



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

Copyright 2000 Sun Microsystems, Inc., 901 San Antonio Road • Palo Alto, CA 94303-4900 USA. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd..

Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2000 Sun Microsystems, Inc., 901 San Antonio Road • Palo Alto, CA 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd. La notice suivante est applicable à Netscape Communicator™: Copyright 1995 Netscape Communications Corporation. Tous droits réservés.

Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



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	[-go] 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
skipca	-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.
	-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 contains HTML and 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.

