IceWall SSO

Version 10.0

Installation Guide for Client Certificates Option

August 2010

Printed in Japan

HP Part No. B1544-97005

Rev.111007A

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.

– Table of Contents –

1 Introduction

The Client Certificates Option ensures secure and reliable identification between the client and IceWall server by using a client certificate.

Note: If using the Microsoft Active Directory as the Authentication DB, you cannot use this option.

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 to the version enclosed in the square. In this case, the designation indicates the item was added to 10.0.
(10.0)	An item where the specification was changed or function added to the version enclosed in the oval mark. In this case, the designation indicates a specification change or function addition to 10.0.

1.2 Terminology

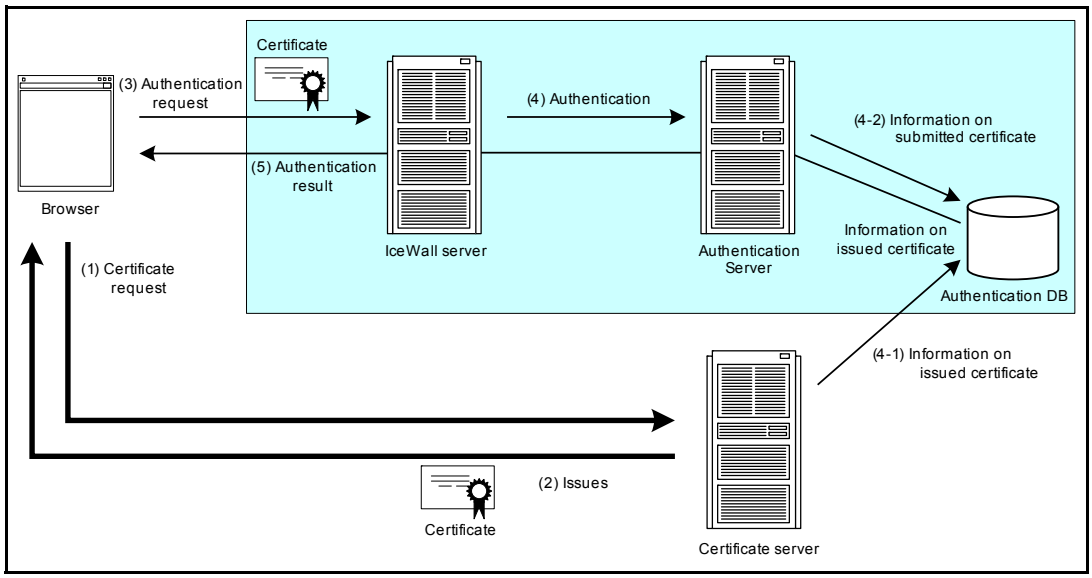
The following terminology is used in the text.

Terminology	Meaning
ORACLE edition	Oracle Database 11g 10.0
LDAP edition	Sun Java System Directory Server
	Netscape Directory Server
	Red Hat Directory Server
OpenLDAP edition	OpenLDAP
NED edition	Novell eDirectory
MySQL edition	MySQL Server
MSAD edition	Microsoft Active Directory
	Microsoft Active Directory Lightweight Directory Services
Apache	Apache HTTP Server
	HP-UX Apache-Based Web Server

2 System Overview for Installing Client Certificates Option

This chapter describes the system components and processing flow for installing the Client Certificates Option.

2.1 System components and processing flow



(1) The client requests the issue of a certificate.
(2) The certificate issuing server issues a certificate and saves its information in the Authentication DB. The issued certificate is installed on the client browser.
(3) An authentication request is submitted with a certificate to IceWall SSO. The certificate presented by the IceWall server is decoded to acquire the information required for authentication.
(4) The acquired certificate information is sent to the Authentication Server for authentication.
  (4-1) The issued certificate information saved in the Authentication DB is acquired and certificate validity check is performed.
  (4-2) When the certificate is authenticated, the presented certificate information is saved in the Authentication DB.
  * The authentication performed for the first time after a certificate is issued is called “initial authentication.” The authentication performed for the first time using an updated certificate is called “initial authentication after update.”
(5) The client browser is notified of the authentication result by the IceWall server.

2.2 Restriction on user authentication

When the client certificate is used, the following restrictions are applied to user authentication.

(1) Browser
A user can log in from any client when authentication is based on the user ID. On the other hand, when a certificate is used for authentication, the certificate must be installed on the browser (or external medium).

(2) Authentication based on the user ID after using a certificate
Once a user has been authenticated by a certificate, he or she is prohibited from using the user ID for authentication (hereinafter called user ID authentication) instead of the certificate. (You can disable this restriction via configuration.)

(3) Validity of certificate after update
The certificate used for user authentication is valid only for a single generation (i.e., only the current certificate is valid). However, after a certificate is updated, the user can be authenticated with the current certificate until authentication is performed using the updated certificate.

(4) Characters available for certificate information
The following restrictions are applied to characters available for cn and ou.

Area name	Available characters (* Single-byte characters only)
cn	Alphanumeric - .
ou	Alphanumeric - . _

Note that a period (.) cannot be used at the end.

3 Certificate Information to be Saved in the Authentication DB

The Client Certificates Option needs to save the certificate information in the Authentication DB for validating the identity of the client certificate. The following lists the types of information to be saved at different timings.

3.1 When the certificate is issued and updated

When a client certificated is issued and updated, the certificate information must be saved in the Authentication DB. The information to be saved includes the following: (Information is saved automatically by the certificate issuing server or manually by the administrator.)

Data name	Description
Serial number when certificate is issued	The serial number (X.509 area name is "SerialNumber") and issuer name (X.509 area name is "Issuer") of the issued client certificate are combined into unique certificate information and saved in the Authentication DB. This information is saved in the format "serial number:issuer name."
Issuer name when certificate is issued	

3.2 When the user is authenticated

When the user is initially authenticated after the client certificate is issued or updated, the certificate information is saved in the Authentication DB by the Authentication Module. The saved certificate information includes the following: (The information is saved by IceWall SSO.)

Data name	Description
Serial number when certificate is presented	The serial number (X.509 area name is "SerialNumber") and issuer name (X.509 area name is "Issuer") acquired from the certificate presented by the browser are compared with the corresponding values saved in the Authentication DB when the certificated was issued, and if they match, the data saved in the authentication database is copied and saved. The data format is "serial number:issuer name."
Issuer name when certificate is presented	
Certificate expiration date	The expiration date (X.509 area name is "Validity") of the certificate presented by the browser is saved. The data format is "YYYYMMDDhhmmss."
Certificate issue flag	The issue status of the certificate is saved. 0: Certificate has been issued. 1: Certificate has not been issued. 2: Certificate has been issued, but not used.

Data name	Description
Certificate usage flag	The usage of the certificate is saved. 0: Initial authentication not performed with certificate. 1: Initial authentication performed with certificate.

4 Configuration Method

Configure the Client Certificates Option with the procedure described below. IceWall SSO must be already installed and running normally.
Note that you do not need to additionally install the IceWall SSO module.

4.1 Additional configuration of Web server

To the Web server configuration file on the IceWall server, add commands to request the client certificate from the Web server to the browser.

4.1.1 Configuring Apache

Configure the Web server configuration file (ssl.conf for Apache 2.x) as shown below.

If VirtualHost operating in SSL is set to <VirtualHost_default_:443> edit the file as shown in the following configuration example:

```
<VirtualHost _default_:443>
      :
   SSLCACertificatePath /opt/hpws/apache/
   SSLCACertificateFile /opt/hpws/apache/cacert.pem
   SSLVerifyClient 2
   SSLVerifyDepth 10
      :
   <Directory "/opt/icewall-sso/dfw/cgi-bin">
      :
      SSLOptions +StdEnvVars +ExportCertData
      :
   </Directory>
</VirtualHost>
```

The values to be set depend on the environment. For details on these settings, see the manual of the Web server.

4.2 Expanding the Authentication DB

Prepare the Authentication DB columns (i.e., attributes) to save the client certificate information.

The columns (attributes) for the “serial number when certificate is issued” and the “serial number when certificate is presented” stores the serial number and issuer of the certificate. Although the following description uses “256” for each size, determine the actual size by confirming the data sizes of the serial number and issuer name of the certificate used.

* In ORACLE and MySQL editions, tables must be created after adding the necessary columns. When adding columns to existing tables, see the manual of each database product.

4.2.1 ORACLE edition

Add the following columns to the Authentication DB columns.
Authentication table (SQL: Add to the cre_tbl_test.sql file.)

RASERIAL	varchar(256)	NULL,
BSSERIAL	varchar(256)	NULL,
VDATE	char(14)	NULL,
CERT	char(1)	DEFAULT 1 NOT NULL,
APENABLE	char(1)	DEFAULT 0 NOT NULL

* When adding a column to the cre_tbl_test.sql file, note that parameters are separated by commas and that no comma is required after the last parameter.

Log output table (SQL: Add to the cre_tbl_history.sql file.)

RASERIAL	varchar(256)

4.2.2 NED, LDAP, MSAD, and OpenLADP editions

Determine the attributes of the Authentication DB according to the following table.

Intended use	Type	Size	Description
Serial number when certificate is issued	Character type	256	Stores the serial number and issuer name of the certificate issued by the certificate issuing server.
Serial number when certificate is presented	Character type	256	Stores the serial number and issuer name of the certificate presented by the browser.
Certificate expiration date	Character type	14	Stores the expiration date of the certificate presented by the browser.
Certificate issue flag	Character type	1	Stores the issue flag of the certificate.
Certificate usage flag	Character type	1	Stores the certificate usage flag.

* Either create new attributes or use the standard attributes provided by the Directory Server.

4.2.3 CSV edition

Add the following parameters to the text Authentication DB columns.

```
RASERIAL,BSSERIAL,VDATE,CERT,APENABLE
```

4.2.4 MySQL edition

Add the following columns to the table of the Authentication DB.
Authentication table (SQL: Add to the cre_tbl_test.sql file.)

```
RASERIAL    varchar(256)    NULL,
BSSERIAL    varchar(256)    NULL,
VDATE       char(14)        NULL,
CERT        char(1)         DEFAULT 1 NOT NULL,
APENABLE    char(1)         DEFAULT 0 NOT NULL
```

* When adding a column to the cre_tbl_test.sql file, note that parameters are separated by commas and that no comma is required after the last parameter.

4.3 Expanding the Authentication DB configuration of the Authentication Module

Add the client certificate column information to the Authentication DB column information file of the Authentication Module (/opt/icewall-sso/certd/config/dbattr.conf).

Add the following parameters.

Parameter name	Mandatory	Description
RASERIALNO	○	Specifies the column name for storing the serial number and issuer name of the certificate saved by the certificated issuing server.
IWSERIALNO	○	Specifies the column name for storing the serial number and issuer name of the certificate presented by the browser.
CERTEXPDATE	○	Specifies the column name for storing the expiration date of the certificate presented by the browser.
GETCERT	×	Specifies the column name for storing the certificate issue flag.
ONLINE	×	Specifies the column name for storing the certificate usage flag.

4.3.1 ORACLE, CSV, and MySQL editions

Attributes to be added to the Authentication DB column information file (dbattr.conf) (example)

```
RASERIALNO=RASERIAL
IWSERIALNO=BSSERIAL
CERTEXPDATE=VDATE
GETCERT=CERT
ONLINE=APENABLE
```

4.3.2 NED, LDAP, MSAD, and OpenLADP editions

Attributes to be added to the Authentication DB column information file (dbattr.conf) (example)

```
RASERIALNO=destinationIndicator
IWSERIALNO=preferredDeliveryMethod
CERTEXPDATE=x500UniqueIdentifier
GETCERT=registeredAddress
ONLINE=teltexTerminalIdentifier
```

* This example specifies standard attributes provided by Sun Java System Directory Server.

4.4 Expanding the Authentication Module log column configuration file

When the log is output to the history database in the ORACLE edition, you need to add column parameters for the certificate to the Authentication Module log column configuration file (/opt/icewall-sso/certd/config/logdbattr.conf).

Add the following parameters.

Parameter name	Mandatory	Description
SERIAL	○	Specifies the column name for storing the serial number and issuer name of the certificate saved when the certificate was issued.

Attributes added to the log column configuration file (logdbattr.conf) (example)

```
SERIAL=RASERIAL
```

4.5 Operation settings when using the certificate in Authentication Module

You can add the following parameters to the Authentication Module configuration file (cert.conf) and the request control configuration file (request.acl).

For details on how to configure each parameter and the configuration examples, see the “IceWall SSO Reference Manual.”

Authentication Module configuration file (cert.conf)

Parameter name	Mandatory	Description
PARALOGIN	×	Sets whether or not to allow login using the user ID after initial authentication using the client certificate.
ACCCTRLFLG	×	Sets the access control security level when using a client certificate.

Request control configuration file (request.acl)

Parameter name	Mandatory	Description
ACCCTRL	×	Sets control by access type regardless of the login type such as login by user ID and password or login by a client certificate and password.

4.6 Operation settings when using the certificate in Forwarder

You can add the following parameters to the Forwarder configuration file (dfw.conf) and host configuration file (any name).
For details on how to configure each parameter and the configuration examples, see the “IceWall SSO Reference Manual.”

Forwarder configuration file (dfw.conf)

Parameter name	Mandatory	Description
CC_UID	○	Sets the name of the area for acquiring the user ID from the client certificate.
CC_UIDKEYS	×	Sets the string for specifying the start position for acquiring the user ID from the user ID storage area of the client certificate.
CC_UIDKEYE	×	Sets the string for specifying the end position for acquiring the user ID from the user ID storage area of the client certificate. •The length of the search string is not limited. •If no search string is specified, characters up to the end of the CC_UID parameter are regarded as the user ID. •No default value is provided.
CC_ENVNAME	×	Sets the name of the environment variable for obtaining the client certificate information.

Parameter name	Mandatory	Description
CC_DECODE_FLG	×	Turns on/off Forwarder decoding of the client certificate.
CC_ENVUID	×	Sets the name of the environment variable that contains the user ID from the client certificate information.
CC_ENVSERIAL	×	Sets the name of the environment variable that contains the serial number from the client certificate information.
CC_ENVEXPIRE	×	Sets the name of the environment variable that contains the expiration date information from the client certificate information.
CC_ENVISSUER	×	Sets the name of the environment variable that contains the certificate issuer information from the client certificate information.

Host configuration file (arbitrary file name)

Parameter name	Mandatory	Description
HEADER	×	Set to send the certificate data from the client certificate to the certificate issuing server. * Required when issuing the client certificate online.

4.7 Adding parameters to HTML configuration of Forwarder

Add the following parameters to the HTML configuration file of the Forwarder (html.conf):

Parameter name	Mandatory	Description
LOGIN_CERT	×	Specifies the login page for logging in with the client certificate.
LOGIN_ERR_1ST CERT	×	Specifies the initial authenticated error page when the initial authentication using the client certificate has already been performed.
LOGIN_ERR_SERIAL	×	Specifies the serial number error page when logging in with the client certificate.

* These settings have already been configured upon installation.

4.8 Restarting a process

After adding parameters to the configuration files as directed above, restart the following processes.
- Web server instance of the IceWall server
- Authentication Module

Note: The IceWall server must have the server certificate as well as the Trusted Certificate Authority certificate installed on it, and must be able to communicate using SSL3.0.

4.9 When using the SSL accelerator function of load balancer

When a load balancer is placed between the browser and IceWall server and the "SSL accelerator function" is used, the load balancer checks the SSL connection and client certificate.
In this configuration, the connection between the load balancer and IceWall server is made using HTTP.
The IceWall SSO version 8.0.1 (8.0R1) or later allows for using the Client Certificates Option in such a configuration.

4.9.1 Prerequisites for the SSL accelerator function

When using the SSL accelerator function, the client certificate must be decoded by the load balancer and the following information stored in the certificate basic area must be sent to IceWall SSO with an HTTP header.
- Value of the area including the user ID (value of the Subject area, etc.)
- Serial number (value of the SerialNumber area)
- Certificate expiration date (value of the notAfter area)
- Issuer name (value of the Issuer area)

4.9.2 Configuring the Forwarder

Configure the Forwarder as follows to obtain the information sent with the HTTP header from the client certificate.

Forwarder configuration file (dfw.conf)

```
DFW_PROTOCOL=1
CC_DECODE_FLG=0
CC_ENVUID=[Environmental variable from which the user ID can be acquired]
CC_ENVSERIAL=[Environmental variable from which the serial number can be acquired]
CC_ENVEXPIRE=[Environmental variable from which the expiration date can be acquired]
CC_ENVISSUER=[Environmental variable from which the issuer name can be acquired]
```

The DFW_PROTOCOL parameter allows the Forwarder to operate as it does with an SSL connection even when the SSL accelerator of the load balancer is used.
The CC_DECODE_FLG parameter is used to obtain each type of information separately from the client certificate. If this parameter is not set, various types of information cannot be obtained separately from the client certificate.
If the user ID is not the only information to be acquired from the environment variable specified in the CC_ENVUID parameter, use the CC_UIDKEYS and CC_UIDKEYE parameters to acquire the required information.

Also, if you use the SSL accelerator function of the load balancer, the configuration mentioned in “4.1 Additional configuration of Web server” is not required.

5 Expanding the UserExit Routine

Installing Client Certificates Option partially expands the UserExit routine to allow the following process:

•Login process

(1) It can be determined if login is based on user ID or on a certificate.
(2) A “initial authenticated error” can be generated forcibly.
(3) A “certificate serial number error” can be generated forcibly.

For details on the expanded functionality, see the “IceWall SSO UserExit Routine Developer's Manual.”

6 Configuration Examples

The following describes the configuration examples of the Authentication DB column information file (dbattr.conf) and log column configuration file (logdbattr.conf).

6.1 Configuration example of the Authentication DB column information 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=RASERIAL
CERTEXPDATE=VDATE
GETCERT=CERT
ONLINE=APENABLE
```

6.2 Configuration example of the Authentication DB column information file (dbattr.conf) (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
```

6.3 Configuration example of the Authentication DB column information file (dbattr.conf) (OpenLDAP edition)

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

6.4 Configuration example of the Authentication DB column information file (dbattr.conf) (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
```

6.5 Configuration example of the Authentication DB column information file (dbattr.conf) (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
```

6.6 Configuration example of the Authentication DB column information file (dbattr.conf) (CSV edition)

```
#-------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: dbattr.conf $ $Revision: 1 $ $Date: 10/03/27 15:10 $
#-------------------------------------------------------------------------
#-------------------------------------------------------------------------
#  [ 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
```

6.7 Configuration example of the Authentication DB column information file (dbattr.conf) (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
```

6.8 Configuration example of the log column configuration file (logdbattr.conf) (ORACLE edition only)

```
#-------------------------------------------------------------------------
#  IceWall SSO 10.0 Configuration File for Certification Module.
#  $Workfile: logdbattr.conf $ $Revision: 1 $ $Date: 10/03/27 15:35 $
#-------------------------------------------------------------------------
#-------------------------------------------------------------------------
#  [ Access Log Database Table's Column Info ]
#    NO    : Sequential Numer of Log.
#    TIME  : Output Time of Log.
#    UID   : UserID.
#    KIND  : Kind of Log Message.
#    RESULT: Proccess Result Code.
#    MSG   : Log Message.
#    CLIP  : IP Address of Client.
#-------------------------------------------------------------------------
NO=UKENO
TIME=UKEDATE
UID=USERID
KIND=KIND
RESULT=RESCODE
MSG=MESSAGE
CLIP=IPADDR
```