# Sun™ Crypto 加速器 4000 板 1.1 版本说明

Sun Microsystems, Inc.
www.sun.com

部件号 817-5932-10
2004 年 1 月，修订版 A

请访问以下网址提交关于本文档的意见：http://www.sun.com/hwdocs/feedback

---

请回收

Adobe PostScript

# Sun Crypto 加速器 4000 板 1.1 版本说明

此版本说明介绍了 Sun Crypto 加速器 4000 板的已知问题。有关本文档的最新版本以及最新的已知问题，请参阅：

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

有关最新的修补程序、更新版本和要求，请访问以下地址的产品网页：

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

本文档中列出的修补程序在 `http://sunsolve.sun.com` 中提供。 Solaris 更新版本包含以前版本的修补程序。使用 `showrev -p` 命令可以确定是否已经安装了必要的修补程序。

安装最新版本的修补程序。每发布一个新版本的修补程序，破折号后的数字 （例如 -01）就会增加。如果 Web 站点上的版本高于本文档中列出的版本，请使用最新的版本。

如果 SunSolve℠ Web 站点中未提供您需要的修补程序，请与本地销售或服务代表联系。

# 与 Sun Crypto 加速器 4000 软件相关的已知问题

## Sun Fire 15K 支持问题

Sun Fire 15K 平台上必须具有以下修补程序，才能获得动态重配置 (DR) 支持：

- 对于 Solaris 8，请安装修补程序 110900-10 和修补程序 110824-04
- 对于 Solaris 9，请安装修补程序 113068-04 和修补程序 112838-08

### Sun Fire 15K 平台上的千兆位性能

以下修补程序改进了板的性能，使其能在 Sun Fire 15K 平台上达到千兆位速率。

- 对于 Solaris 9，请安装修补程序 113218-08
- 对于 Solaris 9，请安装修补程序 112904-08
- 对于 Solaris 9，请安装修补程序 112233-08

### Sun Fire 15K 平台的插槽要求

在 Sun Fire 15K 平台上，只有 66 MHz 插槽中才支持 Sun Crypto 加速器 4000 板。

## Sun ONE Application Server 7 的评估版本

用于安装应用服务器软件的 `iplsslcfg` 脚本与 Sun ONE Application Server 7 的评估版本不兼容。此脚本与其它所有版本都能配合使用。请使用 `modutil` 命令来安装应用服务器的评估版本。

## `vcaadm` 锁定文件

`vcaadm` 锁定文件 (`.trustlock`) 用于防止两个 `vcaadm` 进程之间的更改改写。如果 `vcaadm` 实用程序未正确关闭，此锁定文件可能会阻止对信任数据库的访问。如果出现此问题，您会收到以下错误消息：

```
Lock file prevented read access to trust DB: Timer expired
```

解决方法：删除 ${HOME}/.vcaadm 目录中的 .trustlock 锁定文件。

```
# rm ${HOME}/.vcaadm/.trustlock
```

## 错误 ID 4948204 FCODE 成功运行后， pcicfg 不能重新浏览 BAR

如果 pcicfg 实用程序在 FCODE 中断后重新浏览基地址寄存器 (BAR)，则会将不正确的地址空间量分配给 BAR。如果分配的地址空间少于 FCODE 需要的空间， busra 实用程序会检测到错误的自由调用并导致无配置进程期间的操作失败。

- 对于 Solaris 9，请安装修补程序 112838-08
- 对于 Solaris 8，请安装修补程序 110900-10

## 错误 ID 4922816 带外 IPsec 可能不卸载

如果硬件的版本比 Security Association (SA) 的版本更新，带外 IPsec 则不会卸载。如果 Sun Crypto 加速器 4000 板配置为在系统中使用现有的 SA 来执行直插式 IPsec 加速，则必须重新加载 Security Association 数据库 (SADB) 才能使用现有的 SA。通过重新引导系统或使用 ipseckey 实用程序，即可执行重新加载。有关如何使用 ipseckey 实用程序的信息，请参阅 《*IPsec and IKE Administration Guide*》。

## 错误 ID 4979555 vca 初始化失败

在某些系统上对 vca 驱动程序进行初始化期间，消息日志中可能会写入以下警告消息：

```
WARNING: vca0: Unknown pci device(0x582114e4) found on bus 1, slot 0
vca0: PCI initialization failed, retry ...
```

这些消息表示对 Sun Crypto 加速器 4000 板进行的内部 PCI 总线初始扫描失败，同时表示随后重新扫描 （重试）已成功。如果重新扫描失败，则会在这些消息后随附其它信息，但是这些初始消息并不表示板出现故障。

## 错误 ID 4721396 vca 内存漏失

Sun Crypto 加速器 4000 驱动程序 vca 可能会导致核心内存漏失。此错误的修复方案中提供了一个 vca.conf 变量，在 Solaris 软件解决此错误之前，可以手动添加此变量以解决此错误。

解决方法：在 kernel/drv/vca.conf 文件中添加以下条目：

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

此解决方法仅适用于低端平台，例如， Sun Blade™ 100 和 150。

- 对于 Solaris 9，请安装修补程序 113218-08

## 错误 ID 4762081 总线速率检测

在正常的开机过程中，可能不会执行总线速率检测。

- 对于 Solaris 9，请安装修补程序 113068-04
- 对于 Solaris 8，请安装修补程序 110842-11

## 错误 ID 4698278 动态重配置

在 Sun Fire™ V880 服务器上对 Sun Crypto 加速器 4000 板进行 DR 时，偶尔可能会导致系统紧急状况。

此问题出现在 DR 的连接阶段。此外，板有时可能会被识别为 unknown。 33 MHz 和 66 MHz 插槽都会受此影响。

- 对于 Solaris 9，请安装修补程序 113068-04
- 对于 Solaris 8，请安装修补程序 110842-11

## 错误 ID 4718370 使用热插拔方法配置 PCI 卡时出现系统紧急状况

即使 PCI 配置空间中的所有寄存器均未初始化，也仍然会启用 I/O 空间、内存空间和总线主控。此外，还会为导致系统紧急状况的两个资源分配 PCI 内存地址。

基地址寄存器 (BAR) 在对插槽进行先关再开操作后保留其值，而系统软件需要初始化 BAR 后才能启动 I/O 和内存访问。

- 对于 Solaris 9，请安装修补程序 112838-08
- 对于 Solaris 8，请安装修补程序 110824-04 和修补程序 110900-10

# 错误 ID 4847585 小节点名称冲突

网络驱动程序的例程（例如 `fred`）可以通过创建两个小节点来同时支持 DLPI Style 1 和 Style 2 接口，一个使用名称 `fred` 来支持 Style 2，一个使用名称 `fred0` 来支持 Style 1。

`ip_rcm` 模块不支持此小节点命名惯例，并且可能会尝试配置或取消配置 `fred0` 两次，而不管以下实际情况：IP 只需要探测 Style 1 和 Style 2 的其中一个而不是两个都要探测。

解决方法：如果驱动程序 `fred` 的例程号为零，则不创建有冲突的小节点 — 例如 `fred` 和 `fred0`。

- 对于 Solaris 9，请安装修补程序 114758-01
- 对于 Solaris 8，请安装修补程序 110839-04

# 错误 ID 4836686 DLPI 提供商名称

为 Style 1 DLPI 提供商构建 “导出”名称时， `network_rcm.c` 模块可能会使用 'name' OBP 属性。这样会导致导出名称使用 `network0` 形式而不是 `vca0` 形式。

- 对于 Solaris 9，请安装修补程序 114758-01
- 对于 Solaris 8，请安装修补程序 110839-04

# 错误 ID 4470196 Solaris 8 必需的修补程序

对于 Solaris 8，必须在安装 Sun Crypto 加速器 4000 软件之前安装修补程序 112438-01 和修补程序 109234-09。这些修补程序位于产品 CD 的 `patches` 子目录下，也可以从 `http://sunsolve.sun.com` 下载。

---

**注意 –** 应用这些修补程序后，您***必须***重新引导系统方可安装 Sun Crypto 加速器 4000 软件。

---

# 错误 ID 4621453 密钥抽取

Sun™ ONE Web 服务器 4.x 版本没有附带用于抽取密钥的软件工具，但 Sun ONE Web 服务器 6.x 版本附带了此类工具。

---

**注意 –** Sun ONE Web 服务器以前称为 iPlanet™ Web 服务器。

---

可用两种方法来解决软件 （内部）数据库密钥抽取问题：

- 从 `http://www.mozilla.org` 网站下载 NSPR 4.12 和 NSS 3.3 （或更高版本）

  安装这些软件产品，然后在数据库上运行 `pk12util`，以便从软件 （内部）数据库抽取证书和密钥。
- 使用 Netscape Communicator 4.x 或 6.x 从软件 （内部）数据库抽取密钥。

## 错误 ID 4630250 密钥和证书资料

本文档出版时，还没有办法从 Sun Crypto 加速器 4000 板抽取密钥和证书资料。您可访问 `http://sunsolve.sun.com` 网站的修补程序数据库，看看是否提供了能够解决这一问题的修补程序。

## 错误 ID 4836099 在没有回送电缆时， SunVTS `netlbtest` 内部回送失败

Sun Crypto 加速器 4000 在 MMF 板上运行 SunVTS™ 测试软件包 `netlbtest` 的内部回送测试程序时，可能会失败，并且会出现以下错误消息：

```
"
12/19/02 17:20:03 username SunVTS4.5: VTSID 8003 netlbtest.
  FATAL vca1:    "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.
```

可以忽略这些消息。

解决方法：在连接回送电缆后执行 SunVTS 内部回送测试。

## 错误 ID 4826508 单命令模式登录

在单命令模式下使用 `vcaadm` 且登录失败时，程序会输出以下外来错误消息。请将其忽略：

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

Error writing data: Bad file number
```

## 错误 ID 4816009 启用 FIPS 模式

如果安全主管拥有未初始化的板，并在该板有效执行操作时启用 FIPS 模式，则板可能会挂起。

解决方法：在将加密请求提交给板时，不要零置 FIPS 模式下的板，或者不要初始化板以用于 FIPS 模式。

## RFE ID 4753295

默认情况下，系统会为 Apache Web 服务器软件启用批量加密，且不能禁用。对于 Sun ONE 服务器软件，批量加密在默认情况下禁用，并且必须通过以下手动方法才能启用：创建空文件 (`/etc/opt/SUNWconn/cryptov2/sslreg`)，然后重新启动 Sun ONE 服务器软件。为 Sun ONE 服务器软件启用批量加密后，传送较大文件的速率会大大提高，但对于较小文件，速率可能会稍微降低。

解决方法：仅在传送大文件的情况下为 Sun ONE 服务器软件启用批量加密。

## 错误 ID 4822356 使用 vcaadm 重新设置主密钥

执行 `rekey master` 命令时，`vcaadm` 会返回消息：“无法从固件中获得新的模板”。这并非表示主密钥未被重新生成。此错误消息无效；命令实际上已成功完成。

```
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.
```

## 错误 ID 4852120 可能出现超时错误

在网络通信极其繁忙时，如果执行加密操作，则可能会显示与以下内容相似的错误信息。

```
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: vca1: fault detected in device;
service unavailable
Apr 17 23:44:37 xc15p13-b0 genunix: WARNING: vca1: crypto job timeout (device
hung?)
Apr 17 23:44:37 xc15p13-b0 vca: NOTICE: vca1: Resetting board...
Apr 18 00:08:47 xc15p13-b0 vca: WARNING: vca1: Device is in failed state!
Apr 18 00:08:47 xc15p13-b0 last message repeated 1 time
```

解决方法：重置 Sun Crypto 加速器 4000 板。

## 错误 ID 4757594 vca.conf 变量

此错误的修复方案中提供了一个 vca.conf 变量，在 Solaris 软件解决此错误之前，可以手动添加此变量以解决此错误。此错误已在 Solaris 9 4/03 中修复。

解决方法：在 kernel/drv/vca.conf 文件中添加以下条目：

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

此解决方法仅适用于低端平台，例如， Sun Blade™ 100 和 150。

- 对于 Solaris 9 4/03 之前的 Solaris 版本，请安装修补程序 112233-08
- 对于 Solaris 8，请安装修补程序 108528-23

# 与 Sun ONE Web 服务器相关的已知问题

## 错误 ID 4532645 管理服务器消息

运行 Sun ONE 4.x 或 6.x 管理服务器时，如果没有运行它所管理的 Web 服务器，则在数种情形下，可能会出现要求输入令牌密码的对话框。如果使用很大的字体，或者存在多种令牌 （因此需要输入很多密码：行），则不会显示面板底部的按钮，因为对话框太小，且大小固定。由于对话框的大小无法调整，因此无法从面板底部选择 “接受”按钮来提交您的更改。

该问题有两种解决方法：

- 首先从命令行或管理窗口启动 Web 服务器，并将 GUI 首选项设为开/关。
- 在不启动 Web 服务器的前提下应用配置：Apply （应用） → Load Configuration Files （加载配置文件）。

## 错误 ID 4532941 和 4593111 多个密钥库

Sun ONE Web 服务器不便与具有多个密钥库的配置一起工作。此问题会在 Sun ONE Web 服务器 6.0 服务包 5 (SP5) 中得到解决。

解决方法：只为所有 Web 服务器例程配置一个密钥库。然后，您可以为每个 Web 服务器例程配置不同的密钥库用户，从而使每个 Web 服务器例程的密钥相互独立。

## 错误 ID 4620283 pk12util 实用程序

Sun ONE 附带了实用程序 pk12util，用于从内部软件数据库中导出证书和密钥，然后将其导入外部硬件数据库。但是 pk12util 实用程序不能从外部硬件数据库 （例如 Sun Crypto 加速器板）中导出证书或密钥：

```
% 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.
```

解决方法：使用 pk11export 实用程序从板中抽取密钥有关详情，请参阅 《*Sun Crypto 加速器 4000 板安装和用户指南*》。

## 错误 ID 4607112 密码默认设置

配置 Sun ONE Web 服务器 6.0 期间，在选择 “Cipher Default”设置、选择证书、选择 “OK”按钮并选择右上角的 “Apply”链接以应用密码之后，如果不严格按照 《*Sun Crypto 加速器 4000 板安装和用户指南*》中介绍的顺序进行操作，则 *username:password* 条目可能会被删除。此问题会在 Sun ONE Web 服务器 6.0 服务包 3 (SP3) 中得到解决。

这是 Web 服务器正确启动 Sun Crypto 加速器 4000 板必不可少的条目。按以下顺序执行这些步骤时会出现此条目：

1. 选择 “Cipher Default”、 SSL2 密码或 SSL3 密码
2. 选择 “OK”
3. 选择 “Apply”
4. 选择 “Load Configuration”

如果您确信按上述顺序执行了这些步骤，但 Web 服务器并未正确启动，请采用以下解决方法：

- 编辑文件：

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

- 找到以下列内容开头的行：

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

- 在此行的文字 `Server-Cert` 之前插入文字 *keystore_name*:，如下所示：

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

- 重新启动 Web 服务器。

# Apache Web 服务器的支持版本

本 Sun Crypto 加速器 4000 软件版本支持 Apache 1.3.26。

# 与 Apache Web 服务器相关的已知问题

## 错误 ID 4766977 Solaris 8 必需的修补程序

要在 Solaris 8 下配置 Sun Crypto 加速器 4000 板以便与 Apache Web 服务器配合使用，必须在安装 Sun Crypto 加速器 4000 软件之前先安装修补程序 109234-09。此修补程序位于产品 CD 的 `patches` 子目录下，也可以从 `http://sunsolve.sun.com` 下载。

---

**注意 –** 应用此修补程序后，您***必须***重新引导系统方可安装 Sun Crypto 加速器 4000 软件。

---

Apache Web 服务器不能同时与 *Sun Crypto 加速器* ***1000*** 板和 *Sun Crypto 加速器* ***4000*** 板配合使用。如果让这两个板同时使用 Apache Web 服务器， Apache 将无法正常工作。

只有您准备将板与 Apache Web 服务器 1.3.26 配合使用时，才有必要安装 Sun Crypto 加速器 4000 `SUNWkcl2a` 软件包。如果使用其它配置或 Apache Web 服务器版本，则不必安装 `SUNWkcl2a` 软件包。

# 启动文件

Apache 的启动文件 (`/etc/rc3.d/S50apache`) 与 `dtlogin` 的启动文件 (`/etc/rc2.d/S99dtlogin`) 的顺序会导致计算机启动时的顺序问题。这可能会导致启动时不可访问控制台而无法输入 Apache 密码。

解决方法：以 root 用户身份发出以下命令，重新调整 Apache Web 服务器的启动顺序：

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