SunScreen™ SKIP, Release 1.5.1 Release Notes

For the Solaris Operating Environment

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A. 650-960-1300

Part No.: 806-4160-10
Revision A, May 2000

Please
Recycle

SunScreen SKIP, Release 1.5.1 Release Notes

This document contains information that was not available when the *SunScreen SKIP User's Guide, Release 1.5.1,* was printed. These release notes are the companion to that manual.

This document contains the following information:

- What is new in this release
- SKIP manuals on Product CD
- Upgrading to SKIP 1.5.1
- Upgrading cryptography modules

What is New in This Release

SunScreen SKIP 1.5.1 contains support for the Solaris™ 8 operating environment and is functionally identical to SKIP 1.5.

Features in SunScreen SKIP 1.5.1

This information is included for customers who are upgrading from older releases of SunScreen SKIP. All this information applies to SunScreen SKIP 1.5.1. SunScreen SKIP 1.5.1 is the upgrade for SunScreen SKIP 1.1.1 and SunScreen SKIP 1.5. The following is a list of the features for SunScreen SKIP 1.5.1.

- Support for Solaris 8 32–bit and 64–bit modes and IPv4.
- Support for Solaris 7 32–bit mode and 64-bit mode has been added.

Note – RC2 Cryptor is currently only available in 32-bit mode.

- The product includes numerous bug fixes and enhancements such as the support for an unlimited number of SKIP local identities as well as ACL entries and an improved random number generator.

Note – By unlimited, read “without known intrinsic limit” of the product. SunScreen SKIP 1.5.1 is bound by the resources (CPU, memory) of the system on which it is running.

- Support for 4096–bit Diffie-Hellman modulus and new DH primes has been added.
- RC–128 cryptor has been developed.
- End System and Key Store are packaged separately for easier integration with SunScreen 3.1.

ATM Limitation in SunScreen SKIP 1.5.1

SunScreen Skip 1.5.1 does not support ATM interfaces.

Fixed in SunScreen SKIP 1.5.1

The following problem is fixed in this release:

- 4297271 skiptool only sees on local certificate, when there are more available.

Features Removed from SunScreen SKIP 1.5.1

The following features were removed from SunScreen SKIP 1.5.1:

- The manual keying option for encryption/authentication modes has been removed. There is no more ESP/AH option available.
- The skiptool Unauthorized System button has been removed.

Command Changes in SunScreen SKIP 1.5.1

No commands have changed for the SunScreen SKIP 1.5.1. TABLE 1 shows the changes in commands between SunScreen SKIP1.1.1 and SunScreen SKIP 1.5.

TABLE 1 Command Changes between SunScreen Skip 1.1.1 and SunScreen Skip 1.5

Command	New Option	Old Option	Description
`skiplocal`	`-a`	`add`	`-T slottype -t certtype -n nsid -Z secret-file -c cert-file` Adds local identity to trusted CA database.
	`-r`	`rm`	`[-v] -s slot-number` Deletes the LocalID in specified slot number.
	`-l`	`list`	`[-vV] [-s slot-number]` Lists the local IDs present on the system.
	`-i`	`init`	`[-qo]` Initializes Local ID database. Creates the database if one does not exist.The `-o` option forcibly reinitializes and destroys all current identities in the database.
	`-e`	`extract`	`-s slot-number` Writes certificate that is in specified slot number to standard output.
	`-k`	`keygen`	`[-m modulus] [-E exponent] [-L lifetime] [-pV]` Generates new secret key and UDH certificate.
	`-x`	`export`	`[-s slot] [-n nsid]` Displays a skiphost command line that can be used to add ACL entry on remote system for the local host.
	`-P`	`passwd`	no options... Allows you to assign or change the password used to encrypt locally stored secrets.
	`-R`	`rmpasswd`	no options... Allows you to remove the password that is used to encrypt locally stored secrets.
`skipdb`	-a	add	`-t cert-tye -n nsid -d filename` Adds certificates to the certificate database.
	-r	rm	`[-H handle] -n nsid -k keyid` Deletes certificates from the certificate database.
	-l	list	`[-vVL] [-n nsid -k keyid]` Lists certificates in the certificate database.

TABLE 1 Command Changes between SunScreen Skip 1.1.1 and SunScreen Skip 1.5

Command	New Option	Old Option	Description
	-i	init	no options... Initializes certificate database. If the database already exists, the contents will be deleted.
	-e	extract	`[-H handle] -n nsid -k keyid` Extracts certificate to standard output.
skipca	-a	add	`-c ca-file` Adds certificates to the trusted CA database.
	-r	rm	`[-s ca-slot]` Deletes CA certificates.
	-l	list	`[-vVxL] [-s ca-slot]` Lists certificates in the trusted CA database.
	-i	init	`[qo]` Initializes the trusted CA database. Creates the database if one does not exist.The `-o` option forcibly reinitializes and destroys all current certificates in the database.
	-e	extract	`[-s ca-slot]` Extracts CA certificate to standard output.
	-R	revoke	`-s ca-slot -S serial-number` Revokes specific CA certificates.
	-U	unrevoke	`-s ca-slot -S serial-number` Extracts certificate to standard output.

For complete information, see the man pages for these commands.

Note – You can no longer list network interface statistics using the `skipstat -i` command. The new command for this is `skiphost -h`.

SKIP Manuals on Product CD

This release containsHTML adn PDF version of the *SunScreen SKIP User's Guide, Release 1.5.1,* at the following locations:

- HTML Version: `/docs/html/*`
- PDF Version: `/docs/SKIP_UG.pdf`

Upgrading to SunScreen SKIP 1.5.1

If you are upgrading from an earlier release of SKIP to SKIP 1.5 or SKIP 1.5.1, you cannot use an `acl.`*interface_name* file from the earlier version because it contains incorrect commands.

Encryption Strengths and Export Information

Encryption is 56 bits and offers a 128-bit SKIP upgrade to increase the encryption strength. This product is subject to the following export and import restrictions.

Export and Import Laws

This product is subject to United States export laws and may be subject to export and import laws of other countries. Customers will strictly comply with all such laws and obtain licenses to export, re-export, or import as may be required. Unless authorized by the United States Government, Customers will not, directly or indirectly, export or re-export products or services, nor direct products therefrom, to Afghanistan, Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, or to any embargoed or restricted country identified in the United States export laws, including but not limited to the Export Administration Regulations (15 C.F.R. Parts 730-774).

In addition, the 128-bit version of this product may only be exported or re-exported to individuals, commercial firms, and non-government end users unless otherwise authorized by the United States Government.

Customers must not be identified on any United States Government export exclusion lists. Customers will not use this product for nuclear, missile, chemical-biological weaponry, or other weapons of mass destruction.