IceWall SSO

Version 10.0

Sample Setup Guide

August 2010

Printed in Japan

HP Part No. B1544-97007

Rev.111006A

Notice

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

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

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

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

IceWall is a trademark of Hewlett-Packard.

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

– Table of Contents –

1 Introduction

This document describes the method for displaying IceWall SSO sample pages. As an example, this document illustrates the case of installing all IceWall SSO modules on one server.

1.1 Version designations in the text

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

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

2 Sample Overview

In this manual, you can configure IceWall SSO according to “Setting Up the Sample” and verify the procedures up to installing a simple menu page to check the operation of IceWall SSO.
Although the actual server configuration may be more complicated than the sample, completing the sample setup can help you understand the basic procedures for setting up IceWall SSO.

<Prerequisite conditions>

(1) All the IceWall SSO modules must be installed on the same server following the procedure in “IceWall SSO Installation Guide” and their operation verified.

(2) A web server compatible with a platform supporting IceWall must be installed.

(3) The Authentication DB to be used must be installed.

(4) If using Oracle Database as the Authentication DB, the SID must be set to “ORCL”.

(5) If using Sun Java System Directory Server, HP Directory Server, OpenLDAP, or Novell eDirectory as the Authentication DB, the directory entry must be “o=Alias.com”.

(6) If using Microsoft Active Directory or Microsoft Active Directory Lightweight Directory Services as the Authentication DB, the directory entry must be “CN=Users,DC=Alias,DC=com”.

(7) If using MySQL as the Authentication DB, the database name must be “icewalldb”.

(8) IceWall server must have access to the Internet without using a proxy.

The following chapters describe the sample configuration method and other processes. The web server and database terminology below are used.

Terminology	Corresponding products
Apache	HP-UX Apache-based Web Server v2.2.x (64 bit) (“x” is 8 or higher) Apache HTTP Server 2.2.3
ORACLE	Oracle Database 11g Release 1 Standard Edition Oracle Database 11g Release 1 Enterprise Edition Oracle Database 11g Release 2 Standard Edition Oracle Database 11g Release 2 Standard Edition
LDAP OpenLDAP	Sun Java System Directory Server 7.0 HP Directory Server 8.1 OpenLDAP 2.4.x (“x” is 16 or higher)
NED	Novell eDirectory 8.8 Novell eDirectory 8.8.x (“x” is 1 or higher)

Terminology	Corresponding products
MSAD	Microsoft Active Directory (Windows Server 2008) Microsoft Active Directory (Windows Server 2008 SP2) Microsoft Active Directory (Windows Server 2008 R2) Microsoft Active Directory Lightweight Directory Services (Windows Server 2008) Microsoft Active Directory Lightweight Directory Services (Windows Server 2008 SP2) Microsoft Active Directory Lightweight Directory Services (Windows Server 2008 R2)
CSV	Text Authentication DB file
MySQL	MySQL 5.1.x (“x” is 40 or higher)

3 Setting Up the Sample

Configure the items below to run the IceWall SSO sample.

- Configuring the web server to run Forwarder
- Configuring the Backend Web Server to display the Sample Menu page
- Configuring the registration of the Sample Menu page as content for Forwarder’s Backend Web Server
- Configuring access control in the Authentication Module to reference the Sample Menu page
- Creating tables and users for the Authentication DB

The rest of this chapter explains how to configure these items.

3.1 Configuring the web server to run Forwarder

Configure the web server so that Forwarder operates on client requests. For details on this configuration, see the “IceWall SSO Installation Guide.”

3.2 Configuring the Backend Web Server to display the Sample Menu page

Create the Sample Menu content and configure the Backend Web Server so that the Sample Menu page is displayed in response to requests from Forwarder. Place the Sample Menu page in a location that can be accessed by the Backend Web Server. For the Sample Menu page source code, see “3.8 Sample Menu page”.

3.3 Configuring the registration of the Sample Menu page as content for Forwarder’ s Backend Web Server

Configure the Sample Menu page so it can be accessed as content displayed by Forwarder’s Backend Web Server.

3.3.1 Configuring the Forwarder configuration file

Configure the configuration file using the following method.

(1) Open the Forwarder configuration file (dfw.conf) with an editor.

```
# vi /opt/icewall-sso/dfw/cgi-bin/dfw.conf
```

(2) Add the following line:

```
HOST=SAMPLEMENU=[host name]:[port number]
```

Specify the host name and port number of the Backend Web Server that will display the Sample Menu page for [host name] and [port number].

(3) Also add the following line:

```
SVRFILE=SAMPLEMENU,./sample.conf
```

(4) Save the configuration file and close the editor.

3.4 Configuring access control in the Authentication Module to reference Sample Menu Page

Configure access privilege to Sample Menu page accessed as Forwarder’s Backend Web Server.

3.4.1 Configuring the access control file

Configure the configuration file using the following method.

(1) Open the access control file (cert.acl) with an editor.

```
# vi /opt/icewall-sso/certd/config/cert.acl
```

(2) Add the following line:

```
http://[host name]:[port number]/=ALL|SccOnly|HpOnly
```

Specify the host name and port number of the web server that will display the Sample Menu page for [host name] and [port]. However, if the port number is the standard web server port 80, there is no need to set the port number since it is omitted by Forwarder.

(3) Save the configuration file and close the editor.

(4) Restart the Authentication Module.

3.5 Creating tables and users for the Authentication DB

Create the table to register the users who log in to IceWall SSO and create users. The method for creating the table and users differs depending on the type of the Authentication DB.

3.5.1 If the Authentication DB is ORACLE

If the Authentication DB is ORACLE, you must create the table and users.
The creation method below is used when the passwords for sample users are MD5 encrypted.
(1) Creating the authentication table
Execute the SQL statement below with SQL*Plus to create the authentication

table. Use scott/tiger (user ID/password) to execute SQL*Plus. (The environment must be one in which this user ID and password can be used.)
SQL for creating the sample authentication table (/opt/icewall-sso/tools/cre_tbl_test.sql)

```
create table icewalltest (
   USERID          varchar(64)        NOT NULL,
   PASSWD          char(37)           NOT NULL,
   PASSCHANGE      char(1)            NOT NULL,
   PASSWDEXP       char(14)           NULL,
   PASSWDHIS       char(109)          NULL,
   CHGDATE         char(14)           NULL,
   LOGONDATE       char(14)           NULL,
   LASTDATE        char(14)           NULL,
   LOGONFAIL       char(14)           NULL,
   FAILCOUNT       number(38)         DEFAULT 0 NOT NULL,
   LOCKOUT         char(1)            DEFAULT 0 NOT NULL,
   LOGONSTOP       char(1)            DEFAULT 0 NOT NULL,
   LOCKDATE        char(14)           NULL,
   LOGSTATUS       char(1)            DEFAULT 0 NOT NULL
);
```

(2) Creating the sample users

After creating the authentication table, create the users to be used in the sample. Use SQL*Plus to create the users just like you did to create the authentication table.

SQL for creating sample users (/opt/icewall-sso/tools/add_test_user.sql)

```
INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user01','{MD5}b75705d7e35e70
14521a46b532236ec3','1','0','0','0','0' );

INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user02','{MD5}8bd108c8a01a89
2d129c52484ef97a0d','1','0','0','0','0' );

INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user03','{MD5}a7d39043afa25b
e5cc235d943b64917a','1','0','0','0','0' );

INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user04','{MD5}9e3526e252e6d5
914ec1bdaabc680436','1','0','0','0','0' );
```

Note: The passwords are the same as the user IDs.

(3) Creating the history table

Execute the SQL statement below with SQL*Plus to create the history table. Use scott/tiger (user ID/password) to execute SQL*Plus. (The environment must be one in which this user ID and password can be used.)

SQL for creating the sample history table (/opt/icewall-sso/tools/cre_tbl_history.sql)

```
create table history (
   UKENO           CHAR(16)          NOT NULL,
   UKEDATE         CHAR(14)          NOT NULL,
   USERID          VARCHAR2(64),
   KIND            CHAR(1)           NOT NULL,
   RESCODE         CHAR(1)           NOT NULL,
   MESSAGE         VARCHAR2(256)     NOT NULL,
   IPADDR          CHAR(39)
);
```

(4) Creating the sequence object

Execute the SQL statement below with SQL*Plus to create the sequence object. Use scott/tiger (user ID/password) to execute SQL*Plus. (The environment must be one in which this user ID and password can be used.)

SQL for creating the sample sequence object (/opt/icewall-sso/tools/cre_sequence.sql)

```
create sequence WEB_REVIEW_SEQ increment by 1 start with 1
maxvalue 9999999999999999 cycle cache 20 order;
```

3.5.2 If the Authentication DB is LDAP, NED, or OpenLDAP

If the Authentication DB is LDAP, NED, or OpenLDAP, you do not need to create any tables because the base directory of the instance is used. Only users are created. The creation method below is used when the passwords for sample users are SHA encrypted.

(1) Creating the sample users

Create the sample users using the tool provided with the Authentication Module. Execute the commands below as root user.

```
# cd /opt/icewall-sso/tools
# ./mkuser TEMPLATE.ldif DATA.txt > SampleUser.ldif
```

After creating the sample users LDIF file, use the tool provided with the server (LDPA: ldapmodify, NED: ice) to register the LDIF file. (Set the desired passwords.)

Note: For details on mkuser, see the “IceWall SSO Batch Registration Tool Manual.”

3.5.3 If the Authentication DB is MSAD

When using MSAD as the Authentication DB, a table does not need to be created.
Use the MSAD management tool to create the following users to be used in the sample.
The creation method below is used when the passwords for sample users are SHA encrypted.

User name	User ID
Sample user 1	user01
Sample user 2	user02
Sample user 3	user03
Sample user 4	user04

Note: Set the desired passwords.

3.5.4 If the Authentication DB is CSV

If the Authentication DB is CSV, use the installed CSV file (sample.csv) already created for the sample. Sample users user01 through user04 have been created in advance. (The passwords are the same as the user IDs.)

3.5.5 If the Authentication DB is MySQL

If the Authentication DB is MySQL, you must create the table and users.
The creation method below is used when the passwords for sample users are MD5 encrypted.

(1) Creating the authentication table
Execute the SQL statement below with a mysql command to create the authentication table.

SQL for creating the sample authentication table (/opt/icewall-sso/tools/cre_tbl_test.sql)

```
create table icewalltest (
   USERID            varchar(20)         PRIMARY KEY,
   PASSWD            char(37)            NOT NULL,
   PASSCHANGE        char(1)             NOT NULL,
   PASSWDEXP         char(14)            NULL,
   PASSWDHIS         char(109)           NULL,
   CHGDATE           char(14)            NULL,
   LOGONDATE         char(14)            NULL,
   LASTDATE          char(14)            NULL,
   LOGONFAIL         char(14)            NULL,
   FAILCOUNT         numeric(38)         DEFAULT 0 NOT NULL,
   LOCKOUT           char(1)             DEFAULT 0 NOT NULL,
   LOGONSTOP          char(1)            DEFAULT 0 NOT NULL,
   LOCKDATE          char(14)            NULL,
   LOGSTATUS         char(1)             DEFAULT 0 NOT NULL
) ENGINE=InnoDB;
```

(2) Creating the sample users
After creating the authentication table, create the users to be used in the sample. Use a mysql command to create the users just like you did to create the authentication table.

SQL for creating sample users (/opt/icewall-sso/tools/add_test_user.sql)

```
INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user01','{MD5}b75705d7e35e70
14521a46b532236ec3','1','0','0','0','0' );

INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user02','{MD5}8bd108c8a01a89
2d129c52484ef97a0d','1','0','0','0','0' );

INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user03','{MD5}a7d39043afa25b
e5cc235d943b64917a','1','0','0','0','0' );

INSERT INTO icewalltest ( USERID,PASSWD,PASSCHANGE,FAILCOUNT,LO
CKOUT,LOGONSTOP,LOGSTATUS )VALUES ( 'user04','{MD5}9e3526e252e6d5
914ec1bdaabc680436','1','0','0','0','0' );
```

Note: The passwords are the same as the user IDs.

3.6 Forwarder configuration files

These are the configuration values of the Forwarder configuration files used in the sample. The portions of the Forwarder configuration files other than the bold, underlined portions are configured when installed.

3.6.1 Forwarder configuration file (dfw.conf)

```
#---------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Document Forwarder.
#  $Workfile: dfw.conf $ $Revision: 26 $ $Date: 10/08/16 21:22 $
#---------------------------------------------------------------------------
#---------------------------------------------------------------------------
#  [ Log File Info ]
#    ALEVEL      : access log level
#              0 : no output
#              1 : user request  (default)
#              2 : user request, content size and IP address
#    ELEVEL      : error log level
#              0 : no output
#              1 : fatal messages only (default)
#              2 : fatal and warning messages
#              3 : fatal, warning and information messages
#    ACCESS      : access log file location
#              (default: /opt/icewall-sso/logs/dfw.log)
#    ERROR       : error log file location
#              (default: /opt/icewall-sso/logs/dfwerr.log)
#    TRACE       : trace log file location
#    CATALOG     : message catalog file location
#    ERRORINFO   : Additional information on an error log
#               ERRORINFO=[info],[info]...
#                [info]
#                  UID   : UserID of a client
#                  URL   : request URL
#                  IP    : IPAddress of a client
#                  AGENT : USER_AGENT of a client
#                ex. ERRORINFO=UID,URL,IP,AGENT
#    SECURITY    : security log file location
#    SECINFO     : Additional information on a security log
#               SECINFO=[info],[info]...
#                [info]
#                  LOGIN  : login successful log
#                  LOGOUT : logout successful log
#                  PWDCHG : password change successful log
#                  AGENT  : agent process successful log
#                  PAGE   : output page log
#                  REQUEST : request filtered log
#    SECLEVEL    : security log level
#              0 : agent hostname only
#              1 : agent hostname, IPAddress and UserID of a client
#              2 : agent hostname, IPAddress and UserID of a client
#                  , AGENT_KEY
#    SECEXCPAGE  : page name not output to security log
#              SECEXCPAGE=[page name],[page name]...
#               page name : template HTML configuration name
#    SPKEY_TOPPAGE_URL : the system wide top page URL to be replaced
#                   with the specific keyword $TOPPAGE_URL
#                   SPKEY_TOPPAGE_URL=top page URL
#    TRANSID : switches whether logging the transaction ID or not
#           0 : do not output the transaction ID to the log (default)
#           1 : log the transaction ID
#    TRANSID_STR : String to identify the forwarder to be in the transaction ID
#               dfw : the default string
#               (string in [a-zA-Z0-9][a-zA-Z0-9]* up to 16 characters)
#    TRACETIME : log file name for trace time log
#             TRACETIME=trace time log file name up to 255 characters
#---------------------------------------------------------------------------
ALEVEL=1
```

```
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/dfw.log
ERROR=/opt/icewall-sso/logs/dfwerr.log
#ERRORINFO=UID,URL,IP,AGENT
#TRACE=/opt/icewall-sso/logs/dfwtrace.log
CATALOG=/opt/icewall-sso/messages/C/icewall.cat
#SECURITY=/opt/icewall-sso/logs/dfwsec.log
#SECINFO=LOGIN,LOGOUT,PWDCHG,AGENT,PAGE
#SECLEVEL=1
#SECEXCPAGE=LOGIN_UID,LOGIN_CERT,LOGIN_FORCE,LOGOUT,PWDCHG
SPKEY_TOPPAGE_URL=http://www.hp.com/
TRANSID=1
TRANSID_STR=dfw01
#TRACETIME=/opt/icewall-sso/logs/dfwtracetime.log

#---------------------------------------------------------------------------
#  [ IceWall Certification Module Info ]
#    CERT : certification module's hostname or IP address:port no.
#          (default:localhost)
#    ICP_VERSION    : IceWall Cert Protocol Version
#                   1.1 : Vesion 1.1 (default)
#                   2.0 : Vesion 2.0
#    ICP_AGENTSTR   : agent string for IceWall Cert Protocol 2.0
#    ICP_ENCSTR     : ID string of ICP2.0 encryption method to be sent to
#                   authentication module
#                   icewall : icewall builtin encryption method(default)
#                   originalenc(for example) : user defined encryption method
#                                       configured in authentication module
#    CERTFAILBACK : original certification module connection order
#                 referred on failback
#                  CERTLBFAILBACK=hostname1[:port1],hostname2[:port2]
#    CERTLBFAILBACK : original load balancing certification module
#                   connection order referred on failback
#                    CERTLBFAILBACK=hostname1[:port1],hostname2[:port2]
#    CERTLB : certification module connection info on load balancing
#              CERTLB=authentification_module_identification_key=hostname[:port]
#    CERTLB_TYPE : certification module load balancing method
#                0 : based on the random number
#                1 : based on user ID (default)
#---------------------------------------------------------------------------
CERT=localhost:14142
ICP_VERSION=2.0
#ICP_AGENTSTR=DFW
#ICP_ENCSTR=originalenc
#CERTFAILBACK=localhost:14142,localhost:14143
#CERTLBFAILBACK=a=localhost:14142,localhost:14143
#CERTLBFAILBACK=b=localhost2:14142,localhost2:14143
#CERTLB=a=localhost:14142,localhost:14143
#CERTLB=b=localhost2:14142,localhost2:14143
#CERTLB_TYPE=1

#---------------------------------------------------------------------------
#  [ Session Control Info ]
#    COOKIENAME   : session ID name (default:IW_INFO)
#    SESSION      : HTTP session management style
#                 0 : use cookies for HTTP session management (default)
#                 1 : use URL cookies for HTTP session management
#    COOKIEATTR   : additional Cookie attribute
#                 ex. COOKIEATTR=path=/fw/dfw
#                     COOKIEATTR=domain=hp.com; path=/
#    COOKIEALWAYS : control of session ID set to browser
#                 0 : set after login only (default)
#               1 : set for each access (only for the conversion contents)
#               2 : set for each access (for any contents)
#    POSTLIMIT_PAGE : Template pages whose validity periods are checked
#                 at the receiving time of the POST request
#                 LOGIN      : UserID login page and
#                           client certificate login page
#                 FORCELOGIN : Force login page
#                 PWDCHG     : Password change page
#    POSTLIMIT_TIME : Validity period of the Post request sent thru
#                 Template pages (default: 3min)
#    POSTLIMIT_ENC  : Key string to encrypt/decrypt data in Template pages
#                 used checking validity period of POST request
#    FORCELOGIN_ENC : Key string to encrypts/decrypt User info in Force
#                 login page
#---------------------------------------------------------------------------
COOKIENAME=IW_INFO
SESSION=0
#COOKIEATTR=domain=hp.com
#COOKIEALWAYS=0
#POSTLIMIT_PAGE=LOGIN,FORCELOGIN,PWDCHG
#POSTLIMIT_TIME=3
#POSTLIMIT_ENC=abc123ABC-_!
#FORCELOGIN_ENC=abc123ABC-_!
#---------------------------------------------------------------------------
#  [ POST Data Keyword Info ]
#    POSTKEY_LOGIN  : login POST data keyword (default:ICEWALL_LOGIN)
#    POSTKEY_LOGOUT : logout POST data keyword (default:ICEWALL_LOGOUT)
#    POSTKEY_PWDCHG : password change POST data keyword
#                 (default:ICEWALL_PWDCHG)
#---------------------------------------------------------------------------
POSTKEY_LOGIN=ICEWALL_LOGIN
POSTKEY_LOGOUT=ICEWALL_LOGOUT
POSTKEY_PWDCHG=ICEWALL_PWDCHG

#---------------------------------------------------------------------------
#  [ Post data Inherit Setting Info  ]
#    POST_INHERIT   : Post data inherit
#                 0 : Post data is not inherited to.(default)
#                 1 : Post data is inherited to.
#    MAXPOST       : maximum Post data length allowed (for Post data inherit)
#    POSTNAME       : parameter name included in QueryString
#    POST_HTML      : template error HTML for Post data transmission
#    POST_ENC       : key letter strings to encrypts/decrypts Post data
#---------------------------------------------------------------------------
#POST_INHERIT=1
#MAXPOST=1024
#POSTNAME=iwpost
#POST_HTML=./iw_postdata.html
#POST_ENC=abc123ABC-_!

#---------------------------------------------------------------------------
#  [ Redirect URL Info ]
#    REDIRECT=[redirect URL]
#---------------------------------------------------------------------------
#REDIRECT=http://www.scc-kk.co.jp/index.html

#---------------------------------------------------------------------------
#  [ Reverse Certification Info ]
#    REV_PATH=[URL]
#---------------------------------------------------------------------------
#REV_PATH=http://welcome.hp.com/
```

```
#------------------------------------------------------------------------------
#  [ Logout Info ]
#    LOALIAS : logout ALIAS
#------------------------------------------------------------------------------
LOALIAS=IW-LOGOUT

#------------------------------------------------------------------------------
#  [ Template HTML File Info ]
#    DOCS          : template HTML configuration file location
#                  (default: /opt/icewall-sso/dfw/cgi-bin/html.conf)
#    LOCATIONURL   : location allowed for redirection in the template HTML
#    LOCATIONRETRY : retries allowed for redirection to the template HTML page
#                  (default: 1)
#    HTML_CHARSET  : character set for the template HTML
#------------------------------------------------------------------------------
DOCS=/opt/icewall-sso/dfw/cgi-bin/html.conf
#LOCATIONURL=welcome.hp.com:80
#LOCATIONRETRY=3
HTML_CHARSET=Shift_JIS

#------------------------------------------------------------------------------
#  [ Backend Web Server Info ]
#    HOST=[alias]=[hostname or IP address: port no.](proxy server:port no.)
#    SHOST=[alias]=[hostname or IP address: port no.]
#    ex. HOST=SVR=www.XXX.com(proxy.XXX.com:8080)
#------------------------------------------------------------------------------
HOST=SCC=www.scc-kk.co.jp:80
HOST=HPJP=welcome.hp.com:80
HOST=sys=localhost:80
HOST=DM=[host name]:[port]

#------------------------------------------------------------------------------
#  [ Backend Web Server Configuration File ]
#    SVRFILE=[alias],[file location]
#------------------------------------------------------------------------------
SVRFILE=SCC,./sample.conf
SVRFILE=HPJP,./sample.conf
SVRFILE=LOCALHOST,./sample.conf
SVRFILE=SAMPLEMENU,./sample.conf

#------------------------------------------------------------------------------
#  [ Password Policy Info ]
#    PWDALIAS : password change ALIAS
#------------------------------------------------------------------------------
PWDALIAS=IW-PWDCHG

#------------------------------------------------------------------------------
#  [ Network Connection Info ]
#    RETRYCNTC : number of retries allowed for certification module connection
#              (default: 10)
#    RETRYTMC  : time of retry intervals at the connection failures to the
#              certification module (default: 3sec)
#------------------------------------------------------------------------------
RETRYCNTC=10
RETRYTMC=3

#------------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#    ALLOC        : buffer allocation size (default: 65536Byte)
#    CERT_TOUT    : the total time the forwarder will allow to receive a
#                 response from a certification module (default: 600sec)
#    POSTWAITTIME : the total time the forwarder will allow to read
#               Post data (default: 180sec)
#--------------------------------------------------------------------------
ALLOC=65536
CERT_TOUT=600
#POSTWAITTIME=180

#--------------------------------------------------------------------------
#  [ Special Operation Info ]
#    DFW_PROTOCOL    : protocol that dfw operates
#                 0 : dfw operates as HTTP
#                 1 : dfw operates as SSL
#    REQUEST_URI     : Environment variable to acquire connected passing
#                 to BackendWebServer.
#                 0 : from PATH_INFO(default)
#                 1 : from REQUEST_URI(for Apache only)
#    VIRTUALPATH_ENV : environment variable for Original URL
#    VIRTUALURL_ALIAS : Mapping between a string in a URL sent from
#                  Web clients and an ALIAS for a Backend Web server
#                 [alias]=[character string included in URL]
#--------------------------------------------------------------------------
#DFW_PROTOCOL=0
#REQUEST_URI=1
#VIRTUALPATH_ENV=IW_PATH
#VIRTUALURL_ALIAS=HPJP=www.XXX.com

#--------------------------------------------------------------------------
#  [ Content-length Header Info ]
#    SET_CONTENT_LENGTH : Content-length header addition
#             0 : a Content-length header is not added (default)
#             1 : a Content-length header is added
#--------------------------------------------------------------------------
SET_CONTENT_LENGTH=0

#--------------------------------------------------------------------------
#  [ Security Setting Info ]
#    MAXURL          : maximum URL length allowed
#    MAXQUERY        : maximum QUERY_STRING length allowed
#    SESSION_ENC_KEY  : key letter strings to encrypts/decrypts session ID
#    DFWFILTER       : a tag in the Specific keyword to filter
#                  0 : no filter
#                  1 : only filter specific keyword in template HTML
#                     (default)
#                  2 : filter all Specific keyword
#    NOCHK_EXT_ALIAS  : The file extensions(ex. "jpg")
#                  that disable authentication and authorization
#                  for the backend webservers defined as "alias".
#                  NOCHK_EXT_ALIAS=[alias],[flg],[extension]...
#                  ex. NOCHK_EXT_ALIAS=SVR,0,gif,jpeg
#    REQUESTFILTER : request types to be filtered
#                any access from clients should be rejected with the filter
#                REQUESTFILTER=request_type1[,request_type2,...]
#                [request type]
#                 LOGIN     : login, view login page
#                 AGTLOGIN  : login, view login page with Agent Option
#                 LOGOUT    : logout, view logout page
#                 ACCESS    : accses control
#                 PWDCHG    : password change, view password change page
#                 AGTPWDCHG : password change, view password change page
#                        with Agent Option
#--------------------------------------------------------------------------
MAXURL=512
MAXQUERY=512
```

```
#SESSION_ENC_KEY=aaaaa
#DFWFILTER=1
#NOCHK_EXT_ALIAS=
#REQUESTFILTER=AGTLOGIN,AGTPWDCHG

#---------------------------------------------------------------------------
#  [ Client Certificate Info ]
#    CC_UID        : field in the client certificate to be used for userid
#                  (CN, EMAIL, or OU)
#    CC_UIDKEYS    : start point for userid division
#    CC_UIDKEYE    : end point for userid division
#    CC_ENVNAME    : the environment variable name of a client certificate.
#    CC_DECODE_FLG : The flag to enable CC_ENVUID, CC_ENVSERIAL,
CC_ENVEXPIRE,
#                  CC_ENVISSUER.
#    CC_ENVUID     : The environment variable which stores the value retrieved
#                  from the userID field of a client certificate.
#    CC_ENVSERIAL  : The environment variable which stores the value retrieved
#                  from the serial number field of a client certificate.
#    CC_ENVEXPIRE  : The environment variable which stores the value retrieved
#                  from the expiration date field of a client certificate.
#    CC_ENVISSUER  : The environment variable which stores the value retrieved
#                  from the issuer field of a client certificate.
#---------------------------------------------------------------------------
#CC_UID=CN
#CC_UID=CN
#CC_UIDKEYS=
#CC_UIDKEYE=
#CC_ENVNAME=CLIENT_CERT
#CC_DECODE_FLG=
#CC_ENVUID=
#CC_ENVSERIAL=
#CC_ENVEXPIRE=
#CC_ENVISSUER=

#---------------------------------------------------------------------------
#  [ Agent Recognition Info ]
#    AGENT_KEY      : agent recognition keyword
#                   AGENT_KEY=[Recognition keyword],[alias]
#    AENT_PERMIT    : The Agent information used to permit
#                   its connection with dfw
#                   AENT_PERMIT=[alias],[method]
#                          ,[IPaddress or Hostname or Domain]
#    QUERY_ENC      : key letter strings to encrypts/decrypts
#                   argument of dfw-Agent
#    QUERY_ENC_NAME : parameter name included in QueryString
#    QUERY_ENC_KIND : encryption judgment type parameter name
#    RELOGIN_KEY    : Agent re-login parameter
#---------------------------------------------------------------------------
#AGENT_KEY=AGENT_KEY
#AGENT_PERMIT=
#QUERY_ENC=abc123ABC-_!
#QUERY_ENC_NAME=param
#QUERY_ENC_KIND=agtkind
#RELOGIN_KEY=ForceAuthn=true
```

Specify the host name and port number of the web server that will display the Sample Menu page for [host name] and [port].

3.6.2 Host configuration file (sample.conf)

```
#---------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Document Forwarder.
#  $Workfile: sample.conf $ $Revision: 16 $ $Date: 10/07/01 14:50 $
#---------------------------------------------------------------------------
#---------------------------------------------------------------------------
#  [ Backend Web Server Configuration ]
#---------------------------------------------------------------------------

#---------------------------------------------------------------------------
#  [ Content-Type for URL Conversion ]
#    CTYPE=[Content-Type]
#---------------------------------------------------------------------------
CTYPE=text/plain
CTYPE=text/html
CTYPE=application/x-javascript
CTYPE=application/x-www-form-urlencoded
#---------------------------------------------------------------------------
#  [ URLConversion ]
#    URLKEY=[HTML tag name],[HTML tag attribute name] (ex URLKEY=A,HREF)
#---------------------------------------------------------------------------
URLKEY=A,HREF
URLKEY=BASE,HREF
URLKEY=FRAME,SRC
URLKEY=FORM,ACTION
URLKEY=BASE,TARGET
URLKEY=IMG,SRC
URLKEY=SCRIPT,SRC
URLKEY=BODY,BACKGROUND
URLKEY=TD,BACKGROUND
URLKEY=TR,BACKGROUND
URLKEY=TABLE,BACKGROUND
URLKEY=APPLET,CODEBASE
URLKEY=INPUT,SRC
URLKEY=LINK,HREF

#---------------------------------------------------------------------------
#  [ Keyword Conversion ]
#    REPKEY=[original string],[new string]
#    REPKEY_EXT=[target keyword],[string to be replaced with the target]
#---------------------------------------------------------------------------
#REPKEY=<img src='/stdnav/,<img src='/fw/dfw/HPJP/stdnav/
#REPKEY_EXT=<img alt='a\,b' src='/stdnav/,<img alt='a\,b' src='/fw/dfw/HPJP/std-
nav/

#---------------------------------------------------------------------------
#  [ URL Conversion Flag ]
#    URLCONV_FLG : Conversion mode for the attribute that contains ">"
#                0 : Handle ">" as the end of the tag (default)
#                1 : Handle ">" as a character
#    URLCONV_ATTR_FLG : switches if multiple attributes to be converted or not
#                    0 : one attribute by one tag, for the attribute
#                        name beginning with the keyword (default)
#                    1 : multiple different attributes by one tag,
#                        for each attribute name matching exactly with
#                        the keyword
#---------------------------------------------------------------------------
URLCONV_FLG=1
URLCONV_ATTR_FLG=1
```

```
#--------------------------------------------------------------------------
#  [Character sensitivity flag on handling attribute-value delimiters]
#    ATTRQUOT_FLG : Character sensitivity on handling attribute delimiters
#                0 : Identify APOSTROPHE with QUOTATION
#                1 : Distinguish between APOSTROPHE/QUOTATION MARK (default)
#--------------------------------------------------------------------------
#ATTRQUOT_FLG=1

#--------------------------------------------------------------------------
#  [ Specific Keyword Control ]
#    CTRL_SPKEY=[Specific Keyword],[Specific Keyword]...
#--------------------------------------------------------------------------
CTRL_SPKEY=$DFW,$REQUEST_URL,$HIDEURL,$ALIAS,$IW_INFO,$KEY_LOGI
N,$KEY_LOGOUT,$KEY_PWDCHG,$PWDCHG_URL,$LOGOUT_URL

#--------------------------------------------------------------------------
#  [ Backend Web Server Error HTML ]
#    SYSERR=file://[local HTML file path]
#          http://[host:port no. ][[file path]
#          https://[host: port no.][[file path]
#
#    SYSTOUT=file://[local HTML file path]
#           http://[host:port][[file path]
#           https://[host:port][[file path]
#
#    ERRKEY=[search string],file://[local HTML file path]
#          [search string],http://[host:port][file path]
#          [search string],https://[host:port][file path]
#--------------------------------------------------------------------------
SYSERR=file:///opt/icewall-sso/dfw/html/system_backend_error.html
SYSTOUT=file:///opt/icewall-sso/dfw/html/system_timeout_bkend.html
#ERRKEY=Server Error,file:///opt/icewall-sso/dfw/html/system_error.html

#--------------------------------------------------------------------------
#  [ Basic Authentication ]
#    BASICAUTH : send basic authorization header
#              0 : don't send (default)
#              1 : send
#    BA_UID    : name of the database column to use for userid in the
#              authorization header
#    BA_PWD    : name of the database column to use for password in the
#              authorization header
#--------------------------------------------------------------------------
BASICAUTH=0
BA_UID=DEFAULT
BA_PWD=DEFAULT

#--------------------------------------------------------------------------
#  [ Database Column(Attribute) Transmission ]
#    HTTPDATA=[database column(attribute) name],[new header name]
#--------------------------------------------------------------------------
HTTPDATA=LOGONDATE,LOGONDATE

#--------------------------------------------------------------------------
#  [ HTTP-RequestHeader Transmission ]
#    HEADER=[original header name],[new header name | NOTSEND]
#
#    HEADER=[header name],[process],[value]
#           [process]
#            ADD      : add header
#                     [add header name],ADD,[add value]
#            ENVADD   : add environment value
#                   [add header name],ENVADD,[add environment name]
#           NOTSEND  : notsend header
#                   [delete header name],NOTSEND
#           MODNAME  : modify header name
#                   [old header name],MODNAME,[new header name]
#           MODVALUE : modify header value
#                   [modify header name],MODVALUE,[new header value]
#    HEADER_FILTER=[HTTP request header to filter]
#               UID     : filter userid
#               SESSION : filter session ID
#               COOKIE  : filter cookie
#               TRANSID : filter transaction ID
#    COOKIE_FILTER=[name of the cookie to filter]
#    HEADER_NAME_TID=[Transaction ID information header name]
#               (default: X-iw-transid)
#               (valid header name from 1 character up to 64 characters)
#    HEADER_NAME_UID=[User ID information header name]
#               (default: Uid)
#    HEADER_NAME_SID=[Session ID information header name]
#               (default: Session)
#               (valid header name from 1 character up to 64 characters)
#---------------------------------------------------------------------------
#HEADER=USER_AGENT,MODNAME,BROWSER
HEADER=HOST_SOFTWARE,ENVADD,SERVER_SOFTWARE
HEADER=IF_MODIFIED_SINCE,NOTSEND
HEADER=UID,NOTSEND
#HEADER_FILTER=UID
#HEADER_FILTER=SESSION
#HEADER_FILTER=COOKIE
#COOKIE_FILTER=IW_INFO
HEADER_NAME_TID=X-iw-transid
HEADER_NAME_UID=Uid
HEADER_NAME_SID=Session

#---------------------------------------------------------------------------
#  [ HTTP-ResponseHeader Transmission ]
#    RES_HEADER=[original header name],[method],[value]
#    UNCONV_HEADER=[header name],[header name]
#---------------------------------------------------------------------------
#RES_HEADER=SAMPLE_ADDHEADER,ADD,headervalue
#RES_HEADER=SAMPLE_HEADER,NOTSEND
RES_HEADER=Pragma,NOTSEND
RES_HEADER=Pragma,ADD,no-cache
RES_HEADER=Cache-Control,NOTSEND
RES_HEADER=Cache-Control,ADD,no-cache
#UNCONV_HEADER=LOCATION,SET-COOKIE

#---------------------------------------------------------------------------
#  [ Semicolon Conversion ]
#    URL_SCOLON : conversion of the semicolon contained in URL
#              0 : convert to [%3b] (default)
#              1 : no convert ([%3b] is convert to semicolon)
#---------------------------------------------------------------------------
URL_SCOLON=0

#---------------------------------------------------------------------------
#  [ Cross Site Scripting ]
#  [ GET Request Filter ]
#    GETFILTER     : a tag in the QUERY_STRING to filter
#    GETEXCEPTION  : allow the use of tags specified in GETFILTER, if the tag
#                 is specified under a variable specified in GETEXCEPTION
#    GETFILTERERR  : upon filtering
#                 0 : don't display an error page (default)
#                 1 : display an error page
#                 2 : error logging only with no actual ofiltering
#   GETFILTER_LOG_FLG : When outputting the filtered QueryString data to
#                    the error log
#                    0 : Do not mask the QueryString data (default)
#                    1 : Mask the QueryString data
#
# [ POST Request Filter ]
#   POSTFILTER    : a tag in the POST data to filter
#   POSTEXCEPTION : allow the use of tags specified in POSTFILTER, if the tag
#                 is specified under a variable specified in POSTEXCEPTION
#   POSTFILTERERR : upon filtering
#                 0 : don't display an error page (default)
#                 1 : display an error page
#                 2 : error logging only with no actual ofiltering
#   POSTFILTER_LOG_FLG : When outputting the filtered POST data to
#                     the error log
#                     0 : Do not mask the POST data (default)
#                     1 : Mask the POST data
#
# [ HTML Filter ]
#   HTMLFILTER    : a tag in the HTML to filter
#   HTMLFILTERERR : upon filtering
#                 0 : don't display an error page (default)
#                 1 : display an error page
#                 2 : error logging only with no actual ofiltering
#
# [ Server Filter ]
#   SVRFILTER     : server filter option
#                 0 : no filter (default)
#                 1 : only filter hosts specified in URLKEY
#                 2 : filter all hosts
#   SVREXCEPTION  : specify a host not to filter
#   SVRFILTERERR  : upon filtering
#                 0 : don't display an error page (default)
#                 1 : display an error page
#                 2 : error logging only with no actual ofiltering
#   SVRFILTERSTR  : string to substitute upon server filtering
#---------------------------------------------------------------------------
#GETFILTER=SCRIPT
#GETEXCEPTION=Name1
#GETFILTERERR=0
#GETFILTER_LOG_FLG=0
#POSTFILTER=SCRIPT
#POSTEXCEPTION=Name1
#POSTFILTERERR=0
#POSTFILTER_LOG_FLG=0
#HTMLFILTER=SCRIPT
#HTMLFILTERERR=0
#SVRFILTER=0
#SVREXCEPTION=http://www.svr.com
#SVRFILTERERR=0
#SVRFILTERSTR=BadHostName
#---------------------------------------------------------------------------
#  [ Network Connection Info ]
#   RETRYCNTW      : number of retries allowed for backend web server
#                connection (default: 10)
#   RETRYTMW       : time of retry intervals at the connection failures to
#                backend web servers (default: 3sec)
#   TIMEOUT        : the total time the forwarder will allow to receive a
#                response from a backend web server (default: 180sec)
#   CLOSETIME      : the total time the forwarder will allow before closing
#                 a connection with a backend web server
#                 (default: if not specified, set to the value of TIMEOUT)
#   BUFFER        : buffer flag
#                 0 : no buffer
#                 1 : buffer (default)
#   LASTMOD_HEADER : Last-Modified header switch
#                 0 : send (default)
#                 1 : don't send
#   CENCODE       : Content-encoding switch
#                 0 : ignore (default)
#                 1 : allow
#   RECV_ZERO_FLG  : receive data 0 bytes switch
#                 0 : error
#                 1 : continue (default)
#   FO_SEND       : send failover switch
#                 0 : error
#                 1 : failover (default)
#   FO_RECV       : receive failover switch
#                 0 : error
#                 1 : failover (default)
#   FO_NODATA      : received no data failover switch
#                 0 : error(default)
#                 1 : failover
#-----------------------------------------------------------------------------
RETRYCNTW=10
RETRYTMW=3
TIMEOUT=180
CLOSETIME=3
BUFFER=0
LASTMOD_HEADER=0
CENCODE=0
RECV_ZERO_FLG=1
#FO_SEND=1
#FO_RECV=1
#FO_NODATA=1

#-----------------------------------------------------------------------------
#  [ SSL Cipher Info ]
#   SSL_CIPHER_SUITE : chipher list which the permitted negotiate
#-----------------------------------------------------------------------------
#SSL_CIPHER_SUITE=RC4+RSA:-HIGH

#-----------------------------------------------------------------------------
#  [ Automatic Form Certification Info ]
#   FORM_FILE      : form certification configuration file
#                   FORM_FILE=[FormGroup],[path]
#   FORM_METHOD    : form transmitting method
#                   FORM_METHOD=[FormGroup],[GET or POST]
#   FORM_SEND      : form transmission place path
#                   FORM_SEND=[FormGroup],[path]
#   FORM_URL       : path which performs automatic form certification
#                   FORM_URL=[FormGroup],[path]
#   FORM_KEY       : the keyword of the contents which perform automatic
#                 form certification
#                   FORM_KEY=[FormGroup],[keyword]
#   FORM_HTML      : HTML used by the indirect transmitting system
#                   FORM_HTML=[FormGroup],[path]
#   FORM_DATA_STR  : transmission of string data
#                   FORM_DATA_STR=[FormGroup],[method],[name],[value]
#   FORM_DATA_USR  : transmission of user data
#                   FORM_DATA_USR=[FormGroup],[method],[name],[data name]
#    FORM_DATA_PAGE : transmission of contents data
#                   FORM_DATA_PAGE=[FormGroup],[method],[name],[data name]
#    FORM_KEY_EXCEPTION : a page with the keyword should be excluded
#                     FORM_KEY_EXCEPTION=[FormGroup],[keyword]
#    FORM_DATA_PAGE_REF : reference treatment flag to be replaced
#                     with the entity or not
#                     0 : do not replace (default)
#                     1 : replace
#------------------------------------------------------------------------------
#FORM_FILE=FORMGRP,./form.conf
```

3.7 Authentication Module configuration files

These are the configuration values of the Authentication Module configuration files used in the sample. The portions of the access control files other than the bold, underlined portions are configured when installed.

3.7.1 Authentication Module configuration file (cert.conf)

ORACLE edition

```
#------------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.conf $ $Revision: 12 $ $Date: 10/08/13 18:52 $
#------------------------------------------------------------------------------
#------------------------------------------------------------------------------
#  [ Log File Info ]
#    ALEVEL      : access log level
#              0 : no output
#              1 : fatal messages only (default)
#              2 : fatal and warning messages
#              3 : fatal, warning and information messages
#    ELEVEL      : error log level
#              0 : no output
#              1 : fatal messages only (default)
#              2 : fatal and warning messages
#              3 : fatal, warning and information messages
#    ACCESS      : access log file location
#              (default: /opt/icewall-sso/logs/cert.log)
#    ERROR       : error log file location
#              (default: /opt/icewall-sso/logs/certerr.log)
#    TRACE       : trace log file location
#    CATALOG     : message catalog file location
#    LOGINFO     : output ICP client information.
#              0 : no output (default)
#              1 : IP Address.
#              2 : IP Address and AGENT ID.
#    LOGPERF     : output performance log
#              0 : no output (default)(if PERFORMANCE=log default to 1)
#              1 : output
#    TRANSID     : output of Transaction IDs into log files
#              0 : no output (default)
#              1 : output
#    PERFORMANCE : performance log file location
#              (default: access log file location)
#    INFORMATION : information log file location
#              (default: access log file location)
#------------------------------------------------------------------------------
ALEVEL=1
```

```
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/cert.log
ERROR=/opt/icewall-sso/logs/certerr.log
#TRACE=/opt/icewall-sso/logs/certtrc.log
CATALOG=/opt/icewall-sso/messages/C/icewall_certd.cat
LOGINFO=0
LOGPERF=0
TRANSID=1
#PERFORMANCE=/opt/icewall-sso/logs/certperf.log
#INFORMATION=/opt/icewall-sso/logs/certinfo.log

#----------------------------------------------------------------------------
#  [ Access Control File Info ]
#   GROUP      : group info file location
#              (default: /opt/icewall-sso/certd/config/cert.grp)
#   ACL        : access control list file location
#              (default: /opt/icewall-sso/certd/config/cert.acl)
#   ACLREQUEST : request control list file location
#              (default: none)
#----------------------------------------------------------------------------
GROUP=/opt/icewall-sso/certd/config/cert.grp
ACL=/opt/icewall-sso/certd/config/cert.acl
#ACLREQUEST=/opt/icewall-sso/certd/config/request.acl

#----------------------------------------------------------------------------
#  [ Network Parameter Info ]
#   PORT           : certification module port no. (default: 14142)
#   IPV6LISTEN     : IP version of the requests that a certification module
#                  receives
#                  0 : IPv4 only (default)
#                  1 : IPv6 only
#                  2 : Both IPv4 and IPv6
#   HTTPPORT       : port number to receive HTTP based ICP2.0 requests
#   HTTPECHOHEADER : add request header, received from web clients, to
#                  response header ( HTTP based ICP2.0 resquests only )
#                  0 : not add (default)
#                  1 : add
#----------------------------------------------------------------------------
PORT=14142
#IPV6LISTEN=0
#HTTPPORT=8080
#HTTPECHOHEADER=0

#----------------------------------------------------------------------------
#  [ Session Control Info ]
#   COOKIERETRY   : cookie create retry count(default: 10)
#   COOKIETIME    : cookie expiration time (default: 60minutes)
#   COOKIEEXP     : cookie expiration switch
#                 0 : OFF (default)
#                 1 : ON (if LOMETHOD=1 defaults to 0)
#   LOMETHOD      : count session expiration time
#                 0 : from login (default)
#                 1 : from last access
#   DUPLOGIN      : allow duplicate login
#                 0 : disallow (default)
#                 1 : allow
#   DUPKIND       : duplicate login method
#                 0 : force login (default)
#                 1 : display force-login page
#   PARALOGIN     : allow/disallow a user to login again with a userid and
#                 a password ,who has previously logged into thesystem with
#                 a client certificate
#              0 : disallow (default)
#              1 : allow
#   ACCCTRLFLG    : use check and userid check of a client certificate
#              0 : check for using client certificate, and login userid
#                 (default)
#              1 : check for using client certificate only
#              2 : no check
#   SESSIONIDLEN  : byte length of the session ID a certification module
#              generates (default: 32 byte length)
#   CERTUNIQUEKEY : unique key to identify group of certification modules
#              (default: 0)
#-----------------------------------------------------------------------------
COOKIERETRY=10
COOKIETIME=60
#COOKIEEXP=1
LOMETHOD=1
DUPLOGIN=1
#PARALOGIN=0
#ACCCTRLFLG=0
#SESSIONIDLEN=32
#CERTUNIQUEKEY=

#-----------------------------------------------------------------------------
#  [ Password Control Info ]
#   PWDLOGINHASH : a password hash method at the time of the login :
#             (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#             (default: AUTO-PLAIN)
#   PWDCHGHASH   : a password hash method at the time of the password change :
#             (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#             (default: AUTO-PLAIN)
#   PWDMINLEN    : minimum character length of a new password at the time of
#             the password change (default: 3)
#   PWDMAXLEN    : maximum character length of a new password at the time of
#             the password change (default: 6)
#   PWDALPHANUM  : combination of the character set available as a password
#             (0-13)(default: 1)
#   PWDEXPIRE    : the number of days which the password expires (default: 72)
#   PWDSAMEPASS  : use of password identical to user id
#             0 : accepted
#             1 : not accepted (default)
#   LOCKCOUNT    : maximum number of password retries allowed (default: 0)
#   PWDEXPCHK    : password expiration check switch
#             0 : OFF (default)
#             1 : ON
#   PWDHISCHK    : password history check switch
#             0 : OFF (default)
#             1 : ON
#   PWDHISCNT    : password history count (1-20) (default: 1)
#   PWDFORBID    : forbidden password file location
#             (default: /opt/icewall-sso/certd/config/pwdforbid.conf)
#   PWDEXPWARN   : password expiration warning day check (0-365)
#             (default: 0)
#-----------------------------------------------------------------------------
#PWDLOGINHASH=AUTO-PLAIN
#PWDCHGHASH=AUTO-PLAIN
PWDMINLEN=3
PWDMAXLEN=6
PWDALPHANUM=0
PWDEXPIRE=72
PWDSAMEPASS=0
LOCKCOUNT=5
PWDEXPCHK=1
```

```
PWDHISCHK=1
PWDHISCNT=3
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDEXPWARN=0

#-----------------------------------------------------------------------------
#  [ Certification Database Control Info ]
#    DBHOST        : oracle network client name
#    DBUID         : userid to use for accessing the user authentication table
#    DBPWD         : password to use for accessing the user authentication
#                table
#    DBTBL         : user authentication table name
#    DBATTR        : database attribute file location
#                (default: /opt/icewall-sso/certd/config/dbattr.conf)
#    DBEXATTR      : extra columns to use for environment variables
#    DBCRYPTOTYPE   : a hash method used for decryption of the target column
#                data(0-3) (default: 0)
#    DBIWCRYPTOSEED : a seed value for decoding to be passed to the
#                certification DB encryption standard library
#    DBCRYPTOATTR   : target column names to be decrypted
#-----------------------------------------------------------------------------
DBHOST=ORCL
DBUID=scott
DBPWD=tiger
DBTBL=icewalltest
DBATTR=/opt/icewall-sso/certd/config/dbattr.conf
#DBEXATTR=PASSWD1,PASSWD2
#DBCRYPTOTYPE=
#DBIWCRYPTOSEED=
#DBCRYPTOATTR=

#-----------------------------------------------------------------------------
#  [ Access Log Database Control Info ]
#    LOGDBTBL     : login/logout history table name
#    LOGDBATTR    : login/logout history table attribute file location
#    LOGDBSEQNAME : login/logout history table sequence object name
#-----------------------------------------------------------------------------
#LOGDBTBL=history
#LOGDBATTR=/opt/icewall-sso/certd/config/logdbattr.conf
#LOGDBSEQNAME=WEB_REVIEW_SEQ

#-----------------------------------------------------------------------------
#  [ Reference Database Control Info ]
#    REFTBL  : user reference table name
#    REFATTR : user reference table attribute
#    REFUID  : column to use for userid in the reference table
#-----------------------------------------------------------------------------
#REFTBL=icewalltest
REFATTR=PASSWD1,PASSWD2
REFUID=USERID

#-----------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#    MAXREQTHREAD : maximum number of request threads (default: 10)
#    ACCTHREAD    : the number of access threads, which are assigned to the
#               requests that does not need DB connection (default: 0)
#    REQQUESIZE   : request queue size (default: 20)
#    MAXDBCONNECT : maximum number of database connection threads (default: 2)
#    DBQUESIZE    : Size of data queue, in which DB update data
#               for certification DB is temporarily queued
#               in user logout processing. (default: same as CACHE)
#               Specifying LOGINSTAT parameter in dbattr.conf
#              is required. NO change from default value is recommended.
#   LOGDBQUESIZE : Size of data queue, in which DB update data
#              for audit log table is temporarily queued in
#              user logout processing. (default: same as 50% of CACHE)
#              It is required that Audit log output function works.
#              NO change from default value is recommended.
#   LOGBUFSIZE   : access and error log buffer size (default: 1000)
#   CACHE        : maximum number of login user (default: 10)
#   MAXLOGINUSER : the number of the users who can log in
#   RECVWAITTIME : request recv wait time (1-60) (default: 3sec)
#   THREADSTACKSIZE : thread stack size (default: 256Kbytes)
#   LOGMULTITHREAD  : multithreading on log generation
#                0 : single-thread mode (default)
#                1 : multi-thread mode
#-----------------------------------------------------------------------------
MAXREQTHREAD=10
#ACCTHREAD=0
REQQUESIZE=20
MAXDBCONNECT=2
LOGBUFSIZE=1000
CACHE=100
#MAXLOGINUSER=
RECVWAITTIME=3
THREADSTACKSIZE=256
LOGMULTITHREAD=1

#-----------------------------------------------------------------------------
#  [ Replication Control Info ]
#   CERT          : [hostname:port no. ] replication target
#   CERTREPTYPE     : replication type
#                0 : primary side
#                1 : secondary side
#   RETRYCNTC      : number of retries allowd for the replication server
#                connection (default: 10)
#   RETRYTMC       : time of retry intervals at the connection failure to
#                the replication server (default: 3sec)
#   LIVETIMER      : replication interval after detecting that the
#                replication target has gone down (default: 60sec)
#   HEALTHTIMER     : replication interval (secondary side only)
#                (default: 5sec)
#   HEALTHCNT      : replication count (secondary side only) (default: 12)
#   DOWNLOADCONFFLG : download the configuration information from
#                certification module of replication target at time of
#                startup
#                0 : not download
#                1 : download (default)
#   FAILBACK       : add alive information of master certification module to
#                ICP 2.0 response headers which the replica certification
#                module returns (0-1) (default: 0)
#-----------------------------------------------------------------------------
#CERT=
#CERTREPTYPE=
#RETRYCNTC=5
#RETRYTMC=3
#LIVETIMER=30
#HEALTHTIMER=5
#HEALTHCNT=12
#DOWNLOADCONFFLG=1
#FAILBACK=0

#-----------------------------------------------------------------------------
#  [ Replication Performance Tuning Info ]
#   MAXREPTHREAD : maximum number of replication threads (default: 5)
#   REPQUESIZE   : replication queue size (default: 1000)
#--------------------------------------------------------------------------
#MAXREPTHREAD=5
#REPQUESIZE=1000
```

LDAP edition

```
#--------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.conf $ $Revision: 14 $ $Date: 10/08/13 18:51 $
#--------------------------------------------------------------------------
#--------------------------------------------------------------------------
#  [ Log File Info ]
#   ALEVEL      : access log level
#               0 : no output
#               1 : fatal messages only (default)
#               2 : fatal and warning messages
#               3 : fatal, warning and information messages
#   ELEVEL      : error log level
#               0 : no output
#               1 : fatal messages only (default)
#               2 : fatal and warning messages
#               3 : fatal, warning and information messages
#   ACCESS      : access log file location
#               (default: /opt/icewall-sso/logs/cert.log)
#   ERROR       : error log file location
#               (default: /opt/icewall-sso/logs/certerr.log)
#   TRACE       : trace log file location
#   CATALOG     : message catalog file location
#   LOGINFO     : output ICP client information.
#               0 : no output (default)
#               1 : IP Address.
#               2 : IP Address and AGENT ID.
#   LOGPERF     : output performance log
#               0 : no output (default)(if PERFORMANCE=log default to 1)
#               1 : output
#   TRANSID     : output of Transaction IDs into log files
#               0 : no output (default)
#               1 : output
#   PERFORMANCE : performance log file location
#               (default: access log file location)
#   INFORMATION : information log file location
#               (default: access log file location)
#--------------------------------------------------------------------------
ALEVEL=1
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/cert.log
ERROR=/opt/icewall-sso/logs/certerr.log
#TRACE=/opt/icewall-sso/logs/certtrc.log
CATALOG=/opt/icewall-sso/messages/C/icewall_certd.cat
LOGINFO=0
LOGPERF=0
TRANSID=1
#PERFORMANCE=/opt/icewall-sso/logs/certperf.log
#INFORMATION=/opt/icewall-sso/logs/certinfo.log

#--------------------------------------------------------------------------
#  [ Access Control File Info ]
#   GROUP       : group info file location
#              (default: /opt/icewall-sso/certd/config/cert.grp)
#   ACL        : access control list file location
#              (default: /opt/icewall-sso/certd/config/cert.acl)
#   ACLREQUEST : request control list file location
#              (default: none)
#------------------------------------------------------------------------------
GROUP=/opt/icewall-sso/certd/config/cert.grp
ACL=/opt/icewall-sso/certd/config/cert.acl
#ACLREQUEST=/opt/icewall-sso/certd/config/request.acl

#------------------------------------------------------------------------------
#  [ Network Parameter Info ]
#   PORT          : certification module port no. (default: 14142)
#   IPV6LISTEN     : IP version of the requests that a certification module
#                  receives
#                  0 : IPv4 only (default)
#                  1 : IPv6 only
#                  2 : Both IPv4 and IPv6
#   HTTPPORT       : port number to receive HTTP based ICP2.0 requests
#   HTTPECHOHEADER : add request header, received from web clients, to
#                  response header ( HTTP based ICP2.0 resquests only )
#                  0 : not add (default)
#                  1 : add
#------------------------------------------------------------------------------
PORT=14142
#IPV6LISTEN=0
#HTTPPORT=8080
#HTTPECHOHEADER=0

#------------------------------------------------------------------------------
#  [ Session Control Info ]
#   COOKIERETRY   : cookie create retry count(default: 10)
#   COOKIETIME    : cookie expiration time (default: 60minutes)
#   COOKIEEXP     : cookie expiration switch
#                 0 : OFF (default)
#                 1 : ON (if LOMETHOD=1 defaults to 0)
#   LOMETHOD      : count session expiration time
#                 0 : from login (default)
#                 1 : from last access
#   DUPLOGIN      : allow duplicate login
#                 0 : disallow (default)
#                 1 : allow
#   DUPKIND       : duplicate login method
#                 0 : force login (default)
#                 1 : display force-login page
#   PARALOGIN     : allow/disallow a user to login again with a userid and
#                 a password ,who has previously logged into thesystem with
#                 a client certificate
#                 0 : disallow (default)
#                 1 : allow
#   ACCCTRLFLG    : use check and userid check of a client certificate
#                 0 : check for using client certificate, and login userid
#                     (default)
#                 1 : check for using client certificate only
#                 2 : no check
#   SESSIONIDLEN  : byte length of the session ID a certification module
#                 generates (default: 32 byte length)
#   CERTUNIQUEKEY : unique key to identify group of certification modules
#                 (default: 0)
#------------------------------------------------------------------------------
COOKIERETRY=10
COOKIETIME=60
#COOKIEEXP=1
```

```
LOMETHOD=1
DUPLOGIN=1
#DUPKIND=0
#PARALOGIN=0
#ACCCTRLFLG=0
#SESSIONIDLEN=32
#CERTUNIQUEKEY=

#-----------------------------------------------------------------------------
#  [ Password Control Info ]
#    PWDLOGINHASH : a password hash method at the time of the login :
#                (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#                (default: AUTO-PLAIN)
#    PWDCHGHASH   : a password hash method at the time of the password change :
#                (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#                (default: AUTO-PLAIN)
#    PWDMINLEN    : minimum character length of a new password at the time of
#                the password change (default: 3)
#    PWDMAXLEN    : maximum character length of a new password at the time of
#                the password change (default: 6)
#    PWDALPHANUM  : combination of the character set available as a password
#                (0-13)(default: 1)
#    PWDEXPIRE    : the number of days which the password expires (default: 72)
#    PWDSAMEPASS  : use of password identical to user id
#                0 : accepted
#                1 : not accepted (default)
#    LOCKCOUNT    : maximum number of password retries allowed (default: 0)
#    PWDEXPCHK    : password expiration check switch
#                0 : OFF (default)
#                1 : ON
#    PWDHISCHK    : password history check switch
#                0 : OFF (default)
#                1 : ON
#    PWDHISCNT    : password history count (1-20) (default: 1)
#    PWDFORBID    : forbidden password file location
#                (default: /opt/icewall-sso/certd/config/pwdforbid.conf)
#    PWDEXPWARN   : password expiration warning day check (0-365)
#                (default: 0)
#-----------------------------------------------------------------------------
#PWDLOGINHASH=AUTO-PLAIN
#PWDCHGHASH=AUTO-PLAIN
PWDMINLEN=3
PWDMAXLEN=6
PWDALPHANUM=0
PWDEXPIRE=72
PWDSAMEPASS=0
LOCKCOUNT=5
PWDEXPCHK=1
PWDHISCHK=1
PWDHISCNT=3
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDEXPWARN=0

#-----------------------------------------------------------------------------
#  [ Certification Database Control Info ]
#    DBHOST          : ldap server host name
#    DBUID           : userid to use for accessing the user authentication
#                table
#    DBPWD           : password to use for accessing the user authentication
#                table
#    DBTBL           : user authentication table name
#    DBATTR          : database attribute file location
#                 (default: /opt/icewall-sso/certd/config/dbattr.conf)
#    DBEXATTR          : extra columns to use for environment variables
#    DBCRYPTOTYPE      : a hash method used for decryption of the target column
#                 data(0-3) (default: 0)
#    DBIWCRYPTOSEED    : a seed value for decoding to be passed to the
#                 certification DB encryption standard library
#    DBCRYPTOATTR      : target column names to be decrypted
#    LDAPBIND          : use LDAP bind operation mode
#                 0 : OFF (default)
#                 1 : ON
#    LDAPPCHG          : use LDAP password change operation mode
#                 0 : OFF
#                 1 : ON (default)
#    LDAPLANG          : use code set conversion mode
#                 0 : OFF
#                 1 : ON (default)
#    LDAPSSL           : specify whether to use SSL in order to communicate
#                 with the ldap server
#                 0 : OFF (default)
#                 1 : ON
#    LDAPCACERT        : location of the PEM-encoded X.509 CA certificate file
#    LDAPVERIFYSVRCERT : specify whether to verify the CA certificate
#                 0 : OFF
#                 1 : ON (default)
#    LDAPCIPHERSUITE   : cipher preference for SSL communication with the LDAP
#                 server
#    LDAPSSLBIND       : specify whether to use SSL at the time of LDAP bind
#                 0 : OFF
#                 1 : ON (default)
#    LDAPMULTIVAL      : specify whether to obtain multiple values from each
#                 LDAP attribute
#                 0 : OFF (default)
#                 1 : ON
#    LDAPREFERRAL      : Enable LDAP referral
#                 0 : OFF
#                 1 : ON (default)
#-----------------------------------------------------------------------------
DBHOST=localhost:389
DBUID=uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot
DBPWD=passwd
DBTBL=o=Alias.com
DBATTR=/opt/icewall-sso/certd/config/dbattr.conf
#DBEXATTR=registeredAddress,teletexTerminalIdentifier
#DBCRYPTOTYPE=
#DBIWCRYPTOSEED=
#DBCRYPTOATTR=
LDAPBIND=0
LDAPPCHG=1
LDAPLANG=1
LDAPSSL=0
LDAPCACERT=/opt/icewall-sso/certd/config/cacert.pem
LDAPVERIFYSVRCERT=1
#LDAPCIPHERSUITE=
LDAPSSLBIND=1
LDAPMULTIVAL=0
LDAPREFERRAL=1

#-----------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#    MAXREQTHREAD : maximum number of request threads (default: 10)
#    ACCTHREAD    : the number of access threads, which are assigned to the
#               requests that does not need DB connection (default: 0)
#    REQQUESIZE   : request queue size (default: 20)
#    MAXDBCONNECT : maximum number of database connection threads (default: 2)
#    DBQUESIZE    : Size of data queue, in which DB update data
#                for certification DB is temporarily queued
#                in user logout processing. (default: same as CACHE)
#                Specifying LOGINSTAT parameter in dbattr.conf
#                is required. NO change from default value is recommended.
#    LOGBUFSIZE   : access and error log buffer size (default: 1000)
#    CACHE        : maximum number of login user (default: 10)
#    MAXLOGINUSER : the number of the users who can log in
#    RECVWAITTIME : request recv wait time (1-60) (default: 3sec)
#    THREADSTACKSIZE : thread stack size (default: 256Kbytes)
#    LOGMULTITHREAD  : multithreading on log generation
#                  0 : single-thread mode (default)
#                  1 : multi-thread mode
#-----------------------------------------------------------------------------
MAXREQTHREAD=10
#ACCTHREAD=0
REQQUESIZE=20
MAXDBCONNECT=2
LOGBUFSIZE=1000
CACHE=100
#MAXLOGINUSER=
RECVWAITTIME=3
THREADSTACKSIZE=256
LOGMULTITHREAD=1

#-----------------------------------------------------------------------------
#  [ Replication Control Info ]
#    CERT            : [hostname:port no. ] replication target
#    CERTREPTYPE     : replication type
#                  0 : primary side
#                  1 : secondary side
#    RETRYCNTC       : number of retries allowd for the replication server
#                  connection (default: 10)
#    RETRYTMC        : time of retry intervals at the connection failure to
#                  the replication server (default: 3sec)
#    LIVETIMER       : replication interval after detecting that the
#                  replication target has gone down (default: 60sec)
#    HEALTHTIMER     : replication interval (secondary side only)
#                  (default: 5sec)
#    HEALTHCNT       : replication count (secondary side only) (default: 12)
#    DOWNLOADCONFFLG : download the configuration information from
#                  certification module of replication target at time of
#                  startup
#                  0 : not download
#                  1 : download (default)
#    FAILBACK        : add alive information of master certification module to
#                  ICP 2.0 response headers which the replica certification
#                  module returns (0-1) (default: 0)
#-----------------------------------------------------------------------------
#CERT=
#CERTREPTYPE=
#RETRYCNTC=5
#RETRYTMC=3
#LIVETIMER=30
#HEALTHTIMER=5
#HEALTHCNT=12
#DOWNLOADCONFFLG=1
#FAILBACK=0

#-----------------------------------------------------------------------------
```

```
#  [ Replication Performance Tuning Info ]
#    MAXREPTHREAD : maximum number of replication threads (default: 5)

#    REPQUESIZE   : replication queue size (default: 1000)
#-----------------------------------------------------------------------------
#MAXREPTHREAD=5
#REPQUESIZE=1000
```

OpenLDAP edition

```
#-----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.conf $ $Revision: 8 $ $Date: 10/08/13 18:52 $
#-----------------------------------------------------------------------------
#-----------------------------------------------------------------------------
#  [ Log File Info ]
#    ALEVEL      : access log level
#              0 : no output
#              1 : fatal messages only (default)
#              2 : fatal and warning messages
#              3 : fatal, warning and information messages
#    ELEVEL      : error log level
#              0 : no output
#              1 : fatal messages only (default)
#              2 : fatal and warning messages
#              3 : fatal, warning and information messages
#    ACCESS      : access log file location
#              (default: /opt/icewall-sso/logs/cert.log)
#    ERROR       : error log file location
#              (default: /opt/icewall-sso/logs/certerr.log)
#    TRACE       : trace log file location
#    CATALOG     : message catalog file location
#    LOGINFO     : output ICP client information.
#              0 : no output (default)
#              1 : IP Address.
#              2 : IP Address and AGENT ID.
#    LOGPERF     : output performance log
#              0 : no output (default)(if PERFORMANCE=log default to 1)
#              1 : output
#    TRANSID     : output of Transaction IDs into log files
#              0 : no output (default)
#              1 : output
#    PERFORMANCE : performance log file location
#              (default: access log file location)
#    INFORMATION : information log file location
#              (default: access log file location)
#-----------------------------------------------------------------------------
ALEVEL=1
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/cert.log
ERROR=/opt/icewall-sso/logs/certerr.log
#TRACE=/opt/icewall-sso/logs/certtrc.log
CATALOG=/opt/icewall-sso/messages/C/icewall_certd.cat
LOGINFO=0
LOGPERF=0
TRANSID=1
#PERFORMANCE=/opt/icewall-sso/logs/certperf.log
#INFORMATION=/opt/icewall-sso/logs/certinfo.log
#-----------------------------------------------------------------------------
#  [ Access Control File Info ]
#    GROUP       : group info file location
#             (default: /opt/icewall-sso/certd/config/cert.grp)
#    ACL         : access control list file location
#             (default: /opt/icewall-sso/certd/config/cert.acl)
#    ACLREQUEST : request control list file location
#             (default: none)
#---------------------------------------------------------------------------
GROUP=/opt/icewall-sso/certd/config/cert.grp
ACL=/opt/icewall-sso/certd/config/cert.acl
#ACLREQUEST=/opt/icewall-sso/certd/config/request.acl

#---------------------------------------------------------------------------
#  [ Network Parameter Info ]
#    PORT          : certification module port no. (default: 14142)
#    IPV6LISTEN     : IP version of the requests that a certification module
#                 receives
#                 0 : IPv4 only (default)
#                 1 : IPv6 only
#                 2 : Both IPv4 and IPv6
#    HTTPPORT       : port number to receive HTTP based ICP2.0 requests
#    HTTPECHOHEADER : add request header, received from web clients, to
#                 response header ( HTTP based ICP2.0 resquests only )
#                 0 : not add (default)
#                 1 : add
#---------------------------------------------------------------------------
PORT=14142
#IPV6LISTEN=0
#HTTPPORT=8080
#HTTPECHOHEADER=0

#---------------------------------------------------------------------------
#  [ Session Control Info ]
#    COOKIERETRY   : cookie create retry count(default: 10)
#    COOKIETIME    : cookie expiration time (default: 60minutes)
#    COOKIEEXP     : cookie expiration switch
#               0 : OFF (default)
#               1 : ON (if LOMETHOD=1 defaults to 0)
#    LOMETHOD      : count session expiration time
#               0 : from login (default)
#               1 : from last access
#    DUPLOGIN      : allow duplicate login
#               0 : disallow (default)
#               1 : allow
#    DUPKIND       : duplicate login method
#               0 : force login (default)
#               1 : display force-login page
#    PARALOGIN     : allow/disallow a user to login again with a userid and
#               a password ,who has previously logged into thesystem with
#               a client certificate
#               0 : disallow (default)
#               1 : allow
#    ACCCTRLFLG    : use check and userid check of a client certificate
#               0 : check for using client certificate, and login userid
#                   (default)
#               1 : check for using client certificate only
#               2 : no check
#    SESSIONIDLEN  : byte length of the session ID a certification module
#               generates (default: 32 byte length)
#    CERTUNIQUEKEY : unique key to identify group of certification modules
#               (default: 0)
#---------------------------------------------------------------------------
COOKIERETRY=10
COOKIETIME=60
#COOKIEEXP=1
LOMETHOD=1
```

```
DUPLOGIN=1
#DUPKIND=0
#PARALOGIN=0
#ACCCTRLFLG=0
#SESSIONIDLEN=32
#CERTUNIQUEKEY=

#-----------------------------------------------------------------------------
#  [ Password Control Info ]
#    PWDLOGINHASH : a password hash method at the time of the login :
#                (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#                (default: AUTO-PLAIN)
#    PWDCHGHASH   : a password hash method at the time of the password change :
#                (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#                (default: AUTO-PLAIN)
#    PWDMINLEN    : minimum character length of a new password at the time of
#                the password change (default: 3)
#    PWDMAXLEN    : maximum character length of a new password at the time of
#                the password change (default: 6)
#    PWDALPHANUM  : combination of the character set available as a password
#                (0-13)(default: 1)
#    PWDEXPIRE    : the number of days which the password expires (default: 72)
#    PWDSAMEPASS  : use of password identical to user id
#                0 : accepted
#                1 : not accepted (default)
#    LOCKCOUNT    : maximum number of password retries allowed (default: 0)
#    PWDEXPCHK    : password expiration check switch
#                0 : OFF (default)
#                1 : ON
#    PWDHISCHK    : password history check switch
#                0 : OFF (default)
#                1 : ON
#    PWDHISCNT    : password history count (1-20) (default: 1)
#    PWDFORBID    : forbidden password file location
#                (default: /opt/icewall-sso/certd/config/pwdforbid.conf)
#    PWDEXPWARN   : password expiration warning day check (0-365)
#                (default: 0)
#-----------------------------------------------------------------------------
#PWDLOGINHASH=AUTO-PLAIN
#PWDCHGHASH=AUTO-PLAIN
PWDMINLEN=3
PWDMAXLEN=6
PWDALPHANUM=0
PWDEXPIRE=72
PWDSAMEPASS=0
LOCKCOUNT=5
PWDEXPCHK=1
PWDHISCHK=1
PWDHISCNT=3
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDEXPWARN=0

#-----------------------------------------------------------------------------
#  [ Certification Database Control Info ]
#    DBHOST          : ldap server host name
#    DBUID          : userid to use for accessing the user authentication
#                   table
#    DBPWD           : password to use for accessing the user authentication
#                   table
#    DBTBL          : user authentication table name
#    DBATTR          : database attribute file location
#                   (default: /opt/icewall-sso/certd/config/dbattr.conf)
#   DBEXATTR          : extra columns to use for environment variables
#   DBCRYPTOTYPE      : a hash method used for decryption of the target column
#                 data(0-3) (default: 0)
#   DBIWCRYPTOSEED    : a seed value for decoding to be passed to the
#                 certification DB encryption standard library
#   DBCRYPTOATTR      : target column names to be decrypted
#   LDAPBIND          : use LDAP bind operation mode
#                 0 : OFF (default)
#                 1 : ON
#   LDAPPCHG          : use LDAP password change operation mode
#                 0 : OFF
#                 1 : ON (default)
#   LDAPLANG          : use code set conversion mode
#                 0 : OFF
#                 1 : ON (default)
#   LDAPSSL           : specify whether to use SSL in order to communicate
#                 with the ldap server
#                 0 : OFF (default)
#                 1 : ON
#   LDAPCACERT        : location of the PEM-encoded X.509 CA certificate file
#   LDAPVERIFYSVRCERT : specify whether to verify the CA certificate
#                 0 : OFF
#                 1 : ON (default)
#   LDAPCIPHERSUITE   : cipher preference for SSL communication with the LDAP
#                 server
#   LDAPSSLBIND       : specify whether to use SSL at the time of LDAP bind
#                 0 : OFF
#                 1 : ON (default)
#   LDAPMULTIVAL      : specify whether to obtain multiple values from each
#                 LDAP attribute
#                 0 : OFF (default)
#                 1 : ON
#   LDAPREFERRAL      : Enable LDAP referral
#                 0 : OFF
#                 1 : ON (default)
#---------------------------------------------------------------------------
DBHOST=openldapsvr:389
DBUID=cn=Manager,dc=jpn.dc=hp,dc=com
DBPWD=password
DBTBL=ou=icewalltest,dc=jpn,dc=hp,dc=com
DBATTR=/opt/icewall-sso/certd/config/dbattr.conf
#DBEXATTR=registeredAddress,teletexTerminalIdentifier
#DBCRYPTOTYPE=
#DBIWCRYPTOSEED=
#DBCRYPTOATTR=
LDAPBIND=0
LDAPPCHG=1
LDAPLANG=1
LDAPSSL=0
LDAPCACERT=/opt/icewall-sso/certd/config/cacert.pem
LDAPVERIFYSVRCERT=1
#LDAPCIPHERSUITE=
LDAPSSLBIND=1
LDAPMULTIVAL=0
LDAPREFERRAL=1

#---------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#   MAXREQTHREAD : maximum number of request threads (default: 10)
#   ACCTHREAD    : the number of access threads, which are assigned to the
#              requests that does not need DB connection (default: 0)
#   REQQUESIZE   : request queue size (default: 20)
#   MAXDBCONNECT : maximum number of database connection threads (default: 2)
#   DBQUESIZE    : Size of data queue, in which DB update data
#             for certification DB is temporarily queued
#             in user logout processing. (default: same as CACHE)
#             Specifying LOGINSTAT parameter in dbattr.conf
#             is required. NO change from default value is recommended.
#   LOGBUFSIZE   : access and error log buffer size (default: 1000)
#   CACHE        : maximum number of login user (default: 10)
#   MAXLOGINUSER : the number of the users who can log in
#   RECVWAITTIME : request recv wait time (1-60) (default: 3sec)
#   THREADSTACKSIZE : thread stack size (default: 256Kbytes)
#   LOGMULTITHREAD  : multithreading on log generation
#               0 : single-thread mode (default)
#               1 : multi-thread mode
#-----------------------------------------------------------------------------
MAXREQTHREAD=10
#ACCTHREAD=0
REQQUESIZE=20
MAXDBCONNECT=2
LOGBUFSIZE=1000
CACHE=100
#MAXLOGINUSER=
RECVWAITTIME=3
THREADSTACKSIZE=256
LOGMULTITHREAD=1

#-----------------------------------------------------------------------------
#  [ Replication Control Info ]
#   CERT            : [hostname:port no. ] replication target
#   CERTREPTYPE     : replication type
#               0 : primary side
#               1 : secondary side
#   RETRYCNTC       : number of retries allowd for the replication server
#               connection (default: 10)
#   RETRYTMC        : time of retry intervals at the connection failure to
#               the replication server (default: 3sec)
#   LIVETIMER       : replication interval after detecting that the
#               replication target has gone down (default: 60sec)
#   HEALTHTIMER     : replication interval (secondary side only)
#               (default: 5sec)
#   HEALTHCNT       : replication count (secondary side only) (default: 12)
#   DOWNLOADCONFFLG : download the configuration information from
#               certification module of replication target at time of
#               startup
#               0 : not download
#               1 : download (default)
#   FAILBACK        : add alive information of master certification module to
#               ICP 2.0 response headers which the replica certification
#               module returns (0-1) (default: 0)
#-----------------------------------------------------------------------------
#CERT=
#CERTREPTYPE=
#RETRYCNTC=5
#RETRYTMC=3
#LIVETIMER=30
#HEALTHTIMER=5
#HEALTHCNT=12
#DOWNLOADCONFFLG=1
#FAILBACK=0

#-----------------------------------------------------------------------------
#  [ Replication Performance Tuning Info ]
#    MAXREPTHREAD : maximum number of replication threads (default: 5)
#    REPQUESIZE   : replication queue size (default: 1000)
#--------------------------------------------------------------------------
#MAXREPTHREAD=5
#REPQUESIZE=1000
```

MSAD edition

```
#--------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.conf $ $Revision: 11 $ $Date: 10/08/13 18:51 $
#--------------------------------------------------------------------------
#--------------------------------------------------------------------------
#  [ Log File Info ]
#    ALEVEL      : access log level
#               0 : no output
#               1 : fatal messages only (default)
#               2 : fatal and warning messages
#               3 : fatal, warning and information messages
#    ELEVEL      : error log level
#               0 : no output
#               1 : fatal messages only (default)
#               2 : fatal and warning messages
#               3 : fatal, warning and information messages
#    ACCESS      : access log file location
#               (default: /opt/icewall-sso/logs/cert.log)
#    ERROR       : error log file location
#               (default: /opt/icewall-sso/logs/certerr.log)
#    TRACE       : trace log file location
#    CATALOG     : message catalog file location
#    LOGINFO     : output ICP client information.
#               0 : no output (default)
#               1 : IP Address.
#               2 : IP Address and AGENT ID.
#    LOGPERF     : output performance log
#               0 : no output (default)(if PERFORMANCE=log default to 1)
#               1 : output
#    TRANSID     : output of Transaction IDs into log files
#               0 : no output (default)
#               1 : output
#    PERFORMANCE : performance log file location
#               (default: access log file location)
#    INFORMATION : information log file location
#               (default: access log file location)
#--------------------------------------------------------------------------
ALEVEL=1
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/cert.log
ERROR=/opt/icewall-sso/logs/certerr.log
#TRACE=/opt/icewall-sso/logs/certtrc.log
CATALOG=/opt/icewall-sso/messages/C/icewall_certd.cat
LOGINFO=0
LOGPERF=0
TRANSID=1
#PERFORMANCE=/opt/icewall-sso/logs/certperf.log
#INFORMATION=/opt/icewall-sso/logs/certinfo.log

#--------------------------------------------------------------------------
#  [ Access Control File Info ]
#    GROUP           : group info file location
#                    (default: /opt/icewall-sso/certd/config/cert.grp)
#   ACL             : access control list file location
#                  (default: /opt/icewall-sso/certd/config/cert.acl)
#   ACLREQUEST      : request control list file location
#                  (default: none)
#   ADGROUP         : specify whether or not AD group information is added
#                  as an attribute of user information
#                  0 : OFF (default)
#                  1 : ON
#   ADGROUPDN       : DNs in which AD group information exists
#                  (default: DBTBL value)
#   ADGROUPINTERVAL  : time interval at which AD group information query
#                  is issued to an AD
#                  (default: 60seconds)
#   ADGROUPPRINAME   : attribute name for a Primary group name obtained from
#                  user's AD group information.
#                  (default: ADGROUP_PRIMARY)
#   ADGROUPPREFIX    : a prefix for an AD group name obtained from user's AD
#                  information
#                  (default: ADGROUP_)
#   ADGROUPMAXMEMBER : maximum number of the parent groups to be searched
#                  (default: 20)
#-----------------------------------------------------------------------------
GROUP=/opt/icewall-sso/certd/config/cert.grp
ACL=/opt/icewall-sso/certd/config/cert.acl
#ACLREQUEST=/opt/icewall-sso/certd/config/request.acl
ADGROUP=0
#ADGROUPDN=
ADGROUPINTERVAL=60
ADGROUPPRINAME=ADGROUP_PRIMARY
ADGROUPPREFIX=ADGROUP_
#ADGROUPMAXMEMBER=20

#-----------------------------------------------------------------------------
#  [ Network Parameter Info ]
#   PORT            : certification module port no. (default: 14142)
#   IPV6LISTEN      : IP version of the requests that a certification module
#                 receives
#                 0 : IPv4 only (default)
#                 1 : IPv6 only
#                 2 : Both IPv4 and IPv6
#   HTTPPORT        : port number to receive HTTP based ICP2.0 requests
#   HTTPECHOHEADER : add request header, received from web clients, to
#                 response header ( HTTP based ICP2.0 resquests only )
#                 0 : not add (default)
#                 1 : add
#-----------------------------------------------------------------------------
PORT=14142
#IPV6LISTEN=0
#HTTPPORT=8080
#HTTPECHOHEADER=0

#-----------------------------------------------------------------------------
#  [ Session Control Info ]
#   COOKIERETRY   : cookie create retry count(default: 10)
#   COOKIETIME    : cookie expiration time (default: 60minutes)
#   COOKIEEXP     : cookie expiration switch
#               0 : OFF (default)
#               1 : ON (if LOMETHOD=1 defaults to 0)
#   LOMETHOD      : count session expiration time
#               0 : from login (default)
#               1 : from last access
#   DUPLOGIN      : allow duplicate login
#              0 : disallow (default)
#              1 : allow
#   DUPKIND      : duplicate login method
#              0 : force login (default)
#              1 : display force-login page
#   PARALOGIN    : allow/disallow a user to login again with a userid and
#              a password ,who has previously logged into thesystem with
#              a client certificate
#              0 : disallow (default)
#              1 : allow
#   ACCCTRLFLG   : use check and userid check of a client certificate
#              0 : check for using client certificate, and login userid
#                 (default)
#              1 : check for using client certificate only
#              2 : no check
#   SESSIONIDLEN  : byte length of the session ID a certification module
#              generates (default: 32 byte length)
#   CERTUNIQUEKEY : unique key to identify group of certification modules
#              (default: 0)
#----------------------------------------------------------------------------
COOKIERETRY=10
COOKIETIME=60
#COOKIEEXP=1
LOMETHOD=1
DUPLOGIN=1
#DUPKIND=0
#PARALOGIN=0
#ACCCTRLFLG=0
#SESSIONIDLEN=32
#CERTUNIQUEKEY=

#----------------------------------------------------------------------------
#  [ Password Control Info ]
#   PWDLOGINHASH : a password hash method at the time of the login :
#             (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#             (default: AUTO-PLAIN)
#   PWDCHGHASH   : a password hash method at the time of the password change :
#             (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#             (default: AUTO-PLAIN)
#   PWDMINLEN    : minimum character length of a new password at the time of
#             the password change (default: 3)
#   PWDMAXLEN    : maximum character length of a new password at the time of
#             the password change (default: 6)
#   PWDALPHANUM  : combination of the character set available as a password
#             (0-13)(default: 1)
#   PWDEXPIRE    : the number of days which the password expires (default: 72)
#   PWDSAMEPASS  : use of password identical to user id
#             0 : accepted
#             1 : not accepted (default)
#   LOCKCOUNT    : maximum number of password retries allowed (default: 0)
#   PWDEXPCHK    : password expiration check switch
#             0 : OFF (default)
#             1 : ON
#   PWDHISCHK    : password history check switch
#             0 : OFF (default)
#             1 : ON
#   PWDHISCNT    : password history count (1-20) (default: 1)
#   PWDFORBID    : forbidden password file location
#             (default: /opt/icewall-sso/certd/config/pwdforbid.conf)
#   PWDEXPWARN   : password expiration warning day check (0-365)
#             (default: 0)
#----------------------------------------------------------------------------
```

```
PWDLOGINHASH=PLAIN
PWDCHGHASH=PLAIN
PWDMINLEN=3
PWDMAXLEN=6
PWDALPHANUM=0
PWDEXPIRE=72
PWDSAMEPASS=0
LOCKCOUNT=5
PWDEXPCHK=0
PWDHISCHK=0
PWDHISCNT=1
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDEXPWARN=0

#---------------------------------------------------------------------------
#  [ Certification Database Control Info ]
#   DBHOST          : msad server host name
#   DBUID           : userid to use for accessing the user authentication
#                   table
#   DBPWD           : password to use for accessing the user authentication
#                   table
#   DBTBL           : user authentication table name
#   DBATTR          : database attribute file location
#                   (default: /opt/icewall-sso/certd/config/dbattr.conf)
#   DBEXATTR        : extra columns to use for environment variables
#   DBCRYPTOTYPE    : a hash method used for decryption of the target column
#                   data(0-3) (default: 0)
#   DBIWCRYPTOSEED  : a seed value for decoding to be passed to the
#                   certification DB encryption standard library
#   DBCRYPTOATTR    : target column names to be decrypted
#   LDAPBIND        : use LDAP bind operation mode
#                   0 : OFF (default)
#                   1 : ON
#   LDAPPCHG        : use LDAP password change operation mode
#                   0 : OFF
#                   1 : ON (default)
#   LDAPLANG        : use code set conversion mode
#                   0 : OFF
#                   1 : ON (default)
#   LDAPSSL         : specify whether to use SSL in order to communicate
#                   with the MSAD server
#                   0 : OFF (default)
#                   1 : ON
#   LDAPCACERT      : location of the PEM-encoded X.509 CA certificate file
#   LDAPVERIFYSVRCERT : specify whether to verify the CA certificate
#                   0 : OFF
#                   1 : ON (default)
#   LDAPCIPHERSUITE  : cipher preference for SSL communication with the LDAP
#                   server
#   LDAPSSLBIND     : specify whether to use SSL at the time of LDAP bind
#                   0 : OFF
#                   1 : ON (default)
#   ADPCHG          : enable AD password change operation
#                   0 : OFF (default)
#                   1 : ON
#   LDAPMULTIVAL    : specify whether to obtain multiple values from each
#                   LDAP attribute
#                   0 : OFF (default)
#                   1 : ON
#   LDAPREFERRAL    : Enable LDAP referral
#                   0 : OFF
#                   1 : ON (default)
#   ADDGFWBIND       : specify whether to do LDAP bind operation at the DGFW
#                      authentication time
#                      0 : OFF
#                      1 : ON (default)
#---------------------------------------------------------------------------
DBHOST=localhost:389
DBUID=CN=Administrator,CN=Users,DC=is,DC=com
DBPWD=Administrator
DBTBL=CN=Users,DC=is,DC=com
DBATTR=/opt/icewall-sso/certd/config/dbattr.conf
#DBEXATTR=description
#DBCRYPTOTYPE=
#DBIWCRYPTOSEED=
#DBCRYPTOATTR=
LDAPBIND=1
LDAPPCHG=0
LDAPLANG=0
LDAPSSL=0
LDAPCACERT=/opt/icewall-sso/certd/config/cacert.pem
LDAPVERIFYSVRCERT=1
#LDAPCIPHERSUITE=
LDAPSSLBIND=1
ADPCHG=0
LDAPMULTIVAL=0
LDAPREFERRAL=1
ADDGFWBIND=1

#---------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#   MAXREQTHREAD : maximum number of request threads (default: 10)
#   ACCTHREAD    : the number of access threads, which are assigned to the
#                  requests that does not need DB connection (default: 0)
#   REQQUESIZE   : request queue size (default: 20)
#   MAXDBCONNECT : maximum number of database connection threads (default: 2)
#   DBQUESIZE    : Size of data queue, in which DB update data
#                  for certification DB is temporarily queued
#                  in user logout processing. (default: same as CACHE)
#                  Specifying LOGINSTAT parameter in dbattr.conf
#                  is required. NO change from default value is recommended.
#   LOGBUFSIZE   : access and error log buffer size (default: 1000)
#   CACHE        : maximum number of login user (default: 10)
#   MAXLOGINUSER : the number of the users who can log in
#   RECVWAITTIME : request recv wait time (1-60) (default: 3sec)
#   THREADSTACKSIZE : thread stack size (default: 256Kbytes)
#   LOGMULTITHREAD  : multithreading on log generation
#                     0 : single-thread mode (default)
#                     1 : multi-thread mode
#---------------------------------------------------------------------------
MAXREQTHREAD=10
#ACCTHREAD=0
REQQUESIZE=20
MAXDBCONNECT=2
LOGBUFSIZE=1000
CACHE=100
#MAXLOGINUSER=
RECVWAITTIME=3
THREADSTACKSIZE=256
LOGMULTITHREAD=1

#---------------------------------------------------------------------------
#  [ Replication Control Info ]
#   CERT         : [hostname:port no. ] replication target
#   CERTREPTYPE     : replication type
#                  0 : primary side
#                  1 : secondary side
#   RETRYCNTC       : number of retries allowd for the replication server
#                  connection (default: 10)
#   RETRYTMC        : time of retry intervals at the connection failure to
#                  the replication server (default: 3sec)
#   LIVETIMER       : replication interval after detecting that the
#                  replication target has gone down (default: 60sec)
#   HEALTHTIMER     : replication interval (secondary side only)
#                  (default: 5sec)
#   HEALTHCNT       : replication count (secondary side only) (default: 12)
#   DOWNLOADCONFFLG : download the configuration information from
#                  certification module of replication target at time of
#                  startup
#                  0 : not download
#                  1 : download (default)
#   FAILBACK        : add alive information of master certification module to
#                  ICP 2.0 response headers which the replica certification
#                  module returns (0-1) (default: 0)
#-----------------------------------------------------------------------------
#CERT=
#CERTREPTYPE=
#RETRYCNTC=5
#RETRYTMC=3
#LIVETIMER=30
#HEALTHTIMER=5
#HEALTHCNT=12
#DOWNLOADCONFFLG=1
#FAILBACK=0

#-----------------------------------------------------------------------------
#  [ Replication Performance Tuning Info ]
#   MAXREPTHREAD : maximum number of replication threads (default: 5)
#   REPQUESIZE   : replication queue size (default: 1000)
#-----------------------------------------------------------------------------
#MAXREPTHREAD=5
#REPQUESIZE=1000
```

NED edition

```
#-----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.conf $ $Revision: 9 $ $Date: 10/08/13 18:52 $
#-----------------------------------------------------------------------------
#-----------------------------------------------------------------------------
#  [ Log File Info ]
#   ALEVEL      : access log level
#              0 : no output
#              1 : fatal messages only (default)
#              2 : fatal and warning messages
#              3 : fatal, warning and information messages
#   ELEVEL      : error log level
#              0 : no output
#              1 : fatal messages only (default)
#              2 : fatal and warning messages
#              3 : fatal, warning and information messages
#   ACCESS      : access log file location
#              (default: /opt/icewall-sso/logs/cert.log)
#   ERROR       : error log file location
#              (default: /opt/icewall-sso/logs/certerr.log)
#    TRACE       : trace log file location
#    CATALOG     : message catalog file location
#    LOGINFO     : output ICP client information.
#                0 : no output (default)
#                1 : IP Address.
#                2 : IP Address and AGENT ID.
#    LOGPERF     : output performance log
#                0 : no output (default)(if PERFORMANCE=log default to 1)
#                1 : output
#    TRANSID     : output of Transaction IDs into log files
#                0 : no output (default)
#                1 : output
#    PERFORMANCE : performance log file location
#                (default: access log file location)
#    INFORMATION : information log file location
#                (default: access log file location)
#----------------------------------------------------------------------------
ALEVEL=1
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/cert.log
ERROR=/opt/icewall-sso/logs/certerr.log
#TRACE=/opt/icewall-sso/logs/certtrc.log
CATALOG=/opt/icewall-sso/messages/C/icewall_certd.cat
LOGINFO=0
LOGPERF=0
TRANSID=1
#PERFORMANCE=/opt/icewall-sso/logs/certperf.log
#INFORMATION=/opt/icewall-sso/logs/certinfo.log

#----------------------------------------------------------------------------
#  [ Access Control File Info ]
#    GROUP      : group info file location
#               (default: /opt/icewall-sso/certd/config/cert.grp)
#    ACL        : access control list file location
#               (default: /opt/icewall-sso/certd/config/cert.acl)
#    ACLREQUEST : request control list file location
#               (default: none)
#----------------------------------------------------------------------------
GROUP=/opt/icewall-sso/certd/config/cert.grp
ACL=/opt/icewall-sso/certd/config/cert.acl
#ACLREQUEST=/opt/icewall-sso/certd/config/request.acl

#----------------------------------------------------------------------------
#  [ Network Parameter Info ]
#    PORT           : certification module port no. (default: 14142)
#    IPV6LISTEN     : IP version of the requests that a certification module
#                   receives
#                   0 : IPv4 only (default)
#                   1 : IPv6 only
#                   2 : Both IPv4 and IPv6
#    HTTPPORT       : port number to receive HTTP based ICP2.0 requests
#    HTTPECHOHEADER : add request header, received from web clients, to
#                   response header ( HTTP based ICP2.0 resquests only )
#                   0 : not add (default)
#                   1 : add
#----------------------------------------------------------------------------
PORT=14142
#IPV6LISTEN=0
#HTTPPORT=8080
#HTTPECHOHEADER=0

#----------------------------------------------------------------------------
```

```
#  [ Session Control Info ]
#    COOKIERETRY   : cookie create retry count(default: 10)
#    COOKIETIME    : cookie expiration time (default: 60minutes)
#    COOKIEEXP     : cookie expiration switch
#               0 : OFF (default)
#               1 : ON (if LOMETHOD=1 defaults to 0)
#    LOMETHOD      : count session expiration time
#               0 : from login (default)
#               1 : from last access
#    DUPLOGIN      : allow duplicate login
#               0 : disallow (default)
#               1 : allow
#    DUPKIND       : duplicate login method
#               0 : force login (default)
#               1 : display force-login page
#    PARALOGIN     : allow/disallow a user to login again with a userid and
#               a password ,who has previously logged into thesystem with
#               a client certificate
#               0 : disallow (default)
#               1 : allow
#    ACCCTRLFLG    : use check and userid check of a client certificate
#               0 : check for using client certificate, and login userid
#                  (default)
#               1 : check for using client certificate only
#               2 : no check
#    SESSIONIDLEN  : byte length of the session ID a certification module
#               generates (default: 32 byte length)
#    CERTUNIQUEKEY : unique key to identify group of certification modules
#               (default: 0)
#-----------------------------------------------------------------------------
COOKIERETRY=10
COOKIETIME=60
#COOKIEEXP=1
LOMETHOD=1
DUPLOGIN=1
#DUPKIND=0
#PARALOGIN=0
#ACCCTRLFLG=0
#SESSIONIDLEN=32
#CERTUNIQUEKEY=

#-----------------------------------------------------------------------------
#  [ Password Control Info ]
#    PWDLOGINHASH : a password hash method at the time of the login :
#              (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#              (default: AUTO-PLAIN)
#    PWDCHGHASH   : a password hash method at the time of the password change :
#              (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#              (default: AUTO-PLAIN)
#    PWDMINLEN    : minimum character length of a new password at the time of
#              the password change (default: 3)
#    PWDMAXLEN    : maximum character length of a new password at the time of
#              the password change (default: 6)
#    PWDALPHANUM  : combination of the character set available as a password
#              (0-13)(default: 1)
#    PWDEXPIRE    : the number of days which the password expires (default: 72)
#    PWDSAMEPASS  : use of password identical to user id
#              0 : accepted
#              1 : not accepted (default)
#    LOCKCOUNT    : maximum number of password retries allowed (default: 0)
#    PWDEXPCHK    : password expiration check switch
#              0 : OFF (default)
#              1 : ON
#   PWDHISCHK    : password history check switch
#              0 : OFF (default)
#              1 : ON
#   PWDHISCNT    : password history count (1-20) (default: 1)
#   PWDFORBID    : forbidden password file location
#              (default: /opt/icewall-sso/certd/config/pwdforbid.conf)
#   PWDEXPWARN   : password expiration warning day check (0-365)
#              (default: 0)
#----------------------------------------------------------------------------
PWDLOGINHASH=SHA
PWDCHGHASH=SHA
PWDMINLEN=3
PWDMAXLEN=6
PWDALPHANUM=0
PWDEXPIRE=72
PWDSAMEPASS=0
LOCKCOUNT=5
PWDEXPCHK=1
PWDHISCHK=1
PWDHISCNT=3
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDEXPWARN=0

#----------------------------------------------------------------------------
#  [ Certification Database Control Info ]
#   DBHOST           : e-directory server host name
#   DBUID            : userid to use for accessing the user authentication
#                table
#   DBPWD            : password to use for accessing the user authentication
#                table
#   DBTBL            : user authentication table name
#   DBATTR           : database attribute file location
#                (default: /opt/icewall-sso/certd/config/dbattr.conf)
#   DBEXATTR         : extra columns to use for environment variables
#   DBCRYPTOTYPE      : a hash method used for decryption of the target column
#                data(0-3) (default: 0)
#   DBIWCRYPTOSEED    : a seed value for decoding to be passed to the
#                certification DB encryption standard library
#   DBCRYPTOATTR      : target column names to be decrypted
#   LDAPBIND         : use LDAP bind operation mode
#                0 : OFF (default)
#                1 : ON
#   LDAPPCHG         : use LDAP password change operation mode
#                0 : OFF
#                1 : ON (default)
#   LDAPLANG         : use code set conversion mode
#                0 : OFF
#                1 : ON (default)
#   LDAPSSL          : specify whether to use SSL in order to communicate
#                with the e-directory server
#                0 : OFF (default)
#                1 : ON
#   LDAPCACERT       : location of the PEM-encoded X.509 CA certificate file
#   LDAPVERIFYSVRCERT : specify whether to verify the CA certificate
#                0 : OFF
#                1 : ON (default)
#   LDAPCIPHERSUITE   : cipher preference for SSL communication with the LDAP
#                server
#   LDAPSSLBIND       : specify whether to use SSL at the time of LDAP bind
#                0 : OFF
#                1 : ON (default)
#    LDAPMULTIVAL      : specify whether to obtain multiple values from each
#                    LDAP attribute
#                    0 : OFF (default)
#                    1 : ON
#    LDAPREFERRAL      : Enable LDAP referral
#                    0 : OFF
#                    1 : ON (default)
#------------------------------------------------------------------------------
DBHOST=localhost:389
DBUID=cn=admin,o=Alias.com
DBPWD=passwd
DBTBL=o=Alias.com
DBATTR=/opt/icewall-sso/certd/config/dbattr.conf
#DBEXATTR=registeredAddress,teletexTerminalIdentifier
#DBCRYPTOTYPE=
#DBIWCRYPTOSEED=
#DBCRYPTOATTR=
LDAPBIND=1
LDAPPCHG=1
LDAPLANG=1
LDAPSSL=0
LDAPCACERT=/opt/icewall-sso/certd/config/cacert.pem
LDAPVERIFYSVRCERT=1
#LDAPCIPHERSUITE=
LDAPSSLBIND=1
LDAPMULTIVAL=0
LDAPREFERRAL=1

#------------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#    MAXREQTHREAD : maximum number of request threads (default: 10)
#    ACCTHREAD    : the number of access threads, which are assigned to the
#                 requests that does not need DB connection (default: 0)
#    REQQUESIZE   : request queue size (default: 20)
#    MAXDBCONNECT : maximum number of database connection threads (default: 2)
#    DBQUESIZE    : Size of data queue, in which DB update data
#                 for certification DB is temporarily queued
#                 in user logout processing. (default: same as CACHE)
#                 Specifying LOGINSTAT parameter in dbattr.conf
#                 is required. NO change from default value is recommended.
#    LOGBUFSIZE   : access and error log buffer size (default: 1000)
#    CACHE        : maximum number of login user (default: 10)
#    MAXLOGINUSER : the number of the users who can log in
#    RECVWAITTIME : request recv wait time (1-60) (default: 3sec)
#    THREADSTACKSIZE : thread stack size (default: 256Kbytes)
#    LOGMULTITHREAD  : multithreading on log generation
#                   0 : single-thread mode (default)
#                   1 : multi-thread mode
#------------------------------------------------------------------------------
MAXREQTHREAD=10
#ACCTHREAD=0
REQQUESIZE=20
MAXDBCONNECT=2
LOGBUFSIZE=1000
CACHE=100
#MAXLOGINUSER=
RECVWAITTIME=3
THREADSTACKSIZE=256
LOGMULTITHREAD=1

#------------------------------------------------------------------------------
#  [ Replication Control Info ]
#   CERT            : [hostname:port no. ] replication target
#   CERTREPTYPE     : replication type
#                 0 : primary side
#                 1 : secondary side
#   RETRYCNTC       : number of retries allowd for the replication server
#                 connection (default: 10)
#   RETRYTMC        : time of retry intervals at the connection failure to
#                 the replication server (default: 3sec)
#   LIVETIMER       : replication interval after detecting that the
#                 replication target has gone down (default: 60sec)
#   HEALTHTIMER     : replication interval (secondary side only)
#                 (default: 5sec)
#   HEALTHCNT       : replication count (secondary side only) (default: 12)
#   DOWNLOADCONFFLG : download the configuration information from
#                 certification module of replication target at time of
#                 startup
#                 0 : not download
#                 1 : download (default)
#   FAILBACK        : add alive information of master certification module to
#                 ICP 2.0 response headers which the replica certification
#                 module returns (0-1) (default: 0)
#------------------------------------------------------------------------------
#CERT=
#CERTREPTYPE=
#RETRYCNTC=5
#RETRYTMC=3
#LIVETIMER=30
#HEALTHTIMER=5
#HEALTHCNT=12
#DOWNLOADCONFFLG=1
#FAILBACK=0

#------------------------------------------------------------------------------
#  [ Replication Performance Tuning Info ]
#   MAXREPTHREAD : maximum number of replication threads (default: 5)
#   REPQUESIZE   : replication queue size (default: 1000)
#------------------------------------------------------------------------------
#MAXREPTHREAD=5
#REPQUESIZE=1000
```

CSV edition

```
#------------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.conf $ $Revision: 12 $ $Date: 10/08/13 18:51 $
#------------------------------------------------------------------------------
#------------------------------------------------------------------------------
#  [ Log File Info ]
#   ALEVEL      : access log level
#             0 : no output
#             1 : fatal messages only (default)
#             2 : fatal and warning messages
#             3 : fatal, warning and information messages
#   ELEVEL      : error log level
#             0 : no output
#             1 : fatal messages only (default)
#             2 : fatal and warning messages
#             3 : fatal, warning and information messages
#   ACCESS      : access log file location
#             (default: /opt/icewall-sso/logs/cert.log)
#   ERROR       : error log file location
#            (default: /opt/icewall-sso/logs/certerr.log)
#   TRACE     : trace log file location
#   CATALOG    : message catalog file location
#   LOGINFO    : output ICP client information.
#            0 : no output (default)
#            1 : IP Address.
#            2: IP Address and AGENT ID.
#   LOGPERF    : output performance log
#            0: no output (default)(if PERFORMANCE=log default to 1)
#            1: output
#   TRANSID    : output of Transaction IDs into log files
#            0 : no output (default)
#            1 : output
#   PERFORMANCE : performance log file location
#            (default: access log file location)
#   INFORMATION : information log file location
#            (default: access log file location)
#-----------------------------------------------------------------------------
ALEVEL=1
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/cert.log
ERROR=/opt/icewall-sso/logs/certerr.log
#TRACE=/opt/icewall-sso/logs/certtrc.log
CATALOG=/opt/icewall-sso/messages/C/icewall_certd.cat
LOGINFO=0
LOGPERF=0
TRANSID=1
#PERFORMANCE=/opt/icewall-sso/logs/certperf.log
#INFORMATION=/opt/icewall-sso/logs/certinfo.log

#-----------------------------------------------------------------------------
#  [ Access Control File Info ]
#   GROUP     : group info file location
#            (default: /opt/icewall-sso/certd/config/cert.grp)
#   ACL      : access control list file location
#            (default: /opt/icewall-sso/certd/config/cert.acl)
#   ACLREQUEST : request control list file location
#            (default: none)
#-----------------------------------------------------------------------------
GROUP=/opt/icewall-sso/certd/config/cert.grp
ACL=/opt/icewall-sso/certd/config/cert.acl
#ACLREQUEST=/opt/icewall-sso/certd/config/request.acl

#-----------------------------------------------------------------------------
#  [ Network Parameter Info ]
#   PORT         : certification module port no. (default: 14142)
#   IPV6LISTEN    : IP version of the requests that a certification module
#              receives
#              0 : IPv4 only (default)
#              1 : IPv6 only
#              2 : Both IPv4 and IPv6
#   HTTPPORT      : port number to receive HTTP based ICP2.0 requests
#   HTTPECHOHEADER : add request header, received from web clients, to
#              response header ( HTTP based ICP2.0 resquests only )
#              0 : not add (default)
#              1 : add
#-----------------------------------------------------------------------------
PORT=14142
#IPV6LISTEN=0
#HTTPPORT=8080
#HTTPECHOHEADER=0
```

```
#----------------------------------------------------------------------------
#  [ Session Control Info ]
#    COOKIERETRY   : cookie create retry count(default: 10)
#    COOKIETIME    : cookie expiration time (default: 60minutes)
#    COOKIEEXP     : cookie expiration switch
#                0 : OFF (default)
#                1 : ON (if LOMETHOD=1 defaults to 0)
#    LOMETHOD      : count session expiration time
#                0 : from login (default)
#                1 : from last access
#    DUPLOGIN      : allow duplicate login
#                0 : disallow (default)
#                1 : allow
#    DUPKIND       : duplicate login method
#                0 : force login (default)
#                1 : display force-login page
#    PARALOGIN     : allow/disallow a user to login again with a userid and
#                a password ,who has previously logged into thesystem with
#                a client certificate
#                0 : disallow (default)
#                1 : allow
#    ACCCTRLFLG    : use check and userid check of a client certificate
#                0 : check for using client certificate, and login userid
#                   (default)
#                1 : check for using client certificate only
#                2 : no check
#    SESSIONIDLEN  : byte length of the session ID a certification module
#                generates (default: 32 byte length)
#    CERTUNIQUEKEY : unique key to identify group of certification modules
#                (default: 0)
#----------------------------------------------------------------------------
COOKIERETRY=10
COOKIETIME=60
#COOKIEEXP=1
LOMETHOD=1
DUPLOGIN=1
#DUPKIND=0
#PARALOGIN=0
#ACCCTRLFLG=0
#SESSIONIDLEN=32
#CERTUNIQUEKEY=

#----------------------------------------------------------------------------
#  [ Password Control Info ]
#    PWDLOGINHASH : a password hash method at the time of the login :
#               (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#               (default: AUTO-PLAIN)
#    PWDCHGHASH   : a password hash method at the time of the password change :
#               (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#               (default: AUTO-PLAIN)
#    PWDMINLEN    : minimum character length of a new password at the time of
#               the password change (default: 3)
#    PWDMAXLEN    : maximum character length of a new password at the time of
#               the password change (default: 6)
#    PWDALPHANUM  : combination of the character set available as a password
#               (0-13)(default: 1)
#    PWDEXPIRE    : the number of days which the password expires (default: 72)
#    PWDSAMEPASS  : use of password identical to user id
#               0 : accepted
#               1 : not accepted (default)
#    LOCKCOUNT    : maximum number of password retries allowed (default: 0)
#    PWDEXPCHK    : password expiration check switch
#               0 : OFF (default)
#               1 : ON
#   PWDHISCHK    : password history check switch
#               0 : OFF (default)
#               1 : ON
#   PWDHISCNT    : password history count (1-20) (default: 1)
#   PWDFORBID    : forbidden password file location
#               (default: /opt/icewall-sso/certd/config/pwdforbid.conf)
#   PWDEXPWARN   : password expiration warning day check (0-365)
#               (default: 0)
#---------------------------------------------------------------------------
#PWDLOGINHASH=AUTO-PLAIN
#PWDCHGHASH=AUTO-PLAIN
PWDMINLEN=3
PWDMAXLEN=6
PWDALPHANUM=0
PWDEXPIRE=72
PWDSAMEPASS=0
LOCKCOUNT=5
PWDEXPCHK=1
PWDHISCHK=1
PWDHISCNT=3
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDEXPWARN=0

#---------------------------------------------------------------------------
#  [ Certification Database Control Info ]
#   DBTBL           : user authentication CSV file location
#   DBATTR          : database attribute file location
#                 (default: /opt/icewall-sso/certd/config/dbattr.conf)
#   DBEXATTR         : extra columns to use for environment variables
#   DBCRYPTOTYPE      : a hash method used for decryption of the target column
#                 data(0-3) (default: 0)
#   DBIWCRYPTOSEED    : a seed value for decoding to be passed to the
#                 certification DB encryption standard library
#   DBCRYPTOATTR      : target column names to be decrypted
#---------------------------------------------------------------------------
DBTBL=/opt/icewall-sso/certd/config/sample.csv
DBATTR=/opt/icewall-sso/certd/config/dbattr.conf
#DBEXATTR=PASSWD1,PASSWD2
#DBCRYPTOTYPE=
#DBIWCRYPTOSEED=
#DBCRYPTOATTR=

#---------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#   MAXREQTHREAD : maximum number of request threads (default: 10)
#   ACCTHREAD    : the number of access threads, which are assigned to the
#               requests that does not need DB connection (default: 0)
#   REQQUESIZE   : request queue size (default: 20)
#   DBQUESIZE    : Size of data queue, in which DB update data
#               for certification DB is temporarily queued
#               in user logout processing. (default: same as CACHE)
#               Specifying LOGINSTAT parameter in dbattr.conf
#               is required. NO change from default value is recommended.
#   LOGBUFSIZE   : access and error log buffer size (default: 1000)
#   CACHE       : maximum number of login user (default: 10)
#   MAXLOGINUSER : the number of the users who can log in
#   RECVWAITTIME : request recv wait time (1-60) (default: 3sec)
#   THREADSTACKSIZE : thread stack size (default: 256Kbytes)
#   LOGMULTITHREAD  : multithreading on log generation
#                 0 : single-thread mode (default)
#                     1 : multi-thread mode
#--------------------------------------------------------------------------------
MAXREQTHREAD=10
#ACCTHREAD=0
REQQUESIZE=20
LOGBUFSIZE=1000
CACHE=100
#MAXLOGINUSER=
RECVWAITTIME=3
THREADSTACKSIZE=256
LOGMULTITHREAD=1
```

MySQL edition

```
#--------------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.conf $ $Revision: 10 $ $Date: 10/08/13 18:52 $
#--------------------------------------------------------------------------------
#  [ Log File Info ]
#    ALEVEL      : access log level
#               0 : no output
#               1 : fatal messages only (default)
#               2 : fatal and warning messages
#               3 : fatal, warning and information messages
#    ELEVEL      : error log level
#               0 : no output
#               1 : fatal messages only (default)
#               2 : fatal and warning messages
#               3 : fatal, warning and information messages
#    ACCESS      : access log file location
#               (default: /opt/icewall-sso/logs/cert.log)
#    ERROR       : error log file location
#               (default: /opt/icewall-sso/logs/certerr.log)
#    TRACE       : trace log file location
#    CATALOG     : message catalog file location
#    LOGINFO     : output ICP client information.
#               0 : no output (default)
#               1 : IP Address.
#               2 : IP Address and AGENT ID.
#    LOGPERF     : output performance log
#               0 : no output (default)(if PERFORMANCE=log default to 1)
#               1 : output
#    TRANSID     : output of Transaction IDs into log files
#               0 : no output (default)
#               1 : output
#    PERFORMANCE : performance log file location
#               (default: access log file location)
#    INFORMATION : information log file location
#               (default: access log file location)
#--------------------------------------------------------------------------------
ALEVEL=1
ELEVEL=1
ACCESS=/opt/icewall-sso/logs/cert.log
ERROR=/opt/icewall-sso/logs/certerr.log
#TRACE=/opt/icewall-sso/logs/certtrc.log
CATALOG=/opt/icewall-sso/messages/C/icewall_certd.cat
LOGINFO=0
LOGPERF=0
TRANSID=1
#PERFORMANCE=/opt/icewall-sso/logs/certperf.log
#INFORMATION=/opt/icewall-sso/logs/certinfo.log
```

```
#-----------------------------------------------------------------------------
#  [ Access Control File Info ]
#    GROUP      : group info file location
#              (default: /opt/icewall-sso/certd/config/cert.grp)
#    ACL        : access control list file location
#              (default: /opt/icewall-sso/certd/config/cert.acl)
#    ACLREQUEST : request control list file location
#              (default: none)
#-----------------------------------------------------------------------------
GROUP=/opt/icewall-sso/certd/config/cert.grp
ACL=/opt/icewall-sso/certd/config/cert.acl
#ACLREQUEST=/opt/icewall-sso/certd/config/request.acl

#-----------------------------------------------------------------------------
#  [ Network Parameter Info ]
#    PORT          : certification module port no. (default: 14142)
#    IPV6LISTEN    : IP version of the requests that a certification module
#                 receives
#                 0 : IPv4 only (default)
#                 1 : IPv6 only
#                 2 : Both IPv4 and IPv6
#    HTTPPORT      : port number to receive HTTP based ICP2.0 requests
#    HTTPECHOHEADER : add request header, received from web clients, to
#                 response header ( HTTP based ICP2.0 resquests only )
#                 0 : not add (default)
#                 1 : add
#-----------------------------------------------------------------------------
PORT=14142
#IPV6LISTEN=0
#HTTPPORT=8080
#HTTPECHOHEADER=0

#-----------------------------------------------------------------------------
#  [ Session Control Info ]
#    COOKIERETRY   : cookie create retry count(default: 10)
#    COOKIETIME    : cookie expiration time (default: 60minutes)
#    COOKIEEXP     : cookie expiration switch
#                0 : OFF (default)
#                1 : ON (if LOMETHOD=1 defaults to 0)
#    LOMETHOD      : count session expiration time
#                0 : from login (default)
#                1 : from last access
#    DUPLOGIN      : allow duplicate login
#                0 : disallow (default)
#                1 : allow
#    DUPKIND       : duplicate login method
#                0 : force login (default)
#                1 : display force-login page
#    PARALOGIN     : allow/disallow a user to login again with a userid and
#                a password ,who has previously logged into thesystem with
#                a client certificate
#                0 : disallow (default)
#                1 : allow
#    ACCCTRLFLG    : use check and userid check of a client certificate
#                0 : check for using client certificate, and login userid
#                   (default)
#                1 : check for using client certificate only
#                2 : no check
#    SESSIONIDLEN  : byte length of the session ID a certification module
#                generates (default: 32 byte length)
#    CERTUNIQUEKEY : unique key to identify group of certification modules
#               (default: 0)
#--------------------------------------------------------------------------
COOKIERETRY=10
COOKIETIME=60
#COOKIEEXP=1
LOMETHOD=1
DUPLOGIN=1
#DUPKIND=0
#PARALOGIN=0
#ACCCTRLFLG=0
#SESSIONIDLEN=32
#CERTUNIQUEKEY=

#--------------------------------------------------------------------------
#  [ Password Control Info ]
#    PWDLOGINHASH : a password hash method at the time of the login :
#               (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#               (default: AUTO-PLAIN)
#    PWDCHGHASH   : a password hash method at the time of the password change :
#               (MD5/SHA/SHA256/PLAIN/AUTO-PLAIN/AUTO-MD5)
#               (default: AUTO-PLAIN)
#    PWDMINLEN    : minimum character length of a new password at the time of
#               the password change (default: 3)
#    PWDMAXLEN    : maximum character length of a new password at the time of
#               the password change (default: 6)
#    PWDALPHANUM  : combination of the character set available as a password
#               (0-13)(default: 1)
#    PWDEXPIRE    : the number of days which the password expires (default: 72)
#    PWDSAMEPASS  : use of password identical to user id
#               0 : accepted
#               1 : not accepted (default)
#    LOCKCOUNT    : maximum number of password retries allowed (default: 0)
#    PWDEXPCHK    : password expiration check switch
#               0 : OFF (default)
#               1 : ON
#    PWDHISCHK    : password history check switch
#               0 : OFF (default)
#               1 : ON
#    PWDHISCNT    : password history count (1-20) (default: 1)
#    PWDFORBID    : forbidden password file location
#               (default: /opt/icewall-sso/certd/config/pwdforbid.conf)
#    PWDEXPWARN   : password expiration warning day check (0-365)
#               (default: 0)
#--------------------------------------------------------------------------
#PWDLOGINHASH=AUTO-PLAIN
#PWDCHGHASH=AUTO-PLAIN
PWDMINLEN=3
PWDMAXLEN=6
PWDALPHANUM=0
PWDEXPIRE=72
PWDSAMEPASS=0
LOCKCOUNT=5
PWDEXPCHK=1
PWDHISCHK=1
PWDHISCNT=3
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDFORBID=/opt/icewall-sso/certd/config/pwdforbid.conf
PWDEXPWARN=0

#--------------------------------------------------------------------------
#  [ Certification Database Control Info ]
#    DBHOST        : mysql server network client name
#   DBUID          : userid to use for accessing the user authentication
#                 table
#   DBPWD          : password to use for accessing the user authentication
#                 table
#   DBTBL          : user authentication table name
#   DBATTR         : database attribute file location
#                 (default: /opt/icewall-sso/certd/config/dbattr.conf)
#   DBEXATTR       : extra columns to use for environment variables
#   DBCRYPTOTYPE   : a hash method used for decryption of the target column
#                 data(0-3) (default: 0)
#   DBIWCRYPTOSEED : a seed value for decoding to be passed to the
#                 certification DB encryption standard library
#   DBCRYPTOATTR   : target column names to be decrypted
#----------------------------------------------------------------------------
DBHOST=icewalldb:odbchost:3306:MySQL ODBC 5.1.6 Driver
DBUID=root
DBPWD=new_password
DBTBL=icewalltest
DBATTR=/opt/icewall-sso/certd/config/dbattr.conf
#DBEXATTR=PASSWD1,PASSWD2
#DBCRYPTOTYPE=
#DBIWCRYPTOSEED=
#DBCRYPTOATTR=

#----------------------------------------------------------------------------
#  [ Reference Database Control Info ]
#   REFTBL  : user reference table name
#   REFATTR : user reference table attribute
#   REFUID  : column to use for userid in the reference table
#----------------------------------------------------------------------------
#REFTBL=icewalltest
REFATTR=PASSWD1,PASSWD2
REFUID=USERID

#----------------------------------------------------------------------------
#  [ Performance Tuning Info ]
#   MAXREQTHREAD : maximum number of request threads (default: 10)
#   ACCTHREAD    : the number of access threads, which are assigned to the
#               requests that does not need DB connection (default: 0)
#   REQQUESIZE   : request queue size (default: 20)
#   MAXDBCONNECT : maximum number of database connection threads (default: 2)
#   DBQUESIZE    : Size of data queue, in which DB update data
#               for certification DB is temporarily queued
#               in user logout processing. (default: same as CACHE)
#               Specifying LOGINSTAT parameter in dbattr.conf
#               is required. NO change from default value is recommended.
#   LOGBUFSIZE   : access and error log buffer size (default: 1000)
#   CACHE        : maximum number of login user (default: 10)
#   MAXLOGINUSER : the number of the users who can log in
#   RECVWAITTIME : request recv wait time (1-60) (default: 3sec)
#   THREADSTACKSIZE : thread stack size (default: 256Kbytes)
#   LOGMULTITHREAD  : multithreading on log generation
#                  0 : single-thread mode (default)
#                  1 : multi-thread mode
#----------------------------------------------------------------------------
MAXREQTHREAD=10
#ACCTHREAD=0
REQQUESIZE=20
MAXDBCONNECT=2
LOGBUFSIZE=1000
CACHE=100
#MAXLOGINUSER=
RECVWAITTIME=3
THREADSTACKSIZE=256
LOGMULTITHREAD=1

#------------------------------------------------------------------------------
#  [ Replication Control Info ]
#    CERT            : [hostname:port no. ] replication target
#    CERTREPTYPE     : replication type
#                 0 : primary side
#                 1 : secondary side
#    RETRYCNTC       : number of retries allowd for the replication server
#                 connection (default: 10)
#    RETRYTMC        : time of retry intervals at the connection failure to
#                 the replication server (default: 3sec)
#    LIVETIMER       : replication interval after detecting that the
#                 replication target has gone down (default: 60sec)
#    HEALTHTIMER     : replication interval (secondary side only)
#                 (default: 5sec)
#    HEALTHCNT       : replication count (secondary side only) (default: 12)
#    DOWNLOADCONFFLG : download the configuration information from
#                 certification module of replication target at time of
#                 startup
#                 0 : not download
#                 1 : download (default)
#    FAILBACK        : add alive information of master certification module to
#                 ICP 2.0 response headers which the replica certification
#                 module returns (0-1) (default: 0)
#------------------------------------------------------------------------------
#CERT=
#CERTREPTYPE=
#RETRYCNTC=5
#RETRYTMC=3
#LIVETIMER=30
#HEALTHTIMER=5
#HEALTHCNT=12
#DOWNLOADCONFFLG=1
#FAILBACK=0

#------------------------------------------------------------------------------
#  [ Replication Performance Tuning Info ]
#    MAXREPTHREAD : maximum number of replication threads (default: 5)
#    REPQUESIZE   : replication queue size (default: 1000)
#------------------------------------------------------------------------------
#MAXREPTHREAD=5
#REPQUESIZE=1000
```

3.7.2 Column information configuration file (dbattr.conf)

ORACLE edition

```
#------------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 15:35 $
#------------------------------------------------------------------------------
#------------------------------------------------------------------------------
#  [ Authentication Database Table's Column Info ]
#    UID         : UserID.
#    PASSWORD    : Password.
#    PWDEXPDATE  : Password Expiration Date.
#    PWDHISTORY  : Password History.
#    PCHGOK      : Password Change OK/NG.
#   PCHGDATE    : Password Change Date.
#   PLOGINDATE  : Login Date.
#   LLOGINDATE  : Last Login Date.
#   FLOGINDATE  : Login Failure Date.
#   PWDRETRY    : Password Retry Count.
#   PWDLOCK     : Account Lock ON/OFF.
#   LOGINOK     : Login OK/NG.
#   LOCKDATE    : Account Lock Date.
#   LOGINSTAT   : Login Status.
#
#  [ for Client Certificate Option Define ]
#   RASERIALNO  : RA Serial Number.
#   IWSERIALNO  : Certificate Serial Number.
#   CERTEXPDATE : Certificate Expiration Date.
#   GETCERT     : Client Certificate Regist/Download Switch.
#   ONLINE      : Certificate Login Status.
#---------------------------------------------------------------------------
UID=USERID
PASSWORD=PASSWD
PWDEXPDATE=PASSWDEXP
PWDHISTORY=PASSWDHIS
PCHGOK=PASSCHANGE
PCHGDATE=CHGDATE
PLOGINDATE=LOGONDATE
LLOGINDATE=LASTDATE
FLOGINDATE=LOGONFAIL
PWDRETRY=FAILCOUNT
PWDLOCK=LOCKOUT
LOGINOK=LOGONSTOP
LOCKDATE=LOCKDATE
LOGINSTAT=LOGSTATUS
#RASERIALNO=RASERIAL
#IWSERIALNO=BSSERIAL
#CERTEXPDATE=VDATE
#GETCERT=CERT
#ONLINE=APENABLE
```

LDAP edition

```
#---------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 16:02 $
#---------------------------------------------------------------------------
#---------------------------------------------------------------------------
#  [ Authentication Directory Attributes Info ]
#   UID         : UserID.
#   PASSWORD    : Password.
#   PWDEXPDATE  : Password Expiration Date.
#   PWDHISTORY  : Password History.
#   PCHGOK      : Password Change OK/NG.
#   PCHGDATE    : Password Change Date.
#   PLOGINDATE  : Login Date.
#   LLOGINDATE  : Last Login Date.
#   FLOGINDATE  : Login Failure Date.
#   PWDRETRY    : Password Retry Count.
#   PWDLOCK     : Account Lock ON/OFF.
#   LOGINOK     : Login OK/NG.
#   LOCKDATE    : Account Lock Date.
#   LOGINSTAT   : Login Status.

#  [ for Client Certificate Option Define ]
#    RASERIALNO  : RA Serial Number.
#    IWSERIALNO  : Certificate Serial Number.
#    CERTEXPDATE : Certificate Expiration Date.
#    GETCERT     : Client Certificate Regist/Download Switch.
#    ONLINE      : Certificate Login Status.
#---------------------------------------------------------------------------
UID=uid
PASSWORD=userPassword
PWDEXPDATE=passwordExpirationTime
PWDHISTORY=passwordHistory
PCHGOK=mobile
PCHGDATE=manager
PLOGINDATE=pager
LLOGINDATE=displayName
FLOGINDATE=givenName
PWDRETRY=passwordRetryCount
PWDLOCK=employeeNumber
LOGINOK=homePostalAddress
LOCKDATE=title
LOGINSTAT=initials
#RASERIALNO=roomNumber
#IWSERIALNO=telexnumber
#CERTEXPDATE=homePhone
#ONLINE=registeredAddress
#GETCERT=facsimileTelephoneNumber
```

OpenLDAP

```
#---------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 2 $ $Date: 10/04/21 15:08 $
#---------------------------------------------------------------------------
#---------------------------------------------------------------------------
#  [ Authentication Directory Attributes Info ]
#    UID         : UserID.
#    PASSWORD    : Password.
#    PWDEXPDATE  : Password Expiration Date.
#    PWDHISTORY  : Password History.
#    PCHGOK      : Password Change OK/NG.
#    PCHGDATE    : Password Change Date.
#    PLOGINDATE  : Login Date.
#    LLOGINDATE  : Last Login Date.
#    FLOGINDATE  : Login Failure Date.
#    PWDRETRY    : Password Retry Count.
#    PWDLOCK     : Account Lock ON/OFF.
#    LOGINOK     : Login OK/NG.
#    LOCKDATE    : Account Lock Date.
#    LOGINSTAT   : Login Status.
#
#  [ for Client Certificate Option Define ]
#    RASERIALNO  : RA Serial Number.
#    IWSERIALNO  : Certificate Serial Number.
#    CERTEXPDATE : Certificate Expiration Date.
#    GETCERT     : Client Certificate Regist/Download Switch.
#    ONLINE      : Certificate Login Status.
#---------------------------------------------------------------------------
UID=uid
PASSWORD=userPassword
PWDEXPDATE=departmentNumber
PWDHISTORY=userPKCS12
PCHGOK=mobile
```

```
PCHGDATE=employeeType
PLOGINDATE=pager
LLOGINDATE=displayName
FLOGINDATE=givenName
PWDRETRY=roomNumber
PWDLOCK=employeeNumber
LOGINOK=homePostalAddress
LOCKDATE=title
LOGINSTAT=initials
#RASERIALNO=jpegPhoto
#IWSERIALNO=registeredAddress
#CERTEXPDATE=homePhone
#GETCERT=facsimileTelephoneNumber
#ONLINE=telexNumber
```

MSAD edition

```
#-----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 2 $ $Date: 10/03/27 17:00 $
#-----------------------------------------------------------------------------
#-----------------------------------------------------------------------------
#  [ Authentication Directory Attributes Info ]
#    UID          : UserID.
#    PASSWORD     : Password.
#    PWDEXPDATE   : Password Expiration Date.
#    PWDHISTORY   : Password History.
#    PCHGOK       : Password Change OK/NG.
#    PCHGDATE     : Password Change Date.
#    PLOGINDATE   : Login Date.
#    LLOGINDATE   : Last Login Date.
#    FLOGINDATE   : Login Failure Date.
#    PWDRETRY     : Password Retry Count.
#    PWDLOCK      : Account Lock ON/OFF.
#    LOGINOK      : Login OK/NG.
#    LOCKDATE     : Account Lock Date.
#    LOGINSTAT    : Login Status.
#
#  [ for Client Certificate Option Define ]
#    RASERIALNO   : RA Serial Number.
#    IWSERIALNO   : Certificate Serial Number.
#    CERTEXPDATE  : Certificate Expiration Date.
#    GETCERT      : Client Certificate Regist/Download Switch.
#    ONLINE       : Certificate Login Status.
#-----------------------------------------------------------------------------
UID=CN
PASSWORD=unicodePWD
PWDEXPDATE=street
PWDHISTORY=
PCHGOK=mobile
PCHGDATE=info
PLOGINDATE=pager
LLOGINDATE=homePhone
FLOGINDATE=givenName
PWDRETRY=st
PWDLOCK=comment
LOGINOK=homePostalAddress
LOCKDATE=title
LOGINSTAT=initials
#RASERIALNO=employeeNumber
#IWSERIALNO=employeeType
```

```
#CERTEXPDATE=primaryTelexNumber
#GETCERT=facsimileTelephoneNumber
#ONLINE=postalCode
```

* If using Microsoft Active Directory Lightweight Directory Services, the attribute name info used by PCHGDATE may not exist. Please verify it.

NED edition

```
#-----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 18:22 $
#-----------------------------------------------------------------------------
#-----------------------------------------------------------------------------
#  [ Authentication Directory Attributes Info ]
#    UID          : UserID.
#    PASSWORD     : Password.
#    PWDEXPDATE   : Password Expiration Date.
#    PWDHISTORY   : Password History.
#    PCHGOK       : Password Change OK/NG.
#    PCHGDATE     : Password Change Date.
#    PLOGINDATE   : Login Date.
#    LLOGINDATE   : Last Login Date.
#    FLOGINDATE   : Login Failure Date.
#    PWDRETRY     : Password Retry Count.
#    PWDLOCK      : Account Lock ON/OFF.
#    LOGINOK      : Login OK/NG.
#    LOCKDATE     : Account Lock Date.
#    LOGINSTAT    : Login Status.
#
#  [ for Client Certificate Option Define ]
#    RASERIALNO   : RA Serial Number.
#    IWSERIALNO   : Certificate Serial Number.
#    CERTEXPDATE  : Certificate Expiration Date.
#    GETCERT      : Client Certificate Regist/Download Switch.
#    ONLINE       : Certificate Login Status.
#-----------------------------------------------------------------------------
UID=cn
PASSWORD=userPassword
PWDEXPDATE=x500UniqueIdentifier
PWDHISTORY=userSMIMECertificate
PCHGOK=mobile
PCHGDATE=jobCode
PLOGINDATE=pager
LLOGINDATE=displayName
FLOGINDATE=givenName
PWDRETRY=workforceID
PWDLOCK=employeeNumber
LOGINOK=homePostalAddress
LOCKDATE=title
LOGINSTAT=initials
#RASERIALNO=masvDefaultRange
#IWSERIALNO=telexNumber
#CERTEXPDATE=homePhone
#ONLINE=registeredAddress
#GETCERT=facsimileTelephoneNumber
```

CSV edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 2 $ $Date: 10/08/17 11:14 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ Authentication Database Table's Column Info ]
#    UID          : UserID.
#    PASSWORD     : Password.
#    PWDEXPDATE   : Password Expiration Date.
#    PWDHISTORY   : Password History.
#    PCHGOK       : Password Change OK/NG.
#    PCHGDATE     : Password Change Date.
#    PLOGINDATE   : Login Date.
#    LLOGINDATE   : Last Login Date.
#    FLOGINDATE   : Login Failure Date.
#    PWDRETRY     : Password Retry Count.
#    PWDLOCK      : Account Lock ON/OFF.
#    LOGINOK      : Login OK/NG.
#    LOCKDATE     : Account Lock Date.
#    LOGINSTAT    : Login Status.
#
#  [ for Client Certificate Option Define ]
#    RASERIALNO   : RA Serial Number.
#    IWSERIALNO   : Certificate Serial Number.
#    CERTEXPDATE  : Certificate Expiration Date.
#    GETCERT      : Client Certificate Regist/Download Switch.
#    ONLINE       : Certificate Login Status.
#----------------------------------------------------------------------------
UID=USERID
PASSWORD=PASSWD
PWDEXPDATE=PASSWDEXP
PWDHISTORY=PASSWDHIS
PCHGOK=PASSCHANGE
PCHGDATE=CHGDATE
PLOGINDATE=LOGONDATE
LLOGINDATE=LASTDATE
FLOGINDATE=LOGONFAIL
PWDRETRY=FAILCOUNT
PWDLOCK=LOCKOUT
LOGINOK=LOGONSTOP
LOCKDATE=LOCKDATE
LOGINSTAT=LOGSTATUS
#RASERIALNO=RASERIAL
#IWSERIALNO=BSSERIAL
#CERTEXPDATE=VDATE
#GETCERT=CERT
#ONLINE=APENABLE
```

MySQL edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 16:47 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ Authentication Database Table's Column Info ]
#    UID          : UserID.
#    PASSWORD     : Password.
#    PWDEXPDATE   : Password Expiration Date.
#    PWDHISTORY  : Password History.
#    PCHGOK      : Password Change OK/NG.
#    PCHGDATE    : Password Change Date.
#    PLOGINDATE  : Login Date.
#    LLOGINDATE  : Last Login Date.
#    FLOGINDATE  : Login Failure Date.
#    PWDRETRY    : Password Retry Count.
#    PWDLOCK     : Account Lock ON/OFF.
#    LOGINOK     : Login OK/NG.
#    LOCKDATE    : Account Lock Date.
#    LOGINSTAT   : Login Status.
#
#  [ for Client Certificate Option Define ]
#    RASERIALNO  : RA Serial Number.
#    IWSERIALNO  : Certificate Serial Number.
#    CERTEXPDATE : Certificate Expiration Date.
#    GETCERT     : Client Certificate Regist/Download Switch.
#    ONLINE      : Certificate Login Status.
#-----------------------------------------------------------------------------
UID=USERID
PASSWORD=PASSWD
PWDEXPDATE=PASSWDEXP
PWDHISTORY=PASSWDHIS
PCHGOK=PASSCHANGE
PCHGDATE=CHGDATE
PLOGINDATE=LOGONDATE
LLOGINDATE=LASTDATE
FLOGINDATE=LOGONFAIL
PWDRETRY=FAILCOUNT
PWDLOCK=LOCKOUT
LOGINOK=LOGONSTOP
LOCKDATE=LOCKDATE
LOGINSTAT=LOGSTATUS
#RASERIALNO=RASERIAL
#IWSERIALNO=BSSERIAL
#CERTEXPDATE=VDATE
#GETCERT=CERT
#ONLINE=APENABLE
```

3.7.3 Group configuration file (cert.grp)

ORACLE edition

```
#-----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.grp $ $Revision: 1 $ $Date: 10/03/27 15:35 $
#-----------------------------------------------------------------------------
#-----------------------------------------------------------------------------
#  [ User's Group Info ]
#   [GroupName],[Database Column Name]=[Value or Regular Expression]
#              ,REMOTE_ADDR=[IP Address]
#              ,REMOTE_ADDR=[IP Address]-[IP Address]
#
#   Possible Operators: |[or],&[and],![not],(,)
#-----------------------------------------------------------------------------
ALL,USERID=user01
SccOnly,USERID=user02
HpOnly,USERID=user03
## GRP Configuration Start
```

LDAP edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.grp $ $Revision: 1 $ $Date: 10/03/27 16:02 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ User's Group Info ]
#   [GroupName],[Database Column Name]=[Value or Regular Expression]
#             ,REMOTE_ADDR=[IP Address]
#             ,REMOTE_ADDR=[IP Address]-[IP Address]
#
#   Possible Operators: |[or],&[and],![not],(,)
#----------------------------------------------------------------------------
ALL,uid=user01
SccOnly,uid=user02
HpOnly,uid=user03
## GRP Configuration Start
```

OpenLDAP edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.grp $ $Revision: 1 $ $Date: 10/03/27 19:35 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ User's Group Info ]
#   [GroupName],[Database Column Name]=[Value or Regular Expression]
#             ,REMOTE_ADDR=[IP Address]
#             ,REMOTE_ADDR=[IP Address]-[IP Address]
#
#   Possible Operators: |[or],&[and],![not],(,)
#----------------------------------------------------------------------------
ALL,uid=user01
SccOnly,uid=user02
HpOnly,uid=user03
## GRP Configuration Start
```

MSAD edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.grp $ $Revision: 3 $ $Date: 10/03/27 17:00 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ User's Group Info ]
#   [GroupName],[Database Column Name]=[Value or Regular Expression]
#             ,REMOTE_ADDR=[IP Address]
#             ,REMOTE_ADDR=[IP Address]-[IP Address]
#
#   Possible Operators: |[or],&[and],![not],(,)
#----------------------------------------------------------------------------
ALL,CN=user01
SccOnly,CN=user02
HpOnly,CN=user03
## GRP Configuration Start
```

NED edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.grp $ $Revision: 1 $ $Date: 10/03/27 18:22 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ User's Group Info ]
#   [GroupName],[Database Column Name]=[Value or Regular Expression]
#            ,REMOTE_ADDR=[IP Address]
#            ,REMOTE_ADDR=[IP Address]-[IP Address]
#
#   Possible Operators: |[or],&[and],![not],(,)
#----------------------------------------------------------------------------
ALL,cn=user01
SccOnly,cn=user02
HpOnly,cn=user03
## GRP Configuration Start
```

CSV edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.grp $ $Revision: 1 $ $Date: 10/03/27 15:10 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ User's Group Info ]
#   [GroupName],[Database Column Name]=[Value or Regular Expression]
#            ,REMOTE_ADDR=[IP Address]
#            ,REMOTE_ADDR=[IP Address]-[IP Address]
#
#   Possible Operators: |[or],&[and],![not],(,)
#----------------------------------------------------------------------------
ALL,USERID=user01
SccOnly,USERID=user02
HpOnly,USERID=user03
## GRP Configuration Start
```

MySQL edition

```
#----------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: cert.grp $ $Revision: 1 $ $Date: 10/03/27 16:47 $
#----------------------------------------------------------------------------
#----------------------------------------------------------------------------
#  [ User's Group Info ]
#   [GroupName],[Database Column Name]=[Value or Regular Expression]
#            ,REMOTE_ADDR=[IP Address]
#            ,REMOTE_ADDR=[IP Address]-[IP Address]
#
#   Possible Operators: |[or],&[and],![not],(,)
#----------------------------------------------------------------------------
ALL,USERID=user01
SccOnly,USERID=user02
HpOnly,USERID=user03
## GRP Configuration Start
```

3.7.4 Access control file (cert.acl)

```
#---------------------------------------------------------------------------
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: cert.acl $ $Revision: 1 $ $Date: 10/03/27 15:35 $
#---------------------------------------------------------------------------
#---------------------------------------------------------------------------
# [ Access Control Info ]
#  [URL]=[Group Name(defined in cert.grp)]
#
#  Possible Operators: |[or],&[and],![not],(,)
#---------------------------------------------------------------------------
http://www.scc-kk.co.jp/=ALL|SccOnly
http://welcome.hp.com/=ALL|HpOnly
http://localhost/=ALL|SccOnly|HpOnly
http://[host name]:[port number]/=ALL|SccOnly|HpOnly
## ACL Configuration Start
```

Specify the host name and port number of the web server that will display the Sample Menu page for [host name] and [port].

3.7.5 Request control configuration file (request.acl)

```
#---------------------------------------------------------------------------
# IceWall SSO 10.0 Configuration File for Certification Module.
# $Workfile: request.acl $ $Revision: 1 $ $Date: 10/03/27 16:47 $
#---------------------------------------------------------------------------
#---------------------------------------------------------------------------
# [ Request Control Info ]
#   TARGET=[Client Environment Name]=[Value or Regular Expression]
#         SOURCE_ADDR=[IP Address]
#         SOURCE_ADDR=[IP Address]-[IP Address]
#   {
#   VERSION=[1.0|2.0]
#   REJECT=[LOGINUID|FLOGINUID|LOGINCERT|FLOGINCERT|ACCESSUID
|ACCESSCERT|
#          PWDCHG|LOGOUT|ALL]
#   SEND=[Database Column Name]
#       [IW_UID] (IPC2.0 Only)
#       [IW_PWD] (ICP2.0 Only)
#       [Client Environment Name] (ICP2.0 Only)
#   NOTSEND=[Database Column Name]
#          [IW_UID] (IPC2.0 Only)
#          [IW_PWD] (ICP2.0 Only)
#          [Client Environment Name] (ICP2.0 Only)
#   ACCCTRL=[UID|CERT|CERTNOUID]
#   }
#---------------------------------------------------------------------------
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
NOTSEND=IW_UID,IW_PWD
}
```

```
TARGET=SOURCE_ADDR=192.168.0.40&AGENT_ID=IceWall SSO DFW
{
REJECT=FLOGINUID,FLOGINCERT
}

## REQUEST ACL Configuration Start
```

3.8 Sample Menu page

This is the source code for the Sample Menu page. This source code is not in the install package. To use this source code, create a file referring to the source code below.

3.8.1 Sample Menu page (index.html)

```
<html>
<head>
<title>Sample Menu</title>
<meta http-equiv="Content-Type" content="text/html; charset=x-sjis">
<meta http-equiv="Pragma"      content="no-cache">

<style type="text/css">
<!--
BODY, TD {
   font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
   font-size: 12px;
}
a:link   {
   color: #333333;
   text-decoration: none;
}
a:visited   {
   color: #666666;
   text-decoration: none;
}
a:hover   {
   color: #ff3300;
   text-decoration: underline;
}
.title   {
   font-size: 18px;
   font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
}
.sub-title   {
   font-size: 16px;
   font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
   line-height: 18px;
}
.sub-title2   {
   font-size: 14px;
   font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
}
.footer   {
   font-size: 11px;
   font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
}
```

```
-->
</style>

</head>

<body bgcolor="#ffffff" text="#000000" link="#333333" vlink="#666666"
 alink="#ff3300" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">

<table border="0" width="100%" height="98%" cellpadding="0" cellspacing="0">
  <tr>
    <td width="195" height="80" bgcolor="#336699" valign="top" class="title"
     nowrap>&nbsp;
    </td>
    <td width="15" bgcolor="#6699cc" rowspan="2" nowrap>
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#6699cc" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="15" bgcolor="#99ccff" rowspan="2" nowrap>
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#99ccff" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="100%" height="100%" valign="top" rowspan="2">
      <table border="0" width="100%" cellspacing="0" cellpadding="0">
        <tr>
          <td width="100%" height="50" align="left"
           class="sub-title">&nbsp;<b>Sample Menu</b> </td>
        </tr>
        <tr>
          <td height="15" bgcolor="#e6e6e6" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td height="15" bgcolor="#99ccff" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td height="70" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td align="center" nowrap>
            <table border="0" height="100%" cellspacing="0" cellpadding="0">
              <tr>
                <td width="240" height="100%" nowrap>
<!-- Menu Button -->
<table border="0">
  <tr><td>
    <table border="0" width="220" height="22" cellpadding="0" cellspacing="0">
      <tr><td bgcolor="#333333" nowrap>
        <table border="0" width="220" height="22" cellpadding="3" cellspacing="1">
          <tr>
            <td width="15" bgcolor="#3399cc" align="center" nowrap>
              <table border="0" width="15" height="5" cellpadding="0"
               cellspacing="0">
                <tr>
                  <td width="15" height="5" bgcolor="#3399cc" nowrap>&nbsp;</td>
                </tr>
              </table>
            </td>
```

```
-->
</style>

</head>

<body bgcolor="#ffffff" text="#000000" link="#333333" vlink="#666666"
 alink="#ff3300" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">

<table border="0" width="100%" height="98%" cellpadding="0" cellspacing="0">
  <tr>
    <td width="195" height="80" bgcolor="#336699" valign="top" class="title"
     nowrap>&nbsp;
    </td>
    <td width="15" bgcolor="#6699cc" rowspan="2" nowrap>
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#6699cc" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="15" bgcolor="#99ccff" rowspan="2" nowrap>
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#99ccff" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="100%" height="100%" valign="top" rowspan="2">
      <table border="0" width="100%" cellspacing="0" cellpadding="0">
        <tr>
          <td width="100%" height="50" align="left"
           class="sub-title">&nbsp;<b>Sample Menu</b> </td>
        </tr>
        <tr>
          <td height="15" bgcolor="#e6e6e6" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td height="15" bgcolor="#99ccff" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td height="70" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td align="center" nowrap>
            <table border="0" height="100%" cellspacing="0" cellpadding="0">
              <tr>
                <td width="240" height="100%" nowrap>
<!-- Menu Button -->
<table border="0">
  <tr><td>
    <table border="0" width="220" height="22" cellpadding="0" cellspacing="0">
      <tr><td bgcolor="#333333" nowrap>
        <table border="0" width="220" height="22" cellpadding="3" cellspacing="1">
          <tr>
            <td width="15" bgcolor="#3399cc" align="center" nowrap>
              <table border="0" width="15" height="5" cellpadding="0"
               cellspacing="0">
                <tr>
                  <td width="15" height="5" bgcolor="#3399cc" nowrap>&nbsp;</td>
                </tr>
              </table>
            </td>
```

```
-->
</style>

</head>

<body bgcolor="#ffffff" text="#000000" link="#333333" vlink="#666666"
 alink="#ff3300" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">

<table border="0" width="100%" height="98%" cellpadding="0" cellspacing="0">
  <tr>
    <td width="195" height="80" bgcolor="#336699" valign="top" class="title"
     nowrap>&nbsp;
    </td>
    <td width="15" bgcolor="#6699cc" rowspan="2" nowrap>
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#6699cc" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="15" bgcolor="#99ccff" rowspan="2" nowrap>
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#99ccff" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="100%" height="100%" valign="top" rowspan="2">
      <table border="0" width="100%" cellspacing="0" cellpadding="0">
        <tr>
          <td width="100%" height="50" align="left"
           class="sub-title">&nbsp;<b>Sample Menu</b> </td>
        </tr>
        <tr>
          <td height="15" bgcolor="#e6e6e6" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td height="15" bgcolor="#99ccff" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td height="70" nowrap>&nbsp;</td>
        </tr>
        <tr>
          <td align="center" nowrap>
            <table border="0" height="100%" cellspacing="0" cellpadding="0">
              <tr>
                <td width="240" height="100%" nowrap>
<!-- Menu Button -->
<table border="0">
  <tr><td>
    <table border="0" width="220" height="22" cellpadding="0" cellspacing="0">
      <tr><td bgcolor="#333333" nowrap>
        <table border="0" width="220" height="22" cellpadding="3" cellspacing="1">
          <tr>
            <td width="15" bgcolor="#3399cc" align="center" nowrap>
              <table border="0" width="15" height="5" cellpadding="0"
               cellspacing="0">
                <tr>
                  <td width="15" height="5" bgcolor="#3399cc" nowrap>&nbsp;</td>
                </tr>
              </table>
            </td>
            <td width="205" bgcolor="#ffffff" nowrap>
              &nbsp;<A HREF="http://welcome.hp.com/country/jp/jpn/welcome.htm">
              <b>Hewlett-Packard Japan</b></A>
            </td>
          </tr>
        </table>
      </td></tr>
    </table><br><p>
  </td></tr>
  <tr><td>
    <table border="0" width="220" height="22" cellpadding="0" cellspacing="0">
      <tr><td bgcolor="#333333" nowrap>
        <table border="0" width="220" height="22" cellpadding="3" cellspacing="1">
          <tr>
            <td width="15" bgcolor="#3399cc" align="center" nowrap>
              <table border="0" width="15" height="5" cellpadding="0"
               cellspacing="0">
                <tr>
                  <td width="15" height="5" bgcolor="#3399CC" nowrap>&nbsp;</td>
                </tr>
              </table>
            </td>
            <td width="205" bgcolor="#ffffff" nowrap>
              &nbsp;<A HREF="http://www.scc-kk.co.jp/"><b>SCC Japan</b></A>
            </td>
          </tr>
        </table>
      </td></tr>
    </table><br><p>
  </td></tr>
  <tr><td>
    <table border="0" width="220" height="22" cellpadding="0" cellspacing="0">
      <tr><td bgcolor="#333333" nowrap>
        <table border="0" width="220" height="22" cellpadding="3" cellspacing="1">
          <tr>
            <td width="15" bgcolor="#ff6666" align="center" nowrap>
              <table border="0" width="15" height="5" cellpadding="0"
               cellspacing="0">
                <tr>
                  <td width="15" height="5" bgcolor="#ff6666" nowrap>&nbsp;</td>
                </tr>
              </table>
            </td>
            <td width="205" bgcolor="#ffffff" nowrap>
              &nbsp;<b><a href="$DFW/IW-PWDCHG">Change password</a></b>
            </td>
          </tr>
        </table>
      </td></tr>
    </table><br><p>
  </td></tr>
  <tr><td>
    <form method="POST" target="_top" action="$DFW">
      <input type="hidden" name="LOGOUT" value="ICEWALL_LOGOUT">
      <input type="submit" name="submit" value="Logout">
    </form>
  </td></tr>
</table>
                </td>
              </tr>
            </table>
          </td>
        </tr>
      </table>
    </td>
    <td width="15" height="100%" bgcolor="#99ccff" rowspan="2" nowrap>
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#99ccff" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="15" nowrap bgcolor="#6699cc" rowspan="2">
      <table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="15" height="5" bgcolor="#6699cc" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
    <td width="30" bgcolor="#336699" rowspan="2" nowrap>
      <table border="0" width="30" height="5" cellpadding="0" cellspacing="0">
        <tr>
          <td width="30" height="5" bgcolor="#336699" nowrap>&nbsp;</td>
        </tr>
      </table>
    </td>
  </tr>
  <tr>
    <td width="195" height="100%" bgcolor="#336699" align="left" valign="top"
     nowrap>&nbsp;</td>
  </tr>
</table>

</body>
</html>
```

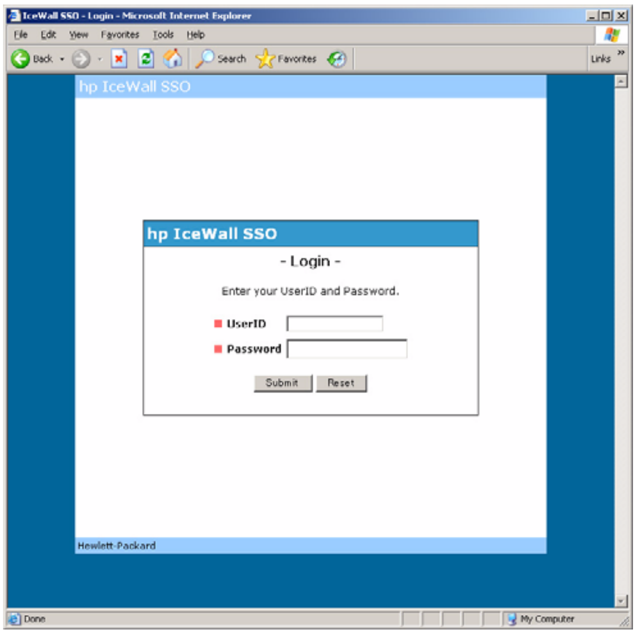
4 Using the Sample

You can view the IceWall SSO sample login page and experience the access privileges for each login user by configuring the server up to this point and performing the operating procedures below.
If you wish to log in again as a different user while operating the sample, log out from the Sample Menu page or close all browsers. While logged in, the Sample Menu page for the authenticated user is displayed without showing the login page, even if the URL below is entered.

(1) Open the browser and specify the URL below to display the sample login page. (fw is the CGI prefix defined in “3.1 Configure the web server to run Forwarder.”)

```
http://[host name]/fw/dfw/SAMPLEMENU/menu/index.html
```

Note: Specify the configured IceWall server name or IP address for the [host name] portion.
In the configuration example, the Sample Menu page is placed in a location that can be accessed at “http://[host name]:[port number]/menu/index.html” on the Backend Web Server.



IceWall SSO - Login - Microsoft Internet Explorer

hp IceWall SSO

- Login -

Enter your UserID and Password.

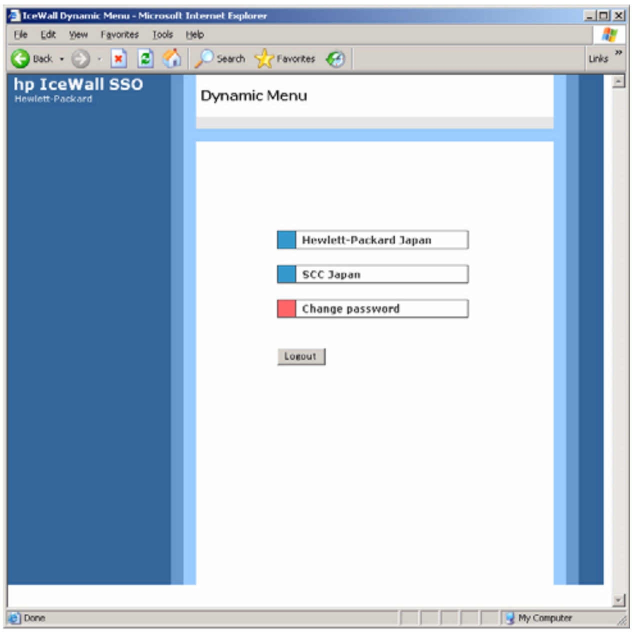
UserID

Password

Sample login page

(2) Log in with a user name (user01) and password (user01) on the sample login page. The following page appears when you are logged in.

For the user "user01", both "Hewlett-Packard Japan" and "SCC Japan" that are displayed can be accessed.

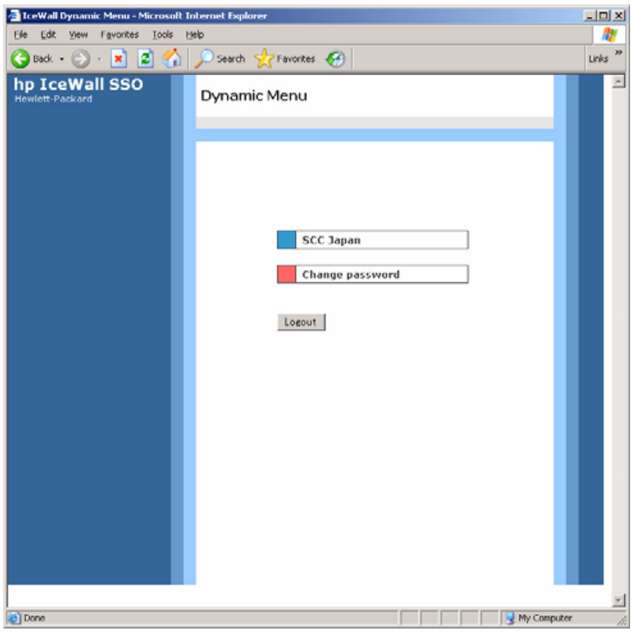


Sample Menu page

Note: If the IceWall server is not connected to the Internet, the "Hewlett-Packard Japan" and "SCC Japan" websites will not be displayed, even when the respective buttons are clicked.

(3) Next, log in with the user user02. Log out and then display the sample login page again with step (1). Log in with a user name (user02) and password (user02).

The user “user02” has no access privilege to “Hewlett-Packard Japan,” so when the “Hewlett-Package Japan” button on the Sample Menu page is clicked, the access privilege error page is displayed.


IceWall Dynamic Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Links
hp IceWall SSO
Hewlett-Packard
Dynamic Menu
SCC Japan
Change password
Logout
Done
My Computer

Access privilege error page

(4) Finally, log in with the user “user03”. Log out and then display the sample login page again with step (1). Log in with a user name (user03) and password (user03).

The user “user03” has no access privilege to “SCC Japan,” so when the “SCC Japan” button on the Sample Menu page is clicked, the access privilege error page is displayed.

The above is a simple IceWall operation using the sample.
For details on how to use IceWall and an explanation of its functions, see the “IceWall SSO User's Manual” and the “IceWall SSO Reference Manual.”