IceWall SSO

Version 10.0

Installation Guide
for HP-UX

August 2010

<p style="text-align:center">− Table of Contents −</p>

1   Introduction

This guide contains information about the installation and configuration of IceWall SSO.

1.1   Version designations in respective items

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

Designation	Meaning
10.0	Item added in the version enclosed in a square. In this case, the designation indicates the item was added with 10.0.
10.0	Specification modified or functions added in the version enclosed in an oval. In this case, the designation indicates a specification change or added function with 10.0.

2   System Requirements

The following sections provide system requirements for IceWall SSO. See the Hewlett-Packard Japan website (http://www.hp.com/jp/icewall/) for the latest information.

2.1   System requirements for Forwarder (dfw)

- Server
  HP Integrity server

- OS
HP-UX 11i v3 (Itanium) [10.0] [*1]
*1 HP-UX 11i v3 with Standard Patch Bundle dated March 2009 or later must be installed.

- Web server
  For HP-UX 11i v3 (Itanium)
    HP-UX Apache-based Web Server v2.2.8 and later versions [10.0] [*2]

*2 Only packages provided by the OS vendors are supported. Customer-compiled packages are not supported.
- Notes
  1. Development of UserExit routines is supported for Enterprise Edition only. For Standard Edition, you need to purchase an SE Forwarder upgrade License to support this functionality.

2.2   System requirements for the Authentication Module (certd)

- Server
  HP Integrity server

- OS
  HP-UX 11i v3 (Itanium) [*3]

*3 HP-UX 11i v3 with Standard Patch Bundle dated March 2009 or later must be installed.

- Database (Authentication DB)
  Oracle Database 11g Release 1 Standard Edition (Oracle Net required) [10.0]
  Oracle Database 11g Release 1 Enterprise Edition (Oracle Net required) [10.0]
  Oracle Database 11g Release 2 Standard Edition (Oracle Net required) [10.0]
  Oracle Database 11g Release 2 Enterprise Edition (Oracle Net required) [10.0]
  Sun Java System Directory Server 7.0 [10.0]
  Novell eDirectory Server 8.8 and later versions
  HP Directory Server 8.1 [10.0]
  Microsoft Active Directory (Microsoft Windows Server 2008) [10.0]
  Microsoft Active Directory (Microsoft Windows Server 2008 SP2) [10.0]
  Microsoft Active Directory (Microsoft Windows Server 2008 R2) [10.0]
  Microsoft Active Directory Lightweight Directory Services
  (Microsoft Windows Server 2008)

Microsoft Active Directory Lightweight Directory Services
(Microsoft Windows Server 2008 SP2)
Microsoft Active Directory Lightweight Directory Services
(Microsoft Windows Server 2008 R2)
Text Authentication DB file (CSV format)

• Notes
   1. If the Authentication DB is Oracle, Oracle Net Services is required. In this case, only the
      following combinations are supported:

Database	Client
Oracle Database 11g Release 1 Standard Edition	Oracle Net R11.1.0
Oracle Database 11g Release 1 Enterprise Edition	Oracle Net R11.1.0
Oracle Database 11g Release 2 Standard Edition	Oracle Net R11.2.0
Oracle Database 11g Release 2 Enterprise Edition	Oracle Net R11.2.0

   2. The following restrictions apply if the Authentication DB is Microsoft Active Directory:
      • The password history save function is not supported.
      • Checking of the password expiration date during user authentication is not available.

   3. The following restrictions apply if Authentication DB is CSV:
      • Failover option is not available.

   4. Check if the value for the kernel parameter maxdsiz_64bit is sufficient. Although the
      Authentication Module supports more than 2 GB of memory allocation, the size of the
      allocated memory cannot exceed the value specified in maxdsiz_64bit. It is necessary to set
      the value of the kernel parameter maxdsiz_64bit to a value that is greater than that of the
      memory capacity to be allocated. See the HP-UX manual for more information on how to set
      the kernel parameters.

   5. Development of UserExit routines is supported for Enterprise Edition only. For Standard
      Edition, you need to purchase SE User Certification Server upgrade License to support this
      functionality.

2.3 Other Topics

• Browser
  See the following URL for the latest list of tested and verified browsers.
  http://h50146.www5.hp.com/products/software/security/icewall/sso/spec/browser.html

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

Terminology	Corresponding products
Apache	HP-UX Apache-based Web Server v2.2.8
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 Enterprise Edition
LDAP	Sun Java System Directory Server 7.0
	HP Directory Server 8.1
NED	Novell eDirectory 8.8
	Novell eDirectory 8.8.1
MSAD	Microsoft Active Directory
	Microsoft Active Directory Lightweight Directory Services
CSV	Text Authentication DB file

3　Installation

For the IceWall SSO, you need to install each module separately.
Before installation, make sure that none of the modules is installed. (You cannot overwrite the existing module. If there is a previous installation present in the system, it must first be uninstalled.)

Follow these steps to check your system.

(1) Log in as root user to the server where the installation takes place.

(2) Enter the following command:

```
# swlist | grep "IceWall"
```

(3) If the module you want to install is displayed, uninstall it.

For the installation method of each optional product, see their respective installation guides.

3.1　Installing the Forwarder

Follow these steps for installation.

(1) Log in as root user to the server where the installation takes place.

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

(3) Enter the following command to check the device file name for the CD-ROM drive.

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

(4) Enter the following command to mount the CD-ROM.

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

Example: Device file name: "/dev/dsk/c1t2d0," mount point: "SD_CDROM"
　　# mount /dev/dsk/c1t2d0 /SD_CDROM
(If there is no mount point directory of SD_CDROM, create one with the mkdir command.)

(5) Enter the following command to install the module.

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

(6) Use the following command to confirm that it is installed.

```
# swlist dfw
```

(7) Enter the following command to change the owner of the directories and files related to the Forwarder to the user executing the web server. In the following example, the execution user of the web server is www:other.

```
# chown -R www:other /opt/icewall-sso/dfw
```

(8) Configure the Forwarder in the web server. The Forwarder requires that environment variable for the library search path, the CGI path, and the document path. See the following configuration example(s) used to display samples (These are the example configuration(s) to display samples.)

For Apache HTTP Server
① Edit the Apache configuration file (httpd.conf).
<Example for modifying httpd.conf>

```
Alias /img/ "/opt/icewall-sso/dfw/html/image/"

ScriptAlias /fw/ "/opt/icewall-sso/dfw/cgi-bin/"

<Directory "/opt/icewall-sso/dfw/html/image">
  Order allow,deny
  Allow from all
</Directory>

<Directory "/opt/icewall-sso/dfw/cgi-bin">
  AllowOverride None
  Options None
  Order allow,deny
  Allow from all
  SetEnv SHLIB_PATH "/opt/icewall-sso/lib/dfw:/usr/lib/hpux64"
</Directory>
```

② Restart Apache.

Apache displays a list of the files within the directory by default; change this so as not to display the list of files.

3.2 Installing the Authentication Module

Follow these steps for installation.

(1) Log in as root user to the server where the installation takes place.

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

(3) Enter the following command to check the CD-ROM drive's device file name.

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

(4) Enter the following command to mount the CD-ROM.

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

Example: Device file name: "/dev/dsk/c1t2d0," mount point: "SD_CDROM"
   # mount /dev/dsk/c1t2d0 /SD_CDROM
(If there is no SD_CDROM directory, create one with the mkdir command.)

(5) Select the name of the target Authentication DB for use and enter the following command to install the Authentication Module.

```
#  swinstall  -s  /SD_CDROM/hpux/IceWall-SSO-ia64_e.sw  [target
name]
```

Authentication DB	Target name	Remarks
Oracle11g	certd_oracle1110	K
LDAP	certd_ldap	
NED	certd_ned	
MSAD	certd_msad	
CSV	certd_csv	

(6) Use the following command to confirm that it is installed.

```
# swlist [target name]
```

Installation package	Target name
Oracle11g edition	certd_oracle1110 K
LDAP edition	certd_ldap
NED edition	certd_ned
MSAD edition	certd_msad

Installation package	Target name
CSV edition	certd_csv

(7) Create a user for executing the Authentication Module using SMH. k

Parameter name	Value
Login Name	iwadmin
Primary Group Name	users
Home Directory	Any
Login Shell (Startup Program)	Any (POSIX shell (/usr/bin/sh) is recommended)

(8) Modify the settings for the Authentication Module commands.
  If ORACLE is used as the Authentication DB, modify the following files.
  (There is no need for modification if LDAP, NED, MSAD, CSV is used.)
    /opt/icewall-sso/certd/bin/start-cert
    /opt/icewall-sso/certd/bin/end-cert
    /opt/icewall-sso/certd/bin/info-cert
    /opt/icewall-sso/certd/bin/reload-cert
    /opt/icewall-sso/certd/bin/logout-cert
    /opt/icewall-sso/certd/bin/cdump-cert

  For example, the start-cert for Oracle11g is the following:

```
#!/bin/sh

export ORACLE_HOME=/home/oracle/app/oracle/product/11.1.0/client_1
export IW_HOME=/opt/icewall-sso
export SHLIB_PATH=$ORACLE_HOME/lib:$IW_HOME/lib/certd
export LD_LIBRARY_PATH=$SHLIB_PATH
export TWO_TASK=ORCL

$IW_HOME/certd/bin/certd -c $IW_HOME/certd/config/cert.conf
```

  Change "ORACLE_HOME" to the name of the directory in which Oracle products are installed. The directory name to be set is displayed for the Oracle user with the following command:

```
$ env | grep ORACLE_HOME
```

  Change SHLIB_PATH to the set descriptions in the example above.
  Set TWO_TASK to the connect identifier for the database.

(9) Modify the settings for the startup command.
The following shows the modified startup command:

```
#!/bin/sh

export IW_HOME=/opt/icewall-sso
export SHLIB_PATH=$IW_HOME/lib/certd
export LD_LIBRARY_PATH=$SHLIB_PATH
export PTHREAD_MUTEX_SPINVAL=old

$IW_HOME/certd/bin/certd -c $IW_HOME/certd/config/cert.conf
```

(10) Change the owner of the directories and files related to the Authentication Module to the user created in (7).

Example for the command to be used:

```
#chown -R iwadmin:users /opt/icewall-sso/certd
```

3.3   Configuration after installation

After installation, perform the following settings to run IceWall SSO.

3.3.1   Configuring encryption libraries

When installing the Authentication Module, the following password encryption library is installed

Library name	Intended use
libiwPwdHash.sl	Password encryption library

Depending on the database used, PWDLOGINHASH and PWDCHGHASH paramters in the Authentication Module configuration file (cert.conf) may need to be changed.
For details, see "IceWall SSO Reference Manual."

3.3.2   Configuring password for LDAP server

The user password encryption algorithm can be specified arbitrarily; however, when using a library **other than SHA** in the LDAP edition, set the password encryption of the LDAP server instance to ClearText (non-encryption).

3.3.3   Configuring the Authentication Module for automatic startup

To start up the Authentication Module automatically using the startup script for init:
• Use sleep within the automatic startup script until the Authentication Module starts up.
• Set trap in the startup command of the Authentication Module (start-cert) to ignore the signal SIGHUP.
The following is an example of an automatic startup script:

```
#!/sbin/sh
#
#         Copyright I 2002-2007, Hewlett-Packard Development Company, L.P.
#
# NOTE:   This script is not configurable!  Any changes made to this
#          script will be overwritten when you upgrade to the next
#          release of IceWall.
#
#

IW_HOME=/opt/icewall-sso

rval=0
set_return() {
        x=$?
        if [ $x -ne 0 ]; then
                echo "EXIT CODE: $x"
                rval=1  # always 1 so that 2 can be used for other reasons
        fi
}



case $1 in
start_msg)
        echo "Starting IceWall Certification Server Version 10.0 "
        ;;

stop_msg)
        echo "Stopping IceWall Certification Server Version 10.0 "
        ;;

'start')
        echo "¥n#### Start ${IW_HOME}/bin/certd ####"

        cd $IW_HOME/certd/bin
        if [ -f $IW_HOME/certd/bin/certd.pid ] ; then
                ./end-cert
                /usr/bin/rm -f $IW_HOME/certd/bin/certd.pid
        fi

        /usr/bin/su iwadmin ./start-cert >> /tmp/icewallstart.log
        /usr/bin/sleep 60
        /usr/bin/ps -ef | /usr/bin/grep certd >> /tmp/icewallstart.log

       exit 0;
       ;;
```

```
'stop')
        echo "¥n#### Stop ${IW_HOME}/bin/certd ####"
        for certdir in $IW_HOME/certd; do
            cd $certdir/bin
            ./end-cert
        done
        set_return
        ;;

*)
        echo "usage: $0 {start|stop}"
        rval=1
        ;;
esac

exit $rval
```

The following is an example of a startup command (start-cert) for the Authentication Module:
(ORACLE edition)

```
#!/bin/sh

export ORACLE_HOME=/home/oracle/app/oracle/product/11.1.0/
client_1
export IW_HOME=/opt/icewall-sso
export SHLIB_PATH=$ORACLE_HOME/lib:/usr/lib
export LD_LIBRARY_PATH=$SHLIB_PATH
export TWO_TASK=ORCL
export PTHREAD_MUTEX_SPINVAL=old

trap "" 1

$IW_HOME/certd/bin/certd -c $IW_HOME/certd/config/cert.conf
```

3.4   Recommended configurations

Although not essential for operating IceWall SSO, there are some recommended settings:

3.4.1   Configuring timeout value for FIN_WAIT_2 (a common setting for both IceWall server and the Authentication Server)

Perform the following settings as root user. Set the timeout value appropriate for your system environment.

(1) Open /etc/rc.config.d/nddconf in the text editor.

```
# vi /etc/rc.config.d/nddconf
```

(2) Add the following lines: (in this example, the timeout value is set to 180 seconds)

TRANSPORT_NAME[n]=tcp
NDD_NAME[n]=tcp_fin_wait_2_timeout
NDD_VALUE[n]=180000
∗ Set the index value for [n].

(3) Save /etc/rc.config.d/nddconf.

(4) Enter the following command to apply changed values.

```
# ndd -c
```

(5) Execute the following command to verify that the changes have been reflected:

```
# ndd -get /dev/tcp tcp_fin_wait_2_timeout
```

3.4.2   Configuring Keep-Alive of a web server instance

Set the Keep-Alive configuration of the Backend Web Server instance to OFF. If the Backend Web Server is a Microsoft Internet Information Services server, it is recommended to set the Keep-Alive configuration of the web server instance to ON. If the setting is OFF, even if the contents had been displayed, the connection is not disconnected until the Forwarder times out, and the browser falls into a state where the web server seems to continue sending data.

3.4.3   Setting the SSLSessionCache when using SSL connection

If the Backend Web Server is Apache HTTP Server, and SSL connection are used, configure Apache so that shared memory is used with the SSLSessionCache directive. Without this setting, the performance may deteriorate.

4   Uninstallation

Each IceWall SSO module is uninstalled separately, just like the installation.

4.1   Uninstalling the Forwarder

Follow these steps for uninstallation.

(1) Log in as root user to the server where the uninstallation takes place.

(2) Stop the web server.

(3) Delete the setting that runs the Forwarder from the web server configuration file.

(4) Enter the following command to uninstall.

```
# swremove dfw
```

4.2   Uninstalling the Authentication Module

Follow these steps for uninstallation.

(1) Log in as root user to the server where the uninstallation takes place.

(2) Use the following command to stop the Authentication Module when it is running.

```
# /opt/icewall-sso/certd/bin/end-cert
```

(3) Enter the following command to uninstall. Select the target name from the following.

```
# swremove [target name]
```

Installation package	Target name
Oracle11g	certd_oracle1110 **10.0**
LDAP edition	certd_ldap
NED edition	certd_ned
MSAD edition	certd_msad
CSV edition	certd_csv

5   Verification of Installation

The following three steps should be taken to verify the proper installation of IceWall SSO.

5.1   Quick verification on modules

For each of the installed modules, perform the relevant verification steps that are described in this chapter.

5.1.1   Verifying the Forwarder

Verify the operational state of the Forwarder using a user on the web server. Here the web server user should be www. After logging in as root user, follow these steps to verify the Forwarder: (As the configuration file is assumed to be in the current directory, the steps below should be followed.)

```
$ su - www
$ cd /opt/iceawll-sso/dfw/cgi-bin/
$ env SHLIB_PATH=/opt/icewall-sso/lib/dfw HTTP_HOST=localhost ./
dfw
```

Check if the following output is displayed.

```
<html>
<head>
<title>IceWall SSO - No Alias Error</title>
<meta http-equiv="Content-Type" content="text/html;charset=ISO-8859-1">
<meta http-equiv="Pragma"        content="no-cache">

<style type="text/css">
<!--
BODY, TD {
    font-family: Verdana, Arial, Helvetica, Sans-serif;
    font-size: 12px;
}
a:hover     {
    color: #ff3300;
    text-decoration: underline;
}
.title    {
    font-size: 18px;
    font-family: Verdana, Arial, Helvetica, Sans-serif;
}
```

```
.sub-title    {
    font-size: 16px;
    font-family: Verdana, Arial, Helvetica, Sans-serif;
    line-height: 18px;
}
.sub-title2    {
    font-size: 14px;
    font-family: Verdana, Arial, Helvetica, Sans-serif;
}
.footer    {
    font-size: 11px;
    font-family: Verdana, Arial, Helvetica, Sans-serif;
}
-->
</style>

</head>

<body bgcolor="#006699" text="#000000" link="#336699" alink="#ff3300"
topmargin="0" marginheight="0">

<center>
<table border="0" width="80%" height="92%" bgcolor="#ffffff"
cellpadding="0" cellspacing="0">
  <tr>
    <td height="28" align="center">
      <table border="0" width="100%" height="28" cellpadding="1"
cellspacing="0">
        <tr>
          <td bgcolor="#99ccff"><img src="/img/header.gif" width="150"
height="28"></td>
        </tr>
      </table>
    </td>
  </tr>
  <tr>
    <td height="100%" align="center">
      <table border="0" width="420" cellpadding="0" cellspacing="0">
        <tr bgcolor="#cc3333">
          <td width="18" height="35"><img src="/img/curve_r.gif" width="18"
height="35"></td>
          <td width="175" height="35"><img src="/img/title_r.gif"
width="175" height="35"></td>
          <td width="227" height="35" align="right"><font color="#ffffff"> ■
</font> </td>
        </tr>
      </table>
      <table border="0" width="420" cellpadding="0" cellspacing="0">
        <tr>
          <td bgcolor="#666666">
            <table border="0" width="420" cellpadding="3" cellspacing="1">
              <tr>
                <td height="180" bgcolor="#ffffff" align="center">
                  <div class="sub-title"><b>- No Alias Error -</b></div><br>
                   <img src="/img/error.gif" width="180" height="50"
alt="ERROR">
                   <p><div class="sub-title2"><b>Analias was not specified</
b></div>
                </td>
```

```
            </tr>
          </table>
        </td>
      </tr>
    </table>
  </td>
</tr>
<tr>
  <td height="15" align="center">
    <table border="0" width="100%" height="15" cellpadding="1"
cellspacing="0">
      <tr>
        <td bgcolor="#99ccff"><img src="/img/footer.gif" width="100"
height="15"></td>
      </tr>
    </table>
  </td>
</tr>
</table>
</center>

</body>
</html>
```

5.1.2 Verifying the Authentication Module

Execute the startup command (start-cert) as an iwadmin user to start up the Authentication Module.

```
$ /opt/icewall-sso/certd/bin/start-cert
```

Note: Before taking these steps, check if you can access the Authentication DB with SQL*Plus, ldapsearch, or ice commands.

After executing the startup command (start-cert), enter the following command to see if the Authentication Module is running.

```
$ ps -ef | grep certd
```

If it is not running, an error may have occurred. Check the error log file (/opt/icewall-sso/logs/ certerr.log).

5.2 Verification by displaying the sample pages

To verify overall IceWall SSO system operation, it is recommended that you check to see if the sample pages is displayed by configuring the Authentication DB and web server in accordance with the "IceWall SSO Sample Setup Guide."
For details, refer to the "IceWall SSO Sample Setup Guide."

5.3 Verifying installed files

Each package file is installed in the directory under /opt/icewall-sso, but the installed files differ depending on the type of module to be installed. After installation, verify the file structure under the /opt/icewall-sso directory.

5.3.1 Forwarder package

Directory and file names (permission)			
/dfw(775)	/cgi-bin(775)	dfw(755) dfw.conf(644) sample.conf(644) html.conf(644) chtml.conf(644) form.conf(644) autologin.html(644) iw_postdata.html(644)	
	/chtml(755)	/image(755)	i-error.gif(444) i-line.gif(444) i-logout.gif(444) i-title.gif(444)
		access_error.html(644) datasend_error.html(644) filter_get_error.html(644) filter_html_error.html(644) filter_post_error.html(644) filter_request_error.html(644) `10.0` filter_svr_error.html(644) login.html(644) login_force.html(644) login_group_error.html(644) login_limit_error.html(644) login_lock_error.html(644) login_postlimit_error.html(644) `10.0` login_pwd_error.html(644) login_stop.html(644) login_userid_error.html(644) logout.html(644) logout_error.html(644) logout_no.html(644) logout_ok.html(644) max_postsize_err.html(644) pwdchg.html(644) pwdchg_err.html(644) pwdchg_nologin.html(644) pwdchg_ok.html(644) pwdchg_oldpasserr.html(644) pwdchg_policy_err.html(644) pwdchg_postlimit_err.html(644) `10.0` pwdchg_pwvioerr.html(644) pwdchg_repasserr.html(644) pwdchg_warning.html(644) request_acl_error.html(644) `10.0` system_alias_error.html(644) system_backend_error.html(644) system_busy_database.html(644) `10.0` system_certd_error.html(644) system_error.html(644)	

Directory and file names (permission)			
			system_ldap_error.html(644)
			system_server_error.html(644)
			system_timeout_bkend.html(644)
			system_timeout_certd.html(644)
			usr_ext1.html(644)
			usr_ext2.html(644)
			usr_ext3.html(644)
			usr_ext4.html(644)
			usr_ext5.html(644)
			usr_ext6.html(644)
/dfw(775)	/html(755)	/image(755)	arrow.gif(444)
			arrow2.gif(444)
			curve_b.gif(444)
			curve_r.gif(444)
			error.gif(444)
			footer.gif(444)
			header.gif(444)
			title_b.gif(444)
			title_r.gif(444)
		access_error.html(644)	
		datasend_error.html(644)	
		filter_get_error.html(644)	
		filter_html_error.html(644)	
		filter_post_error.html(644)	
		filter_request_error.html(644) 10.0	
		filter_svr_error.html(644)	
		login.html(644)	
		login_cert.html(644)	
		login_cert_error.html(644)	
		login_error.html(644)	
		login_force.html(644)	
		login_group_error.html(644)	
		login_limit_error.html(644)	
		login_lock_error.html(644)	
		login_postlimit_error.html(644) 10.0	
		login_pwd_error.html(644)	
		login_stop.html(644)	
		login_userid_error.html(644)	
		logout.html(644)	
		logout_error.html(644)	
		logout_no.html(644)	
		logout_ok.html(644)	
		max_postsize_err.html(644)	
		pwdchg.html(644)	
		pwdchg_err.html(644)	
		pwdchg_nologin.html(644)	
		pwdchg_ok.html(644)	
		pwdchg_oldpasserr.html(644)	
		pwdchg_policy_err.html(644)	
		pwdchg_postlimit_err.html(644) 10.0	
		pwdchg_pwvioerr.html(644)	
		pwdchg_repasserr.html(644)	
		pwdchg_warning.html(644)	
		request_acl_error.html(644) 10.0	
		system_alias_error.html(644)	
		system_backend_error.html(644)	
		system_busy_database.html(644) 10.0	
		system_certd_error.html(644)	
		system_error.html(644)	
		system_ldap_error.html(644)	
		system_server_error.html(644)	
		system_timeout_bkend.html(644)	

Directory and file names (permission)			
		system_timeout_certd.html(644) usr_ext1.html(644) usr_ext2.html(644) usr_ext3.html(644) usr_ext4.html(644) usr_ext5.html(644) usr_ext6.html(644)	
/iwpmd(775)	/bin(775)	iwpmd(755) iwpmdd(755)	
	/conf(775)	iwpmd.conf(644)	
	/data(775)		
	/run(775)		
	/script(775)	iwpmd_analyselog.pl(755) iwpmd_calcaverage_perf.pl(755) iwpmd_count_errlog.pl(755) iwpmd_printdata_perf.pl(755) iwpmd_printdata_screen.pl(755) iwpmd_printheader_perf.pl(755)	
	/tmp(775)		
/lib(555)	/dfw(555)	libDfwExit.so(755) * Link libsidcrypto.so(755) * Link libssl.so(755) * Link libcrypto.so(755) * Link libCryptoExit.so(755) * Link	
	libDfwExit.sl(555) libsidcrypto.sl(555) libDfwCryptoExit.sl(555)		
/logs(777)			
/messages(555)	/C(555)	icewall_dfw.cat(444)	
/developkit(775) [10.0]	/dfw(755)	/DfwExit(755)	Makefile(644) dfwinterface.c(644) dfwinterface.h(444)
		/DfwCryptoExit (755)	Makefile(644) iwcrypto.c(644) iwcrypto.h(444) libcpt.a(444)

5.3.2 Authentication Module package

Directory and file names (permission)		
/certd(775)	/bin(775)	certd(755) logout-cert(755) [10.0] cdump-cert(755) [10.0] start-cert(755) end-cert(755) info-cert(755) reload-cert(755)
	/config(775)	cert.conf(644) cert.grp(644) cert.acl(644) dbattr.conf(644) logdbattr.conf (644) * For ORACLE edition only pwdforbid.conf(644) request.acl(644) sample.csv(644) * For CSV edition only

Directory and file names (permission)			
/iwpmc(775)	/bin(775)	iwpmc(755) iwpmcd(755)	
	/conf(775)	iwpmc.conf(644)	
	/data(775)		
	/run(775)		
	/script(775)	iwpmc_analyselog.pl(755) iwpmc_calcavarage_info.pl(755) iwpmc_calcavarage_perf.pl(755) iwpmc_printdata_info.pl(755) iwpmc_printdata_perf.pl(755) iwpmc_printdata_screen.pl(755) iwpmc_printheader_info.pl(755) iwpmc_printheader_perf.pl(755)	
	/tmp(775)		
/lib(555)	/certd(555)	libDB.so(755)　　　　　　　 * Link libPH.so(755)　　　　　　　 * Link, libCertExit.so(755)　　　　　 * Link libCryptoExit.so(755)　　　　 * Link libExCryptoExit.so(755)　　　 * Link libCreateSidExit.so(755)　　　 * Link libiwDBCrypto.so(755)　　　　 * Link libiwDBCryptoExit.so(755)　　 * Link libssl.so(755)　　　　　　　 * Link libcrypto.so(755)　　　　　　 * Link liblber.so(755)　　　　　　　 * Link 　　　　　　　　　　　 For LDAP, NED, MSAD edition only libldap.so(755)　　　　　　　 * Link 　　　　　　　　　　　 For LDAP, NED, MSAD edition only libsasl2.so(755)　　　　　　 * Link 　　　　　　　　　　　 For LDAP, NED, MSAD edition only	
	libCertExit.sl(555) libCryptoExit.sl(555) libExCryptoExit.sl(555) libiwORA1110.sl(555)　　* For ORACLE edition only [10.0] libiwLDAP.sl(555)　　　* For LDAP, MSAD, NED edition only libiwCSV.sl(555)　　　　* For CSV edition only libiwPwdHash.sl(555)　　[10.0] liblber.sl(555)　　　　　* For LDAP, MSAD, NED edition only libldap.sl(555)　　　　　* For LDAP, MSAD, NED edition only libsasl2.sl(555)　　　　　* For LDAP, MSAD, NED edition only libiwDBCrypto.sl(555)　　[10.0] libiwDBCryptoExit.sl(555)　[10.0]		
/lib32(555) *Except MSAD edition	/mkuser(555) *Except MSAD edition	libcrypto.so(755)　　　　 * Link 　　　　　　　　　　 Except MSAD edition	
/logs(777)			
/messages(555)	/C(555)	icewall_certd.cat(444) ⑩.⓪	
/developkit(775) [10.0]	/certd(755) [10.0]	/CertExit(755)	Makefile(644) iwintface.c(644) iwintface.h(444)

Directory and file names (permission)			
		/PwdLib(755)	Makefile(644) iwphash.c(644) iwphash.h(444)
		/CryptoExit(755)	Makefile(644) iwcrypto.c(644) iwcrypto.h(444) libcpt.a(444)
		/ExCryptoExit(755)	Makefile(644) csexicpcrypto.c(644) csexicpcrypto.h(444) iwcrypto.h(444) libcpt.a(444)
		/SidExit(755)	Makefile(644) iwcreatesid.c(644) iwcreatesid.h(444)
		/DBCryptoExit(755)	Makefile(644) csexdbcrypto.c(644) csexdbcrypto.h(444)
/sample_src(775)	/ICP20(755)	/sample1(755)	Makefile(644) Sample1.java(644) sample1.c(644)
		/sample2(755)	Makefile(644) Sample2.java(644) sample2.c(644)
		/agent(755)	Makefile(644) mod_sample.c(644)
/tools(775) *Except MSAD version	mkuser(755) mkuser.seed(644) TEMPLATE.sql(644) TEMPLATE.ldif(644) TEMPLATE.csv(644) add_test_user.sql(644) cre_sequence.sql(644) cre_tbl_history.sql(644) cre_tbl_test.sql(644) DATA.txt(644)	* Except MSAD edition * Except MSAD edition * For ORACLE edition only * For LDAP, MSAD edition only * For CSV edition only * For ORACLE edition only * For ORACLE edition only * For ORACLE edition only * For ORACLE edition only * Except MSAD edition	

5.4   Verifying version information

After installation, verify that the binary of this version is installed. This information is necessary when contacting technical support for troubleshooting.

5.4.1   Verifying version information for Forwarder

Follow these steps to verify version information for Forwarder.

(1) Move to a directory where a binary file is located:

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

(2) Enter the following command:

```
# what dfw
```

(3) The following information is displayed:
The displayed information may vary depending on the OS and the processor.

Example: Command output for HP-UX 11i v3

```
dfw:
    Version: 10.00.00.xxxxxxX
    OS : HP-UX B.11.23
    CPU: Itanium
    Bit: 64bit
    (c) Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
    IceWall SSO dfw
```

5.4.2　Verifying version information for Authentication Module

For the Authentication Module, you need to verify version information for two modules: the binary of the main component for the Authentication Module and the Authentication DB connection library. Follow these steps to find the version information.

<The binary for Authentication Module main component>
(1) Move to a directory where a binary file is located:

```
# cd /opt/icewall-sso/certd/bin
```

(2) Enter the following command:

```
# what certd
```

(3) The following information is displayed.

Example: Command output for HP-UX 11i v3

```
certd:
    IceWall SSO certd
    Version: 10.00.00.xxxxxxX
    OS : HP-UX B.11.23
    CPU: Itanium
    Bit: 64bit
    (c)Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
```

<Authentication DB connection library>
(1) Move to a directory where a binary file is located:

```
# cd /opt/icewall-sso/lib/certd
```

(2) Enter the following command:

```
# what libDB.so
```

(3) The following information is displayed.
    The displayed information may vary depending on the Authentication DB.

Example: Oracle11g version (Itanium version)

```
libDB.so:
   IceWall SSO Database Plug-in Oracle 11.1.0.6.0
   Version: 10.00.00.xxxxxxX
   OS : HP-UX B.11.23
   CPU: Itanium
   Bit: 64bit
   (c) Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
```

6   Upgrading from Previous Versions

Follow the steps provided in the section below to upgrade to this version from a previous version.
*   **Note that upgrading using a method other than the one that uses the following steps, such as replacing only partial binary files, is not supported.**

6.1   Upgrade procedure

Follow these steps to upgrade to this product.

(1) Stop the web server on the IceWall server.
(2) Stop the Authentication Module on the Authentication Server.
(3) Back up the configuration files for the IceWall server and Authentication Server that are currently in use.
(4) If you are using the IceWall server and the Authentication Server with your own programs, such as a privately developed UserExit or password encryption library, back up those programs.
(5) If you need to keep the IceWall server and Authentication Server log files, back up those files.
(6) When upgrading from versions prior to 8.0, delete the symbolic links of the libraries that were configured under the /usr/lib directory while the existing version was being installed.
When upgrading from 8.0 or later versions, go to step (7).
(7) Uninstall the previous version of IceWall. See the "IceWall SSO Installation Guide" of the previous version for information about the uninstallation procedure.
(8) Install this version.
(9) If any libraries were backed up in (4), restore them under the /opt/icewall-sso/lib directory. On the Authentication Server, if you are using the password encryption library other than the default library, change the link to the library. (However, you cannot use the libraries from the previous version without any modification. Refer to the considerations section later in this chapter.)
(10) Restore the configuration files backed up in (3).
(11) If you are using a listen port number that is different from the default, edit the Authentication Module commands (end-cert, reload-cert, info-cert, logout-cert, cdump-cert) so that they have that port number.

The upgrade should now be completed.
Since backwards compatibility is guaranteed for the IceWall SSO configuration files, you can use those files from the previous version without any modification.
* However, regular expressions become default for the forbidden password configuration file, resulting in partial matches. To make complete matches as before, you must enclose the front and back of the forbidden password with a caret [^] and a dollar sign [$].

6.2 Common considerations for previous versions

There are certain points that should be kept in mind for all previous versions when an upgrade is being performed.

(1) If you have added any instructions (codes) to the Authentication Module commands (start-cert, end-cert, reload-cert, info-cert, logout-cert, cdump-cert), you will need to add those codes to the Authentication Module commands for this version, as well.

(2) Since the default value for the CTYPE parameter was changed to "None," the following parameter must be added to the host configuration file.
CTYPE=text/html

(3) If you used a privately developed UserExit routine in previous versions, you will need to rebuild the routine.

(4) If you used a privately developed password encryption library in previous versions, you will need to rebuild the routine.

(5) The module bit count from this version is 64 bits. If the 32-bit runtime libraries are specified in versions before 8.0 R3, you will need to ensure that the 64-bit runtime libraries are specified when upgrading. ⟨**10.0**⟩

(6) When Forwarder uses the alias "LOCALHOST" and the host name "localhost" and the port number "80" that are being kept fixed as the internal host setting, set the following parameter at the top of the HOST parameter in the Forwarder configuration file.
HOST=LOCALHOST=localhost:80 ⟨**10.0**⟩

(7) The number of digits for the three times that are output in the access log has changed from milliseconds (1/1000) to microseconds (1/1000000). Please be aware when using these times for monitoring and other purposes. ⟨**10.0**⟩

(8) Libraries have been merged so MD5, SHA1, SHA256, PLAIN, and multiple hashes can be handled with one password encryption library. Set the PWDLOGINHASH parameter in the Authentication Module configuration file (cert.conf) to the hash in the Authentication DB. ⟨**10.0**⟩

(9) Please note the items below when the encryption library (libiwPMHO.sl) was used with pre-fix-less MD5 in previous versions. ⟨**10.0**⟩
  • Notes when using the password change function
    If the password is changed by the password change function, the prefix {MD5} is added when the new password is stored in the Authentication DB. Therefore, expand the data size for the Authentication DB column (attribute) to 37 bytes.
  • Setting the hashing method when logging in
    When login does not use BIND authentication, set PWDLOGINHASH to AUTO-MD5.
    When login uses BIND authentication, set PWDLOGINHASH to MD5.

(10) The message output by the operating information output command (info-cert) has been changed. For details, see the "IceWall SSO User's Manual." ⎡**10.0**⎤

(11) When set to generate session IDs 64 bytes long, the length of the session ID retrieved by UserExit must accommodate a length of 64 bytes. ⎡**10.0**⎤

(12) The message catalog file name has been changed. For details, see the CATALOG configuration parameter for the Forwarder configuration file and the Authentication Module configuration file in the "IceWall SSO Reference Manual." ⎡**10.0**⎤

(13) Starting with this version, the settings related to the password policy have been moved from Forwarder to the Authentication Module. The settings in Forwarder are valid as they have been in previous versions, but we recommend moving the settings to the Authentication Module side.
If you upgrade with the settings related to the password policy configured unchanged on the Forwarder side, the initial values on the Authentication Module side may become valid. In this situation, configure the Authentication Module side to the same settings as the Forwarder side. ⎡**10.0**⎤

6.3   Common considerations for version 8.0 or earlier

There are certain points that should be kept in mind for all previous versions earlier than 10.0 when performing an upgrade.

(1) The library structure is changed. In the previous versions the necessary links were created under /usr/lib, but now all the links are moved under /opt/icewall-sso/lib/dfw and /opt/icewall-sso/lib/certd. See "5.3 Verifying installed files" for details.
The configuration of the web server running the Forwarder need to be changed. For details, see "3.1 Installing the Forwarder (8)."

6.4   Version-specific upgrade considerations

Various functions have been added and specifications modified for previous versions of IceWall SSO. Therefore, considerations are different for each version.

6.4.1 Upgrading from 4.0

- The If-modified-since header is forwarded to the Backend Web Server. When running based on the old specification, add the following setting to the host configuration file.
    HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND
- The specification for UserExit routine of Authentication Module has changed. It is necessary to edit the source code for the UserExit routine.
- If the client certificates option is used, the serial number and the Issuer are stored into the columns of both the certificate issue serial number and the received serial number, so it is necessary to extend the column sizes.

6.4.2 Upgrading from 5.0i, 5.0iSP1 and 5.1i

- The specification for UserExit routine of Authentication Module has changed. It is necessary to edit the source code for the UserExit routine.
- The If-modified-since header is forwarded to the Backend Web Server. When running based on the old specification, add the following setting to the host configuration file.
  HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND

6.4.3 Upgrading from 5.1iSP1 and 5.1iSP2

- The specification for UserExit routine of Authentication Module has changed. It is necessary to edit the source code for the UserExit routine.
- The If-modified-since header is forwarded to the Backend Web Server. When running based on the old specification, add the following setting to the host configuration file.
    HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND
- If the Authentication DB is MSAD, add the following parameter to the configuration file for Authentication Module.
    LDAPBIND=1
    LDAPPCHG=0
    LDAPLANG=0

6.4.4 Upgrading from 6.0, 6.0SP1 and 6.0.1SE

- The specification for UserExit routine of Authentication Module has changed. It is necessary to edit the source code for the UserExit routine.
- The If-modified-since header is forwarded to the Backend Web Server. When running based on the old specification, add the following setting to the host configuration file.
    HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND
- If the Authentication DB is MSAD, add the following parameter to the configuration file for Authentication Module.
    LDAPBIND=1
    LDAPPCHG=0
    LDAPLANG=0

6.4.5 Upgrading from 7.0

- The If-modified-since header is forwarded to the Backend Web Server. When running based on the old specification, add the following setting to the host configuration file.
    HEADER=HTTP_IF_MODIFIED_SINCE,NOTSEND

• If the Authentication DB is MSAD, add the following parameter to the configuration file for Authentication Module.
> LDAPBIND=1
> LDAPPCHG=0
> LDAPLANG=0

6.4.6 Upgrading from 7.0SP1, 7.0SP2, 7.0SP3 and 7.0.1SE

• If the Authentication DB is MSAD, add the following parameter to the configuration file for Authentication Module.
> LDAPBIND=1
> LDAPPCHG=0
> LDAPLANG=0

• If the Authentication DB is NED, add the following parameter to the configuration file for Authentication Module.
> LDAPBIND=1
> LDAPPCHG=1
> LDAPLANG=1

6.4.7 Upgrading from 8.0, 8.0.1(8.0R1), 8.0 R2, and 8.0 R3

• Only the "Common considerations for previous versions" apply.

7   Restrictions

Be aware of the following restrictions when using this version.

7.1   Notes on using the failover option

Processing requests with both Authentication Modules in a replication configuration (Primary/ Secondary) is not supported except during failures. After recovering from a failure, ensure that only the Primary Authentication Module processes the requests. Please note that, in replication configuration, since the Primary module is replicated to the Secondary module, splitting requests among the Primary and Secondary modules does not result in load balancing.

7.2   Size of content with Range specification

If the Range is specified for content that is subject to conversion, since content size is different due to content conversion between the browser and Forwarder, and between Forwarder and web server, the acquired position may shift.

7.3   Unable to download files in SSL communication when using IE6.x

If an HTTP header contains "Pragma: no-cache", the file download will fail. This problem occurs when the client accesses web server with Microsoft Internet Explorer 6.x in SSL communication. This is a problem with Microsoft Internet Explorer 6.x. This problem also occurs when the client tries to connect to the web server directly without going through IceWall.

8   Reading Documents

Manuals and documents on the CD-ROM are provided as PDF files. Adobe Systems Adobe Reader is required to read these files.

Note: Adobe Reader can be downloaded from the Adobe Systems website free of charge. For details on how to install and use Adobe Reader, see the Adobe Reader manual.

9 Notes

Hewlett-Packard Japan, Ltd. reserves all rights for the sample files included in the product. However, these samples are not supported.

IceWall SSO patches can be downloaded from the IceWall SSO Support Information Website.

10 Related URL and Contact Information

<IceWall SSO related>
Product information
  Hewlett-Packard Japan, Ltd.
    (http://www.hp.com/jp/icewall_eng (English))
    (http://www.hp.com/jp/icewall (Japanese))

<OTHERS>
  Oracle Corporation Japan
    (http://www.oracle.com/)
  Sun Microsystems, Inc.
    (http://www.sun.com/)
  Adobe Systems Incorporated
    (http://www.adobe.com/)
  Red Hat, Inc.
    (http://www.redhat.com/)
  Apache Software Foundation
    (http://www.apache.org/)
  Novell, Inc.
    (http://www.novell.com/)
  Microsoft Corporation
    (http://www.microsoft.com/)