HP-UX Secure Shell A.06.20.004, A.06.20.005, and A.06.20.006 Release Notes

HP-UX 11i V1, HP-UX 11i V2, and HP-UX 11i V3

HP Part Number: 5900-3159
Published: July 2013
Edition: 1

Copyright 2011, 2013 Hewlett-Packard Development Company, L.P. Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. UNIX is a registered trademark of The Open Group.

Contents

1 HP-UX Secure Shell A.06.20

This document describes the most recent product information for HP-UX Secure Shell versions A.06.20.004, A.06.20.005, and A.06.20.006 that are supported on HP-UX 11i V1, HP-UX 11i V2, and HP-UX 11i V3 respectively. This document addresses the following topics:

Announcement

HP-UX Secure Shell version A.06.20 is based on OpenSSH 6.2p2 and it offers transparent encrypted security for HP-UX 11i V1, HP-UX 11i V2, and HP-UX 11i V3. HP-UX Secure Shell supports the SSH-1 and SSH-2 protocols and provides secured remote login, file transfer, and remote command execution.

HP-UX Secure Shell uses hashing to ensure data integrity and provides secure tunneling features, port forwarding, and an SSH agent to maintain private keys on the client. HP-UX Secure Shell supports several authentication methods and schemes. These include:

- Kerberos5/GSSAPI
- Public Key
- Host-based
- Keyboard-interactive
- Password

HP supports HP-UX Secure Shell at no additional cost to customers with the HP-UX support agreements. HP-UX Secure Shell is a fully tested HP product. The following is a partial list of the technologies tested with HP-UX Secure Shell:

- Kerberos5/GSSAPI
- OpenSSL
- IPv6
- Trusted Systems
- TCP Wrappers
- PAM (PAM_UNIX, PAM_Kerberos, PAM_LDAP)

HP-UX Secure Shell version A.06.20 is built with the following libraries:

- zlib V1.2.3
- OpenSSL v0.9.8y — For HP-UX 11i V3, OpenSSL is a shared library
- TCP Wrappers V7.6-ipv6.4

Secure Shell versions on HP-UX

Table 1 lists the versions of HP-UX Secure Shell products available for HP-UX 11i V1, HP-UX 11i V2, and HP-UX 11i V3.

Table 1 Availability of Secure Shell Versions on HP-UX

Supported Operating System	Version
HP-UX 11i V1	HP-UX Secure Shell version A.06.20.004
HP-UX 11i V2	HP-UX Secure Shell version A.06.20.005
HP-UX 11i V3	HP-UX Secure Shell version A.06.20.006

Support notice

HP provides software technical support for HP-UX Secure Shell for the latest, currently shipping version, and the previous version of the product.

New features

HP-UX Secure Shell version A.06.20 is based on OpenSSH 6.2p2. A number of features have been added. The new features of OpenSSH are available at http://www.openssh.org/txt/release-6.2p2 and http://www.openssh.org/txt/release-6.2

Support for the `Sftpfilecontrol` patch

HP-UX Secure Shell supports the `Sftpfilecontrol` patch. This patch enables administrators to set the `umask` on `sftp` sessions and to control the issue of `chown` and `chmod` commands in an `sftp` session. As a result, the following server configuration directives (`/opt/ssh/etc/sshd_config`) related to `Sftpfilecontrol` are supported in this release:

- `#SftpUmask`
- `#SftpPermitChmod yes`
- `#SftpPermitChown yes`

This patch supersedes the `sftplogging` patch for HP-UX Secure Shell versions A.04.50 and higher.

Defects fixed in OpenSSH 6.2p2

The HP-UX Secure Shell version A.06.20 is based on OpenSSH 6.2p2 and includes the defect fixes mentioned in http://www.openssh.org/txt/release-6.2p2 and http://www.openssh.org/txt/release-6.2

OpenSSH 6.2p2 also includes fixes for some security vulnerabilities.

For more information on these defect fixes, see the Bugzilla website at: http://bugzilla.mindrot.org.

Defects fixed in HP-UX Secure Shell A.06.20.004, A.06.20.005, and A.06.20.006

Removed dependency on Kerberos client (KRB5CLIENT) product, which was introduced in HP-UX Secure Shell A.06.20.001, A.06.20.002 and A.06.20.003.

Defects fixed in HP-UX Secure Shell A.06.20.001, A.06.20.002, and A.06.20.003

- Fixed the issue to properly display the Korean banner message properly when user connects with SSH.
- Added a new `sshd_config` keyword `DisplayHostNameInAuditLog` to have the hostname reported in syslog for ssh. This new config option logs the hostname in addition to the IP Address in syslog.
- Added the `sshd_config` option `AuthorizedKeysCommand` to obtain the authorized_keys from a command in addition to (or instead of) the fetching from the filesystem. The command is executed under an account specified by an `AuthorizedKeysCommandUser sshd_config` option.
- Fixed the issue to prevent the hanging of `scp` and `sftp` commands when you enable keystroke logging using HPUX-RBAC (HP-UX Role-Based Access Control).

Known problems and workarounds

The following are the known problems and workarounds in HP-UX Secure Shell A.06.20:

WARNING! Do not specify user specific information during configuration of host-based authentication. Host-based authentication supports only authentication of hosts. It does not allow user-specific authentication. When the user configures the host-based authentication with the following, `# cat /etc/hosts.equivmyhost.mydomain.com specificuser`, it allows the `specificuser@myhost.mydomain.com` to login to any local account on the remote machine.

- The base code of OpenSSH 6.2p2 supports logging of `sftp` transactions. `LogFacility` and `LogLevel` options are added to sftp-server as command-line options to log these transactions. As a result, the following directives are not supported in this release of HP-UX Secure Shell:
  - `#LogSftp no`
  - `#SftpLogFacility AUTH`
  - `#SftpLogLevel INFO`
- The following SMSE behavior is seen in this version of HP-UX Secure Shell:

  Audit log messages show repeated entries for a user. This occurs because bad login attempts are logged in the audit file.

Example 1 Public key authentication With Bad RSA, ECDSA and DSA Keys

If you try Public key authentication with bad RSA, ECDSA and DSA keys, it results in a bad login attempt for each key type. In such a scenario, the audit log has the following entries:

```
SELF-AUDITING TEXT: User= root uid=0 ssh authentication method PUBKEY – failed
SELF-AUDITING TEXT: User= root uid=0 ssh authentication method PUBKEY – failed
SELF-AUDITING TEXT: User= root uid=0 ssh authentication method PUBKEY – failed
SELF-AUDITING TEXT: User= root uid=0 ssh authentication success - user logged in
SELF-AUDITING TEXT: User= root uid=0 ssh session open
```

Example 2 Public Key Authentication With Bad RSA, ECDSA and Correct DSA Keys

If you try Public Key Authentication with bad RSA, ECDSA and correct DSA keys, it results in two bad logins for RSA and ECDSA. In such a scenario, the audit log has the following two entries:

```
SELF-AUDITING TEXT: User= root uid=0 ssh authentication method PUBKEY - failed
SELF-AUDITING TEXT: User= root uid=0 ssh authentication method PUBKEY - failed
SELF-AUDITING TEXT: User= root uid=0 ssh authentication success - user logged in
SELF-AUDITING TEXT: User= root uid=0 ssh session open
```

Example 3 Wrong Typing of a Password

If you type a wrong password and it results in authentication failure, the failure is considered a bad login. All such bad logins result in separate entries in the audit file.

For more information on HP-UX SMSE, see http://www.hp.com/go/hpux-security-docs

- HP-UX Secure Shell user authentication using public-key fails in a server environment if `UsePAM` is set to `YES` and `pam.conf` is set to `PAM_LDAP`.

  Workaround: HP recommends the `PAM_AUTHZ` mechanism for HP-UX Secure Shell environments that use public-key authentication with PAM_LDAP-based account management.

- On some systems, the following messages appears in the `syslog.log` file, when a user logs out of a Secure Shell session:

  ```
  pam_setcred: error Authentication failed
  pam_setcred: error Permission denied
  ```

  These messages appears only when the daemon is running in debug mode. These messages are not relevant to (and does not affect) HP-UX Secure Shell operations. The PAM function `pam_setcred` generates this message. These error messages appear for the scenarios listed in Table 2.

Table 2 Scenarios where `pam_setcred` Generates Error Messages

User	UsePriv	KeyServ Running	Error Messages
root	yes	no	Permission denied
non-root	yes	no	Authentication failed
root	no	no	Permission denied
non-root	no	no	Permission denied
root	yes	yes	Permission denied
non-root	yes	yes	No message
root	no	yes	Permission denied
non-root	no	yes	Permission denied

- A Kerberos ticket on a Secure Shell server system gets inadvertently deleted in the following scenario:
  1. User U1 creates a Kerberos ticket file on a Secure Shell server system, S1.
  2. The SSH server on S1 is set up for `PAM_KERBEROS` authentication.
  3. User U1 now remotely connects to the SSH instance on S1 using public-key authentication.
  4. User U1 exits.

  The `kinit`-generated ticket file created in Step 1 gets deleted when the user exits the Secure Shell session.

  Workaround: Create the Kerberos ticket file (Step 1) in a non-default location and selectively communicate this file name to Secure Shell processes using the `KRB5CCNAME` environment variable.

- The `chroot` functionality does not work if the `UseLogin` configuration directive in `sshd_config` is set to `YES`.
- In a chroot-ed environment, you do not see a subset of syslog messages. HP-UX Secure Shell writes syslog messages during authentication and when the session is terminated. The `syslogd` daemon reads the syslog messages written by all subsystems and reports it to the `/dev/log` file. In a chroot-ed environment, the `sshd` daemon writes its syslog messages to *`<newroot>`*`/dev/log`. You cannot link the *`<newroot>`*`/dev/log` file to the `/dev/log` file, so you are not able to view the subset of syslog messages.

  Workaround: Please see HP-UX - How to Configure SFTP Logging in a Chrooted Environment? Users of chroot-ed HP-UX Secure Shell environments must be aware that a subset of messages written by the sshd daemon will not show up in syslog.

- QXCR1000868044

  This occurs when sshd is being used by SIM System Insight Manager and the CMS and gWLM. In some systems, when kerberos authentication is set to yes, ChallengeResponseAuthentication is commented out in sshd_config, and kerberos is not configured in the system, sshd will have a very long timeout.

- QXCR1001102145

  ssh-keygen displays only the first key and does not handle multiple keys present in a file. This issue is same as http://bugzilla.mindrot.org/show_bug.cgi?id=1319

- QXCR1001200464

  ECDSA key storing on LDAP server is NOT supported on HP-UX Secure Shell A.06.20.

- NO JAG

  Privsep using sandboxing is not supported on HP-UX Secure Shell A.06.20.

- NO JAG

  Login to MP/iLO with HP-UX Secure Shell A.05.80 onwards fails with *Client Disconnect*. This is a known issue with Secure Shell while attempting to login to HP MP/iLO. Secure Shell A.05.80 and above has added additional key exchange protocols that the MP/iLO receiving buffer cannot handle. HP is currently developing a fix for the MP/iLO firmware issue.

  The current workaround is to shorten the Host Key Algorithms list. You can use one of the following commands:

  ```
  #ssh -oHostKeyAlgorithms=ssh-dss admin@my-mp
  #ssh -oHostKeyAlgorithms=ssh-rsa admin@my-mp
  #ssh -oHostKeyAlgorithms=ssh-rsa,ssh-dss admin@my-mp
  ```

HP-UX and the strong random number generator

HP-UX Secure Shell requires that a random number generator to be located on the system. It searches for `/dev/urandom` and `/dev/random` (in that sequence) on the system and uses the first device that it finds. The `/dev/urandom` and `/dev/random` devices are available by default on HP-UX 11i V1, HP-UX 11i V2, and HP-UX 11i V3 systems.

HP-UX Secure Shell resources

For more information about Secure Shell, see the following:

- HTML and pdf versions at http://www.hp.com/go/hpux-security-docs (*Internet and Security Solutions*)
- A README text version in the software at: `/opt/ssh/README.hp`
- The HP Instant Information CD beginning with Application Release 0902
- OpenSSH at http://www.openssh.com
    - FAQs, Mail List Archives, Security pages, manpages
- IETF at http://www.ietf.org/ (go to Working Groups > Security)
- The HP book *HP-UX 11i Security* by Chris Wong.
- Secure Shell FAQs at: http://www.employees.org/~satch/ssh/faq/ssh-faq.html
- Barrett, Daniel J. and Richard E. Silverman, 2005. *SSH, The Secure Shell: The Definitive Guide*. California: O'Reilly and Associates Inc.,

HP-UX Secure Shell commands

Table 3 lists the HP-UX Secure Shell commands and provides a brief description of each. For more information, see the manpage for each command.

Table 3 HP-UX Secure Shell Commands

Command	Description
ssh	client program similar to rlogin and rsh
sshd	secure shell server daemon
sftp	secure ftp program
scp	secure file copy program similar to rcp
slogin	symbolic link to ssh
ssh-agent	authentication agent to store private keys
ssh-add	tool for adding keys to ssh-agent
ssh-keygen	tool for manually creating public and private keys
sftp-server	sftp server subsystem automatically initiated by sshd
ssh-keyscan	tool for gathering public host keys
ssh-keysign	ssh helper program for host-based authentication
ssh-pkcs11-helper	ssh-agent helper program for PKCS#11 support

Prerequisites

This section discusses the prerequisites for installing HP-UX Secure Shell A.06.20.

System requirements

Table 4 lists the minimum system requirements for installing HP-UX Secure Shell A.06.20.

Table 4 System Requirements for Installing HP-UX Secure Shell A.06.20

Component	Requirement
Operating System	• HP-UX 11i V1 • HP-UX 11i V2 • HP-UX 11i V3
Hardware	• HP/9000 servers • HP Integrity servers
Disk Space	Approximately 32MB
Software	HP-UX Secure Shell A.06.20 requires OpenSSL version A.00.09.08g.003 or later
Software availability in native languages	English only

Patch requirements

HP has tested HP-UX Secure Shell A.06.20 with the Support Plus patches listed in Table 5.

Table 5 Support Plus Patches for HP-UX Secure Shell on HP-UX Operating Systems

Operating System	Recommended Support Plus Patch
HP-UX 11i V1	December 2002 Support Plus release / media
HP-UX 11i V2	No Support Plus patch required
HP-UX 11i V3	No Support Plus patch required

The standard HP-UX patch bundles index page lists the release dates for the current patch bundles. Selecting a specific release date provides you with a list of all the patch bundles released on that particular date.

NOTE: The standard HP-UX patch bundles are cumulative. If you do not find an earlier bundle, you can select the latest HP-UX release and use the latest version of the particular patch bundle.

HP recommends that you install the `libc`, PAM, and pthreads patches listed in Table 6 with HP-UX Secure Shell A.06.20.

Table 6 libc, PAM and pthreads Patch Requirements

Operating System Version	libc Patch	PAM Patch	pthreads Patch
HP-UX 11i V1	PHCO_27740	• PHCO_27064 • PHCO_30402 • PHCO_33215	PHCO_26466
HP-UX 11i V2	No libc patch required	No PAM patch required	No pthreads patch required
HP-UX 11i V3	No libc patch required	No PAM patch required	No pthreads patch required

NOTE: The PHCO_33215 patch fixes a PAM-related issue. Without this patch, `pam_acct_mgmt` returned success messages on locked accounts. With this patch, account management fails for locked accounts (this is the appropriate behavior). To log in using ssh, you must unlock your accounts.

HP-UX Secure Shell software availability

HP-UX Secure Shell is available on the following:

- HP Software Depot at: http://www.software.hp.com
- HP-UX Application Release CDs
- HP-UX 11i V1 Operating Environment (OE)
- HP-UX 11i V2 Operating Environment (OE)
- HP-UX 11i V3 Operating Environment (OE)

NOTE: HP-UX Secure Shell is available on the HP-UX Application Release CD, HP-UX 11i V1 OE, HP-UX 11i V2 OE, and HP-UX 11i V3 OE whenever the CD and OEs are available.

Installing HP-UX Secure Shell

You must not remove any earlier versions of HP-UX Secure Shell before upgrading to HP-UX Secure Shell A.06.20. However, if you want to revert to an earlier version of HP-UX Secure Shell, HP recommends that you remove the new product before reverting to it.

To install HP-UX Secure Shell:

1. Log in as root.
2. Insert the software CD into the appropriate drive, if you are installing from the Application Release CD. If you are installing from http://software.hp.com, download the depot and use the `swinstall` directions provided on the Installation page.
3. Run `$ swinstall -s <fully-qualified depot source path>` at the command prompt.
4. Enter the drive mount point In the `Source Depot Path` field, and then click **OK**. If required, change the`Source Host Name`.
5. Select **`T1471AA`** (for HP-UX 11i V1 and HP-UX 11i V2) or **`SecureShell`** (for HP-UX 11i V3) from the list of available software, and click **Mark for Install** on the Actions menu.
6. Click **Install** on the Actions menu.
7. Click **OK** in the Install Analysis window when the Status field displays a Ready message.
8. Click **Yes**. The `swinstall` command loads the HP-UX Secure Shell files on the system in approximately 3 to 5 minutes.

NOTE: The `sshd` daemon is pre-configured, and it is started after installation.

The `swinstall` command installs HP-UX Secure Shell in the `/opt/ssh/` directory.

HP-UX Secure Shell and chroot environments

HP-UX Secure Shell version A.06.20 supports `chroot` functionality for the `ssh`, `sftp`, and `scp` commands. The `chroot` functionality is mainly used as an added security measure.

When you enable `chroot`, you can start an application in a specified directory and enable access for all its users to that directory and the directories below it. It prevents users from using the `cd` command to access directories at a higher level. Use this functionality to enable restricted file and directory access to users of a particular application. This is not an end-user feature. The system administrator must enable the `chroot` functionality for an application. All users of that application will automatically be subject to the restrictions imposed by `chroot`.

For more information on setting up the`chroot` functionality, see `README` file at `/opt/ssh/README.hp`. The `chroot` setup script is available at `/opt/ssh/utils/ssh_chroot_setup.sh`.

Frequently Asked Questions (FAQ)

This section discusses questions frequently asked about HP-UX Secure Shell.

1. What is the difference between HP-UX Secure Shell A.06.20 and OpenSSH 6.2p2?

   OpenSSH 6.2p2 is a free version of the SSH protocol suite of network connectivity tools. OpenSSH supports SSH protocol versions 1.3, 1.5, and 2.0 and now more people on the internet are relying on it.

   HP-UX Secure Shell is a binary package compiled with support for PAM, gssapi, krb5, and libwrap, but there is no support for Smartcard. HP-UX Secure Shell is built to install and un-install using the SD-UX utility and includes all required pre-requisites.

2. Why should HP-UX Secure Shell be used?

   The standard services for interactive sessions on remote machines lack sufficient security. This results in the server system becoming vulnerable to a wide variety of attacks. HP-UX Secure Shell offers strong encryption during authentication and for the entire session, which makes it a perfect replacement for these services.

3. How does HP-UX Secure Shell authenticate?

   HP-UX Secure Shell authenticates using one or more of the following:

   - Password (the /etc/passwd or /etc/shadow in UNIX)
   - User public key (RSA, ECDSA or DSA, depending on the release)
   - Kerberos5/GSSAPI for SSH-2

4. What are the supported features?

   HP-UX Secure Shell supports both SSH-1 and SSH-2 protocols. HP recommends not to use SSH-1 to avoid the risk of an insertion attack.

5. Does HP-UX Secure Shell support Smart Card authentication?

   No. HP-UX Secure Shell is compiled without smart card support.

6. Will HP support recompiled versions of HP-UX Secure Shell?

   The source code is provided for reference only. HP does not support recompiled versions. The following archive libraries are not provided with the code:

   - zlib v1.2.3
   - OpenSSL v0.9.8y
   - tcp_wrappers_7.6-ipv6.4 (source code provided, no library)

7. What are the limitations of this product?

   HP-UX Secure Shell is not a true shell like UNIX Bourne Shell or C Shell. Therefore, it does not provide complete security solutions.

8. Does installing HP-UX Secure Shell require a kernel rebuild?

   No. HP-UX Secure Shell is an application level protocol and does not require a kernel rebuild or system reboot.

9. How can I remove HP-UX Secure Shell?

   Use `swremove` to remove the product.

10. How does HP-UX Secure Shell perform?

    Compared to the conventional file transfer, scp is two to three times slower than rcp. As Secure Shell authenticates both the server and the users, and encrypts both the data and the password, sftp is two to three times slower than ftp.

    HP recommends using /dev/random on your system to significantly speed-up program initialization. HP is continually striving for performance enhancements for future releases.

11. Does HP-UX Secure Shell support `rdist` or `rsync`?

    No. HP-UX Secure Shell cannot be specified as the connection mechanism to HP's `rdist`. HP has not officially certified Secure Shell with the open source versions of `rdist` or `rsync`.

12 Does HP-UX Secure Shell support the DenyHosts parameter?

No. For access control, HP-UX Secure Shell does not support the DenyHosts, AllowHosts, DenySHosts, and IgnoreRootRhosts parameters. However, HP-UX Secure Shell supports the AllowUsers, DenyUsers, AllowGroups, and DenyGroups parameters.

13 How can I configure HP-UX Secure Shell to allow multiple users (more clients) access to an SFTP server using one login and encrypt the connection?

Use public key authentication. Each local user gets a pair of public and private keys. All the public keys are added to the ~/.ssh/authorized_keys file of a single user on the remote machine. Each local user can then issue the sftp command and log in as the remote user. All local users share access to the remote user. Remember that all local users can also use ssh to access the remote user.

14 What diagnostic tools does HP-UX Secure Shell have? Where can I find error messages, log files, and so on?

HP-UX Secure Shell logs debug and error messages using syslog. Logging is controlled by two configuration keywords: SyslogFacility and LogLevel.

Use the appropriate syslog log levels (QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG) to gather more information about error scenarios. As defined by sshd_config, the default for syslogFacility is set to AUTH and LogLevel is set to INFO, as in the following:

- #SyslogFacility AUTH
- #LogLevel INFO

If sshd runs in debug mode (-d), logging goes to standard error instead of to syslog. Get more debugging information by using additional d's for sshd and additional v's for ssh, as in the following:

- ssh -v
- ssh -vv
- ssh -vvv
- sshd -d
- sshd -dd
- sshd -ddd

Other commands with debugging option -v are:

- ssh-keyscan -v
- sftp -v
- scp -v
- ssh-keyscan -v

15 How do I find out the version of HP-UX Secure Shell I am using? How do I find out whether I am running HP-UX Secure Shell or the public domain version of OpenSSH?

Use the `swlist` command to display the name and version number of HP-UX Secure Shell. For example:

```
# swlist  | grep T1471
T1471AA A.06.20 HP-UX Secure Shell
```

You can also use the `what` command as shown in the following example:

```
 # what /usr/bin/scp
```

16 Is `libwrap.a` linked in HP-UX Secure Shell? Must I only configure `hosts.allow` and `hosts.deny` to use the access control provided by `tcp_wrapper`?

Yes, the `libwrap.a` archive library consisting of `tcp_wrapper version 7.6-ipv6.4`, is linked to HP-UX Secure Shell. You only need to configure `hosts.allow` and `hosts.deny` to use the access control provided by `tcp_wrapper`.

17 Is HP-UX Secure Shell vulnerable to the reported double free bug in the `zlib` compression algorithm documented at http://www.cert.org/advisories/CA-2002-07.html?

All versions of HP-UX Secure Shell starting from A.03.10 are built with support for `zlib-1.1.4` or later. So, HP-UX Secure Shell is not affected by the bug described above.

HP-UX Secure Shell versions A.06.20.004, A.06.20.005, and A.06.20.006 are built with zlib v1.2.3.

18 Is HP-UX Secure Shell vulnerable to the following CERTs: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0147 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0131?

This version of HP-UX Secure Shell is built with OpenSSL-0.9.8y and is not affected by these two CERTs. The vulnerabilities were fixed in OpenSSL-0.9.7d.

19 What options is HP-UX Secure Shell compiled with?

HP-UX Secure Shell is compiled with the following options:

- Options defined in config.h:
  - #define USE_PAM 1
  - #define IPV4_IN_IPV6 1
  - #define GSSAPI 1
  - #define KRB5 1
  - #define LIBWRAP 1
  - #define HAVE_MD5_PASSWORDS 1
  - #undef SMARTCARD
- Options defined in ssh.h:
  - #define SSH_DEFAULT_PORT 22
  - #define SSH_SERVICE_NAME ssh
- Options defined in makefile:
  - prefix=/opt/ssh
  - mandir=/opt/ssh/share/man
  - piddir=/var/run
  - PRIVSEP_PATH=/var/empty
  - bindir=/opt/ssh/bin
  - sbindir=/opt/ssh/sbin
  - xauth_path=/usr/bin/X11/xauth
  - sysconfdir=/opt/ssh/etc
  - LIBPAM=-lpam
  - LIBWRAP=-lwrap

20 As Cisco routers and switches are enabled with SSH-1 and use only DES, how do I configure HP-UX Secure Shell to work with CISCO SSH-1?

By default SSH-1 is disabled in ssh_config. To enable SSH-1, either modify the configuration file or override the protocol on the command line. The client supports DES but the server does not support DES. Issue the following command to enable SSH-1:

ssh -1 -c des

21 When two systems are separated by a firewall, can I use a HP-UX Secure Shell connection to 'swinstall' (SD-UX) to a system in a secure way?

Yes, there is a workaround to secure communication. HP-UX Secure Shell uses one connection for communication. SD-UX uses more than one connection. SD-UX first checks the system it is running on and then the system you are trying to talk to. SD-UX may then use UDP, which is not supported by HP-UX Secure Shell . A workaround to secure the communication in HP-UX Secure Shell is to use a depot file (created usign swpackage). Use either sftp or scp to copy the depot file to the local machine and then use swinstall locally with the depot file. In this scenario, the network traffic is secure. However, ensure you get the correct depot file manually and do not allow SD to select an inappropriate for your OS.

22 What is chroot? What is the procedure for setup of chroot? How does it work? Where is chroot supported in Secure Shell

The chroot functionality is an added security measure. It enables an application to start in a specified directory, restricts all its users to access that directory and the directories below it, and prevents the user from doing a cd above that specified directory. It allows restricted file and directory access to users of that application. Chroot is not an end-user feature. The system administrator must enable the chroot functionality for an application. All users of that application will automatically be subject to the restrictions imposed by chroot. For chroot to take effect, the administrator must create new directories and copy the relevant set of files to the new directories. Configuration for chroot can also be done using the script provided with the depot. For A.04.30.004/005 release or later, this script [ssh_chroot_setup.sh] is available in /opt/ssh/utils directory instead of /opt/ssh.