



Sun™ Crypto Accelerator 4000 Board Release Notes

Sun Microsystems, Inc.
www.sun.com

Part No. 817-0432-11
August 2003, Revision 1.0

Submit comments about this document at: <http://www.sun.com/hwdocs/feedback>

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 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 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 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 4000 Board Release Notes

These release notes describe known issues of the Sun Crypto Accelerator 4000 board. For the latest version of this document, refer to:

```
http://www.sun.com/products-n-solutions/hardware/docs/Network_Connectivity/  
Crypto_Boards/index.html
```

For the latest patches, updates, and requirements, please visit the product web pages at:

```
http://www.sun.com/products/networking/sslaccel/suncryptoaccel4000/
```

Patch 114795-01 is automatically installed when the Sun Crypto Accelerator 4000 software is installed. To verify the revision of this patch for future updates, use the `showrev -p` command.

Known Issues With the Sun Crypto Accelerator 4000 Software

Sun Fire 15K Support Issues

Patch 114795-02 for both Solaris™ 8 and 9 is required for Sun Fire 15K support.

The following patches are required on the Sun Fire 15K platform for dynamic reconfiguration (DR) support:

- Solaris 8—Patch 110900-09 and Patch 110824-04
- Solaris 9—Patch 113068-04 and Patch 112838-07

Gigabit Performance on the Sun Fire 15K Platform

The following patches enhance the board performance for Gigabit speed on the Sun Fire 15K platform.

- Patch 113218-08 for Solaris 9
- Patch 112904-08 for Solaris 9
- Patch 112233-08 for Solaris 9

The patches listed in this section are available at:

<http://sunsolve.sun.com>

Slot Requirements for the Sun Fire 15K Platform

The Sun Crypto Accelerator 4000 board is supported in 66 MHz slots only on the Sun Fire 15K platform. The board is not supported in 33 MHz PCI slots on the Sun Fire 15K platform.

Sun Crypto Accelerator 4000 Board Installation and User's Guide Errata

This section describes known errors in the *Sun Crypto Accelerator 4000 Board Installation and User's Guide*.

Supported SSL Algorithms

In Table 1-1, Supported SSL Algorithms, the ARCFOUR algorithm is supported in software for Apache Web Servers.

Zeroizing the Hardware

Appendix F describes how to perform a hardware zeroize of the board by placing a two-pin shunt (jumper) on pins 0 and 1 of the board's jumper block. However, the board does not include a jumper for this purpose, and the jumper block pins are labeled 1 through 8 and not 0 through 7. In addition, the pin set designated for performing a hardware zeroize of the board is not labeled with a Z.

FCODE Version

The FCODE version for Sun Crypto Accelerator 4000 board is 2.11. On page 15, the correct FCODE version is not listed in the `.properties` output.

Bug ID 4860042 Possible Hang on Reboot

After rebooting the system, there is a small chance that the system might hang.

Workaround: Install Patch 114795-02

Bug ID 4721396 `vca` Memory Leak

The Sun Crypto Accelerator 4000 driver `vca` may cause a memory leak. The fix for this bug provides a `vca.conf` variable to use as a manual workaround until this bug is fixed in the Solaris software.

Workaround: Add the following entry in the `kernel/drv/vca.conf` file:

```
dma-mode=1;
```

This workaround should only be necessary for low-end platforms, for example, Sun Blade™ 100 and 150.

For Solaris 9, install Patch 113218-07.

For Solaris 8, there is currently no patch.

Bug ID 4762081 Bus Speed Detection

The bus speed detection may not occur in the correct sequence on power up.

For Solaris 9, install Patch 113068-04.

For Solaris 8, install Patch 110842-11.

Bug ID 4698278 Dynamic Reconfiguration

DR of the Sun Crypto Accelerator 4000 board on Sun Fire™ V880 servers may occasionally cause a system panic.

This problem occurs during the connect phase of DR. In addition, sometimes the board may be identified as `unknown`. Both 33 MHz and 66 MHz slots are affected.

For Solaris 9, install Patch 113068-04.

For Solaris 8, install Patch 110842-11.

Bug ID 4718370 Panic When PCI Card is Configured With Hot Plug

I/O space, memory space, and the bus master are enabled even if all of the registers in the PCI configuration space are not initialized. Additionally, a PCI memory address is assigned to two resources which causes a panic.

Base address registers (BARs) are retaining the values after a power cycle to the slot while the system software needs to initialize the BARs before turning on the I/O and memory access.

For Solaris 9, install Patch 112838-07.

For Solaris 8, install Patches 110824-04 and 110900-09

Bug ID 4847585 Conflicting Minor Node Names

An instance of a network driver (for example, `fred`) can support both DLPI Style 1 and Style 2 interfaces by creating two minor modes, one with the name `fred` to support Style 2 and one with the name `fred0` to support Style 1.

The `ip_rcm` module does not support this minor node naming convention and may try to configure or unconfigure `fred0` twice despite the fact that the IP only needs to plumb either the Style 1 or Style 2 interface and not both.

Workaround: Do not create conflicting minor nodes—for example, `fred` and `fred0` where the instance number of driver `fred` is zero.

For Solaris 9, install Patch 114758-01.

For Solaris 8, install Patch 110839-04.

Bug ID 4836686 DLPI Provider Names

The `network_rcm.c` module may use the 'name' OBP property when constructing the "exported" name for Style 1 DLPI providers. This results in the exported name taking the form `network0` instead of `vca0`.

For Solaris 9, install Patch 114758-01.

For Solaris 8, install Patch 110839-04.

Bug ID 4470196 Required Solaris 8 Patches

For Solaris 8, you must install patch numbers 112438-01 and 109234-09 prior to installing the Sun Crypto Accelerator 4000 software. These patches are available on the product CD in the `patches` subdirectory, and are available for download at <http://sunsolve.sun.com>.

Note – After applying these patches, you must reboot the system *before* installing the Sun Crypto Accelerator 4000 software.

Bug ID 4621453 Key Extraction

Software tools for key extraction are not supplied with the Sun™ ONE Web Server 4.x release because they are supplied with the Sun ONE Web Server 6.x release.

Note – Sun ONE Web Servers were previously named iPlanet™ Web Servers.

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.mozilla.org>
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.

Bug ID 4630250 Keys and Certificate Material

At the time of this document, a mechanism for extracting keys and certificate material from Sun Crypto Accelerator 4000 board is not available. Check the patch database at <http://sunsolve.sun.com> to see if a patch has been created to solve this problem.

Bug ID 4796664 Internal Loopback Test

Sun Crypto Accelerator 4000 MMF boards may fail the internal loopback test of the SunVTS™ test, netlbttest. The following error messages might occur:

```
"
12/19/02 17:20:03 username SunVTS4.5: VTSID 8003 netlbttest.
FATAL vcal: "Failed to get the link up.
Probable_Cause(s):
(1)Loopback cable not connected.
(2)Faulty loopback cable.
Recommended_Action(s):
(1)Check and replace, if necessary, the loopback cable.
(2)If problem persists, call your authorized Sun service
provider.
```

Bug ID 4826508 Single Command Mode Login

When using vcaadm in Single Command mode and the login fails, the program outputs the following extraneous error message, which should be ignored:

```
Security Officer Login: so
Security Officer Password:
Login failed.

Error writing data: Bad file number
```

Bug ID 4816009 Enabling FIPS Mode

If the security officer takes ownership of an uninitialized board and enables FIPS mode while the board is actively performing operations, the board may hang.

Workaround: Do not zeroize a board that is in FIPS mode, nor initialize a card for FIPS mode while submitting cryptographic requests to the board.

Bug ID 4825721 Testing the Sun Fire 15K System

When performing Sun Fire 15K tests in a point to point configuration on MMF and UTP boards, the following errors are displayed on the console:

```
Feb 27 11:39:04 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:40:29 xc15p13-b3 vca: [ID 214153 kern.warning] WARNING:
vca1: Can't determine link paramaters!
Feb 27 11:40:29 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca1: link up 0 Mbps half duplex
Feb 27 11:40:29 xc15p13-b3 vca: [ID 732820 kern.warning] WARNING:
vca1: vce_link_stats_set: cant determine params
Feb 27 11:41:08 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link down
Feb 27 12:01:07 xc15p13-b3 vca: [ID 702911 kern.notice] NOTICE:
vca0: link up 1000 Mbps full duplex
```

This does not cause any loss of communication because the link comes back up after a few minutes.

RFE ID 4753295

By default, bulk encryption is enabled for Apache Web Server software and cannot be disabled. For Sun ONE server software, bulk encryption is disabled by default and must be enabled manually by creating an empty file (`/etc/opt/SUNWconn/criptov2/sslreg`) and restarting the Sun ONE server software. When bulk encryption is enabled for Sun ONE server software, the performance rate increases significantly for transferring large files, but may decrease slightly for small files.

Workaround: Enable bulk encryption for Sun ONE server software only when you are transferring primarily large files.

Bug ID 4822356 Rekeying the Master Key With vcaadm

When performing the `rekey master` command, `vcaadm` will return the message “Cannot get new modulus from firmware.” This does not indicate that the master key has not been regenerated. The error message is invalid; the command actually finishes successfully.

```
vcaadm{vca0@localhost, sec_officer}> rekey master
WARNING: Rekeying the master key will render all old board backups
        useless with the new keystore file.  If other boards use
this
        keystore, you will need to back up this new key and
initialize
        the other boards to use the keystore, providing the backed
up
        master key in the process.

Rekey board? (Y/Yes/N/No) [No]: y
Rekeying crypto accelerator board.  This may take a few
minutes...Done.
Cannot get new modulus from firmware.
```

Bug ID 4852120 Possible Time-Out Error

When experiencing extremely heavy network traffic and performing cryptographic operations at the same time, error messages similar to the following might be displayed.

```
Apr 17 23:44:37 xc15p13-b0 vca: WARNING: stale job(s) found in ring 30000978718
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         request 0x7820aa68
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         =====
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_id[0]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_id[1]: 0x00000000
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_cmd: 0x0013
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_flags[0]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_key_flags[1]: 0x0
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_in_len: 192
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE:         vr_out_len: 192
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vcal: fault detected in device;
service unavailable
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vcal: crypto job timeout (device
hung?)
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE: vcal: Resetting board...
Apr 18 00:08:47 xc15p13-b0 vca: WARNING: vcal: Device is in failed state!
Apr 18 00:08:47 xc15p13-b0 last message repeated 1 time
```

Workaround: Reset the Sun Crypto Accelerator 4000 board.

Known Issues With Sun ONE Web Servers

Bug ID 4532645 Administration Server Messages

If you are running the Sun ONE 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 if 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 window with the GUI Preference set to On/Off.
- Apply the configuration without starting up the server: Apply→Load Configuration Files.

Bug ID 4532941 and 4593111 Multiple Keystores

Sun ONE Web Servers have difficulty working with configurations where more than one keystore exists. This issue is fixed in Sun ONE Web Server 6.0 Service Pack 5 (SP5).

Workaround: Configure no more than one keystore for all web server instances. You may then configure a different keystore user for each web server instance. This will keep keys for each web server instance separate from one another.

Bug ID 4620283 pk12util Utility

The Sun ONE 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.
```

Bug ID 4607112 Cipher Default Settings

In configuring Sun ONE Web Server 6.0, after selecting the Cipher Default settings, selecting the certificate, selecting the OK button and selecting the Apply link in the far upper right corner to apply the ciphers, the `username:password` entry may be removed if the steps are not executed in the exact order as prescribed in the *Sun Crypto Accelerator 4000 Board Installation and User's Guide*. This issue is fixed in Sun ONE Web Server 6.0 Service Pack 3 (SP3).

This entry is required for the web server to start up correctly with the Sun Crypto Accelerator 4000 board. You may see this when steps are executed in the following order:

1. Select Cipher Default, SSL2 ciphers, or SSL3 ciphers
2. Select OK
3. Select Apply
4. Select 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 *keystore_name*: prior to the text *Server-Cert* in the line, so that the changed line is as follows:

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

- Restart the web server.

Supported Version of Apache Web Server

This release of the Sun Crypto Accelerator 4000 software supports Apache 1.3.26.

Known Issues With Apache Web Servers

Bug ID 4766977 Required Solaris 8 Patches

To configure the Sun Crypto Accelerator 4000 board for use with the Apache Web Server in Solaris 8, the patch number 109234-09 must be installed prior to installing the Sun Crypto Accelerator 4000 software. This patch is available on the product CD in the `patches` subdirectory, and is available for download at <http://sunsolve.sun.com>.

Note – After applying this patch, you must reboot the system **before** installing the Sun Crypto Accelerator 4000 software.

The Apache Web Server cannot be configured for use with the *Sun Crypto Accelerator 1000* board and the *Sun Crypto Accelerator 4000* board at the same time. If both boards are configured to use the Apache Web Server at the same time, Apache will not work correctly.

Only install the Sun Crypto Accelerator 4000 `SUNWkc12a` software package if you plan to use the board with Apache Web Server 1.3.26. If you plan to use any other configuration or version of Apache Web Server, do not install the `SUNWkc12a` package.

Startup Files

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.

Workaround: Become root and issue the following command to reorder the startup of the Apache Web Server:

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

