



# **IceWall SSO**

Version 10.0

## **Installation Guide** for Linux

August 2010

**Printed in Japan**

**HP Part No. B1544-93001**

**Rev.111028A**

## Notice

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

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

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

The copyright of this document is assigned to Hewlett-Packard Development Company, L.P. No part of this document may be photocopied or reproduced without prior written consent by Hewlett-Packard Japan, Ltd.

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

IceWall is a trademark of Hewlett-Packard Japan, Ltd.

Adobe is a trademark of Adobe Systems Incorporated in the United States and/or other countries.

Intel, the Intel logo, Intel. Leap ahead., Intel. Leap ahead. logo, Itanium and Itanium Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

## – Table of Contents –

1	Introduction .....	1
1.1	Version designations in respective items .....	1
2	System Requirements .....	2
2.1	System requirements for Forwarder (dfw) .....	2
2.2	System requirements for the Authentication Module (certd) .....	2
2.3	Other Topics .....	3
3	Installation .....	5
3.1	Installing the Forwarder .....	5
3.2	Installing the Authentication Module .....	6
3.3	Configuration after installation .....	8
3.3.1	Configuring encryption libraries .....	8
3.3.2	Configuring password for LDAP server .....	9
3.4	Recommended configurations .....	9
3.4.1	Configuring Keep-Alive of a web server instance .....	9
3.4.2	Setting the SSLSessionCache when using SSL connection .....	9
4	Uninstallation .....	10
4.1	Uninstalling the Forwarder .....	10
4.2	Uninstalling the Authentication Module .....	10
5	Verification of Installation .....	11
5.1	Quick verification on modules .....	11
5.1.1	Verifying the Forwarder .....	11
5.1.2	Verifying the Authentication Module .....	13
5.2	Verification by displaying the sample pages .....	13
5.3	Verifying installed files .....	14
5.3.1	Forwarder package .....	14
5.3.2	Authentication Module package .....	16
5.4	Verifying version information .....	18
5.4.1	Verifying version information for Forwarder .....	18
5.4.2	Verifying version information for Authentication Module .....	19
6	Upgrading from Previous Versions .....	21
6.1	Upgrade procedure .....	21
6.2	Common considerations for previous versions .....	22
6.3	Common considerations for version 8.0 or earlier .....	23
6.4	Version-specific upgrade considerations .....	23
6.4.1	Upgrading from 5.1i .....	24
6.4.2	Upgrading from 5.1iSP1 and 5.1iSP2 .....	24
6.4.3	Upgrading from 6.0, 6.0SP1 and 6.0.1SE .....	24
6.4.4	Upgrading from 7.0 .....	24
6.4.5	Upgrading from 7.0SP1, 7.0SP2, 7.0SP3 and 7.0.1SE .....	25
6.4.6	Upgrading from 8.0, 8.0.1(8.0R1), 8.0 R2, and 8.0 R3 .....	25
7	Restrictions .....	26
7.1	Notes on using the failover option .....	26



7.2	Size of content with Range specification .....	26
7.3	Unable to download files in SSL communication when using IE6.x .....	26
8	Reading Documents .....	27
9	Notes .....	28
10	Related URL and Contact Information .....	29

## **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.

<b>Designation</b>	<b>Meaning</b>
	Item added in the version enclosed in a square. In this case, the designation indicates the item was added with 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 ProLiant or equivalent compatible server (recommended by HP)
- OS

Red Hat Enterprise Linux 5.4(x86 64bit) and later versions **10.0** \*1

\*1 Operation is not guaranteed in an environment with NSA Security-Enhanced Linux (SELinux) enabled.

- Web server  
For Red Hat Enterprise Linux 5.4 and later versions  
Apache HTTP Server 2.2.3 and later versions (64bit) **10.0** \*2\*3

\*2 Only packages provided by the OS vendors are supported. Customer-compiled packages are not supported.

\*3 Only MPM: prefork is 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 ProLiant or equivalent compatible server (recommended by HP)
- OS

Red Hat Enterprise Linux 5.4(x86 64bit) and later versions **10.0** \*4

\*4 Operation is not guaranteed in an environment with NSA Security-Enhanced Linux (SELinux) enabled.

- 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)  
MySQL Server 5.1.40 and later versions **10.0**  
OpenLDAP 2.4.16 and later versions **10.0**

- 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 Database 11g Release 2 Standard Edition	Oracle Net R11.2.0
Oracle Database 11g Release 2 Enterprise Edition	

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. If the Authentication DB is MySQL, the ODBC driver “MyODBC” for connection and database server “MySQL” of MySQL AB are required.  
The supported versions are listed below.
  - MyODBC (Connector/ODBC) 5.1.7
  - unixODBC (ODBC Driver Manager) 2.2.14 and later versions
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.

<b>Terminology</b>	<b>Corresponding products</b>
Apache	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 Enterprise Edition
LDAP	Sun Java System Directory Server 7.0 HP Directory Server 8.1 OpenLDAP 2.4.16
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
MySQL	MySQL 5.1.40



### 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:

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

(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.

Enter the following command to mount the CD-ROM.

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

\* This is an example when the mount point is /mnt/cdrom. If the mount point does not exist, create one with the mkdir command.

(3) Enter the following command to install the Authentication Module.

```
# rpm -ivh --nodeps /mnt/cdrom/SSO/linux/IceWall-SSO-dfw_e-10.0.0-1.x86_64.rpm
```

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

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

- (5) Enter the following command to change the owner of the directories and files related to the Forwarder to the user executing Apache. In the following example, the execution user of Apache is apache:apache.

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

- (6) Configure the Forwarder in Apache. 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.)

① Edit the Apache configuration file (httpd.conf).

<Example for modifying httpd.conf>

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

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

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

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

Enter the following command to mount the CD-ROM.

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

\* This is an example when the mount point is /mnt/cdrom. If there is no mount point, create one with the mkdir command.

- (3) Select the name of the installation package for the Authentication DB for use and enter the following command to install the Authentication Module.

```
# rpm -ivh --nodeps /mnt/cdrom/SSO/linux/[installation package name]
```

Note that the name of the installation package varies depending on the version of the IceWall SSO.

Authentication DB	Installation package name
Oracle11g edition	IceWall-SSO-cert_d_oracle1110_e-10.0.0-1.x86_64.rpm
MySQL edition	IceWall-SSO-cert_d_odbc_e-10.0.0-1.x86_64.rpm
LDAP edition	IceWall-SSO-cert_d_ldap_e-10.0.0-1.x86_64.rpm
OpenLDAP edition	IceWall-SSO-cert_d_openldap_e-10.0.0-1.x86_64.rpm
NED edition	IceWall-SSO-cert_d_ned_e-10.0.0-1.x86_64.rpm
MSAD edition	IceWall-SSO-cert_d_msad_e-10.0.0-1.x86_64.rpm
CSV edition	IceWall-SSO-cert_d_csv_e-10.0.0-1.x86_64.rpm

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

```
# rpm -qa | grep [target name]
```

Installation package	Target name
Oracle11g edition	IceWall-SSO-cert_d_oracle1110_e K
LDAP edition	IceWall-SSO-cert_d_ldap_e
NED edition	IceWall-SSO-cert_d_ned_e
MSAD edition	IceWall-SSO-cert_d_msad_e
CSV edition	IceWall-SSO-cert_d_csv_e
OpenLDAP edition	IceWall-SSO-cert_d_openldap_e
MySQL edition	IceWall-SSO-cert_d_odbc_e

- (5) Use the following command to create a user for executing the Authentication Module.

```
# useradd -g users iwadmin
```

- (6) Modify the settings for the Authentication Module commands.

Modify the following files only if ORACLE is used as the Authentication DB.

(There is no need for modification if LDAP, NED, MSAD, CSV or MySQL is used.)

```
/opt/icewall-ss0/certd/bin/start-cert  
/opt/icewall-ss0/certd/bin/end-cert  
/opt/icewall-ss0/certd/bin/info-cert  
/opt/icewall-ss0/certd/bin/reload-cert  
/opt/icewall-ss0/certd/bin/logout-cert  
/opt/icewall-ss0/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 connection identifier for the database.

- (7) Change the owner of the directories and files related to the Authentication Module to the user created in (5).

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).

## **3.4 Recommended configurations**

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

### **3.4.1 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.

### **3.4.2 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 Apache.
- (3) Delete the setting that runs the Forwarder from the Apache configuration file.
- (4) Enter the following command to uninstall.

```
# rpm -e IceWall-SSO-dfw_e
```

### 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-ss0/certd/bin/end-cert
```

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

```
# rpm -e [target name]
```

Installation package	Target name
Oracle11g edition	IceWall-SSO-certd_oracle1110_e K
LDAP edition	IceWall-SSO-certd_ldap_e
NED edition	IceWall-SSO-certd_ned_e
MSAD edition	IceWall-SSO-certd_msad_e
CSV edition	IceWall-SSO-certd_csv_e
OpenLDAP edition	IceWall-SSO-certd_openldap_e
MySQL edition	IceWall-SSO-certd_odbc_e

## 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 apache. 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.)

For Red Hat Enterprise Linux v.5.4 (x86 64bit)

```
# cd /opt/icewall-ss0/dfw/cgi-bin/  
# sudo -u apache env LD_LIBRARY_PATH=/opt/icewall-ss0/lib/dfw HT  
TP_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"></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"></td>
                    <td width="175" height="35"></td>
                    <td width="227" height="35" align="right"><font color="#ffffff"> ■
</font>&nbsp;</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>
                                    
                                    <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"></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-ss0/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-ss0/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-ss0, but the installed files differ depending on the type of package to be installed. After installation, verify the file structure under the /opt/icewall-ss0 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_pvwioerr.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) <b>10.0</b> 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) <b>10.0</b> 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) <b>10.0</b> pwdchg_pwvioerr.html(644) pwdchg_repasserr.html(644) pwdchg_warning.html(644) request_acl_error.html(644) <b>10.0</b> system_alias_error.html(644) system_backend_error.html(644) system_busy_database.html(644) <b>10.0</b> 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)	
/iwpmdd(775)	/bin(775)	iwpmdd(755) iwpmdd(755)	
	/conf(775)	iwpmdd.conf(644)	
	/data(775)		
	/run(775)		
	/script(775)	iwpmdd_analyselogs.pl(755) iwpmdd_calccoverage_perf.pl(755) iwpmdd_count_errlog.pl(755) iwpmdd_printdata_perf.pl(755) iwpmdd_printdata_screen.pl(755) iwpmdd_printhead_perf.pl(755)	
	/tmp(775)		
/lib(555)	/dfw(555)	libDfwExit.so(777) * Link libsidcrypto.so(777) * Link libssl.so(777) * Link libcrypto.so(777) * Link libCryptoExit.so(777) * Link	
		libDfwExit.sl(555) libsidcrypto.sl(555) libssl.sl(555) libcrypto.sl(555) libDfwCryptoExit.sl(555)	
/logs(777)			
/messages(555)	/C(555)	icewall_dfw.cat(444) ⑩⑩	
/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) ⑩⑩ cdump-cert(755) ⑩⑩ 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	

## IceWall SSO Version 10.0 / Installation Guide for Linux

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_analyselogs.pl(755) iwpmc_calcavarage_info.pl(755) iwpmc_calcavarage_perf.pl(775) iwpmc_printdata_info.pl(755) iwpmc_printdata_perf.pl(755) iwpmc_printdata_screen.pl(755) iwpmc_printhead_info.pl(755) iwpmc_printhead_perf.pl(755)	
	/tmp(775)		
	/lib(555)	/certd(555)	libDB.so(777)
libPH.so(777)			* Link
libCertExit.so(777)			* Link
libCryptoExit.so(777)			* Link 10.0
libExCryptoExit.so(777)			* Link
libCreateSidExit.so(777)			* Link
libiwDBCrypto.so(777)			* Link 10.0
libiwDBCryptoExit.so(777)			* Link 10.0
libcrypto.so(777)			* Link
libssl.so(777)			* Link For LDAP, OpenLDAP, NED, MSAD edition only
liblber.so(777)			* Link For LDAP, OpenLDAP, NED, MSAD edition only
libldap.so(777)			* Link For LDAP, OpenLDAP, NED, MSAD edition only
libsasl2.so(777)		* Link For LDAP, OpenLDAP, NED, MSAD edition only	
libCertExit.sl(555)			
libCryptoExit.sl(555)			
libExCryptoExit.sl(555)			
libCreateSidExit.sl(555)			
libiwORA1110.sl(555)			
libiwODBC.sl(555)			
libiwLDAP.sl(555)			
libiwCSV.sl(555)			
libiwPwdHash.sl(555)			
liblber.sl(555)			
libldap.sl(555)			
libsasl2.sl(555)			
libcrypto.sl(555)			
libssl.sl(555)			
libiwDBCrypto.sl(555)			
libiwDBCryptoExit.sl(555)			
/lib32(555)	libcrypto.sl(555)	* Except MSAD edition	
*Except MSAD edition	/mkuser(555)	libcrypto.so(777)	* 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 edition	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, MySQL edition only * For LDAP, OpenLDAP, NED edition only * For CSV edition only * For ORACLE, MySQL edition only * For ORACLE edition only * For ORACLE edition only * For ORACLE, MySQL 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-ssso/dfw/cgi-bin
```

- (2) Enter the following command:

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

(3) The following information is displayed:

Example:

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

#### **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-ssso/certd/bin
```

(2) Enter the following command:

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

The following information is displayed.

Example:

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

<Authentication DB connection library>

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

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

(2) Enter the following command:

```
# strings libDB.so | grep '@(#) '
```

(3) The following information is displayed.

The displayed information may vary depending on the Authentication DB.

Example: Oracle11g version

```
@(#)IceWall SSO Database Plug-in Oracle 11.1.0.6.0
@(#)Version: 10.00.00.xxxxxxxX
@(#)OS: Linux 2.6.18
@(#)CPU: x86_64
@(#)Bit: 64bit
@#)(c) Copyright 2001-2010 Hewlett-Packard Development
Company, L.P.
```



## 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-ssso/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. The Authentication Module commands from previous versions will not work with this version.
- (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 prefix-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-ssolib/dfw and /opt/icewall-ssolib/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 (6).”

### **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 5.1i**

- 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.

#### **6.4.2 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

#### **6.4.3 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

#### **6.4.4 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

#### **6.4.5 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

#### **6.4.6 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](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/>)