



Sun™ Crypto Accelerator 1000 Board Release Notes

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

Part No. 816-2451-10
February 2002, Revision A

Send comments about this document to: docfeedback@sun.com

Copyright 2002 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303-4900 U.S.A. All rights reserved.

This product or document is 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, SunVTS, AnswerBook2, docs.sun.com, iPlanet, Sun Enterprise, Sun Enterprise Volume Manager, 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. Netscape is a trademark or registered trademark of Netscape Communications Corporation. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).

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.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

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 2002 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est 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.

Sun, Sun Microsystems, le logo Sun, SunVTS, AnswerBook2, docs.sun.com, iPlanet, Sun Enterprise, Sun Enterprise Volume Manager, 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. Netscape est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays. Ce produit comprend le logiciel développé par le Project OpenSSL pour l'utilisation dans le Toolkit OpenSSL (<http://www.openssl.org/>). Ce produit comprend le logiciel cryptographique écrite par Eric Young (eay@cryptsoft.com). Ce produit comprend le logiciel développé par Ralf S. Engelschall <rse@engelschall.com> pour l'utilisation dans le projet mod_ssl (<http://www.modssl.org/>).

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.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



Sun Crypto Accelerator 1000 Board Release Notes

This release note provides information not available at the time the *Sun Crypto Accelerator 1000 Board Installation and User's Guide* was completed.

Known Problems with iPlanet Web Servers

1. If you are running the iPlanet 4.x or 6.x administration server and the web server being managed is not running, there are several situations where dialog boxes asking for token passwords are displayed. If very large fonts are used or there are many tokens (and consequently many Enter password: lines) the buttons on the panel bottom are not displayed because the fixed size dialog box is too small. It is impossible to select the Accept button on the bottom of the panel to submit the change because the dialog box is not resizable.

There are two workarounds for this problem:

- Start the web server first from the command line or from the administration with the GUI Preference set to On/Off.
- Apply the configuration without starting up the server: Apply-> Load Configuration Files.

Reference bug: 4532645

2. iPlanet web servers cannot work with configurations where more than one realm exists, or where different users are used for different web servers.

There are two workarounds for this problem:

- Configure no more than one realm and one user for each web server.

- You can run different instances of iPlanet web server as different UNIX users, and configure `$HOME/.SUNWconn_crypto_slots` as desired for each user. Refer to the *Sun Crypto Accelerator 1000 Board Installation and User's Guide* for more information on Slot Files.

Reference bug: 4532941 and 4593111

3. The iPlanet provided utility, `pk12util` exports certificates and keys from internal (software) databases and will import them to external (hardware) databases, but will not export certificates or keys from an external database:

```
% cd /usr/iplanet/servers/alias
% pk12util -o temp.p12 -n "Our Token:Server-Cert" -d .
Enter Password or Pin for "Our Token":
Enter password for PKCS12 file:
Re-enter password:
pk12util: add cert and key failed: Unable to export. Private Key
could not be located and exported.
```

Reference bug: 4620283

4. In configuring iPlanet Web Server 6.0, after selecting the Cipher Default settings, selecting the certificate, clicking the OK button and selecting the Apply link in the far upper right corner to apply the ciphers, the `user@realm-name` entry may be removed if the steps are not executed in the exact order as prescribed in the *Sun Crypto Accelerator 1000 Board Installation and User's Guide*.

This entry is required for the web server to start up correctly with the Sun Crypto Accelerator 1000. You may see this when steps are executed in the following order:

- Select Cipher Default, SSL2 ciphers, or SSL3 ciphers
- Click on OK
- Click on Apply
- Click on Load Configuration

If you think you have executed these steps and the web server does not start up correctly, use the following workaround:

- Edit the file:

```
/usr/iplanet/servers/https-hostname.domain/config/server.xml
```

- Find the line starting with:

```
<SSLPARAMS servercertnickname="Server-Cert". . .
```

- Insert the text `user@realm-name:` prior to the text `Server-Cert` in the line, so that the changed line looks like the following:

```
<SSLPARAMS servercertnickname="user@realm-name:Server-Cert" . . .
```

- Restart the web server.
Reference bug: 4607112

Known Problems with Apache Web Servers

1. The ordering of the startup files for Apache (`/etc/rc3.d/S50apache`) and `dtlogin` (`/etc/rc2.d/S99dtlogin`) causes an ordering problem at machine boot. This may cause the console to be inaccessible for Apache password entry on startup. To work around the problem, become root and execute the following command to re-order the startup of the Apache web server:

```
# mv /etc/rc3.d/S50apache /etc/rc2.d/S95apache
```

Known Problems with the Sun Crypto Accelerator 1000 Software

1. The patch number 112438-01 must be installed prior to Sun Crypto Accelerator 1000 software installation. This patch was unavailable at press time to include on the product CD. You must download this patch from <http://sunsolve.sun.com>.
Reference bug: 4470196
2. If a slot file label is in the wrong format, slot enumeration fails. This can result in the iPlanet web server or administration server not starting. To re-enable slot enumeration, remove the incorrectly formatted slot label. Formatting problems known to cause slot-enumeration failure are:
 - missing @ symbol between user name and realm name
 - null user name or realm name

- length of username greater than 30 bytes
- token label greater than 32 bytes

If invalid labels exist in the slot file, it might prevent valid slot labels from being used. To fix this problem, edit the slot file and rename the offending slot to a name that meets the label naming restrictions and restart your web server.

Reference bug: 4622746 and 4622875

3. Software tools for key extraction are not supplied with the iPlanet Web Server 4.x release as they are with the iPlanet Web Server 6.x release.

There are two workarounds for software (internal) database key extraction:

- Download NSPR 4.12 and NSS 3.3 (or later releases) from the following website: <http://www.iplanet.com/downloads>

Install these software distributions and then run `pk12util` on the databases in order to extract certificates and keys from the software (internal) databases.

- Use Netscape Communicator 4.x or 6.x to extract the keys from the software (internal) databases.

There is not currently a work-around for extracting keys managed by the Sun Crypto Accelerator 1000 card.

Reference bug: 4621453

4. The Sun Crypto Accelerator 1000 may show up differently or not at all using `prtdiag(1M)` due to different platform implementations of the `prtdiag` utility and Open Boot PROM. For example, on an Enterprise 450 the Sun Crypto Accelerator 1000 shows up as:

```
SYS  PCI    66    4  pciclass,100000
```

Reference bug: 4343467 and 4526901

5. At the time of this document, a mechanism for extracting keys and certificate material from Sun Crypto Accelerator I is not available. Check the patch database at <http://sunsolve.sun.com> to see if a patch has been created to solve this problem.

Reference bug: 4630250