



Sun™ Crypto Accelerator 1000 板 1.1 版本发布说明

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

部件编号 816-4574-11
2002 年 7 月，修订版 A

请将有关本文档的意见发送至: docfeedback@sun.com

版权所有 2002 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A。保留所有权利。

本产品或文档的发行受限制本产品或文档使用、复制、发行和反编译的许可证的制约。没有 Sun 和其许可证发行者事先书面授权，不得以任何形式、任何方法复制本产品或文档的任何部分。第三方软件，包括字体技术已从 Sun 供应商获得版权和许可。

产品的某些部件可能源于 Berkeley BSD 系统 - 已从 University of California 获得相关许可。UNIX 是在美国及其它国家 / 地区的注册商标，Sun 已从 X/Open Company, Ltd. 获得独占使用许可。

Sun、Sun Microsystems、Sun 徽标、SunVTS、AnswerBook2、docs.sun.com、iPlanet、Sun Enterprise、Sun Enterprise Volume Manager 以及 Solaris 是 Sun Microsystems, Inc. 在美国以及其它国家 / 地区的商标、注册商标或服务标志。所有 SPARC 商标的使用都受许可证的制约，而且所有 SPARC 商标都是 SPARC International, Inc. 在美国以及其它国家 / 地区的商标或注册商标。带有 SPARC 商标的产品，其体系结构以 Sun Microsystems, Inc. 开发的体系结构为基础。Netscape 是 Netscape Communications Corporation 的商标或注册商标。本产品包括 OpenSSL Project 开发的用于 OpenSSL Toolkit 的软件 (<http://www.openssl.org/>)。本产品包括 Eric Young (eay@cryptsoft.com) 编写的加密软件。本产品包括 Ralf S. Engelschall <rse@engelschall.com> 的用于 mod_ssl 项目的软件 (<http://www.modssl.org/>)。

OPEN LOOK 和 Sun™ Graphical User Interface 是由 Sun Microsystems, Inc. 为其用户和许可证持有者开发的。Sun 承认 Xerox 为计算机行业研究和开发可视或图形用户界面方面所做的先行努力。Sun 以非独占方式从 Xerox 获得 Xerox 图形用户界面的许可证，该许可证涵盖实施 OPEN LOOK GUI 和 Sun 书面许可证协议的许可证持有人。

文档以“原样”提供，除非所拒绝的在法律上无效，否则不进行任何明文或隐含的担保，不做担保的范围包括但不限于以下方面：销路好坏、特殊用途的适用性或侵权与否等。



请回收
利用



Adobe PostScript

Sun Crypto Accelerator 1000 板 1.1 版本发布说明

本发布说明提供 *Sun Crypto Accelerator 1000 板 1.1 版本安装与用户指南* 完成时未提供的信息。

iPlanet Web 服务器的已知问题

1. 运行 iPlanet 4.x 或 6.x 管理服务器时，如果被管理的 Web 服务器没有运行，则在多数情形下会出现要求输入标记密码的对话框。如果使用的是大字体或者存在多种标记（以及随后输入很多密码：行），屏幕上就不会显示出面板底部的按钮，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。

该问题有两个临时解决办法：

- 将 GUI 参数选择设为开 / 关，从命令行或管理工具启动 Web 服务器。
- 在不启动服务器的情况下应用配置：Apply（应用）->Load Configuration Files（载入配置文件）。

问题参考号：4532645

2. 在以下配置下，iPlanet Web 服务器无法运行：不同 Web 服务器包含多个领域、使用不同的用户。

该问题有两个临时解决办法：

- 仅为每个 Web 服务器配置不超过一个的领域和单一用户。

- 可以使用不同的 UNIX 用户身份来运行不同的 iPlanet Web 服务器实例，并按需为每个用户配置 `$HOME/.SUNWconn_crypto_slots`。有关插槽文件的详细信息，请参阅 *Sun Crypto Accelerator 1000 板 1.1 版本安装与用户指南*。

问题参考号：4532941 和 4593111

3. iPlanet 附带的实用程序 `pk12util` 将从内部（软件）数据库导出证书和密钥，并将他们导入外部（硬件）数据库，但并不从外部数据库导出证书或密钥：

```
% 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.
```

问题参考号：4620283

4. 在配置 iPlanet Web Server 6.0 时，在选择 Cipher Default（密码默认值）设置、选择证书、单击 OK（确定）按钮并选择右上角的 Apply（应用）链接以应用密码之后，如果不是严格按照 *Sun Crypto Accelerator 1000 板 1.1 版本安装与用户指南* 中介绍的顺序进行操作，`user@realm-name` 条目可能会被删除。

这是 Web 服务器正确启动 Sun Crypto Accelerator 1000 板必不可少的条目。按以下顺序执行这些操作之后就会出现此条目：

- 依次选择 Cipher Default（密码默认值）、SSL2 密码或 SSL3 密码
- 单击 OK（确定）
- 单击 Apply（应用）
- 单击 Load Configuration（载入配置）

如果您确认已经执行了这些操作，但 Web 服务器却并未正确启动，请采用以下解决办法：

- 编辑此文件：

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

- 找到以此开头的行：

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

- 在此行的文字 `Server-Cert` 之前插入文字 `user@realm-name:`，这样，此行更改后就与下行类似：

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

- 重新启动 Web 服务器。

问题参考号：4607112

支持的 Apache Web 服务器版本

此 Sun Crypto Accelerator 1000 软件版本支持 Solaris 8 上的 Apache 1.3.12 和 1.3.26。另外，它还支持 Solaris 9 上的 Apache 1.3.22 和 Apache 1.3.26。此支持通告适用于操作系统附带的 Apache 版本以及通过正式 Sun 补丁程序发布的 Apache 版本。

Apache Web 服务器的已知问题

1. Apache (`/etc/rc3.d/S50apache`) 与 `dtlogin` (`/etc/rc2.d/S99dtlogin`) 启动文件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无法访问控制台，以输入 Apache 密码。要解决这一问题，请以 `root` 身份执行以下命令，调整 Apache Web 服务器的启动顺序：

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

Sun Crypto Accelerator 1000 1.1 版本软件的已知问题

1. 对于 Solaris 8 操作系统，安装 Sun Crypto Accelerator 1000 1.1 版本软件之前，必须先安装编号为 112438-01 的补丁程序。该补丁程序位于产品 CD 的 `patches` 子目录下；您也可以从 <http://sunsolve.sun.com> 下载该补丁程序。

问题参考号：4470196

2. iPlanet Web Server 4.x 版本没有附带用于提取密钥的软件工具，而 iPlanet Web Server 6.x 版本附带了此工具。

有两种途径可以解决软件（内部）数据库密钥提取问题：

- 从网站 <http://www.iplanet.com/downloads> 下载 NSPR 4.12 和 NSS 3.3（或更新版本）

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）数据库提取证书和密钥。

- 使用 Netscape Communicator 4.x 或 6.x 从软件（内部）数据库提取密钥。

目前还没有方法提取由 Sun Crypto Accelerator 1000 板管理的密码。

问题参考号：4621453

3. 使用 `prtdiag(1M)` 时 Sun Crypto Accelerator 1000 板会以不同方式显现或是根本不显现，这是由于 `prtdiag` 实用程序的不同平台实现方法以及 Open Boot PROM 所致。例如，在 Enterprise 450 上，Sun Crypto Accelerator 1000 板将按以下形式显现：

SYS	PCI	66	4	pciclass,100000
-----	-----	----	---	-----------------

问题参考号：4343467 和 4526901

4. 在本文档出版时，还没有办法从 Sun Crypto Accelerator I 提取密钥和证书资料。请参阅 <http://sunsolve.sun.com> 上的补丁程序数据库，看看其中是否提供了能够解决这一问题的补丁程序。

问题参考号：4630250

5. 在运行 Solaris 9 操作系统的 Sun Fire™ V880 系统中，用户不能在 66 MHz 插槽中热插拔 Sun Crypto Accelerator 1000 板，而运行 Solaris 8 的系统则不会发生此问题。将来的补丁程序将会解决此问题。

在 Solaris 9 操作系统中，用户可在关闭电源的情况下将 Sun Crypto Accelerator 1000 板装入此类插槽中，并且随后即可使用。另外，在 Solaris 9 操作系统中，用户还可在 33 MHz 插槽中热插拔此板。

问题参考号：4698278