=HTTP\_IW\_CLIENT\_CERT**

**Remarks**

- If this parameter is set to 0, the CC\_ENVUID parameter, CC\_ENVSERIAL parameter, CC\_ENVEXPIRE parameter, and CC\_ENVISSUER parameter (all described later) must be set.
- The “IceWall SSO Client Certificates Option” is required only when using this parameter for client certificates in IceWall SSO. This requirement does not apply if IceWall SSO client certificates will not be used.

**See also**

CC\_ENVNAME  
CC\_ENVUID  
CC\_ENVSERIAL  
CC\_ENVEXPIRE  
CC\_ENVISSUER

---

**Forwarder configuration file (dfw.conf)**

---

## CC\_ENVUID

Overview	Sets the name of the environment variable that contains the user ID from the client certificate information
Format	<p><b>CC_ENVUID=<u>environment variable name</u></b></p> <ul style="list-style-type: none"><li>Define the name that can be acquired as the environment variable name. Example: When HTTP_SSLCC_SUBJECT is the environment variable name: ○ : HTTP_SSLCC_SUBJECT × : SSLCC_SUBJECT</li><li>There is no default value in the executable binary file.</li><li>The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To acquire the user ID of the client certificate from the environment variable HTTP_IW_CC_SUBJECT: <b>CC_DECODE_FLG=0</b> <b>CC_ENVUID=HTTP_IW_CC_SUBJECT</b></p>
Remarks	<ul style="list-style-type: none"><li>This parameter must be set when CC_DECODE_FLG is set to 0.</li><li>This parameter is ineffective when CC_DECODE_FLG is set to 1.</li><li>Use the CC_UIDKEYS parameter and CC_UIDKEYE parameter when retrieving a part of the value for the environment variable specified by this parameter as a user ID.</li><li>When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	<p>CC_UIDKEYS CC_UIDKEYE CC_DECODE_FLG CC_ENVSERIAL CC_ENVEXPIRE CC_ENVISSUER</p>



## CC\_ENVSERIAL

Overview	Sets the name of the environment variable that contains the serial number from the client certificate information.
Format	<p><b>CC_ENVSERIAL=<u>environment variable name</u></b></p> <ul style="list-style-type: none"><li>Define the name that can be acquired as the environment variable name. Example: When HTTP_SSLCC_SERIAL is the environment variable name: ○ : HTTP_SSLCC_SERIAL × : SSLCC_SERIAL</li><li>There is no default value in the executable binary file.</li><li>The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To acquire the client certificate serial number from the environment variable HTTP_IW_CC_SERIAL:</p> <p><b>CC_DECODE_FLG=0</b> <b>CC_ENVSERIAL=HTTP_IW_CC_SERIAL</b></p>
Remarks	<ul style="list-style-type: none"><li>This parameter must be set when CC_DECODE_FLG is set to 0.</li><li>This parameter is ineffective when CC_DECODE_FLG is set to 1.</li><li>When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	<p>CC_DECODE_FLG CC_ENVUID CC_ENVEXPIRE CC_ENVISSUER</p>

## CC\_ENVEXPIRE

Overview	Sets the name of the environment variable that contains the expiration date information from the client certificate information.
Format	<p><b>CC_ENVEXPIRE=<u>environment variable name</u></b></p> <ul style="list-style-type: none"><li>• Define the name that can be acquired as the environment variable name. Example: When HTTP_SSLCC_EXPIRE is the environment variable name: ○ : HTTP_SSLCC_EXPIRE × : SSLCC_EXPIRE</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To acquire the client certificate expiration date information from the environment variable HTTP_IW_CC_EXPIRE:</p> <p><b>CC_DECODE_FLG=0</b> <b>CC_ENVEXPIRE=HTTP_IW_CC_EXPIRE</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter must be set when CC_DECODE_FLG is set to 0.</li><li>• This parameter is ineffective when CC_DECODE_FLG is set to 1.</li><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	<p>CC_DECODE_FLG CC_ENVUID CC_ENVSERIAL CC_ENVISSUER</p>

# CC\_ENVISSUER

Overview	Sets the name of the environment variable that contains the certificate issuer information from the client certificate information.
Format	<p><b>CC_ENVISSUER=<u>environment variable name</u></b></p> <ul style="list-style-type: none"><li>Define the name that can be acquired as the environment variable name. Example: When HTTP_SSLCC_ISSUER is the environment variable name: ○ : HTTP_SSLCC_ISSUER × : SSLCC_ISSUER</li><li>There is no default value in the executable binary file.</li><li>The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To acquire the client certificate issuer information from the environment variable HTTP_IW_CC_ISSUER:</p> <p><b>CC_DECODE_FLG=0</b> <b>CC_ENVISSUER=HTTP_IW_CC_ISSUER</b></p>
Remarks	<ul style="list-style-type: none"><li>This parameter must be set when CC_DECODE_FLG is set to 0.</li><li>This parameter is ineffective when CC_DECODE_FLG is set to 1.</li><li>Make sure to use to separate the acquired issuer information using a forward slash. Example: /C=jp/ST=tokyo...</li><li>When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	<p>CC_DECODE_FLG CC_ENVUID CC_ENVSERIAL CC_ENVEXPIRE</p>

### 2.1.9 POST data inheritance parameters

These parameters are used to configure the POST data inheritance functions.

Parameter name	Mandatory	Overview
POST_INHERIT	×	Turns on/off the POST data inheritance function
MAXPOST	×	Sets the maximum size of the inheritable POST data
POSTNAME	×	Sets the QueryString name when inheriting
POST_HTML	×	Sets the POST data inheritance template HTML file
POST_ENC	×	Sets the key which acts as the argument for inheriting

For details on these parameters, see the following pages.

# POST\_INHERIT

Overview	Turns on/off the function to resend the POST data after relogin from a session timeout.
Format	<p><b>POST_INHERIT=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : POST data is not inherited</li><li>1 : POST data is inherited</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To enable the POST data inheritance function: <b>POST_INHERIT=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• POST data can be inherited only when Content-type is “application/x-www-form-urlencoded.”</li><li>• The POST_HTML parameter must be set in order to set the POST_INHERIT parameter to 1 to perform inheritance of POST data.</li></ul>
See also	<p>MAXPOST POSTNAME POST_HTML POST_ENC MAXPOST_ERR (HTML configuration file)</p>

# MAXPOST

Overview	Sets the maximum size of the inheritable POST data.
Format	<b>MAXPOST=<u>maximum size (bytes)</u></b> <ul style="list-style-type: none"><li>• The maximum size is specified in bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set the maximum size of the inheritable POST data to 1024 bytes: <b>MAXPOST=1024</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is disabled when the POST_INHERIT parameter is set to 0.</li><li>• Because QueryString is used in the inheritance of the POST data, it may be restricted by the browser or web server even if the size of the POST data is equal to or less than the value set by this parameter. For details on the browser and web server restrictions, check their respective specifications.<ul style="list-style-type: none"><li>* In Internet Explorer 6.0, the upper limit of the URL is 2083 bytes.</li></ul></li><li>• POST data is inherited using the QueryString function, which has length restriction set by the MAXQUERY parameter. Take note of the value of the MAXQUERY parameter when setting this parameter.</li></ul>
See also	POST_INHERIT POSTNAME POST_HTML POST_ENC MAXPOST_ERR (HTML configuration file)

# POSTNAME

Overview	Sets the parameter name to be used for inheriting POST data
Format	<b>POSTNAME=<u>parameter name</u></b> <ul style="list-style-type: none"><li>• Use characters that can be specified in QueryString to set the parameter name.</li><li>• The parameter name must be at least 1 character in length with a maximum of 64 characters.</li><li>• The default value set in the executable binary file is iwpost.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	1) To enable the POST data inheritance function and set the parameter name when inheriting to “icewallpost”: <b>POST_INHERIT=1</b> <b>POSTNAME=icewallpost</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is disabled when the POST_INHERIT parameter is set to 0.</li><li>• This parameter cannot be set to the same value as the AGENT_KEY parameter, QUERY_ENC_NAME parameter, and RELOGIN_KEY parameter (both described later).</li></ul>
See also	POST_INHERIT MAXPOST POST_HTML POST_ENC MAXPOST_ERR (HTML configuration file)

Forwarder configuration file (dfw.conf)

---

## POST\_HTML

Overview	Sets the POST data inheritance template HTML file that automatically sends the POST data that is inherited after login.
Format	<b>POST_HTML=<u>POST data inheritance template HTML file path</u></b> <ul style="list-style-type: none"><li>• The file path has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set to the standard POST data inheritance template HTML file: <b>POST_HTML=/opt/icewall-ss0/html/iw_postdata.html</b>
Remarks	<ul style="list-style-type: none"><li>• JavaScript must be configured in the POST data inheritance template defined by this parameter to allow automatic sending of data at the browser side.</li></ul>
See also	POST_INHERIT MAXPOST POSTNAME POST_HTML MAXPOST_ERR (HTML configuration file)



## POST\_ENC

Overview	Specifies the character string to be used as a key when encrypting and decrypting the argument for inheriting POST data.
Format	<p><b>POST_ENC=<u>encryption/decryption key</u></b></p> <ul style="list-style-type: none"><li>• Encryption/decryption keys may contain the following types of characters.<ul style="list-style-type: none"><li>Numbers (0-9)</li><li>Alphabetical characters (a-z, A-Z)</li><li>Symbols (“-”   “_”   “.”   “!”   “~”   “*”   “”   “(”   “)”</li></ul></li><li>• The encryption/decryption key has a maximum length of 256 bytes.</li><li>• This parameter must be configured to enable encryption/decryption.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set the key to the character string “abc123ABC-!”:</p> <p><b>POST_ENC=abc123ABC-!</b></p>
Remarks	<ul style="list-style-type: none"><li>• The system is not guaranteed to work as expected if characters other than those that are permitted to be set are used in the key.</li></ul>
See also	<p>POST_INHERIT MAXPOST POSTNAME POST_HTML MAXPOST_ERR (HTML configuration file)</p>

### 2.1.10 Agent parameters

These parameters are used to configure the Agent Option.

Parameter name	Mandatory	Overview
AGENT_KEY	×	Sets the agent link identification keyword
AGENT_PERMIT	×	Sets the conditions for enabling agent links
QUERY_ENC	×	Sets the key for encrypting and decrypting parameters between agents
QUERY_ENC_NAME	×	Sets the character string used as the judgment parameter when encrypting and decrypting arguments
QUERY_ENC_KIND <span>10.0</span>	×	Sets the character string used as the judgment parameter for the encryption type when encrypting and decrypting arguments
RELOGIN_KEY	×	Sets the parameter for relogin from the agent

For details on these parameters, see the following pages.

# AGENT\_KEY

Overview	Sets the keyword that identifies a request as coming from an agent.
Format	<b>AGENT_KEY=<u>identification keyword</u>[,<u>agent alias</u>]</b> <ul style="list-style-type: none"><li>• The identification keyword and agent alias has a maximum length of 32 bytes.</li><li>• Set the same identification keyword as the one set in the agent configuration file (agent.conf).</li><li>• The agent alias may be omitted, but this will result in link processing will occur for any requests that match the identification keyword.</li><li>• Set character strings for the agent alias that group the settings.</li><li>• This parameter can span multiple lines.</li><li>• If the same value is set multiple times for the identification keyword, only the first setting will be effective.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) To set AGENT_DFW as the identification keyword: <b>AGENT_KEY=AGENT_DFW</b></li><li>2) To set the identification keywords AGENT_DFW1 and AGENT_DFW2 as the agent group AGENT1: <b>AGENT_KEY=AGENT_DFW1,AGENT1</b> <b>AGENT_KEY=AGENT_DFW2,AGENT1</b></li></ol>
Remarks	<ul style="list-style-type: none"><li>• When using this parameter, the “IceWall SSO Agent Option” is required.</li><li>• The same value cannot be set to the POSTNAME parameter, QUERY_ENC_NAME parameter (described later), or RELOGIN_KEY parameter (described later).</li></ul>
See also	POSTNAME AGENT_PERMIT QUERY_ENC_NAME RELOGIN_KEY

## AGENT\_PERMIT <sup>(10.0)</sup>

**Overview**                Sets the conditions for permitting agent requests.

Additional functionality of this parameter is available since version 10.0.

**Format**                **AGENT\_PERMIT=agent alias,analysis method,value**

- The values used for the analysis method are as follows:
  - IP                : IPv4 address-based analysis
  - IPV6            : IPv6 address-based analysis <sup>(10.0)</sup>
  - HOST            : Host-based analysis
  - DOMAIN        : Domain-based analysis
- This parameter can span multiple lines.
- Set the agent alias to the same value as the AGENT\_KEY parameter.
- If one agent alias has multiple lines of configuration, analysis will be performed in order from top to bottom.
- When the analysis method is IP and IPV6, a range of IP addresses can be specified using the “-” character. If the agent URL information includes the host name, it will be converted to an IP address for proper analysis. <sup>(10.0)</sup>
- HOST-based analysis functions using complete matches. Port numbers are ineffective even if defined. IP addresses included in the URL agent information will not be converted to a host name for analysis purposes.
- Domain-based analysis uses the end of the character string to perform matches.
- When the analysis method is IPV6, use "::" and the IPv6 address can be omitted. <sup>(10.0)</sup>
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)

**Configuration example**

- 1) To set host-based analysis:  
**AGENT\_KEY=AGENTKEY1,AGENT1**  
**AGENT\_PERMIT=AGENT1,HOST,www.xxx.co.jp**

In this example, a successful match results if the host is “www.xxx.co.jp.”

- 2) To set host-based and IPv4 address-based analysis:

```
AGENT_KEY=AGENTKEY2,AGENT2
AGENT_PERMIT=AGENT2,HOST,www.xxx.co.jp
AGENT_PERMIT=AGENT2,HOST,www2.xxx.co.jp
AGENT_PERMIT=AGENT2,IP,192.168.0.1
```

In this example, a successful match results if the agent host name is either “www.xxx.co.jp” or “www2.xxx.co.jp,” or the IPv4 address is “192.168.0.1.”

- 3) To set host-based, IPv4 address-based, and domain-based analysis to perform analysis on the two AGENT\_KEY as a group:

```
AGENT_KEY=AGENTKEY3,AGENT3
AGENT_KEY=AGENTKEY4,AGENT3
AGENT_PERMIT=AGENT3,HOST,www.xxx.co.jp
AGENT_PERMIT=AGENT3,HOST,www2.xxx.co.jp
AGENT_PERMIT=AGENT3,IP,192.168.0.1-192.168.0.64
AGENT_PERMIT=AGENT3,DOMAIN,yyy.co.jp
```

In this example, a successful match will result if the host name is either “www.xxx.co.jp” or “www2.xxx.co.jp,” if the IPv4 address is in the range of “192.168.0.1” - “192.168.0.64,” or if the domain name is “yyy.co.jp.”

- 4) To set IPv6 address-based analysis:

```
AGENT_KEY=AGENTKEY4,AGENT4
AGENT_PERMIT=AGENT4,IPV6,fe80:0:0:0:0:0:0:1
```

In this example, a successful match will result if the agent's IPv6 address is “fe80:0:0:0:0:0:0:1.”

#### Remarks

- This parameter requires the agent alias to be set in the AGENT\_KEY parameter.
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. [10.0](#)
- When using this parameter, the “IceWall SSO Agent Option” is required.

#### See also

AGENT\_KEY

Forwarder configuration file (dfw.conf)

---

## QUERY\_ENC

Overview	Sets the key used for encryption/decryption of parameters sent between Forwarder and Agent.
Format	<p><b>QUERY_ENC=<u>encryption/decryption key</u></b></p> <ul style="list-style-type: none"><li>• The encryption/decryption key has a maximum length of 256 bytes.</li><li>• The key may contain uppercase and lowercase alphanumeric characters as well as the special characters (“-”   “_”   “.”   “!”   “~”   “*”   “”   “(”   “)”).</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To create the key using “abc123ABC-!”:</p> <p><b>QUERY_ENC=abc123ABC-!</b></p>
Remarks	<ul style="list-style-type: none"><li>• If this parameter is set, the key for performing encryption/decryption must be set in the agent QUERY_ENC parameter.</li></ul>
See also	QUERY_ENC (agent configuration file)

# QUERY\_ENC\_NAME

Overview	<p>Sets the character string used as the judgment parameter name when encrypting and decrypting arguments.</p> <p>This parameter name is system-wide, which necessitates the same character string to be specified for Forwarder and Agent.</p>
Format	<p><b><u>QUERY_ENC_NAME=parameter name</u></b></p> <ul style="list-style-type: none"><li>• The parameter name has a maximum length of 16 single byte alphanumeric characters.</li><li>• If multiple lines are set, only the final line is effective.</li><li>• The parameter name is case sensitive.</li><li>• The default value set in the executable binary file is param.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To set the parameter name between Forwarder and Agent to “agtparam”:</p> <p><b>QUERY_ENC_NAME=agtparam</b></p>
Remarks	<ul style="list-style-type: none"><li>• The same value cannot be set to the parameter name in the AGENT_KEY parameter, POSTNAME parameter, or RELOGIN_KEY parameter (described later).</li></ul>
See also	<p>RELOGIN_KEY QUERY_ENC POSTNAME QUERY_ENC_NAME (Agent configuration file)</p>

---

**Forwarder configuration file (dfw.conf)**

---

## QUERY\_ENC\_KIND

Overview	<p>Sets the character string used as the judgment parameter name for the encryption type when encrypting and decrypting arguments.</p> <p>This parameter name is system-wide, which necessitates the same character string to be specified for Forwarder and Agent.</p>
Format	<p><b><u>QUERY_ENC_KIND=parameter name</u></b></p> <ul style="list-style-type: none"><li>• The parameter name has a maximum length of 16 single byte alphanumeric characters.</li><li>• If multiple lines are set, only the final line is effective.</li><li>• The default value set in the executable binary file is agtkind.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To set the judgment parameter name for the encryption type between Forwarder and Agent to “enckind”:</p> <p><b>QUERY_ENC_KIND=enckind</b></p>
Remarks	None
See also	<p>QUERY_ENC</p> <p>QUERY_ENC_NAME</p> <p>QUERY_ENC_KIND (Agent configuration file)</p>



# RELOGIN\_KEY

**Overview** Sets the parameter for receiving a relogin request from the agent.

**Format** **RELOGIN\_KEY=parameter name**

- The parameter is defined using the “Name=Value” format.
- The parameter name has a maximum length of 64 bytes.
- If multiple lines are set, only the final line is effective.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)

**Configuration example** 1) To set “ForceAuthn=True” as the relogin parameter:  
**RELOGIN\_KEY=ForceAuthn=True**

**Remarks**

- Use the URL-encoded value of %3D to input the “=” sign.
- This parameter must be set to the same value as the agent RELOGIN\_KEY parameter.
- Multiple parameters cannot be set by separating them with ampersands “&.”
- If this parameter is not set, relogin requests cannot be received from the agent.
- If a relogin occurs using the settings in this parameter, the fixed value “ICEWALL\_RELOGIN” is replaced by a specific keyword in the login page send keyword LOGIN.
- The same value cannot be set to the parameter name in the AGENT\_KEY parameter, POSTNAME parameter, and QUERY\_ENC\_NAME parameter.

**See also** AGENT\_KEY  
QUERY\_ENC\_NAME  
POSTNAME  
RELOGIN\_KEY (agent configuration file)

## 2.2 Host configuration file [arbitrary file name]

### Overview

This configuration file is used to configure each Backend Web Server uniquely.

Parameters available to the user are as follows:

Parameter group	Parameter name
Parameters for content conversion	CTYPE
	URLKEY
	REPKEY
	REPKEY_EXT 10.0
	URLCONV_FLG
	URLCONV_ATTR_FLG 10.0
	ATTRQUOTE_FLG
Error page parameters	SYSERR 10.0
	SYSTOUT 10.0
	ERRKEY 10.0
Basic authentication parameters	BASICAUTH
	BA_UID
	BA_PWD
Parameters for information inheritance	HTTPDATA
	HEADER
	HEADER_FILTER 10.0
	COOKIE_FILTER
	HEADER_NAME_TID 10.0
	HEADER_NAME_UID 10.0
	HEADER_NAME_SID 10.0
	RES_HEADER 10.0
	UNCONV_HEADER
	CTRL_SPKEY 10.0

Parameter group	Parameter name
Cross site scripting handling parameters	GETFILTER
	GETEXCEPTION
	GETFILTERERR (10.0)
	POSTFILTER_LOG_FLG
	POSTFILTER
	POSTEXCEPTION
	POSTFILTERERR (10.0)
	POSTFILTER_LOG_FLG
	HTMLFILTER
	HTMLFILTERERR (10.0)
	SVRFILTER
	SVREXCEPTION
	SVRFILTERERR (10.0)
	SVRFILTERSTR
System tuning configuration parameters	RETRYCNTW
	RETRYTMW (10.0)
	TIMEOUT
	CLOSETIME (10.0)
	BUFFER
	LASTMOD_HEADER
	CENCODE
	URL_SCOLON
	FO_SEND
	FO_RECV
	FO_NODATA
	RECV_ZERO_FLG
Form authentication configuration parameters	FORM_FILE
Security parameters	SSL_CIPHER_SUITE

**Storage location**

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

**Remarks**

This file is specified with the SVRFILE parameter in the Forwarder configuration file.

Parameters that can be set in this file can also be specified in the Forwarder configuration file with the exception of HTTPDATA, HEADER, RES\_HEADER, and FORM\_FILE. The Forwarder configuration file serves as a general system configuration, which will be effective for all Backend Web Servers.

Parameters are processed differently for parameters that allow multiple-line configuration when a particular parameter is configured in both the Forwarder configuration file and the host configuration file.

- Multiple-line configurable parameters:  
The configuration from both the Forwarder configuration file and host configuration file is used to process content.
- Single-line only parameters:  
Only the configuration from the host configuration file is used to process content.

These parameters are described in the following pages.

### 2.2.1 Parameters for content conversion

These parameters are used to configure content conversions from Backend Web Servers.

Parameter name	Mandatory	Overview
CTYPE	×	Sets the conversion content MIME type
URLKEY	×	Sets the HTML tags targeted for URL conversion
REPKEY	×	Sets the keyword conversion
REPKEY_EXT <b>10.0</b>	×	Sets a keyword for extended keyword conversion to convert a URL that cannot be converted with the URLKEY parameter to a URL through the IceWall server
URLCONV_FLG	×	Turns on/off the function to use the ">" symbol in the attribute value to mark the end of tags
URLCONV_ATTR_FLG <b>10.0</b>	×	Sets whether or not to perform URL conversion on multiple attributes with different attribute names in a single tag when performing URL conversion with the URLKEY parameter
ATTRQUOT_FLG	×	Sets the quotation determination method during URL conversion tag extraction

For details on these parameters, see the following pages.

# CTYPE

Overview	Sets the conversion content MIME type for content received from Backend Web Servers.
Format	<p><b>CTYPE=<u>MIME type</u></b></p> <ul style="list-style-type: none"><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: text/plain text/html application/x-javascript application/x-www-form-urlencoded</li></ul>
Configuration example	<p>1) To enable content conversion of JavaScript library files: <b>CTYPE=application/x-javascript</b></p>
Remarks	<ul style="list-style-type: none"><li>• Content is converted when content matching the MIME type of this parameter is received.</li><li>• Do not set a binary file MIME type because doing so can corrupt the content.</li><li>• Do not set MIME multi-part content as it may include binary code.</li><li>• Content with MIME types not specified in this parameter are processed in non-buffering mode (BUFFER=0).</li></ul>
See also	URLKEY REPKEY BUFFER

# URLKEY

**Overview** Sets attribute names for tags that are included in content received from a Backend Web Server, which are converted to URLs through the IceWall server.  
This parameter is enabled only for content that is set by the CTYPE parameter.

**Format** **URLKEY=tag name,attribute name**

- The tag name has a maximum length of 30 bytes.
- The attribute name has a maximum length of 32 bytes.
- The tag name and attribute name are not case sensitive.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:

A,HREF  
BASE,HREF  
FRAME,SRC  
FORM,ACTION  
BASE,TARGET  
IMG,SRC  
SCRIPT,SRC  
BODY,BACKGROUND  
TD,BACKGROUND  
TR,BACKGROUND  
TABLE,BACKGROUND  
APPLET,CODEBASE  
INPUT,SRC  
LINK,HREF

**Configuration example**

- 1) To specify general link tags:  
**URLKEY=A,HREF**
- 2) To convert URLs that are redirected through META tag Refresh:  
**URLKEY=META,CONTENT**

**Remarks**

- URLs specified as tag attribute values can only be converted when they are specified with an absolute URL or an absolute path from the document root directory. URLs specified with relative paths from the current directory cannot be converted.

**Host configuration file [arbitrary file name]**

---

- Tags within the content are referenced in the order they are specified in this parameter. Specify tags that appear frequently within the content, such as A,HREF or IMG,SRC, before other tags.
- Please do not configure this parameter with tags that do not appear in content, as this may improve performance.
- Because HTTP-compressed content is handled as binary code in the URL conversion function, no URL conversion can be performed.
- For details on the URL conversion function, see the “IceWall SSO Web Application Developer's Manual.”

See also

CTYPE  
REPKEY  
URLCONV\_ATTR\_FLG



# REPKEY

Overview	<p>Sets a URL conversion keyword to enable IceWall server conversion of URLs that cannot be specified with the URLKEY parameter. This parameter is enabled only for content that is set by the CTYPE parameter.</p>
Format	<p><b>REPKEY=<u>search keyword</u>,<u>substitute string</u></b></p> <ul style="list-style-type: none"><li>• The search keyword is case sensitive.</li><li>• Commas and line feed codes cannot be used to set the search keyword and substitution string.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To convert a URL within JavaScript: <b>REPKEY=location.url=/index.html,location.url=/fw/dfw/XXX/index.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• Regular expressions cannot be used in the search keyword setting.</li><li>• Keyword conversion is normally used for URLs within JavaScript.</li><li>• Even when multiple attributes that can be converted exist in a single tag, all of the attributes can be converted.</li><li>• This parameter will apply to HTTP headers sent from Backend Web Servers in addition to general content.</li><li>• When cookies issued from Backend Web Servers have domain attributes set, the domain attribute must be changed or deleted by this parameter. (Set-cookie header example) Set-Cookie: Name=Value; domain=www.hp.com</li></ul> <p>If the IceWall server domain is www.hp.com, there is no need to make a change. However, if the domain is different, it must be changed as follows: (In this example, the IceWall server domain is icewall.hp.com.)</p>

---

Host configuration file [arbitrary file name]

---

REPKEY=domain=www.hp.com,domain=icewall.hp.com

- If cookies issued from Backend Web Servers have the secure attribute set, this attribute can be disabled by changing or deleting it with this parameter.

Example of deleting a secure attribute

REPKEY=domain=www.hp.com secure,domain=www.hp.com

- The keyword conversion function is executed in this order: HTTP header URL conversion function → Keyword conversion function → Extended keyword conversion function → URL conversion function within content. As a result, to convert the URL included in the HTTP header, the HTTP header URL conversion function must be used to specify the converted value as a search keyword.
- Shift JIS, EUC, and Unicode (UTF-8) are the supported character encoding types for the Backend Web Server content. The character encoding type must be configured to properly convert double-byte content using this keyword conversion parameter.
- To perform keyword conversion on URLs contained within text-format XML files, set the MIME type of the relevant XML file using the CTYPE parameter.
- The following characters cannot be used: null (0x00), line feeds (0x0a), and commas (0x2c).

See also

CTYPE  
URLKEY  
REPKEY\_EXT

## REPKEY\_EXT 10.0

**Overview** Sets a keyword for extended keyword conversion that converts a keyword that cannot be converted by the URLKEY parameter. This parameter is enabled only for content that is set by the CTYPE parameter.

This parameter is available since version 10.0.

**Format** **REPKEY\_EXT=search keyword,substitute string**

- The search keyword is case sensitive.
- To perform keyword conversion on a comma (“,”), define it as “\,”.
- To perform keyword conversion on 1-byte control codes (“\r”, “\n”, “\t”), define them as 2-byte character strings (“\r”, “\n”, “\t”).
- To perform keyword conversion on a 1-byte “\”, define it as “\\”.
- To perform keyword conversion on the 2-byte character strings “\r”, “\n”, and “\t” as they are, define them as 3-byte character strings (“\\r”, “\\n”, “\\t”).
- If a 1-byte “\” is defined by itself, it is deleted as an escape character.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)

**Configuration example** 1) To perform keyword conversion on “aaaa,bbbb” including a comma (,) and convert it to “cccc,dddd”:

**REPKEY\_EXT=aaaa¥,bbbb,cccc¥,dddd**

2) To perform keyword conversion on “AAAA(\n)BBBB” including a newline code (\n) and convert it to “CCCC(\n)DDDD”:

**REPKEY\_EXT=AAAA¥nBBBB,CCCC¥nDDDD**

**Remarks**

- Regular expressions cannot be used in the search keyword setting.
- Since extended keyword conversion for this parameter is processed immediately after keyword conversion by the REPKEY parameter, it is performed before URL conversion by the URLKEY parameter.
- Strings that include the null character (0x00) cannot be set.

**Host configuration file [arbitrary file name]**

---

- Except for the description above, extended keyword conversion is completely the same as keyword conversion by the REPKEY parameter. For the rest of the specification, see the REPKEY parameter.

See also        CTYPE  
                 URLKEY  
                 REPKEY

# URLCONV\_FLG

**Overview** Sets the tag extraction method for URL conversions.

**Format** **URLCONV\_FLG=flag**

- One of the following values can be set to the flag:
  - 0 : Bracket precedence extraction method [conventional method]
  - 1 : Quotation precedence extraction method
- The default value set in the executable binary file is 0.
- The initial value set in the standard configuration file is 1.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To set tag extraction for URL conversions to the quotation precedence extraction method:  
**URLCONV\_FLG=1**

**Remarks**

- The bracket precedence method extracts tags by only searching for brackets (<, >).
- The quotation precedence extraction method extracts tags while checking for quotation marks (" , ') paired with attribute values in tags.
- Use the quotation precedence method when brackets (<, >) are found in attribute values as shown below.  
Example: <a href="/index.cgi?name=aaaaa>bbbbbb">
- \* When the bracket precedence method is used:  
<a href="/index.cgi?name=aaaaa> is mistakenly recognized as a tag.
- Setting this parameter to the quotation precedence method may increase the functionality of the URLKEY parameter to include tags that were previously handled by the REPKEY parameter, and HTML tags defined in JavaScript code.
- In situations where attribute values are enclosed by quotation marks (single or double), a format error may result with the quotation precedence extraction method and the URL may not be converted if

**Host configuration file [arbitrary file name]**

---

even one of the conditions below is satisfied. In these situations, fix the content or use the bracket precedence extraction method.

- 1) Quotation marks are defined as attribute values
- 2) Either the first or last single-quote or double-quote is not defined

See also      URLKEY  
                 REPKEY

## URLCONV\_ATTR\_FLG 10.0

Overview	<p>Sets whether or not to perform URL conversion on multiple attributes with different attribute names in a single tag when performing URL conversion with the URLKEY parameter.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>URLCONV_ATTR_FLG=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Compares the prefix match of a single attribute in a single tag and performs URL conversion (backward compatibility)</li><li>1 : Compares the complete match of multiple attribute values with different attribute names in a single tag and performs URL conversion</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To compare the complete match of attribute value and attribute value2 included in a single input tag and perform URL conversion:</p> <p><b>URLKEY=input,value</b> <b>URLKEY=input,value2</b> <b>URLCONV_ATTR_FLG=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• Even when this parameter is set to 1, if there are multiple attributes with the same name in a single tag, only the first detected attribute is converted.</li><li>• Be aware that if this parameter is set to 0, the tag attribute name comparison method is prefix match. If this parameter is set to 1, the tag attribute name comparison method is complete match.</li><li>• The tag name comparison method is complete match, regardless of the setting for this parameter.</li></ul>

**Host configuration file [arbitrary file name]**

---

- Please be aware that performance may deteriorate if this parameter is set to 1 when it was set to 0.

See also           URLKEY



# ATTRQUOT\_FLG

Overview	Sets the quotation determination method during URL conversion tag extraction.
Format	<b>ATTRQUOT_FLG=<u>flag</u></b> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Do not determine the type of quotation mark (" or ').</li><li>1 : Determine the type of quotation mark.</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To determine the type of quotation mark: <b>ATTRQUOT_FLG=1</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when the URLCONV_FLG parameter is set to 1. Quotation marks are not used in tag extraction when set to 0.</li><li>• Always set this parameter to 1 when the HTMLFILTER parameter is set.</li><li>• Set this parameter to 0 when using quotation marks as shown below for attribute values in tags that are subject to URL conversion in the content. The type of opening and closing quotation marks is different (" and ' or ' and ", etc.)</li></ul>
See also	URLCONV_FLG HTMLFILTER

### **2.2.2 Error page parameters**

These parameters are used to configure the page displays when errors occur in Backend Web Servers.

<b>Parameter name</b>	<b>Mandatory</b>	<b>Overview</b>
SYSERR (10.0)	×	Sets the connection failure error page
SYSTOUT (10.0)	×	Sets the receive timeout error page
ERRKEY (10.0)	×	Sets the keyword substitution error page

For details on these parameters, see the following pages.

## **SYSERR** 10.0

**Overview** Sets the error page to be displayed when a Backend Web Server is down.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSERR=storage location file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Absolute paths must be used.
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_backend\_error.html.
- If this parameter is not set, the error page that was set in the SYSTEM\_DOWN\_HTTP parameter of the HTML configuration file is displayed.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set the Backend Web Server error page:  
**SYSERR=file:///opt/icewall-ssso/dfw/html/webserver\_down.html**
- 2) To set the Backend Web Server error page, status to “200,” and the status message to “System Error”:  
**SYSERR=file:///opt/icewall-ssso/dfw/html/webserver\_down.html,200, System Error**

**Remarks**

- The status code and status message are settable only when a local file is set for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).

**Host configuration file [arbitrary file name]**

---

- The status code must also be set if a status message is set.
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
- The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
- A special keyword conversion function is implemented for the error page specified by this parameter. For this reason, the error page must be in text format.
  - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”

See also

SYSTOUT

SYSTEM\_DOWN\_HTTP (HTML configuration file)

# SYSTOUT 10.0

**Overview** Sets an error page to be displayed when a timeout occurs while receiving content from a Backend Web Server.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSTOUT=**storage location file name**[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Absolute paths must be used.
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_timeout\_bkend.html.
- If this parameter is not set, the error page that was set in the SYSTEM\_TOUT\_HTTP parameter of the HTML configuration file is displayed.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set the Backend Web Server receive timeout page:  
**SYSTOUT= file:///opt/icewall-ssso/dfw/html/webserver\_timeout.html**
- 2) To set the Backend Web Server receive timeout page, status to “200,” and the status message to “System Error”:  
**SYSTOUT= file:///opt/icewall-ssso/dfw/html/webserver\_timeout.html,200,System Error**

**Remarks**

- The status code and status message are settable only when a local file is set for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).

**Host configuration file [arbitrary file name]**

---

- The status code must also be set if a status message is set.
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
- The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
- A special keyword conversion function is implemented for the error page specified by this parameter. For this reason, the error page must be in text format.
  - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”

See also

SYSERR

SYSTEM\_TOUT\_HTTP (HTML configuration file)

## ERRKEY 10.0

**Overview** Sets a substitution page for content received from a Backend Web Server when set keywords are included in that received content. This parameter is enabled only for content that is set by the CTYPE parameter.

Additional functionality of this parameter is available since version 10.0.

**Format** **ERRKEY=search keyword,storage location HTML file**

- The search keyword is case sensitive.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example** 1) To display a previously prepared error page when the received content includes the keyword "Server Error":  
**ERRKEY=Server Error,file:///opt/icewall-ssso/dfw/html/system\_error.html**

**Remarks**

- The keyword search only applies to the actual conversion content. It does not include the header.
- A keyword set with this parameter takes priority over a keyword set with the REPKEY parameter.
- For details about connections in the IPv6 format, see "8.2 IPv6 support in Forwarder" in the User's Manual. 10.0
- The "IceWall SSO SSL Option" is required to set SSL servers in this parameter.

**Host configuration file [arbitrary file name]**

---

- A specific keyword conversion function is implemented for the substitute content specified by this parameter. For this reason, the error page must be in text format.
  - \* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”

See also        CTYPE  
                  REPKEY



### **2.2.3 Basic authentication parameters**

These parameters enable the single sign on function for Backend Web Servers set up for basic authentication.

<b>Parameter name</b>	<b>Mandatory</b>	<b>Overview</b>
BASICAUTH	×	Enables/disables the sending of the basic authentication header
BA_UID	×	Sets user IDs for basic authentication
BA_PWD	×	Sets passwords for basic authentication

For details on these parameters, see the following pages.

# BASICAUTH

**Overview**                      Enables/disables Backend Web Server basic authentication.

**Format**                        **BASICAUTH=flag**

- One of the following values can be set to the flag:
  - 0 : Do not send the basic authentication header
  - 1 : Send the basic authentication header
- The default value set in the executable binary file is 0.
- The initial value set in the standard configuration file is 0.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**      1) To enable basic authentication on a Backend Web Server:  
**BASICAUTH=1**

**Remarks**

- If this parameter is not set but a connection is made to a Backend Web Server configured for basic authentication, it will send a basic authentication request to the client, but the user ID and password entered from the client browser will not be forwarded back to the server.
- This cannot be used in Reverse Proxy mode.
- The password input by the user is not sent by default when using ICP 2.0. For details, see the SEND parameter in the request control configuration file (request.acl).

**See also**                      BA\_UID  
                                    BA\_PWD  
                                    SEND (request control configuration file)

## BA\_UID

Overview	Sets the user ID used for basic authentication by extraction from user information sent from the Authentication Module.
Format	<b>BA_UID=<u>authentication DB column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The “BA_UID=DEFAULT” setting results in the use of the same user ID extracted from the Authentication Module information (login user ID).</li><li>• This parameter must be configured if the BASICAUTH parameter is set to 1.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is DEFAULT.</li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) To use the user ID that was entered at login: <b>BA_UID=DEFAULT</b></li><li>2) To use an arbitrary column in the Authentication DB: <b>BA_UID=basic_uid</b><ul style="list-style-type: none"><li>* In this case, a basic_uid column exists in the Authentication DB table.</li></ul></li></ol>
Remarks	<ul style="list-style-type: none"><li>• This cannot be used in Reverse Proxy mode.</li></ul>
See also	BASICAUTH BA_PWD

## BA\_PWD

Overview	Sets the password used for basic authentication by extraction from user information sent from the Authentication Module.
Format	<p><b>BA_PWD=<u>authentication DB column (attribute) name</u></b></p> <ul style="list-style-type: none"><li>• The “BA_PWD=DEFAULT” setting results in the use of the same password extracted from the Authentication Module information.</li><li>• This parameter must be configured if the BASICAUTH parameter is set to 1.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is DEFAULT.</li></ul>
Configuration example	<p>1) To use the password that was entered at login: <b>BA_PWD=DEFAULT</b></p> <p>2) To use an arbitrary column in the Authentication DB: <b>BA_PWD=basic_pwd</b> * In this case, a basic_pwd column exists in the Authentication DB table.</p>
Remarks	<ul style="list-style-type: none"><li>• When setting an Authentication DB password column, the password needs to be encrypted and saved to be used. If there is no basic authentication password available, please set this parameter to DEFAULT.</li><li>• This cannot be used in Reverse Proxy mode.</li></ul>
See also	BASICAUTH BA_UID

### 2.2.4 Parameters for information inheritance

These parameters are used to configure the forwarding of private user information for users currently logged into Backend Web Servers, and header information sent by browsers.

Parameter name	Mandatory	Overview
HTTPDATA	×	Sets the user information to be forwarded
HEADER	×	Sets the HTTP header to be forwarded
HEADER_FILTER (10.0)	×	Sets controls for the HTTP headers sent by IceWall
COOKIE_FILTER	×	Sets controls for HTTP-Cookie forwarding
HEADER_NAME_TID (10.0)	×	Sets the transmission header name for the transaction ID information sent to the Backend Web Server
HEADER_NAME_UID (10.0)	×	Sets the transmission header name for the user ID information sent to the Backend Web Server
HEADER_NAME_SID (10.0)	×	Sets the transmission header name for the session ID information sent to the Backend Web Server
RES_HEADER (10.0)	×	Sets controls for the response header from the Backend Web Server
UNCONV_HEADER	×	Sets the response header URL conversion control
CTRL_SPKEY (10.0)	×	Sets the specific keyword that is substituted within the Backend Web Server content

For details on these parameters, see the following pages.

# HTTPDATA

Overview	Sets the login user information from the Authentication Module data that is to be forwarded to the Backend Web Server as an HTTP header.
Format	<p><b><u>HTTPDATA=authentication DB column (attribute) name[,send header name]</u></b></p> <ul style="list-style-type: none"><li>• The Authentication DB column names refer to certain settings configured on the Authentication Module. Details are provided below.<ol style="list-style-type: none"><li>(1) Column that was set in the Authentication DB column information file</li><li>(2) Column that was set in the DBEXATTR parameter of the Authentication Module configuration file</li><li>(3) Column that was set in the REFATTR parameter of the Authentication Module configuration file</li></ol></li><li>• The Authentication DB column name is not case sensitive.</li><li>• If the send header name is omitted, the Authentication DB column name is sent unchanged as the header name.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file. However, the user ID is always sent.</li><li>• The initial value set in the standard configuration file is LOGONDATE,LOGONDATE.</li></ul>
Configuration example	<p>1) To send the Authentication DB column LLOGINDATE to a Backend Web Server using the name LAST_LOGIN_DATE: <b>HTTPDATA=LLOGINDATE,LAST_LOGIN_DATE</b></p> <p>2) To send the Authentication DB column LLOGINDATE to a Backend Web Server without changing the name: <b>HTTPDATA=LLOGINDATE</b> or <b>HTTPDATA=LLOGINDATE,LLOGINDATE</b></p>
Remarks	<ul style="list-style-type: none"><li>• The user information is forwarded to the Backend Web Server as header information. CGI is sent as an environment variable, and Servlet info is sent as a header object.</li><li>• If the data in the Authentication DB column is Null, a header without any value is sent to the Backend Web Server.</li></ul>

See also        HEADER  
                 DBEXATTR (Authentication Module configuration file)  
                 REFATTR (Authentication Module configuration file)  
                 Authentication DB column configuration file

# HEADER

**Overview**                      Enables/disables the forwarding of HTTP headers from clients to Backend Web Servers.

**Format**                      **HEADER=header name,process name[,value]**

- Make sure to change all hyphens to underscores and use only uppercase letters when configuring the header names.  
(Example: To use the User-Agent header as the header name, set USER\_AGENT)
- One of the following values can be set for the process name:
  - ADD**                      : Adds a new header specified by the header name and value.
  - ENVADD**                : Creates a new header name by adding the value from an environment variable to the header name.
  - NOTSEND**              : Deletes the header specified by the header name. The value does not need to be specified.
  - MODNAME**              : Changes the header name to the specified name.
  - MODVALUE**            : Modifies the header name value to a specified value.
- This parameter can span multiple lines.
- There is no default value in the executable binary file, but not defining this parameter will result in all client HTTP headers forwarded to the Backend Web Server.
- The initial values in the standard configuration file are as follows:  
HOST\_SOFTWARE,ENVADD,SERVER\_SOFTWARE  
IF\_MODIFIED\_SINCE,NOTSEND  
UID,NOTSEND

**Configuration example**

- 1) To add a new header:  
**HEADER=ICEWALL,ADD,SSO**
- 2) To add a new environment variable to the header:  
**HEADER=CLIENT\_REMOTE\_ADDR,ENVADD,REMOTE\_ADDR**
- 3) To change the specified header name to another name:  
**HEADER=USER\_AGENT,MODNAME,CLIENT\_BROWSER**
- 4) To change the value of the specified header:  
**HEADER=USER\_AGENT,MODVALUE,Browser**



Remarks	<ul style="list-style-type: none"><li>• Send header names and header values are converted and sent according to the following rules:<ul style="list-style-type: none"><li>(1) Convert the first character to uppercase</li><li>(2) Convert underscores “_” to hyphens “-”</li><li>(3) Convert the character following the converted hyphen to uppercase</li><li>(4) Convert all the other characters to lowercase</li></ul>(Example: USER_AGENT → User-Agent)<ul style="list-style-type: none"><li>* For information about excluded HTTP headers, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• Only data that can be acquired as an environment variable can be forwarded to Backend Web Servers controlled by Forwarder. Any other data cannot be sent to the server.</li><li>• Browser Uid headers will be combined with the IceWall SSO Uid header, which results in 2 Uids sent to the Backend Web Server. The Uid header will contain two lines (the browser Uid header, followed by the IceWall SSO header). Use the following configuration to stop the transmission of browser Uid headers. HEADER=HTTP_UID,NOTSEND</li><li>• The authorization header sent from the browser cannot be forwarded.</li><li>• Do not set any double-byte characters in the send header name.</li><li>• In order to maintain backward compatibility with versions older than 8.0 R2, a setting in the format below will also work. <b>HEADER= <u>target header name</u>,<u>send header name</u></b> For details, see the “IceWall SSO Version 8.0, 8.0.1 (8.0R1), 8.0 R2, 8.0 R3 Reference Manual.”</li></ul>
See also	HTTPDATA

## HEADER\_FILTER ⑩.0

**Overview** Turns off the normal system function of sending IceWall session-related information to Backend Web Servers.

Additional functionality of this parameter is available since version 10.0.

**Format** **HEADER\_FILTER=**header identifier

- The following values can be set for the header identifier:
  - UID : Do not send user ID
  - SESSION : Do not send session ID
  - COOKIE : Do not send cookie
  - TRANSID : Do not send the transaction ID ⑩.0
- When “COOKIE” is specified for the header identifier, cookies sent by a client are no longer forwarded to Backend Web Servers.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)
- The system is not guaranteed to work as expected if the value for this parameter is out of range.

**Configuration example**

- 1) To prevent the sending of user IDs only to Backend Web Servers:  
**HEADER\_FILTER=UID**
- 2) To prevent the sending of user IDs and session IDs to Backend Web Servers:  
**HEADER\_FILTER=UID**  
**HEADER\_FILTER=SESSION**  
\* The sequence in which they are configured does not matter.
- 3) To prevent the sending of cookies only to Backend Web Servers:  
**HEADER\_FILTER=COOKIE**

**Remarks**

- When this parameter is not specified, user IDs, session IDs, and cookies are always sent to the Backend Web Server.
- The transaction ID can only be controlled when the TRANSID parameter is set to 1.

See also

- COOKIE\_FILTER
- TRANSID (Forwarder configuration file)
- HEADER\_NAME\_UID
- HEADER\_NAME\_SID

## COOKIE\_FILTER

Overview	Creates a filter to prevent certain types of client cookies from being forwarded to Backend Web Servers.
Format	<p><b>COOKIE_FILTER=<u>cookie name</u></b></p> <ul style="list-style-type: none"><li>• The cookie names used to configure this parameter are derived from the name portion of the “Name=Value” character strings.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>When the following cookies are sent from the browser: DATA=100; CORP=HP; FLAG=OFF</p> <p>1) To prevent the sending of CORP cookies only to Backend Web Servers: <b>COOKIE_FILTER=CORP</b></p> <p>2) To prevent the sending of DATA and FLAG cookies to Backend Web Servers: <b>COOKIE_FILTER=DATA</b> <b>COOKIE_FILTER=FLAG</b> * The sequence in which they are configured does not matter.</p>
Remarks	<ul style="list-style-type: none"><li>• If the IceWall authentication cookie (initial value of IW_INFO) is set, the authentication cookie is not sent to a Backend Web Server.</li><li>• If “COOKIE” is specified for the HEADER_FILTER parameter, this parameter setting is disabled.</li></ul>
See also	<p>HEADER_FILTER UNCONV_HEADER</p>

## HEADER\_NAME\_TID 10.0

Overview	<p>Sets the transmission header name for the transaction ID information sent to the Backend Web Server.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>HEADER_NAME_TID=<u>header name</u></b></p> <ul style="list-style-type: none"><li>• For the header name, set the header name used when sending transaction ID information to the Backend Web Server.</li><li>• The header name must contain at least one byte, with a maximum length of 64 bytes.</li><li>• The characters used in the header name are based on general HTTP header specifications.</li><li>• The default value set in the executable binary file is X-iw-transid.</li><li>• The initial value set in the standard configuration file is X-iw-transid.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To change the header name for the transaction ID information sent to the Backend Web Server to Icewall-transactionid:</p> <p><b>TRANSID=1</b> <b>HEADER_NAME_TID=Icewall-transactionid</b></p>
Remarks	<ul style="list-style-type: none"><li>• The system is not guaranteed to work as expected when using characters that cannot be used as an HTTP header in the header name.</li><li>• The character string set for the header name is sent to the Backend Web Server unmodified as an HTTP header.</li><li>• This parameter is ineffective when the TRANSID parameter is set to 0.</li><li>• This parameter is ineffective when the HEADER_FILTER parameter is set to not send the transaction ID.</li></ul>
See also	<p>TRANSID (Forwarder configuration file) HEADER_FILTER</p>

## HEADER\_NAME\_UID 10.0

Overview	<p>Sets the transmission header name for the user ID information sent to the Backend Web Server.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>HEADER_NAME_UID=<u>header name</u></b></p> <ul style="list-style-type: none"><li>• For the header name, set the header name used when sending user ID information to the Backend Web Server.</li><li>• The header name must contain at least one byte, with a maximum length of 64 bytes.</li><li>• The characters used in the header name are based on general HTTP header specifications.</li><li>• The default value set in the executable binary file is Uid.</li><li>• The initial value set in the standard configuration file is Uid.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To change the header name for the user ID information sent to the Backend Web Server to Iw-Uid:</p> <p><b>HEADER_NAME_UID=Iw-Uid</b></p>
Remarks	<ul style="list-style-type: none"><li>• The system is not guaranteed to work as expected when using characters that cannot be used as an HTTP header in the header name.</li><li>• The character string set for the header name is sent to the Backend Web Server unmodified as an HTTP header.</li><li>• This parameter is ineffective when the HEADER_FILTER parameter is set to not send the user ID.</li></ul>
See also	<p>HEADER_NAME_SID</p> <p>HEADER_FILTER</p>

## HEADER\_NAME\_SID 10.0

**Overview** Sets the transmission header name for the session ID information sent to the Backend Web Server.

This parameter is available since version 10.0.

**Format** **HEADER\_NAME\_SID=header name**

- For the header name, set the header name used when sending user ID information to the Backend Web Server.
- The header name must contain at least one byte, with a maximum length of 64 bytes.
- The characters used in the header name are based on general HTTP header specifications.
- The default value set in the executable binary file is Session.
- The initial value set in the standard configuration file is Session.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

**Configuration example** 1) To change the header name for the session ID information sent to the Backend Web Server to Iw-Session:  
**HEADER\_NAME\_UID=Iw-Uid**

**Remarks**

- The system is not guaranteed to work as expected when using characters that cannot be used as an HTTP header in the header name.
- The character string set for the header name is sent to the Backend Web Server unmodified as an HTTP header.
- This parameter is ineffective when the HEADER\_FILTER parameter is set to not send the user ID.

**See also** HEADER\_NAME\_UID  
HEADER\_FILTER

## RES\_HEADER 10.0

**Overview** Sets the control method for headers that are included in responses from Backend Web Servers.

Some specifications of this parameter have been modified since version 10.0.

**Format** **RES\_HEADER=header name,process name[,value]**

- One of the following values can be set for the process name:
  - ADD : Adds a header having the specified value
  - NOTSEND : Deletes the header (value does not need to be specified)
  - MODNAME : Modifies the header name to a name set by the value
  - MODVALUE : Modifies the header value to a name set by the value
- Make sure to change all hyphens to underscores and use only uppercase letters when configuring the header names.  
Example: Test-Header → TEST\_HEADER
- Characters set to a value by MODNAME are converted in the same way as the header name.
- Characters that are configured by a value in MODVALUE are kept unchanged as header values.
- Invalid process names will be ignored.
- The status line, Content-Type, and Content-Length headers cannot be controlled by this parameter.
- If the process name is ADD, it is added even if a header with the same name already exists. (After it is added, there are two headers with the same name.)
- Setting this parameter will activate header control for all headers of any content type.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial values set in the standard configuration file are “Pragma,NOTSEND”, “Pragma,ADD,no-cache”, “Cache-Control,NOTSEND”, and “Cache-Control,ADD,no-cache”. 10.0

**Configuration example**

- 1) To add “Sample-Header: xxxxx” to the response header:  
**RES\_HEADER=SAMPLE\_HEADER,ADD,xxxxx**
- 2) To delete “Sample-Header: xxxxx” from the response header:  
**RES\_HEADER=SAMPLE\_HEADER,NOTSEND**



- 3) To change the header name “Sample-Header: xxxxx” to “Modified-Header”:

**RES\_HEADER=SAMPLE\_HEADER,MODNAME,MODIFIED\_HEADER**

- 4) To change the header value of “Sample-Header: xxxxx” to “yyyyy”:

**RES\_HEADER=SAMPLE\_HEADER,MODVALUE,yyyyy**

#### Remarks

- Header add and name changes are converted according to the following rules before transmission to the client.
  - (1) Convert the first character to uppercase
  - (2) Convert underscores “\_” to hyphens “-”
  - (3) Convert the character following the converted hyphen to uppercase
  - (4) Convert all other characters to lowercase
  - (Example: TEST\_HEADER → Test-Header)
- Header comparisons are not case-sensitive.
- The parameter performs the response header control process before the keyword conversion function (REPKEY).
- As with previous versions, use the REPKEY parameter to change domain attributes for Set-cookie headers because some values cannot be changed with this parameter.
- Changing headers that effect browser operations such as Etag and Content-Encoding may result in operational errors.
- Configuring this parameter with many lines may cause a reduction in performance.
- This parameter can also be used to retrieve the remote template HTML.
- Header names cannot be dynamically generated and specified.

#### See also

HEADER  
REPKEY

## UNCONV\_HEADER

**Overview**                Sets URL conversion control for Location and Set-cookie headers received from Backend Web Servers.

**Format**                **UNCONV\_HEADER=header name[,header name][,...]**

- Specified header names will avoid response header URL conversion.
- The header names that currently can be set are shown below.  
LOCATION  
SET-COOKIE
- The header name must be configured using uppercase letters.
- Ineffective header names that can not be used will be ignored.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)

**Configuration example**    1) To cancel URL conversion of the Location and Set-cookie in response headers:  
**UNCONV\_HEADER=LOCATION,SET-COOKIE**

2) To cancel URL conversion of the Location in response headers:  
**UNCONV\_HEADER=LOCATION**

**Remarks**                None

**See also**                None

## CTRL\_SPKEY 10.0

**Overview**                Sets specific substitution keyword names for each Backend Web Server.

Additional functionality of this parameter is available since version 10.0.

**Format**                **CTRL\_SPKEY=specific keyword name[,specific keyword name][,...]**

- One of the following values can be set for the specific keyword name.
  - \$DFW                    : Path to Forwarder
  - \$REQUEST\_URL        : Requested path
  - \$HIDEURL             : Connection path after login
  - \$ALIAS                : Alias of requested URL
  - \$USER\_ID             : User ID of login user
  - \$PASSWORD           : Password entered at login
  - \$IW\_INFO             : Session ID
  - \$KEY\_LOGIN           : Login identification key
  - \$KEY\_LOGOUT          : Logout identification key
  - \$KEY\_PWDCHG         : Password change identification key
  - \$PWDCHG\_URL         : URL for viewing password change screen
  - \$LOGOUT\_URL          : URL for viewing logout screen
  - \$TOPPAGE\_URL        : System top page URL 10.0
  - \$PWDHIDEURL         : Return URL after password change  
(Only when linking with Agent) 10.0
  - \$IWTID                : Transaction ID 10.0
- Any content containing data other than the specific keyword names above are ignored.
- If this parameter is not set, all specific keywords are substituted (backward compatibility).
- Configure this parameter with no value to prevent all substitutions.
- Specific keywords set for no substitution remain unchanged in the content.
- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is  
\$DFW,\$REQUEST\_URL,\$HIDEURL,\$ALIAS,\$IW\_INFO,  
\$KEY\_LOGIN,\$KEY\_LOGOUT,\$KEY\_PWDCHG,\$PWDCHG\_URL,  
\$LOGOUT\_URL. 10.0

**Configuration example**        1) To permit conversion only of \$USER\_ID and \$ALIAS in the Backend Web Server content:  
**CTRL\_SPKEY=\$USER\_ID,\$ALIAS**

---

Host configuration file [arbitrary file name]

---

- 2) To disable all specific keyword conversion of Backend Web Server content:

**CTRL\_SPKEY=**

Remarks

- This parameter only applies to Backend Web Server content; it will not have any effect on template HTML output by Forwarder.
- Care must be taken when configuring this parameter, as it directly manipulates Backend Web Server content.
- It is recommended to disable the conversion of any keywords not necessary for web applications and content to prevent unnecessary disclosure of information.

See also

None

### 2.2.5 Parameters for handling cross site scripting

These parameters are used to set up filters that help prevent cross site scripting attacks contained in Backend Web Server POST data, content, or QueryString data. Please note that when the configuration parameters below are enabled, a large amount of memory may be consumed.

Parameter name	Mandatory	Overview
GETFILTER	×	Sets a filter for GET requests
GETEXCEPTION	×	Sets an exception filter for GET requests
GETFILTERERR 10.0	×	Sets an error page for the GET filter
GETFILTER_LOG_FLG	×	Sets the flag controlling output error log information when filtering is performed by QueryString in the request sent to the Backend Web Server
POSTFILTER	×	Sets a filter for POST requests
POSTEXCEPTION	×	Sets an exception filter for POST requests
POSTFILTERERR 10.0	×	Sets an error page for the POST filter
POSTFILTER_LOG_FLG	×	Sets the flag controlling output error log information when filtering is performed by POST data in the request sent to the Backend Web Server
HTMLFILTER	×	Sets tag filters for content
HTMLFILTERERR 10.0	×	Sets an error page for the content tag filter
SVRFILTER	×	Sets a host filter for content
SVREXCEPTION	×	Sets an exception host filter for content
SVRFILTERERR 10.0	×	Sets an error page for the content host filter
SVRFILTERSTR	×	Sets a substitute string for the content host filter

For details on these parameters, see the following pages.

# GETFILTER

Overview	Sets cross site script filtering of QueryString data from requests to Backend Web Servers.
Format	<b>GETFILTER=<u>filtered tag name</u></b> <ul style="list-style-type: none"><li>• The tag name is not case sensitive.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) To perform filtering on QueryString SCRIPT tags only: <b>GETFILTER=SCRIPT</b></li><li>2) To perform filtering on QueryString SCRIPT and EMBED tags: <b>GETFILTER=SCRIPT</b> <b>GETFILTER=EMBED</b></li></ol>
Remarks	<ul style="list-style-type: none"><li>• The filtered tags are converted as follows: Before conversion : &lt;SCRIPT LANGUAGE="JavaScript"&gt; After conversion : &amp;lt;SCRIPT LANGUAGE="JavaScript"&gt; * The actual part of the "&lt;" and "&gt;" characters are URL encoded.</li><li>• This parameter filters the entire QueryString. To exclude sections of the data, use the GETEXCEPTION parameter.</li></ul>
See also	GETEXCEPTION GETFILTERERR

# GETEXCEPTION

**Overview** Sets exceptions to be excluded from cross site filtering of the QueryString data from requests sent to Backend Web Servers.

**Format** **GETEXCEPTION=excluded Name of name=value pairs**

- The exception is not case sensitive.
- Encode exceptions that use special characters as text strings.
- This parameter can span multiple lines.
- This parameter is effective only when the GETFILTER parameter is set.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)

**Configuration example** The following configuration examples use this example QueryString data.

Name1=<SCRIPT>&Name2=<EMBED>&Name3=<SCRIPT>

- 1) To exclude Name1 from a SCRIPT tag filter:

**GETFILTER=SCRIPT**  
**GETEXCEPTION=Name1**

- 2) To exclude Name1 and Name3 from a SCRIPT tag filter:

**GETFILTER=SCRIPT**  
**GETEXCEPTION=Name1**  
**GETEXCEPTION=Name3**

The following configuration example uses this example QueryString data. (The pound sign is encoded by "%23.")

NAME%231=<SCRIPT>&NAME%232=<SCRIPT>

- 3) To exclude NAME#1 from a SCRIPT tag filter:

**GETFILTER=SCRIPT**  
**GETEXCEPTION=NAME%231**

**Remarks** None

**See also** GETFILTER  
GETFILTERERR

## GETFILTERERR (10.0)

**Overview** Determines the behavior for handling tag matches to the configured GETFILTER parameter, which searches QueryString data from requests to Backend Web Servers. The possible options are to filter the tag or display an error page.

Additional functionality of this parameter is available since version 10.0.

**Format** **GETFILTERERR=flag**

- One of the following values can be set to the flag:
    - 0 : Perform filtering
    - 1 : Display an error page
    - 2 : Only output the error log without displaying a filtering error page
- (10.0)
- The error page displayed is configured by the FILTER\_GET parameter used in the HTML configuration file.
  - This parameter is effective only when the GETFILTER parameter is set.
  - The default value set in the executable binary file is 0.
  - The initial value is not set in the standard configuration file.  
(commented out)
  - The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
  - If the value for this parameter is out of range, the default value is used.

**Configuration example** The following configuration examples use this example QueryString data.

DATA1=<SCRIPT>&DATA2<EMBED>

- 1) To output an error page when SCRIPT tags are found:

**GETFILTER=SCRIPT**  
**GETFILTERERR=1**

- 2) To output an error page when SCRIPT tags are found, with the exception of DATA1:

**GETFILTER=SCRIPT**  
**GETEXCEPTION=DATA1**  
**GETFILTERERR=1**



In this example, an error page would not be displayed as DATA1 has been configured as an exception.

- 3) To output an error page when SCRIPT tags are found, with the exception of DATA2:

**GETFILTER=SCRIPT**  
**GETEXCEPTION=DATA2**  
**GETFILTERERR=1**

In this example, an error page would be displayed.

- 4) To output the error log only when SCRIPT tags are found (10.0)

**GETFILTER=SCRIPT**  
**GETFILTERERR=2**

#### Remarks

- Since the error log output when the filtering target is found is at a warning level, an error log is not output when ELEVEL is 1 or lower.
- Flag setting 2 is for verifying the configuration of the filter function. Since filtering is not performed, use this setting for testing when installing the system. If a filtering target is found, the test error log output is shown below. (10.0)

Warning: GET Filter TEST. Host:[www.host.com:80] Path:[/index.cgi]  
QUERY\_STRING:[aaa=<script>] Tag:[<script] [EI75704-16023]

The Backend Web Server host, path, QueryString, and filtering target tag are output.

- QUERY\_STRING content in the error log is masked if the GETFILTER\_LOG\_FLG parameter is set to 1.

#### See also

GETFILTER  
GETEXCEPTION  
GETFILTER\_LOG\_FLG  
FILTER\_GET (HTML configuration file)

## GETFILTER\_LOG\_FLG

Overview	Sets the flag controlling output error log information when filtering is performed by QueryString in the request sent to the Backend Web Server.
Format	<p><b>GETFILTER_LOG_FLG=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Do not mask QueryString output in the error log.</li><li>1 : Mask QueryString output in the error log.</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To mask QueryString output in the error log when filtering SCRIPT tags containing a QueryString:</p> <p><b>GETFILTER=SCRIPT</b> <b>GETFILTER_LOG_FLG=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when the GETFILTER parameter is set.</li><li>• If QueryString is masked, it is output after being changed to “*****”.</li><li>• This parameter can also be set in the Forwarder configuration file. In this case, the same setting is made for all Backend Web Servers.</li></ul>
See also	<p>GETFILTER GETFILTERERR</p>

# POSTFILTER

Overview	Sets cross site script filtering of POST data from requests to Backend Web Servers.
Format	<b>POSTFILTER=<u>filtered tag name</u></b> <ul style="list-style-type: none"><li>• The tag name is not case sensitive.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To perform filtering on POST SCRIPT tags only: <b>POSTFILTER=SCRIPT</b></p> <p>2) To perform filtering on POST SCRIPT and EMBED tags: <b>POSTFILTER=SCRIPT</b> <b>POSTFILTER=EMBED</b></p>
Remarks	<ul style="list-style-type: none"><li>• The filtered tags are converted as follows: Before conversion : &lt;SCRIPT LANGUAGE="JavaScript"&gt; After conversion : &amp;lt;SCRIPT LANGUAGE="JavaScript"&gt; * The actual part of the "&lt;" and "&gt;" characters are URL encoded.</li><li>• This parameter filters the entire POST data. To exclude sections of the data, use the POSTEXCEPTION parameter.</li><li>• In Backend Web Servers that perform file uploading, this function cannot be used because the uploaded file can potentially be corrupted.</li><li>• When performing filtering with this parameter, memory use will increase since memory for the filtering process will be allocated.</li></ul>
See also	POSTEXCEPTION POSTFILTERERR

# POSTEXCEPTION

**Overview** Sets exceptions to be excluded from cross site filtering of the POST data from requests sent to Backend Web Servers.

**Format** **POSTEXCEPTION=excluded Name of name=value pairs**

- The exception is not case sensitive.
- Encode exceptions that use special characters as text strings.
- This parameter can span multiple lines.
- This parameter is effective only when the POSTFILTER parameter is set.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)

**Configuration example** The following configuration examples use this example POST data.  
Name1=<SCRIPT>&Name2=<EMBED>&Name3=<SCRIPT>

1) To exclude Name1 from a SCRIPT tag filter:

**POSTFILTER=SCRIPT**  
**POSTEXCEPTION=Name1**

2) To exclude Name1 and Name3 from a SCRIPT tag filter:

**POSTFILTER=SCRIPT**  
**POSTEXCEPTION=Name1**  
**POSTEXCEPTION=Name3**

The following configuration example uses this example QueryString data. (The pound sign is encoded by “%23.”)

NAME%231=<SCRIPT>&NAME%232=<SCRIPT>

3) To exclude NAME#1 from a SCRIPT tag filter:

**POSTFILTER=SCRIPT**  
**POSTEXCEPTION=NAME%231**

**Remarks** None

**See also** POSTFILTER  
POSTFILTERERR

## POSTFILTERERR 10.0

**Overview** Determines the behavior for handling tag matches to the configured POSTFILTER parameter, which searches POST data from requests to Backend Web Servers. The possible options are to filter the tag or display an error page.

Additional functionality of this parameter is available since version 10.0.

**Format** **POSTFILTERERR=flag**

- One of the following values can be set to the flag:
  - 0 : Perform filtering
  - 1 : Display an error page
  - 2 : Only output the error log without displaying a filtering error page
- 10.0
- The error page displayed is configured by the FILTER\_POST parameter used in the HTML configuration file.
- This parameter is effective only when the POSTFILTER parameter is set.
- The default value set in the executable binary file is 0.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** The following configuration examples use this example POST data.  
DATA1=<SCRIPT>&DATA2<EMBED>

- 1) To output an error page when SCRIPT tags are found:  
**POSTFILTER=SCRIPT**  
**POSTFILTERERR=1**
- 2) To output an error page when SCRIPT tags are found, with the exception of DATA1:  
**POSTFILTER=SCRIPT**  
**POSTEXCEPTION=DATA1**  
**POSTFILTERERR=1**

---

**Host configuration file [arbitrary file name]**


---

In this example, an error page would not be displayed as DATA1 has been configured as an exception.

- 3) To output an error page when SCRIPT tags are found, with the exception of DATA2:

**POSTFILTER=SCRIPT**  
**POSTEXCEPTION=DATA2**  
**POSTFILTERERR=1**

In this example, an error page would be displayed.

- 4) To output the error log only when SCRIPT tags are found (10.0)

**POSTFILTER=SCRIPT**  
**POSTFILTERERR=2**

**Remarks**

- Since the error log output when the filtering target is found is at a warning level, an error log is not output when ELEVEL is 1 or lower.
- Flag setting 2 is for verifying the configuration of the filter function. Since filtering is not performed, use this setting for testing when installing the system. If a filtering target is found, the test error log output is shown below. (10.0)  
Warning: POST Filter TEST. Host:[www.host.com:80] Path:[/index.cgi]  
POSTDATA:[aaa=<script>] Tag:[<script] [EI75705-16024]  
  
The Backend Web Server host, path, POSTDATA, and filtering target tag are output.
- POSTDATA content in the error log is masked if the POSTFILTER\_LOG\_FLG parameter is set to 1.

**See also**

POSTFILTER  
POSTEXCEPTION  
POSTFILTER\_LOG\_FLG  
FILTER\_POST (HTML configuration file)

# POSTFILTER\_LOG\_FLG

Overview	Sets the flag controlling output error log information when filtering is performed by POST data in the request sent to the Backend Web Server.
Format	<p><b>POSTFILTER_LOG_FLG=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Do not mask POST data output in the error log.</li><li>1 : Mask POST data output in the error log.</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To mask POST data output in the error log when filtering SCRIPT tags contained in POST data:</p> <p><b>POSTFILTER=SCRIPT</b> <b>POSTFILTER_LOG_FLG=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when the POSTFILTER parameter is set.</li><li>• If POST data is masked, it is output after being changed to “*****”.</li><li>• This parameter can also be set in the Forwarder configuration file. In this case, the same setting is made for all Backend Web Servers.</li></ul>
See also	<p>POSTFILTER POSTFILTERERR</p>

# HTMLFILTER

**Overview**                Sets cross site script filtering of tag attribute values, which are set with the URLKEY parameter, from content received from Backend Web Servers.

**Format**                **HTMLFILTER=filtered tag name**

- The tag name is not case sensitive.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)

**Configuration example**        Here is an example output of received content:  
                                     <A HREF="www.hp.com<SCRIPT>">www.hp.com</A>

1) To convert the URL A tag's HREF attribute, and filter links that contain SCRIPT tags:  
**URLKEY=A,HREF**  
**HTMLFILTER=SCRIPT**

**Remarks**                • The filtered tags are converted as follows:  
                                     Before conversion : <A HREF="www.hp.com<SCRIPT>">  
                                     After conversion    : <A HREF="www.hp.com&lt;SCRIPT>">

**See also**                HTMLFILTERERR



## HTMLFILTERERR (10.0)

**Overview** Determines the behavior for handling tag matches to the configured HTMLFILTER parameter, which searches tag attribute values (URLKEY parameter) from received Backend Web Server content. The possible options are to filter the tag or display an error page.

Additional functionality of this parameter is available since version 10.0.

**Format** **HTMLFILTERERR=flag**

- One of the following values can be set to the flag:
  - 0 : Perform filtering
  - 1 : Display an error page
  - 2 : Only output the error log without displaying a filtering error page (10.0)
- The error page displayed is configured by the FILTER\_HTML parameter used in the HTML configuration file.
- This parameter is effective only when the HTMLFILTER parameter is set.
- The default value set in the executable binary file is 0.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**

Here is an example output of received content:

```
<A HREF="www.hp.com<SCRIPT>">www.hp.com</A>
```

- 1) To output an error page only when SCRIPT tags are found within tag attribute values which are subject to URL conversion:

```
HTMLFILTER=SCRIPT
HTMLFILTERERR=1
```

- 2) To output the error log only when SCRIPT tags are found within tag attribute values which are subject to URL conversion: (10.0)

```
HTMLFILTER=SCRIPT
HTMLFILTERERR=2
```

---

Host configuration file [arbitrary file name]

---

Remarks

- Since the error log output when the filtering target is found is at a warning level, an error log is not output when ELEVEL is 1 or lower.
- Flag setting 2 is for verifying the configuration of the filter function. Since filtering is not performed, use this setting for testing when installing the system. If a filtering target is found, the test error log output is shown below. ⑩⑩

Warning: HTML Filter TEST. Host:[www.host.com:80] Path: [/index.cgi] Tag:[<script] [EI75706-16022]  
The Backend Web Server host, path, and filtering target tag are output.

See also

HTMLFILTER  
FILTER\_HTML (HTML configuration file)

# SVRFILTER

**Overview** Determines the behavior for handling host name filtering for host names (found in Backend Web Server content) that are not defined in the HOST and SHOST parameters.

**Format** **SVRFILTER=flag**

- One of the following values can be set to the flag:
  - 0 : Do not filter the host name
  - 1 : Filter only host names that are included in the attribute values configured with the URLKEY parameter
  - 2 : Perform host name filtering for all content
- The default value set in the executable binary file is 0.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To filter undefined hosts included in attribute values of tags which are subject to URL conversion:  
**SVRFILTER=1**

**Remarks** • Setting this parameter to 1 may cause errors in JavaScript filtering as the “<” and “>” characters used to identify HTML tags are also used in the script code for other functions.

Example: URLKEY=FORM,ACTION is set.

```
<SCRIPT LANGUAGE="JavaScript">
```

```
if (hour <now) {  
    document.write("AM");  
}
```

```
</SCRIPT>
```

```
<FORM METHOD="POST" ACTION="/cgi-bin/sample.cgi">
```

In this example, the “if (hour <now) {}” section will be identified as part of a tag, which causes an error in detecting the <FORM> tag. In these types of cases, set the flag to 2.

**Host configuration file [arbitrary file name]**

---

See also           SVREXCEPTION  
                    SVRFILTERERR  
                    SVRFILTERSTR

# SVREXCEPTION

**Overview** Sets exceptions to be excluded from host filtering of Backend Web Server content.

**Format** **SVREXCEPTION=excluded host name**

- The host name is not case sensitive.
- The protocol is also specified in the host name.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)

**Configuration example**

1) To exclude http://www.hp.com from undefined hosts included in attribute values of tags that are subject to URL conversion:  
**SVRFILTER=1**  
**SVREXCEPTION=http://www.hp.com**

2) To exclude http://www.hp.com:81 from undefined hosts that are included in content:  
**SVRFILTER=2**  
**SVREXCEPTION=http://www.hp.com:81**

**Remarks**

- The port number can be omitted if the host to be excluded is running using the default port number.

**See also**

SVRFILTER  
SVRFILTERERR  
SVRFILTERSTR

## SVRFILTERERR (10.0)

**Overview** Determines the behavior for Backend Web Server content host filtering of hosts not configured in the HOST and SHOST parameters. The possible options are to filter the tag or display an error page.

Additional functionality of this parameter is available since version 10.0.

### Format

**SVRFILTERERR=flag**

- One of the following values can be set to the flag:
  - 0 : Perform filtering
  - 1 : Display an error page
  - 2 : Only output the error log without displaying a filtering error page
- (10.0)
- This parameter is effective only when the SVRFILTER parameter is set.
- The default value set in the executable binary file is 0.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

### Configuration example

The following configuration examples use this example content output.

```
<A HREF="http://www.hp.com">Hewlett-Packard</A>
```

- 1) To display an error page when undefined servers are included in attribute values of tags that are subject to URL conversion:

```
URLKEY=A,HREF
SVRFILTER=1
SVRFILTERERR=1
```

The following configuration examples use this example content output.

```
<A HREF="http://www.hp.com">www.hp.co.jp</A>
```

- 2) To display an error page when undefined servers are included in content:

```
HOST=XXX=www.hp.com
SVRFILTER=2
SVRFILTERERR=1
```

- 3) To output the error log when undefined servers are included in attribute values of tags that are subject to URL conversion: (10.0)

**URLKEY=A,HREF**  
**SVRFILTER=1**  
**SVRFILTERERR=2**

#### Remarks

- See the SVRFILTERSTR parameter for information about filtering unset hosts.
- Since the error log output when the filtering target is found is at a warning level, an error log is not output when ELEVEL is 1 or lower.
- Flag setting 2 is for verifying the configuration of the filter function. Since filtering is not performed, use this setting for testing when installing the system. If a filtering target is found, the test error log output is shown below. (10.0)

Warning: SVR Filter TEST. Host:[www.host.com:80] Path:[/index.cgi]  
FilterHost:[http://www.filter.com] [EI10409-16021]

The Backend Web Server host, path, and filtering target host are output.

#### See also

SVRFILTER  
SVREXCEPTION  
SVRFILTERSTR  
FILTER\_SVR (HTML configuration file)

# SVRFILTERSTR

Overview	Defines a replacement text string used to change host names, contained in Backend Web Server content, that are configured in the HOST and SHOST parameters, but do not exist.
Format	<p><b>SVRFILTERSTR=<u>character string after substitution</u></b></p> <ul style="list-style-type: none"><li>• This parameter is effective only when the SVRFILTER parameter is set.</li><li>• The default value set in the executable binary file is "Bad Hostname".</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>The following configuration examples use this example content output.</p> <pre>&lt;A HREF="http://www.hp.co.jp"&gt;http://www.hp.co.jp&lt;/A&gt;</pre> <p>1) To perform filtering when undefined servers are included in attribute values of tags that are subject to URL conversion:</p> <pre>URLKEY=A,HREF SVRFILTER=1 SVRFILTERERR=0 SVRFILTERSTR=Bad Hostname</pre> <p>The content in this case is changed as follows:</p> <pre>&lt;A HREF="Bad Hostname"&gt; http://www.hp.co.jp&lt;/A&gt;</pre> <p>2) To perform filtering when undefined servers are included in content:</p> <pre>SVRFILTER=2 SVRFILTERERR=0 SVRFILTERSTR=Bad Hostname</pre> <p>The content in this case is changed as follows:</p> <pre>&lt;A HREF="Bad Hostname"&gt;Bad Hostname&lt;/A&gt;</pre>
Remarks	<ul style="list-style-type: none"><li>• Filtering for undefined servers in content is performed only when an absolute path is specified (starting with http:// or https://).</li></ul>
See also	SVRFILTER SVREXCEPTION



SVRFILTERERR

### 2.2.6 System tuning configuration parameters

These parameters are used to configure Backend Web Server system parameter settings, such as response or timeouts.

Parameter name	Mandatory	Overview
RETRYCNTW	×	Sets the number of connect retries
RETRYTMW <small>(10.0)</small>	×	Sets the connect retry interval
TIMEOUT	×	Sets receive timeouts
CLOSETIME <small>(10.0)</small>	×	Sets disconnection waiting timeouts
BUFFER	×	Sets the transfer method for content
LASTMOD_HEADER	×	Sets transfer of the Last-Modified header
CENCODE	×	Sets HTTP compression transfer
URL_SCOLON	×	Sets the encoding method for semicolons
FO_SEND	×	Sets the failover operation when a send error occurs during Backend Web Server communication
FO_RECV	×	Sets the failover operation when a receive error occurs during Backend Web Server communication
FO_NODATA	×	Sets the failover operation when a receive size of 0 occurs during Backend Web Server communication
RECV_ZERO_FLG	×	Sets up the operation when the receive data size from the Backend Web Server is 0 bytes

For details on these parameters, see the following pages.

# RETRYCNTW

**Overview** Sets the number of retries when an error occurs connecting to a Backend Web Server.

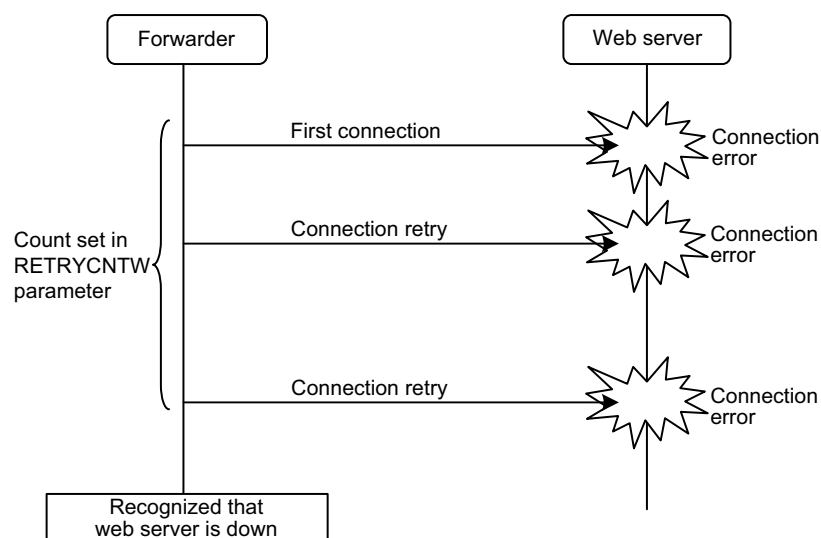
**Format** **RETRYCNTW=number of retries**

- The default value set in the executable binary file is 10.
- The initial value set in the standard configuration file is 10.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

**Configuration example** 1) To set five as the retry count when attempting to connect to a Backend Web Server results in error:  
**RETRYCNTW=5**

**Remarks**

- The first connection attempt is included in the retry count.
- This retry counter only applies when actively attempting a connection with a Backend Web Server. It does not apply to web server responses.



**See also** RETRYTMW

# RETRYTMW <sup>(10.0)</sup>

**Overview** Sets the retry interval when connection to the Backend Web Server fails.

Some specifications of this parameter have been modified since version 10.0.

**Format** **RETRYTMW=time value (seconds)**

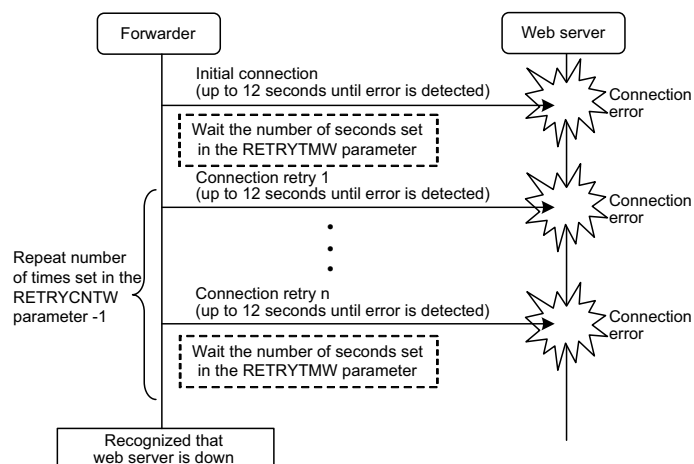
- The unit for setting the timer value is seconds.
- The default value set in the executable binary file is 3 seconds.
- The initial value set in the standard configuration file is 3 seconds.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

**Configuration example** 1) To retry after five seconds when an error occurs while attempting to connect to a Backend Web Server:  
**RETRYTMW=5**

**Remarks**

- The detection of a connection error to the Backend Web Server can take up to 12 seconds if no web server is found. If a web server is detected, but the port is down, the error is detected virtually instantly. The actual time for the error detection to occur is dependant on the network status and cannot be configured.
- The total time to determine an offline Backend Web Server is calculated by: “(RETRYCNTW parameter setting value × maximum of 12 seconds) + (RETRYCNTW parameter setting value × (RETRYTMW parameter setting value - 1).” <sup>(10.0)</sup>  
Example: RETRYCNTW=5,  
RETRYTMW=2  
In this case, the total time to determine an offline web server is calculated by:  
 $(5 \times 12) + (2 \times (5 - 1)) = 68$  seconds.

The value calculated with the formula above is the maximum value. Use caution as Forwarder may not always wait until the calculated value depending on factors such as the network settings and environment.



See also

RETRYCNTW

# TIMEOUT

**Overview** Sets the timeout value when waiting for a response from a connected Backend Web Server. TIMEOUT also operates as a receive interval timer.

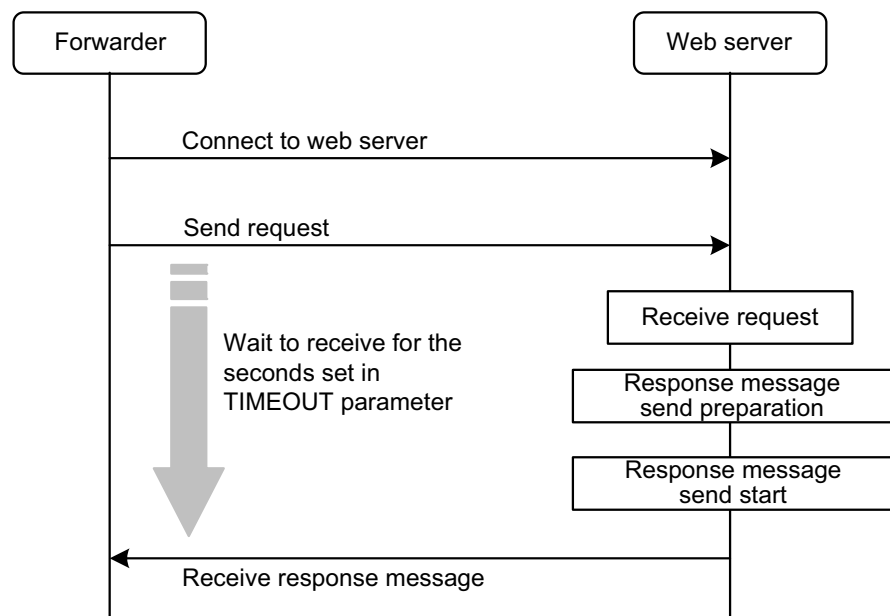
**Format** **TIMEOUT=**timeout value (seconds)

- The unit for setting the timeout value is seconds.
- The default value set in the executable binary file is 180 seconds.
- The initial value set in the standard configuration file is 180 seconds.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

**Configuration example** 1) To set the Backend Web Server response timeout to one minute:  
**TIMEOUT=60**

**Remarks**

- Once connectivity to the Backend Web Server has been established, this parameter specifies the timeout counter for receiving a response message after a request has been sent. Please note that it does not specify the timeout for connecting to the web server.



- This parameter also functions as the timeout counter when the response message is disrupted.
- The Backend Web Server timeout error page will be displayed when a timeout occurs. However, if the SYSTOUT parameter is set, the page set by SYSTOUT is displayed.

See also

CLOSETIME

SYSTOUT

SYSTEM\_TOUT\_HTTP (HTML configuration file)

## CLOSETIME 10.0

**Overview** Sets the wait time until Forwarder disconnects a connection that the Backend Web Server failed to disconnect. CLOSETIME also operates as a receive interval timer.

Some specifications of this parameter have been modified since version 10.0.

**Format** CLOSETIME=timeout value (seconds)

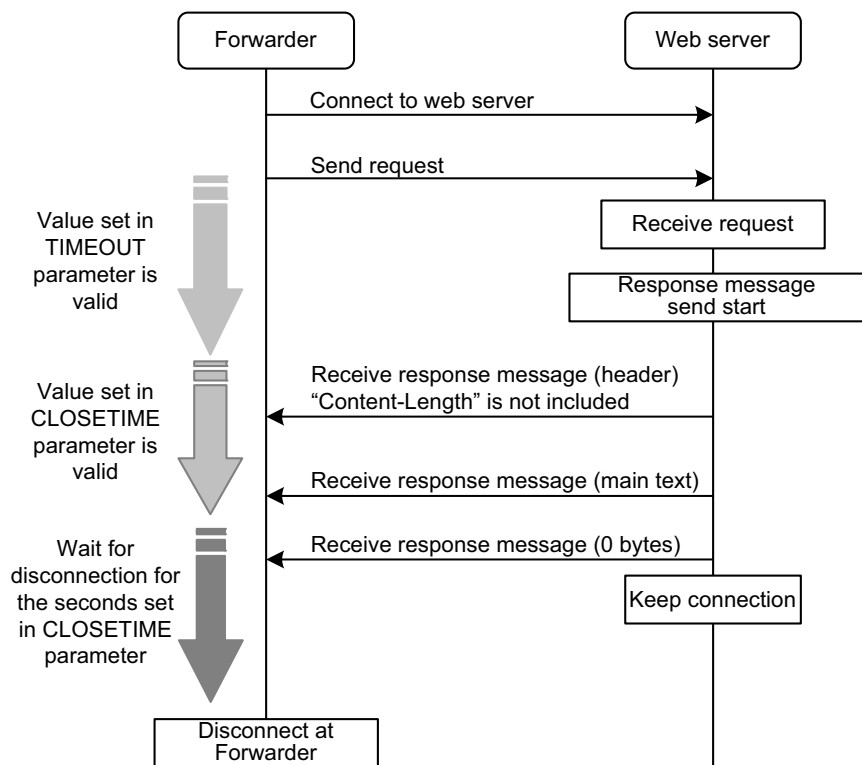
- The unit for setting the timeout value is seconds.
- The default value in the executable binary file is the value set to the TIMEOUT parameter.
- The initial value set in the standard configuration file is 3 seconds.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

**Configuration example** 1) To set the disconnect wait timer to 3 seconds:  
**CLOSETIME=3**

**Remarks**

- The value set by this parameter is used under the following conditions:
  - 1) “Content-Length” is not included in the HTTP header Backend Web Server response messages.





- In an environment where this parameter is used, the set disconnection waiting time applies each time a Backend Web Server is accessed.
- This parameter is effective when there is no “Content-Length” header in HTTP headers and a receive wait occurs while waiting for a response message.
- A **warning level error is output** if a timeout occurs due to the value of this parameter, but response messages received will be forwarded to the browser until the timer expires. (10.0)
- If a timeout occurs due to the value of this parameter, response messages received will be forwarded to the browser until the timer expires. The error log below is output when a timeout occurs.

Warning: recv() Timeout. [CLOSETIME] [host name:port number where timeout occurred]

See also **TIMEOUT**

## BUFFER

Overview	Sets the transfer method for Backend Web Server content that is not subject to content conversion.
Format	<p><b>BUFFER=flag</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : No Forwarder buffering</li><li>1 : Forwarder buffering (as in earlier versions)</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To transfer non-conversion content in non-buffering mode: <b>BUFFER=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is effective only when content belonging to MIME types not set in the CTYPE parameter is received from Backend Web Servers.</li><li>• Non-buffering mode (BUFFER=0) will improve performance for large files such as images and PDFs.</li></ul>
See also	CTYPE

# LASTMOD\_HEADER

**Overview** Turns on/off the function to send the Last-Modified header received from Backend Web Servers to browsers.

**Format** **LASTMOD\_HEADER=flag**

- One of the following values can be set to the flag:
  - 0 : Send the header to the browser
  - 1 : Do not send the header to the browser
- The default value set in the executable binary file is 0.
- The initial value set in the standard configuration file is 0.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To prevent sending Last-Modified headers to the browser:  
**LASTMOD\_HEADER=1**

**Remarks**

- This parameter is set so that Backend Web Server content is not cached at the web server run by Forwarder. It does not normally need to be set.
- If this parameter is set to not send the header (LASTMOD\_HEADER=1), the header is not sent to the browser even if a Last-Modified header is added to the RES\_HEADER parameter.

**See also** RES\_HEADER

# CENCODE

Overview	Turns on/off the function to ignore the Content-type header and prevent content conversion for content that contains a Content-encoding header.
Format	<p><b>CENCODE=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Ignore the Content-encoding header</li><li>1 : Enable the Content-encoding header</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To prevent compressed HTTP files received from Backend Web Servers from conversion: <b>CTYPE=text/html</b> <b>CENCODE=1</b></p> <p>In the above example, uncompressed HTTP files will still be converted.</p> <p>2) To prevent compressed HTTP files received from Backend Web Servers from conversion, and set the transfer mode to non-buffering: <b>CTYPE=text/html</b> <b>CENCODE=1</b> <b>BUFFER=0</b></p> <p>In the above example, all content not subject to conversion will be transferred in non-buffering mode (including HTML with HTTP compression).</p>
Remarks	<ul style="list-style-type: none"><li>• Setting this parameter to prevent conversion will still result in the Set-cookie header path attribute and Location header URL to be converted if the UNCONV_HEADER parameter is set to not convert (UNCONV_HEADER=header name).</li></ul>
See also	CTYPE

BUFFER  
UNCONV\_HEADER

## URL\_SCOLON

Overview	Turns on/off encoding of semicolons in URLs to be encoded.
Format	<p><b>URL_SCOLON=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Semicolon is encoded.</li><li>1 : Semicolon is not encoded.</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To not encode the semicolons included in the URL: <b>URL_SCOLON=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• Set this parameter when using a web server where an error occurred due to a request that has encoded semicolons in the URL.</li><li>• This parameter can also be set in the Forwarder configuration file. In this case, the same setting is made for all Backend Web Servers.</li><li>• The setting value of this parameter is ignored when the REQUEST_URI parameter is set to 1.</li><li>• The data in the QueryString is not encoded.</li></ul>
See also	REQUEST_URI (Forwarder configuration file)

## FO\_SEND

Overview	Sets the failover mode when Backend Web Server communication experiences send errors.
Format	<b>FO_SEND=flag</b> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Terminates with an error</li><li>1 : Failover is performed</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To perform a failover when a send error occurs in communication with the Backend Web Server: <b>FO_SEND=1</b>
Remarks	<ul style="list-style-type: none"><li>• The default value provides failover functionality when a communication error occurs during sending. However, be aware that a failover is not performed when a non-communication critical error occurs.</li></ul>
See also	FO_RECV FO_NODATA

## FO\_RECV

Overview	Sets the failover mode when Backend Web Server communication experiences receive errors.
Format	<p><b>FO_RECV=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Terminates</li><li>1 : Failover is performed</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To “terminate with error” when a receive error occurs during Backend Web Server communication:</p> <p><b>FO_RECV=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• The default value provides failover functionality when a communication error occurs during receiving. However, be aware that a failover is not performed when a non-communication critical error occurs.</li></ul>
See also	FO_SEND FO_NODATA



# FO\_NODATA

Overview	Sets the failover mode when Backend Web Server communication experiences receive sizes of 0.
Format	<p><b>FO_NODATA=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Terminates with an error</li><li>1 : Failover is performed</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To “terminate with error” when a receive size of 0 bytes occurs during Backend Web Server communication:</p> <p><b>FO_NODATA=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• A failover occurs if this is set to 1 when the receive size is 0 bytes. However, be aware that a failover is not performed when a non-communication critical error occurs.</li><li>• This is also effective when the RECV_ZERO_FLG parameter (described later) is set to 0.</li></ul>
See also	FO_SEND FO_RECV RECV_ZERO_FLG

Host configuration file [arbitrary file name]

---

## RECV\_ZERO\_FLG

Overview	Sets the operation when the receive data size from the Backend Web Server is 0 bytes.
Format	<p><b>RECV_ZERO_FLG=[flag]</b></p> <ul style="list-style-type: none"><li>• One of the following values can be set to the flag:<ul style="list-style-type: none"><li>0 : Receiving of 0 bytes results in an error.</li><li>1 : Receiving of 0 bytes does not result in an error.</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li></ul>
Configuration example	<p>1) To set error generation when the receive data size from the Backend Web Server is 0 bytes: <b>RECV_ZERO_FLG=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• Be aware that the FO_NODATA parameter setting value is ineffective when this parameter is set to 1 because errors can no longer be identified.</li></ul>
See also	FO_NODATA

### 2.2.7 Form authentication configuration parameters

This parameter is used to configure Automatic Form Authentication for Backend Web Servers.

Parameter name	Mandatory	Overview
FORM_FILE	×	Sets the form authentication configuration file

For details on these parameters, see the following pages.

## FORM\_FILE

Overview	Sets the name of the form authentication configuration file used to set Automatic Form Authentication for Backend Web Servers.
Format	<b><u>FORM_FILE=form group name,form authentication configuration file name</u></b> <ul style="list-style-type: none"><li>• The form group name and the form authentication configuration file name cannot be omitted.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set the form group name to Form1 and set the form authentication configuration file to this group and set its name to /opt/icewall-ss0/dfw/cgi-bin/form1.conf:</p> <p><b>FORM_FILE=Form1,/opt/icewall-ss0/dfw/cgi-bin/form1.conf</b></p>
Remarks	<ul style="list-style-type: none"><li>• An actual form name (value set with the FORM tag NAME attribute) does not need to be set for the form group name.</li><li>• If a form authentication configuration file name is set with a relative path, set the relative path from the Forwarder binary file.</li></ul>
See also	FORM_METHOD (form authentication configuration file) FORM_SEND (form authentication configuration file) FORM_URL (form authentication configuration file) FORM_KEY (form authentication configuration file) FORM_HTML (form authentication configuration file) FORM_DATA_STR (form authentication configuration file) FORM_DATA_USR (form authentication configuration file) FORM_DATA_PAGE (form authentication configuration file) FORM_KEY_EXCEPTION (form authentication configuration file)

### 2.2.8 Security parameters

This parameter is used to establish security settings for Backend Web Server communication.

Parameter name	Mandatory	Overview
SSL_CIPHER_SUITE	×	Sets the SSL encryption format

For details on these parameters, see the following pages.

## SSL\_CIPHER\_SUITE

**Overview**                Sets the SSL encryption format used in communication with the Backend Web Server.

**Format**                **SSL\_CIPHER\_SUITE=encryption format**

- The encryption format can be set in the same section as the SSLCipherSuite directive of Apache HTTP servers.
- The encryption format has a maximum length of 512 bytes.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)

**Configuration example**    1) To set the encryption format to “RC4+RSA”:  
**SSL\_CIPHER\_SUITE=RC4+RSA**

**Remarks**

- Backend Web Servers must be able to encrypt data according to the encryption format set with this parameter.
- The “IceWall SSO SSL Option” is required to use this parameter.
- If this parameter is not set, the default value of the OpenSSL library is used.

**See also**                SHOST

## 2.3 Form authentication configuration file (arbitrary file)

**Overview** This file is used to configure Forwarder to enable Automatic Form Authentication with Backend Web Servers.  
Parameters available to the user are as follows:

Parameter group	Parameter name
Form authentication configuration parameters	FORM_METHOD
	FORM_SEND
	FORM_URL
	FORM_KEY
	FORM_KEY_EXCEPTION 10.0
	FORM_HTML
	FORM_DATA_STR
	FORM_DATA_USR
	FORM_DATA_PAGE 10.0
	FORM_DATA_PAGE_REF 10.0

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

**Remarks** Parameters that can be set in this configuration file can also be defined in the host configuration file.

Operations for different settings in configuration files and host configuration files with the same form group name differ for parameters that allow multiple-line configuration.

- Multiple-line configurable parameters:  
The configuration from both the Forwarder configuration file and host configuration file is used to process content.
- Single-line only parameters:  
Only the configuration from the host configuration file is used to process content.

These parameters are described on the following pages.

### 2.3.1 Form authentication configuration parameters

These parameters are used to configure Automatic Form Authentication with Backend Web Servers.

Parameter name	Mandatory	Overview
FORM_METHOD	×	Sets the form authentication method
FORM_SEND	×	Sets the form authentication recipient
FORM_URL	×	Sets the form authentication target URL
FORM_KEY	×	Sets the form authentication target keyword
FORM_KEY_EXCEPTION <b>10.0</b>	×	Sets the keyword not included in the login page that is subject to form authentication residing on a Backend Web Server
FORM_HTML	×	Sets the indirect authentication HTML of the form authentication
FORM_DATA_STR	×	Sets the fixed value that is sent by form authentication
FORM_DATA_USR	×	Sets the user information that is sent by form authentication
FORM_DATA_PAGE	×	Sets the content attributes that are sent by form authentication
FORM_DATA_PAGE_REF <b>10.0</b>	×	Sets whether or not to replace the entity references included in the value retrieved with the FORM_DATA_PAGE parameter during the direct transmission method with the original characters

For details on these parameters, see the following pages.



## FORM\_METHOD

Overview	Sets the send method for form authentication files that reside on Backend Web Servers.
Format	<p><b>FORM_METHOD=<u>form group name</u>,<u>method name</u></b></p> <ul style="list-style-type: none"><li>• Use the form group name set by the FORM_FILE parameter in the host configuration file, if one exists. Otherwise, set a new name here.</li><li>• One of the following values can be set to the method name: GET : Send using the GET method for form authentication POST : Send using the POST method for form authentication</li><li>• This parameter is required for performing form authentication.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for the method name is out of range.</li></ul>
Configuration example	<p>1) To set the form group name to Form1 and use the GET method: <b>FORM_METHOD=Form1,GET</b></p> <p>2) To set the form group name to Form2 and use the POST method: <b>FORM_METHOD=Form2,POST</b></p>
Remarks	<ul style="list-style-type: none"><li>• The use of this parameter requires the FORM_URL and FORM_KEY parameters (both described later) to also be set.</li></ul>
See also	FORM_FILE (host configuration file) FORM_SEND FORM_URL FORM_KEY FORM_HTML FORM_DATA_STR FORM_DATA_USR FORM_DATA_PAGE FORM_KEY_EXCEPTION

---

Form authentication configuration file (arbitrary file)

---

## FORM\_SEND

Overview	Sets the path to store the form authentication data residing on Backend Web Servers.
Format	<p><b>FORM_SEND=<u>form group name</u>,<u>recipient path</u></b></p> <ul style="list-style-type: none"><li>• Use the form group name configured in the FORM_FILE or FORM_METHOD parameters.</li><li>• Use the location of the program receiving the data for the recipient path. Normally, this is the value set with the FORM tag ACTION attribute.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set the form group name to Form1, and the data recipient path to /cgi-bin/login.cgi:</p> <p><b>FORM_SEND=Form1,/cgi-bin/login.cgi</b></p>
Remarks	<ul style="list-style-type: none"><li>• If this parameter is not set, the value of the ACTION attribute set in the FORM tag of the target form authentication is retrieved. However, if there are multiple form authentications within the content, the form authentication that is specified first is subject to form authentication. For more information about the target form authentication, see the FORM_URL parameter and FORM_KEY parameter below.</li></ul>
See also	<p>FORM_FILE (host configuration file) FORM_METHOD FORM_URL FORM_KEY FORM_HTML FORM_DATA_STR FORM_DATA_USR FORM_DATA_PAGE FORM_KEY_EXCEPTION</p>

## FORM\_URL

Overview	Sets the path used to display the login page for form authentication files residing on Backend Web Servers.
Format	<b>FORM_URL=<u>form group name</u>,<u>target path</u></b> <ul style="list-style-type: none"><li>• Use the form group name configured in the FORM_FILE or FORM_METHOD parameters.</li><li>• Set the path to display the login page for form authentication files residing on Backend Web Servers.</li><li>• This parameter is required for performing form authentication.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set Form1 as the form authentication group name with a login page displayed from the path /cgi-bin/login.cgi: <b>FORM_URL=Form1,/cgi-bin/login.cgi</b>
Remarks	<ul style="list-style-type: none"><li>• Client requests to the path set by this parameter will be subject to the form authentication process.</li><li>• Because matches are determined based on the beginning of strings, using a directory name for this setting will cause everything within the directory to undergo form authentication.</li></ul>
See also	FORM_FILE (host configuration file) FORM_METHOD FORM_SEND FORM_KEY FORM_HTML FORM_DATA_STR FORM_DATA_USR FORM_DATA_PAGE FORM_KEY_EXCEPTION

---

**Form authentication configuration file (arbitrary file)**

---

## FORM\_KEY

Overview	Sets the keyword included in the login page that is subject to form authentication residing on a Backend Web Server. The page that includes the keyword set here is identified as the form authentication login page.
Format	<p><b>FORM_KEY=<u>form group name</u>,<u>search keyword</u></b></p> <ul style="list-style-type: none"><li>• Use the form group name configured in the FORM_FILE or FORM_METHOD parameters.</li><li>• Set a character string to be used as the search keyword for determining the login page for form authentication.</li><li>• Setting text for a form can span multiple lines.</li><li>• This parameter is required for performing form authentication.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set form authentication with a form group name of Form1 and “APP LOGIN” as the keyword that identifies the login page: <b>FORM_KEY=Form1,APP LOGIN</b></p> <p>2) To set form authentication with a form group name of Form2 and “APP LOGIN” and “Welcome” as the keywords that determine the login page: <b>FORM_KEY=Form2,APP LOGIN</b> <b>FORM_KEY=Form2&gt;Welcome</b></p>
Remarks	<ul style="list-style-type: none"><li>• The search keywords set by this parameter apply to all content starting from the path that was set by the FORM_URL parameter.</li><li>• HTTP headers sent from Backend Web Servers are also included in the search range, and so a character string unique to the login page content must be used as the search keyword.</li><li>• Compressed content cannot be judged as the login screen.</li><li>• The keyword search for this parameter is processed before URLKEY and REPKEY keyword conversion.</li></ul>

- If multiple search keywords are set, form authentication is performed only when all the search keywords match.
- There are no restrictions on the type of character encoding that can be used for the search keywords; however, the type of character encoding used for search keywords must be the same as the type of character encoding used for the actual content of a search.
- Commas and line feeds cannot be used in search keywords set by this parameter. When setting multi-byte characters, character strings cannot be set that include NUL characters (0x00), line feeds (0x0a), and commas (0x2c).
- Search keywords are case sensitive, and so must be complete matches.

See also

FORM\_FILE (host configuration file)  
FORM\_METHOD  
FORM\_SEND  
FORM\_URL  
FORM\_HTML  
FORM\_DATA\_STR  
FORM\_DATA\_USR  
FORM\_DATA\_PAGE  
FORM\_KEY\_EXCEPTION

## FORM\_KEY\_EXCEPTION 10.0

**Overview** Sets the keyword that is not included in the login page that is subject to form authentication residing on a Backend Web Server. The page that includes the keywords set with the FORM\_KEY parameter and does not include the keywords set here is judged as the login page for form authentication.

This parameter is available since version 10.0.

**Format** **FORM\_KEY\_EXCEPTION=**form group name,target path

- Use the form group name configured in the FORM\_FILE or FORM\_METHOD parameters.
- For the search keyword, set a character string that is not included on the login page for determining the login page for form authentication.
- Setting text for a form can span multiple lines.
- This parameter is ineffective if the FORM\_KEY parameter is not set.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)

**Configuration example** 1) To set form authentication with a form group name of Form1 including the keyword “LOG IN” and not including the keyword “RELOGIN” as the conditions for identifying the login page:

```
FORM_KEY=Form1,LOGIN  
FORM_KEY_EXCEPTION=Form1,RELOGIN
```

- 2) To set form authentication with a form group name of Form2 that has including the keyword “LOG IN” and not including the keywords “RELOGIN” and “ERROR” as the conditions for identifying the login page:

```
FORM_KEY=Form2,LOGIN  
FORM_KEY_EXCEPTION=Form2,RELOGIN  
FORM_KEY_EXCEPTION=Form2,ERROR
```

**Remarks**

- The search keywords set by this parameter apply to all content starting from the path that was set by the FORM\_URL parameter.
- HTTP headers sent from Backend Web Servers are also included in the search range, and so a character string unique to the login page

content must be used as the search keyword.

- Compressed content cannot be judged as the login screen.
- The keyword search for this parameter is processed before URLKEY and REPKEY keyword conversion.
- When multiple search keywords are set, form authentication is not performed even if one line of the search keywords matches.
- There are no restrictions on the type of character encoding that can be used for the search keywords; however, the type of character encoding used for search keywords must be the same as the type of character encoding used for the actual content of a search.
- Commas and line feeds cannot be used in search keywords set by this parameter. When setting multi-byte characters, character strings cannot be set that include NUL characters (0x00), line feeds (0x0a), and commas (0x2c).
- Search keywords are case sensitive, and so must be complete matches.

See also

FORM\_METHOD  
FORM\_SEND  
FORM\_URL  
FORM\_KEY  
FORM\_HTML  
FORM\_DATA\_STR  
FORM\_DATA\_USR  
FORM\_DATA\_PAGE  
FORM\_FILE (host configuration file)

---

**Form authentication configuration file (arbitrary file)**

---

## FORM\_HTML

Overview	Sets the template HTML file to be used if an indirect transfer method from a browser is selected for login to form authentication files residing on Backend Web Servers.
Format	<p><b>FORM_HTML=<u>form group name,template HTML file name</u></b></p> <ul style="list-style-type: none"><li>• Use the form group name configured in the FORM_FILE or FORM_METHOD parameters.</li><li>• If this parameter is set, the form authentication configuration uses the indirect transfer method. If this parameter is not set, the form authentication configuration uses the direct transfer method.</li><li>• Set a local file as the template HTML file name.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set the indirect transfer method template HTML file to /opt/icewall-ssso/dfw/html/form-trans.html for form group name Form1:</p> <p><b>FORM_HTML=Form1,/opt/icewall-ssso/dfw/html/form-trans.html</b></p>
Remarks	<ul style="list-style-type: none"><li>• JavaScript is used to automatically send browser requests of template HTML that normally uses indirect transfer samples. Browsers that support JavaScript or otherwise set to use JavaScript must be used to employ the sample template HTML.</li><li>• For information about differences between the direct transfer method and the indirect transfer method, see the “IceWall SSO Automatic Form Authentication Configuration Manual.”</li><li>• If the user ID and password sent by IceWall SSO fail form authentication, FORM authentication may be repeated endlessly under certain conditions. For details, see the “IceWall SSO Automatic Form Authentication Configuration Manual.”</li></ul>
See also	FORM_FILE (host configuration file) FORM_METHOD FORM_SEND FORM_URL FORM_KEY



FORM\_DATA\_STR  
FORM\_DATA\_USR  
FORM\_DATA\_PAGE  
FORM\_DATA\_PAGE\_REF  
FORM\_KEY\_EXCEPTION

---

**Form authentication configuration file (arbitrary file)**

---

## FORM\_DATA\_STR

**Overview**                Sets parameters so that custom values can be sent as the data required for form authentication files residing on Backend Web Servers.

**Format**                **FORM\_DATA\_STR=form group name,transmission data type,attribute name,attribute value**

- Use the form group name configured in the FORM\_FILE or FORM\_METHOD parameters.
- Set one of the following values for the transmission data type, depending on the transmission method.
  - Direct transmission method
    - POSTDATA    : Send using POST data
    - QUERY        : Send using QueryString
  - Indirect transmission method
    - ENCVAL       : Replaces the template HTML keyword using the indirect transmission method with URL encoding
    - NOENCVAL    : Replaces the template HTML keyword using the indirect transmission method without encoding
- Set the attribute name to a parameter name required by the form authentication process.
- Set a custom character string for the attribute value.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- The system is not guaranteed to work as expected when the transmission data type is set outside the configurable range.

**Configuration example**

- 1) To send USERID=user01 as POST data:  
**FORM\_DATA\_STR=Form1,POSTDATA,USERID,user01**
- 2) To send PASSWORD=passwd as QueryString:  
**FORM\_DATA\_STR=Form1,QUERY,PASSWORD,passwd**
- 3) To replace the keyword HIDEURL in the indirect transmission method template HTML with /sys/ using encoding:  
**FORM\_DATA\_STR=Form1,ENCVAL,HIDEURL,/sys/**

- |         |  |
|---------|--|
| Remarks | <ul style="list-style-type: none"><li>• This parameter is ineffective if the POSTDATA is the transmission method and the FORM_METHOD parameter is set to a value other than POST.</li><br/><li>• This parameter is ineffective if ENCVAl or NOENCVAL is the direct transmission method, or if POSTDATA or QUERY is the indirect transmission method.</li><br/><li>• If ENCVAl is set for the indirect transmission method, all characters except for the unreserved characters specified in RFC2396 (URI) are URL encoded.</li></ul> |
|---------|--|

See also	FORM_FILE (host configuration file) FORM_METHOD FORM_SEND FORM_URL FORM_KEY FORM_HTML FORM_DATA_USR FORM_DATA_PAGE FORM_KEY_EXCEPTION
----------	---

---

**Form authentication configuration file (arbitrary file)**

---

## FORM\_DATA\_USR

**Overview**                Sets parameters to enable user login data to be sent as the data required for form authentication files residing on Backend Web Server.

**Format**                **FORM\_DATA\_USR=form group name,transmission data type,attribute name,authentication DB column name**

- Use the form group name configured in the FORM\_FILE or FORM\_METHOD parameters.
- Set one of the following values for the transmission data type, depending on the transmission method.
  - Direct transmission method
    - POSTDATA : Send using POST data
    - QUERY : Send using QueryString
  - Indirect transmission method
    - ENCVAL : Replaces the template HTML keyword using the indirect transmission method with URL encoding
    - NOENCVAL : Replaces the template HTML keyword using the indirect transmission method without encoding
- Set the Authentication DB column name to the column name set in the Authentication Module. The following reserved words are provided for the Authentication DB column name.
  - [Authentication DB column name reserved words]
    - DEFAULTUID : The user ID that was entered at login is used. For client certificates, the user ID in the certificate is used.
    - DEFAULTPWD : The password that was used at login is used.
- This parameter can span multiple lines.
- Values that are acquired in the Authentication DB column name are values transferred from the Authentication Module.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- The system is not guaranteed to work as expected when the transmission data type is set outside the configurable range.

**Configuration example**        1) To send a UID column value for the USERID attribute as POST data:  
**FORM\_DATA\_USR=Form1,POSTDATA,USERID,UID**

- 2) To send a passwd column value for the PASSWORD attribute as QueryString:  
**FORM\_DATA\_USR=Form1,QUERY,PASSWORD,passwd**
- 3) To encode and replace the template HTML keyword DATE attribute using the indirect transmission method with the LOGONDATE column value:  
**FORM\_DATA\_USR=Form1,ENCVAL,DATE,LOGONDATE**
- 4) To send the login user ID to the attribute name UserID and the login password to the attribute name Password as POST data:  
**FORM\_DATA\_USR=Form1,POSTDATA,UserID,DEFAULTUID**  
**FORM\_DATA\_USR=Form1,POSTDATA>Password,DEFAULTPWD**

## Remarks

- This parameter is ineffective if the POSTDATA is the transmission method and the FORM\_METHOD parameter is set to a value other than POST.
- This parameter is ineffective if ENCVAL or NOENCVAL is the direct transmission method, or if POSTDATA or QUERY is the indirect transmission method.
- If ENCVAL is set for the indirect transmission method, all characters except for the unreserved characters specified in RFC2396 (URI) are URL encoded.
- If a column name that does not exist is set, it is treated as “No value” in the same way as “Attribute name=.”
- DEFAULTUID and DEFAULTPWD cannot be used as Authentication DB column names.

## See also

FORM\_FILE (host configuration file)  
FORM\_METHOD  
FORM\_SEND  
FORM\_URL  
FORM\_KEY  
FORM\_HTML  
FORM\_DATA\_STR  
FORM\_DATA\_PAGE  
FORM\_KEY\_EXCEPTION

## FORM\_DATA\_PAGE ⑩.0

**Overview** Sets an attribute name to be used as the value of the INPUT tag contained in the login pages for form authentication files residing on Backend Web Servers. Initial values are preset to the form authentication page, and this parameter is used for these initial values.

Some specifications of this parameter have been modified since version 10.0.

**Format** **FORM\_DATA\_PAGE=form group name,transmission data type,transmission attribute name,search attribute name**

- Use the form group name configured in the FORM\_FILE or FORM\_METHOD parameters.
- Set one of the following values for the transmission data type, depending on the transmission method.
  - Direct transmission method
    - POSTDATA : Send using POST data
    - QUERY : Send using QueryString
  - Indirect transmission method
    - ENCVAL : Replaces the template HTML keyword using the indirect transmission method with URL encoding
    - NOENCVAL : Replaces the template HTML keyword using the indirect transmission method without encoding
- Set the send attribute name to a parameter name required for form authentication.
- Set the search attribute name to the NAME attribute in the INPUT tag.
- This parameter can span multiple lines.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- The system is not guaranteed to work as expected when the transmission data type is set outside the configurable range.

**Configuration example**

- 1) To send the value of the INPUT tag in the NAME attribute UID for the USERID attribute as POST data:  
**FORM\_DATA\_PAGE=Form1,POSTDATA,USERID,UID**
- 2) To send the value of the INPUT tag in the NAME attribute “passwd” for the PASSWORD attribute as QueryString:

**FORM\_DATA\_PAGE=Form1,QUERY,PASSWORD,passwd**

- 3) To encode and replace the template HTML keyword DATE attribute using the indirect transmission method by the “LOGONDATE” INPUT tag value:

**FORM\_DATA\_PAGE=Form1,ENCVAL,DATE,LOGONDATE****Remarks**

- This parameter is ineffective if the POSTDATA is the transmission method and the FORM\_METHOD parameter is set to a value other than POST.
- This parameter is ineffective if ENCVAL or NOENCVAL is the direct transmission method, or if POSTDATA or QUERY is the indirect transmission method.
- If ENCVAL is set for the indirect transmission method, all characters except for the unreserved characters specified in RFC2396 (URI) are URL encoded.
- If a search attribute name that does not exist is specified, it is treated as “No value” in the same way as “Send attribute name=.”
- If the value retrieved with this parameter contains an entity reference, set the FORM\_DATA\_PAGE\_REF parameter to 1. (10.0)

**See also**

FORM\_FILE (host configuration file)  
FORM\_METHOD  
FORM\_SEND  
FORM\_URL  
FORM\_KEY  
FORM\_HTML  
FORM\_DATA\_STR  
FORM\_DATA\_USR  
FORM\_KEY\_EXCEPTION  
FORM\_DATA\_PAGE\_REF

## Form authentication configuration file (arbitrary file)

**FORM\_DATA\_PAGE\_REF** 10.0

**Overview** Sets whether or not to replace the entity references included in the value retrieved with the FORM\_DATA\_PAGE parameter during the direct transmission method with the original characters.

This parameter is available since version 10.0.

**Format** **FORM\_DATA\_PAGE\_REF=**form group name**,flag**

- Use the form group name configured in the FORM\_FILE or FORM\_METHOD parameters.
- One of the following values can be set to the flag:
  - 0 : Do not replace entity references (backward compatibility)
  - 1 : Replace entity references
- The default value set in the executable binary file is 0.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To replace the entity references with the original characters when they are included in the form information retrieved with the FORM\_DATA\_PAGE parameter during direct transmission method using Automatic Form Authentication:  
**FORM\_DATA\_PAGE\_REF=Form1,1**

**Remarks**

- The target entity references and the characters they are replaced with are as follows:
  - &nbsp;(&#160; &#xa0;) → is No break space
  - &lt;(&#60; &#x3c;) → <
  - &gt;(&#62; &#x3e;) → >
  - &amp;(&#38; &#x26;) → &
  - &quot;(&#34; &#x22;) → “
  - &apos;(&#39; &#x27;) → ‘
- \* Both character entity references and numerical character references will be replaced.
- \* Character entity references (such as “&amp”) are case sensitive. Numerical character references (such as “&# ~”) are not case



sensitive.

- This parameter is ineffective when there is no FORM\_DATA\_PAGE parameter.
- This parameter is only effective when the direct transmission method (FORM\_HTML parameter not included) is used. It is ineffective when the indirect transmission method (FORM\_HTML parameter included) is used.

See also

FORM\_HTML  
FORM\_DATA\_PAGE

## 2.4 HTML configuration file (html.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 by each Forwarder. Parameters available to the user are as follows:

Parameter group	Parameter name
Login related page parameters	LOGIN_UID (10.0)
	LOGIN_CERT (10.0)
	LOGIN_FORCE (10.0)
	LOGIN_ERR_UID (10.0)
	LOGIN_ERR_PWD (10.0)
	LOGIN_ERR_LOCK (10.0)
	LOGIN_ERR_1STCERT (10.0)
	LOGIN_ERR_SERIAL (10.0)
	LOGIN_ERR_NOGRP (10.0)
	LOGIN_ERR_STOP (10.0)
	LOGIN_ERR_LIMIT (10.0)
	LOGIN_ERR_POSTLIMIT (10.0)
Access control related page parameters	ACCESS_DENY (10.0)
	DATA_SEND_ERR (10.0)
	REQUEST_ACL_ERR (10.0)
	FILTER_REQUEST (10.0)
POST data inheritance related page parameters	MAXPOST_ERR (10.0)
Logout related page parameters	LOGOUT (10.0)
	LOGOUT_SUCCESS (10.0)
	LOGOUT_EXPIRE (10.0)
	LOGOUT_FAILURE (10.0)
Password change related page parameters	PWDCHG (10.0)
	PWDCHG_SUCCESS (10.0)
	PWDCHG_ERR_OLD (10.0)
	PWDCHG_ERR_REENT (10.0)
	PWDCHG_ERR_POLICY (10.0)
	PWDCHG_ERR_LOGNG (10.0)
	PWDCHG_ERR_VIO (10.0)
	PWDCHG_FAILURE (10.0)
	PWDCHG_WARNING (10.0)
	PWDCHG_ERR_POSTLIMIT (10.0)

Parameter group	Parameter name
Cross site script error related page parameters	FILTER_GET 10.0
	FILTER_POST 10.0
	FILTER_HTML 10.0
	FILTER_SVR 10.0
System error related page parameters	SYSTEM_ERR 10.0
	SYSTEM_ERR_NOALIAS 10.0
	SYSTEM_ERR_BADALIAS 10.0
	SYSTEM_DOWN_CERTD 10.0
	SYSTEM_DOWN_DB 10.0
	SYSTEM_DOWN_HTTP 10.0
	SYSTEM_TOUT_CERTD 10.0
	SYSTEM_TOUT_HTTP 10.0
User-defined error related page parameters	SYSTEM_BUSY_DB 10.0
	USREXT_ERR1 10.0
	USREXT_ERR2 10.0
	USREXT_ERR3 10.0
	USREXT_ERR4 10.0
	USREXT_ERR5 10.0
	USREXT_ERR6 10.0

## Storage location

The following is the default storage location for the HTML configuration file:

/opt/icewall-ssso/dfw/cgi-bin/html.conf

In addition, the storage location and file name for the Compact HTML configuration file, included in the standard installation, is as follows:

/opt/icewall-ssso/dfw/cgi-bin/cht.html.conf

## Remarks

None

For details on these parameters, see the following pages.

### 2.4.1 Login related page parameters

These parameters are used to configure the HTML pages displayed when logging into IceWall.

Parameter name	Mandatory	Overview
LOGIN_UID (10.0)	×	Sets the login page for user ID
LOGIN_CERT (10.0)	×	Sets the login page for client certificates
LOGIN_FORCE (10.0)	×	Sets the forced login page
LOGIN_ERR_UID (10.0)	×	Sets the user ID error page
LOGIN_ERR_PWD (10.0)	×	Sets the password error page
LOGIN_ERR_LOCK (10.0)	×	Sets the account lock error page
LOGIN_ERR_1STCERT (10.0)	×	Sets the pre-authenticated error page
LOGIN_ERR_SERIAL (10.0)	×	Sets the invalid certificate error page
LOGIN_ERR_NOGRP (10.0)	×	Sets the no group error page
LOGIN_ERR_STOP (10.0)	×	Sets the login stop error page
LOGIN_ERR_LIMIT (10.0)	×	Sets the maximum login counts error page
LOGIN_ERR_POSTLIMIT (10.0)	×	Sets the login transmission time limit error page displayed when POST data is transmitted after exceeding the time limit during logins including forced logins

For details on these parameters, see the following pages.

## LOGIN\_UID 10.0

**Overview** Sets the login page displayed that allows users to enter their user ID and password.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGIN\_UID=storage location login page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/login.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/login.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the login page:  
**LOGIN\_UID=file:///opt/icewall-sso/dfw/html/login.html**
- 2) To set a local file as the login page, the status code to “200,” and the status message to “IceWall Login”:  
**LOGIN\_UID=file:///opt/icewall-sso/dfw/html/login.html,200,IceWall Login**

---

HTML configuration file (html.conf)

---

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGIN_CERT LOGIN_FORCE

# LOGIN\_CERT 10.0

**Overview**                Sets the login page for logins using client certificates and passwords.

Additional functionality of this parameter is available since version 10.0.

**Format**                **LOGIN\_CERT=storage location login page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file://    : An HTML file on the local server
  - http://    : An HTML file on a remote server
  - https://   : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/login\_cert.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/login\_cert.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the login page:  
**LOGIN\_CERT=file:///opt/icewall-ssso/dfw/html/login\_cert.html**
- 2) To set a local file as the login page, the status code to “200,” and the status message to “IceWall Login”:  
**LOGIN\_CERT=file:///opt/icewall-ssso/dfw/html/login\_cert.html,200,Ice Wall Login**

---

HTML configuration file (html.conf)

---

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO Client Certificates Option” is required to use this parameter.</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGIN_UID LOGIN_FORCE



# LOGIN\_FORCE 10.0

Overview	<p>Sets the forced login page that is displayed if a duplicate login is attempted when exclusive login is set forbidding duplicate logins.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>LOGIN_FORCE=storage location forced login page file name[,status code][,status message]</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The following values can be set for the storage location:<ul style="list-style-type: none"><li>file:// : An HTML file on the local server</li><li>http:// : An HTML file on a remote server</li><li>https:// : An HTML file on a remote server (SSL)</li></ul></li><li>• Use status codes that are valid settings for web servers.</li><li>• The status message can use any selected character string up to a maximum of 255 bytes.</li><li>• The status code and status message are settable only when a local file is specified for the storage location.</li><li>• The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).</li><li>• The status code must also be set if a status message is set.</li><li>• The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/login_force.html.</li><li>• The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/login_force.html.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <span style="border: 1px solid black; border-radius: 50%; padding: 0 2px;">10.0</span></li></ul>
Configuration example	<p>1) To set a local file as the forced login page: <b>LOGIN_FORCE=file:///opt/icewall-ssso/dfw/html/login_force.html</b></p> <p>2) To set a local file as the forced login page, the status code to “200,” and the status message to “IceWall Login”: <b>LOGIN_FORCE=file:///opt/icewall-ssso/dfw/html/login_force.html,200, IceWall Login</b></p>

---

HTML configuration file (html.conf)

---

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGIN_UID LOGIN_CERT

## LOGIN\_ERR\_UID 10.0

Overview	<p>Sets the user ID error page that is displayed when a login is attempted with an unregistered user ID.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>LOGIN_ERR_UID=storage location user ID error page file name[,status code][,status message]</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The following values can be set for the storage location:<ul style="list-style-type: none"><li>file:// : An HTML file on the local server</li><li>http:// : An HTML file on a remote server</li><li>https:// : An HTML file on a remote server (SSL)</li></ul></li><li>• Use status codes that are valid settings for web servers.</li><li>• The status message can use any selected character string up to a maximum of 255 bytes.</li><li>• The status code and status message are settable only when a local file is specified for the storage location.</li><li>• The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).</li><li>• The status code must also be set if a status message is set.</li><li>• The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/login_userid_error.html.</li><li>• The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/login_userid_error.html.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <span style="border: 1px solid black; border-radius: 50%; padding: 0 2px;">10.0</span></li></ul>
Configuration example	<p>1) To set a local file as the user ID error page: <b>LOGIN_ERR_UID=file:///opt/icewall-ssso/dfw/html/login_userid_error.html</b></p> <p>2) To set a local file as the user ID error page, the status code to “200,” and the status message to “Login Error”: <b>LOGIN_ERR_UID=file:///opt/icewall-ssso/dfw/html/login_userid_error.html,200,Login Error</b></p>

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_PWD  
LOGIN\_ERR\_LOCK  
LOGIN\_ERR\_NOGRP  
LOGIN\_ERR\_STOP  
LOGIN\_ERR\_LIMIT  
LOGIN\_ERR\_1STCERT  
LOGIN\_ERR\_SERIAL

## LOGIN\_ERR\_PWD 10.0

**Overview** Sets the password error page that is displayed when a login is attempted with an invalid password.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGIN\_ERR\_PWD=storage location password error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/login\_pwd\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/login\_pwd\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the password error page:  
**LOGIN\_ERR\_PWD=file:///opt/icewall-sso/dfw/html/login\_pwd\_error.html**
- 2) To set a local file as the password error page, the status code to “200,” and the status message to “Login Error”:  
**LOGIN\_ERR\_PWD=file:///opt/icewall-sso/dfw/html/login\_pwd\_error.html,200,Login Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_UID  
LOGIN\_ERR\_LOCK  
LOGIN\_ERR\_NOGRP  
LOGIN\_ERR\_STOP  
LOGIN\_ERR\_LIMIT  
LOGIN\_ERR\_1STCERT  
LOGIN\_ERR\_SERIAL

## LOGIN\_ERR\_LOCK 10.0

**Overview** Sets the account lock error page that is displayed when a password error occurs more than the specified number of times.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGIN\_ERR\_LOCK=storage location account lock error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/login\_lock\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/login\_lock\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the account lock error page:  
**LOGIN\_ERR\_LOCK=file:///opt/icewall-sso/dfw/html/login\_lock\_error.html**
- 2) To set a local file as the account lock error page, the status code to “200,” and the status message to “Login Error”:  
**LOGIN\_ERR\_LOCK=file:///opt/icewall-sso/dfw/html/login\_lock\_error.html,200,Login Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_UID  
LOGIN\_ERR\_PWD  
LOGIN\_ERR\_NOGRP  
LOGIN\_ERR\_STOP  
LOGIN\_ERR\_LIMIT  
LOGIN\_ERR\_1STCERT  
LOGIN\_ERR\_SERIAL



## LOGIN\_ERR\_1STCERT <sup>(10.0)</sup>

**Overview** Sets the pre-authenticated error page that is displayed when a login with a user ID and password is attempted after an initial login using a client certificate.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGIN\_ERR\_1STCERT=storage location login pre-authenticated error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/login\_cert\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/login\_cert\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the pre-authenticated error page:  
**LOGIN\_ERR\_1STCERT=file:///opt/icewall-sso/dfw/html/login\_cert\_error.html**
- 2) To set a local file as the pre-authenticated error page, the status code to “200,” and the status message to “Login Error”:  
**LOGIN\_ERR\_1STCERT=file:///opt/icewall-sso/dfw/html/login\_cert\_error.html,200,Login Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO Client Certificates Option” is required to use this parameter.
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_UID  
LOGIN\_ERR\_PWD  
LOGIN\_ERR\_LOCK  
LOGIN\_ERR\_NOGRP  
LOGIN\_ERR\_STOP  
LOGIN\_ERR\_SERIAL  
LOGIN\_ERR\_LIMIT

## LOGIN\_ERR\_SERIAL <sup>(10.0)</sup>

### Overview

Sets the certificate serial number error page that is displayed when the serial number of a client certificate is invalid due to certificate renewal.

Additional functionality of this parameter is available since version 10.0.

### Format

**LOGIN\_ERR\_SERIAL=storage location certificate serial number error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/login\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/login\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

### Configuration example

- 1) To set a local file as the certificate serial number error page:  
**LOGIN\_ERR\_SERIAL=file:///opt/icewall-ssso/dfw/html/login\_error.html**
- 2) To set a local file as the certificate serial number error page, the status code to “200,” and the status message to “Login Error”:  
**LOGIN\_ERR\_SERIAL=file:///opt/icewall-ssso/dfw/html/login\_error.html,200,Login Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO Client Certificates Option” is required to use this parameter.
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_UID  
LOGIN\_ERR\_PWD  
LOGIN\_ERR\_LOCK  
LOGIN\_ERR\_NOGRP  
LOGIN\_ERR\_STOP  
LOGIN\_ERR\_1STCERT  
LOGIN\_ERR\_LIMIT

## LOGIN\_ERR\_NOGRP 10.0

**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.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGIN\_ERR\_NOGRP=storage location no group error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/login\_nogrp\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/login\_group\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the no group error page:  
**LOGIN\_ERR\_NOGRP=file:///opt/icewall-sso/dfw/html/login\_nogrp\_error.html**
- 2) To set a local file as the no group error page, the status code to “200,” and the status message to “Login Error”:  
**LOGIN\_ERR\_NOGRP=file:///opt/icewall-sso/dfw/html/login\_nogrp\_error.html,200,Login Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_UID  
LOGIN\_ERR\_PWD  
LOGIN\_ERR\_LOCK  
LOGIN\_ERR\_STOP  
LOGIN\_ERR\_LIMIT  
LOGIN\_ERR\_1STCERT  
LOGIN\_ERR\_SERIAL

## LOGIN\_ERR\_STOP <sup>(10.0)</sup>

**Overview** Sets the login stop error page that is displayed when a login is attempted with a user ID for which login has stopped.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGIN\_ERR\_STOP=storage location login stop error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/login\_stop.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/login\_stop.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the login stop error page:  
**LOGIN\_ERR\_STOP=file:///opt/icewall-sso/dfw/html/login\_stop.html**
- 2) To set a local file as the login stop error page, the status code to “200,” and the status message to “Login Error”:  
**LOGIN\_ERR\_STOP=file:///opt/icewall-sso/dfw/html/login\_stop.html, 200,Login Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_UID  
LOGIN\_ERR\_PWD  
LOGIN\_ERR\_LOCK  
LOGIN\_ERR\_NOGRP  
LOGIN\_ERR\_LIMIT  
LOGIN\_ERR\_1STCERT  
LOGIN\_ERR\_SERIAL



## LOGIN\_ERR\_LIMIT <sup>(10.0)</sup>

**Overview** Sets the login limit error page that is displayed on a login attempt when the number of users currently logged in exceeds the number of users that can log in or when the maximum number of simultaneously logged in users is reached. <sup>(10.0)</sup>

The operation of this parameter has been slightly changed starting from version 10.0.

**Format** **LOGIN\_ERR\_LIMIT=storage location login limit error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/login\_limit\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/login\_limit\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the login limit error page:  
**LOGIN\_ERR\_LIMIT=file:///opt/icewall-ssso/dfw/html/login\_limit\_error.html**
- 2) To set a local file as the login limit error page, the status code to “200,” and the status message to “Login Error”:

---

HTML configuration file (html.conf)

---

**LOGIN\_ERR\_LIMIT=file:///opt/icewall-ssso/dfw/html/login\_limit\_error.html,200,Login Error**

Remarks

- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
- The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
- 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.
  - \* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
- When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

LOGIN\_ERR\_UID  
LOGIN\_ERR\_PWD  
LOGIN\_ERR\_LOCK  
LOGIN\_ERR\_NOGRP  
LOGIN\_ERR\_STOP  
LOGIN\_ERR\_1STCERT  
LOGIN\_ERR\_SERIAL  
CACHE (Authentication Module configuration file)

## LOGIN\_ERR\_POSTLIMIT <sup>(10.0)</sup>

**Overview** Sets the login transmission time limit error page displayed when POST data is transmitted after exceeding the time limit during logins including forced logins and the status code returned to the client.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGIN\_ERR\_POSTLIMIT=storage location login transmission time limit error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/login\_postlimit\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/login\_postlimit\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the login transmission time limit error page:  
**LOGIN\_ERR\_POSTLIMIT=file:///opt/icewall-sso/dfw/html/login\_postlimit\_error.html**
- 2) To set a local file as the login transmission time limit error page, the status code to “200,” and the status message to “Login Error”:  
**LOGIN\_ERR\_POSTLIMIT=file:///opt/icewall-sso/dfw/html/login\_postlimit\_error.html,200,Login Error**

---

HTML configuration file (html.conf)

---

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGIN_UID LOGIN_CERT LOGIN_FORCE

### 2.4.2 Access control related page parameters

These parameters are used to configure the HTML pages displayed when an access control error occurs.

Parameter name	Mandatory	Overview
ACCESS_DENY <small>(10.0)</small>	×	Sets the access privilege error page
DATA_SEND_ERR <small>(10.0)</small>	×	Sets the data send error page
REQUEST_ACL_ERR <small>(10.0)</small>	×	Sets the request ACL error page displayed when the connection to the Authentication Module was not permitted
FILTER_REQUEST <small>(10.0)</small>	×	Sets the request filter error page displayed when a request specifies a request type not available for accepting a request

For details on these parameters, see the following pages.

## ACCESS\_DENY <sup>(10.0)</sup>

**Overview** Sets the access privilege error page displayed when a request is made for a page for which the logged in user does not have permission to view.

Additional functionality of this parameter is available since version 10.0.

**Format** **ACCESS\_DENY=storage location access privilege error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/access\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the access privilege error page:  
**ACCESS\_DENY=file:///opt/icewall-sso/dfw/html/access\_error.html**
- 2) To set a local file as the access privilege error page, the status code to “200,” and the status message to “Access Deny”:  
**ACCESS\_DENY=file:///opt/icewall-sso/dfw/html/access\_error.html,200,Access Deny**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	DATA_SEND_ERR

## DATA\_SEND\_ERR <sup>(10.0)</sup>

**Overview** Sets the data send error page displayed when an attempt is made to send POST data to a Backend Web Server after the login has expired.

Additional functionality of this parameter is available since version 10.0.

**Format** **DATA\_SEND\_ERR=storage location data send error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/datasend\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/datasend\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the data send error page:  
**DATA\_SEND\_ERR=file:///opt/icewall-sso/dfw/html/datasend\_error.html**
- 2) To set a local file as the data send error page, the status code to “200,” and the status message to “Data Send Error”:  
**DATA\_SEND\_ERR=file:///opt/icewall-sso/dfw/html/datasend\_error.html,200,Data Send Error**



Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	ACCESS_DENY

## REQUEST\_ACL\_ERR 10.0

**Overview**                Sets the request ACL error page displayed when the connection to the Authentication Module was not permitted.

Additional functionality of this parameter is available since version 10.0.

**Format**                **DATA\_SEND\_ERR=storage location request ACL error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file://    : An HTML file on the local server
  - http://    : An HTML file on a remote server
  - https://   : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/request\_acl\_error.html .
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/request\_acl\_error.html .
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the request ACL error page:  
**REQUEST\_ACL\_ERR=file:///opt/icewall-ssso/dfw/html/request\_acl\_error.html**
- 2) To set a local file as the request ACL error page, the status code to “200,” and the status message to “RequestACL Error”:  
**REQUEST\_ACL\_ERR=file:///opt/icewall-ssso/dfw/html/request\_acl\_error.html,200,RequestACL Error**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	Request control configuration file

## FILTER\_REQUEST 10.0

**Overview** Sets the request filter error page displayed when a request specifies a request type not available for accepting access.

This parameter is available since version 10.0.

**Format** **FILTER\_REQUEST=storage location request filter error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/filter\_request\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/filter\_request\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the request filter error page:  
**FILTER\_REQUEST=file:///opt/icewall-ssso/dfw/html/filter\_request\_error.html**
- 2) To set a local file as the request filter error page, the status code to “200,” and the status message to “RequestFilter Error”:  
**FILTER\_REQUEST=file:///opt/icewall-ssso/dfw/html/filter\_request\_error.html,200, RequestFilter Error**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	REQUESTFILTER (Forwarder configuration file)

### 2.4.3 POST data inheritance related page parameters

This parameter is used for configuring the HTML page displayed if an error occurs in POST data inheritance.

Parameter name	Mandatory	Overview
MAXPOST_ERR (10.0)	×	Sets the POST data maximum size error page

For details on these parameters, see the following pages.

## MAXPOST\_ERR <sup>(10.0)</sup>

**Overview** Sets the POST data maximum size error page displayed and the status code that is returned to the client when, at login, the size of the inherited POST data exceeds the limit.

Additional functionality of this parameter is available since version 10.0.

**Format** **MAXPOST\_ERR=storage location POST data maximum size error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK.”
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/max\_postsize\_err.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/max\_postsize\_err.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file to the POST data maximum size error page:  
**MAXPOST\_ERR=file:///opt/icewall-sso/dfw/html/  
max\_postsize\_err.html**
- 2) To set a local file as the POST data maximum size error page, the status code to “200,” and the status message to “System Error”:  
**MAXPOST\_ERR=file:///opt/icewall-sso/dfw/html/  
max\_postsize\_err.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also            MAXPOST (Forwarder configuration file)



#### 2.4.4 Logout related page parameters

These parameters are used to configure the HTML pages displayed when logging out of IceWall.

Parameter name	Mandatory	Overview
LOGOUT <sup>(10.0)</sup>	×	Sets the logout page
LOGOUT_SUCCESS <sup>(10.0)</sup>	×	Sets the logout success page
LOGOUT_EXPIRE <sup>(10.0)</sup>	×	Sets the logged out page
LOGOUT_FAILURE <sup>(10.0)</sup>	×	Sets the logout error page

For details on these parameters, see the following pages.

# LOGOUT 10.0

**Overview** Sets the logout page displayed when a user logs out.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGOUT=storage location logout page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:  
   file:// : An HTML file on the local server  
   http:// : An HTML file on a remote server  
   https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/logout.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/logout.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the logout page:  
**LOGOUT=file:///opt/icewall-ssso/dfw/html/logout.html**
- 2) To set a local file as the logout page, the status code to “200,” and the status message to “IceWall Logout”:  
**LOGOUT=file:///opt/icewall-ssso/dfw/html/logout.html,200,IceWall Logout**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGOUT_SUCCESS LOGOUT_EXPIRE LOGOUT_FAILURE

## LOGOUT\_SUCCESS <sup>(10.0)</sup>

**Overview** Sets the logout success page displayed when the user performs a successful logout.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGOUT\_SUCCESS=storage location logout success page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/logout\_ok.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/logout\_ok.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the logout success page:  
**LOGOUT\_SUCCESS=file:///opt/icewall-sso/dfw/html/logout\_ok.html**
- 2) To set a local file as the logout success page, the status code to “200,” and the status message to “IceWall Logout”:  
**LOGOUT\_SUCCESS=file:///opt/icewall-sso/dfw/html/logout\_ok.html,200,IceWall Logout**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGOUT_EXPIRE LOGOUT_FAILURE

## LOGOUT\_EXPIRE <sup>(10.0)</sup>

Overview	<p>Sets the logged out page displayed when the user reattempts a logout after the process has already been completed.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>LOGOUT_EXPIRE=storage location logged out page file name[,status code][,status message]</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The following values can be set for the storage location:<ul style="list-style-type: none"><li>file:// : An HTML file on the local server</li><li>http:// : An HTML file on a remote server</li><li>https:// : An HTML file on a remote server (SSL)</li></ul></li><li>• Use status codes that are valid settings for web servers.</li><li>• The status message can use any selected character string up to a maximum of 255 bytes.</li><li>• The status code and status message are settable only when a local file is specified for the storage location.</li><li>• The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).</li><li>• The status code must also be set if a status message is set.</li><li>• The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/logout_no.html.</li><li>• The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/logout_no.html.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup></li></ul>
Configuration example	<p>1) To set a local file as the logged out page: <b>LOGOUT_EXPIRE=file:///opt/icewall-sso/dfw/html/logout_no.html</b></p> <p>2) To set a local file as the logged out page, the status code to “200,” and the status message to “IceWall Logout”: <b>LOGOUT_EXPIRE=file:///opt/icewall-sso/dfw/html/logout_no.html,200,IceWall Logout</b></p>

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGOUT_SUCCESS LOGOUT_FAILURE

## LOGOUT\_FAILURE <sup>(10.0)</sup>

**Overview** Sets the logout error page displayed when a logout fails.

Additional functionality of this parameter is available since version 10.0.

**Format** **LOGOUT\_FAILURE=storage location logout error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/logout\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/logout\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the logout error page:  
**LOGOUT\_FAILURE=file:///opt/icewall-ssso/dfw/html/logout\_error.html**
- 2) To set a local file as the logout error page, the status code to “200,” and the status message to “Logout Error”:  
**LOGOUT\_FAILURE=file:///opt/icewall-ssso/dfw/html/logout\_error.html,200,Logout Error**



Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	LOGOUT_SUCCESS LOGOUT_EXPIRE

### 2.4.5 Password change related page parameters

These parameters are used to configure the HTML pages displayed when changing IceWall passwords.

Parameter name	Mandatory	Overview
PWDCHG (10.0)	×	Sets the password change page
PWDCHG_SUCCESS (10.0)	×	Sets the password change success page
PWDCHG_ERR_OLD (10.0)	×	Sets the current password input error page
PWDCHG_ERR_REENT (10.0)	×	Sets the new password input error page
PWDCHG_ERR_POLICY (10.0)	×	Sets the password policy error page
PWDCHG_ERR_LOGNG (10.0)	×	Sets the no login error page
PWDCHG_ERR_VIO (10.0)	×	Sets the password change prohibited error page
PWDCHG_FAILURE (10.0)	×	Sets the password change failure page
PWDCHG_WARNING (10.0)	×	Sets the password expiration warning page
PWDCHG_ERR_POSTLIMIT (10.0)	×	Sets the password change transmission time limit error page displayed when POST data is transmitted after exceeding the time limit during password changes

For details on these parameters, see the following pages.

# PWDCHG <sup>(10.0)</sup>

Overview	<p>Sets the password change page displayed when changing passwords.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>PWDCHG=storage location password change page file name[,status code][,status message]</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The following values can be set for the storage location:<ul style="list-style-type: none"><li>file:// : An HTML file on the local server</li><li>http:// : An HTML file on a remote server</li><li>https:// : An HTML file on a remote server (SSL)</li></ul></li><li>• Use status codes that are valid settings for web servers.</li><li>• The status message can use any selected character string up to a maximum of 255 bytes.</li><li>• The status code and status message are settable only when a local file is specified for the storage location.</li><li>• The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).</li><li>• The status code must also be set if a status message is set.</li><li>• The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/pwdchg.html.</li><li>• The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/pwdchg.html.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup></li></ul>
Configuration example	<p>1) To set a local file as the password change page: <b>PWDCHG=file:///opt/icewall-ssso/dfw/html/pwdchg.html</b></p> <p>2) To set a local file as the password change page, the status code to “200,” and the status message to “IceWall Pwdchg”: <b>PWDCHG=file:///opt/icewall-ssso/dfw/html/pwdchg.html,200,IceWall Pwdchg</b></p>

---

HTML configuration file (html.conf)

---

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	None

# PWDCHG\_SUCCESS <sup>(10.0)</sup>

**Overview** Sets the password change success page displayed when a password is successfully changed.

Additional functionality of this parameter is available since version 10.0.

**Format** **PWDCHG=storage location password change success page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/pwdchg\_ok.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/pwdchg\_ok.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the password change success page:  
**PWDCHG\_SUCCESS=file:///opt/icewall-ssso/dfw/html/pwdchg\_ok.html**
- 2) To set a local file as the password change success page, the status code to “200,” and the status message to “IceWall Pwdchg”:  
**PWDCHG\_SUCCESS=file:///opt/icewall-ssso/dfw/html/pwdchg\_ok.html,200,IceWall Pwdchg**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_ERR\_OLD  
PWDCHG\_ERR\_REENT  
PWDCHG\_ERR\_POLICY  
PWDCHG\_ERR\_LOGNG  
PWDCHG\_ERR\_VIO  
PWDCHG\_FAILURE

## PWDCHG\_ERR\_OLD 10.0

### Overview

Sets the current password input error page displayed when the current password is incorrectly entered during a password change.

Additional functionality of this parameter is available since version 10.0.

### Format

**PWDCHG\_ERR\_OLD=storage location current password input error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// : An HTML file on the local server
  - http:// : An HTML file on a remote server
  - https:// : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/pwdchg\_oldpasserr.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/pwdchg\_oldpasserr.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

### Configuration example

- 1) To set a local file as the current password input error page:  
**PWDCHT\_ERR\_OLD=file:///opt/icewall-ssso/dfw/html/pwdchg\_oldpasserr.html**
- 2) To set a local file as the current password input error page, the status code to “200,” and the status message to “Pwdchg Error”:  
**PWDCHT\_ERR\_OLD=file:///opt/icewall-ssso/dfw/html/pwdchg\_oldpasserr.html,200,Pwdchg Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_SUCCESS  
PWDCHG\_ERR\_REENT  
PWDCHG\_ERR\_POLICY  
PWDCHG\_ERR\_LOGNG  
PWDCHG\_ERR\_VIO  
PWDCHG\_FAILURE



## PWDCHG\_ERR\_REENT <sup>(10.0)</sup>

Overview	<p>Sets the new password input error page displayed when the new password and confirmation password do not match during a password change.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>PWDCHG_ERR_REENT=storage location new password input error page file name[,status code][,status message]</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The following values can be set for the storage location:<ul style="list-style-type: none"><li>file:// : An HTML file on the local server</li><li>http:// : An HTML file on a remote server</li><li>https:// : An HTML file on a remote server (SSL)</li></ul></li><li>• Use status codes that are valid settings for web servers.</li><li>• The status message can use any selected character string up to a maximum of 255 bytes.</li><li>• The status code and status message are settable only when a local file is specified for the storage location.</li><li>• The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).</li><li>• The status code must also be set if a status message is set.</li><li>• The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/pwdchg_repasserr.html.</li><li>• The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/pwdchg_repasserr.html.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup></li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) To set a local file as the new password input error page: <b>PWDCHG_ERR_REENT=file:///opt/icewall-sso/dfw/html/pwdchg_repasserr.html</b></li><li>2) To set a local file as the new password input error page, the status code to “200,” and the status message to “Pwdchg Error”: <b>PWDCHG_ERR_REENT=file:///opt/icewall-sso/dfw/html/pwdchg_repasserr.html,200,Pwdchg Error</b></li></ol>

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_SUCCESS  
PWDCHG\_ERR\_OLD  
PWDCHG\_ERR\_POLICY  
PWDCHG\_ERR\_LOGNG  
PWDCHG\_ERR\_VIO  
PWDCHG\_FAILURE

## PWDCHG\_ERR\_POLICY 10.0

### Overview

Sets the password policy error page displayed when the new password violates the password policy during a password change.

Additional functionality of this parameter is available since version 10.0.

### Format

**PWDCHG\_ERR\_POLICY=storage location password policy error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/pwdchg\_policy\_err.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/pwdchg\_policy\_err.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

### Configuration example

- 1) To set a local file as the password policy error page:  
**PWDCHG\_ERR\_POLICY=file:///opt/icewall-ssso/dfw/html/pwdchg\_policy\_err.html**
- 2) To set a local file as the password policy error page, the status code to “200,” and the status message to “Pwdchg Error”:  
**PWDCHG\_ERR\_POLICY=file:///opt/icewall-ssso/dfw/html/pwdchg\_policy\_err.html,200,Pwdchg Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_SUCCESS  
PWDCHG\_ERR\_OLD  
PWDCHG\_ERR\_REENT  
PWDCHG\_ERR\_LOGNG  
PWDCHG\_ERR\_VIO  
PWDCHG\_FAILURE

## PWDCHG\_ERR\_LOGNG 10.0

### Overview

Sets the no login error page displayed when a forced logout due to timeout occurs during a password change.

Additional functionality of this parameter is available since version 10.0.

### Format

**PWDCHG\_ERR\_REENT=storage location no login error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/pwdchg\_nologin.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/pwdchg\_nologin.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

### Configuration example

- 1) To set a local file as the no login error page:  
**PWDCHG\_ERR\_LOGNG=file:///opt/icewall-ssso/dfw/html/pwdchg\_nologin.html**
- 2) To set a local file as the no login error page, the status code to “200,” and the status message to “Pwdchg Error”:  
**PWDCHG\_ERR\_LOGNG=file:///opt/icewall-ssso/dfw/html/pwdchg\_nologin.html,200,Pwdchg Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_SUCCESS  
PWDCHG\_ERR\_OLD  
PWDCHG\_ERR\_REENT  
PWDCHG\_ERR\_POLICY  
PWDCHG\_ERR\_VIO  
PWDCHG\_FAILURE

## PWDCHG\_ERR\_VIO 10.0

**Overview** Sets the password change prohibited error page displayed when a password change is attempted by a user who does not have permission to change passwords.

Additional functionality of this parameter is available since version 10.0.

**Format** **PWDCHG\_ERR\_VIO=storage location password change prohibited error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/pwdchg\_pwvioerr.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/pwdchg\_pwvioerr.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the password change prohibited error page:  
**PWDCHG\_ERR\_VIO=file:///opt/icewall-sso/dfw/html/pwdchg\_pwvioerr.html**
- 2) To set a local file as the password change prohibited error page, the status code to “200,” and the status message to “Pwdchg Error”:  
**PWDCHG\_ERR\_VIO=file:///opt/icewall-sso/dfw/html/pwdchg\_pwvioerr.html,200,Pwdchg Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_SUCCESS  
PWDCHG\_ERR\_OLD  
PWDCHG\_ERR\_REENT  
PWDCHG\_ERR\_POLICY  
PWDCHG\_ERR\_LOGNG  
PWDCHG\_FAILURE



## PWDCHG\_FAILURE 10.0

**Overview** Sets the password change failure page displayed when an error occurs on the Authentication Module during a password change.

Additional functionality of this parameter is available since version 10.0.

**Format** **PWDCHG\_FAILURE=storage location password change failure page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/pwdchg\_err.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/pwdchg\_err.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the password change failure page:  
**PWDCHG\_FAILURE=file:///opt/icewall-ssso/dfw/html/pwdchg\_err.html**
- 2) To set a local file as the password change failure page, the status code to “200,” and the status message to “Pwdchg Error”:  
**PWDCHG\_FAILURE=file:///opt/icewall-ssso/dfw/html/pwdchg\_err.html,200,Pwdchg Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_SUCCESS  
PWDCHG\_ERR\_OLD  
PWDCHG\_ERR\_REENT  
PWDCHG\_ERR\_POLICY  
PWDCHG\_ERR\_LOGNG  
PWDCHG\_ERR\_VIO

## PWDCHG\_WARNING ⑩.0

Overview	<p>Sets the password expiration warning page displayed for password expiration warnings.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>PWDCHG_WARNING=storage location password expiration warning page file name[,status code][,status message]</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The following values can be set for the storage location:<ul style="list-style-type: none"><li>file:// :An HTML file on the local server</li><li>http:// :An HTML file on a remote server</li><li>https:// :An HTML file on a remote server (SSL)</li></ul></li><li>• Use status codes that are valid settings for web servers.</li><li>• The status message can use any selected character string up to a maximum of 255 bytes.</li><li>• The status code and status message are settable only when a local file is specified for the storage location.</li><li>• The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).</li><li>• The status code must also be set if a status message is set.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is file:///opt/icewall-ss0/dfw/html/pwdchg_warning.html.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). ⑩.0</li></ul>
Configuration example	<p>1) To set a local file as the password expiration warning page: <b>PWDCHG_WARNING=file:///opt/icewall-ss0/dfw/html/pwdchg_warning.html</b></p> <p>2) To set a local file as the password expiration warning page, the status code to “200,” and the status message to “IceWall Pwdchg”: <b>PWDCHG_WARNING=file:///opt/icewall-ss0/dfw/html/pwdchg_warning.html,200,IceWall Pwdchg</b></p>

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG\_SUCCESS  
PWDCHG\_ERR\_OLD  
PWDCHG\_ERR\_REENT  
PWDCHG\_ERR\_POLICY  
PWDCHG\_ERR\_LOGNG  
PWDCHG\_ERR\_VIO  
PWDCHG\_FAILURE  
PWDEXPWARN (Authentication Module configuration file)

## PWDCHG\_ERR\_POSTLIMIT 10.0

Overview	<p>Sets the password change transmission time limit error page displayed when POST data is transmitted after exceeding the time limit during password changes and the status code returned to the client.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>PWDCHG_ERR_POSTLIMIT=storage location password change transmission time limit error page file name[,status code][,status message]</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The following values can be set for the storage location:<ul style="list-style-type: none"><li>file:// :An HTML file on the local server</li><li>http:// :An HTML file on a remote server</li><li>https:// :An HTML file on a remote server (SSL)</li></ul></li><li>• Use status codes that are valid settings for web servers.</li><li>• The status message can use any selected character string up to a maximum of 255 bytes.</li><li>• The status code and status message are settable only when a local file is specified for the storage location.</li><li>• The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).</li><li>• The status code must also be set if a status message is set.</li><li>• The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/pwdchg_postlimit_err.html.</li><li>• The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/pwdchg_postlimit_err.html.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <span style="border: 1px solid black; border-radius: 50%; padding: 0 2px;">10.0</span></li></ul>
Configuration example	<p>1) To set a local file as the password change transmission time limit error page:</p> <p><b>PWDCHG_ERR_POSTLIMIT=file:///opt/icewall-sso/dfw/html/pwdchg_postlimit_err.html</b></p>

---

HTML configuration file (html.conf)

---

- 2) To set a local file as the password change transmission time limit error page, the status code to “200,” and the status message to “Pwdchg Error”:

**PWDCHG\_ERR\_POSTLIMIT=file:///opt/icewall-ssso/dfw/html/  
pwdchg\_postlimit\_err.html,200,Pwdchg Error**

Remarks

- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
- The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
- 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.
  - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
- When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

PWDCHG

#### 2.4.6 Cross site scripting error related page parameters

These parameters are used to configure the HTML pages displayed, which would normally be filtered, when there is a possibility of cross site scripting in POST data or HTML that passes through IceWall.

Parameter name	Mandatory	Overview
FILTER_GET <a href="#">10.0</a>	×	Sets the GET filter error page
FILTER_POST <a href="#">10.0</a>	×	Sets the POST filter error page
FILTER_HTML <a href="#">10.0</a>	×	Sets the HTML filter error page
FILTER_SVR <a href="#">10.0</a>	×	Sets the HOST filter error page

For details on these parameters, see the following pages.

## FILTER\_GET 10.0

**Overview** Sets the GET filter error page displayed, in place of filtering, when there is cross site scripting within a QUERYSTRING sent to a Backend Web Server.

Additional functionality of this parameter is available since version 10.0.

**Format** **FILTER\_GET=storage location GET filter error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/filter\_get\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/filter\_get\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the GET filter error page:  
**FILTER\_GET=file:///opt/icewall-sso/dfw/html/filter\_get\_error.html**
- 2) To set a local file as the GET filter error page, the status code to “200,” and the status message to “Filter Error”:  
**FILTER\_GET=file:///opt/icewall-sso/dfw/html/filter\_get\_error.html,200,Filter Error**



Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	GETFILTERERR (host configuration file) FILTER_POST FILTER_HTML FILTER_SVR

## FILTER\_POST <sup>(10.0)</sup>

**Overview** Sets the POST filter error page displayed, in place of filtering, when there is cross site filtering within POST data sent to a Backend Web Server.

Additional functionality of this parameter is available since version 10.0.

**Format** **FILTER\_GET=storage location POST filter error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:  
file:// :An HTML file on the local server  
http:// :An HTML file on a remote server  
https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/filter\_post\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/filter\_post\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the POST filter error page:  
**FILTER\_POST=file:///opt/icewall-sso/dfw/html/filter\_post\_error.html**
- 2) To set a local file as the POST filter error page, the status code to “200,” and the status message to “Filter Error”:  
**FILTER\_POST=file:///opt/icewall-sso/dfw/html/filter\_post\_error.html,200,Filter Error**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	POSTFILTERERR (host configuration file) FILTER_GET FILTER_HTML FILTER_SVR

## **FILTER\_HTML** ⑩.0

**Overview** Sets the HTML filter error page displayed, in place of filtering, when there is cross site scripting on a link in the content received from a Backend Web Server.

Additional functionality of this parameter is available since version 10.0.

**Format** **FILTER\_HTML=storage location HTML filter error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/filter\_html\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/filter\_html\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). ⑩.0

**Configuration example**

- 1) To set a local file as the HTML filter error page:  
**FILTER\_HTML=file:///opt/icewall-sso/dfw/html/filter\_html\_error.html**
- 2) To set a local file as the HTML filter error page, the status code to “200,” and the status message to “Filter Error”:  
**FILTER\_HTML=file:///opt/icewall-sso/dfw/html/filter\_html\_error.html,200,Filter Error**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	HTMLFILTERERR (host configuration file) FILTER_GET FILTER_POST FILTER_SVR

## **FILTER\_SVR** ⑩.0

**Overview** Sets the HOST filter error page displayed, in place of filtering, when there is an undefined host in the content received from a Backend Web Server.

Additional functionality of this parameter is available since version 10.0.

**Format** **FILTER\_SVR=storage location HOST filter error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/filter\_svr\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/filter\_svr\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). ⑩.0

**Configuration example**

- 1) To set a local file as the HOST filter error page:  
**FILTER\_SVR=file:///opt/icewall-sso/dfw/html/filter\_svr\_error.html**
- 2) To set a local file as the HOST filter error page, the status code to “200,” and the status message to “Filter Error”:  
**FILTER\_SVR=file:///opt/icewall-sso/dfw/html/filter\_svr\_error.html,200,Filter Error**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual.<a href="#">(10.0)</a></li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	<p>SVRFILTERERR (host configuration file) FILTER_GET FILTER_POST FILTER_HTML</p>

### 2.4.7 System error related page parameters

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

Parameter name	Mandatory	Overview
SYSTEM_ERR 10.0	×	Sets the system error page
SYSTEM_ERR_NOALIAS 10.0	×	Sets the no alias error page
SYSTEM_ERR_BADALIAS 10.0	×	Sets the undefined alias error page
SYSTEM_DOWN_CERTD 10.0	×	Sets the Authentication Module down error page
SYSTEM_DOWN_DB 10.0	×	Sets the Authentication DB down error page
SYSTEM_DOWN_HTTP 10.0	×	Sets the Backend Web Server down error page
SYSTEM_TOUT_CERTD 10.0	×	Sets the Authentication Module timeout error page
SYSTEM_TOUT_HTTP 10.0	×	Sets the Backend Web Server timeout error page
SYSTEM_BUSY_DB 10.0	×	Sets the database busy error page displayed when processing cannot be performed on the Authentication Module because there are too many accesses to the database connection

For details on these parameters, see the following pages.



## SYSTEM\_ERR <sup>(10.0)</sup>

**Overview** Sets the system error page displayed when an error occurs in Forwarder or the Authentication Module.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSTEM\_ERR=storage location system error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/system\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the system error page:  
**SYSTEM\_ERR=file:///opt/icewall-ssso/dfw/html/system\_error.html**
- 2) To set a local file as the system error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_ERR=file:///opt/icewall-ssso/dfw/html/system\_error.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSTEM\_ERR\_NOALIAS  
SYSTEM\_ERR\_BADALIAS  
SYSTEM\_DOWN\_CERTD  
SYSTEM\_DOWN\_DB  
SYSTEM\_DOWN\_HTTP  
SYSTEM\_TOUT\_CERTD  
SYSTEM\_TOUT\_HTTP

## SYSTEM\_ERR\_NOALIAS 10.0

**Overview** Sets the no alias error page displayed when no alias name is included in a URL requested by a client.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSTEM\_ERR\_NOALIAS=storage location no alias error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/system\_server\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_server\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the no alias error page:  
**SYSTEM\_ERR\_NOALIAS=file:///opt/icewall-ssso/dfw/html/system\_server\_error.html**
- 2) To set a local file as the no alias error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_ERR\_NOALIAS=file:///opt/icewall-ssso/dfw/html/system\_server\_error.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSTEM\_ERR  
SYSTEM\_ERR\_BADALIAS  
SYSTEM\_DOWN\_CERTD  
SYSTEM\_DOWN\_DB  
SYSTEM\_DOWN\_HTTP  
SYSTEM\_TOUT\_CERTD  
SYSTEM\_TOUT\_HTTP

## SYSTEM\_ERR\_BADALIAS 10.0

**Overview** Sets the undefined alias error page displayed when a URL that does not include an alias name set by Forwarder is requested by a client.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSTEM\_ERR\_BADALIAS=storage location undefined alias error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/system\_alias\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_alias\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the undefined alias error page:  
**SYSTEM\_ERR\_BADALIAS=file:///opt/icewall-ssso/dfw/html/system\_alias\_error.html**
- 2) To set a local file as the undefined alias error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_ERR\_BADALIAS=file:///opt/icewall-ssso/dfw/html/system\_alias\_error.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSTEM\_ERR  
SYSTEM\_ERR\_NOALIAS  
SYSTEM\_DOWN\_CERTD  
SYSTEM\_DOWN\_DB  
SYSTEM\_DOWN\_HTTP  
SYSTEM\_TOUT\_CERTD  
SYSTEM\_TOUT\_HTTP

## SYSTEM\_DOWN\_CERTD 10.0

**Overview** Sets the Authentication Module down error page displayed when Forwarder attempts to communicate with a downed Authentication Module.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSTEM\_DOWN\_CERTD=storage location authentication module down error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/system\_certd\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/system\_certd\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the Authentication Module down error page:  
**SYSTEM\_DOWN\_CERTD=file:///opt/icewall-sso/dfw/html/system\_certd\_error.html**
- 2) To set a local file as the Authentication Module down error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_DOWN\_CERTD=file:///opt/icewall-sso/dfw/html/system\_certd\_error.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSTEM\_ERR  
SYSTEM\_ERR\_NOALIAS  
SYSTEM\_ERR\_BADALIAS  
SYSTEM\_DOWN\_DB  
SYSTEM\_DOWN\_HTTP  
SYSTEM\_TOUT\_CERTD  
SYSTEM\_TOUT\_HTTP



## SYSTEM\_DOWN\_DB <sup>(10.0)</sup>

**Overview** Sets the Authentication DB down error page displayed if the Authentication DB is down when accessed by the Authentication Module.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSTEM\_DOWN\_DB=storage location authentication DB down error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/system\_ldap\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_ldap\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the Authentication DB down error page:  
**SYSTEM\_DOWN\_DB=file:///opt/icewall-ssso/dfw/html/system\_ldap\_error.html**
- 2) To set a local file as the Authentication DB down error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_DOWN\_DB=file:///opt/icewall-ssso/dfw/html/system\_ldap\_error.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSTEM\_ERR  
SYSTEM\_ERR\_NOALIAS  
SYSTEM\_ERR\_BADALIAS  
SYSTEM\_DOWN\_CERTD  
SYSTEM\_DOWN\_HTTP  
SYSTEM\_TOUT\_CERTD  
SYSTEM\_TOUT\_HTTP

## SYSTEM\_DOWN\_HTTP <sup>(10.0)</sup>

### Overview

Sets the Backend Web Server down error page displayed when Forwarder attempts to connect to a downed Backend Web Server.

Additional functionality of this parameter is available since version 10.0.

### Format

**SYSTEM\_DOWN\_HTTP=storage location backend web server down error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/system\_backend\_error.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_backend\_error.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

### Configuration example

- 1) To set a local file as the Backend Web Server down error page:  
**SYSTEM\_DOWN\_HTTP=file:///opt/icewall-ssso/dfw/html/system\_backend\_error.html**
- 2) To set a local file as the Backend Web Server down error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_DOWN\_HTTP=file:///opt/icewall-ssso/dfw/html/system\_backend\_error.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - This parameter specifies the common error page displayed when Forwarder attempts to connect to a downed Backend Web Server. Use the SYSERR parameter in the host configuration file to set an error page specific to each Backend Web Server.
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSERR (host configuration file)  
SYSTEM\_ERR  
SYSTEM\_ERR\_NOALIAS  
SYSTEM\_ERR\_BADALIAS  
SYSTEM\_DOWN\_CERTD  
SYSTEM\_DOWN\_DB  
SYSTEM\_TOUT\_CERTD  
SYSTEM\_TOUT\_HTTP

## SYSTEM\_TOUT\_CERTD <sup>10.0</sup>

**Overview** Sets the Authentication Module timeout error page displayed if a timeout occurs when Forwarder is communicating with the Authentication Module and waiting for a response message.

Additional functionality of this parameter is available since version 10.0.

**Format** **SYSTEM\_TOUT\_CERTD=storage location authentication module timeout error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/system\_timeout\_certd.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_timeout\_certd.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>10.0</sup>

**Configuration example**

- 1) To set a local file as the Authentication Module timeout error page:  
**SYSTEM\_TOUT\_CERTD=file:///opt/icewall-ssso/dfw/html/system\_timeout\_certd.html**
- 2) To set a local file as the Authentication Module timeout error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_TOUT\_CERTD=file:///opt/icewall-ssso/dfw/html/system\_timeout\_certd.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSTEM\_ERR  
SYSTEM\_ERR\_NOALIAS  
SYSTEM\_ERR\_BADALIAS  
SYSTEM\_DOWN\_CERTD  
SYSTEM\_DOWN\_DB  
SYSTEM\_DOWN\_HTTP  
SYSTEM\_TOUT\_HTTP

## SYSTEM\_TOUT\_HTTP ⑩.0

### Overview

Sets the Backend Web Server timeout error page displayed if a timeout occurs when Forwarder is communicating with a Backend Web Server and waiting for a response message.

Additional functionality of this parameter is available since version 10.0.

### Format

**SYSTEM\_TOUT\_HTTP=storage location backend web server timeout error page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-sso/dfw/html/system\_timeout\_bkend.html.
- The initial value set in the standard configuration file is file:///opt/icewall-sso/dfw/html/system\_timeout\_bkend.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). ⑩.0

### Configuration example

- 1) To set a local file as the Backend Web Server timeout error page:  
**SYSTEM\_TOUT\_HTTP=file:///opt/icewall-sso/dfw/html/system\_timeout\_bkend.html**
- 2) To set a local file as the Backend Web Server timeout error page, the status code to “200,” and the status message to “System Error”:  
**SYSTEM\_TOUT\_HTTP=file:///opt/icewall-sso/dfw/html/system\_timeout\_bkend.html,200,System Error**

---

HTML configuration file (html.conf)

---

- Remarks
- For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)
  - This parameter specifies the common error page displayed if a timeout occurs when IceWall is communicating with a Backend Web Server and waiting for a response message. Use the SYSTOUT parameter in the host configuration file to set an error page specific to each Backend Web Server.
  - The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.
  - 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.
    - \* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”
  - When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.

See also

SYSTOUT (host configuration file)  
SYSTEM\_ERR  
SYSTEM\_ERR\_NOALIAS  
SYSTEM\_ERR\_BADALIAS  
SYSTEM\_DOWN\_CERTD  
SYSTEM\_DOWN\_DB  
SYSTEM\_DOWN\_HTTP  
SYSTEM\_TOUT\_CERTD



## SYSTEM\_BUSY\_DB 10.0

**Overview** Sets the database busy error page displayed when processing cannot be performed on the Authentication Module because there are too many accesses to the database connection.

This parameter is available since version 10.0.

**Format** **SYSTEM\_BUSY\_DB=storage location database busy error page file name [,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file:// :An HTML file on the local server
  - http:// :An HTML file on a remote server
  - https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/system\_busy\_database.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/system\_busy\_database.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the database busy error page:  
**SYSTEM\_BUSY\_DB=file:///opt/icewall-ssso/dfw/html/system\_busy\_database.html**
- 2) To set a local file as the database busy error page, the status code to “200,” and the status message to “DatabaseBusy Error”:  
**SYSTEM\_BUSY\_DB=file:///opt/icewall-ssso/dfw/html/system\_busy\_database.html,200,DatabaseBusy Error**

---

HTML configuration file (html.conf)

---

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	None

### 2.4.8 User defined error related page parameters

These parameters are used to configure the HTML pages, defined by users, that contain UserExit routines usable by Forwarder and the Authentication Module.

Parameter name	Mandatory	Overview
USREXT_ERR1 <a href="#">10.0</a>	×	Sets the user-defined error 1 page
USREXT_ERR2 <a href="#">10.0</a>	×	Sets the user-defined error 2 page
USREXT_ERR3 <a href="#">10.0</a>	×	Sets the user-defined error 3 page
USREXT_ERR4 <a href="#">10.0</a>	×	Sets the user-defined error 4 page
USREXT_ERR5 <a href="#">10.0</a>	×	Sets the user-defined error 5 page
USREXT_ERR6 <a href="#">10.0</a>	×	Sets the user-defined error 6 page

For details on these parameters, see the following pages.

# USREXT\_ERR1 <sup>(10.0)</sup>

**Overview** Sets the user-defined error 1 page defined in the Authentication Module UserExit routine.

Additional functionality of this parameter is available since version 10.0.

**Format** **USREXT\_ERR1=storage location user defined error 1 page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:  
   file:// :An HTML file on the local server  
   http:// :An HTML file on a remote server  
   https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/usr\_ext1.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/usr\_ext1.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value set in the standard configuration file is out of range, the default value is used.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). <sup>(10.0)</sup>

**Configuration example**

- 1) To set a local file as the user-defined error 1 page:  
**USREXT\_ERR1=file:///opt/icewall-ssso/dfw/html/usr\_ext1.html**
- 2) To set a local file as the user-defined error 1 page, the status code to “200,” and the status message to “UserExit”:  
**USREXT\_ERR1=file:///opt/icewall-ssso/dfw/html/  
 usr\_ext1.html,200,UserExit**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	USREXT_ERR2 USREXT_ERR3 USREXT_ERR4 USREXT_ERR5 USREXT_ERR6

## USREXT\_ERR2 10.0

**Overview** Sets the user-defined error 2 page defined in the Authentication Module UserExit routine.

Additional functionality of this parameter is available since version 10.0.

**Format** **USREXT\_ERR2=storage location user defined error 2 page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:  
 file:// :An HTML file on the local server  
 http:// :An HTML file on a remote server  
 https:// :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/usr\_ext2.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/usr\_ext2.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the user-defined error 2 page:  
**USREXT\_ERR2=file:///opt/icewall-ssso/dfw/html/usr\_ext2.html**
- 2) To set a local file as the user-defined error 2 page, the status code to “200,” and the status message to “UserExit”:  
**USREXT\_ERR2=file:///opt/icewall-ssso/dfw/html/  
usr\_ext2.html,200,UserExit**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	USREXT_ERR1 USREXT_ERR3 USREXT_ERR4 USREXT_ERR5 USREXT_ERR6

## USREXT\_ERR3 10.0

**Overview**                Sets the user-defined error 3 page defined in the Authentication Module UserExit routine.

Additional functionality of this parameter is available since version 10.0.

**Format**                **USREXT\_ERR3=storage location user defined error 3 page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file://    :An HTML file on the local server
  - http://    :An HTML file on a remote server
  - https://   :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/usr\_ext3.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/usr\_ext3.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the user-defined error 3 page:  
**USREXT\_ERR3=file:///opt/icewall-ssso/dfw/html/usr\_ext3.html**
- 2) To set a local file as the user-defined error 3 page, the status code to “200,” and the status message to “UserExit”:  
**USREXT\_ERR3=file:///opt/icewall-ssso/dfw/html/  
usr\_ext3.html,200,UserExit**



Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual.<a href="#">(10.0)</a></li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	USREXT_ERR1 USREXT_ERR2 USREXT_ERR4 USREXT_ERR5 USREXT_ERR6

## USREXT\_ERR4 10.0

**Overview**                Sets the user-defined error 4 page defined in the Authentication Module UserExit routine.

Additional functionality of this parameter is available since version 10.0.

**Format**                **USREXT\_ERR4=storage location user defined error 4 page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file://    :An HTML file on the local server
  - http://    :An HTML file on a remote server
  - https://   :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/usr\_ext4.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/usr\_ext4.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the user-defined error 4 page:  
**USREXT\_ERR4=file:///opt/icewall-ssso/dfw/html/usr\_ext4.html**
- 2) To set a local file as the user-defined error 4 page, the status code to “200,” and the status message to “UserExit”:  
**USREXT\_ERR4=file:///opt/icewall-ssso/dfw/html/  
usr\_ext4.html,200,UserExit**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	USREXT_ERR1 USREXT_ERR2 USREXT_ERR3 USREXT_ERR5 USREXT_ERR6

## USREXT\_ERR5 10.0

**Overview**                Sets the user-defined error 5 page defined in the Authentication Module UserExit routine.

Additional functionality of this parameter is available since version 10.0.

**Format**                **USREXT\_ERR5=storage location user defined error 5 page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file://    :An HTML file on the local server
  - http://    :An HTML file on a remote server
  - https://   :An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/usr\_ext5.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/usr\_ext5.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the user-defined error 5 page:  
**USREXT\_ERR5=file:///opt/icewall-ssso/dfw/html/usr\_ext5.html**
- 2) To set a local file as the user-defined error 5 page, the status code to “200,” and the status message to “UserExit”:  
**USREXT\_ERR5=file:///opt/icewall-ssso/dfw/html/  
usr\_ext5.html,200,UserExit**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the special keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	USREXT_ERR1 USREXT_ERR2 USREXT_ERR3 USREXT_ERR4 USREXT_ERR6

## USREXT\_ERR6 10.0

**Overview**                Sets the user-defined error 6 page defined in the Authentication Module UserExit routine.

Additional functionality of this parameter is available since version 10.0.

**Format**                **USREXT\_ERR6=storage location user defined error 6 page file name[,status code][,status message]**

- The file name has a maximum length of 255 bytes.
- The following values can be set for the storage location:
  - file://    :An HTML file on the local server
  - http://    :An HTML file on a remote server
  - https://   : An HTML file on a remote server (SSL)
- Use status codes that are valid settings for web servers.
- The status message can use any selected character string up to a maximum of 255 bytes.
- The status code and status message are settable only when a local file is specified for the storage location.
- The status code and status message are optional. When both of these are omitted, the status code defaults to “200,” and the status message defaults to “OK” (backward compatibility).
- The status code must also be set if a status message is set.
- The default value set in the executable binary file is file:///opt/icewall-ssso/dfw/html/usr\_ext6.html.
- The initial value set in the standard configuration file is file:///opt/icewall-ssso/dfw/html/usr\_ext6.html.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- When connecting to the remote server in IPv6 format, enclose the host name or IP address in square brackets ([ ]). 10.0

**Configuration example**

- 1) To set a local file as the user-defined error 6 page:  
**USREXT\_ERR6=file:///opt/icewall-ssso/dfw/html/usr\_ext6.html**
- 2) To set a local file as the user-defined error 6 page, the status code to “200,” and the status message to “UserExit”:  
**USREXT\_ERR6=file:///opt/icewall-ssso/dfw/html/  
usr\_ext6.html,200,UserExit**

Remarks	<ul style="list-style-type: none"><li>• For details about connections in the IPv6 format, see “8.2 IPv6 support in Forwarder” in the User's Manual. (10.0)</li><li>• The “IceWall SSO SSL Option” is required to set SSL servers in this parameter.</li><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.<ul style="list-style-type: none"><li>* For information about the specific keyword conversion function, see the “IceWall SSO Web Application Developer's Manual.”</li></ul></li><li>• When setting the content on the remote server, its Content-type should be text/html. Error may result if another type of content is set.</li></ul>
See also	USREXT_ERR1 USREXT_ERR2 USREXT_ERR3 USREXT_ERR4 USREXT_ERR5

### 3 Authentication Module

The Authentication Module uses the following seven configuration files.

- Authentication Module configuration file
- Group configuration file
- Access control file
- Authentication DB column information file
- Log column information file
- Forbidden password configuration file
- Request control configuration file

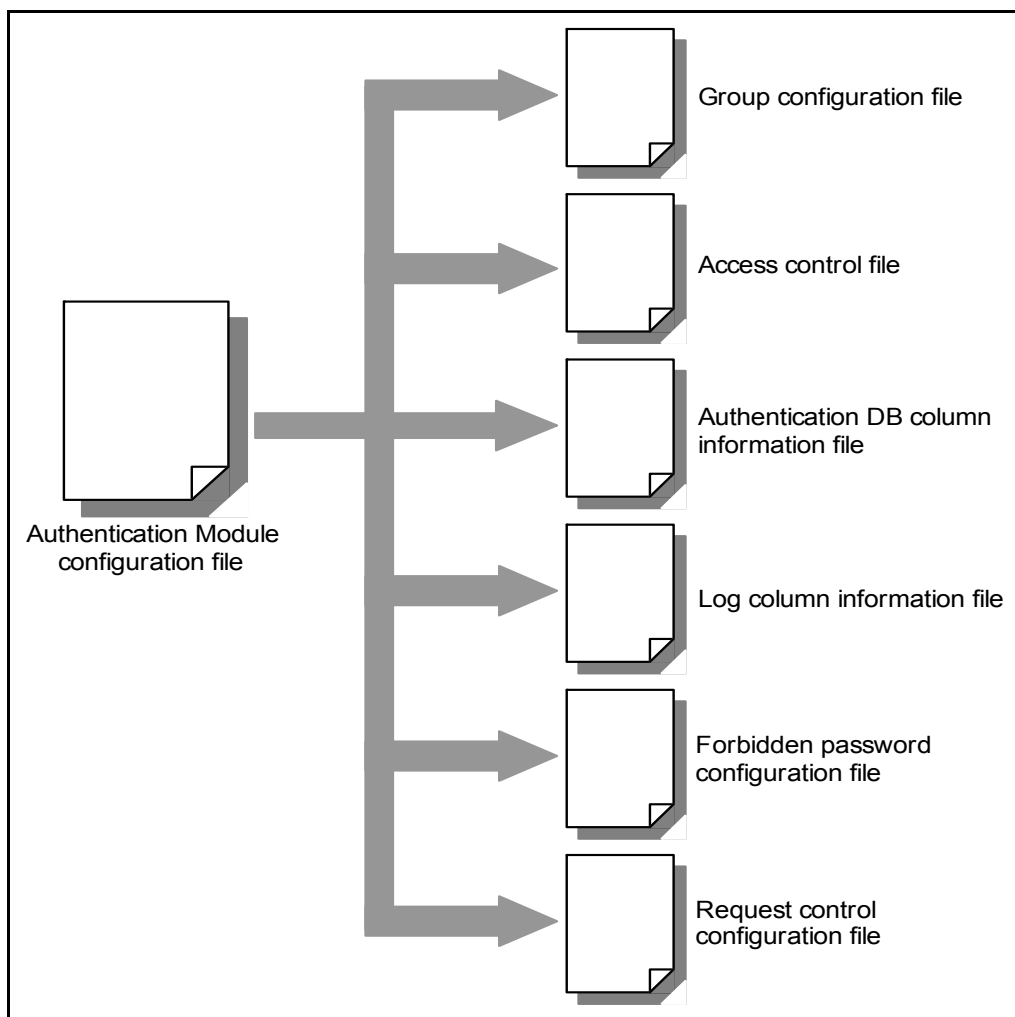


Diagram of configuration file relationships

Six Authentication Module commands have also been provided to perform operations such as starting and stopping the Authentication Module.

- Startup command (start-cert)
- Stop command (end-cert)
- Operating information output command (info-cert)
- Reload command (reload-cert)



- Log out all users command (logout-cert)
- Configuration file information output command (cdump-cert)

This chapter describes the parameters in these configuration files and options for the commands.

\* Configuration values when using a replication configuration

When using a replication configuration, configuration parameter values are downloaded and synchronized between the two Authentication Modules to make the operation of the Primary and Secondary Authentication Modules be the same. In this chapter, it is described whether each parameter is the object parameter of downloading or synchronization in the description for the parameter in each configuration file. Consider these when executing the commands.

- Downloading

When executing the startup command (start-cert), the configuration parameter values are set to download to the same values as the values configured in the replication target Authentication Module configuration parameters.

If replication target Authentication Module is not running, those parameters are not downloaded.

- Synchronization

When executing the reload command (reload-cert), the configuration parameter values are set to download to the same values as the values configured in the replication target Authentication Module configuration parameters.

If replication target Authentication Module is not running, those parameters are not downloaded.

---

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


---

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

This configuration file configures the values needed to run the Authentication Module, as well as the shared settings used by the entire system.

Parameters available to the user are as follows:

Parameter group	Parameter name
Basic configuration parameters	ALEVEL
	ELEVEL
	ACCESS
	ERROR
	TRACE
	CATALOG (10.0)
	LOGINFO
	LOGPERF
	TRANSID (10.0)
	PERFORMANCE
	INFORMATION
	PORT
	IPV6LISTEN (10.0)
	HTTPPORT (10.0)
	HTTPECHOHEADER (10.0)
Access control related parameters	GROUP
	ACL
	ACLREQUEST
	ADGROUP
	ADGROUPDN
	ADGROUPINTERVAL
	ADGROUPPRINAME
	ADGROUPPREFIX
	ADGROUPMAXMEMBER
Session policy related parameters	COOKIERETRY
	COOKIETIME
	COOKIEEXP
	LOMETHOD
	DUPLOGIN
	DUPKIND
	PARALOGIN
	ACCCTRLFLG
	SESSIONIDLEN (10.0)
	CERTUNIQUEKEY (10.0)

## Authentication Module configuration file (cert.conf)

Parameter group	Parameter name
Password policy related parameters	PWDLOGINHASH <b>10.0</b>
	PWDCHGHASH <b>10.0</b>
	PWDMINLEN <b>10.0</b>
	PWDMAXLEN <b>10.0</b>
	PWDALPHANUM <b>10.0</b>
	PWDEXPIRE <b>10.0</b>
	PWDSAMEPASS <b>10.0</b>
	LOCKCOUNT
	PWDEXPCHK
	PWDHISCHK
	PWDHISCNT
	PWDFORBID
	PWDEXPWARN
Authentication DB related parameters	DBHOST <b>10.0</b>
	DBUID <small>Overwrite</small>
	DBPWD <small>Overwrite</small>
	DBTBL
	DBATTR
	DBEXATTR
	DBCRYPTOTYPE <b>10.0</b>
	DBIWCRYPTOSEED <b>10.0</b>
	DBCRYPTOATTR <b>10.0</b>
	LDAPBIND
	LDAPPCHG
	LDAPLANG
	LDAPSSL
	LDAPCACERT
	LDAPVERIFYSVRCERT
	LDAPCIPHERSUITE
	LDAPSSLBIND
	ADPCHG
	LDAPMULTIVAL
	LDAPREFERRAL
	ADDGFWBIND
Audit log table related parameters (For ORACLE edition only)	LOGDBTBL
	LOGDBATTR
	LOGDBSEQNAME
Reference table related parameters (For ORACLE and MySQL editions only)	REFTBL
	REFATTR
	REFUID

## Authentication Module configuration file (cert.conf)

Parameter group	Parameter name
System tuning related parameters	MAXREQTHREAD
	ACCTHREAD <b>10.0</b>
	REQQESIZE
	MAXDBCONNECT
	DBQUESIZE <b>10.0</b>
	LOGDBQUESIZE <b>10.0</b>
	LOGBUFSIZE
	CACHE
	MAXLOGINUSER <b>10.0</b>
	RECVWAITTIME
	THREADSTACKSIZE
	LOGMULTITHREAD <b>10.0</b>
	DOWNLOADCONFFLG <b>10.0</b>
Replication related parameters	CERT <b>10.0</b>
	CERTREPTYPE
	RETRYCNTC
	RETRYTMC
	LIVETIMER
	HEALTHTIMER
	HEALTHCNT
	FAILBACK <b>10.0</b>
	MAXREPTHREAD
	REPQUESIZE

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

**Remarks**      None

The following pages describe these parameters.

### 3.1.1 Basic configuration parameters

These parameters are shared over the entire system and used to run the Authentication Module.

Parameter name	Mandatory	Overview
ALEVEL	×	Sets the access log output level
ELEVEL	×	Sets the error log output level
ACCESS	×	Sets the access log file
ERROR	×	Sets the error log file
TRACE	×	Sets the trace log file
CATALOG	×	Sets the message catalog
LOGINFO	×	Sets the request sender information output
LOGPERF	×	Sets the request process elapsed time output
TRANSID <b>10.0</b>	×	Sets whether or not to output transaction ID information sent to the Authentication Module in the access log, error log, and performance log
PERFORMANCE	×	Sets the performance log file
INFORMATION	×	Sets the information log file
PORT	×	Sets the listen port number
IPV6LISTEN <b>10.0</b>	×	Sets the IP version for requests received by the Authentication Module
HTTPPORT <b>10.0</b>	×	Sets the port number for receiving HTTP requests
HTTPECHOHEADER <b>10.0</b>	×	Sets whether or not to append the header sent from the client to the header of response when using HTTP

For details on these parameters, see the following pages.

# ALEVEL

Overview                Sets the access log output level.

Format                 **ALEVEL=access log level**

- Set this parameter to one of the following values:
  - 0 : No output
  - 1 : Fatal and performance related information (Fatal)
  - 2 : Fatal information, performance related information, and warnings (Warning)
  - 3 : Includes all information (Information)
- The default value set in the executable binary file is 1.
- The initial value set in the standard configuration file is 1.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

Configuration example    1) To set the access log output level to 1:  
                              **ALEVEL=1**

Remarks                • This parameter is subject to the reload command (reload-cert).

                              • This parameter is not downloaded at startup when using a replication configuration.

See also                ACCESS (Authentication Module configuration file)  
                              LOGPERF  
                              INFORMATION

# ELEVEL

Overview                Sets the error log output level.

Format                 **ELEVEL=error log level**

- Set this parameter to one of the following values:
  - 0 : No output
  - 1 : Fatal information only (Fatal)
  - 2 : Includes fatal information and warnings (Warning)
  - 3 : Includes all information (Information)
- The default value set in the executable binary file is 1.
- The initial value set in the standard configuration file is 1.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

Configuration example    1) To set the error log output level to 1:  
                              **ELEVEL=1**

Remarks                • This parameter is subject to the reload command (reload-cert).

                              • This parameter is not downloaded at startup when using a replication configuration.

See also                 ERROR (Authentication Module configuration file)

# ACCESS

Overview	Sets the access log file name.
Format	<b>ACCESS=<u>access log file name</u></b> <ul style="list-style-type: none"><li>• This parameter has a maximum length of 255 bytes.</li><li>• The default value set in the executable binary file is /opt/icewall-ss/logs/cert.log.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ss/logs/cert.log.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set the same access log file name as in the standard configuration file: <b>ACCESS=/opt/icewall-ss/logs/cert.log</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><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 permissions for the file set with this parameter require write permission for the user that runs the Authentication Module.</li></ul>
See also	ALEVEL (Authentication Module configuration file) LOGINFO LOGPERF



# ERROR

Overview	Sets the error log file name.
Format	<b>ERROR=<u>error log file name</u></b> <ul style="list-style-type: none"><li>• The error log file name has a maximum length of 255 bytes.</li><li>• The default value set in the executable binary file is /opt/icewall-ss/logs/certerr.log.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ss/logs/certerr.log.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set the same error log file name as in the standard configuration file: <b>ERROR=/opt/icewall-ss/logs/certerr.log</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><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 permissions for the file set by this parameter require write permission for the user that runs the Authentication Module.</li></ul>
See also	ELEVEL (Authentication Module configuration file) LOGINFO

---

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

---

# TRACE

Overview                Sets the trace log file name.

Format                   **TRACE=trace log file name**

- The trace log file name has a maximum length of 255 bytes.
- If this parameter is not set, no trace log file is created.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- The system is not guaranteed to work as expected if the value for this parameter is out of range.

Configuration example    1) To output a trace log file:  
**TRACE=/opt/icewall-ss0/logs/certtrace.log**

Remarks

- This parameter is not subject to the reload command (reload-cert).
- This parameter is not downloaded at startup when using a replication configuration.
- 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.
- The owner and permissions for the file set by this parameter require write permission for the user that runs the Authentication Module.
- Setting this parameter causes a drop in the Authentication Module's performance.
- Normally there is no need to set this parameter. It should be set only in situations such as when providing information to technical support.
- HP is not able to answer inquiries regarding the content of the trace log file.

See also                None

# CATALOG 10.0

Overview	<p>Sets the file name for the message catalog file.</p> <p>Some specifications of this parameters have been modified since version 10.0.</p>
Format	<p><b>CATALOG=<u>message catalog file name</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ssso/messages/C/icewall_certd.cat.</li><li>• If no parameter is set, the message catalog file set to the environment variable NLSPATH is used.</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To set the same message catalog file name as in the standard configuration file:</p> <p><b>CATALOG=/opt/icewall-ssso/messages/C/icewall_certd.cat</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• The message below will be output instead of the message that is normally output to the error log when there is an error with the message catalog, such as when this parameter has not been set, or the file name is incorrect. Message Nothing</li></ul>
See also	CATALOG (Forwarder configuration file)

# LOGINFO

Overview	Sets the output of the request sender information to the access log, error log, and performance log.
Format	<p><b>LOGINFO=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : No output</li><li>1 : Outputs the IP address of request sender</li><li>2 : Outputs the IP address of request sender and agent ID (ICP2.0 only)</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To output the IP address of the request sender: <b>LOGINFO=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• The request sender information cannot be output to only the access log, error log, or performance log.</li><li>• The request agent ID that is output must be 256 bytes or less. The ID may not be output if it is 257 bytes or more.</li><li>• The sender IP address and agent ID are output in this order to the access log, error log, and the performance log.</li><li>• The sender IP address is output as "SOURCE_ADDR=IP address."</li></ul>

- The agent ID is output as “AGENT\_ID=agent ID.”
- The output position is between the log message and message ID.

See also

ACCESS (Authentication Module configuration file)  
ERROR (Authentication Module configuration file)  
PERFORMANCE

# LOGPERF

Overview	Sets the output of the request process elapsed time and process time for accessing the Authentication DB to the access log.
Format	<p><b>LOGPERF=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : No output</li><li>1 : Outputs the process elapsed time to the access log</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To output the request process elapsed time to the logs: <b>LOGPERF=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• The message output when this parameter is 1 is treated as an error level. As a result, messages are output when ALEVEL is set to 1 or higher.</li><li>• Regardless of the value set to this parameter, if the PERFORMANCE parameter is set, log messages about elapsed processing time are not output to the access log, but they are output to the performance log.</li><li>• For details on the request and elapsed time that are output to the access log and performance log, see the “IceWall SSO User's Manual.”</li></ul>
See also	ALEVEL (Authentication Module configuration file) ACCESS (Authentication Module configuration file) PERFORMANCE

## TRANSID 10.0

Overview	<p>Sets whether or not to output the transaction ID sent from the request sender to the Authentication Module logs (access log, error log, performance log).</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>TRANSID=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not output the transaction ID to the logs (backward compatibility)</li><li>1 : Output the transaction ID to the logs</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To output the transaction ID to the logs:</p> <p><b>TRANSID=1</b></p>
Output example	<p>1) [Date and time] [Log message] [Transaction ID] [Message ID] <b>[2010/08/05 13:52:41] User Login. UserID=user01 TID= TID201001020 30405678901A0-dfwsvr01 [AC10124-25065]</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• This parameter is only effective when using ICP 2.0.</li><li>• Even when this parameter is set to output the transaction ID, it is not output when the request sender does not send a transaction ID. The request sender must be configured to send a transaction ID to the Authentication Module.</li></ul>

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

---

See also           TRANSID (Forwarder configuration file)  
                    TRANSID\_STR (Forwarder configuration file)



# PERFORMANCE

Overview	<p>Sets the performance log file name.</p> <p>Instead of the access log, the performance log outputs the request process elapsed time and access process time to the Authentication DB.</p>
Format	<p><b>PERFORMANCE=<u>performance log file name</u></b></p> <ul style="list-style-type: none"><li>• The performance log file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To output the request process elapsed time and other data to the performance log:</p> <p><b>PERFORMANCE=/opt/icewall-ss0/logs/certperf.log</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><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 permissions for the file set by this parameter require write permission for the user that runs the Authentication Module.</li><li>• When this parameter is set, log messages pertaining to the process elapsed time are output to the performance log regardless of the ALEVEL, ACCESS, and LOGPERF parameter setting values.</li><li>• When this parameter is set, if the LOGINFO parameter is set to 1 or 2, the request sender information is added in the same way as for the access log.</li><li>• If this parameter is not set, log messages pertaining to the process elapsed time are output to the access log.</li></ul>

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

---

- Be aware that if the data is output to the performance log, the message ID is not output.

See also            LOGINFO

# INFORMATION

Overview	<p>Sets the information log file name.</p> <p>Instead of the access log, the information log outputs the execution results for the operating information output command (info-cert).</p>
Format	<p><b>INFORMATION=<u>information log file name</u></b></p> <ul style="list-style-type: none"><li>• The information log file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To output the execution results for the operating information output command (info-cert) to the information log:</p> <p><b>INFORMATION=/opt/icewall-ss0/logs/certinfo.log</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><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 permissions for the file set by this parameter require write permission for the user that runs the Authentication Module.</li><li>• When this parameter is set, the execution results for the operating information output command (info-cert) are output regardless of the values set to the ALEVEL and ACCESS parameters.</li><li>• If this parameter is not set, the execution results for the operating information output command (info-cert) are output to the access log.</li><li>• Be aware that if the data is output to the information log, the message ID is not output.</li></ul>
See also	<p>ALEVEL (Authentication Module configuration file)</p>

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

---

ACCESS (Authentication Module configuration file)

# PORT

Overview	Sets port numbers for connecting the Authentication Module with Forwarder and the Authentication Module that runs replication.
Format	<p><b>PORT=<u>port number</u></b></p> <ul style="list-style-type: none"><li>• The configurable range is between 1 and 65535.</li><li>• The default value set in the executable binary file is 14142.</li><li>• The initial value set in the standard configuration file is 14142.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set 14142 as the listen port number:</p> <p><b>PORT=14142</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• If the listen port number was modified, change the following Authentication Module commands: /opt/icewall-ssso/certd/bin/end-cert /opt/icewall-ssso/certd/bin/info-cert /opt/icewall-ssso/certd/bin/reload-cert /opt/icewall-ssso/certd/bin/cdump-cert /opt/icewall-ssso/certd/bin/logout-cert</li></ul> <p>Example: To change the listen port number to 14143: \$IW_HOME/certd/bin/certd -F -K -H localhost -P <b>14143</b></p> <ul style="list-style-type: none"><li>• ICANN (Internet Corporation for Assigned Names and Numbers: An international nonprofit corporation that assigns and manages Internet address resources) has assigned IceWall Cert Protocol the port number 14142.</li></ul>

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

---

See also            CERT (Authentication Module configuration file)  
                     CERT (Forwarder configuration file)  
                     IPV6LISTEN  
                     HTTPPORT

## IPV6LISTEN 10.0

**Overview**                Sets the IP version number of requests to be received.

This parameter is available since version 10.0.

**Format**                **IPV6LISTEN=flag**

- Set one of the following values for the flag:
  - 0 : Receive IPv4 requests only
  - 1 : Receive IPv6 requests only
  - 2 : Receive IPv4 and IPv6 requests
- The default value set in the executable binary file is 0.
- The initial value set in the standard configuration file is 0.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**

1) To receive IPv6 requests only:  
**IPV6LISTEN=1**

2) To receive IPv4 and IPv6 requests:  
**IPV6LISTEN=2**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is not downloaded at startup when using a replication configuration.
- The port number for receiving requests is the same when performing IPv4 and IPv6 communication.
- For the replication configuration, the specification method for the host name or IP address in the replicated Authentication Module must match with this configuration.

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

---

- The specification method for the host name or IP address for the CERT parameter in the Forwarder configuration file must match with this configuration.
- Change the content of the Authentication Modules below when set to only receive IPv6 requests.  
/opt/icewall-ssso/certd/bin/end-cert  
/opt/icewall-ssso/certd/bin/info-cert  
/opt/icewall-ssso/certd/bin/reload-cert  
/opt/icewall-ssso/certd/bin/cdump-cert  
/opt/icewall-ssso/certd/bin/logout-cert

Example: When set to receive only IPv6

`$IW_HOME/certd/bin/certd -F -K -H [localhost] -P 14142`

See also

CERT  
PORT  
HTTPPORT



# HTTPPORT 10.0

**Overview** Sets the port number for receiving HTTP requests.

This parameter is available since version 10.0.

**Format** **HTTPPORT=port number**

- The configurable range is between 1 and 65535.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)
- This function is ineffective when there is no configuration parameter.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To accept HTTP requests on port number 8080:  
**HTTPPORT=8080**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is not downloaded at startup when using a replication configuration.
- The port number for this parameter cannot be set in the Authentication Module commands below.  
/opt/icewall-ss0/certd/bin/end-cert  
/opt/icewall-ss0/certd/bin/info-cert  
/opt/icewall-ss0/certd/bin/reload-cert  
/opt/icewall-ss0/certd/bin/logout-cert

**See also** PORT  
IPV6LISTEN  
HTTPECHOHEADER

## HTTPECHOHEADER 10.0

Overview	<p>Sets whether or not to append the HTTP request header sent from the client to the header of the response.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>HTTPECHOHEADER=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not include the header received during the request with the response header</li><li>1 : Include the header received during the request with the response header (Compatible with ICP 2.0)</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To include the HTTP request header sent from the client with the response header:</p> <p><b>HTTPECHOHEADER=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• Effective when HTTPPORT is set.</li><li>• Only effective for requests sent by HTTP.</li></ul>
See also	HTTPPORT

### 3.1.2 Access control related parameters

These parameters set access control for requests from the client.

Parameter name	Mandatory	Overview
GROUP	×	Sets the group configuration file
ACL	×	Sets the access control file
ACLREQUEST	×	Sets the request control configuration file
ADGROUP	×	Sets whether or not to add Active Directory group information to the user information
ADGROUPDN	×	Sets the DN which includes the Active Directory group information
ADGROUPINTERVAL	×	Sets the interval to retrieve Active Directory group information
ADGROUPPRNAME	×	Sets the primary group name for users retrieved from the Active Directory group information
ADGROUPPREFIX	×	Sets the characters to apply to the group name retrieved from the Active Directory group information
ADGROUPMAXMEMBER	×	Sets how many levels to retrieve groups that users belong to

For details on these parameters, see the following pages.

---

Authentication Module configuration file (cert.conf)

---

# GROUP

Overview	Sets the file name of the group configuration file that defines user groups.
Format	<p><b>GROUP=<u>group configuration file name</u></b></p> <ul style="list-style-type: none"><li>• The group configuration file name has a maximum length of 255 bytes.</li><li>• The default value set in the executable binary file is /opt/icewall-sso/certd/config/cert.grp.</li><li>• The initial value set in the standard configuration file is /opt/icewall-sso/certd/config/cert.grp.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the standard group configuration file name: <b>GROUP=/opt/icewall-sso/certd/config/cert.grp</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	ACL

# ACL

Overview	Sets the file name of the access control file that defines access control information.
Format	<b>ACL=<u>access control file name</u></b> <ul style="list-style-type: none"><li>• The access control file name has a maximum length of 255 bytes.</li><li>• The default value set in the executable binary file is /opt/icewall-ssso/certd/config/cert.acl.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ssso/certd/config/cert.acl.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set the default access control file name: <b>ACL=/opt/icewall-ssso/certd/config/cert.acl</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	GROUP

# ACLREQUEST

Overview	Sets the file name for the request control configuration file that controls executable requests.
Format	<b>ACLREQUEST=<u>request control configuration file name</u></b> <ul style="list-style-type: none"><li>• The request control configuration file name has a maximum length of 255 bytes.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• If the value for this parameter is out of range, the default value is used. If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set the standard request control configuration file: <b>ACLREQUEST=/opt/icewall-ssso/certd/config/request.acl</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• The request control function does not work unless this parameter is set.</li></ul>
See also	None

# ADGROUP

Overview	Sets whether or not to add Active Directory group information to the user information.
Format	<p>MSAD edition only</p> <p><b>ADGROUP=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not use AD group function (backward compatibility/default operation)</li><li>1 : Use AD group function</li></ul></li><li>• This parameter does not need to be set in editions other than the MSAD edition.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To use Active Directory group information with IceWall SSO:</p> <p><b>ADGROUP=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>LDAPMULTIVAL</p> <p>ADGROUPDN</p> <p>ADGROUPINTERVAL</p> <p>ADGROUPPRNAME</p> <p>ADGROUPPREFIX</p> <p>ADGROUPMAXMEMBER</p>

# ADGROUPDN

Overview	Sets the DN which includes the Active Directory group information.
Format	<p>MSAD edition only</p> <p><b>ADGROUPDN=<u>group search DN</u></b></p> <ul style="list-style-type: none"><li>• Group search DN has a maximum length of 255 bytes.</li><li>• This parameter does not need to be set in editions other than the MSAD edition.</li><li>• The default value in the executable binary file is the same setting as DBTBL.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• This parameter is effective only when ADGROUP=1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To retrieve Active Directory group information from “dc=groups,dc=icewall,dc=local”:</p> <p><b>ADGROUPDN=dc=groups,dc=icewall,dc=local</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>LDAPMULTIVAL</p> <p>ADGROUP</p> <p>ADGROUPINTERVAL</p> <p>ADGROUPPRINAME</p> <p>ADGROUPPREFIX</p>



# ADGROUPINTERVAL

Overview	Sets the interval to retrieve Active Directory group information.
Format	<p>MSAD edition only</p> <p><b>ADGROUPINTERVAL=<u>AD group retrieval thread processing interval</u></b></p> <ul style="list-style-type: none"><li>• Set the AD group retrieval interval within 0 to 86400 seconds (1 day).</li><li>• This parameter does not need to be set in editions other than the MSAD edition.</li><li>• If set to 0, AD group information is retrieved only at initial startup. It is not retrieved after that.</li><li>• This parameter is effective only when ADGROUP=1.</li><li>• The default value set in the executable binary file is 60.</li><li>• The initial value set in the standard configuration file is 60.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the interval to retrieve Active Directory group information to 1 day:</p> <p><b>ADGROUPINTERVAL=86400</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>LDAPMULTIVAL</p> <p>ADGROUP</p> <p>ADGROUPPDN</p> <p>ADGROUPPRNAME</p> <p>ADGROUPPREFIX</p>

# ADGROUPPRINAME

Overview	Sets the primary group name for users retrieved from the Active Directory group information.
Format	<p>MSAD edition only</p> <p><b>ADGROUPPRINAME=<u>primary group attribute value name</u></b></p> <ul style="list-style-type: none"><li>• The primary group attribute value name has a maximum length of 255 bytes.</li><li>• This parameter does not need to be set in editions other than the MSAD edition.</li><li>• This parameter is effective only when ADGROUP=1.</li><li>• The default value set in the executable binary file is ADGROUP_PRIMARY.</li><li>• The initial value set in the standard configuration file is ADGROUP_PRIMARY.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the user information primary group name to "IW_PRIMARY":</p> <p><b>ADGROUPPRINAME=IW_PRIMARY</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>LDAPMULTIVAL</p> <p>ADGROUP</p> <p>ADGROUPDN</p> <p>ADGROUPINTERVAL</p> <p>ADGROUPPREFIX</p>

# ADGROUPPREFIX

Overview	Sets the prefix to add to the group name retrieved from the Active Directory group information.
Format	<p>MSAD edition only</p> <p><b><u>ADGROUPPREFIX=group name prefix</u></b></p> <ul style="list-style-type: none"><li>• The group name prefix has a maximum length of 255 bytes.</li><li>• This parameter does not need to be set in editions other than the MSAD edition.</li><li>• Group names stored in the user information have a maximum length of 255 bytes combined with the length of the group name.</li><li>• This parameter is effective only when ADGROUP=1.</li><li>• The default value set in the executable binary file is ADGROUP_.</li><li>• The initial value set in the standard configuration file is ADGROUP_.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set “IW_ADGRP_” as the group users belong to:</p> <p><b>ADGROUPPREFIX=IW_ADGRP_</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>LDAPMULTIVAL</p> <p>ADGROUP</p> <p>ADGROUPPDN</p> <p>ADGROUPINTERVAL</p> <p>ADGROUPPRNAME</p>

# ADGROUPMAXMEMBER

Overview	Sets how many levels to retrieve groups that users belong to.
Format	<p>MSAD edition only</p> <p><b>ADGROUPMAXMEMBER=<u>maximum number of groups retrieved</u></b></p> <ul style="list-style-type: none"><li>• Define the maximum number of retrieved groups within the range of 0 to 50.</li><li>• This parameter does not need to be set in editions other than the MSAD edition.</li><li>• This parameter is effective only when ADGROUP=1.</li><li>• The default value set in the executable binary file is 20.</li><li>• The initial value set in the standard configuration file is 20.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To retrieve parent groups across three levels:</p> <p><b>ADGROUPINTERVAL=3</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>LDAPMULTIVAL</p> <p>ADGROUP</p>

### 3.1.3 Session policy related parameters

These parameters configure the policy for sessions in the entire system.

Parameter name	Mandatory	Overview
COOKIERETRY	×	Sets the number of attempts to generate session IDs
COOKIETIME	×	Sets the login expiration time
COOKIEEXP	×	Enables or disables an expiration time for authentication cookies
LOMETHOD	×	Sets the handling of the login expiration time
DUPLOGIN	×	Sets whether or not to forbid duplicate logins
DUPKIND	×	Sets the operation for when duplicate logins are forbidden
PARALOGIN	×	Sets authentication after the initial authentication
ACCCTRLFLG	×	Sets the access control security level
SESSIONIDLEN <b>10.0</b>	×	Sets the byte length for the session ID generated by the Authentication Module
CERTUNIQUEKEY <b>10.0</b>	×	Sets the key for Authentication Module assignments

For details on these parameters, see the following pages.

# COOKIERETRY

Overview	Sets the retry count for generating session IDs.
Format	<b>COOKIERETRY=<u>retry count</u></b> <ul style="list-style-type: none"><li>• If 0 is set to the retry count, the system keeps on trying to generate session IDs until a unique ID is obtained.</li><li>• The default value set in the executable binary file is 10.</li><li>• The initial value set in the standard configuration file is 10.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set the number of attempts to generate session IDs to 5: <b>COOKIERETRY=5</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• A system error occurs if this parameter is set to 1 or higher and if a unique session ID is not generated after the number of attempts specified with this parameter.</li><li>• Do not set this parameter to 0 when generating arbitrary session IDs after developing a session ID generation routine.</li></ul>
See also	None

# COOKIE TIME

**Overview**                Sets the login expiration time for the user.

**Format**                **COOKIE TIME=expiration time (minutes)**

- The expiration time is specified in minutes.
- The default value set in the executable binary file is 60.
- The initial value set in the standard configuration file is 60.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**    1) To set the login expiration time to 10 minutes:  
**COOKIE TIME=10**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is downloaded at startup when using a replication configuration.
- Only one setting can be defined for this parameter throughout the whole system. Therefore, expiration times cannot be set to each individual user.

**See also**                LOMETHOD  
COOKIEEXP

# COOKIEEXP

Overview	Sets whether to add an expiration time to the authentication cookie issued to a client when a user logs in.
Format	<p><b>COOKIEEXP=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not set an expiration time</li><li>1 : Set an expiration time</li></ul></li><li>• If the LOMETHOD parameter is 1, this parameter is unconditionally set to 0.</li><li>• The default for the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set an expiration time for the authentication cookie: <b>COOKIEEXP=1</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• If an expiration time is not set to the authentication cookie, it is discarded when the browser is closed on the client side. (However, the user is still logged in to the Authentication Module.) In this case, if the browser is opened again and a connection is made to IceWall, the login page is displayed and login is requested.</li><li>• If the expiration time is set to authentication cookies, the cookie is not discarded within the expiration time even if the browser is closed on the client side. In this case, if the browser is opened again and a connection is made to IceWall, no login is required.</li></ul>



See also        LOMETHOD  
                 COOKIETIME

# LOMETHOD

Overview	Sets the method for calculating the login expiration time.
Format	<b>LOMETHOD=<u>flag</u></b> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Calculate from the time the login was performed</li><li>1 : Calculate from the time the last access was performed</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To calculate the login expiration time from the time the user logged in: <b>LOMETHOD=0</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• If the login expiration time is calculated from the time the login was performed, the login expires when the period set in the COOKIETIME parameter has elapsed after the user logged in. Then the user is automatically logged out. In this case, a user may be requested to log in again while accessing pages.</li><li>• If the login expiration time is calculated from the time of the last access, the login expires when the period set in the COOKIETIME parameter has elapsed after the user's last access. Then the user is automatically logged out. In this case, the expiration time is reset by continuing to access IceWall within the expiration period, and the user is no longer requested to log in again.</li></ul>

See also            COOKIETIME

# DUPLOGIN

Overview	Sets whether a duplicate login with the same user ID is allowed.
Format	<p><b>DUPLOGIN=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Forbid duplicate logins</li><li>1 : Allow duplicate logins</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To allow a duplicate login with the same user ID:</p> <p><b>DUPLOGIN=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When duplicate logins are forbidden, either of the following two actions can be selected for users attempting a duplicate login:<ul style="list-style-type: none"><li>1) Override login</li><li>2) Exclusive login</li></ul>For details about these logins, see the DUPKIND parameter.</li></ul>
See also	DUPKIND

# DUPKIND

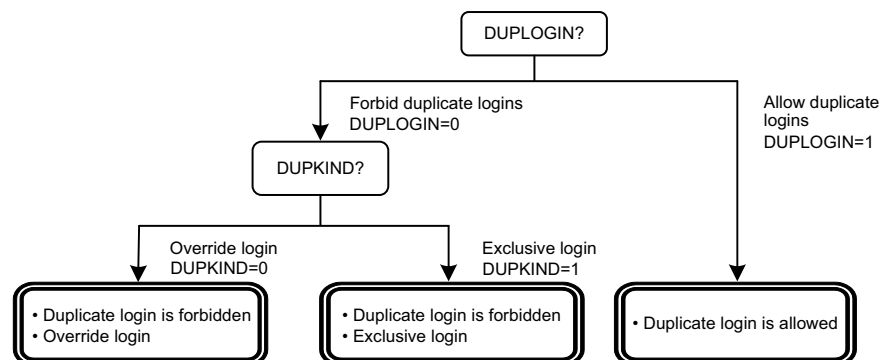
Overview	Sets the action for users attempting a duplicate login when duplicate logins are forbidden.
Format	<p><b>DUPKIND=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Override login (able to login)</li><li>1 : Exclusive login (unable to login)</li></ul></li><li>• This parameter is effective only when 0 is set to the DUPLOGIN parameter.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To allow the latest user to log in when duplicate logins are forbidden:</p> <p><b>DUPLOGIN=0</b> <b>DUPKIND=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When a duplicate login is attempted with override login enabled, the user logged in before that time is forcibly logged out, and the user who is attempting the duplicate login is able to login.</li></ul>

---

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

---

- When a duplicate login is attempted with exclusive login, the user logged in before that time continues to be logged in and the user who is attempting to login is not able to login. With this setting, the forced login page is displayed in the browser of the user attempting the duplicate login. If the user logs in from the forced login page, the action is the same as if it were an override login.
- The relationship between forbidding and allowing duplicate logins is as follows:



See also

DUPLOGIN

# PARALOGIN

Overview	Sets whether or not authentication with a user ID and password is allowed after an initial authentication is performed with a client certificate.
Format	<p><b>PARALOGIN=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Forbid authentication with a user ID and password after initial authentication</li><li>1 : Allow authentication with a user ID and password after initial authentication</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To forbid authentication with user ID and password after initial authentication with a client certificate:</p> <p><b>PARALOGIN=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li></ul>
See also	None

# ACCCTRLFLG

Overview	Sets the access control security level when using a client certificate.
Format	<p><b>ACCCTRLFLG=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Perform client certificate presentation check and user ID check</li><li>1 : Perform client certificate presentation check only</li><li>2 : Do not perform client certificate presentation check or user ID check</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the access control security level when using a client certificate to “Do not perform client certificate presentation check or user ID check”:</p> <p><b>ACCCTRLFLG=2</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li><li>• Since the access control security level is reduced whenever this parameter is set to a value other than 0, setting the value to 0 is recommended.</li><li>• The user ID output to the Authentication Module's access log is the user ID at login, even if 1 or 2 is set to this parameter and using a client certificate for a user ID that is different from the one at login</li></ul>



during access control.

- This parameter setting is applied to the entire system. To change the security level from the request sender, use the ACCCTRL parameter in the request control configuration file.

See also           ACCCTRL (request control configuration file)

## SESSIONIDLEN 10.0

Overview	<p>Sets the byte length for the IceWall session ID generated by the Authentication Module.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>SESSIONIDLEN=<u>byte length</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following byte lengths:<ul style="list-style-type: none"><li>32 : Set the generated session ID length to 32 bytes (backward compatibility)</li><li>64 : Set the generated session ID length to 64 bytes</li></ul></li><li>• The default value set in the executable binary file is 32.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the session ID byte length to 64:</p> <p><b>SESSIONIDLEN=64</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• The 64-byte long session ID is generated only when SESSIONIDLEN is set to 64 and there is an ICP 2.0 login request.</li><li>• For ICP 1.x login requests when SESSIONIDLEN is 64, a session ID generation error is returned to the login request sender.</li><li>• The setting for SESSIONIDLEN must be the same setting on the Primary and Secondary modules.</li></ul>

- To change the SESSIONIDLEN setting, you must stop both the Primary and Secondary modules. (The setting cannot be changed for the modules one at a time.)
- For session management using URL-Cookie, caution is required in some cases, such as with browsers that cannot use long URLs, because a 32-byte or 64-byte session ID is included in the URL.

See also           None

## CERTUNIQUEKEY 10.0

Overview	<p>Sets a unique key for each Authentication Module group so that the Authentication Modules can be assigned.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>CERTUNIQUEKEY=<u>authentication module identification key</u></b></p> <ul style="list-style-type: none"><li>• The Authentication Module identification key can be a single character only (0-9, a-z).</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the Authentication Module identification key to “a”:</p> <p><b>CERTUNIQUEKEY=a</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• For this parameter, the Primary and Secondary modules in each Authentication Module group must be the same value.</li><li>• To use the Forwarder connection target Authentication Module assignment function, you must configure the CERTLB parameter in the Forwarder configuration file.</li></ul>
See also	<p>CERTLB (Forwarder configuration file)</p>

### 3.1.4 Password policy related parameters

These parameters are used to configure the password policy when the users log in and when changing passwords.

Parameter name	Mandatory	Overview
PWDLOGINHASH <small>10.0</small>	×	Sets the hashing method when logging in
PWDCHGHASH <small>10.0</small>	×	Sets the hashing method when changing passwords
PWDMINLEN <small>10.0</small>	×	Sets the minimum password length for new passwords when changing passwords
PWDMAXLEN <small>10.0</small>	×	Sets the maximum password length for new passwords when changing passwords
PWDALPHANUM <small>10.0</small>	×	Sets the combination of characters that are available for generic passwords
PWDEXPIRE <small>10.0</small>	×	Sets the number of days a newly set password expires
PWDSAMEPASS <small>10.0</small>	×	Sets whether or not to allow a password identical to the user ID when changing passwords
LOCKCOUNT	×	Sets the number of password retries
PWDEXPCHK	×	Enables/disables the password expiration check
PWDHISCHK	×	Enables/disables the password history check when the password is changed
PWDHISCNT <small>10.0</small>	×	Sets the number of passwords stored in the password history
PWDFORBID	×	Sets the forbidden password configuration file
PWDEXPWARN	×	Sets the period when the password expiration date warning starts

For details on these parameters, see the following pages.

## PWDLOGINHASH 10.0

Overview	<p>Sets the hashing method when logging in.</p> <p>This parameter is required when using BIND authentication.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>PWDLOGINHASH=<u>hash flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the hash flag:<ul style="list-style-type: none"><li>MD5: MD5 hashing</li><li>SHA: SHA1 hashing</li><li>SHA256: SHA256 hashing</li><li>PLAIN: Do not hash</li><li>AUTO-PLAIN: Determine a hashing method from prefix (judge as PLAIN when no prefix)</li><li>AUTO-MID5: Determine a hashing method from prefix (judge as MD5 when no prefix)</li></ul></li><li>• The default value in the executable binary file is AUTO-PLAIN.</li><li>• The initial value in the standard configuration file is set to the values below.<ul style="list-style-type: none"><li>MSAD edition: PLAIN</li><li>NED edition: SHA</li><li>Other editions: AUTO-PLAIN on a comment line</li></ul></li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To set the hashing method to SHA256 when logging in:</p> <p><b>PWDLOGINHASH=SHA256</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• This parameter can only be used with the password encryption library bundled in SSO.</li></ul>

- If the settings for the hashing method when logging in (PWDLOGINHASH) and the hashing method when changing the password (PWDCHGHASH) are different, users may not be able to log in after changing their passwords.
- When not performing BIND authentication, the hashing method is determined by the password prefix registered in the Authentication DB. Hashes are generated with the value set to this parameter when there is no prefix.
- When performing BIND authentication, hashes are generated with the value set to this parameter because the prefix cannot be retrieved from the Authentication DB.

See also

LDAPBIND  
PWDCHGHASH

## PWDCHGHASH 10.0

**Overview**                Sets the hashing method when changing passwords.

This parameter is available since version 10.0.

**Format**                **PWDCHGHASH=hash flag**

- Set one of the following values for the hash flag:
  - MD5:            MD5 hashing
  - SHA:            SHA1 hashing
  - SHA256:        SHA256 hashing
  - PLAIN:         Do not hash
  - AUTO-PLAIN: Determine a hashing method from prefix (judge as  
                  PLAIN when no prefix)
  - AUTO-MID5: Determine a hashing method from prefix (judge as MD5  
                  when no prefix)
- The default value in the executable binary file is AUTO-PLAIN.
- The initial value in the standard configuration file is set to the values below.
  - MSAD edition: PLAIN
  - NED edition: SHA
  - Other editions: AUTO-PLAIN on a comment line
- The system is not guaranteed to work as expected if the value for this parameter is out of range.

**Configuration example**    1) To operate with the hashing method as SHA256 when changing passwords:  
**PWDCHGHASH=SHA256**

- Remarks**
- This parameter is not subject to the reload command (reload-cert).
  - This parameter is downloaded at startup when using a replication configuration.
  - This parameter can only be used with the password encryption library bundled in SSO.
  - This parameter must be set if changing the hashing method when changing passwords.



- If the settings for the hashing method when logging in (PWDLOGINHASH) and the hashing method when changing the password (PWDCHGHASH) are different, users may not be able to log in after changing their passwords.
- To perform BIND authentication, this parameter must be set to the same value as PWDLOGINHASH.

See also

LDAPBIND  
PWDLOGINHASH

## PWDMINLEN<sup>10.0</sup>

**Overview** Sets the minimum password length for new passwords.

This parameter is available since version 10.0.

**Format** **PWDMINLEN=password minimum characters**

- The minimum password length can be a maximum of 128 bytes.
- The default value set in the executable binary file is 3.
- The initial value set in the standard configuration file is 3.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To set the minimum number of characters for the password length to 5:  
**PWDMINLEN=5**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is downloaded at startup when using a replication configuration.
- Password changes will result in error if this parameter is set to a value larger than the value set to the MAXLEN parameter.
- Setting this parameter to "0" does not result in a "no password" setting.

**See also** PWDMAXLEN  
MAXLEN (Forwarder configuration file)

# PWDMAXLEN<sup>10.0</sup>

**Overview** Sets the maximum password length for new passwords.

This parameter is available since version 10.0.

**Format** **PWDMAXLEN=password maximum characters**

- The maximum password length can be a maximum of 128 bytes.
- The default value set in the executable binary file is 6.
- The initial value set in the standard configuration file is 6.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To set the maximum number of characters for the password length to 6:  
**PWDMAXLEN=6**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is downloaded at startup when using a replication configuration.
- Password changes will result in error if this parameter is set to a value smaller than the value set to the MINLEN parameter.

**See also** PWDMINLEN  
MINLEN (Forwarder configuration file)

## PWDALPHANUM<sup>10.0</sup>

**Overview**                Sets the type of characters that are available for use in passwords.

This parameter is available since version 10.0.

**Format**                **PWDALPHANUM=combination flag**

- Set one of the following values for the combination flag:
  - 0 : All character types allowed, including alphabetical, numerical, and special characters.
  - 1 : Password must contain both alphabetical and numerical characters; no special characters allowed.
  - 2 : Numerical characters only
  - 3 : Alphabetical characters only
  - 4 : Special characters only
  - 5 : Password must contain both numerical and special characters; no alphabetical characters allowed.
  - 6 : Passwords must contain both alphabetical and special characters; no numerical characters allowed.
  - 7 : Password must contain all character types, including alphabetical, numerical, and special characters.
  - 8 : Password must contain both alphabetical and numerical characters; special characters allowed.
  - 9 : Password must contain numerical characters; alphabetical and special characters allowed.
  - 10 : Password must contain alphabetical characters; numerical and special characters allowed.
  - 11 : Password must contain special characters; alphabetical and numerical characters allowed.
  - 12 : Password must contain both numerical and special characters; alphabetical characters allowed.
  - 13 : Password must contain both alphabetical and special characters; numerical characters allowed.
- The following special characters are supported. Blank spaces may not be used.  
!"#\$%&()\*+,-./:;<=>?@[ \ ] ^ \_ ` { | } ~
- The default value set in the executable binary file is 1.
- The initial value set in the standard configuration file is 0.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.

- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

Configuration example

- 1) To configure passwords to require both alphabetical and numerical characters:  
**PWDALPHANUM=1**

Remarks

- This parameter is not subject to the reload command (reload-cert).
- This parameter is downloaded at startup when using a replication configuration.
- It is recommended to enforce a password policy that required multiple character types to help ensure good security measures.
- Double-byte characters and single-byte katakana cannot be used.

See also

ALPHANUM (Forwarder configuration file)

## PWDEXPIRE<sup>10.0</sup>

**Overview**                Sets the number of days a new password change is valid.

This parameter is available since version 10.0.

**Format**                **PWDEXPIRE=password expiration days**

- The unit for setting this value is in days.
- If “0” is set, the password will not expire (no expiration date).
- The default value set in the executable binary file is 72.
- The initial value set in the standard configuration file is 72.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

**Configuration example**        1) To set new passwords to expire after 72 days:  
**PWDEXPIRE=72**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is downloaded at startup when using a replication configuration.
- This parameter can only have one setting, which applies to the entire system.
- Individual users cannot have different expiration times.
- The user’s password expiration time is not updated if the PWDEXPCHK parameter in the Authentication Module configuration file is set to 0 (do not check password expiration time). The value set to the PWDEXPCHK parameter has priority.
- Users will be asked to change their password when logging in after the password has expired. (Authentication Module must be set to check for expiration data.)

See also           PWDEXPCHK  
                    EXPIRE (Forwarder configuration file)

## PWDSAMEPASS<sup>10.0</sup>

Overview	<p>Sets whether to allow or disallow passwords identical to the user ID.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>PWDSAMEPASS=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Allows passwords identical to the user ID</li><li>1 : Prohibits passwords identical to the user ID</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To prohibit passwords that are identical to the user ID:</p> <p><b>PWDSAMEPASS=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• It is recommended to set this parameter to 1 (prohibit) to help ensure good security measures.</li></ul>
See also	<p>SAMEPASS (Forwarder configuration file)</p>



# LOCKCOUNT

Overview	Sets the password retry count allowed before the account is locked due to a password entry error at login.
Format	<b>LOCKCOUNT=<u>retry count</u></b> <ul style="list-style-type: none"><li>• Set one of the following values for the count:<ul style="list-style-type: none"><li>0 : Account is not locked</li><li>1 or higher : Account is locked if the number of failures equals this value</li></ul></li><li>• Define the retry count in the range from 0 to 256.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 5.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To disable account lock and set no limitation on the number of password entry errors: <b>LOCKCOUNT=0</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• The account is locked at the moment the number of password entry failures at login equals the number set by this parameter.</li><li>• The retry count is reset to 0 and saved to the Authentication DB only when the login is successful.</li><li>• Locked accounts are not released. To release, the lock flag in the Authentication DB for the locked user must be reset.</li></ul>
See also	None

# PWDEXPCHK

Overview	Sets whether to check the password expiration date at login.
Format	<p><b>PWDEXPCHK=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not check the password expiration date</li><li>1 : Check the password expiration date</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To check the password expiration date at login:</p> <p><b>PWDEXPCHK=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When this parameter is set to 1, the password change page is displayed instead of the requested page when a user logs in with an expired password. The content on the Backend Web Server cannot be accessed unless the password is changed on that page.</li><li>• If changing the password is forbidden for a user (PCHGOK=0), the password expiration date is not checked, regardless of the setting for this parameter.</li></ul>
See also	<p>PCHGOK (Authentication DB column information file)</p> <p>PWDEXPIRE</p>

# PWDHISCHK

Overview	Sets whether to check if the new password is the same as a past one during a password change. Enabling this parameter forbids users to change the password to any of the past passwords that are stored.
Format	<p><b>PWDHISCHK=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not check the password history</li><li>1 : Check the password history</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To forbid changing a password to one that has been set in the past:</p> <p><b>PWDHISCHK=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• For details about the password history, see the PWDHISTORY parameter in the Authentication DB column information file.</li></ul>
See also	<p>PWDHISCNT</p> <p>PWDHISTORY (Authentication DB column information file)</p>

## PWDHISCNT 10.0

Overview	<p>Sets the maximum number of used passwords to store as the password history when changing a password.</p> <p>Some specifications of this parameters have been modified since version 10.0.</p>
Format	<p><b>PWDHISCNT=<u>maximum number saved</u></b></p> <ul style="list-style-type: none"><li>• A number from 1 to 20 can be set for the number stored.</li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 3.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To store nine passwords in the password history:</p> <p><b>PWDHISCNT=9</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• For details about the password history, see the PWDHISTORY parameter in the Authentication DB column information file.</li></ul>
See also	<p>PWDHISTORY (Authentication DB column information file)</p>

# PWDFORBID

Overview	Sets the path for the forbidden password configuration file.
Format	<b>PWDFORBID=<u>forbidden password configuration file name</u></b> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The Authentication Module will not start if this file does not exist.</li><li>• The Authentication Module will not start if loading the forbidden password strings configuration file is enabled and all the forbidden password strings have been commented out.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is /opt/icewall-sso/certd/config/pwdforbid.conf.</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	1) To set the standard forbidden password configuration file: <b>PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	Forbidden password configuration file

## PWDEXPWARN

Overview	Sets the period when the password expiration time warning starts.
Format	<b>PWDEXPWARN=<u>number of days before expiration date to start warning</u></b> <ul style="list-style-type: none"><li>• The unit for setting this value is in days.</li><li>• The number of days ranges from 0 to 365.</li><li>• If the number of days is set to 0, no expiration date warning is made.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set a password expiration time warning to start three days before the password expires: <b>PWDEXPWARN=3</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When logging in during the expiration time warning period, the warning screen is displayed after login. Content is visible even if the password is not changed during the warning period.</li><li>• The password expiration time warning is not checked if any of the following conditions is met.<ul style="list-style-type: none"><li>• The user cannot change the password (when the password change enable/disable flag column is a value other than 1 (including NULL)).</li><li>• The password expiration check is not performed (PWDEXPCHK=0).</li><li>• The password expiration time was not set for the user (column for password expiration time is not set, or the column value is NULL or 0).</li><li>• The password expiration time has already passed when the user logs in.</li></ul></li></ul>

- This parameter was set to 0.
- The password expiration time warning is not calculated precisely from the password expiration time. The number of days is calculated by rounding off the hours from the expiration date.

See also

PWDCHG\_WARNING (HTML configuration file)

PWDEXPCHK

PWDEXPDATE (Authentication DB column information file)

PCHGOK (Authentication DB column information file)

### 3.1.5 Authentication DB related parameters

These parameters configure the Authentication DB that the Authentication Module connects to.

Parameter name	Mandatory	Overview
DBHOST <small>(10.0)</small>	<input type="radio"/>	Sets where the Authentication DB is connected to
DBUID <small>Overwrite</small>	<input type="radio"/>	Sets the connecting user ID
DBPWD <small>Overwrite</small>	<input type="radio"/>	Sets the password for the connecting user ID
DBTBL	<input type="radio"/>	Sets the authentication table
DBATTR	<input type="radio"/>	Configures the Authentication DB column information file
DBEXATTR	×	Configures columns added to the default columns
DBCRYPTOTYPE <small>(10.0)</small>	×	Sets the encryption type for decrypting data encrypted in the Authentication DB
DBIWCRYPTOSEED <small>(10.0)</small>	×	Sets the seed passed to the Authentication DB encryption library for the product's standard encryption
DBCRYPTOATTR <small>(10.0)</small>	×	Sets the column using the encrypted value
LDAPBIND	×	Sets the bind authentication
LDAPPCHG	×	Sets the Authentication DB update function for changing passwords
LDAPLANG	×	Sets the character code conversion function
LDAPSSL	×	Enables/disables SSL connections with the LDAP server
LDAPCACERT	×	Sets the CA certificate file when establishing SSL connections with the LDAP server
LDAPVERIFYSVRCERT	×	Enables/disables CA certificate verification when establishing SSL connections with the LDAP server
LDAPCIPHERSUITE	×	Sets the SSL encryption strength when establishing SSL connections with the LDAP server
LDAPSSLBIND	×	Enables/disables use of SSL communication when using LDAP BIND and SSL communication
ADPCHG	×	Enables/disables password change operations for Active Directory



Parameter name	Mandatory	Overview
LDAPMULTIVAL	×	Sets whether or not to retrieve all values when there are multiple LDAP attribute values
LDAPREFERRAL	×	Enables/disables the LDAP referral function
ADDGFWBIND	×	Enables/disables implementation of BIND authentication when using the Domain Gateway Option

For details on these parameters, see the following pages.

---

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


---

# DBHOST 10.0

**Overview**                      Sets where the Authentication DB is connected to.

**Format**                        ORACLE edition  
**DBHOST=**host ID (SID)

- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is ORCL.

LDAP, MSAD, NED and OpenLDAP editions

**DBHOST=**host name (or IP address):port number for search or update[:port number for BIND][,host name]:port number for search or update[:port number for BIND]

- The default value set in the executable binary file is localhost:389:389. However, the value is localhost:636:636 when LDAPSSL=1 or LDAPSSLBIND=1; and the value is localhost:636:389 when LDAPSSL=1 or LDAPSSLBIND=0.
- The initial value set in the standard configuration file is localhost:389.
- If the port number for BIND is omitted, the default value is set.

MySQL edition

**DBHOST=**database name:host name (or IP address):[port number]:ODBC drive name[,database name:host name]:[port number]:ODBC driver name]

- The database name, host name, and ODBC driver name cannot be omitted.
- The port number defaults to 3306 if omitted.
- The delimiter character “:” is required even if the port number is omitted.
- The ODBC driver name is set in the odbinst.ini file, and the MySQL-Connector library must be set to the Drive parameter in this file.
- There is no default value in the executable binary file.
- The initial value set in the standard configuration file is icewalldb:odbhost:3306:MySQL ODBC 5.1.6 Driver.

CSV edition

- This parameter does not need to be set in the CSV edition.

Configuration example	<ol style="list-style-type: none"> <li>1) To set the Authentication DB host ID to “ORCL” in the ORACLE edition: <b>DBHOST=ORCL</b></li> <li>2) To set the Authentication DB host name to “ldapsvr” and the port number to 389 in the LDAP edition: <b>DBHOST=ldapsvr:389</b></li> <li>3) To configure failover in the MSAD edition with ldapsvr:389 and ldaphost:389: <b>DBHOST=ldapsvr:389,ldaphost:389</b></li> <li>4) To set the Authentication DB host name to “ldapsvr” and the port number to 389 in the NED edition: <b>DBHOST=ldapsvr:389</b></li> <li>5) To set the database name to “icewalldb,” the host name to “mysqlsvr,” and the ODBC driver name to “mysqldr” in the MySQL edition: <b>DBHOST=icewalldb:mysqlsvr::mysqldr</b></li> <li>6) To set the port number for search and update to 636 and the port number for BIND to 389 in the LDAP, MSAD, NED and OpenLDAP editions: <b>DBHOST=localhost:636:389</b></li> </ol>
Remarks	<ul style="list-style-type: none"> <li>• This parameter is not subject to the reload command (reload-cert).</li> <li>• This parameter is not downloaded at startup when using a replication configuration.</li> <li>• Failover settings for the Authentication DB are supported in the LDAP, MSAD, NED, MySQL, and OpenLDAP editions (multi-master configuration) only.</li> <li>• In the MySQL edition, localhost cannot be set for the host name.</li> <li>• Because the case-sensitive setting for the MySQL edition database name depends on the MySQL initialization parameter “lower_case_table_names,” set that parameter to 1 to make the name case-insensitive.</li> <li>• In the LDAP, MSAD, NED, and OpenLDAP editions, IPv6 can be set for the IP address.</li> </ul>

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

---

See also

- DBTBL
- LDAPSSL
- LDAPCACERT
- LDAPVERIFYSVRCERT
- LDAPCIPHERSUITE
- LDAPSSLBIND
- ADPCHG

## DBUID overwrite

Overview	Sets the user ID for connecting to the Authentication DB.
Format	<p>ORACLE, LDAP, MSAD, NED, MySQL, and OpenLDAP editions</p> <p><b>DBUID=<u>user ID</u></b></p> <ul style="list-style-type: none"> <li>The user ID can be described in cleartext, but after the Authentication Module starts, it is encrypted as follows: DBUID={IW}[encrypted user ID]</li> <li>This parameter does not need to be set in the CSV edition.</li> <li>There is no default value in the executable binary file.</li> <li>The initial value in the standard configuration file is set to the values below.</li> </ul> <p>ORACLE edition : scott</p> <p>LDAP edition : uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot</p> <p>MSAD edition : CN=Administrator,CN=Users,DC=is,DC=com</p> <p>NED edition : cn=admin,o=Alias.com</p> <p>MySQL edition : root</p> <p>OpenLDAP edition: cn=Manager,dc=jpn.dc=hp,dc=com</p>
Configuration example	<ol style="list-style-type: none"> <li>To set the user ID to “scott” for connecting to the Authentication DB in the ORACLE and MySQL editions: <b>DBUID=scott</b></li> <li>To set the user ID to “admin” for connecting to Sun Java System Directory Server in the LDAP edition: <b>DBUID=uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot</b></li> <li>To set the user ID to “Administrator” for connecting to Microsoft Active Directory in the MSAD edition: <b>DBUID=CN=Administrator,CN=Users,DC=Alias,DC=com</b></li> <li>To set the user ID to “admin” for connecting to Novell eDirectory in the NED edition: <b>DBUID=cn=admin,o=Alias.com</b></li> </ol>
Remarks	<ul style="list-style-type: none"> <li>This parameter is not subject to the reload command (reload-cert).</li> </ul>

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

---

- This parameter is not downloaded at startup when using a replication configuration.
- If the failover settings for the Authentication DB are made in the LDAP, MSAD, NED, MySQL, or OpenLDAP editions, the user ID that was set by this parameter is used for all databases. As a result, the user IDs connected to each database must be unified.
- In the MySQL edition, the user ID is case sensitive. In other Authentication DB, the user ID is not case sensitive.

See also            DBPWD

## DBPWD overwrite

Overview	Sets the user password for connecting to the Authentication DB.
Format	<p>ORACLE, LDAP, MSAD, NED, MySQL, and OpenLDAP editions</p> <p><b>DBPWD=<u>password</u></b></p> <ul style="list-style-type: none"><li>• The password can be described in cleartext, but after the Authentication Module starts, it is encrypted as follows: DBPWD={IW}[encrypted password]</li><li>• This parameter does not need to be set in the CSV edition.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value in the standard configuration file is set to the values below. ORACLE edition : tiger LDAP edition : passwd MSAD edition : Administrator NED edition : passwd MySQL edition : new_password OpenLDAP edition: password</li></ul>
Configuration example	<p>1) To set “tiger” as the password for the user connecting to the Authentication DB:</p> <p><b>DBPWD=tiger</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• If the failover settings for the Authentication DB are made in the LDAP, MSAD, NED, or MySQL editions, the password that was set by this parameter is used for all databases. As a result, the passwords connected to each database must be unified.</li></ul>
See also	DBUID

---

Authentication Module configuration file (cert.conf)

---

## DBTBL

Overview	Sets the Authentication DB table name, directory entry name, or database file name.
Format	<p>ORACLE and MySQL editions <b>DBTBL=<u>table name</u></b></p> <ul style="list-style-type: none"><li>• Read and update permissions for the table/view are required.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is icewalltest.</li></ul> <p>LDAP, MSAD, NED, and OpenLDAP editions <b>DBTBL=<u>directory entry name=value</u>[, ...]</b></p> <ul style="list-style-type: none"><li>• There is no default value in the executable binary file.</li><li>• The initial value in the standard configuration file is set to the values below. LDAP edition : o=Alias.com MSAD edition : CN=Users,DC=is,DC=com NED edition : o=Alias.com OpenLDAP edition: ou=icewalltest,dc=jpn,dc=hp,dc=com</li></ul> <p>CSV edition <b>DBTBL=<u>CSV database file name</u></b></p> <ul style="list-style-type: none"><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ssso/certd/config/sample.csv.</li></ul>
Configuration example	<p>1) To set “icewalluser” as the Authentication DB table name in the ORACLE edition: <b>DBTBL=icewalluser</b> <b>DBTBL=icewall.icewalluser</b> (For a table created by the user “icewall”)</p> <p>2) To set “ou=org1,o=Alias.com” as the Authentication DB directory entry name in the LDAP edition: <b>DBTBL=ou=org1,o=Alias.com</b></p>



- 3) To set “CN=Users,DC=hp,DC=com” as the Authentication DB directory entry name in the MSAD edition:  
**DBTBL=CN=Users,DC=hp,DC=com**
- 4) To set “o=Alias.com” as the Authentication DB directory entry name in the NED edition:  
**DBTBL=o=Alias.com**
- 5) To set “icewalluser” as the Authentication DB table name in the MySQL edition:  
**DBTBL=icewalluser**
- 6) To set /opt/icewall-ss0/certd/config/sample.csv as the CSV database file name in the CSV edition:  
**DBTBL=/opt/icewall-ss0/certd/config/sample.csv**

Remarks

- This parameter is not subject to the reload command (reload-cert).
- This parameter is not downloaded at startup when using a replication configuration.
- Because the data under the directory entry set by this parameter in the LDAP, MSAD, NED, and OpenLDAP editions is subject to user search, users registered in the subdirectories are also subject to authentication.
- Because the case-sensitive setting for the MySQL edition database name depends on the MySQL initialization parameter “lower\_case\_table\_names,” set that parameter to 1 to make the name case-insensitive.

See also

LOGDBTBL  
REFTBL

## DBATTR

Overview	Sets the file name for the Authentication DB column information file.
Format	<b>DBATTR=<u>authentication DB column information file name</u></b> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• The default value set in the executable binary file is /opt/icewall-ss0/certd/config/dbattr.conf.</li><li>• The initial value set in the standard configuration file is /opt/icewall-ss0/certd/config/dbattr.conf.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	1) To set the standard Authentication DB column information file name: <b>DBATTR=/opt/icewall-ss0/certd/config/dbattr.conf</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• The setting value for this parameter does not vary by Authentication DB.</li></ul>
See also	LOGDBATTR

# DBEXATTR

Overview	Sets additionally referenced columns (attributes) other than the ones IceWall uses on the Authentication DB.
Format	<b>DBEXATTR=<u>column name 1</u>[,<u>column name 2</u>][, ...]</b> <ul style="list-style-type: none"><li>• Multiple column names can be specified by separating them with a comma.</li><li>• The total number of bytes for all column names must be 4087 or less per line, including the commas used to separate the column names.</li><li>• This parameter can span multiple lines.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set “PASSWD1” and “PASSWD2” as additionally referenced columns: <b>DBEXATTR=PASSWD1,PASSWD2</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• The setting value for this parameter does not vary by Authentication DB.</li><li>• Columns set with this parameter must be included in the table set with the DBTBL parameter. Columns in other tables cannot be referenced.</li><li>• Columns cannot be set by this parameter in the Authentication DB column information file (dbattr.conf).</li><li>• The number of columns that can be set, including the number set in the column information configuration file and the number set in this</li></ul>

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

parameter, must total 1000 or less. The number of columns that can be set by combining the tables used is shown below.

Used tables & columns	Number of available columns
Authentication table (no additional columns)	Up to 1000 columns in the authentication table only
Authentication table + additional columns	Up to a total of 1000 columns for the authentication table + additional columns
Authentication table Reference table	Up to 1000 columns in the reference table only
Authentication table + additional columns Reference table	Up to 1000 columns in the reference table only
Authentication table Audit log output table	Up to 1000 columns in the authentication table only
Authentication table + additional columns Audit log output table	Up to a total of 1000 columns for the authentication table + additional columns
Authentication table + additional columns Reference table Audit log output table	Up to 1000 columns in the reference table only

Authentication itself will succeed if the number of columns is set to 1001 or higher, but the columns starting from 1025 cannot be referenced.

- In the ORACLE edition, about 16 kilobytes is provided for the length of the SQL statement issued when the Authentication Module acquires the data from the Authentication DB. As a result, if 1000 columns are used, set the length of one column up to a maximum of 16 bytes. If the number of columns used is small, the length of a column name can exceed 16 bytes without a problem.
- Be aware that if multiple columns are set with the same name in this parameter, the value is set to all columns in the ORACLE, CSV, and MySQL editions, but the value is not set except for the starting column in the LDAP, MSAD, and NED editions.
- Both the DBEXATTR parameter and the DBCRYPTOATTR parameter must be configured for columns subject to encryption. Be aware that columns are not subject to encryption if only the DBEXATTR attribute is configured.

See also

DBCRYPTOATTR  
REFATTR

# DBCRYPTOTYPE 10.0

Overview	<p>Sets the encryption type for decrypting data encrypted in the Authentication DB.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>DBCRYPTOTYPE=<u>type</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the type:<ul style="list-style-type: none"><li>0 : Do not use the Authentication DB column encryption function</li><li>1 : Use only the product's standard encryption</li><li>2 : Use only the custom encryption</li><li>3 : Use both the product's standard encryption and custom encryption</li></ul></li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li><li>• This setting makes the columns configured in the DBCRYPTOATTR parameter subject to decryption.</li></ul>
Configuration example	<p>1) When additionally referenced columns have been encrypted with the product's standard encryption only:</p> <p><b>DBCRYPTOTYPE=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li></ul>
See also	<p>DBCRYPTOATTR</p> <p>DBIWCRYPTOSEED</p>

# DBIWCRYPTOSEED 10.0

**Overview** Sets the seed passed to the Authentication DB encryption library for the product's standard encryption.

This parameter is available since version 10.0.

**Format** **DBIWCRYPTOSEED=seed**

- The seed may contain the following types of characters:
  - Numerical characters (0 to 9)
  - Alphabetical characters (a to z, A to Z)
  - Symbols ("-", "\_", ".", "!", "~", "\*", "(", ")")
- Define the seed within 1 to 255 bytes.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file.  
(commented out)
- The system is not guaranteed to work as expected if the value for this parameter is out of range.
- This parameter is used by the Authentication DB encryption library for the product's standard encryption.
- The seed can be defined in clear text, but it is encrypted after the Authentication Module starts and becomes the line below.  
DBIWCRYPTOSEED={IW}encrypted seed

**Configuration example** 1) To set the seed value used when decrypting values encrypted with the product's standard encryption:  
**DBIWCRYPTOSEED=cryptoseed**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is downloaded at startup when using a replication configuration.
- Set this parameter when DBCRYPTOTYPE is 1 or 3.
- Errors may result if the seed uses unsupported characters or does not fit within the guidelines presented here.

**See also** DBCRYPTOATTR  
DBCRYPTOTYPE

# DBCRYPTOATTR 10.0

**Overview** Sets the column using the encrypted value.

This parameter is available since version 10.0.

**Format** **DBCRYPTOATTR=column name 1[, column name 2]**

- The total number of bytes for all column names must be 4087 or less, including the commas used to separate the column names.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)
- The system is not guaranteed to work as expected if the value for this parameter is out of range.
- This parameter can be the same as the column names set in DBEXATTR.
- The system is not guaranteed to work as expected when the column names set to this parameter are other than those set in DBEXATTR.
- If any column is not set to this parameter, decryption is not performed in the Authentication DB encryption library.

**Configuration example** 1) When additionally referenced columns are encrypted:  
**DBCRYPTOATTR=CRYPTODATA1,CRYPTODATA2**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is downloaded at startup when using a replication configuration.

**See also** DBEXATTR  
DBCRYPTOTYPE  
DBIWCRYPTOSEED

---

Authentication Module configuration file (cert.conf)

---

## LDAPBIND

Overview	Sets whether judgment is performed by bind authentication on the Authentication DB during user authentication.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPBIND=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : No BIND authentication is performed</li><li>1 : BIND authentication is performed</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• If any other value is set, the parameter defaults to 0.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value in the standard configuration file is set to the values below.<ul style="list-style-type: none"><li>LDAP edition : 0</li><li>MSAD edition : 1</li><li>NED edition : 1</li><li>OpenLDAP edition: 0</li></ul></li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To perform judgment by BIND authentication during user authentication:</p> <p><b>LDAPBIND=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When this parameter is set to 1, user authentication is judged pass/fail by BIND authentication, but the user information is acquired for the user that was set in DBUID and DBPWD.</li></ul>



See also        DBUID  
                 DBPWD  
                 LDAPPCHG  
                 LDAPLANG

## LDAPPCHG

Overview	Sets whether an update is made to the Authentication DB when the password is changed.								
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPPCHG=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not update the Authentication DB</li><li>1 : Update the Authentication DB</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value in the standard configuration file is set to the values below.<table><tr><td>LDAP edition</td><td>: 1</td></tr><tr><td>MSAD edition</td><td>: 0</td></tr><tr><td>NED edition</td><td>: 1</td></tr><tr><td>OpenLDAP edition:</td><td>1</td></tr></table></li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>	LDAP edition	: 1	MSAD edition	: 0	NED edition	: 1	OpenLDAP edition:	1
LDAP edition	: 1								
MSAD edition	: 0								
NED edition	: 1								
OpenLDAP edition:	1								
Configuration example	<p>1) To update the Authentication DB when the password is changed:</p> <p><b>LDAPPCHG=1</b></p>								
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• When using Microsoft Active Directory for the Authentication DB, set the LDAPPCH and ADPCHG parameters to 1 to use the password change function.</li></ul>								
See also	<p>ADPCHG</p> <p>LDAPBIND</p>								

LDAPLANG

# LDAPLANG

Overview	Sets whether to convert the character code of the user information obtained from the Authentication DB.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPLANG=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : No character code conversion is performed</li><li>1 : Character code conversion is performed</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value in the standard configuration file is set to the values below. LDAP edition : 1 MSAD edition : 0 NED edition : 1 OpenLDAP edition: 1</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To convert the character code of the user information:</p> <p><b>LDAPLANG=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• Character code conversion uses the iconv function of the OS to convert from Unicode (UTF-8) to the code that was set by the environment variable IW_LANG. If the user information was not saved in Unicode in the Authentication DB, the character code is not converted even if the flag is set to 1</li></ul>

- This parameter should be set to 0 when using Microsoft Active Directory for the Authentication DB because the character code conversion function is not supported.

See also      LDAPBIND  
                 LDAPPCHG

# LDAPSSL

Overview	Sets whether to use SSL when connecting to the LDAP server.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPSSL=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : SSL connection is not used (backward compatibility/default operation)</li><li>1 : SSL connection is used</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• For LDAPSSL=1, the default port for the server in DBHOST changes from 389 to 636.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To connect to the LDAP server using an SSL connection:</p> <p><b>LDAPSSL=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>DBHOST LDAPCACERT LDAPVERIFYSVRCERT LDAPCIPHERSUITE LDAPSSLBIND ADPCHG</p>

# LDAPCACERT

Overview	Sets the CA certificate file when establishing SSL connections with the LDAP server.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPCACERT=<u>CA certificate file name</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The PEM format is supported for the certificate file format.</li><li>• Effective only when LDAPSSL=1.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is /opt/icewall-sso/certd/config/cacert.pem.</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To set the CA certificate that is the default value in the standard configuration file:</p> <p><b>LDAPCACERT=/opt/icewall-sso/certd/config/cacert.pem</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>DBHOST LDAPSSL LDAPVERIFYSVRCERT LDAPCIPHERSUITE LDAPSSLBIND ADPCHG</p>

# LDAPVERIFYSVRCERT

Overview	Sets whether or not to verify the CA certificate with the certificate presented by the server when establishing SSL connections with the LDAP server.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPVERIFYSVRCERT=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not verify the presented certificate</li><li>1 : Verify the presented certificate</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• Effective only when LDAPSSL=1.</li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To not check the details of the server certificate:</p> <p><b>LDAPVERIFYSVRCERT=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>DBHOST LDAPSSL LDAPCACERT LDAPCIPHERSUITE LDAPSSLBIND ADPCHG</p>



# LDAPCIPHERSUITE

Overview	Sets the SSL encryption strength when establishing SSL connections with the LDAP server.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPCIPHERSUITE=<u>encryption format</u></b></p> <ul style="list-style-type: none"><li>• The encryption format has a maximum length of 255 bytes.</li><li>• The encryption format set to this parameter is the same as the encryption format used by openssl. In an environment with OpenSSL installed, check the cipher characters with “openssl ciphers -v”.</li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• Effective only when LDAPSSL=1.</li><li>• The default value in the executable binary file is “Do not configure”.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To use “AES128-MD5” as the encryption format for SSL connections:</p> <p><b>LDAPVERIFYSVRCERT=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>DBHOST LDAPSSL LDAPCACERT LDAPVERIFYSVRCERT LDAPSSLBIND ADPCHG</p>

# LDAPSSLBIND

Overview	When using LDAP BIND and SSL communication, sets whether or not to use SSL communication during only BIND.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPSSLBIND=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not establish SSL connections during BIND</li><li>1 : Establish SSL connections during BIND (default operation)</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• Effective only when LDAPSSL=1.</li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) Connections are normally established using SSL, but to not use SSL in LDAP BIND authentication:</p> <p><b>LDAPSSLBIND=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>DBHOST LDAPBIND LDAPSSL LDAPCACERT LDAPVERIFYSVRCERT LDAPCIPHERSUITE ADPCHG</p>

# ADPCHG

Overview	Sets whether or not to perform password change operations for Active Directory.
Format	<p>MSAD edition only</p> <p><b>ADPCHG=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not perform password change operations for Active Directory (backward compatibility/default operation)</li><li>1 : Perform password change operations for Active Directory</li></ul></li><li>• This parameter does not need to be set in the editions other than the MSAD edition.</li><li>• Effective only when LDAPSSL=1.</li><li>• The default value set in the executable binary file is 0.</li><li>• The default value in the standard configuration file is set to 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To use the password change function for users in Active Directory:</p> <p><b>ADPCHG=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• PASSWORD (Authentication DB column information file) must be set with unicodePWD.</li></ul>
See also	<p>DBHOST</p> <p>LDAPSSL</p> <p>LDAPCACERT</p> <p>LDAPVERIFYSVRCERT</p> <p>LDAPCIPHERSUITE</p> <p>LDAPSSLBIND</p>

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

---

LDAPPCHG

PASSWORD (Authentication DB column information file)

# LDAPMULTIVAL

Overview	Sets whether or not to retrieve all values when there are multiple LDAP attribute values.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPMULTIVAL=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Disable the multi-value function (backward compatibility/default operation)</li><li>1 : Enable the multi-value function</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 0.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To support LDAP multi-values:</p> <p><b>LDAPMULTIVAL=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>ADGROUP ADGROUPDN ADGROUPINTERVAL ADGROUPPRINAME ADGROUPPREFIX</p>

# LDAPREFERRAL

Overview	Sets whether or not to disable the LDAP referral function.
Format	<p>LDAP, MSAD, NED, and OpenLDAP editions only</p> <p><b>LDAPREFERRAL=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Disable the referral function</li><li>1 : Enable the referral function (backward compatibility/default operation)</li></ul></li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To not use the LDAP referral function:</p> <p><b>LDAPREFERRAL=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	None

# ADDGFWBIND

Overview	Sets whether or not to perform BIND authentication during authentication when using the Domain Gateway Option.
Format	<p>MSAD edition only</p> <p><b>ADDGFWBIND=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : BIND authentication is performed</li><li>1 : No BIND authentication is performed (backward compatibility/default operation)</li></ul></li><li>• This parameter does not need to be set when LDAPBIND is set to a value other than 1.</li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To not perform LDAP BIND when using the Domain Gateway Option:</p> <p><b>ADDGFWBIND=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• This configuration parameter can be used with the Domain Gateway Option and the SAML Option.</li></ul>
See also	LDAPBIND

### **3.1.6 Audit log table related parameters**

These parameters configure an audit log output table other than the Authentication DB's authentication table. These parameters are only for the ORACLE edition.

<b>Parameter name</b>	<b>Mandatory</b>	<b>Overview</b>
LOGDBTBL	×	Sets the audit log output table
LOGDBATTR	×	Sets the audit log columns
LOGDBSEQNAME	×	Sets the sequential object for audit log output

For details on these parameters, see the following pages.



# LOGDBTBL

Overview	Sets the table name where the login/logout audit message log is output.
Format	<p>ORACLE edition only</p> <p><b>LOGDBTBL=<u>log output table name</u></b></p> <ul style="list-style-type: none"><li>• Insert permission for the table is required.</li><li>• If this parameter is omitted, login/logout audit messages are output to the access log file without writing to the log output table.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set “HISTORYTBL” as the log output table:</p> <p><b>LOGDBTBL=HISTORYTBL</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• The table set with this parameter must exist within the host ID set with the DBHOST parameter. A table with a different host ID cannot be set.</li><li>• When this parameter is set, the target log messages are no longer output to the access log file, but they are output to the access log file if output to the table fails.</li></ul>
See also	<p>DBTBL</p> <p>REFTBL</p> <p>LOGDBSEQNAME</p>

# LOGDBATTR

Overview	Sets the file name for the log column information file.
Format	<p>ORACLE edition only</p> <p><b>LOGDBATTR=<u>log column information file name</u></b></p> <ul style="list-style-type: none"><li>• The file name has a maximum length of 255 bytes.</li><li>• If LOGDBTBL has been specified, this parameter is required.</li><li>• The default value set in the executable binary file is /opt/icewall-ssocertd/config/logdbattr.conf.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the standard log column information file:</p> <p><b>LOGDBATTR=/opt/icewall-ssocertd/config/logdbattr.conf</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>DBATTR</p> <p>LOGDBSEQNAME</p>

# LOGDBSEQNAME

Overview	Sets the name of the object that issues sequential numbers for the log output table.
Format	<p>ORACLE edition only</p> <p><b>LOGDBSEQNAME=<u>sequential type object name</u></b></p> <ul style="list-style-type: none"><li>• If the LOGDBTBL parameter has been specified, this parameter is required.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set “SEQ” as the sequential object for the log output table:</p> <p><b>LOGDBSEQNAME=SEQ</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li></ul>
See also	<p>LOGDBTBL</p> <p>LOGBATTR</p>

### **3.1.7 Reference table related parameters**

These parameters configure a reference table other than the authentication table included in the Authentication DB. These parameters are for the ORACLE and MySQL editions only.

<b>Parameter name</b>	<b>Mandatory</b>	<b>Overview</b>
REFTBL	×	Sets the reference table
REFATTR	×	Sets the reference table columns
REFUID	×	Sets the user ID column for the reference table

For details on these parameters, see the following pages.

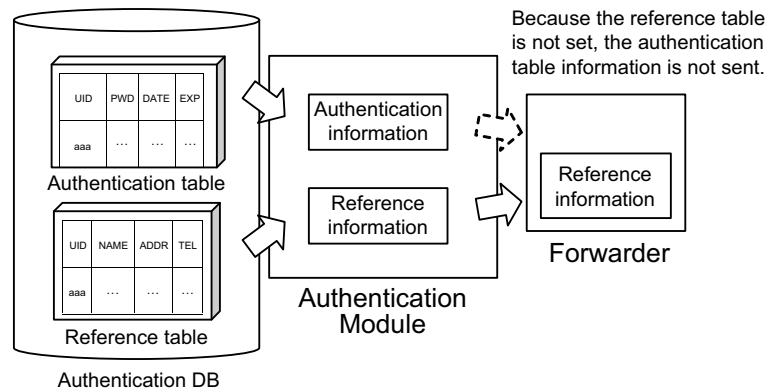
# REFTBL

Overview	Sets the reference table name for referring to user information other than the table name used for user authentication.
Format	<p>ORACLE and MySQL editions only</p> <p><b>REFTBL=<u>reference table name</u></b></p> <ul style="list-style-type: none"><li>• Reference permission is required for the specified table.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	<p>1) To set “REF_TBL” as the reference table name:</p> <p><b>REFTBL=REF_TBL</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• For the ORACLE edition, the table set with this parameter must exist within the host ID set with the DBHOST parameter. A table with a different host ID cannot be set.</li><li>• For the MySQL edition, the table set with this parameter must exist within the database set with the DBHOST parameter. A table with a different database name cannot be set.</li><li>• The Authentication DB encryption library cannot decrypt the column in the reference table.</li><li>• When a reference table is set, only information in the reference table columns can be sent to the Backend Web Server as user information. Authentication table columns are not sent. Also, additional reference table columns set with the DBEXATTR parameter are not sent.</li></ul>

---

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

---



See also

DBTBL  
LOGDBTBL  
REFATTR  
REFUID

# REFATTR

Overview	Sets the column names for the reference table.
Format	<p>ORACLE and MySQL editions only</p> <p><b>REFATTR=<u>column name 1</u>[,<u>column name 2</u>][, ...]</b></p> <ul style="list-style-type: none"><li>• Up to 1000 column names can be set.</li><li>• The total number of bytes for all column names must be 4087 or less, including the commas used to separate the column names.</li><li>• This parameter can span multiple lines.</li><li>• If the REFTBL parameter has been specified, this parameter is required.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is PASSWD1,PASSWD2.</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To set “PASSWD1” and “PASSWD2” as column names in the reference table:</p> <p><b>REFATTR=PASSWD1,PASSWD2</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• SQL reserved words cannot be specified for the column names set to this parameter.</li></ul>
See also	<p>DBEXATTR</p> <p>REFTBL</p> <p>REFUID</p>

## REFUID

Overview	Sets the column name used as the user ID in the reference table columns.
Format	<p>Oracle and MySQL editions only</p> <p><b>REFUID=<u>column name for user ID</u></b></p> <ul style="list-style-type: none"><li>• If the REFTBL parameter has been specified, this parameter is mandatory.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is USERID.</li></ul>
Configuration example	<p>1) To set “USERID” as the user ID column for the reference table:</p> <p><b>REFUID=USERID</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• The column set by this parameter is used to find information about the logged in user using the reference table.</li><li>• If the logged in user does not exist in the reference table, a system error occurs.</li></ul>
See also	None



### 3.1.8 System tuning related parameters

These parameters are used to perform system tuning for the Authentication Module.

Parameter name	Mandatory	Overview
MAXREQTHREAD	×	Sets the number of request threads
ACCTHREAD <b>10.0</b>	×	Sets the number of access threads (threads allocated to requests that do not require DB connections)
REQQUEUE	×	Sets the request queue size
MAXDBCONNECT	×	Sets the number of Authentication DB connections
DBQUEUE <b>10.0</b>	×	Sets the size of the queue that the update process data (the login status update process performed when the user logs out) for the Authentication DB is temporarily saved in.
LOGDBQUEUE <b>10.0</b>	×	Sets the size of the queue to temporarily save audit log data for the historical DB
LOGBUFSIZE	×	Sets the log buffer size
CACHE	×	Sets the maximum number of logins
MAXLOGINUSER <b>10.0</b>	×	Sets the allowable user logins
RECVWAITTIME	×	Sets the receive timeout time
THREADSTACKSIZE	×	Sets the stack size of the thread created by the Authentication Module
LOGMULTITHREAD <b>10.0</b>	×	Sets whether or not to output the access log, error log, and the performance log to files with a multi-threaded operation
DOWNLOADCONFFLG <b>10.0</b>	×	Sets whether or not to download configuration information from the replication target at startup

For details on these parameters, see the following pages.

# MAXREQTHREAD

Overview	Sets the number of threads for request processing.
Format	<b>MAXREQTHREAD=<u>number of threads</u></b> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is 10.</li><li>• The initial value set in the standard configuration file is 10.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If this parameter is set to 0 or less, the system operates with the default value.</li></ul>
Configuration example	1) To set 10 for the number of threads for request processing: <b>MAXREQTHREAD=10</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• Calculate the number of request threads with the formulas below as a reference, taking into consideration the number of possible requests to the Authentication Module and the processing time to the Authentication DB. If ACCTHREAD is not configured: <math display="block">\text{MAXREQTHREAD} = \text{MAXDBCONNECT} + (\text{number of CPUs}^{*1} \times 2)</math> If ACCTHREAD is configured: <math display="block">\text{MAXREQTHREAD} = \text{MAXDBCONNECT} + \text{ACCTHREAD} + \text{DB connection wait count}^{*2}</math>  <p>*1 For multi-core CPUs, a single core is counted as one CPU.</p><p>*2 A DB connection busy error is returned for the DB connection requests exceeding (MAXREQTHREAD-ACCTHREAD) when ACCTHREAD is configured. Set MAXREQTHREAD so that it includes the DB connection wait count that equals or exceeds the number of requests within the DB processing time.</p></li></ul>

Example 1:

MAXDBCONNECT is 2, the number of CPUs is 3, ACCTHREAD is not set (2+6), then  
MAXREQTHREAD=8

Example 2:

MAXDBCONNECT is 2, the number of CPUs is 3, DB connection wait count is 4, ACCTHREAD is set (2+6+4), then  
MAXREQTHREAD=12

- HP recommends changing the kernel parameters values below to those calculated from the formulas.  
max\_thread\_proc=MAXREQTHREAD+MAXREPTHREAD+10 or more  
maxfiles=MAXREQTHREAD+MAXREPTHREAD+MAXDBCONNECT+10 or more.

See also

MAXDBCONNECT  
MAXREPTHREAD  
ACCTHREAD

## ACCTHREAD 10.0

Overview	<p>Sets the number of request threads for requests that do not require DB connections in the request thread.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>ACCTHREAD=<u>number of threads</u></b></p> <ul style="list-style-type: none"><li>• The configurable range is between 0 and (MAXREQTHREAD-1).</li><li>• The default value in the executable binary file is 0. (backward compatibility)</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To allocate 3 threads for requests that do not require DB connections out of 10 request threads:</p> <p><b>MAXREQTHREAD=10</b> <b>ACCTHREAD=3</b></p> <p>In this case, 7 threads are used both for requests that require DB connections and for requests that do not require DB connections, and 3 threads are only used for requests that do not require DB connections.</p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• If this parameter is not configured or if this parameter is set to 0, there is no thread allocated exclusively for requests that do not require DB connections. All request threads process requests without differentiating the need for DB connections. (backward compatibility)</li></ul>

- Calculate the number of threads based on the formula below.

$ACCTHREAD = (\text{number of CPUs} \times 2)$

Example: If the number of CPUs is 3 ( $3 \times 2$ )

$ACCTHREAD=6$

\* For multi-core CPUs, a single core is counted as one CPU.

- Set this parameter so that  $(MAXREQTHREAD - ACCTHREAD) > MAXDBCONNECT$ .
- Adjust the value calculated with  $MAXREQTHREAD - ACCTHREAD - MAXDBCONNECT$  to be equal or larger than the average "number of requests that require DB connections by DB processing time" so that the DB connection busy error occurs less frequently.  
However, if DB connection requests occur that instantaneously exceed  $(MAXREQTHREAD - ACCTHREAD)$ , the DB connection busy error is returned without waiting for DB connections to be freed.

See also

`MAXREQTHREAD`  
`MAXDBCONNECT`

# REQQESIZE

Overview                Sets the request queue size.

Format                 **REQQESIZE=queue size**

- The default value set in the executable binary file is 20.
- The initial value set in the standard configuration file is 20.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If this parameter is set to 0 or less, the system operates with the default value.

Configuration example    1) To set 20 as the request queue size:  
                              **REQQESIZE=20**

Remarks                • This parameter is not subject to the reload command (reload-cert).

                              • This parameter is not downloaded at startup when using a replication configuration.

                              • All requests enter the request queue, and then afterward, they are processed in request threads.

                              • If the value for the MAXREPTHREAD parameter is larger than the value for this parameter, the queue may overflow in replication operations, so set the value of this parameter to be larger than MAXREPTHREAD.

See also                REPQESIZE  
                              MAXREQTHREAD

# MAXDBCONNECT

Overview	Sets the number of simultaneous connections to the Authentication DB.
Format	<p>ORACLE, LDAP, MSAD, NED, MySQL, and OpenLDAP editions only</p> <p><b>MAXDBCONNECT=number of simultaneous connections</b></p> <ul style="list-style-type: none"><li>• This parameter does not need to be set in the CSV edition.</li><li>• The default value set in the executable binary file is 2.</li><li>• The initial value set in the standard configuration file is 2.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If this parameter is set to 0 or less, the system operates with the default value.</li></ul>
Configuration example	<p>1) To set 4 as the number of simultaneous connections to the Authentication DB:</p> <p><b>MAXDBCONNECT=4</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• If the number of simultaneous connections is 2 or more, additional Authentication DB user licenses may be required.</li><li>• When the Authentication Module is started, it establishes the number of simultaneous connections set by this parameter to the Authentication DB. The Authentication Module uses these connections to reference/change the Authentication DB. If the connections established at startup are disabled for reasons such as the Authentication DB disconnecting, an error is detected when these connections are used, and they are reconnected. The connection between the Authentication Module and the Authentication DB is not connected and disconnected per single request.</li></ul>
See also	MAXREQTHREAD

Authentication Module configuration file (cert.conf)

---

ACCTHREAD



## DBQUEUESIZE 10.0

Overview	<p>Sets the size of the queue that the update process data (the login status update process performed when the user logs out) for the Authentication DB is temporarily saved in. The queue is not used when the LOGINSTAT parameter in the Authentication DB column configuration file is not configured</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b><u>DBQUEUESIZE=authentication DB processing queue size</u></b></p> <ul style="list-style-type: none"><li>• The default value in the executable binary file is the value of the CACHE parameter.</li><li>• There is no initial value in the standard configuration file.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If this parameter is set to less than 100, the system operates with the default value.</li></ul>
Configuration example	<p>1) To set the Authentication DB processing queue to 200: <b>DBQUEUESIZE=200</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• Normally there is no need to set this parameter.</li></ul>
See also	<p>CACHE</p>

## LOGDBQUESIZE 10.0

Overview	<p>Sets the size of the queue to temporarily save audit log data for the historical DB.</p> <p>Not used when the historical DB function is disabled.</p> <p>This parameter is available since version 10.0.</p>
Format	<p>Oracle edition only</p> <p><b>LOGDBQUESIZE=log DB processing queue size</b></p> <ul style="list-style-type: none"><li>• The default value in the executable binary file is (the CACHE parameter value / 2).</li><li>• There is no initial value in the standard configuration file.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If this parameter is set to less than 50, the system operates with the default value.</li></ul>
Configuration example	<p>1) To set the log DB processing queue to 100:</p> <p><b>LOGDBQUESIZE=100</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• Normally there is no need to set this parameter.</li></ul>
See also	<p>LOGDBTBL</p> <p>CACHE</p>

# LOGBUFSIZE

Overview	Sets the buffer size for the output log file (number of messages).
Format	<b>LOGBUFSIZE=<u>log buffer size</u></b> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is 1000.</li><li>• The initial value set in the standard configuration file is 1000.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If this parameter is set to 0 or less, the system operates with the default value.</li></ul>
Configuration example	1) To set the log buffer size to 2,000 messages: <b>LOGBUFSIZE=2000</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• Buffer areas are provided for the access log and error log that can store the number of messages based on the value set by this parameter.</li><li>• The performance log is also provided with its own buffer area in the same way as the access log and error log.</li><li>• If the number of messages exceeds the log buffer size, log messages are deleted starting from the oldest ones, and new messages are added.</li><li>• If the number of messages exceeds the log buffer size, the log messages below are output to the system log. certd: [%d]: Log buffer exceeded 'LOGBUFSIZE' value [ACCESS] certd: [%d]: Log buffer exceeded 'LOGBUFSIZE' value [ERROR] certd: [%d]: Log buffer exceeded 'LOGBUFSIZE' value [PERFORMANCE] Output value: [Authentication Module process ID]</li></ul>

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

---

See also            None

# CACHE

Overview	Sets the maximum number of simultaneous user logins.
Format	<b><u>CACHE=maximum number of simultaneous user logins</u></b> <ul style="list-style-type: none"><li>• The default value set in the executable binary file is 10.</li><li>• The initial value set in the standard configuration file is 100.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	1) To set the maximum number of simultaneous user logins to 1,000: <b>CACHE=1000</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• If multiple logins are performed for the same user ID when duplicate logins are allowed (DUPLOGIN=1), each logged in user is counted as a valid user.</li></ul> <p>For example, if 10 is set to this parameter, the maximum number of simultaneous logins is reached at the moment the same user logs in 10 times. A “login limit error” results if an 11th login is performed.</p> <ul style="list-style-type: none"><li>• The limit on the number of logged in users depends on the limit of the memory area supported by the OS. For details about the calculation method for memory used by a single user, see “User's Manual.”</li><li>• If MAXLOGINUSER is configured, the login limit error occurs even when the number of users logged in has not reached the maximum number of simultaneous user logins.</li></ul>
See also	LOGIN_ERR_LIMIT (HTML configuration file) MAXLOGINUSER

## MAXLOGINUSER 10.0

Overview	<p>Sets the number of users that can log in.</p> <p>If this parameter is not configured, the system operates with the maximum number of simultaneous user logins (CACHE parameter value) as the value for this parameter.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>MAXLOGINUSER =<u>allowable user logins</u></b></p> <ul style="list-style-type: none"><li>• The allowable user logins can be set in the range of 0 to the CACHE parameter value.</li><li>• The default value in the executable binary file is the value of the CACHE parameter.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To set the number of users that can login to 500 when the maximum number of simultaneous user logins is 1000:</p> <p><b>CACHE=1000</b></p> <p><b>MAXLOGINUSER=500</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is downloaded at startup when using a replication configuration.</li><li>• A login limit error occurs if a log in request is made that would cause the number of users logged in to exceed the number of users that can log in.</li></ul>

- This parameter is effective for new login. Changing this parameter while an Authentication Module is running does not cause currently logged in users to log out. Authorization, logging out, and changing password of currently logged in users are available after executing the reload command (reload- cert).
- If this parameter is set to 0, users cannot newly log in. For details, see “3.9 Handling Authentication Module maintenance” and “4.20.10 Changing the maximum number of allowable user logins” in the User’s Manual.

See also      LOGIN\_ERR\_LIMIT (HTML configuration file)  
                CACHE

# RCVWAITTIME

Overview                Sets the timeout value (seconds) when receiving a request.

Format                 **RCVWAITTIME=receive timeout value (seconds)**

- The receive timeout value can be set in the range of 1 to 60.
- The unit for setting the receive timeout value is seconds.
- The default value set in the executable binary file is 3.
- The initial value set in the standard configuration file is 3.
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

Configuration example    1) To set the receive timeout value to 10 seconds:  
**RCVWAITTIME=10**

Remarks                • This parameter is not subject to the reload command (reload-cert).

• This parameter is not downloaded at startup when using a replication configuration.

• Normally, this parameter does not need to be set, but it should be set to a higher value if a high volume of network traffic between Forwarder (agent) and the Authentication Module causes receive request errors to occur on the Authentication Module side.

See also                None



# THREADSTACKSIZE

Overview	Sets the stack size of all threads created by the Authentication Module.
Format	<b>THREADSTACKSIZE=<u>stack size of one thread</u> (kilobytes)</b> <ul style="list-style-type: none"><li>• The stack size is specified in kilobytes.</li><li>• The default value set in the executable binary file is 256.</li><li>• The initial value set in the standard configuration file is 256.</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	1) To set the stack size to 512 kilobytes: <b>THREADSTACKSIZE=512</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• The system is not guaranteed to work as expected if a value less than the default value (256 kilobytes) is set.</li><li>• The system minimum value is 4 kilobytes for HP-UX and 16 kilobytes for Linux.</li><li>• If this parameter is set to a value that is too small, the Authentication Module may no longer run. Also, if this parameter is set to a value that is too large, the memory used by the Authentication Module will increase, and the Authentication Module may fail to start.</li><li>• If the setting value is smaller than the system minimum value, the IceWall SSO default value (256 kilobytes) is used.</li></ul>
See also	None

# LOGMULTITHREAD 10.0

Overview	<p>Sets whether or not to output the access log, error log, and the performance log to files with multiple threads.</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>LOGMULTITHREAD=flag</b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Output access log, error log, and performance log in one thread</li><li>1 : Output access log, error log, and performance log in separate threads</li></ul></li><li>• This parameter does not need to be set when LDAPBIND is set to a value other than 1.</li><li>• This parameter does not need to be set in the ORACLE, CSV, and MySQL editions.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value set in the standard configuration file is 1.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To output the access log, error log, and performance log in separate threads:</p> <p><b>LOGMULTITHREAD=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• If this parameter is enabled, a file output thread is allocated to the access log, the error log, and the performance log, and this lowers the possibility of log buffer overflows occurring.</li><li>• The performance log is enabled when PERFORMANCE (Authentication Module configuration file) is configured.</li></ul>

- The trace log and the information log are not subject to this function because they do not use the log buffer.
- Please note: If this parameter is set to 0, the messages in multiple log buffers are output in a single thread. If I/O waiting occurs, the log buffer may overflow.

See also      ACCESS  
                 ERROR  
                 PERFORMANCE  
                 LOGPERF  
                 LOGBUFFER

# DOWNLOADCONFFLG 10.0

Overview	<p>Sets whether or not to download configuration information from the replication target Authentication Module at startup</p> <p>This parameter is available since version 10.0.</p>
Format	<p><b>DOWNLOADCONFFLG=<u>flag</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the flag:<ul style="list-style-type: none"><li>0 : Do not download configuration information from the replication target</li><li>1 : Download configuration information from the replication target (backward compatibility)</li></ul></li><li>• The default value set in the executable binary file is 1.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To not download configuration information from the replication target at startup: <b>LOGMULTITHREAD=1</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• If this function is used, one Authentication Module must always be restarted so that the configuration information of another Authentication Module for the replication target becomes the same.</li><li>• When using this function, HP recommends stopping both the Primary and Secondary modules and changing their configurations in environments where it is possible to stop both modules, because the</li></ul>

modules can end up in a state where the Primary and Secondary configuration information is different.

See also            CERT (Authentication Module configuration file)

### 3.1.9 Replication parameters

These parameters configure replication, which duplicates the Authentication Module.

Parameter name	Mandatory	Overview
CERT <span>10.0</span>	×	Sets the Authentication Module to replicate
CERTREPTYPE	×	Sets the type of operation during replication
RETRYCNTC	×	Sets the number of retries for connecting to the replicated Authentication Module
RETRYTMC	×	Sets the retry interval when connecting to the replicated Authentication Module
LIVETIMER	×	Sets the interval for reconnecting to the replicated Authentication Module when it is down
HEALTHTIMER	×	Sets the interval for checking the existence of the replicated Authentication Module
HEALTHCNT	×	Sets the number of retries for checking the existence of the replicated Authentication Module
FAILBACK <span>10.0</span>	×	Sets whether or not to add alive information if the primary certd is live in the response header to the request sender when the Secondary Authentication Module is using ICP 2.0
MAXREPTHREAD	×	Sets the number of replication processing threads
REPQUESIZE	×	Sets the replication queue size

For details on these parameters, see the following pages.

## CERT 10.0

Overview	<p>Sets the host name and port number for the replication target Authentication Module to duplicate.</p> <p>Additional functionality of this parameter is available since version 10.0.</p>
Format	<p><b><u>CERT=host name (or IP address):port number</u></b></p> <ul style="list-style-type: none"><li>• The host name has a maximum length of 64 bytes.</li><li>• The port number cannot be omitted.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul> <p><b><u>CERT=[host name] (or [IP address]):port number</u></b></p> <ul style="list-style-type: none"><li>• When connecting to the replication target Authentication Module giving IPv6 priority, enclose the host name or IP address in square brackets ([ ]).</li></ul>
Configuration example	<p>1) To set “certsvr” as the host name for the Authentication Module to replicate while using the default port number: <b>CERT=certsvr:14142</b></p> <p>2) If the replication target Authentication Module uses IPv6, and the host name “certsvr” uses the default port number: <b>CERT=[certsvr]:14142</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li><li>• Because the parameter settings are shared throughout the system when DOWNLOADCONFFLG is set to “1”, the setting value of the</li></ul>

---

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


---

Authentication Module that is started first is downloaded by the Authentication Modules that are started after it. When this is done, the configuration file on the downloaded side is updated to match the data in the Authentication Module that was started first. The parameters updated for each file are shown below.

Configuration file name	Updated parameters
Authentication Module configuration file	COOKIETIME COOKIEEXP COOKIERETRY LOMETHOD DUPLOGIN DUPKIND PARALOGIN ACCCTRLFLG LOCKCOUNT PWDEXPCHK PWDHISCHK PWDHISCNT PWDEXPWARN DBEXATTR LDAPBIND LDAPLANG LDAPPCHG REFATTR REFUID CACHE ACCTHREAD 10.0 PWDLOGINHASH 10.0 PWDCHGHASH 10.0 TRANSID 10.0 DBCRYPTOATTR 10.0 DBCRYPTOTYPE 10.0 DBIWCRYPTOSEED 10.0 MAXLOGINUSER 10.0 SESSIONIDLEN 10.0 PWDMINLEN 10.0 PWDMAXLEN 10.0 PWDALPHANUM 10.0 PWDEXPIRE 10.0 PWDSAMEPASS 10.0 CERTUNIQUEKEY 10.0
Group configuration file	All group settings
Access control file	All access control settings
Request control configuration file	All request control settings



---

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

---

Configuration file name	Updated parameters
Authentication DB column configuration file	All columns
Log column information file	All columns
Forbidden password configuration file	All forbidden character strings

After downloading these parameters, the updated values are activated.

- To change the setting values of the downloaded parameters, first stop both the Primary and Secondary Authentication Modules, change the setting values, and then restart. You can also change the setting values on one of the Authentication Modules, and reload the configuration file.
- Note that when downloading configuration files other than the Authentication Module configuration file, comment lines are not downloaded.
- When this parameter exists in a configuration file, a connection to the replication target Authentication Module is always attempted when the Authentication Module is started. Please note that the Authentication Module that started first retries the set number of times and if a connection is not possible, an error indicating that the replicating Authentication Module is down is output to the error log.
- To set this parameter with an IPv6 address, you can set a value that omits 0. **10.0**

See also

PORT  
RETRYCNTC (Authentication Module configuration file)  
RETRYTMC (Authentication Module configuration file)  
LIVETIMER  
IPV6LISTEN  
DOWNLOADCONFFLG

# CERTREPTYPE

Overview	Sets the Primary/Secondary Authentication Module when configuring replication.
Format	<p><b>CERTREPTYPE=<u>authentication module type</u></b></p> <ul style="list-style-type: none"><li>• Set one of the following values for the Authentication Module type:<ul style="list-style-type: none"><li>0 : Primary Authentication Module</li><li>1 : Secondary Authentication Module</li></ul></li><li>• This parameter is required when the CERT parameter is set.</li><li>• The default value set in the executable binary file is 0.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li><li>• If the value for this parameter is out of range, the default value is used.</li></ul>
Configuration example	<p>1) To run as the Primary Authentication Module: <b>CERTREPTYPE=0</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li></ul>

- The differences between primary and secondary operation are shown below.

Type	Operation
Primary	<ul style="list-style-type: none"><li>• All functions operate.</li></ul>
Secondary	<ul style="list-style-type: none"><li>• No automatic logout is executed when a login expires. However, logout is executed when the Primary Authentication Module is down.</li><li>• Verifies whether the Primary Authentication Module is alive.</li></ul>

- When using a replication configuration, a Primary and Secondary module must be specified. Please note that normal operation will not be guaranteed if both Authentication Modules have the same type of setting.  
(If both are set as Secondary Authentication Modules, the user is kept in logged in status until manually logged out because no automatic logout is executed.)
- Although the Secondary Authentication Module performs the automatic logout operation when it detects that the Primary Authentication Module is continuously down, a discrepancy may occur in the login expiration date that was set in the COOKIETIME parameter depending on how long it takes until the down Authentication Module is detected.
- Authentication Module replication uses a two-unit configuration for each Authentication Module group. Replication cannot be performed using more units.
- Even if a fallback occurs when using a replication configuration, there is no change in primary/secondary operation.

See also

CERT (Authentication Module configuration file)  
FAILBACK

# RETRYCNTC

Overview	Sets the number of retries attempted if a connection error occurs when connecting to the replication target Authentication Module for replication.
Format	<b>RETRYCNTC=<u>number of retries</u></b> <ul style="list-style-type: none"><li>• If the number of retries is set to zero or less, no retries will be attempted.</li><li>• The default value set in the executable binary file is 10.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	1) To set the number of connection retries for the replication target Authentication Module to 10: <b>RETRYCNTC=10</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li><li>• For details about the connection retry process when connecting to a replication target Authentication Module, see “Forwarder Configuration File--RETRYCNTC Parameter.”</li></ul>
See also	RETRYCNTC (Forwarder configuration file) RETRYTMC (Forwarder configuration file) RETRYTMC (Authentication Module configuration file)

## RETRYTMC 10.0

Overview	<p>Sets the waiting time until attempting to retry a connection when a connection error occurs when connecting to the replication target Authentication Module for replication.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b>RETRYTMC=<u>retry interval</u> (seconds)</b></p> <ul style="list-style-type: none"><li>• The unit for setting the retry interval is seconds.</li><li>• If the retry interval is set to zero or less, there is no waiting time.</li><li>• The default value set in the executable binary file is 3.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	<p>1) To set the waiting time for reconnecting to the replication target Authentication Module to 3 seconds:</p> <p><b>RETRYTMC=3</b></p>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li><li>• For details about the connection retry process when connecting to a replication target Authentication Module, see “Forwarder Configuration File--RETRYTMC Parameter.”</li></ul>
See also	<p>RETRYCNTC (Forwarder configuration file)</p> <p>RETRYCNTC (Authentication Module configuration file)</p> <p>RETRYTMC (Forwarder configuration file)</p>

# LIVETIMER

Overview	Sets the waiting time until attempting another connection for replication after the replication target Authentication Module is determined to be down.
Format	<b>LIVETIMER=<u>waiting time</u> (seconds)</b> <ul style="list-style-type: none"><li>• The unit for setting the waiting time is seconds.</li><li>• The default value set in the executable binary file is 60.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	1) To set a waiting time of 30 seconds until reconnecting to a replication target Authentication Module that is determined to be down: <b>LIVETIMER=30</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li><li>• The operating environment and timing for monitoring should be taken into consideration when determining a value for this parameter.</li><li>• After the set waiting time has passed, another attempt is made to connect to the Secondary Authentication Module. If the Authentication Module is still down, the connection is retried for the number of times specified by the retry count.</li><li>• Replication target down detection is configured by the RETRYTMC parameter and the RETRYCNTC parameter used in the connection to the replication target Authentication Module.</li></ul>

See also       RETRYTMC  
                  RETRYCNTC

# HEALTHTIMER

Overview	Specifies the interval at which the Secondary Authentication Module performs live verification of the Primary Authentication Module.
Format	<b>HEALTHTIMER=<u>live verification interval</u> (seconds)</b> <ul style="list-style-type: none"><li>• The unit for setting the live verification interval is seconds.</li><li>• This parameter is effective when the CERT parameter is set and the CERTREPTYPE parameter is set to 1 (Secondary Authentication Module).</li><li>• The default value in the executable binary file is 5.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	1) To set the live verification interval for the Primary Authentication Module to 60 seconds: <b>HEALTHTIMER=60</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li><li>• Do not set this parameter to a small value (such as 0 to 2) because performance may suffer due to constant or frequent live verifications.</li><li>• The Primary Authentication Module alive check is configured by the RETRYTMC parameter and the RETRYCNTC parameter used in the connection to the replication target Authentication Module.</li></ul>
See also	CERTREPTYPE HEALTHCNT RETRYTMC



RETRYCNTC

# HEALTHCNT

Overview	Sets the down detection count until starting the automatic logout operation when the Authentication Module operating as the Secondary module has detected the Primary Authentication Module is down by the alive check.
Format	<b>HEALTHCNT=<u>down detection count</u></b> <ul style="list-style-type: none"><li>• This parameter is effective when the CERT parameter is set and the CERTREPTYPE parameter is set to 1 (Secondary Authentication Module).</li><li>• The default value set in the executable binary file is 12.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	1) To set 5 as the number of live verification retries when no response is received from the Primary Authentication Module: <b>HEALTHCNT=5</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li><li>• When the Authentication Module is detected as down continuously by the count set to this parameter, the automatic logout operation is started on the Secondary Authentication Module.</li><li>• If the master Authentication Module is detected as recovered, the automatic logout operation on the Secondary Authentication Module stops.</li></ul>
See also	CERTREPTYPE

HEALTHTIMER

## FAILBACK 10.0

**Overview** Sets whether or not to announce that the Primary Authentication Module is alive to the request sender with the Secondary Authentication Module ICP 2.0 response header.

This parameter is available since version 10.0.

**Format** **FAILBACK=flag**

- This parameter is effective only when the CERTREPTYPE parameter is set to 1.
- This parameter is effective only for ICP 2.0 requests.
- Set one of the following values for the flag:
  - 0 : Do not announce that the Primary Authentication Module is alive to the request sender (backward compatibility)
  - 1 : Announce that the Primary Authentication Module is alive to the request sender
- The default value set in the executable binary file is 0.
- The initial value is not set in the standard configuration file. (commented out)
- The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.
- The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.
- If the value for this parameter is out of range, the default value is used.

**Configuration example** 1) To announce that the Primary Authentication Module is alive to the request sender:  
**FAILBACK=1**

**Remarks**

- This parameter is not subject to the reload command (reload-cert).
- This parameter is not downloaded at startup when using a replication configuration.
- With this function, the Secondary Authentication Module announces to the request sender that the Primary Authentication Module is alive. If the failback function is enabled on the request sender, a

failback operation will be performed from the Secondary module to the Primary module.

See also      CERTREPTYPE  
                 CERTFAILBACK (Forwarder configuration file)  
                 CERTLBFAILBACK (Forwarder configuration file)

# MAXREPTHREAD

Overview	Sets the number of threads for the replication process.
Format	<p><b>MAXREPTHREAD=<u>number of process threads</u></b></p> <ul style="list-style-type: none"> <li>• This parameter is effective only when the CERT parameter is set.</li> <li>• The recommended value for the number of processing threads is MAXDBCONNECT + the number of CPUs × 2. <ul style="list-style-type: none"> <li>* A multicore CPU is calculated as one single-core CPU.</li> </ul> </li> <li>• HP recommends changing the kernel parameters values below to those calculated from the formulas.  max_thread_proc=MAXREQTHREAD+MAXREPTHREAD+10 or more  maxfiles=MAXREQTHREAD+MAXREPTHREAD+MAXDBCONNECT+10 or more.</li> <li>• The default value in the executable binary file is 5.</li> <li>• The initial value is not set in the standard configuration file. (commented out)</li> <li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li> <li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li> </ul>
Configuration example	<p>1) To set the recommended value when MAXDBCONNECT is three and the number of CPUs is one in the server: (3 + 1 × 2).  <b>MAXREPTHREAD=5</b></p>
Remarks	<ul style="list-style-type: none"> <li>• This parameter is not subject to the reload command (reload-cert).</li> <li>• This parameter is not downloaded at startup when using a replication configuration.</li> <li>• When using this parameter, the “IceWall SSO FailOver Option” is also required.</li> <li>• This parameter sets the number of simultaneous processing threads to perform replication. Please note that if the value set is unsuitably high for the environment of the machine that is running the process, it causes a reduction in performance.</li> </ul>

- Since the name of this parameter is similar to MAXREQTHREAD, which sets the number of normal request processing threads, be careful to avoid spelling mistakes.

See also      CERT (Authentication Module configuration file)  
                 MAXREQTHREAD  
                 MAXDBCONNECT

# REPQUESIZE

Overview	Sets the size of the process wait queue for replication processing.
Format	<b>REPQUESIZE=<u>process wait queue size</u></b> <ul style="list-style-type: none"><li>• This parameter is effective only when the CERT parameter is set.</li><li>• The recommended value is 500. However, 1,000 should be set if the number of simultaneous logged in users set by the CACHE parameter exceeds 100,000.</li><li>• The default value set in the executable binary file is 1000.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The default value from the executable binary file is used if the line for this parameter is not present in the configuration file.</li><li>• The system is not guaranteed to work as expected when this parameter is set to a value other than a numerical value.</li></ul>
Configuration example	1) To set 500 as the replication process wait queue size: <b>REPQUESIZE=500</b>
Remarks	<ul style="list-style-type: none"><li>• This parameter is not subject to the reload command (reload-cert).</li><li>• This parameter is not downloaded at startup when using a replication configuration.</li><li>• All replication requests enter the replication queue, and then afterward, they are processed in replication threads.</li><li>• Since the name of this parameter is similar to REQQUESIZE, which sets the wait queue size for the normal request process, be careful to avoid spelling mistakes.</li></ul>
See also	CACHE REQQUESIZE



### 3.2 Group configuration file (cert.grp)

Overview	This configuration file defines the groups used for access control.
Storage location	The following is the default storage location: /opt/icewall-ss0/certd/config/cert.grp
Remarks	<p>This configuration file is subject to the reload command (reload-cert).</p> <p>This configuration file is downloaded at startup when using a replication configuration.</p> <p>The following pages describe these parameters.</p>

## Group settings ⑩.0

**Overview** Configures the groups that users belong to.

Additional functionality of this parameter is available since version 10.0.

**Format** **group name,conditional expression (or logical conditional expression)**

◇ Conditional expression

- The conditional expression is set as the combination: “Name=Value.”
- There are two ways to set “Name=Value,” as follows:

○ Set using an Authentication DB column

**group name,column name=Value**

- The group name has a maximum length of 32 bytes.
- The group name is not case sensitive.
- The group name can be a name set with the Authentication DB column information file or a name set by the DBEXATTR parameter in the Authentication Module configuration file.
- A reference table column (REFATTR parameter) cannot be used for the column name.
- The column name is case sensitive.
- Value is set as a regular expression. However, it is not case sensitive.

○ Set using an IP address:

**group name,REMOTE\_ADDR=IP address [-IP address]**

- REMOTE\_ADDR is a fixed name.
- IP addresses can be connected with a hyphen “-” to specify the range.
- Set the IP address ranges from narrow to wide. Also, do not include any unnecessary spaces before and after the hyphen.
- IP addresses cannot be defined with regular expressions.
- IPv4 or IPv6 formats can be used for the IP address. To use an IPv6-formatted IP address, enclose the character string for the IP address with square brackets ([...]). ⑩.0
- IPv4 and IPv6 cannot be used together in the IP address specification range. ⑩.0

◇ Logical conditional expression

---

**Group configuration file (cert.grp)**


---

A logical conditional expression can be set by combining multiple conditional expressions using logical operators. The following four operators are available for use in logical expressions:

Parentheses : ( )

NOT : !

AND : &

OR : |

- The priority of operators in logical expressions is ( ) ! & | .
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:

ALL,USERID=user01

SccOnly,USERID=user02

HpOnly,USERID=user03

**Configuration example**

- 1) To set STGRP as the group name for users with names in the userid column that start with "ST":  
**STGRP,userid=^ST.\***
- 2) To set HGGRP as the group name for users in the uid column whose user names include "HG":  
**HGGRP,uid=HG**
- 3) To set GUESTGRP as the group name for "GUEST" users in the cn column:  
**GUESTGRP,cn=^GUEST\$**
- 4) To set OPGRP as the group name for users where "OP" is included in the description:  
**OPGRP,description=OP**
- 5) To set IP1GRP as the group name for users who accessed from a specific IP address:  
**IP1GRP,REMOTE\_ADDR=192.168.1.1**
- 6) To set IPFTGRP as the group name for users who accessed from a range of IP addresses:  
**IPFTGRP,REMOTE\_ADDR=192.168.1.1-192.168.1.128**
- 7) To set GRP01 as the group name for users who have an unspecified value in the userid column and also have no value set in the rserial column:  
**GRP01,(userid=.\*)&(!rserial=.\*)**

- 8) To set GRP02 as the group name for users who have “HG” set in the userid column or who have 0 set in the APENABLE column:

**GRP02,userid=HG|APENABLE=^0\$**

- 9) To set GRP03 as the group name for users who have an unspecified value in the userid column and who also accessed from the client IP address 192.168.1.1:

**GRP03,userid=.\*&REMOTE\_ADDR=192.168.1.1**

- 10) To set IPV6RP as the group name for users who accessed from a range of IPv6 addresses:

**IPV6RP,REMOTE\_ADDR=[1234:0000:5678:9abc:1234:::9a00]-  
[1234:0000:5678:9abc:1234:::9abc]**

#### Remarks

- If there are two or more settings for the same group name, it is treated as though an OR condition (“|” operator) was set.

GRP01,userid=admin

GRP01,userid=root

The two lines above have the same meaning as the following line:

GRP01,userid=admin | userid=root

#### See also

DBEXATTR (Authentication Module configuration file)

Access control file

Authentication DB column configuration file

### 3.3 Access control file (cert.acl)

Overview	This configuration file defines access control for a Backend Web Server.
Storage location	The following is the default storage location: /opt/icewall-ss0/certd/config/cert.acl
Remarks	<p>This configuration file is subject to the reload command (reload-cert).</p> <p>This configuration file is downloaded at startup when using a replication configuration.</p> <p>These parameters are described in the following pages.</p>

## Access control settings ⑩.0

**Overview** Configures groups that have permission to access a particular URL with the following format:

Additional functionality of this parameter is available since version 10.0.

**Format** **target URL=group name (or logical conditional expression)**

- The target URL must begin with “http” or “https.”
- The target URL is case sensitive.
- The target URL has a maximum length of 1024 bytes.
- The target URL can be set up to the directory. It can also be set up to the file name.
- The host name included in the target URL must match the host name specified in the HOST or SHOST parameter in the Forwarder configuration file. However, because the port number is omitted at Forwarder when the default port number (http: 80, https: 443) is set for the host name, the target URL port number is also omitted in the description.
- A replacement keyword<sup>\*1</sup> may be used in the target URL. A replacement keyword is set by enclosing the Authentication DB column name with percent signs “%.”
- If a reference table (REFTBL parameter) is defined, only the reference table column name (REFATTR parameter) may be set as a replacement keyword.
- Group\_name sets a group name defined in the group configuration file.
- The group name is not case sensitive.
- Logical conditional expressions can be specified by combining multiple group names with logical operators. The operators available for use in logical expressions are shown below.

Parentheses : ( )

NOT : !

AND : &

OR : |

- The priority of operators in logical expressions is ( ) ! & |.
- Only group names can be set in a conditional expression. The Authentication DB columns and IP addresses cannot be set.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:  
http://www.scc-kk.co.jp/=ALL | SccOnly  
http://welcome.hp.com/=ALL | HpOnly

## Access control file (cert.acl)

http://localhost/=ALL | SccOnly | HpOnly

- If the target URL host name is an IPv6 address, it can be set using notation that omits 0. In this case, enclose the IP address of the host name in square brackets ([...]). (10.0)

\*1 A replacement keyword is a keyword that can be replaced with user information during execution.

## Configuration example

- 1) To set "GRP01 only" as the group that can access the target URL:  
**http://www.hp.com/info=GRP01**
- 2) To set "GRP01 or GRP02" as the group that can access the target URL:  
**http://www.hp.com/info=GRP01|GRP02**
- 3) To set "GRP01 and GRP02, or GRP03" as the groups that can access the target URL:  
**http://www.hp.com/info=(GRP01&GRP02)|GRP03**
- 4) To set "SIGNUP\_OK" as a group that can access target URLs where the directory name has the same value as the value set in the userid column:  
**http://www.hp.com/%userid%=SIGNUP\_OK**
- 5) To set "SHOWME" as a group that can access target URLs where the HTML file name has the same value as the value set in the userid column:  
**http://www.hp.com/%userid%.html=SHOWME**
- 6) To set "GRP01 only" as the group that can access to a URL for certain IPv6 address: (10.0)  
**http://[1234:0000:5678:9abc:1234::9abc]/info=GRP06**  
or  
**http://[1234::5678:9abc:1234:0000:0000:9abc]/info=GRP06**

## Remarks

- A prefix search is performed on the target URLs in the order in which they are specified in the setting.
- If a match is found for the target URL, the URL search ends.
- A prefix search is performed on the target URL. When setting different access privileges for a host based on the directory levels, describe the deepest directories on the directory tree first.

- If the URL includes an equals sign "=", the part preceding the sign is recognized as the URL, and the part following the sign is recognized as the group name.
- Arguments added to a URL following a question mark "?" cannot be checked for access privileges.

- Use Shift JIS to encode double-byte characters such as Chinese characters in Japanese text.

Example: `http://www.hp.com/ お知らせ.html`

- When using replacement keywords, note that if the column names used by the Authentication Module are set as shown below, they will not be replaced with the correct values.

Example:

- The replacement keyword is "%EXTCOL42%".
- The columns are set in the order of "EXTCOL4,EXTCOL42" for the DBEXATTR parameter in the Authentication Module configuration file.

Because a prefix search is made for the search keyword using the DBEXATTR parameter value, it is unintentionally replaced by the EXTCOL4 value.

To prevent this problem from occurring, set the DBEXATTR parameter as shown below.

`DBEXATTR=EXTCOL42,EXTCOL4`

- \* Ensure that the prefix search does not find any results other than the target column

See also

HOST (Forwarder configuration file)  
SHOST (Forwarder configuration file)  
DBEXATTR (Authentication Module configuration file)  
REFTBL (Authentication Module configuration file)  
REFATTR (Authentication Module configuration file)  
Group configuration file  
Authentication DB column configuration file



### 3.4 Authentication DB column information file (dbattr.conf)

**Overview** This configuration file sets the column names for the authentication table.

Parameters available to the user are as follows:

Parameter group	Parameter name
Basic user information parameters	UID
	PASSWORD
	PWDEXPDATE
	PWDHISTORY
	PCHGOK
	PCHGDATE
	LLOGINDATE
	PLOGINDATE
	FLOGINDATE
	PWDRETRY
	PWDLOCK
	LOGINOK
	LOCKDATE
	LOGINSTAT
Client certificate information parameters	RASERIALNO
	IWSERIALNO
	CERTEXPDATE
	GETCERT
	ONLINE

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

**Remarks** This configuration file is subject to the reload command (reload-cert).  
  
This configuration file is downloaded at startup when using a replication configuration.

The following pages describe these parameters.

### 3.4.1 Basic user information parameters

These parameters are used by default as user information in the Authentication Module.

Parameter name	Mandatory	Overview
UID	<input type="radio"/>	Sets the column (attribute) for the user ID
PASSWORD	<input type="radio"/>	Sets the column (attribute) for the password
PWDEXPDATE	×	Sets the column (attribute) for the password expiration time
PWDHISTORY	×	Sets the column (attribute) for the password history
PCHGOK	×	Sets the column (attribute) for the password change permission flag
PCHGDATE	×	Sets the column (attribute) for the password change date
LLOGINDATE	×	Sets the column (attribute) for the last login date
PLOGINDATE	×	Sets the column (attribute) for the previous login date
FLOGINDATE	×	Sets the column (attribute) for the login failure date
PWDRETRY	×	Sets the column (attribute) for the number of password retries
PWDLOCK	×	Sets the column (attribute) for the account lock flag
LOGINOK	×	Sets the column (attribute) for the login admission flag
LOCKDATE	×	Sets the column (attribute) for the account lock date
LOGINSTAT	×	Sets the column (attribute) for the login status flag

For details on these parameters, see the following pages.

---

Authentication DB column information file (dbattr.conf)

---

# UID

Overview	Sets the column (attribute) name for storing the user ID.
Format	<p><b>UID=<u>column (attribute) name</u></b></p> <ul style="list-style-type: none"><li>• The column name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : USERID LDAP edition : uid MSAD edition : CN NED edition : cn CSV edition : USERID MySQL edition : USERID OpenLDAP edition: uid</li></ul>
Configuration example	<p>1) To set “USERID” as the column (attribute) for the user ID: <b>UID=USERID</b></p>
Remarks	<ul style="list-style-type: none"><li>• Set a column (attribute) that satisfies the following conditions: Character type (up to 64 bytes), Not Null</li><li>• Make the user ID unique in the table (or directory).</li></ul>
See also	<p>REFUID (Authentication Module configuration file) UID (log column information file)</p>

# PASSWORD

Overview	Sets the column (attribute) name for storing the password.
Format	<p><b>PASSWORD=<u>column (attribute) name</u></b></p> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : PASSWD LDAP edition : userPassword MSAD edition : userPassword NED edition : userPassword CSV edition : PASSWD MySQL edition : PASSWD OpenLDAP edition: userPassword</li></ul>
Configuration example	<p>1) To set “PASSWD” as the column (attribute) for the password: <b>PASSWORD=PASSWD</b></p>
Remarks	<ul style="list-style-type: none"><li>• The data size of the column (attribute) for storing passwords varies according to the password encryption format. MD5 : A 37-byte area is required. SHA : A 33-byte area is required. SHA256: A 52-byte area is required. Plain : An area up to 128 bytes is required.</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (up to 128 bytes), Not NULL</li></ul>
See also	PWDHISTORY

# PWDEXPDATE

**Overview**                Sets the column (attribute) name for storing the password expiration time.

**Format**                **PWDEXPDATE=column (attribute) name**

- The column (attribute) name is not case sensitive.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:  
ORACLE edition : PASSWDEXP  
LDAP edition    : passwordExpirationTime  
MSAD edition    : street  
NED edition     : x500UniqueIdentifier  
CSV edition     : PASSWDEXP  
MySQL edition   : PASSWDEXP  
OpenLDAP edition: departmentNumber

**Configuration example**    1) To set “PASSWDEXP” as the column (attribute) for the password expiration time:  
**PWDEXPDATE=PASSWDEXP**

**Remarks**                • The format of the value stored as the password expiration time is shown below.  
                              YYYYMMDDhhmmss (14 bytes)

                              • Set a column (attribute) that satisfies the following conditions:  
                              Character type (14 bytes)

**See also**                PCHGDATE  
                              LLOGINDATE  
                              PLOGINDATE  
                              FLOGINDATE  
                              LOCKDATE  
                              CERTEXPDATE  
                              TIME (log column information file)

# PWDHISTORY

Overview	<p>Sets the password history column (attribute) name for storing the previously used passwords when a password is changed.</p> <p>This column (attribute) stores the previously used passwords.</p> <p>A password that matches a password found in this column cannot be used when the password is changed.</p>
Format	<p><b>PWDHISTORY=<u>column (attribute) name</u></b></p> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : PASSWDHIS LDAP edition : passwordHistory MSAD edition : Not set NED edition : userSMIMECertificate CSV edition : PASSWDHIS MySQL edition : PASSWDHIS OpenLDAP edition: userPKCS12</li></ul>
Configuration example	<p>1) To set “PASSWDHIS” as the column (attribute) for the password history: <b>PWDHISTORY=PASSWDHIS</b></p>
Remarks	<ul style="list-style-type: none"><li>• The passwords stored in the password history are separated by spaces.</li><li>• The passwords are stored in sequence in the password history, starting with the most recent. Example: Last_password Second_to_last_password ...</li><li>• The passwords stored in the password history are encrypted.</li><li>• If the encryption method when changing the password is Plain, caution is required because the Plain password is registered in the password history.</li><li>• The data size of the column (attribute) for storing the password history varies according to the password encryption format and the upper limit</li></ul>

---

**Authentication DB column information file (dbattr.conf)**

---

for the number of stored passwords (set by the PWDHISCNT parameter in the Authentication Module configuration file).

MD5	37 bytes × the PWDHISCNT parameter value + (the PWDHISCNT parameter value - 1)
SHA	33 bytes × the PWDHISCNT parameter value + (the PWDHISCNT parameter value - 1)
SHA256	52 bytes × the PWDHISCNT parameter value + (the PWDHISCNT parameter value - 1)
Plain	Arbitrary size × the PWDHISCNT parameter value + (the PWDHISCNT parameter value - 1)

- Set a column that satisfies the following conditions:  
Character type (number of bytes calculated with the formula above)

See also

PASSWORD  
PWDHISCHK (Authentication Module configuration file)  
PWDHISCNT (Authentication Module configuration file)  
PWDCHGHASH

# PCHGOK

Overview	Sets the column (attribute) name for storing the password change flag.
Format	<p><b>PCHGOK=<u>column (attribute) name</u></b></p> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : PASSCHANGE LDAP edition : mobile MSAD edition : mobile NED edition : mobile CSV edition : PASSCHANGE MySQL edition : PASSCHANGE OpenLDAP edition: mobile</li></ul>
Configuration example	<p>1) To set “PASSCHANGE” as the column (attribute) for the password change flag: <b>PCHGOK=PASSCHANGE</b></p>
Remarks	<ul style="list-style-type: none"><li>• The column (attribute) set with this parameter stores the following values: 0 : Cannot change password 1 : Can change password</li><li>• If no value is stored in the column (attribute) set by this parameter, it is treated as a zero, so set the Not NULL attribute for this column.</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (1 byte), Not NULL</li></ul>
See also	LOGINOK PWDLOCK LOGINSTAT GETCERT ONLINE



# PCHGDATE

**Overview**                Sets the column (attribute) name for storing the password change date.

**Format**                **PCHGDATE=column (attribute) name**

- The column (attribute) name is not case sensitive.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:  
ORACLE edition : CHGDATE  
LDAP edition : manager  
MSAD edition : info  
NED edition : jobCode  
CSV edition : CHGDATE  
MySQL edition : CHGDATE  
OpenLDAP edition: employeeType

**Configuration example**    1) To set “PCHGDATE” as the column (attribute) for storing the password change date:  
**PCHGDATE=PCHGDATE**

**Remarks**

- When using Microsoft Active Directory Lightweight Directory Services, attributes set to the initial values in the standard configuration file may not exist. In this case, configure attributes that meet the conditions below.
- The format of the value stored as the password change date is shown below.  
YYYYMMDDhhmmss (14 bytes)
- Set a column (attribute) that satisfies the following conditions:  
Character type (14 bytes)

**See also**                PWDEXPDATE  
LLOGINDATE  
PLOGINDATE  
FLOGINDATE  
LOCKDATE  
CERTEXPDATE  
TIME (log column information file)

# LLOGINDATE

Overview	Sets the column (attribute) name for storing the last login date.
Format	<b>LLOGINDATE=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : LASTDATE LDAP edition : displayName MSAD edition : homePhone NED edition : displayName CSV edition : LASTDATE MySQL edition : LASTDATE OpenLDAP edition: displayName</li></ul>
Configuration example	1) To set “LASTDATE” as the column (attribute) for the last login date: <b>LLOGINDATE=LASTDATE</b>
Remarks	<ul style="list-style-type: none"><li>• The format of the value stored as the last login date is shown below. YYYYMMDDhhmmss (14 bytes)</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (14 bytes)</li></ul>
See also	PWSEXPDATE PCHGDATE PLOGINDATE FLOGINDATE LOCKDATE CERTEXPDATE TIME (log column information file)

# PLOGINDATE

**Overview** Sets the column (attribute) name for storing the previous login date.

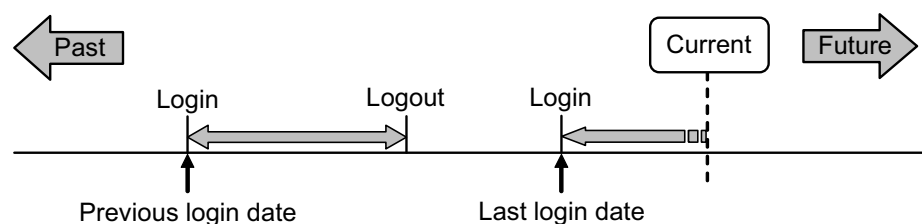
**Format** **PLOGINDATE=**column (attribute) name

- The column (attribute) name is not case sensitive.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:  
 ORACLE edition : LOGONDATE  
 LDAP edition : pager  
 MSAD edition : pager  
 NED edition : pager  
 CSV edition : LOGONDATE  
 MySQL edition : LOGONDATE  
 OpenLDAP edition: pager

**Configuration example** 1) To set “LOGONDATE” as the column (attribute) for the previous login date:

**PLOGINDATE=LOGONDATE**

- Remarks**
- The format of the value stored as the previous login date is shown below.  
 YYYYMMDDhhmmss (14 bytes)
  - The previous login date stores the date of the login performed previous to the currently valid login. The value stored here is older than the last login date.



- Set a column (attribute) that satisfies the following conditions:  
 Character type (14 bytes)

**See also** PWDEXPDATE  
 PCHGDATE

LLOGINDATE  
FLOGINDATE  
LOCKDATE  
CERTEXPDATE  
TIME (log column information file)

# FLOGINDATE

**Overview** Sets the column (attribute) name for storing the most recent login failure date.

**Format** **FLOGINDATE=column (attribute) name**

- The column (attribute) name is not case sensitive.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:  
ORACLE edition : LOGONFAIL  
LDAP edition : givenNamer  
OpenLDAP edition: givenNamer  
MSAD edition : givenName  
NED edition : givenName  
CSV edition : LOGONFAIL  
MySQL edition : LOGONFAIL

**Configuration example** 1) To set “LOGONFAIL” as the column (attribute) for the login failure date:  
**FLOGINDATE=LOGONFAIL**

**Remarks**

- The format of the value stored as the login failure date is shown below.  
YYYYMMDDhhmmss (14 bytes)
- This parameter is updated whenever any of the following events occur.  
(1) Password input error  
(2) Account lock resulting from password input error  
(3) Prohibited login  
(4) Invalid certificate (when using a client certificate)  
(5) Pre-authenticated error (when using a client certificate)
- Set a column (attribute) that satisfies the following conditions:  
Character type (14 bytes)

**See also** PWDEXPDATE  
PCHGDATE  
LLOGINDATE  
PLOGINDATE  
LOCKDATE  
CERTEXPDATE

TIME (log column information file)

# PWDRETRY

**Overview**                Sets the column (attribute) name for storing the login retry count.

**Format**                **PWDRETRY=column (attribute) name**

- The column (attribute) name is not case sensitive.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows:  
ORACLE edition : FAILCOUNT  
LDAP edition : passwordRetryCount  
MSAD edition : st  
NED edition : workforceID  
CSV edition : FAILCOUNT  
MySQL edition : FAILCOUNT  
OpenLDAP edition: roomNumber

**Configuration example**    1) To set “FAILCOUNT” as the column (attribute) for the login retry count:  
**PWDRETRY=FAILCOUNT**

**Remarks**

- When a login is successful, the column (attribute) value is set to 0.
- The value of the column (attribute) set with this parameter is treated as a numeric value. If no value is set, it is treated as 0.
- Set a column (attribute) that satisfies the following conditions:  
Integer type
- \* If the number type is used with the ORACLE edition or MySQL edition, set “Not Null” for the column (attribute).

**See also**                None

# PWDLOCK

Overview	Sets the column (attribute) name for storing the account lock flag.
Format	<b>PWDLOCK=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : LOCKOUT LDAP edition : employeeNumber MSAD edition : comment NED edition : employeeNumber CSV edition : LOCKOUT MySQL edition : LOCKOUT OpenLDAP edition: employeeNumber</li></ul>
Configuration example	1) To set “LOCKOUT” as the column (attribute) for the account lock flag: <b>PWDLOCK=LOCKOUT</b>
Remarks	<ul style="list-style-type: none"><li>• The column (attribute) set with this parameter stores the following values: 0 : Not locked 1 : Locked</li><li>• If no value is stored in the column (attribute) set by this parameter, it is treated as a zero, so set the Not NULL attribute for this column (attribute).</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (1 byte), Not NULL</li></ul>
See also	PCHGOK LOGINOK LOGINSTAT GETCERT ONLINE



# LOGINOK

**Overview**                Sets the column (attribute) name for storing the login availability flag.

**Format**                **LOGINOK=column (attribute) name**

- The column (attribute) name is not case sensitive.
- There is no default value in the executable binary file.  
The initial values in the standard configuration file are as follows:  
ORACLE edition : LOGONSTOP  
LDAP edition : homePostalAddress  
MSAD edition : homePostalAddress  
NED edition : homePostalAddress  
CSV edition : LOGONSTOP  
MySQL edition : LOGONSTOP  
OpenLDAP edition: homePostalAddress

**Configuration example**    1) To set “LOGONSTOP” as the column (attribute) for the login availability flag:  
**LOGINOK=LOGONSTOP**

**Remarks**

- One of the following values can be stored in the column (attribute) set by this parameter:  
0 : Can log in  
1 : Cannot log in
- If no value is stored in the column (attribute) set by this parameter, it is treated as a zero, so set the Not NULL attribute for this column (attribute).
- Set a column (attribute) that satisfies the following conditions:  
Character type (1 byte), Not NULL

**See also**                PCHGOK  
PWDLOCK  
LOGINSTAT  
GETCERT  
ONLINE

# LOCKDATE

Overview	Sets the column (attribute) name for storing the most recent date on which the account was locked due to a password entry error.
Format	<b>LOCKDATE=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : LOCKDATE LDAP edition : title MSAD edition : title NED edition : title CSV edition : LOCKDATE MySQL edition : LOCKDATE OpenLDAP edition: title</li></ul>
Configuration example	1) To set “LOCKDATE” as the column (attribute) for the account lock date: <b>LOCKDATE=LOCKDATE</b>
Remarks	<ul style="list-style-type: none"><li>• The format of the value stored as the account lock date is shown below. YYYYMMDDhhmmss (14 bytes)</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (14 bytes)</li></ul>
See also	PWDEXPDATE PCHGDATE LLOGINDATE PLOGINDATE FLOGINDATE CERTEXPDATE TIME (log column information file)

# LOGINSTAT

Overview	Sets the column (attribute) name for storing the login status.
Format	<b>LOGINSTAT=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows: ORACLE edition : LOGSTATUS LDAP edition : initials MSAD edition : initials NED edition : initials CSV edition : LOGSTATUS MySQL edition : LOGSTATUS OpenLDAP edition: initials</li></ul>
Configuration example	1) To set “LOGSTATUS” as the column (attribute) for the login status: <b>LOGINSTAT=LOGSTATUS</b>
Remarks	<ul style="list-style-type: none"><li>• The column (attribute) set with this parameter stores the following values: 0 : Logged out 1 : Logged in</li><li>• If no value is stored in the column (attribute) set by this parameter, it is treated as a zero, so set the Not NULL attribute for this column (attribute).</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (1 byte), Not NULL</li></ul>
See also	PCHGOK LOGINOK PWDLOCK GETCERT ONLINE

### 3.4.2 Client certificate information parameters

These parameters establish additional settings for when a client certificate is used.

Parameter name	Mandatory	Overview
RASERIALNO	×	Sets the column (attribute) for the certificate issue serial number
IWSERIALNO	×	Sets the column (attribute) for the certificate serial number
CERTEXPDATE	×	Sets the column (attribute) for the certificate expiration date
GETCERT	×	Sets the column (attribute) for the certificate issue flag
ONLINE	×	Sets the column (attribute) for the certificate usage flag

For details on these parameters, see the following pages.

# RASERIALNO

Overview	Sets the column (attribute) name for storing the certificate serial number and issuer name that are saved on the certificate issuing system when a client certificate is issued.
Format	<b>RASERIALNO=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set “RASERIAL” as the column (attribute) for the certificate serial number and issuer name that are saved on the certificate issuing system: <b>RASERIALNO=RASERIAL</b>
Remarks	<ul style="list-style-type: none"><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li><li>• Be sure to set a column with this parameter that has a data size large enough to store the certificate serial numbers and issuer names.</li><li>• Set the column to save a NULL value if a client certificate has not been issued.</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (serial number size + issuer name size +1)</li></ul>
See also	IWSERIALNO SERIAL (log column information file)

# IWSERIALNO

Overview	Sets the column (attribute) name for storing the certificate serial number and issuer name when the data for a certificate presented by a client at the initial authentication after its issue matches the data at the time of issue.
Format	<b>IWSERIALNO=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set “BSSERIAL” as the column (attribute) for saving the certificate serial number and issuer name of the certificate submitted from a client: <b>IWSERIALNO=BSSERIAL</b>
Remarks	<ul style="list-style-type: none"><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li><li>• Be sure to set a column (attribute) with this parameter that has a data size large enough to store the certificate serial numbers and issuer names.</li><li>• Set the column to save a NULL value if a client certificate has not been issued.</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (serial number size + issuer name size +1)</li></ul>
See also	RASERIALNO SERIAL (log column information file)

# CERTEXPDATE

Overview	Sets the column (attribute) name for storing the certificate expiration date in a client certificate submitted from a client at the initial authentication after its issue.
Format	<b>CERTEXPDATE=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set “VDATE” as the column (attribute) for the expiration date of a certificate submitted from a client: <b>CERTEXPDATE=VDATE</b>
Remarks	<ul style="list-style-type: none"><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li><li>• The format of the value stored as the certificate expiration date is shown below. YYYYMMDDhhmmss (14 bytes)</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (14 bytes)</li><li>• Initial authentication after updating the certificate succeeds even if the certificate expiration date is not registered in the Authentication DB.</li></ul>
See also	PWDEXPDATE PCHGDATE LLOGINDATE PLOGINDATE FLOGINDATE LOCKDATE TIME (log column information file)

# GETCERT

Overview	Sets the column (attribute) name for storing the certificate issue flag.
Format	<b>GETCERT=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set “CERT” as the column (attribute) for the certificate issue flag: <b>GETCERT=CERT</b>
Remarks	<ul style="list-style-type: none"><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li><li>• The column (attribute) set with this parameter stores the following values:<ul style="list-style-type: none"><li>0 : Certificate has been issued.</li><li>1 : Certificate has not been issued.</li><li>2 : Certificate has been issued, but not used.</li></ul></li><li>• When initial authentication is done with a certificate, 0 is set.</li><li>• If no value is stored in the column (attribute) set by this parameter, it is treated as a zero, so set the Not NULL attribute for this column (attribute).</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (1 byte), Not NULL</li></ul>
See also	PCHGOK LOGINOK PWDLOCK LOGINSTAT



# ONLINE

Overview	Sets the column (attribute) name for storing the certificate usage flag.
Format	<b>ONLINE=<u>column (attribute) name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set “APENABLE” as the column (attribute) for the certificate usage flag: <b>ONLINE=APENABLE</b>
Remarks	<ul style="list-style-type: none"><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li><li>• The column (attribute) set with this parameter stores the following values:<ul style="list-style-type: none"><li>0 : Initial authentication not performed with certificate.</li><li>1 : Initial authentication performed with certificate.</li></ul></li><li>• When initial authentication is done with a certificate, 1 is set.</li><li>• If no value is stored in the column (attribute) set by this parameter, it is treated as a zero, so set the Not NULL attribute for this column (attribute).</li><li>• Set a column (attribute) that satisfies the following conditions: Character type (1 byte)</li></ul>
See also	PCHGOK LOGINOK PWDLOCK LOGINSTAT GETCERT

### 3.5 Log column information file (logdbattr.conf)

**Overview** This configuration file defines the log table columns (attributes) to output the audit log.  
Parameters available to the user are as follows:

Parameter group	Parameter name
Basic information parameters	NO
	TIME
	UID
	KIND
	RESULT
	MSG
	CLIP
Client certificate information parameters	SERIAL

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

**Remarks** This configuration file is subject to the reload command (reload-cert).  
  
This configuration file is downloaded at startup when using a replication configuration.

The following pages describe these parameters.

### 3.5.1 Basic information parameters

These parameters are used for saving the login/logout log information output from the Authentication Module.

Parameter name	Mandatory	Overview
NO	×	Sets the column for sequential numbers
TIME	×	Sets the column for log output times
UID	×	Sets the column for user IDs
KIND	×	Sets the column for log identification flags
RESULT	×	Sets the column for process results
MSG	×	Sets the column for log messages
CLIP	×	Sets the column name for storing client IP addresses

For details on these parameters, see the following pages.

# NO

Overview	Sets the column name for storing sequential numbers.
Format	<b>NO=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is UKENO.</li></ul>
Configuration example	1) To set “UKENO” as the column for sequential numbers: <b>NO=UKENO</b>
Remarks	<ul style="list-style-type: none"><li>• Set a column that satisfies the following conditions: Character type (bytes equal to the maximum number of digits in the sequential number)</li></ul>
See also	None

# TIME

Overview	Sets the column name for storing processing time.
Format	<b>TIME=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is UKEDATE.</li></ul>
Configuration example	1) To set “UKEDATE” as the column for processing time: <b>TIME=UKEDATE</b>
Remarks	<ul style="list-style-type: none"><li>• The format of the value stored as the processing time is shown below. YYYYMMDDhhmmss (14 bytes)</li><li>• Set a column that satisfies the following conditions: Character type (14 bytes)</li></ul>
See also	PWDEXPDATE (Authentication DB column information file) PCHGDATE (Authentication DB column information file) LLOGINDATE (Authentication DB column information file) PLOGINDATE (Authentication DB column information file) FLOGINDATE (Authentication DB column information file) LOCKDATE (Authentication DB column information file) CERTEXPDATE (Authentication DB column information file)

# UID

Overview	Sets the column name for storing user IDs.
Format	<b>UID=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is USERID.</li></ul>
Configuration example	1) To set “USERID” as the column for user IDs: <b>UID=USERID</b>
Remarks	<ul style="list-style-type: none"><li>• Set a column that satisfies the following conditions: Character type (64 bytes or less)</li></ul>
See also	REFUID (Authentication Module configuration file) UID (Authentication DB column information file)

---

Log column information file (logdbattr.conf)

---

## KIND

Overview	Sets the column name for storing log types.
Format	<b>KIND=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is KIND.</li></ul>
Configuration example	1) To set “KIND” as the column for the log type: <b>KIND=KIND</b>
Remarks	<ul style="list-style-type: none"><li>• One of the following values can be set to the column (attribute) set with this parameter:<ul style="list-style-type: none"><li>1 : Login</li><li>2 : Logout</li><li>3 : Timeout</li><li>4 : Forced logout (duplicate logins)</li></ul></li><li>• Set a column that satisfies the following conditions: Character type (1 byte)</li></ul>
See also	None

# RESULT

Overview	Sets the column name for storing operation results.
Format	<b>RESULT=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is RESCODE.</li></ul>
Configuration example	1) To set “RESCODE” as the column for operation results: <b>RESULT=RESCODE</b>
Remarks	<ul style="list-style-type: none"><li>• One of the following values can be set to the column (attribute) set with this parameter: 0 : Normal 1 : Error</li><li>• Set a column that satisfies the following conditions: Character type (1 byte)</li></ul>
See also	None



Log column information file (logdbattr.conf)

---

## MSG

Overview	Sets the column name for storing login/logout history messages.
Format	<b>MSG=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is MESSAGE.</li></ul>
Configuration example	1) To set “MESSAGE” as the column for history messages: <b>MSG=MESSAGE</b>
Remarks	<ul style="list-style-type: none"><li>• Set a column that satisfies the following conditions: Character type (256 bytes)</li></ul>
See also	None

# CLIP

Overview	Sets the column name for storing client IP addresses.
Format	<b>CLIP=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value set in the standard configuration file is IPADDR.</li></ul>
Configuration example	1) To set “IPADDR” as the column for client IP addresses: <b>CLIP=IPADDR</b>
Remarks	<ul style="list-style-type: none"><li>• Set a column that satisfies the following conditions: Character type (15 bytes)</li></ul>
See also	None

### 3.5.2 Client certificate information parameters

This parameter is used for saving extra login/logout histories output from the Authentication Module when a client certificate is used.

Parameter name	Mandatory	Overview
SERIAL	×	Sets the column for certificate serial numbers

For details on these parameters, see the following pages.

# SERIAL

Overview	Sets the column name for storing certificate serial numbers and issuer names for processed users.
Format	<b>SERIAL=<u>column name</u></b> <ul style="list-style-type: none"><li>• The column (attribute) name is not case sensitive.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li></ul>
Configuration example	1) To set “RASERIAL” as the column for certificate serial numbers and issuers: <b>SERIAL=RASERIAL</b>
Remarks	<ul style="list-style-type: none"><li>• When using this parameter, the “IceWall SSO Client Certificates Option” is required.</li><li>• Be sure to set a column with this parameter that has a data size large enough to store the certificate serial numbers and issuer names.</li><li>• Set the column to save a NULL value if a client certificate has not been issued.</li><li>• Set a column that satisfies the following conditions: Character type (serial number size + issuer name size +1)</li></ul>
See also	RASERIALNO (Authentication DB column information file) IWSERIALNO (Authentication DB column information file)

### 3.6 Forbidden password configuration file (pwdforbid.conf)

Overview	This file defines character strings that are forbidden to be registered as passwords when a password is changed by a user.
Storage location	The following is the default storage location: /opt/icewall-ss0/certd/config/pwdforbid.conf
Remarks	<p>This configuration file is subject to the reload command (reload-cert).</p> <p>This configuration file is downloaded at startup when using a replication configuration.</p> <p>These parameters are described on the following pages.</p>

# Forbidden password configuration overwrite 10.0

Overview	<p>Sets character strings that are forbidden for registration as passwords.</p> <p>Some specifications of this parameter have been modified since version 10.0.</p>
Format	<p><b><u>forbidden character string</u></b></p> <ul style="list-style-type: none"> <li>Forbidden text strings are set with one password per line.</li> <li>Forbidden character strings may be described in up to 256 lines, with each password of 128 bytes or less per line.</li> <li>Forbidden passwords are case sensitive.</li> <li>Forbidden character strings can be set with regular expressions. <small>10.0</small></li> <li>There is no default value in the executable binary file.</li> <li>The initial values in the standard configuration file are as follows: <small>10.0</small> <pre>^password\$ ^abc123\$</pre> </li> </ul>
Configuration example	<ol style="list-style-type: none"> <li>To set AAAA0123 as a forbidden password: <small>10.0</small> <b>^AAAA0123\$</b></li> <li>To forbid a password that contains Userid01: <small>10.0</small> <b>Userid01</b></li> <li>To forbid a password of a character string that does not contain one or more numbers: <small>10.0</small> <b>^[^0-9]*\$</b></li> </ol>
Remarks	<ul style="list-style-type: none"> <li>Prohibited passwords are set for the entire system. They cannot be set individually for each user.</li> <li>When forbidden character strings are set, a password policy error occurs only when the password that the user is attempting to change matches the regular expression. <small>10.0</small></li> <li>Special characters that can be used in passwords are as follows, excluding blank spaces: !"#\$%&amp;()*+,-./:;&lt;=&gt;?@[\\]^_`{ }~</li> </ul> <p>* Single quotes cannot be used starting with version 8.0 R2.</p>

---

**Forbidden password configuration file (pwdforbid.conf)**

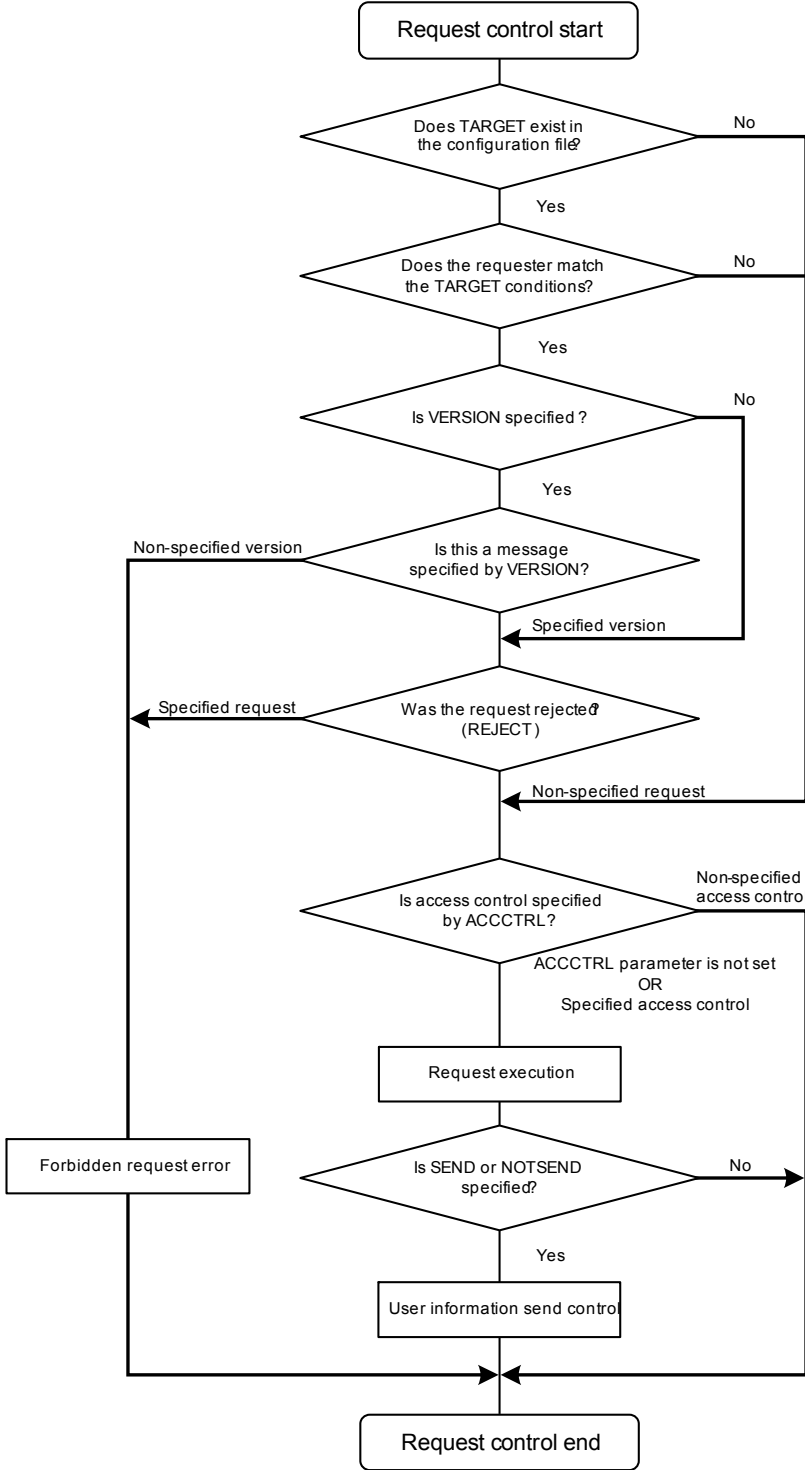
---

See also                None

### 3.7 Request control configuration file (request.acl)

Overview	This file defines the executable request conditions for the requests from Forwarder and Agent.
Storage location	The following is the default storage location: /opt/icewall-ssso/certd/config/request.acl
Format	<pre>TARGET=conditional expression { VERSION=ICP version number REJECT=request[,request,...,request] ACCCTRL=access type SEND=user information name 1[,user information name 2,...,user information name n] }  or  TARGET=conditional expression { VERSION=ICP version number REJECT=request[,request,...,request] ACCCTRL=access type NOTSEND=user information name 1[,user information name 2,...,user information name n] }</pre>
Remarks	<p>This configuration file is subject to the reload command (reload-cert).</p> <p>This configuration file is downloaded at startup when using a replication configuration.</p> <p>The description format used in this configuration file is considerably different from that used in other configuration files of the Authentication Module. The information shown in the above format is a set of control information. When performing control from various sender information, multiple instances of this set are described.</p> <p>Be aware that if a format error is made in this configuration file, such as lack of a "{" or close "}" after a TARGET line, the Authentication Module will fail to start.</p> <p>The operation priority of the information defined in this configuration file is shown below.</p>





If a request execution permission error occurs due to the conditions in this configuration file, an unrecognizable process result is returned in Agent for versions 7.0 SP3 and before, so this is treated as a system error. Also, if access is performed using the JAVA Agent Library, the return value is "RequestResult.OTHER." Forwarder recognizes it as a "Request

execution permission error,” and the ACL error page is displayed on the client. (10.0)

### 3.7.1 Basic configuration parameters

These are parameters used universally by the entire system when controlling requests from the requester.

Parameter name	Mandatory	Overview
TARGET 10.0	×	Sets the specific conditions of the requester
VERSION	×	Sets the ICP target version
REJECT	×	Sets the forbidden request
SEND	×	Sets the user information to send
NOTSEND	×	Sets the user information not to send
ACCCTRL	×	Sets the access type

The following pages describe these parameters.

# TARGET 10.0

**Overview** Sets the conditions to identify the requester.

Additional functionality of this parameter is available since version 10.0.

**Format** **TARGET=conditional expression**

```
{  
}
```

- Multiple instances of this parameter can be described.
- The conditional expression set by this parameter is the “Name=Value” format.
- If the requester performs communication using ICP1.0 (1.1), “SOURCE\_ADDR” can be set for “Name.” If the requester performs communication using ICP2.0, the environment information sent at login from “SOURCE\_ADDR” and the requester can be set for “Name.”
- Value can be set as a regular expression.  
Example: Name1=user[0-9]
- If Name is “SOURCE\_ADDR,” an IP address is set for Value.
- The IP address is set in dotted decimal format.
- IP addresses can be connected with a hyphen “-” to specify the range.  
Example: SOURCE\_ADDR=192.168.0.1-192.168.0.50
- Set the IP address ranges from narrow to wide. Also, do not include any unnecessary spaces before and after the hyphen.
- The IP address cannot be specified as a regular expression.
- Multiple instances of “Name=Value” can be set using logical operators.  
Example: Name1=Value1 | Name2=Value2

If the requester matches multiple conditional expressions, only the condition that was described first is applied.

- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows (in bold letters).

**TARGET=SOURCE\_ADDR=192.168.0.10-192.168.0.20**

```
{  
SEND=LOGONDATE  
SEND=LASTDATE  
}
```

**TARGET=SOURCE\_ADDR=192.168.0.30**

```
{  
VERSION=2.0
```

## Request control configuration file (request.acl)

```
NOTSEND=IW_UID,IW_PWD
}
```

```
TARGET=SOURCE_ADDR=192.168.0.40&AGENT_ID=IceWall
SSO DFW
```

```
{
REJECT=FLOGINUID,FLOGINCERT
}
```

- IPv4 or IPv6 formats can be used for the IP address. To use an IPv6-formatted IP address, enclose the character string for the IP address with square brackets ([...]). (10.0)
- IPv4 and IPv6 cannot be used together in the IP address specification range. (10.0)

## Configuration example

- 1) To specify a specific requester using an IP address:

```
TARGET=SOURCE_ADDR=192.168.0.1
{
}
```

- 2) To specify a range for specific IP addresses:

```
TARGET=SOURCE_ADDR=192.168.0.1-192.168.0.10
{
}
```

- 3) To forbid requests from everyone but a specific requester:

```
TARGET=!(SOURCE_ADDR=192.168.0.1)
{
REJECT=ALL
}
```

- 4) To specify a requester that matches specific environment information (ICP2.0 only):

```
TARGET=USER_AGENT=.*mozilla.*
{
}
```

- 5) To specify a requester that matches a specific IP address or environment information (ICP2.0 only):

```
TARGET=SOURCE_ADDR=192.168.0.1|USER_AGENT=.*mozilla.*
{
}
```

Remarks	<ul style="list-style-type: none"><li>• The IP address set by “SOURCE_ADDR” is that of the server with a module sending requests. Be aware that this is different from the IP addresses of clients. However, if there is network equipment between the module that sends requests and the Authentication Module, in some cases, this is the IP address of the network equipment.</li><li>• If Name is “REMOTE_ADDR,” the IP address is set in Value, but in contrast to “SOURCE_ADDR,” a range of IP addresses cannot be specified.</li><li>• If the request control settings are not made in this configuration file, it operates in the same way as previous versions (backward compatibility).</li><li>• If a format error occurs in the setting information in this configuration file, the Authentication Module does not start.</li></ul>
See also	None

## VERSION

Overview	Sets the version number of the communication message (ICP) of the request to control.
Format	<p><b>VERSION=<u>version number</u></b></p> <ul style="list-style-type: none"><li>• This parameter is described between "{" and "}" of the TARGET parameter.</li><li>• This parameter can span multiple lines.</li><li>• This parameter can be indented. Use single byte space characters or the TAB character to make indents.</li><li>• One of the following values can be set to the version number:<ul style="list-style-type: none"><li>1.0 : Communication is allowed using ICP 1.0 expansion</li><li>2.0 : Communication is allowed using ICP 2.0</li></ul></li><li>• Communication is only allowed for the ICP version that is set by this parameter. Versions not set here are not allowed.</li><li>• If this parameter is not set, communication in all versions is allowed.</li><li>• There is no default value in the executable binary file.</li><li>• The initial values in the standard configuration file are as follows (in bold letters).<pre>TARGET=SOURCE_ADDR=192.168.0.30 { <b>VERSION=2.0</b> NOTSEND=IW_UID,IW_PWD }</pre></li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To allow ICP 1.0 expansion messages only: <b>VERSION=1.0</b></p> <p>2) To allow ICP 2.0 messages only: <b>VERSION=2.0</b></p> <p>3) To allow ICP 1.0 expansion and ICP 2.0 messages: <b>VERSION=1.0</b> <b>VERSION=2.0</b> or (No setting)</p>

---

**Request control configuration file (request.acl)**

---

Remarks	<ul style="list-style-type: none"><li>• If a format error occurs in the setting information in this configuration file, the Authentication Module does not start.</li></ul>
See also	None



## Request control configuration file (request.acl)

# REJECT

**Overview** Sets the requests to forbid the processing of process requests from the requester.

**Format** **REJECT=**request name[request name,...,request name]

- This parameter is described between "{" and "}" of the TARGET parameter.
- This parameter can span multiple lines.
- This parameter can be indented. Use single byte space characters or the TAB character to make indents.
- One of the following values can be set to the request name:

Request name	Description
LOGINUID	Forbids login requests using a user ID and password
FLOGINUID	Prohibits forced login requests using a user ID and password
LOGINCERT	Forbids login requests using a client certificate and password
FLOGINCERT	Forbids forced login requests using a client certificate and password
ACCESSUID	Forbids access control requests using a user ID and password
ACCESSCERT	Forbids access control requests after login using a client certificate and password
PWDCHG	Forbids password change requests
LOGOUT	Forbids logout requests
ALL	Forbids all requests

- Multiple request names can be specified by separating them with commas.
- Request names are not case sensitive.
- If this parameter is not set, all requests are executable.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows (in bold letters).

```
TARGET=SOURCE_ADDR=192.168.0.40&AGENT_ID=IceWall SSO
DFW
{
REJECT=FLOGINUID,FLOGINCERT
}
```

	<ul style="list-style-type: none"><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<ol style="list-style-type: none"><li>1) To forbid a password change request from the requester: <b>REJECT=PWDCHG</b></li><li>2) To forbid forced login using a user ID and password and forced login using a client certificate and password from the requester: <b>REJECT=FLOGINUID</b> <b>REJECT=FLOGINCERT</b> or <b>REJECT=FLOGINUID,FLOGINCERT</b></li></ol>
Remarks	<ul style="list-style-type: none"><li>• When users who can change the password log in, the password change page is displayed if the password expiration time has been reached. However, note that the password cannot be changed if <b>REJECT=PWDCHG</b> is set.</li></ul>
See also	None

## Request control configuration file (request.acl)

# SEND

**Overview** Sets the user information sent to the requester by the access control response message.

**Format** **SEND=user information name[,user information name,...,user information name]**

- This parameter is described between “{” and “}” of the TARGET parameter.
- This parameter can be indented. Use single byte space characters or the TAB character to make indents.
- Only the user information set by this parameter is sent to the requester.
- One of the following values can be set to the user information name:

User information name	Description
Authentication DB column name	A column name defined in the column information configuration file or a column name defined in the DBEXATTR parameter. However, this cannot be set if the reference database is used.
Reference database column name	A column name defined in the REFATTR parameter. (For Oracle and MySQL versions only)
IW_UID	The user ID input during login. If the value was changed in the UserExit routine, that value is sent.
IW_PWD	The password input during login. If the value was changed in the UserExit routine, that value is sent. It is not encrypted.
REMOTE_ADDR (ICP 2.0 only)	The client IP address.
Environment information (ICP 2.0 only)	The environment information that was sent from the requester at login.

- If this parameter is not set, all user information that is sent by default is sent to the requester.
- User information that is sent by default varies based on the communication protocol version as shown below.

User information name	ICP1.0	ICP2.0
Authentication DB column name	<input type="radio"/> *1	<input type="radio"/> *1

User information name	ICP1.0	ICP2.0
Reference database column name	○	○
IW_UID	○	○
IW_PWD	○	×
REMOTE_ADDR	×	○
Environment information	×	○

\*1 When using a reference database, the Authentication DB information is not sent.

- Because IW\_PWD is an unencrypted cleartext password, it is handled differently from other user information and works as follows.

Description	ICP1.0	ICP2.0
ACLREQUEST parameter in cert.conf is not set	○	×
SEND parameter is not set	○	×
IW_PWD is set in SEND parameter	○	○
SEND parameter included, and IW_PWD is not set	×	×

- Multiple instances of this parameter can be described.
- This parameter can describe multiple user information names by separating them with commas.
- The user information name is not case sensitive.
- This parameter cannot be used together with the NOTSEND parameter (described later).
- If the same column name is described multiple times, only one value is sent.
- There is no default value in the executable binary file.
- The initial values in the standard configuration file are as follows (in bold letters).

```
TARGET=SOURCE_ADDR=192.168.0.10-192.168.0.20
{
SEND=LOGONDATE
SEND=LASTDATE
}
```

#### Configuration example

- To send only the user ID and password that was entered at login to the requester:  
**SEND=IW\_UID,IW\_PWD**  
or  
**SEND=IW\_UID**  
**SEND=IW\_PWD**
- To send only the client IP address to the requester:  
**SEND=REMOTE\_ADDR**

**Request control configuration file (request.acl)**

---

Remarks	<ul style="list-style-type: none"><li>• If the requester is Forwarder, be aware that the basic authentication function for the Backend Web Server will not be available unless IW_UID and IW_PWD are sent. Also, in ICP 1.0, these two pieces of user information are required.</li></ul>
See also	EXDBATTR (Authentication Module configuration file) REFUID (Authentication Module configuration file) REFATTR (Authentication Module configuration file) Column information configuration file NOTSEND

# NOTSEND

**Overview** Sets the user information that is not sent to the requester by the access control response message.

**Format** **NOTSEND=**user information name[,user information name,...,user information name]

- This parameter is described between “{” and “}” of the TARGET parameter.
- Information other than the user information set by this parameter is sent to the requester.
- One of the following values can be set to the user information name:

User information name	Description
Authentication DB column name	A column name defined in the column information configuration file or a column name defined in the DBEXATTR parameter. If the reference database is set, this parameter is ignored even if it is set.
Reference database column name	A column name defined in the REFATTR parameter. (For Oracle and MySQL versions only)
IW_UID (ICP2.0 only)	The user ID input during login. The basic authentication header cannot be created at Forwarder unless this user ID is sent.
IW_PWD (ICP2.0 only)	The password input during login. The basic authentication header cannot be created at Forwarder unless this user ID is sent.
REMOTE_ADDR (ICP 2.0 only)	The client IP address.
Environment information (ICP 2.0 only)	The environment information that was sent from the requester at login.

- If this parameter is not set, all user information that is sent by default is sent to the requester.
- User information that is sent by default varies based on the communication protocol version as shown below.

User information name	ICP1.0	ICP2.0
Authentication DB column name	<input type="radio"/> *1	<input type="radio"/> *1
Reference database column name	<input type="radio"/>	<input type="radio"/>
IW_UID	<input type="radio"/>	<input type="radio"/>
IW_PWD	<input type="radio"/>	<input type="radio"/>

## Request control configuration file (request.acl)

User information name	ICP1.0	ICP2.0
REMOTE_ADDR	×	○
Environment information	×	○

\*1 When using a reference database, the Authentication DB information is not sent.

- Because IW\_PWD is an unencrypted cleartext password, it is handled differently from other user information and works as follows.

Description	ICP1.0	ICP2.0
ACLREQUEST parameter in cert.conf is not set	○	×
NOTSEND parameter is not set	○	×
IW_PWD is set in NOTSEND parameter	×	×
NOTSEND parameter included, and IW_PWD is not set	○	○

- Multiple instances of this parameter can be described.
- This parameter can describe multiple user information names by separating them with commas.
- The user information name is not case sensitive.
- This parameter cannot be used together with the SEND parameter.
- There is no default value in the executable binary file.
- The initial value is not set in the standard configuration file. (commented out)

## Configuration example

- 1) To not send the login failure date to the requester:  
**NOTSEND= LOGONFAIL**

## Remarks

- If the requester is Forwarder, be aware that the basic authentication function for the Backend Web Server cannot be used unless IW\_UID and IW\_PWD are sent.
- If this parameter is set, the password is sent to the requester as long as IW\_PWD is not set. If IW\_PWD is not particularly needed at the requester, make the setting below.  
**NOTSEND=IW\_PWD**

## See also

EXDBATTR (Authentication Module configuration file)  
REFUID (Authentication Module configuration file)  
REFATTR (Authentication Module configuration file)  
Column information configuration file  
SEND

# ACCCTRL

Overview	Sets control by access type regardless of the login type such as login by user ID and password or login by a client certificate and password.
Format	<p><b>ACCCTRL=<u>identifier</u></b></p> <ul style="list-style-type: none"><li>• This parameter is described between “[” and “]” of the TARGET parameter.</li><li>• One of the following values can be set to the identifier:<ul style="list-style-type: none"><li>uid : Only allow access without a client certificate</li><li>cert : Only allow access with a client certificate and check the user ID</li><li>certnoid : Only allow access with a client certificate, but do not check the user ID</li></ul></li><li>• This parameter can be indented. Use single byte space characters or the TAB character to make indents.</li><li>• There is no default value in the executable binary file.</li><li>• The initial value is not set in the standard configuration file. (commented out)</li><li>• The system is not guaranteed to work as expected if the value for this parameter is out of range.</li></ul>
Configuration example	<p>1) To allow access without a client certificate only: <b>ACCCTRL=uid</b></p> <p>2) To allow access with a client certificate only and check the user ID: <b>ACCCTRL=cert</b></p> <p>3) To allow access with a client certificate only and not to check the user ID: <b>ACCCTRL=certnoid</b></p>
Remarks	<ul style="list-style-type: none"><li>• Use the parameter when the Agent is installed and the presence of a client certificate is different between login and access.</li><li>• The “IceWall SSO Client Certificates Option” is required when setting cert or cernoid in this parameter, but it is not needed when setting uid only.</li></ul>
See also	ACCCTRLFLG (Authentication Module configuration file)



### 3.8 Authentication Module commands

Overview	Authentication Module commands control the operation of the Authentication Module. These commands are used when starting, stopping, and reloading the Authentication Module, and also when outputting the configuration file information and logging out all users.
Storage location	<p>The followings are the default storage locations:</p> <ul style="list-style-type: none"><li>/opt/icewall-ss0/certd/bin/start-cert</li><li>/opt/icewall-ss0/certd/bin/end-cert</li><li>/opt/icewall-ss0/certd/bin/info-cert</li><li>/opt/icewall-ss0/certd/bin/reload-cert</li><li>/opt/icewall-ss0/certd/bin/logout-cert</li><li>/opt/icewall-ss0/certd/bin/cdump-cert</li></ul>
Remarks	<p>None</p> <p>The following pages describe each command options.</p>

### 3.8.1 Script command options

The configurable options for the Authentication Module commands are listed below.

Command options	Overview
-c	Sets the Authentication Module configuration file
-F	Executes the Authentication Module process in the foreground
-H 10.0	Sets the host name or IP address of the destination to send the request
-K	Sends a request to the Authentication Module to perform the stop operation
-P	Sets the server port number of the destination to send the request
-R	Sends a request to the Authentication Module to perform the reload operation
-U	Sends a request to the Authentication Module to output operating information
--dump-config 10.0	Sends a request to output configuration file information
--silent 10.0	Do not output messages from the Authentication Module to standard output or default error output
--wait-response 10.0	Waits for the response message to return after sending request
--logout-alluser 10.0	Sends a request to the Authentication Module to log out all users that are logged in

For details on these options, see the following pages.

---

Authentication Module commands

---

## **-C**

Overview	Sets the Authentication Module configuration file (cert.conf).
Format	<b>-c [configuration file name]</b> <ul style="list-style-type: none"><li>• The configuration file name has a maximum length of 255 bytes.</li><li>• The default value in the module is /opt/icewall-ss0/certd/config/cert.conf.</li></ul>
Configuration example	1) To set /opt/icewall-ss0/certd/config/cert.conf as the Authentication Module configuration file: <b>/opt/icewall-ss0/certd/bin/certd -c /opt/icewall-ss0/certd/config/cert.conf</b>
Remarks	<ul style="list-style-type: none"><li>• ) This option is set for the Authentication Module command.</li><li>• ) This option can only be set for the Authentication Module startup command (start-cert).</li></ul>
See also	None

## **-F**

Overview	Executes the Authentication Module process in the foreground.
Format	<b>-F</b> <ul style="list-style-type: none"><li>• When this command option is not used, the Authentication Module runs in the background.</li></ul>
Configuration example	1) To run the operation information output command (info-cert) in the foreground: <b>/opt/icewall-ss0/certd/bin/certd -F -U</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can be set for the Authentication Module commands (end-cert, info-cert, reload-cert, cdump-cert, logout-cert) except for the startup command (start-cert).</li></ul>
See also	None

---

**Authentication Module commands**

---

**-H** ⑩.⑩

Overview	Sets the host name of the destination to send the request.
Format	<b>-H [host name]</b> <ul style="list-style-type: none"><li>• The default value in the module is localhost.</li><li>• When the host name is set enclosed in brackets (example: [localhost]), priority is given to IPv6 connections. ⑩.⑩</li></ul>
Configuration example	1) To send a stop operation request to the localhost Authentication Module <b>/opt/icewall-ss0/certd/bin/certd -F -K -H localhost</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can be set for the Authentication Module commands (end-cert, info-cert, reload-cert, cdump-cert, logout-cert) except for the startup command (start-cert).</li><li>• The host name can only be set to host loopback address.</li></ul>
See also	None

## **-K**

Overview	Sends a request to the Authentication Module to perform the stop operation.
Format	<b>-K</b>
Configuration example	1) For the stop command: <b>/opt/icewall-ss0/certd/bin/certd -F -K</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can only be set for the Authentication Module stop command (end-cert).</li></ul>
See also	None

---

Authentication Module commands

---

## -P

Overview	Sets the Authentication Module port number of the destination to send the request.
Format	<b>-P [port number]</b> <ul style="list-style-type: none"><li>• Sets the port number for the destination to send the Authentication Module command request.</li></ul>
Configuration example	1) To specify the port number of the destination to send the stop command (end-cert) request <b>/opt/icewall-ssso/certd/bin/certd -F -K -P 14142</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can be set for the Authentication Module commands (end-cert, info-cert, reload-cert, cdump-cert, logout-cert) except for the startup command (start-cert).</li></ul>
See also	None

## -R

Overview	Sends a request to the Authentication Module to perform the reload operation.
Format	<b>-R</b>
Configuration example	1) To execute the reload command (reload-cert) <b>/opt/icewall-ss0/certd/bin/certd -F -R -P 14142</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can only be set for the Authentication Module reload command (reload-cert).</li></ul>
See also	None



---

Authentication Module commands

---

## -U

Overview	Sends a request to the Authentication Module to output operating information.
Format	<b>-U</b>
Configuration example	1) To execute the operating information output command (info-cert) <b>/opt/icewall-ss0/certd/bin/certd -F -U -P 14142</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can only be set for the operating information output command (info-cert).</li></ul>
See also	None

## --dump-config 10.0

Overview	Sends a request to the Authentication Module to output the configuration files.
Format	<b>--dump-config</b>
Configuration example	1) To execute the configuration file information output command (cdump-cert) <b>/opt/icewall-ssu/certd/bin/certd -F --dump-config -p 14142</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can only be set for the configuration file information output command (cdump-cert).</li></ul>
See also	None

---

**Authentication Module commands**

---

**--silent** 10.0

Overview	Controls messages output by the Authentication Module command.
Format	<b>--silent</b> <ul style="list-style-type: none"><li>• Messages are output when this command option is not used.</li></ul>
Configuration example	1) To not output to standard output the execution results of the operating information output command (info-cert) <b>/opt/icewall-ss0/certd/bin/certd -F -U --silent -p 14142</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can be set for all Authentication Module commands (start-cert, end-cert, info-cert, reload-cert, cdump-cert, logout-cert).</li><li>• Even when this option is set, the end status is still set to output.</li></ul>
See also	None

## --wait-response 10.0

Overview	Sets whether or not to wait for a response after executing an Authentication Module command.
Format	<b>--wait-response</b> <ul style="list-style-type: none"><li>When this command option is not used, the system does not wait for a response after sending a command (start-cert, end-cert, info-cert, reload-cert, cdump-cert, logout-cert) request to the Authentication Module.</li></ul>
Configuration example	1) To wait for a stop command (end-cert) response <b>/opt/icewall-ss0/certd/bin/certd -F -K --wait-response -P 14142</b>
Remarks	<ul style="list-style-type: none"><li>This option is set for the Authentication Module command.</li><li>This option can be set for the Authentication Module commands (end-cert, info-cert, reload-cert, cdump-cert, logout-cert) except for the startup command (start-cert).</li></ul>
See also	None

Authentication Module commands

---

## --logout-alluser 10.0

Overview	Sends a request to log out all logged in users.
Format	<b>--logout-alluser</b>
Configuration example	1) To execute the log out all users command (logout-cert) <b>/opt/icewall-ss0/certd/bin/certd -F --logout-alluser -p 14142</b>
Remarks	<ul style="list-style-type: none"><li>• This option is set for the Authentication Module command.</li><li>• This option can only be set for the log out all users command (logout-cert).</li></ul>
See also	None

## Index

### A

ACCCTRL .....	558
ACCCTRLFLG.....	390
ACCESS(cert.conf).....	350
ACCESS(dfw.conf) .....	9
ACCESS_DENY.....	260
ACCTHREAD .....	458
ACL.....	371
ACLREQUEST .....	372
ADDGFWBIND.....	445
ADGROUP .....	373
ADGROUPDN.....	374
ADGROUPINTERVAL.....	375
ADGROUPMAXMEMBER.....	378
ADGROUPPREFIX .....	377
ADGROUPPRINAME .....	376
ADPCHG .....	441
AGENT_KEY .....	121
AGENT_PERMIT .....	122
ALEVEL(cert.conf) .....	348
ALEVEL(dfw.conf) .....	7
ALLOC .....	87
ALPHANUM.....	80
ATTRQUOT_FLG.....	143

### B

BA_PWD .....	154
BASICAUTH.....	152
BA_UID .....	153
BUFFER.....	200

### C

-c .....	561
CACHE.....	467
CATALOG(cert.conf) .....	353
CATALOG(dfw.conf).....	13
CC_DECODE_FLG.....	109
CC_ENVEXPIRE.....	112
CC_ENVISSUER.....	113
CC_ENVNAME.....	108
CC_ENVSERIAL .....	111
CC_ENVUID.....	110
CC_UID.....	104
CC_UIDKEYE.....	106
CC_UIDKEYS.....	105
CENCODE .....	202
CERT(cert.conf) .....	477

---

CERT(dfw.conf) .....	30
CERTEXPDATE .....	525
CERTFAILBACK .....	36
CERTLB .....	32
CERTLBFAILBACK .....	38
CERTLB_TYPE .....	34
CERTREPTYPE .....	480
CERT_TOUT .....	86
CERTUNIQUEKEY .....	394
CLIP .....	536
CLOSETIME .....	198
COOKIEALWAYS .....	44
COOKIEATTR .....	42
COOKIEEXP .....	382
COOKIE_FILTER .....	162
COOKIENAME(dfw.conf) .....	40
COOKIERETRY .....	380
COOKIETIME .....	381
CTRL_SPKEY .....	169
CTYPE .....	132

## D

DATA_SEND_ERR .....	262
DBATTR .....	424
DBCRYPTOATTR .....	429
DBCRYPTOTYPE .....	427
DBEXATTR .....	425
DBHOST .....	416
DBIWCRYPTOSEED .....	428
DBPWD .....	421
DBQUESIZE .....	463
DBTBL .....	422
DBUID .....	419
DFWFILTER .....	96
DFW_PROTOCOL .....	24
DOCS(dfw.conf) .....	62
DOWNLOADCONFFLG .....	474
--dump-config .....	568
DUPKIND .....	387
DUPLOGIN .....	386

## E

ELEVEL(cert.conf) .....	349
ELEVEL(dfw.conf) .....	8
ERRKEY .....	149
ERROR(cert.conf) .....	351
ERROR(dfw.conf) .....	10
ERRORINFO .....	11
EXPIRE .....	77

---

**F**

-F .....	562
FAILBACK .....	490
FILTER_GET .....	302
FILTER_HTML .....	306
FILTER_POST .....	304
FILTER_REQUEST .....	266
FILTER_SVR .....	308
FLOGINDATE .....	515
FO_NODATA .....	207
FORCELOGIN_ENC .....	49
FO_RECV .....	206
FORM_DATA_PAGE .....	228
FORM_DATA_PAGE_REF .....	230
FORM_DATA_STR .....	224
FORM_DATA_USR .....	226
FORM_FILE .....	210
FORM_HTML .....	222
FORM_KEY .....	218
FORM_KEY_EXCEPTION .....	220
FORM_METHOD .....	215
FORM_SEND .....	216
FORM_URL .....	217
FO_SEND .....	205

**G**

GETCERT .....	526
GETEXCEPTION .....	173
GETFILTER .....	172
GETFILTERERR .....	174
GETFILTER_LOG_FLG .....	176
GROUP .....	370

**H**

-H .....	563
HEADER .....	158
HEADER_FILTER .....	160
HEADER_NAME_SID .....	165
HEADER_NAME_TID .....	163
HEADER_NAME_UID .....	164
HEALTHCNT .....	488
HEALTHTIMER .....	486
HOST .....	67
HTML_CHARSET .....	65
HTMLFILTER .....	182
HTMLFILTERERR .....	183
HTTPDATA .....	156
HTTPCHOHEADER .....	368
HTTPPORT .....	367



**I**

ICP_AGENTSTR .....	58
ICP_ENCSTR.....	60
ICP_VERSION.....	57
INFORMATION .....	361
IPV6LISTEN.....	365
IWSERIALNO.....	524

**K**

-K .....	564
KIND .....	533

**L**

LASTMOD_HEADER.....	201
LDAPBIND .....	430
LDAPCACERT.....	437
LDAPCIPHERSUITE.....	439
LDAPLANG .....	434
LDAPMULTIVAL.....	443
LDAPPCHG .....	432
LDAPREFERRAL.....	444
LDAPSSL .....	436
LDAPSSLBIND .....	440
LDAPVERIFYSVRCERT .....	438
LIVETIMER.....	484
LLOGINDATE .....	512
LOALIAS.....	56
LOCATIONRETRY.....	64
LOCATIONURL .....	63
LOCKCOUNT.....	407
LOCKDATE .....	520
LOGBUFSIZE.....	465
LOGDBATTR.....	448
LOGDBQUESIZE .....	464
LOGDBSEQNAME.....	449
LOGDBTBL .....	447
LOGIN_CERT.....	237
LOGIN_ERR_1STCERT.....	247
LOGIN_ERR_LIMIT .....	255
LOGIN_ERR_LOCK.....	245
LOGIN_ERR_NOGRP .....	251
LOGIN_ERR_POSTLIMIT .....	257
LOGIN_ERR_PWD.....	243
LOGIN_ERR_SERIAL.....	249
LOGIN_ERR_STOP.....	253
LOGIN_ERR_UID .....	241
LOGININFO.....	354
LOGIN_FORCE .....	239
LOGINOK.....	519
LOGINSTAT .....	521

---

---

LOGIN_UID .....	235
LOGMULTITHREAD .....	472
LOGOUT .....	272
--logout-alluser .....	571
LOGOUT_EXPIRE .....	276
LOGOUT_FAILURE .....	278
LOGOUT_SUCCESS .....	274
LOGPERF .....	356
LOMETHOD .....	384

**M**

MAXDBCONNECT .....	461
MAXLEN .....	76
MAXLOGINUSER .....	468
MAXPOST .....	116
MAXPOST_ERR .....	269
MAXQUERY .....	92
MAXREPTHREAD .....	492
MAXREQTHREAD .....	456
MAXURL .....	91
MINLEN .....	75
MSG .....	535

**N**

NO .....	530
NOCHK_EXT_ALIAS .....	98
NOTSEND .....	556

**O**

ONLINE .....	527
--------------	-----

**P**

-P .....	565
PARALOGIN .....	389
PASSWORD .....	506
PCHGDATE .....	511
PCHGOK .....	510
PERFORMANCE .....	359
PLOGINDATE .....	513
PORT .....	363
POST_ENC .....	119
POSTEXCEPTION .....	178
POSTFILTER .....	177
POSTFILTERERR .....	179
POSTFILTER_LOG_FLG .....	181
POST_HTML .....	118
POST_INHERIT .....	115
POSTKEY_LOGIN .....	51
POSTKEY_LOGOUT .....	52

---

---

POSTKEY_PWDCHG.....	53
POSTLIMIT_ENC .....	48
POSTLIMIT_PAGE .....	46
POSTLIMIT_TIME.....	47
POSTNAME.....	117
POSTWAITTIME.....	89
PWDALIAS .....	74
PWDALPHANUM .....	402
PWDCHG.....	281
PWDCHG_ERR_LOGNG .....	291
PWDCHG_ERR_OLD.....	285
PWDCHG_ERR_POLICY.....	289
PWDCHG_ERR_POSTLIMIT.....	299
PWDCHG_ERR_REENT.....	287
PWDCHG_ERR_VIO .....	293
PWDCHG_FAILURE .....	295
PWDCHGHASH .....	398
PWDCHG_SUCCESS.....	283
PWDCHG_WARNING .....	297
PWDEXPCHK.....	408
PWDEXPDATE.....	507
PWDEXPIRE .....	404
PWDEXPWARN .....	412
PWDFORBID.....	411
PWDHISCHK .....	409
PWDHISCNT.....	410
PWDHISTORY .....	508
PWDLOCK.....	518
PWDLOGINHASH .....	396
PWDMAXLEN .....	401
PWDMINLEN.....	400
PWDRETRY.....	517
PWDSAMEPASS .....	406

## Q

QUERY_ENC.....	124
QUERY_ENC_KIND .....	126
QUERY_ENC_NAME.....	125

## R

-R .....	566
RASERIALNO .....	523
RECVWAITTIME .....	470
RECV_ZERO_FLG .....	208
REDIRECT.....	54
REFATTR.....	453
REFTBL .....	451
REFUID .....	454
REJECT .....	551
RELOGIN_KEY.....	127

---

REPKEY.....	135
REPKEY_EXT .....	137
REPQUESIZE.....	494
REQQUESIZE .....	460
REQUEST_ACL_ERR.....	264
REQUESTFILTER .....	101
REQUEST_URI .....	25
RES_HEADER.....	166
RESULT .....	534
RETRYCNTC(cert.conf) .....	482
RETRYCNTC(dfw.conf).....	83
RETRYCNTW .....	193
RETRYTMC(cert.conf).....	483
RETRYTMC(dfw.conf).....	84
RETRYTMW .....	194
REV_PATH .....	93

## S

SAMEPASS.....	79
SECEXCPAGE.....	17
SECINFO .....	15
SECLEVEL .....	16
SECURITY.....	14
SEND.....	553
SERIAL .....	538
SESSION.....	50
SESSION_ENC_KEY.....	95
SESSIONIDLEN .....	392
SET_CONTENT_LENGTH.....	88
SHOST .....	70
--silent .....	569
SPKEY_TOPPAGE_URL .....	18
SSL_CIPHER_SUITE .....	212
SVREXCEPTION .....	187
SVRFILE .....	72
SVRFILTER.....	185
SVRFILTERERR.....	188
SVRFILTERSTR.....	190
SYSERR .....	145
SYSTEM_BUSY_DB .....	327
SYSTEM_DOWN_CERTD.....	317
SYSTEM_DOWN_DB.....	319
SYSTEM_DOWN_HTTP .....	321
SYSTEM_ERR .....	311
SYSTEM_ERR_BADALIAS .....	315
SYSTEM_ERR_NOALIAS .....	313
SYSTEM_TOUT_CERTD.....	323
SYSTEM_TOUT_HTTP .....	325
SYSTOUT.....	147

**T**

TARGET .....	546
THREADSTACKSIZE .....	471
TIME .....	531
TIMEOUT .....	196
TRACE(cert.conf) .....	352
TRACE(dfw.conf) .....	12
TRACETIME .....	23
TRANSID(cert.conf) .....	357
TRANSID(dfw.conf) .....	20
TRANSID_STR .....	22

**U**

-U .....	567
UID(dbattr.conf) .....	505
UID(logdbattr.conf) .....	532
UNCONV_HEADER .....	168
URLCONV_ATTR_FLG .....	141
URLCONV_FLG .....	139
URLKEY .....	133
URL_SCOLON .....	204
USREXT_ERR1 .....	330
USREXT_ERR2 .....	332
USREXT_ERR3 .....	334
USREXT_ERR4 .....	336
USREXT_ERR5 .....	338
USREXT_ERR6 .....	340

**V**

VERSION .....	549
VIRTUALPATH_ENV .....	26
VIRTUALURL_ALIAS .....	27

**W**

--wait-response .....	570
-----------------------	-----