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

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

Part No. 817-0431-10
May 2003, Revision A

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

Declaration of Conformity (Fiber MMF)

Compliance Model Number: Venus-FI

Product Family Name: Sun Crypto Accelerator 4000 - Fiber (X4012A)

EMC

USA - FCC Class B

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass
EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997 Class B

EN55024:1998 Required Limits:

EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines, 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass

EN61000-3-2:1995 + A1, A2, A14 Pass

EN61000-3-3:1995 Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN 60950:2000, 3rd Edition
IEC 60950:2000, 3rd Edition
Evaluated to all CB Countries
UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

Declaration of Conformity (Copper UTP)

Compliance Model Number: Venus-CU
Product Family Name: Sun Crypto Accelerator 4000 - Copper (X4011A)

EMC

USA - FCC Class B

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This equipment may not cause harmful interference.

2) This equipment must accept any interference that may cause undesired operation.

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in both Telecom Centers and Other Than Telecom Centers per (as applicable):

EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class B
EN61000-3-2	Pass
EN61000-3-3	Pass

EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines,
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor Signal Lines > 10m.
EN61000-4-6	3 V
EN61000-4-11	Pass

As information Technology Equipment (ITE) Class B per (as applicable):

EN55022:1998/CISPR22:1997	Class B
EN55024:1998 Required Limits:	
EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines, 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass
EN61000-3-2:1995 + A1, A2, A14	Pass
EN61000-3-3:1995	Pass

Safety

This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN 60950:2000, 3rd Edition

IEC 60950:2000, 3rd Edition

Evaluated to all CB Countries

UL 60950, 3rd Edition, CSA C22.2 No. 60950-00

Supplementary Information

This product was tested and complies with all the requirements for the CE Mark.

/S/

Dennis P. Symanski
Manager, Compliance Engineering
Sun Microsystems, Inc.
4150 Network Circle, MPK15-102
Santa Clara, CA 95054, USA
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Pamela J Dullaghan
Quality Program Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: +44 1 506 672 395
Fax: +44 1 506 672 855

Regulatory Compliance Statements

Your Sun product is marked to indicate its compliance class:

- Federal Communications Commission (FCC) — USA
- Industry Canada Equipment Standard for Digital Equipment (ICES-003) — Canada
- Voluntary Control Council for Interference (VCCI) — Japan
- Bureau of Standards Metrology and Inspection (BSMI) — Taiwan

Please read the appropriate section that corresponds to the marking on your Sun product before attempting to install the product.

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables to comply with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted-pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

FCC Class B Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Shielded Cables: Connections between the workstation and peripherals must be made using shielded cables in order to maintain compliance with FCC radio frequency emission limits. Networking connections can be made using unshielded twisted pair (UTP) cables.

Modifications: Any modifications made to this device that are not approved by Sun Microsystems, Inc. may void the authority granted to the user by the FCC to operate this equipment.

ICES-003 Class A Notice - Avis NMB-003, Classe A

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

ICES-003 Class B Notice - Avis NMB-003, Classe B

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

VCCI 基準について

クラス A VCCI 基準について

クラス A VCCI の表示があるワークステーションおよびオプション製品は、クラス A 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

クラス B VCCI 基準について

クラス B VCCI の表示  があるワークステーションおよびオプション製品は、クラス B 情報技術装置です。これらの製品には、下記の項目が該当します。

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

BSMI Class A Notice

The following statement is applicable to products shipped to Taiwan and marked as Class A on the product compliance label.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻 干擾，在這種情況下，使用者 會被要求採取某些適當的對策。

Contents

Tables

Preface

The *Sun Crypto Accelerator 4000 Board Installation and User's Guide* lists the features, protocols, and interfaces of the Sun™ Crypto Accelerator 4000 board and describes how to install, configure, and manage the board in your system.

This book assumes that you are a network administrator with experience configuring one or more of the following: Solaris™ operating environment, Sun platforms with PCI I/O cards, Sun™ ONE and Apache Web Servers, IPsec, SunVTS™ software, and certification authority acquisitions.

How This Book Is Organized

This book is organized as follows:

- Chapter 1 lists the product features, protocols, and interfaces of the Sun Crypto Accelerator 4000 board, and describes the hardware and software requirements.
- Chapter 2 describes how to install and remove the Sun Crypto Accelerator 4000 hardware and software.
- Chapter 3 defines the Sun Crypto Accelerator 4000 tunable driver parameters and describes how to configure them with the `ndd` utility and the `vca.conf` file. This chapter also describes how to enable autonegotiation or forced mode for link parameters at the OpenBoot™ PROM interface and how to configure the network `hosts` file.
- Chapter 4 describes how to configure the Sun Crypto Accelerator 4000 board and manage keystores with the `vcaadm` and `vcadiag` utilities.
- Chapter 5 explains how to configure the Sun Crypto Accelerator 4000 board for use with Sun ONE Web Servers.
- Chapter 6 explains how to configure the Sun Crypto Accelerator 4000 board for use with Apache Web Servers.

- Chapter 7 describes how to test the Sun Crypto Accelerator 4000 board with the SunVTS diagnostic application and the onboard FCode self-test. This chapter also provides troubleshooting techniques with OpenBoot PROM commands.
- Appendix A lists the specifications for the Sun Crypto Accelerator 4000 board.
- Appendix B lists directives for using Sun Crypto Accelerator 4000 software to configure SSL support for Apache Web Servers.
- Appendix C describes the software supplied with the Sun Crypto Accelerator 4000 board and how to build OpenSSL-compatible applications to take advantage of the cryptographic acceleration features of the board.
- Appendix D provides software notices and licenses from other software organizations that govern the use of third-party software used with the Sun Crypto Accelerator 4000 board.
- Appendix E provides a description of the Sun Crypto Accelerator 4000 commands and lists the online manual pages for each command.
- Appendix F describes how to zeroize the Sun Crypto Accelerator 4000 board to the factory state which is the `failsafe` mode for the board.
- Appendix G provides answers to frequently asked questions.

Using UNIX Commands

This document does not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices.

See one or more of the following for this information:

- *Solaris Hardware Platform Guide*
- Online documentation for the Solaris operating environment available at: `http://docs.sun.com`
- Other software documentation that you received with your system

Typographic Conventions

Typeface	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123`	What you type, when contrasted with on-screen computer output	`% su` `Password:`
AaBbCc123	Book titles, new words or terms, words to be emphasized	Read Chapter 6 in the *User's Guide.* These are called *class* options. You *must* be superuser to do this.
	Command-line variable; replace with a real name or value	To delete a file, type `rm` *filename.*

Shell Prompts

Shell	Prompt
C shell	*machine_name*%
C shell superuser	*machine_name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Accessing Sun Documentation Online

You can view, print, or purchase a broad selection of Sun documentation, including localized versions, at:

`http://www.sun.com/documentation`

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

`docfeedback@sun.com`

Please include the part number (817-0431-10) of your document in the subject line of your email.

CHAPTER 1

Product Overview

This chapter provides an overview of the Sun Crypto Accelerator 4000 board, and contains the following sections:

Product Features

The Sun Crypto Accelerator 4000 board is a Gigabit Ethernet-based network interface card that supports cryptographic hardware acceleration for IPsec and SSL (both symmetric and asymmetric) on Sun servers. In addition to operating as a standard Gigabit Ethernet network interface card for unencrypted network traffic, the board contains cryptographic hardware to support a higher throughput for encrypted IPsec traffic than the standard software solution.

Key Protocols and Interfaces

The Sun Crypto Accelerator 4000 board is interoperable with existing Ethernet equipment assuming standard Ethernet minimum and maximum frame size (64 to 1518 bytes), frame format, and compliance with the following standards and protocols:

- Full-size PCI 33/66 Mhz, 32/64-bit
- IEEE 802.3 CSMA/CD (Ethernet)
- IEEE 802.2 Logical Link Control
- SNMP (limited MIB)
- Full- and half-duplex Gigabit Ethernet interface (IEEE 802.z)
- Universal dual voltage signaling (3.3V and 5V)

Key Features

- Gigabit Ethernet with either copper or fiber interface
- Accelerates IPsec and SSL cryptographic functions
- Session establishment rate: up to 4300 operations per second
- Bulk encryption rate: up to 800 Mbps
- Provides up to 2048-bit RSA encryption
- Delivers up to 10 times faster 3DES bulk data encryption
- Provides tamper-proof, centralized security key and certificate administration for Sun ONE Web Server for increased security and simplified key management
- Designed for FIPS 140-2 Level 3 certification
- Low CPU utilization—frees up server system resource and bandwidth
- Secure private key storage and management
- Dynamic reconfiguration (DR) and redundancy/failover support on Sun's midframe and high-end servers
- Load balancing for RX packets among multiple CPUs
- Full flow control support (IEEE 802.3x)

The Sun Crypto Accelerator 4000 boards are designed to comply with the security requirements for cryptographic modules as documented in the Federal Information Processing Standard (FIPS) 140-2, Level 3.

Supported Applications

- Solaris 8 and 9 operating environments (IPsec VPN)
- Sun ONE Web Server
- Apache Web Server

Supported Cryptographic Protocols

The board supports the following protocols:

- IPsec for IPv4 and IPv6, including IKE
- SSLv2, SSLv3, TLSv1

The board accelerates the following IPsec functions:

- ESP (DES, 3DES) Encryption

The board accelerates the following SSL functions:

- Secure establishment of a set of cryptographic parameters and secret keys between a client and a server
- Secure key storage on the board—keys are encrypted if they leave the board

Diagnostic Support

- User-executable self-test using OpenBoot™ PROM
- SunVTS™ diagnostic tests

Cryptographic Algorithm Acceleration

The Sun Crypto Accelerator 4000 board accelerates cryptographic algorithms in both hardware and software. The reason for this complexity is that the cost of accelerating cryptographic algorithms is not uniform across all algorithms. Some cryptographic algorithms were designed specifically to be implemented in hardware, others were designed to be implemented in software. For hardware acceleration, there is the additional cost of moving data from the user application to the hardware acceleration device, and moving the results back to the user application. Note that a few cryptographic algorithms can be performed by highly tuned software as quickly as they can be performed in dedicated hardware.

Supported Cryptographic Algorithms

The Sun Crypto Accelerator 4000 driver (`vca`) examines each cryptographic request and determines the best location for the acceleration (host processor or Sun Crypto Accelerator 4000), to achieve maximum throughput. Load distribution is based on the cryptographic algorithm, the current job load, and the data size.

Sun Crypto Accelerator 4000 board accelerates the following IPsec algorithms.

TABLE 1-1 IPsec Cryptographic Algorithms

Type	Algorithm
Symmetric	DES, 3DES

The Sun Crypto Accelerator 4000 board accelerates the following SSL algorithms.

TABLE 1-2 SSL Cryptographic Algorithms

Type	Algorithm
Symmetric	DES, 3DES, ARCFOUR
Asymmetric	Diffie-Hellman (Apache only) and RSA (up to 2048 bit key), DSA
Hash	MD5, SHA1

SSL Acceleration

TABLE 1-3 shows which SSL accelerated algorithms may be off-loaded to hardware and which software algorithms are provided for Sun ONE and Apache Web Servers.

TABLE 1-3 Supported SSL Algorithms

	Sun ONE Web Servers		Apache Web Servers	
Algorithm	**Hardware**	**Software**	**Hardware**	**Software**
RSA	X	X	X	X
DSA	X	X	X	X
ARCFOUR		X		
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
MD5	X	X		
SHA1	X	X		

Bulk Encryption

The Sun Crypto Accelerator 4000 bulk encryption feature for Sun ONE server software is disabled by default. You must manually enable this feature by creating a file and restarting the Sun ONE server software.

To enable Sun ONE server software to use bulk encryption on the Sun Crypto Accelerator 4000 board, you simply create an empty file in the `/etc/opt/SUNWconn/cryptov2/` directory named `sslreg`, and restart the server software.

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

To disable the bulk encryption feature, you must delete the `sslreg` file and restart the server software.

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

The bulk encryption feature for Apache Web Server software is enabled by default and cannot be disabled.

Hardware Overview

The Sun Crypto Accelerator 4000 hardware is a full size (4.2 inches x 12.283 inches) cryptographic accelerator PCI Gigabit Ethernet adapter that enhances the performance of IPsec and SSL on Sun servers.

IPsec Hardware Acceleration

The Sun Crypto Accelerator 4000 board encrypts and decrypts IPsec packets in hardware, offloading this high-overhead operation from the SPARC™ processor. The cryptographic hardware also supports general asymmetric and symmetric cryptographic operations for use in other applications and contains a hardware source of random numbers.

Note – No IPsec configuration or tuning is required to use the Sun Crypto Accelerator 4000 board for IPsec acceleration. You simply install the Sun Crypto Accelerator 4000 packages and reboot.

Once the Sun Crypto Accelerator 4000 board and packages are installed, any existing IPsec configuration and any future IPsec configuration will use the Sun Crypto Accelerator 4000 board instead of the core Solaris software. The board handles any supported IPsec algorithm listed in TABLE 1-1. IPsec algorithms not supported by the Sun Crypto Accelerator 4000 board will continue to be handled by the core Solaris encryption software. The configuration of IPsec is documented in the *System Administration Guide* of the Solaris System Administrator Collection at `http://docs.sun.com`.

Sun Crypto Accelerator 4000 MMF Adapter

The Sun Crypto Accelerator 4000 MMF adapter is a single-port Gigabit Ethernet fiber optics PCI bus card. It operates in 1000 Mbps Ethernet networks only.

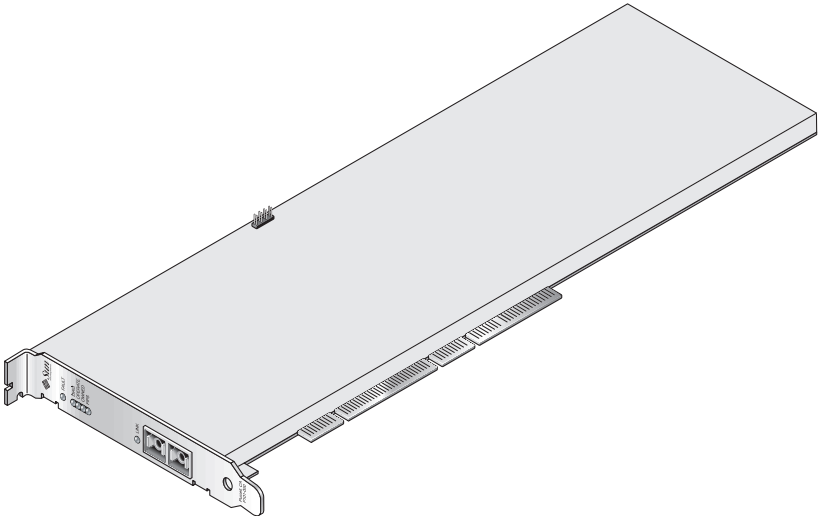

FIGURE 1-1 Sun Crypto Accelerator 4000 MMF Adapter

LED Displays

See TABLE 1-4.

TABLE 1-4 Front Panel Display LEDs for the MMF Adapter

Label	Meaning if Lit	Color
Fault	On when the board is HALTED (fatal error) state or low level hardware initialization failed. Flashing if an error occurred during the boot process.	Red
Diag	On in POST, DIAGNOSTICS, and FAILSAFE (firmware not upgraded) state. Flashing when running DIAGNOSTICS.	Green
Operate	On in POST, DIAGNOSTICS, and DISABLED (driver not attached) state. Flashing in IDLE, OPERATIONAL, and FAILSAFE states.	Green

TABLE 1-4 Front Panel Display LEDs for the MMF Adapter *(Continued)*

Label	Meaning if Lit	Color
Init	On if the security officer has initialized the board with `vcaadm`. See “Initializing the Sun Crypto Accelerator 4000 Board With vcaadm” on page 65. Flashing if the ZEROIZE jumper is present.	Green
FIPS Mode	On when operating in FIPS 140-2 level 3 certified mode. Off when in non-FIPS mode.	Green
Link	Link up.	Green

Sun Crypto Accelerator 4000 UTP Adapter

The Sun Crypto Accelerator 4000 UTP adapter is a single-port Gigabit Ethernet copper-based PCI bus card. It can be configured to operate in 10, 100, or 1000 Mbps Ethernet networks.

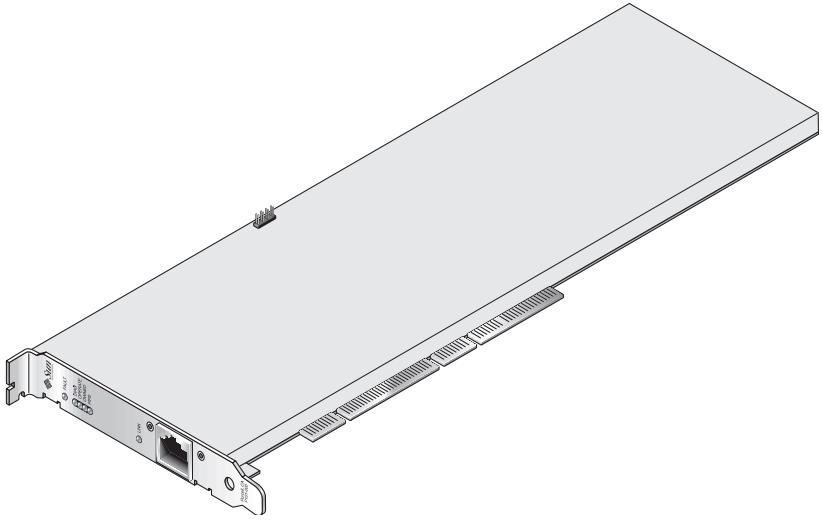

FIGURE 1-2 Sun Crypto Accelerator 4000 UTP Adapter

LED Displays

See TABLE 1-5.

TABLE 1-5 Front Panel Display LEDs for the UTP Adapter

Label	Meaning if Lit	Color
Fault	On when the board is HALTED (fatal error) state or low level hardware initialization failed. Flashing if an error occurred during the boot process.	Red
Diag	On in POST, DIAGNOSTICS, and FAILSAFE (firmware not upgraded) state. Flashing when running DIAGNOSTICS.	Green
Operate	On in POST, DIAGNOSTICS, and DISABLED (driver not attached) state. Flashing in IDLE, OPERATIONAL, and FAILSAFE states.	Green
Init	On if the security officer has initialized the board with `vcaadm`. See “Initializing the Sun Crypto Accelerator 4000 Board With vcaadm” on page 65. Flashing if the ZEROIZE jumper is present.	Green
FIPS Mode	On when operating in FIPS 140-2 level 3 certified mode. Off when in non-FIPS mode.	Green
1000	Indicates Gigabit Ethernet.	Green
Activity (no label)	Link is transmitting or receiving.	Amber
Link (no label)	Link up.	Green

Note – The service pack numbers (SP9 or SP1) are implied whenever Sun ONE Web Server 4.1 or 6.0 is mentioned.

Dynamic Reconfiguration and High Availability

The Sun Crypto Accelerator 4000 hardware and associated software provides the capability to work effectively on Sun platforms supporting Dynamic Reconfiguration (DR) and hot-plugging. During a DR or hot-plug operation, the Sun Crypto Accelerator 4000 software layer automatically detects the addition or removal of a board and adjusts the scheduling algorithms to accommodate the change in hardware resources.

For High Availability (HA) configurations, multiple Sun Crypto Accelerator 4000 boards can be installed within a system or domain to insure that hardware acceleration is continuously available. In the unlikely event of a Sun Crypto Accelerator 4000 hardware failure, the software layer detects the failure and removes the failed board from the list of available hardware cryptographic accelerators. Sun Crypto Accelerator 4000 adjusts the scheduling algorithms to accommodate the reduction in hardware resources. Subsequent cryptographic requests are scheduled to the remaining boards.

Note that the Sun Crypto Accelerator 4000 hardware provides a source for high-quality entropy for the generation of long-term keys. If all the Sun Crypto Accelerator 4000 boards within a domain or system are removed, long-term keys are generated with lower-quality entropy.

Load Sharing

The Sun Crypto Accelerator 4000 software distributes load across as many boards as are installed within the Solaris domain or system. Incoming cryptographic requests are distributed across the boards based on fixed-length work queues. Cryptographic requests are directed to the first board, and subsequent requests stay directed to the first board until it is running at full capacity. Once the first board is running at full capacity, further requests are queued to the first board available that can accept the request of this type. The queueing mechanism is designed to optimize throughput by facilitating request coalescing at the board.

Hardware and Software Requirements

TABLE 1-6 provides a summary of the hardware and software requirements for the Sun Crypto Accelerator 4000 adapter.

TABLE 1-6 Hardware and Software Requirements

Hardware and Software	Requirements
Hardware	Sun Fire™ V120, V210, V240, 280R, V480, V880, 4800, 4810, 6800, 12K, 15K; Netra™ 20 (lw4); Sun Blade™ 100, 150, 1000, 2000
Operating Environment	Solaris 8 2/02 and future compatible releases (Solaris 9 is required for IPsec acceleration.)

Required Patches

Refer to the *Sun Crypto Accelerator 4000 Board Release Notes* for additional required patch information.

The following patches may be required to run the Sun Crypto Accelerator 4000 board on your system. Solaris updates contain patches to previous releases. Use the `showrev -p` command to determine whether the listed patches have already been installed.

You can download the patches from the following web site: `http://sunsolve.sun.com`.

Install the latest version of the patches. The dash number (-01, for example) becomes higher with each new revision of the patch. If the version on the web site is higher than that shown in the following tables, it is simply a later version.

If the patch you need is not available on SunSolve℠, contact your local sales or service representative.

Apache Web Server Patch

If you plan to use the Apache Web Server, you must also install Patch 109234-09. Once the `SUNWkcl2a` package is added, the system will be configured with Apache Web Server mod_ssl 1.3.26.

Solaris 8 Patches

The following tables list required and recommended Solaris 8 patches to use with this product. TABLE 1-7 lists and describes required patches.

TABLE 1-7 Required Solaris 8 Patches for Sun Crypto Accelerator 4000 Software

Patch-ID	Description
110383-01	`libnvpair`
108528-05	`KU-05` (`nvpair` support)
112438-01	`/dev/random`

Solaris 9 Patches

There are currently no required Solaris 9 patches.

CHAPTER 2

Installing the Sun Crypto Accelerator 4000 Board

This chapter describes how to install the Sun Crypto Accelerator 4000 hardware and software. This chapter includes the following sections:

Handling the Board

Each board is packed in a special antistatic bag to protect it during shipping and storage. To avoid damaging the static-sensitive components on the board, reduce any static electricity on your body before touching the board by using one of the following methods:

- Touch the metal frame of the computer.
- Attach an antistatic wrist strap to your wrist and to a grounded metal surface.

Caution – To avoid damaging the sensitive components on the board, wear an antistatic wrist strap when handling the board, hold the board by its edges only, and always place the board on an antistatic surface (such as the plastic bag it came in).

Installing the Board

Installing the Sun Crypto Accelerator 4000 board involves inserting the board into the system and loading the software tools. The hardware installation instructions include only general steps for installing the board. Refer to the documentation that came with your system for specific installation instructions.

▼ To Install the Hardware

1. **As superuser, follow the instructions that came with your system to shut down and power off the computer, disconnect the power cord, and remove the computer cover.**
2. **Locate an unused PCI slot (preferably a 64 bit, 66 MHz slot).**
3. **Attach an antistatic wrist strap to your wrist, and attach the other end to a grounded metal surface.**
4. **Using a Phillips-head screwdriver, remove the screw from the PCI slot cover.**

   Save the screw to hold the bracket in Step 5.
5. **Holding the Sun Crypto Accelerator 4000 board by its edges only, take it out of the plastic bag and insert it into the PCI slot, and then secure the screw on the rear bracket.**
6. **Replace the computer cover, reconnect the power cord, and power on the system.**
7. **Verify that the board is properly installed by issuing the `show-devs` command at the OpenBoot™ PROM (OBP) `ok` prompt:**

```
ok show-devs
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
```

   In the preceding example, the `/pci@8,600000/network@1` identifies the device path to the Sun Crypto Accelerator 4000 board. There will be one such line for each board in the system.

To determine whether the Sun Crypto Accelerator 4000 device properties are listed correctly: from the `ok` prompt, navigate to the device path and type `.properties` to display the list of properties.

```
ok cd /pci@8,600000/network@1
ok .properties
assigned-addresses       82000810 00000000 00102000 00000000 00002000
                          81000814 00000000 00000400 00000000 00000100
                          82000818 00000000 00200000 00000000 00200000
                          82000830 00000000 00400000 00000000 00100000
d-fru-len                00 00 00 00
d-fru-off                00 00 e8 00
d-fru-dev                eeprom
s-fru-len                00 00 08 00
s-fru-off                00 00 e0 00
s-fru-dev                eeprom
compatible               70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                      00000800 00000000 00000000 00000000 00000000
                          02000810 00000000 00000000 00000000 00002000
                          02000814 00000000 00000000 00000000 00000100
                          02000818 00000000 00000000 00000000 00200000
                          02000830 00000000 00000000 00000000 00100000
address-bits             00 00 00 30
max-frame-size           00 00 40 00
network-interface-type   ethernet
device_type              network
name                     network
local-mac-address        08 00 20 aa bb cc
version                  Sun PCI Crypto Accelerator 4000 1000Base-T FCode
2.11.12 02/10/31
phy-type                 mif
board-model              501-6039
model                    SUNW,pci-vca
fcode-rom-offset         00000000
66mhz-capable
fast-back-to-back
devsel-speed             00000001
class-code               00100000
interrupts               00000001
latency-timer            00000040
cache-line-size          00000010
max-latency              00000040
min-grant                00000040
subsystem-id             00003de8
subsystem-vendor-id      0000108e
revision-id              00000002
device-id                0000b555
vendor-id                00008086
```

Installing the Sun Crypto Accelerator 4000 Software

The Sun Crypto Accelerator 4000 software is included on the Sun Crypto Accelerator 4000 CD. You may need to download patches from the SunSolve web site. See “Required Patches” on page 10 for more information.

▼ To Install the Software

1. **Insert the Sun Crypto Accelerator 4000 CD into a CD-ROM drive that is connected to your system.**
   - If your system is running Sun Enterprise Volume Manager™, it should automatically mount the CD-ROM to the `/cdrom/cdrom0` directory.
   - If your system is not running Sun Enterprise Volume Manager, mount the CD-ROM as follows:

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /cdrom
```

You see the following files and directories in the `/cdrom/cdrom0` directory.

TABLE 2-1 Files in the `/cdrom/cdrom0` Directory

File or Directory	Contents	
`Copyright`	U.S. copyright file	
`FR_Copyright`	French copyright file	
`Docs`	*Sun Crypto Accelerator 4000 Board Installation and User's Guide* *Sun Crypto Accelerator 4000 Board Release Notes*	
`Packages`	Contains the Sun Crypto Accelerator 4000 software packages:	
	`SUNWkcl2r`	Cryptography Kernel Components
	`SUNWkcl2u`	Cryptographic Administration Utility and Libraries
	`SUNWkcl2a`	SSL Support for Apache *(optional)*
	`SUNWkcl2m`	Cryptographic Administration Manual Pages (*optional*)
	`SUNWvcar`	VCA Crypto Accelerator (Root)
	`SUNWvcau`	VCA Crypto Accelerator (Usr)
	`SUNWvcaa`	VCA Administration
	`SUNWvcafw`	VCA Firmware
	`SUNWvcamn`	VCA Crypto Accelerator Manual Page (*optional*)
	`SUNWvcav`	SunVTS Test of VCA Crypto Accelerator *(optional)*
	`SUNWkcl2o`	SSL Development Tools and Libraries *(optional)*
	`SUNWkcl2i.u`	IPSec Acceleration with KCLv2 Crypto *(optional)*

The required packages must be installed in a specific order and must be installed before installing any optional packages. Once the required packages are installed, you can install and remove the optional packages in any order.

Install the optional `SUNWkcl2a` package only if you plan to use Apache as your web server.

Install the optional `SUNWkcl2o` package only if you plan to relink to another (unsupported) version of Apache Web Server.

Install the optional `SUNWvcav` package only if you plan to perform the SunVTS tests. You must have SunVTS 4.4 or later up to 5.x installed to install the `SUNWvcav` package.

Note – The optional `SUNWkcl2i.u` package has the `.u` extension only on the Sun Crypto Accelerator 4000 CD. Once this package is installed, the name is changed to `SUNWkcl2i`. The `.u` extension of this package on the CD, defines the package as `sun4u` architecture-specific.

---

2. **Install the required software packages by typing:**

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
```

3. **(Optional) To verify that the software is installed properly, run the** `pkginfo` **command.**

```
# pkginfo SUNWkcl2r SUNWkcl2u SUNWvcar SUNWvcau SUNWvcaa SUNWvcafw
system  SUNWkcl2r   Cryptography Kernel Components
system  SUNWkcl2u   Cryptographic Administration Utility and Libraries
system  SUNWvcar    VCA Crypto Accelerator (Root)
system  SUNWvcau    Crypto Accelerator/Gigabit Ethernet (Usr)
system  SUNWvcaa    VCA Administration
system  SUNWvcafw   VCA Firmware
```

4. **(Optional) To ensure that the driver is attached, you can run the** `prtdiag` **command. Refer to the** `prtdiag`**(1m) online manual pages.**

```
# prtdiag -v
```

5. **(Optional) Run the** `modinfo` **command to see that modules are loaded.**

```
# modinfo | grep Crypto
62   1317f62  20b1f 198   1  vca (VCA Crypto/Ethernet v1.102)
63   13360e9  12510 200   1  kcl2 (Kernel Crypto Library v1.148)
197  136d5d6   19b0 199   1  vcactl (VCA Crypto Control v1.19)
```

Installing the Optional Packages

To install only the optional packages that provide the SSL support for Apache Web Server and the cryptographic administration utility and libraries, type the following:

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m
```

To install all of the optional software packages, type the following:

```
# cd /cdrom/cdrom0/Packages
# pkgadd -d . SUNWkcl2a SUNWkcl2m SUNWvcamn SUNWvcav SUNWkcl2o SUNWkcl2i.u
```

Refer to TABLE 2-1 for a description of the package contents of the optional packages in the previous examples.

Directories and Files

TABLE 2-2 shows the directories created by the default installation of the Sun Crypto Accelerator 4000 software.

TABLE 2-2 Sun Crypto Accelerator 4000 Directories

Directory	Contents
`/etc/opt/SUNWconn/vca/keydata`	Keystore data (encrypted)
`/opt/SUNWconn/cryptov2/bin`	Utilities
`/opt/SUNWconn/cryptov2/lib`	Support libraries
`/opt/SUNWconn/cryptov2/sbin`	Administrative commands

FIGURE 2-1 shows the hierarchy of these directories and files.

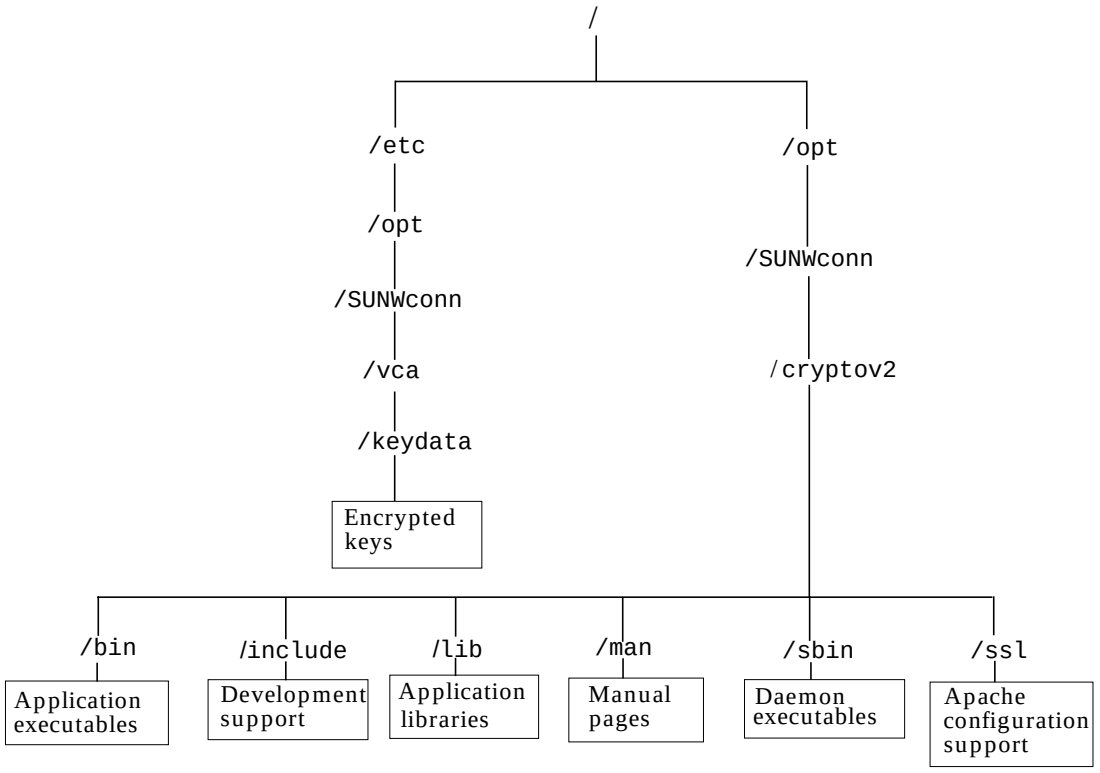

FIGURE 2-1 Sun Crypto Accelerator 4000 Directories and Files

Note – Once you have installed the hardware and software of the board, you need to initialize the board with configuration and keystore information. Refer to “Initializing the Sun Crypto Accelerator 4000 Board With vcaadm” on page 65 for information on how to initialize the board.

Removing the Software

If you have created keystores (refer to “Managing Keystores With vcaadm” on page 69), you must delete the keystore information that the Sun Crypto Accelerator 4000 board is configured with before removing the software. The `zeroize` command removes all key material, but does not delete the keystore files which are stored in the filesystem of the physical host in which the Sun Crypto Accelerator 4000 board is installed. Refer to the “Zeroizing a Sun Crypto Accelerator 4000 Board” on page 80 for details on the `zeroize` command. To delete the keystore files stored in the system, become superuser and remove the keystore files. If you have not yet created any keystores, you can skip this procedure.

Caution – You must not delete a keystore that is currently in use or that is shared by other users and keystores. To free references to keystores, you might have to shut down the web server and/or administration server.

Caution – Before removing the Sun Crypto Accelerator 4000 software you must disable any web servers you have enabled for use with the Sun Crypto Accelerator 4000 board. Failure to do so will leave those web servers nonfunctional.

▼ To Remove the Software

- **As superuser, use the `pkgrm` command to remove only the software packages you installed.**

Caution – Installed packages must be removed in the order shown. Failure to remove them in this order could result in dependency warnings and leave kernel modules loaded.

If you installed all the packages, you would remove them as follows:

```
# pkgrm SUNWkcl2o SUNWvcav SUNWvcar SUNWkcl2a SUNWkcl2u SUNWkcl2r
SUNWvcamn SUNWkcl2m SUNWkcl2i SUNWvcaa SUNWvcafw SUNWvcau
```

Note – After installing or removing the SunVTS test (`SUNWvcav`) for the Sun Crypto Accelerator 4000 board, if SunVTS is already running it might be necessary to reprobe the system to update the available tests. See your SunVTS documentation for more information.

CHAPTER 3

Configuring Driver Parameters

This chapter describes how to configure the vca device driver parameters used by both the Sun Crypto Accelerator 4000 UTP and MMF Ethernet adapters. This chapter contains the following sections:

Sun Crypto Accelerator 4000 Ethernet Device Driver (vca) Parameters

The vca device driver controls the Sun Crypto Accelerator 4000 UTP and MMF Ethernet devices. The vca driver is attached to the UNIX pci name property pci108e,3de8 for the Sun Crypto Accelerator 4000 (108e is the vendor ID and 3de8 is the PCI device ID).

You can manually configure the vca device driver parameters to customize each Sun Crypto Accelerator 4000 device in your system. This section provides an overview of the capabilities of the Sun Crypto Accelerator 4000 Ethernet device used in the board, lists the available vca device driver parameters, and describes how to configure these parameters.

The Sun Crypto Accelerator 4000 Ethernet UTP and MMF PCI adapters are capable of the operating speeds and modes listed in "Setting Autonegotiation or Forced Mode" on page 36. By default, the vca device operates in autonegotiation mode

with the remote end of the link (link partner) to select a common mode of operation for the `speed`, `duplex`, and `link-clock` parameters. The `link-clock` parameter is applicable only if the board is operating at a 1000 Mbps. The `vca` device can also be configured to operate in forced mode for each of these parameters.

Caution – To establish a proper link, both link partners must operate in either autonegotiation or forced mode for each of the `speed`, `duplex`, and `link-clock` (1000 Mbps only) parameters. If both link partners are not operating in the same mode for each of these parameters, network errors will occur. See "Enabling Autonegotiation or Forced Mode for Link Parameters With the OpenBoot PROM" on page 41.

Driver Parameter Values and Definitions

TABLE 3-1 describes the parameters and settings for the `vca` device driver.

TABLE 3-1 `vca` Driver Parameter, Status, and Descriptions

Parameter	Status	Description
`instance`	Read and write	Device instance
`adv-autoneg-cap`	Read and write	Operational mode parameter
`adv-1000fdx-cap`	Read and write	Operational mode parameter (MMF adapter only)
`adv-1000hdx-cap`	Read and write	Operational mode parameter
`adv-100fdx-cap`	Read and write	Operational mode parameter (UTP adapter only)
`adv-100hdx-cap`	Read and write	Operational mode parameter (UTP adapter only)
`adv-10fdx-cap`	Read and write	Operational mode parameter (UTP adapter only)
`adv-10hdx-cap`	Read and write	Operational mode parameter (UTP adapter only)
`adv-asmpause-cap`	Read and write	Flow control parameter
`adv-pause-cap`	Read and write	Flow control parameter
`pause-on-threshold`	Read and write	Flow control parameter
`pause-off-threshold`	Read and write	Flow control parameter
`link-master`	Read and write	1 Gbps speed forced mode parameter
`enable-ipg0`	Read and write	Enable additional delay before transmitting a packet
`ipg0`	Read and write	Additional delay before transmitting a packet
`ipg1`	Read and write	Interpacket Gap parameter

TABLE 3-1 vca Driver Parameter, Status, and Descriptions *(Continued)*

Parameter	Status	Description
ipg2	Read and write	Interpacket Gap parameter
rx-intr-pkts	Read and write	Receive interrupt blanking values
rx-intr-time	Read and write	Receive interrupt blanking values
red-dv4to6k	Read and write	Random early detection and packet drop vectors
red-dv6to8k	Read and write	Random early detection and packet drop vectors
red-dv8to10k	Read and write	Random early detection and packet drop vectors
red-dv10to12k	Read and write	Random early detection and packet drop vectors
tx-dma-weight	Read and write	PCI Interface parameter
rx-dma-weight	Read and write	PCI Interface parameter
infinit-burst	Read and write	PCI Interface parameter
disable-64bit	Read and write	PCI Interface parameter

Advertised Link Parameters

The following parameters determine the transmit and receive speed and duplex link parameters to be advertised by the vca driver to its link partner. TABLE 3-2 describes the operational mode parameters and their default values.

Note – If a parameter's initial setting is 0, it cannot be changed. If you try to change an initial setting of 0, it will revert back to 0. By default, these parameters are set to the capabilities of the vca device.

The Sun Crypto Accelerator 4000 UTP adapter advertised link parameters are different from those of the Sun Crypto Accelerator 4000 MMF adapter as shown in TABLE 3-2.

TABLE 3-2 Operational Mode Parameters

Parameter	Description
The following parameter is for both the Sun Crypto Accelerator 4000 UTP and MMF adapters.	
`adv-autoneg-cap`	Local interface capability advertised by the hardware 0 = Forced mode 1 = Autonegotiation (default)
The following parameter is for the Sun Crypto Accelerator 4000 MMF adapter only.	
`adv-1000fdx-cap`	Local interface capability advertised by the hardware 0 = Not 1000 Mbps full-duplex capable 1 = 1000 Mbps full-duplex capable (default)
The following parameter is for both the Sun Crypto Accelerator 4000 UTP and MMF adapters.	
`adv-1000hdx-cap`	Local interface capability advertised by the hardware 0 = Not 1000 Mbps half-duplex capable 1 = 1000 Mbps half-duplex capable (default)
The following parameters are for the Sun Crypto Accelerator 4000 UTP adapter only.	
`adv-100fdx-cap`	Local interface capability advertised by the hardware 0 = Not 100 Mbps full-duplex capable 1 = 100 Mbps full-duplex capable (default)
`adv-100hdx-cap`	Local interface capability advertised by the hardware 0 = Not 100 Mbps half-duplex capable 1 = 100 Mbps half-duplex capable (default)
`adv-10fdx-cap`	Local interface capability advertised by the hardware 0 = Not 10 Mbps full-duplex capable 1 = 10 Mbps full-duplex capable (default)
`adv-10hdx-cap`	Local interface capability advertised by the hardware 0 = Not 10 Mbps half-duplex capable 1 = 10 Mbps half-duplex capable (default)

If all of the previous parameters are set to 1, autonegotiation will use the highest speed possible. If all of the previous parameters are set to 0, you will receive the following error message:

```
NOTICE: Last setting will leave vca0 with no link capabilities.
WARNING: vca0: Restoring previous setting.
```

Note – In the previous example, `vca0` is the Sun Crypto Accelerator 4000 board device name where the string, `vca`, is used for every Sun Crypto Accelerator 4000 board. This string is always immediately followed by the device instance number of the board. Hence, the device instance number of the `vca0` board is `0`.

Flow Control Parameters

The `vca` device is capable of sourcing (transmitting) and terminating (receiving) pause frames conforming to the IEEE 802.3x Frame Based Link Level Flow Control Protocol. In response to received flow control frames, the `vca` device is capable of reducing its transmit rate. Alternately, the `vca` device is capable of sourcing flow control frames, requesting the link partner to reduce its transmit rate if the link partner supports this feature. By default, the driver advertises both transmit and receive pause capability during autonegotiation.

TABLE 3-3 provides flow control keywords and describes their function.

TABLE 3-3 Read-Write Flow Control Keyword Descriptions

Keyword	Description		
`adv-asmpause-cap`	Both the MMF and UTP adapters support asymmetric pause; hence, the `vca` device can pause only in one direction. 0=Off (default) 1=On		
`adv-pause-cap`	This parameter has two meanings depending on the value of `adv-asmpause-cap`. (Default=0)		
	Parameter Value + `adv-asmpause-cap=`	**Parameter Value =** `adv-pause-cap=`	**Description**
	1	1 or 0	`adv-pause-cap` determines which direction pauses operate on.
	1	1	Pauses are received but are not transmitted.

TABLE 3-3 Read-Write Flow Control Keyword Descriptions

Keyword	Description		
	1	0	Pauses are transmitted but are not received.
	0	1	Pauses are sent and received.
	0	1 or 0	`adv-pause-cap` determines whether the pause capability is on or off.
`pause-on-threshold`	Defines the number of 64 byte blocks in the receive (RX) FIFO which causes the board to generate an XON-PAUSE frame.		
`pause-off-threshold`	Defines the number of 64 byte blocks in the RX FIFO which causes the board to generate an XOFF-PAUSE frame.		

Gigabit Forced Mode Parameter

For Gigabit links, this parameter determines the `link-master`. Generally, switches are enabled as a link master; in which case, this parameter can remain unchanged. If this is not the case, then the `link-master` parameter can be used to enable the `vca` device as a link master.

TABLE 3-4 Gigabit Forced Mode Parameter

Parameter	Description
`link-master`	When set to 1 this parameter enables master operation, assuming the link partner is a slave. When set to 0 this parameter enables slave operation, assuming the link partner is a master. (default)

Interpacket Gap Parameters

The `vca` device supports a programmable mode called `enable-ipg0`.

Before transmitting a packet with `enable-ipg0` enabled (default), the `vca` device adds an additional time delay. This delay, set by the `ipg0` parameter, is in addition to the delay set by the `ipg1` and `ipg2` parameters. The additional `ipg0` delay reduces collisions.

If `enable-ipg0` is disabled, the value of `ipg0` is ignored and no additional delay is set. Only the delays set by `ipg1` and `ipg2` will be used. Disable `enable-ipg0` if other systems keep sending a large number of continuous packets. Systems that

have `enable-ipg0` enabled might not have enough time on the network. You can add the additional delay by setting the `ipg0` parameter from 0 to 255, which is the media byte time delay. TABLE 3-5 defines the `enable-ipg0` and `ipg0` parameters.

TABLE 3-5 Parameters Defining `enable-ipg0` and `ipg0`

Parameter	Values	Description
`enable-ipg0`	0 1	`enable-ipg0` enable `enable-ipg0` disable (Default=1)
`ipg0`	0 to 255	The additional time delay (or gap) before transmitting a packet (after receiving the packet) (Default=8)

The `vca` device supports the programmable interpacket gap parameters (IPG) `ipg1` and `ipg2`. The total IPG is the sum of `ipg1` and `ipg2`. The total IPG is 0.096 microseconds for the link speed of 1000 Mbps.

TABLE 3-6 lists the default values and allowable values for the IPG parameters.

TABLE 3-6 Read-Write Interpacket Gap Parameter Values and Descriptions

Parameter	Values (Byte-time)	Description
`ipg1`	0 to 255	Interpacket gap 1 (Default=8)
`ipg2`	0 to 255	Interpacket gap 2 (Default=4)

By default, the driver sets `ipg1` to 8-byte time and `ipg2` to 4-byte time, which are the standard values. (Byte time is the time it takes to transmit one byte on the link, with a link speed of 1000 Mbps.)

If your network has systems that use longer IPG (the sum of `ipg1` and `ipg2`), and if those machines seem to be slow in accessing the network, increase the values of `ipg1` and `ipg2` to match the longer IPGs of other machines.

Interrupt Parameters

TABLE 3-7 describes the receive interrupt blanking values.

TABLE 3-7 RX Blanking Register for Alias Read

Field Name	Values	Description
`rx-intr-pkts`	0 to 511	Interrupts after this number of packets have arrived since the last packet was serviced. A value of zero indicates no packet blanking. (Default=3)
`rx-intr-time`	0 to 524287	Interrupts after 4.5 microseconds (usecs) have elapsed since the last packet was serviced. A value of zero indicates no time blanking. (Default=3)

Random Early Drop Parameters

These parameters provide the ability to drop packets based on the fullness of the receive FIFO. By default, this feature is disabled. When FIFO occupancy reaches a specific range, packets are dropped according to the preset probability. The probability should increase when the FIFO level increases. Control packets are never dropped and are not counted in the statistics.

TABLE 3-8 RX Random Early Detecting 8-Bit Vectors

Field Name	Values	Description
`red-dv4to6k`	0 to 255	Random early detection and packet drop vectors for when FIFO threshold is greater than 4096 bytes and less than 6,144 bytes. Probability of drop can be programmed on a 12.5 percent granularity. For example, if bit 0 is set, the first packet out of every eight will be dropped in this region. (Default=0)

TABLE 3-8 RX Random Early Detecting 8-Bit Vectors *(Continued)*

Field Name	Values	Description
`red-dv6to8k`	0 to 255	Random early detection and packet drop vectors for when FIFO threshold is greater than 6,144 bytes and less than 8,192 bytes. Probability of drop can be programmed on a 12.5 percent granularity. For example, if bit 8 is set, the first packet out of every eight will be dropped in this region. (Default=0)
`red-dv8to10k`	0 to 255	Random early detection and packet drop vectors for when FIFO threshold is greater than 8,192 bytes and less than 10,240 bytes. Probability of drop can be programmed on a 12.5 percent granularity. For example, if bit 16 is set, the first packet out of every eight will be dropped in this region. (Default=0)
`red-dv10to12k`	0 to 255	Random early detection and packet drop vectors for when FIFO threshold is greater than 10,240 bytes and less than 12,288 bytes. Probability of drop can be programmed on a 12.5 percent granularity. For example, if bit 24 is set, the first packet out of every eight will be dropped in this region. (Default=0)

PCI Bus Interface Parameters

These parameters allow you to modify PCI interface features to gain better PCI interperformance for a given application.

TABLE 3-9 PCI Bus Interface Parameters

Parameter	Description
`tx-dma-weight`	Determines the multiplication factor for granting credit to the transmit (TX) side during a weighted round robin arbitration; the values are 0 to 3 (Default=0). Zero means no extra weighting. The other values are power of 2 extra weighting on that traffic. For example, if `tx-dma-weight` = 0 and `rx-dma-weight` = 3, then as long as RX traffic is continuously arriving, the priority of RX traffic will be 8 times greater than the priority of TX traffic to access the PCI.
`rx-dma-weight`	Determines the multiplication factor for granting credit to the RX side during a weighted round robin arbitration. The values are 0 to 3 (Default=0).
`infinite-burst`	Allows the infinite burst capability to be used when this parameter is enabled and the system supports infinite burst. The adapter will not free the bus until complete packets are transferred across the bus. The values are 0 or 1 (Default=0).
`disable-64bit`	Switches off 64-bit capability of the adapter. Note: for UltraSPARC® III based platforms, this parameter may be set to 1 by default. For UltraSPARC II based platforms, the default is 0. The values are 0 or 1 (Default=0, which enables 64-bit capability).

Setting vca Driver Parameters

You can set the vca device driver parameters in two ways:

- Using the ndd utility
- Using the vca.conf file

If you use the ndd utility, the parameters are valid only until you reboot the system. This method is good for testing parameter settings.

To set parameters so they remain in effect after you reboot the system, create a /kernel/drv/vca.conf file and add parameter values to this file when you need to set a particular parameter for a device in the system. See "To Set Driver Parameters Using a vca.conf File" on page 38 for details.

Setting Parameters Using the ndd Utility

Use the ndd utility to configure parameters that are valid until you reboot the system.

The following sections describe how you can use the vca driver and the ndd utility to modify (with the -set option) or display (without the -set option) the parameters for each vca device.

▼ To Specify Device Instances for the ndd Utility

Before you use the ndd utility to get or set a parameter for a vca device, you must specify the device instance for the utility.

1. **Check the /etc/path_to_inst file to identify the instance number associated with a particular device. Refer to the online manual pages for path_to_inst(4).**

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

In the previous example, the three Sun Crypto Accelerator 4000 Ethernet instances are from the installed adapters. The instance numbers are 0 and 1.

2. **Use the instance number to select the device.**

```
# ndd -set /dev/vcaN
```

Note – In the examples in this user's guide, *N* represents the instance number of the device.

The device remains selected until you change the selection.

Noninteractive and Interactive Modes

You can use the ndd utility in two modes:

- Noninteractive
- Interactive

In noninteractive mode, you invoke the utility to execute a specific command. Once the command is executed, you exit the utility. In interactive mode, you can use the utility to get or set more than one parameter value. Refer to the ndd(1M) online manual page for more information.

Using the ndd *Utility in Noninteractive Mode*

This section describes how to modify and display parameter values.

- **To modify a parameter value, use the** `-set` **option.**

  If you invoke the ndd utility with the `-set` option, the utility passes *value*, which must be specified to the named `/dev/vca` driver instance, and assigns it to the parameter:

```
# ndd -set /dev/vcaN parameter value
```

  When you change any adv parameter, a message similar to the following appears:

```
- link up 1000 Mbps half duplex
```

- **To display the value of a parameter, specify the parameter name and omit the value.**

  When you omit the `-set` option, a query operation is assumed and the utility queries the named driver instance, retrieves the value associated with the specified parameter, and prints it:

```
# ndd /dev/vcaN parameter
```

Using the ndd *Utility in Interactive Mode*

- **To modify a parameter value in interactive mode, specify** `ndd /dev/vca`**, as shown below.**

  The ndd utility then prompts you for the name of the parameter:

```
# ndd /dev/vcaN
name to get/set? (Enter the parameter name or ? to view all
parameters)
```

  After typing the parameter name, the ndd utility prompts you for the parameter value (see TABLE 3-1 through TABLE 3-9).

- **To list all the parameters supported by the** `vca` **driver, type** `ndd /dev/vca`.

  (See TABLE 3-1 through TABLE 3-9 for parameter descriptions.)

```
# ndd /dev/vca
name to get/set ? ?
?                               (read only)
instance                        (read and write)
adv-autoneg-cap                 (read and write)
adv-1000fdx-cap                 (read and write)
adv-1000hdx-cap                 (read and write)
adv-100fdx-cap                  (read and write)
adv-100hdx-cap                  (read and write)
adv-10fdx-cap                   (read and write)
adv-10hdx-cap                   (read and write)
adv-asmpause-cap                (read and write)
adv-pause-cap                   (read and write)
pause-on-threshold              (read and write)
pause-off-threshold             (read and write)
link-master                     (read and write)
enable-ipg0                     (read and write)
ipg0                            (read and write)
ipg1                            (read and write)
ipg2                            (read and write)
rx-intr-pkts                    (read and write)
rx-intr-time                    (read and write)
red-p4k-to-6k                   (read and write)
red-p6k-to-8k                   (read and write)
red-p8k-to-10k                  (read and write)
red-p10k-to-12k                 (read and write)
tx-dma-weight                   (read and write)
rx-dma-weight                   (read and write)
infinite-burst                  (read and write)
disable-64bit                   (read and write)
name to get/set ?
#
```

Setting Autonegotiation or Forced Mode

The following link parameters can be set to operate in either autonegotiation or forced mode:

- `speed`
- `duplex`
- `link-clock`

By default, autonegotiation mode is enabled for these link parameters. When either of these parameters are in autonegotiation mode, the vca device communicates with the link partner to negotiate a compatible value and flow control capability. When a value other than auto is set for either of these parameters, no negotiation occurs and the link parameter is configured in forced mode. In forced mode, the value for the speed parameter must match between link partners. See "Enabling Autonegotiation or Forced Mode for Link Parameters With the OpenBoot PROM" on page 41.

▼ To Disable Autonegotiation Mode

If your network equipment does not support autonegotiation, or if you want to force your network speed, duplex, or link-clock parameters, you can disable the autonegotiation mode on the vca device.

1. **Set the following driver parameters to the values that are described in the documentation delivered with your link partner device (for example, a switch):**
   - adv-1000fdx-cap
   - adv-1000hdx-cap
   - adv-100fdx-cap
   - adv-100hdx-cap
   - adv-10fdx-cap
   - adv-10hdx-cap
   - adv-asmpause-cap
   - adv-pause-cap

   See TABLE 3-2 for the descriptions and possible values of these parameters.

2. **Set the** adv-autoneg-cap **parameter to** 0**.**

```
# ndd -set /dev/vcaN adv-autoneg-cap 0
```

When you change any ndd link parameter, a message similar to the following appears:

```
link up 1000 Mbps half duplex
```

Note – If you disable autonegotiation, you must enable the speed, duplex, and link-clock (1000 Mbps only) parameters to operate in forced mode. For instructions, see "Enabling Autonegotiation or Forced Mode for Link Parameters With the OpenBoot PROM" on page 41.

Setting Parameters Using the vca.conf File

You can also specify the driver parameter properties by adding entries to the vca.conf file in the /kernel/drv directory. The parameter names are the same names listed in “Driver Parameter Values and Definitions” on page 24.

Caution – Do not remove any of the default entries in the /kernel/drv/vca.conf file.

The online manual pages for prtconf(1) and driver.conf(4) include additional details. The next procedure shows an example of setting parameters in a vca.conf file.

Variables defined in the previous section apply to known devices in the system. To set a variable for a Sun Crypto Accelerator 4000 board with the vca.conf file, you must know the following three pieces of information for the device: device name, device parent, and device unit address.

▼ To Set Driver Parameters Using a vca.conf File

1. **Obtain the hardware path names for the** vca **devices in the device tree.**

   a. **Check the** /etc/driver_aliases **file to identify the name associated with a particular device.**

```
# grep vca /etc/driver_aliases
vca "pci108e,3de8"
```

   In the previous example, the device name associated with the Sun Crypto Accelerator 4000 software driver (vca) is ”pci108e,3de8”.

   b. **Locate the device parent name and device unit address in the** /etc/path_to_inst **file.**

   Refer to the online manual pages for path_to_inst(4).

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
"/pci@8,700000/network@1" 1 "vca"
```

In the previous example, there are three columns of output: device path name, instance number, and software driver name.

The device path name in the first line of the previous example is "/pci@8,600000/network@1". Device path names are made up of three parts: device parent name, device node name, and device unit address. See TABLE 3-10.

TABLE 3-10 Device Path Name

Entire Device Path Name	Parent Name Portion	Node Name Portion	Unit Address Portion
"/pci@8,600000/network@1"	/pci@8,600000	network	1
"/pci@8,700000/network@1"	/pci@8,700000	network	1

To identify a PCI device unambiguously in the `vca.conf` file, use the entire device path name (parent name, node name, and the unit address) for the device. Refer to the `pci`(4) online manual page for more information about the PCI device specification.

2. **Set the parameters for the above devices in the `/kernel/drv/vca.conf` file.**

   In the following entry, the `adv-autoneg-cap` parameter is disabled for a particular Sun Crypto Accelerator 4000 Ethernet device.

```
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
```

3. **Save the `vca.conf` file.**
4. **Save and close all files and programs, and exit the windowing system.**
5. **Shut down and reboot the system.**

Setting Parameters for All Sun Crypto Accelerator 4000 `vca` Devices With the `vca.conf` File

If you omit the device path name (parent name, node name, and the unit address), the variable is set for all instances of all Sun Crypto Accelerator 4000 Ethernet devices.

▼ To Set Parameters for All Sun Crypto Accelerator 4000 vca Devices With the vca.conf File

1. **Add a line in the** vca.conf **file to change the value of a parameter for all instances by entering** *parameter=value;***.**

   The following example sets the adv-autoneg-cap parameter to 1 for all instances of all Sun Crypto Accelerator 4000 Ethernet devices:

```
adv-autoneg-cap=1;
```

Example vca.conf File

The following is an example vca.conf file:

```
#
# Copyright 2002 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)vca.conf   1.2     02/06/26 SMI"

#
# Use the new Solaris 9 properties to ensure that the driver is attached
# on boot, to get us to register with KCL2.  This also prevents us from
# being unloaded by the cleanup modunload -i 0.
#
ddi-forceattach=1 ddi-no-autodetach=1;
name="pci108e,3de8" parent="/pci@8,700000" unit-address="1" adv-autoneg-cap=0;
adv-autoneg-cap=1;
```

Enabling Autonegotiation or Forced Mode for Link Parameters With the OpenBoot PROM

The following parameters can be configured to operate in autonegotiation or forced mode at the OpenBoot PROM (OBP) interface:

TABLE 3-11 Local Link Network Device Parameters

Parameter	Description
`speed`	This parameter can be set to `auto`, `1000`, `100`, or `10`; the syntax is as follows: • `speed=auto` (default) • `speed=1000` • `speed=100` • `speed=10`
`duplex`	This parameter can be set to `auto`, `full`, or `half`; the syntax is as follows: • `duplex=auto` (default) • `duplex=full` • `duplex=half`
`link-clock`	This parameter is applicable only if the `speed` parameter is set to `1000` or if you are using a 1000 Mbps MMF Sun Crypto Accelerator 4000 board. The value for this parameter must correspond to the value on the link partner—for example, if the local link has a value of `master`, the link partner must have a value of `slave`. This parameter can be set to `master`, `slave`, or `auto`; the syntax is as follows: • `link-clock=auto` (default) • `link-clock=master` • `link-clock=slave`

To establish a proper link, the `speed`, `duplex`, and `link-clock` (1000 Mbps only) parameters must be configured correctly between the local link and the link partner. Both link partners must operate in either autonegotiation or forced mode for each of the `speed`, `duplex`, and `link-clock` (1000 Mbps only) parameters. A value of `auto` for any of these parameters configures the link to operate in autonegotiation mode for that parameter. The absence of a parameter at the OBP prompt configures that parameter to have a default value of `auto`. A value other than `auto` configures the local link to operate in forced mode for that parameter.

When the local link is operating in autonegotiation mode for the `speed` and `duplex` parameters at 100 Mbps and below and both full and half duplexes, then the link partner uses either the 100 Mbps or 10 Mbps speeds with either duplex.

When the `speed` parameter is operating in forced mode, the value must match the `speed` value of the link-partner. If the `duplex` parameter does not match between the local link and the link partner, the link may come up; however, traffic collisions will occur.

When the local link `speed` parameter is set to autonegotiation and the link partner `speed` parameter is set to forced, the link may come up depending on whether the `speed` value can be negotiated between the local link and the link partner. The interface in autonegotiation mode will always try to establish a link (if there is a speed match) at half duplex by default. Because one of the two interfaces is not in autonegotiation mode, the interface in autonegotiation mode detects only the `speed` parameter; the duplex parameter is not detected. This method is called parallel-detection.

Caution – The establishment of a link with a duplex conflict always leads to traffic collisions.

For a local link parameter to operate in forced mode, the parameter must have a value other than `auto`. For example, to establish a forced mode link at 100 Mbps with half duplex, type the following at the OBP prompt:

```
ok boot net:speed=100,duplex=half
```

Note – In the examples in this section, `net` is an alias for the default, integrated network interface device path. You can configure other network devices by specifying a device path instead of using `net`.

To establish a forced mode link at 1000 Mbps with half duplex that is a clock master, type the following command at the OBP prompt:

```
ok boot net:speed=1000,duplex=half,link-clock=master
```

Note – The `link-clock` parameter must have a value that corresponds to the `link-clock` value of the link partner. For example, if the `link-clock` value on the local link is set to `master`, the `link-clock` value on the link partner must be set to `slave`.

To establish a forced mode for a speed of 10 Mbps and an autonegotiation mode for duplex, type the following at the OBP prompt:

```
ok boot net:speed=10,duplex=auto
```

You could also type the following at the OBP prompt to establish the same local link parameters as the previous example:

```
ok boot net:speed=10
```

Refer to the IEEE 802.3 documentation for further details.

Sun Crypto Accelerator 4000 Cryptographic and Ethernet Driver Operating Statistics

This section describes the statistics presented by the `kstat`(1M) command.

Cryptographic Driver Statistics

TABLE 3-12 describes the cryptographic driver statistics.

TABLE 3-12 Cryptographic Driver Statistics

Parameter	Description	Stable or Unstable
`vs-mode`	The values are `FIPS`, `standard`, or `unitialized`. `FIPS` indicates that the board is in FIPS mode. `standard` indicates that the board is in not in FIPS mode. `unitialized` indicates that the board is not initialized.	Stable
`vs-status`	The values are `ready`, `faulted`, or `failsafe`. `ready` indicates that the board is operating normally. `faulted` indicates that the board not operating. `failsafe` indicates `failsafe` mode which is the original factory state of the board.	Stable

Ethernet Driver Statistics

TABLE 3-13 describes the Ethernet driver statistics.

TABLE 3-13 Ethernet Driver Statistics

Parameter	Description	Stable or Unstable
`ipackets`	Number of inbound packets.	Stable
`ipackets64`	64-bit version of `ipackets`.	Stable
`ierrors`	Total packets received that could not be processed because they contained errors (long).	Stable
`opackets`	Total packets requested to be transmitted on the interface.	Stable
`opackets64`	Total packets requested to be transmitted on the interface (64-bit).	Stable
`oerrors`	Total packets that were not successfully transmitted because of errors (long).	Stable
`rbytes`	Total bytes successfully received on the interface.	Stable
`rbytes64`	Total bytes successfully received on the interface (64-bit).	Stable
`obytes`	Total bytes requested to be transmitted on the interface.	Stable
`obytes64`	Total bytes requested to be transmitted on the interface (64-bit).	Stable
`multircv`	Multicast packets successfully received, including group and functional addresses (long).	Stable
`multixmt`	Multicast packets requested to be transmitted, including group and functional addresses (long).	Stable
`brdcstrcv`	Broadcast packets successfully received (long).	Stable
`brdcstxmt`	Broadcast packets requested to be transmitted (long).	Stable
`norcvbuf`	Times a valid incoming packet was known to have been discarded because no buffer could be allocated for receive (long).	Stable
`noxmtbuf`	Packets discarded on output because transmit buffer was busy, or no buffer could be allocated for transmit (long).	Stable

TABLE 3-14 describes the transmit and receive MAC counters.

TABLE 3-14 TX and RX MAC Counters

Parameter	Description	Stable or Unstable
`tx-collisions`	16-bit loadable counter increments for every frame transmission attempt that resulted in a collision.	Stable
`tx-first-collisions`	16-bit loadable counter increments for every frame transmission that experienced a collision on the first attempt, but was successfully transmitted on the second attempt.	Unstable
`tx-excessive-collisions`	16-bit loadable counter increments for every frame transmission that has exceeded the Attempts Limit.	Unstable
`tx-late-collisions`	16-bit loadable counter increments for every frame transmission that has experienced a collision. It indicates the number of frames that the TxMAC has dropped due to collisions that occurred after it has transmitted at least the Minimum Frame Size number of bytes. Usually this is an indication that there is at least one station on the network that violates the maximum allowed span of the network.	Unstable
`tx-defer-timer`	16-bit loadable timer increments when the TxMAC is deferring to traffic on the network while it is attempting to transmit a frame. The time base for the timer is the media byte clock divided by 256.	Unstable
`tx-peak-attempts`	8-bit register indicates the highest number of consecutive collisions per successfully transmitted frame, that have occurred since this register was last read. The maximum value that this register can attain is 255. A maskable interrupt is generated to the software if the number of consecutive collisions per successfully transmitted frame exceeds 255. This register will be automatically cleared at 0 after it is read.	Unstable

TABLE 3-14 TX and RX MAC Counters *(Continued)*

Parameter	Description	Stable or Unstable
`tx-underrun`	16-bit loadable counter increments after a valid frame has been received from the network.	Unstable
`rx-length-err`	16-bit loadable counter increments after a frame, whose length is greater than the value that was programmed in the Maximum Frame Size Register, has been received from the network.	Unstable
`rx-alignment-err`	16-bit loadable counter increments when an alignment error is detected in a receive frame. An alignment error is reported when a receive frame fails the CRC checking algorithm, AND the frame contains a noninteger number of bytes (that is, the frame size in bits modulo 8 is not equal to zero).	Unstable
`rx-crc-err`	16-bit loadable counter increments when a receive frame fails the CRC checking algorithm, AND the frame contains an integer number of bytes (that is, the frame size in bits modulo 8 is equal to zero).	Unstable
`rx-code-violations`	16-bit loadable counter increments when an Rx_Err indication is generated by the XCVR over the MII, while a frame is being received. This indication is generated by the transceiver when it detects an invalid code in the received data stream. A receive code violation is not counted as an FCS or an Alignment error.	Unstable
`rx-overflows`	Number of Ethernet frames dropped due to lack of resources.	Unstable
`rx-no-buf`	Number of times the hardware cannot receive data because there is no more receive buffer space.	Unstable
`rx-no-comp-wb`	Number of times the hardware cannot post completion entries for received data.	Unstable
`rx-len-mismatch`	Number of received frames where the asserted length does not match the actual frame length.	Unstable

The following Ethernet properties (TABLE 3-15) are derived from the intersection of device capabilities and the link partner capabilities.

TABLE 3-15 describes the current Ethernet link properties.

TABLE 3-15 Current Ethernet Link Properties

Parameter	Description	Stable or Unstable
`ifspeed`	1000, 100, or 10 Mbps	Stable
`link-duplex`	0=half, 1=full	Stable
`link-pause`	Current pause setting for the link, see “Flow Control Parameters” on page 27	Stable
`link-asmpause`	Current pause setting for the link, see “Flow Control Parameters” on page 27	Stable
`link-up`	1=up, 0=down	Stable
`link-status`	1=up, 0=down	Stable
`xcvr-inuse`	Type of transceiver in use: 1=internal MII, 2=external MII, 3=external PCS	Stable

TABLE 3-16 describes the read-only Media Independent Interface (MII) capabilities. These parameters define the capabilities of the hardware. The Gigabit Media Independent Interface (GMII) supports all of the following capabilities.

TABLE 3-16 Read-Only `vca` Device Capabilities

Parameter	Description	Stable or Unstable
`cap-autoneg`	0 = Not capable of autonegotiation 1 = Autonegotiation capable	Stable
`cap-1000fdx`	Local interface full-duplex capability 0 = Not 1000 Mbps full-duplex capable 1 = 1000 Mbps full-duplex capable	Stable
`cap-1000hdx`	Local interface half-duplex capability 0 = Not 1000 Mbps half-duplex capable 1 = 1000 Mbps half-duplex capable	Stable
`cap-100fdx`	Local interface full-duplex capability 0 = Not 100 Mbps full-duplex capable 1 = 100 Mbps full-duplex capable	Stable
`cap-100hdx`	Local interface half-duplex capability 0 = Not 100 Mbps half-duplex capable 1 = 100 Mbps half-duplex capable	Stable

TABLE 3-16 Read-Only vca Device Capabilities *(Continued)*

Parameter	Description	Stable or Unstable
cap-10fdx	Local interface full-duplex capability 0 = Not 10 Mbps full-duplex capable 1 = 10 Mbps full-duplex capable	Stable
cap-10hdx	Local interface half-duplex capability 0 = Not 10 Mbps half-duplex capable 1 = 10 Mbps half-duplex capable	Stable
cap-asm-pause	Local interface flow control capability 0 = Not asymmetric pause capable 1 = Asymmetric pause (from the local device) capable (See “Flow Control Parameters” on page 27)	Stable
cap-pause	Local interface flow control capability 0 = Not Symmetric pause capable 1 = Symmetric pause capable (See “Flow Control Parameters” on page 27)	Stable

Reporting the Link Partner Capabilities

TABLE 3-17 describes the read-only link partner capabilities.

TABLE 3-17 Read-Only Link Partner Capabilities

Parameter	Description	Stable or Unstable
lp-cap-autoneg	0 = No autonegotiation 1 = Autonegotiation	Stable
lp-cap-1000fdx	0 = No 1000 Mbps full-duplex transmission 1 = 1000 Mbps full-duplex	Stable
lp-cap-1000hdx	0 = No 1000 Mbps half-duplex transmission 1 = 1000 Mbps half-duplex	Stable
lp-cap-100fdx	0 = No 100 Mbps full-duplex transmission 1 = 100 Mbps full-duplex	Stable
lp-cap-100hdx	0 = No 100 Mbps half-duplex transmission 1 = 1000 Mbps half-duplex	Stable
lp-cap-10fdx	0 = No 10 Mbps full-duplex transmission 1 = 10 Mbps full-duplex	Stable

TABLE 3-17 Read-Only Link Partner Capabilities *(Continued)*

Parameter	Description	Stable or Unstable
`lp-cap-10hdx`	0 = No 10 Mbps half-duplex transmission 1 = 10 Mbps half-duplex	Stable
`lp-cap-asm-pause`	0 = Not asymmetric pause capable 1 = Asymmetric pause towards link partner capability (See “Flow Control Parameters” on page 27)	Stable
`lp-cap-pause`	0 = Not symmetric pause capable 1 = Symmetric pause capable (See “Flow Control Parameters” on page 27)	Stable

If the link partner is not capable of autonegotiation (when `lp-cap-autoneg` is 0), the remaining information described in TABLE 3-17 is not relevant and the parameter value is 0.

If the link partner is capable of autonegotiation (when `lp-cap-autoneg` is 1), then the speed and mode information is displayed when you use autonegotiation and the link partner capabilities.

TABLE 3-18 describes the driver-specific parameters.

TABLE 3-18 Driver-Specific Parameters

Parameter	Description	Stable or Unstable
`lb-mode`	Copy of the loopback mode the device is in, if any.	Unstable
`promisc`	When enabled, the device is in promiscuous mode. When disabled, the device is not in promiscuous mode.	Unstable
Ethernet Transmit Counters		
`tx-wsrv`	Count of the number of times the transmit ring is full.	Unstable
`tx-msgdup-fail`	Attempt to duplicate packet failure.	Unstable
`tx-allocb-fail`	Attempt to allocate memory failure.	Unstable
`tx-queue0`	Number of packets queued for transmission on the first hardware transmit queue.	Unstable
`tx-queue1`	Number of packets queued for transmission on the second hardware transmit queue.	Unstable
`tx-queue2`	Number of packets queued for transmission on the third hardware transmit queue.	Unstable

TABLE 3-18 Driver-Specific Parameters *(Continued)*

Parameter	Description	Stable or Unstable
`tx-queue3`	Number of packets queued for transmission on the fourth hardware transmit queue.	Unstable
Ethernet Receive Counters		
`rx-hdr-pkts`	Number of packets received that were less than 256 bytes.	Unstable
`rx-mtu-pkts`	Number of packets received that were greater than 256 bytes and less than 1514 bytes.	Unstable
`rx-split-pkts`	Number of packets that were split across two pages.	Unstable
`rx-nocanput`	Number of packets dropped due to failures on delivery to the IP stack.	Unstable
`rx-msgdup-fail`	Number of packets that could not be duplicated.	Unstable
`rx-allocb-fail`	Number of block allocation failures.	Unstable
`rx-new-pages`	Number of pages that got replaced during reception.	Unstable
`rx-new-hdr-pages`	Number of pages that were filled with packets less than 256 bytes that got replaced during reception.	Unstable
`rx-new-mtu-pages`	Number of pages that were filled with packets greater than 256 bytes and less than 1514 that got replaced during reception.	Unstable
`rx-new-nxt-pages`	Number of pages that contained packets that were split across pages that got replaced during reception.	Unstable
`rx-page-alloc-fail`	Number of page allocation failures.	Unstable
`rx-mtu-drops`	Number of times a whole page of packets greater than 256 bytes and less than 1514 was dropped because the driver was unable to map a new one to replace it.	Unstable
`rx-hdr-drops`	Number of times a whole page of packets less than 256 bytes was dropped because the driver was unable to map a new one to replace it.	Unstable
`rx-nxt-drops`	Number of times a page with a split packet was dropped because the driver was unable to map a new one to replace it.	Unstable

TABLE 3-18 Driver-Specific Parameters *(Continued)*

Parameter	Description	Stable or Unstable
`rx-rel-flow`	Number of times the driver was told to release a flow.	Unstable
Ethernet PCI Properties		
`rev-id`	Revision ID of the Sun Crypto Accelerator 4000 Ethernet device useful for recognition of device being used in the field.	Unstable
`pci-err`	Sum of all PCI errors.	Unstable
`pci-rta-err`	Number of target aborts received.	Unstable
`pci-rma-err`	Number of master aborts received.	Unstable
`pci-parity-err`	Number of PCI parity errors detected.	Unstable
`pci-drto-err`	Number of times the delayed transaction retry time-out was reached.	Unstable
`dma-mode`	Used by the Sun Crypto Accelerator 4000 driver (`vca`).	Unstable

▼ To Check Link Partner Settings

- **As superuser, type the** `kstat vca:`*N* **command:**

```
# kstat vca:N
module: vca                             instance: 0
name:   vca0                            class:    misc
```

Note – In the previous example, *N* is the instance number of the `vca` device. This number should reflect the instance number of the board for which you are running the `kstat` command.

Network Configuration

This section describes how to edit the network host files after the adapter has been installed on your system.

Configuring the Network Host Files

After installing the driver software, you must create a `hostname.vca`*N* file for the adapter's Ethernet interface. Note that in the file name `hostname.vca`*N*, *N* corresponds to the instance number of the `vca` interface you plan to use. You must also create both an IP address and a host name for its Ethernet interface in the `/etc/hosts` file.

1. **Locate the correct `vca` interfaces and instance numbers in the `/etc/path_to_inst` file.**

   Refer to the online manual pages for `path_to_inst`(4).

```
# grep vca /etc/path_to_inst
"/pci@8,600000/network@1" 0 "vca"
```

   The instance number in the previous example is `0`.

2. **Use the `ifconfig`(1M) command to set up the adapter's `vca` interface.**

   Use the `ifconfig` command to assign an IP address to the network interface. Type the following at the command line, replacing *ip_address* with the adapter's IP address:

```
# ifconfig vcaN plumb ip_address up
```

Note – In the examples in this section, *N* specifies the instance number of the device.

Refer to the `ifconfig`(1M) online manual page and the Solaris documentation for more information.

- If you want a setup that will remain the same after you reboot, create an `/etc/`*hostname*`.vca`*N* file, where *N* corresponds to the instance number of the `vca` interface you plan to use.

To use the vca interface of the example shown in Step 1, create an /etc/*hostname*.vca*N* file, where *N* corresponds to the instance number of the device which is 0 in this example. If the instance number were 1, the file name would be /etc/*hostname*.vca1.

- Do not create an /etc/*hostname*.vca*N* file for a Sun Crypto Accelerator 4000 interface you plan to leave unused.
- The /etc/*hostname*.vca*N* file must contain the host name for the appropriate vca interface.
- The host name must have an IP address and must be listed in the /etc/hosts file.
- The host name must be different from any other host name of any other interface, for example: /etc/*hostname*.vca0 and /etc/*hostname*.vca1 cannot share the same host name.

The following example shows the /etc/*hostname*.vca*N* file required for a system named zardoz that has a Sun Crypto Accelerator 4000 board (zardoz-11).

```
# cat /etc/hostname.hme0
zardoz
# cat /etc/hostname.vca0
zardoz-11
```

3. **Create an appropriate entry in the** /etc/hosts **file for each active** vca **interface.**

   For example:

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1     localhost
129.144.10.57 zardoz    loghost
129.144.11.83 zardoz-11
```

CHAPTER 4

Administering the Sun Crypto Accelerator 4000 Board With the vcaadm and vcadiag Utilities

This chapter provides an overview of the vcaadm and vcadiag utilities. The following sections are included:

Using vcaadm

The vcaadm program offers a command-line interface to the Sun Crypto Accelerator 4000 board. Only users designated as security officers are allowed to use the vcaadm utility. When you first connect to a Sun Crypto Accelerator 4000 board with vcaadm, you are prompted to create an initial security officer and password.

To access the vcaadm program easily, place the Sun Crypto Accelerator 4000 tools directory in your search path, for example:

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

The vcaadm command-line syntax is:

- vcaadm [-H]
- vcaadm [-y] [-h *host*] [-p *port*] [-d vca*N*] [-f *filename*]
- vcaadm [-y] [-h *host*] [-p *port*] [-d vca*N*] [-s *sec_officer*] *command*

Note – When using the -d attribute, vca*N* is the board's device name where the *N* corresponds to the Sun Crypto Accelerator 4000 device instance number.

TABLE 4-1 shows the options for the vcaadm utility.

TABLE 4-1 vcaadm Options

Option	Meaning
-H	Displays help files for vcaadm commands and exit.
-d vca*N*	Connects to the Sun Crypto Accelerator 4000 board that has *N* as the driver instance number. For example, -d vca1 connects to device vca1 where vca is a string in the board's device name and 1 is the instance number of the device. This value defaults to vca0 and must be in the form of vca*N*, where *N* corresponds to the device instance number.
-f *filename*	Interprets one or more commands from *filename* and exit.
-h *host*	Connects to the Sun Crypto Accelerator 4000 board on *host*. The value for *host* can be a host name or an IP address, and defaults to the loopback address.
-p *port*	Connects to the Sun Crypto Accelerator 4000 board on *port*. The value for *port* defaults to 6870.
-s *sec_officer*	Logs in as a security officer named *sec_officer*.
-y	Forces a yes answer to any command that would normally prompt for a confirmation.

Note – The name *sec_officer* is used throughout this user's guide as an example security officer name.

Modes of Operation

vcaadm can run in one of three modes. These modes differ mainly in how commands are passed into vcaadm. The three modes are Single-Command mode, File mode, and Interactive mode.

Note – To use `vcaadm`, you must authenticate as security officer. How often you need to authenticate as security officer is determined by which operating mode you are using.

Single-Command Mode

In Single-Command mode, you must authenticate as security officer for every command. Once the command is executed, you are logged out of `vcaadm`.

When entering commands in Single-Command mode, you specify the command to be run after all the command-line switches are specified. For example, in Single-Command mode, the following command would show all the users in a given keystore and return the user to the command shell prompt.

```
$ vcaadm show user
Security Officer Name: sec_officer
Security Officer Password:
```

The following command performs a login as the security officer, *sec_officer*, and creates the user *web_admin* in the keystore.

```
$ vcaadm -s sec_officer create user web_admin
Security Officer Password:
Enter new user password:
Confirm password:
User web_admin created successfully.
```

Note – The first password is for the security officer, followed by the password and confirmation for the new user *web_admin*.

All output from Single-Command mode goes to the standard output stream. This output can be redirected using standard UNIX shell-based methods.

File Mode

In File mode, you must authenticate as security officer for every file you run. You are logged out of `vcaadm` after the commands in the command file are executed.

To enter commands in File mode, you specify a file from which `vcaadm` reads one or more commands. The file must be ASCII text, consisting of one command per line. Begin each comment with a pound sign (#) character. If the File mode option is set, `vcaadm` ignores any command-line arguments after the last option. The following example runs the commands in the `deluser.scr` file and answers all prompts in the affirmative:

```
$ vcaadm -f deluser.scr -y
```

Interactive Mode

In Interactive mode, you must authenticate as security officer every time you connect to a board. This is the default operating mode for `vcaadm`. To logout of `vcaadm` in Interactive mode, use the `logout` command. Refer to “Logging In and Out With vcaadm” on page 58.

Interactive mode presents the user with an interface similar to `ftp`(1), where commands can be entered one at a time. The `-y` option is not supported in interactive mode.

Logging In and Out With `vcaadm`

When you use `vcaadm` from the command-line and specify *host*, *port*, and *device* using the `-h`, `-p`, and `-d` attributes respectively, you are immediately prompted to log in as security officer if a successful network connection was made.

The `vcaadm` program establishes an encrypted network connection (channel) between the `vcaadm` application and the Sun Crypto Accelerator 4000 firmware running on a specific board.

During setup of the encrypted channel, boards identify themselves by their hardware Ethernet address and an RSA public key. A trust database (`$HOME/.vcaadm/trustdb`) is created the first time `vcaadm` connects to a board. This file contains all of the boards that are currently trusted by the security officer.

Logging In to a Board With vcaadm

If the security officer connects to a new board, vcaadm will notify the security officer and prompt the following options:

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Trust this board forever (adds the hardware ethernet address
   and RSA public key to the trust database).
```

If the security officer connects to a board that has a remote access key that has been changed, vcaadm will notify the security officer and prompt the following three options:

```
1. Abort the connection
2. Trust the connection one time only (no changes to trust
   database)
3. Replace the old public key bound to this hardware ethernet
   address with the new public key.
```

Logging In to a New Board

Note – The remaining examples in this chapter were created with the Interactive mode of vcaadm.

When connecting to a new board, `vcaadm` must create a new entry in the trust database. The following is an example of logging in to a new board.

```
# vcaadm -h hostname
Warning: MAC ID and Public Key Not Found
-----------------------------------------------------
The MAC ID and public key presented by this board were
not found in your trust database.

MAC ID: 08:00:20:EE:EE:EE
Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Trust the board for all future sessions.

Your Choice -->
```

Logging In to a Board With a Changed Remote Access Key

When connecting to a board that has a changed remote access key, `vcaadm` must change the entry corresponding to the board in the trust database. The following is an example of logging in to a board with a changed remote access key.

```
# vcaadm -h hostname
Warning: Public Key Conflict
-----------------------------------------------------
The public key presented by the board you are connecting
to is different than the public key that is trusted for
this MAC ID.

MAC ID: 08:00:20:EE:EE:EE
New Key Fingerprint: 29FC-7A54-4014-442F-7FD9-5FEA-8411-CFB4
Trusted Key Fingerprint: A508-38D1-FED8-8103-7ACC-0D19-C9C9-11F2
-----------------------------------------------------
Please select an action:

1. Abort this connection
2. Trust the board for this session only.
3. Replace the current trusted key with the new key.

Your Choice -->
```

vcaadm Prompt

The vcaadm prompt in Interactive mode is displayed as follows:

```
vcaadm{vcaN@hostname, sec_officer}> command
```

The following table describes the vcaadm prompt variables:

TABLE 4-2 vcaadm Prompt Variable Definitions

Prompt Variable	Definition
vca*N*	vca is a string that represents the Sun Crypto Accelerator 4000 board. *N* is the device instance number (unit address) that is in the device path name of the board. Refer to "To Set Driver Parameters Using a vca.conf File" on page 38 for details on retrieving this number for a device.
hostname	The name of the host for which the Sun Crypto Accelerator 4000 board is physically connected. *hostname* may be replaced with the physical host's IP address.
sec_officer	The name of the security officer that is currently logged in to the board.

Logging Out of a Board With vcaadm

If you are working in Interactive mode, you may want to disconnect from one board and connect to another board without completely exiting vcaadm. To disconnect from a board and logout, but remain in Interactive mode, use the logout command:

```
vcaadm{vcaN@hostname, sec_officer}> logout
vcaadm>
```

In the previous example, notice the vcaadm> prompt no longer displays the device instance number, hostname, or security officer name. To log in to another device, type the connect command with the following optional parameters.

TABLE 4-3 connect Command Optional Parameters

Parameter	Meaning
dev vca*N*	Connect to the Sun Crypto Accelerator 4000 board with the driver instance number of *N*. For example -d vca1 connects to the device vca1; this defaults to device vca0.
host *hostname*	Connect to the Sun Crypto Accelerator 4000 board on *hostname* (defaults to the loopback address). *hostname* may be replaced with the physical host's IP address.
port *port*	Connect to the Sun Crypto Accelerator 4000 board on port *port* (defaults to 6870).

Example:

```
vcaadm{vcaN@hostname, sec_officer}> logout
vcaadm> connect host hostname dev vca2
Security Officer Login: sec_officer
Security Officer Password:
vcaadm{vcaN@hostname, sec_officer}>
```

vcaadm will not let you issue the connect command if you are already connected to a Sun Crypto Accelerator 4000 board. You must first logout and then issue the connect command.

Each new connection will cause vcaadm and the target Sun Crypto Accelerator 4000 firmware to renegotiate new session keys to protect the administrative data that is sent.

Entering Commands With vcaadm

The vcaadm program has a command language that must be used to interact with the Sun Crypto Accelerator 4000 board. Commands are entered using all or part of a word (enough to uniquely identify that word from any other possibilities). Entering sh instead of show would work, but re is ambiguous because it could be reset or rekey.

The following example shows entering commands using entire words:

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                    Status
-----------------------------------------------------
web_admin                               enabled
Tom                                      enabled
-----------------------------------------------------
```

The same information can be obtained in the previous example using partial words as commands, such as sh us.

An ambiguous command produces an explanatory response:

```
vcaadm{vcaN@hostname, sec_officer}> re
Ambiguous command: re
```

Getting Help for Commands

vcaadm has built-in help functions. To get help, you must enter a question mark (?) character following the command you want more help on. If an entire command is entered and a "?" exists anywhere on the line, you will get the syntax for the command, for example:

```
vcaadm{vcaN@hostname, sec_officer}> create ?
Sub-Command                    Description
-------------------------------------------------
so                             Create a new security officer
user                           Create a new user

vcaadm{vcaN@hostname, sec_officer}> create user ?
Usage: create user [<username>]

vcaadm{vcaN@hostname, sec_officer}> set ?
Sub-Command                    Description
-------------------------------------------------
passreq                        Set password requirements
password                       Change an existing security officer password
timeout                        Set the auto-logout time
```

You can also enter a question mark at the vcaadm prompt to see a list of all of the vcaadm commands and their description, for example:

```
vcaadm{vcaN@hostname, sec_officer}> ?
Sub-Command                    Description
-------------------------------------------------
backup                         Backup master key
connect                        Begin admin session with firmware
create                         Create users and accounts
delete                         Delete users and accounts
diagnostics                    Run diagnostic tests
disable                        Disable a user
enable                         Enable a user
exit                           Exit vcaadm
loadfw                         Load new firmware
logout                         Logout current session
quit                           Exit vcaadm
rekey                          Generate new system keys
reset                          Reset the hardware
set                            Set operating parameters
show                           Show system settings
zeroize                        Delete all keys and reset board
```

When not in vcaadm Interactive mode, the “?” character could be interpreted by the shell in which you are working. In this case, be sure to use the command shell escape character before the question mark.

Quitting the vcaadm Program in Interactive Mode

Two commands allow you to exit from vcaadm: quit and exit. The Ctrl-D key sequence also exits from vcaadm.

Initializing the Sun Crypto Accelerator 4000 Board With vcaadm

The first step in configuring a Sun Crypto Accelerator 4000 board is to initialize it. When you initialize a board it is necessary to create a keystore, refer to “Concepts and Terminology” on page 86. You can either initialize the Sun Crypto Accelerator 4000 board with a new keystore or use a backup file to initialize the board to use an existing keystore.

When you first connect to a Sun Crypto Accelerator 4000 board with vcaadm, you are prompted to initialize the board with a new keystore or initialize the board to use an existing keystore which is stored in a backup file. vcaadm prompts you for all of the required information for either type of board initialization.

▼ To Initialize the Sun Crypto Accelerator 4000 Board With a New Keystore

1. **Enter** `vcaadm` **at a command prompt of the system with the Sun Crypto Accelerator 4000 board installed or enter** `vcaadm -h` *hostname* **if the system is remote, and select 1 to initialize the board**:

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 1
```

2. **Create an initial security officer name and password (Refer to "Naming Requirements" on page 69)**:

```
Initial Security Officer Name: sec_officer
Initial Security Officer Password:
Confirm Password:
```

3. **Create a keystore name (Refer to "Naming Requirements" on page 69)**:

```
Keystore Name: keystore_name
```

4. **Select FIPS 140-2 mode or non-FIPS mode.**

   When in FIPS mode the Sun Crypto Accelerator 4000 board is FIPS 140-2, level 3 compliant. FIPS 140-2 is a federal information processing standard that requires tamper-resistance and a high level of data integrity and security. Refer to the FIPS 140-2 document located at:
   `http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf`

```
Run in FIPS 140-2 mode? (Y/Yes/N/No) [No]: y
```

Note – Before an essential parameter is changed or deleted, or before a command is executed that may have drastic consequences, `vcaadm` prompts you to enter `Y`, `Yes`, `N`, or `No` to confirm. These values are not case sensitive; the default is `No`.

5. **Verify the configuration information**:

```
Board initialization parameters:
-----------------------------------------------------
Initial Security Officer Name: sec_officer
Keystore name: keystore_name
Run in FIPS 140-2 Mode: Yes
-----------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Initializing crypto accelerator board...
```

Initializing the Sun Crypto Accelerator 4000 Board to Use an Existing Keystore

If you are adding multiple boards to a single keystore, you might want to initialize all of the boards to use the same keystore information. In addition, you might want to restore a Sun Crypto Accelerator 4000 board to the original keystore configuration. This section describes how to initialize a board to use an existing keystore which is stored in a backup file.

You must first create a backup file of an existing board configuration before performing this procedure. Creating and restoring a backup file requires a password to encrypt and decrypt the data in the backup file. Refer to “Backing Up the Master Key” on page 74.

▼ To Initialize the Sun Crypto Accelerator 4000 Board to Use an Existing Keystore

1. **Enter** `vcaadm` **at a command prompt of the system with the Sun Crypto Accelerator 4000 board installed or enter** `vcaadm -h` *hostname* **if the system is remote, and select** *2* **to restore the board from a backup:**

```
# vcaadm -h hostname
This board is uninitialized.
You will now initialize the board.  You may
either completely initialize the board and
start with a new keystore or restore the board
using a backup file.

1. Initialize the board with a new keystore
2. Initialize the board to use an existing keystore

Your Choice (0 to exit) --> 2
```

2. **Enter the path and password to the backup file:**

```
Enter the path to the backup file: /tmp/board-backup
Password for restore file:
```

3. **Verify the configuration information:**

```
Board restore parameters:
-----------------------------------------------------
Path to backup file: /tmp/board-backup
Keystore name: keystore_name
-----------------------------------------------------

Is this correct? (Y/Yes/N/No) [No]: y
Restoring data to crypto accelerator board...
```

Managing Keystores With vcaadm

A keystore is a repository for key material. Associated with a keystore are security officers and users. Keystores not only provide storage, but a means for key objects to be owned by user accounts. This enables keys to be hidden from applications that do not authenticate as the owner. Keystores have three components:

- **Key objects –** Long-term keys that are stored for applications such as the Sun ONE Web Server.
- **User accounts –** These accounts provide applications a means to authenticate and access specific keys.
- **Security officer accounts –** These accounts provide access to key management functions through `vcaadm`.

Note – A single Sun Crypto Accelerator 4000 board must have exactly one keystore. Multiple Sun Crypto Accelerator 4000 boards can be configured to collectively work with the same keystore to provide additional performance and fault-tolerance.

Naming Requirements

Security officer names, user names, and keystore names must meet the following requirements:

TABLE 4-4 Security Officer Name, User Name, and Keystore Name Requirements

Name Requirement	Description
Minimum length	At least one character
Maximum length	63 characters for user names and 32 characters for keystore names
Valid characters	Alphanumeric, underscore (_), dash (-), and dot (.)
First character	Must be alphabetic

Password Requirements

Password requirements vary based on the current `set passreq` setting (`low`, `med`, or `high`).

Setting the Password Requirements

Use the `set passreq` command to set the password requirements for the Sun Crypto Accelerator 4000 board. This command sets the password character requirements for any password prompted by `vcaadm`. There are three settings for password requirements:

TABLE 4-5 Password Requirement Settings

Password Setting	Requirements
`low`	Does not require any password restrictions. This is the default while the board is in non-FIPS mode.
`med`	Requires six characters minimum, one character must be nonalphabetic. This is the default setting while the board is in FIPS 140-2 mode and is the minimum password requirements allowed in FIPS 140-2 mode.
`high`	Requires eight characters minimum, three characters must be alphabetic, and one character must be nonalphabetic. This is not a default setting and must be configured manually.

To change the password requirements, enter the `set passreq` command followed by `low`, `med`, or `high`. The following commands set the password requirements for a Sun Crypto Accelerator 4000 board to `high`:

```
vcaadm{vcaN@hostname, sec_officer}> set passreq high

vcaadm{vcaN@hostname, sec_officer}> set passreq
Password security level (low/med/high): high
```

Populating a Keystore With Security Officers

There may be more than one security officer for a keystore. Security officer names are known only within the domain of the Sun Crypto Accelerator 4000 board and do not need to be identical to any user name on the host system.

When creating a security officer, the name is an optional parameter on the command line. If the security officer name is omitted, `vcaadm` will prompt you for the name. (See "Naming Requirements" on page 69.)

```
vcaadm{vcaN@hostname, sec_officer}> create so Alice
Enter new security officer password:
Confirm password:
Security Officer Alice created successfully.

vcaadm{vcaN@hostname, sec_officer}> create so
New security officer name: Bob
Enter new security officer password:
Confirm password:
Security Officer Bob created successfully.
```

Populating a Keystore With Users

These user names are known only within the domain of the Sun Crypto Accelerator 4000 board and do not need to be identical to the UNIX user name that the web server process actually runs as.

When creating a user, the user name is an optional parameter on the command line. If the user name is omitted, `vcaadm` will prompt you for the user name. (See "Naming Requirements" on page 69.)

```
vcaadm{vcaN@hostname, sec_officer}> create user web_admin
Enter new user password:
Confirm password:
User web_admin created successfully.

vcaadm{vcaN@hostname, sec_officer}> create user
New user name: Tom
Enter new user password:
Confirm password:
User Tom created successfully.
```

Users must use this password when authenticating during a web server startup.

Caution – User's must remember their password. Without the password, the users cannot access their keys. There is no way to retrieve a lost password.

Note – The user account is logged out if no commands are entered for more than five minutes. This is a tunable option; see “Setting the Auto-Logout Time” on page 76 for details.

Listing Users and Security Officers

To list users or security officers associated with a keystore, enter the `show user` or `show so` commands.

```
vcaadm{vcaN@hostname, sec_officer}> show user
User                                          Status
-----------------------------------------------------
web_admin                                     Enabled
Tom                                           Enabled
-----------------------------------------------------


vcaadm{vcaN@hostname, sec_officer}> show so
Security Officer
-----------------------------------------------------
sec_officer
Alice
Bob
-----------------------------------------------------
```

Changing Passwords

Only security officer passwords may be changed with `vcaadm`, and the only password that security officers can change are their own. Use the `set password` command to change security officer passwords.

```
vcaadm{vcaN@hostname, sec_officer}> set password
Enter new security officer password:
Confirm password:
Security Officer password has been set.
```

User passwords may be changed through the PKCS#11 interface with the Sun ONE Web Server `modutil` utility. Refer to the Sun ONE Web Server documentation for `modutil` for details.

Enabling or Disabling Users

Note – Security officers cannot be disabled. Once a security officer is created, it is enabled until it is deleted.

By default each user is created in the enabled state. Users may be disabled. Disabled users cannot access their key material with the PKCS#11 interface. Enabling a disabled user will restore access to all of that user's key material.

When enabling or disabling a user, the user name is an optional parameter on the command line. If the user name is omitted, `vcaadm` will prompt you for the user name. To disable a user account, enter the `disable user` command.

```
vcaadm{vcaN@hostname, sec_officer}> disable user Tom
User Tom disabled.
vcaadm{vcaN@hostname, sec_officer}> disable user
User name: web_admin
User web_admin disabled.
```

To enable an account, enter the `enable user` command.

```
vcaadm{vcaN@hostname, sec_officer}> enable user Tom
User Tom enabled.

vcaadm{vcaN@hostname, sec_officer}> enable user
User name: web_admin
User web_admin enabled.
```

Deleting Users

Issue the `delete user` command and specify the user to be deleted. When deleting a user, the user name is an optional parameter on the command line. If the user name is omitted, `vcaadm` will prompt you for the user name.

```
vcaadm{vcaN@hostname, sec_officer}> delete user web_admin
Delete user web_admin? (Y/Yes/N/No) [No]: y
User web_admin deleted successfully.

vcaadm{vcaN@hostname, sec_officer}> delete user
User name: Tom
Delete user Tom? (Y/Yes/N/No) [No]: y
User Tom deleted successfully.
```

Deleting Security Officers

Issue the `delete so` command and specify the security officer to be deleted. When deleting a security officer, the security officer name is an optional parameter on the command line. If the security officer name is omitted, `vcaadm` will prompt you for the security officer name.

```
vcaadm{vcaN@hostname, sec_officer}> delete so Bob
Delete Security Officer Bob? (Y/Yes/N/No) [No]: y
Security Officer Bob deleted.

vcaadm{vcaN@hostname, sec_officer}> delete so
Security Officer name: Alice
Delete Security Officer Alice? (Y/Yes/N/No) [No]: y
Security Officer Alice deleted.
```

Backing Up the Master Key

Keystores are stored on the disk and encrypted in a master key. This master key is stored in the Sun Crypto Accelerator 4000 firmware and can be backed up by a security officer.

To back up the master key, use the `backup` command. The `backup` command requires a path name to a backup file where the backup will be stored. This path name can be placed on the command line or if omitted, `vcaadm` will prompt you for the path name.

A password must be set for the backup data. This password is used to encrypt the master key that is in the backup file.

```
vcaadm{vcaN@hostname, sec_officer}> backup /opt/SUNWconn/vca/backups/bkup.data
Enter a password to protect the data:
Confirm password:
Backup to /opt/SUNWconn/vca/backups/bkup.data successful.
```

Caution – You should choose a password that is very difficult to guess when making backup files because this password protects the master key for your keystore. You must also remember the password you enter. Without the password, you cannot access the master key backup file. There is no way to retrieve the data protected by a lost password.

Locking the Keystore to Prevent Backups

A site might have a strict security policy that doesn't allow the master key for a Sun Crypto Accelerator 4000 board to ever leave the hardware. This can be enforced using the `set lock` command.

Caution – Once this command is issued, all attempts to back up the master key will fail. This lock persists even if the master key is rekeyed. The only way to clear this setting is to zeroize the Sun Crypto Accelerator 4000 board with the `zeroize` command. Refer to "Zeroizing a Sun Crypto Accelerator 4000 Board" on page 80.

```
vcaadm{vcaN@hostname, sec_officer}> set lock
WARNING: Issuing this command will lock the
         master key.  You will be unable to back
         up your master key once this command
         is issued.  Once set, the only way to
         remove this lock is to zeroize the board.
Do you wish to lock the master key? (Y/Yes/N/No) [No]: y
The master key is now locked.
```

Managing Boards With vcaadm

This section describes how to manage Sun Crypto Accelerator 4000 boards with the vcaadm utility.

Setting the Auto-Logout Time

To customize the amount of time before a security officer is automatically logged out of the board, use the set timeout command. To change the auto-logout time, enter the set timeout command followed by a single number that is the number of minutes before a security officer is automatically logged out. A value of 0 will disable the automatic logout feature and the maximum delay is 1,440 minutes (1 day). A newly initialized Sun Crypto Accelerator 4000 board will default to 5 minutes.

The following command changes the auto-logout time for a security officer to 10 minutes:

```
vcaadm{vcaN@hostname, sec_officer}> set timeout 10
```

Displaying Board Status

To get the current status of a Sun Crypto Accelerator 4000 board, issue the `show status` command. This displays the hardware and firmware versions for that board, the MAC address of the network interface, the status (Up versus Down, speed, duplex, and so on.) of the network interface, and the keystore name and ID.

```
vcaadm{vcaN@hostname, sec_officer}> show status
Board Status
----------------------------------------------------------------
Hardware Version: 1.0
Firmware Version: 1.0
Bootstrap Firmware Version: VCA Crypto Accelerator 1.0  March 2003
Current Firmware Version: VCA Crypto Accelerator 1.0  March 2003
MAC Address: 00:03:ba:0e:96:aa
Interface information: Link up, 1000Mbps, Full Duplex
Keystore Name: keystore_name
Keystore ID: 832aece03e654790
Login Session Timeout (in minutes): 10
Password policy security level: HIGH
Number of master key backups: 0
* Device is in FIPS 140-2 Mode
----------------------------------------------------------------
```

Determining if the Board is Operating in FIPS 140-2 Mode

If the Sun Crypto Accelerator 4000 board is operating in FIPS 140-2 mode, the `show status` command will print the following line:

```
* Device is in FIPS 140-2 Mode
```

If the board is not operating in FIPS 140-2 mode, the `show status` command will not print a line specifying FIPS 140-2 mode.

You can also use the `kstat`(1M) utility to determine if the board is operating in FIPS 140-2 mode. The `kstat`(1M) parameter, `vs-mode`, returns a value of `FIPS` if the board is operating in FIPS 140-2 mode. Refer to “Sun Crypto Accelerator 4000 Cryptographic and Ethernet Driver Operating Statistics” on page 43 and the online manual page and for `kstat`(1M).

Loading New Firmware

It is possible to update the firmware for the Sun Crypto Accelerator 4000 board as new features are added. To load firmware, issue the `loadfw` command and provide a path to the firmware file.

A successful update of the firmware requires you to manually reset the board with the `reset` command. When you reset the board, the currently logged in security officer is logged out.

```
vcaadm{vcaN@hostname, sec_officer}> loadfw /opt/SUNWconn/cryptov2/firmware/sca4000fw
Security Officer Login: sec_officer
Security Officer Password:
WARNING: This command will load new firmware onto the
          the target device.  You must issue a reset
          command and log back into the target device in
          order to use the new firmware.

Proceed with firmware update? (Y/Yes/N/No) [No]: y
```

Resetting a Sun Crypto Accelerator 4000 Board

In certain situations, it might be necessary to reset the board. To do this, you must issue the `reset` command. You will be asked if this is what you wish to do. Resetting a Sun Crypto Accelerator 4000 board may temporarily cease the acceleration of cryptography on the system unless there are other active Sun Crypto Accelerator 4000 boards able to take over the load. Also, this command will automatically log you out of `vcaadm`, so you must reconnect to the device by logging back into `vcaadm` if you wish to continue administering it.

```
vcaadm{vcaN@hostname, sec_officer}> reset
WARNING: Issuing this command will reset the
         the board and close this connection.

Proceed with reset? (Y/Yes/N/No) [No]: y
Reset successful.
```

Rekeying a Sun Crypto Accelerator 4000 Board

Over time, it may be necessary because of your security policy to use new keys as the master key or remote access key. The `rekey` command allows you to regenerate either of these keys, or both.

Rekeying the master key also causes the keystore to be reencrypted under the new key, and invalidates older backed up master key files with the new keystore file. It is advisable to make a backup of the master key whenever it is rekeyed. If you have multiple Sun Crypto Accelerator 4000 boards using the same keystore, you will need to backup this new master key and restore it to the other boards.

Rekeying the remote access key logs the security officer out, forcing a new connection that uses the new remote access key.

You may specify one of three key types when issuing the `rekey` command:

TABLE 4-6 Key Types

Key Type	Action
`master`	Rekey the master key.
`remote`	Rekey the remote access key. Logs the security officer out.
`all`	Rekeys both master and remote access keys.

The following is an example of entering a key type of `all` with the `rekey` command:

```
vcaadm{vcaN@hostname, sec_officer}> rekey

Key type (master/remote/all): all
WARNING: Rekeying the master key will render all old board backups
         useless with the new keystore file. If other boards use this
         keystore, they will need to have this new key backed up and
         restored to those boards. Rekeying the remote access key will
         terminate this session and force you to log in again.

Rekey board? (Y/Yes/N/No) [No]: y
Rekey of master key successful.
Rekey of remote access key successful.  Logging out.
```

Zeroizing a Sun Crypto Accelerator 4000 Board

In some situations, it might be necessary to clear a board of all its key material. This can be done using two methods. The first method is with a hardware jumper; this form of zeroizing will return the Sun Crypto Accelerator 4000 board to its original factory state (`failsafe` mode). See "Zeroizing the Sun Crypto Accelerator 4000 Hardware to the Factory State" on page 163. The second method is to use the `zeroize` command.

Note – The `zeroize` command only removes the key material, and leaves any updated firmware intact. This command also logs the security officer out upon successful completion.

To zeroize a board with the `zeroize` command, enter the following:

```
vcaadm{vcaN@hostname, sec_officer}> zeroize
WARNING: Issuing this command will zeroize all keys
         on the board.  Once zeroized, these keys
         cannot be recovered unless you have
         previously backed up your master key.

Proceed with zeroize? (Y/Yes/N/No) [No]: y
All keys zeroized successfully.
```

Using the `vcaadm diagnostics` Command

Diagnostics can be run from the `vcaadm` utility in addition to SunVTS. The `diagnostics` command in `vcaadm` covers three major categories in the Sun Crypto Accelerator 4000 hardware: general hardware, cryptographic subsystem, and network subsystem. Tests for general hardware cover DRAM, flash memory, the PCI

bus, the DMA controller, and other hardware internals. Tests for the cryptographic subsystem cover random number generators and cryptographic accelerators. Tests on the network subsystem cover the `vca` device.

```
vcaadm{vcaN@hostname, sec_officer}> diagnostics
Performing diagnostic tests...Done.
Diagnostic Results
-----------------------------------------------------
General Hardware:               PASS
Cryptographic Subsystem:        PASS
Network Subsystem:              PASS
-----------------------------------------------------
```

Using `vcadiag`

The `vcadiag` program provides a command-line interface to the Sun Crypto Accelerator 4000 board that enables root users to perform administrative tasks without authenticating as security officer. Command-line options determine the actions that `vcadiag` performs.

To access the `vcadiag` program easily, place the Sun Crypto Accelerator 4000 tools directory in your search path, for example:

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

The `vcadiag` command-line syntax is:

- `vcadiag [-D] vcaN`
- `vcadiag [-F] vcaN`
- `vcadiag [-K] vcaN`
- `vcadiag [-Q]`
- `vcadiag [-R] vcaN`
- `vcadiag [-Z] vcaN`

Note – When using the `[-DFKRZ]` attributes, `vcaN` is the board's device name where the *N* corresponds to the Sun Crypto Accelerator 4000 device instance number.

TABLE 4-1 shows the options for the `vcadiag` utility.

TABLE 4-7 `vcadiag` Options

Option	Meaning
`-D vca`*N*	Performs diagnostics on the Sun Crypto Accelerator 4000 board.
`-F vca`*N*	Displays the public key fingerprint used by the Sun Crypto Accelerator 4000 board for securing administration sessions.
`-K vca`*N*	Displays the public key and the public key fingerprint used by the Sun Crypto Accelerator 4000 board for securing administration sessions.
`-Q`	Provides information about Sun Crypto Accelerator 4000 devices and software components. Output is a colon-separated list of the following pieces of information: device, internal function, keystore name, keystore serial number, and keystore reference count. You can use this command to determine the association between devices and keystores.
`-R vca`*N*	Resets the Sun Crypto Accelerator 4000 board.
`-Z vca`*N*	Zeroizes the Sun Crypto Accelerator 4000 board.

The following is an example of the `-D` option:

```
# vcadiag -D vca0
Running vca0 on-board diagnostics.
Diagnostics on vca0 PASSED.
```

The following is an example of the `-F` option:

```
# vcadiag -F vca0
5f26-b516-83b4-d254-a75f-c70d-0544-4de6
```

The following is an example of the `-K` option:

```
# vcadiag -K vca0
Device: vca0
Key Length: 1024 bits
Key Fingerprint: 5f26-b516-83b4-d254-a75f-c70d-0544-4de6
Modulus:
        b7215a99 8bb0dfe9 389363a0 44dac2b0 7c884161
        20ee8c8b d751437d 4e6a5cdb 76fdcb2a ad353c0b
        248edc1d 3c76591d dbca5997 f6ee8022 e8bb5a6d
        465a4f8c 601d46be 573e8681 506e5d8d f240a0db
        11d5c095 2d237061 df27b2de c353900f f531092b
        7d9a755b c5d79782 95a1180b e17303bb aca939ef
        006c73f7 74469031
Public Exponent:
        00010001
```

The following is an example of the `-Q` option:

```
# vcadiag -Q
vca0:cb
vca0:cb:keystore_name:83097c2b3e35ef5b:1
vca0:ca
vca0:ca:keystore_name:83097c2b3e35ef5b:1
kcl2pseudo
vca0:om
vca0:om:keystore_name:83097c2b3e35ef5b:1
libkcl
```

The following is an example of the `-R` option:

```
# vcadiag -R vca0
Resetting device vca0, this may take a minute.
Please be patient.
Device vca0 reset ok.
```

The following is an example of the `-Z` option:

```
# vcadiag -Z vca0
Zeroizing device vca0, this may take a few minutes.
Please be patient.
Device vca0 zeroized.
```

CHAPTER 5

Configuring Sun ONE Server Software for Use With the Sun Crypto Accelerator 4000 Board

This chapter explains how to configure the Sun Crypto Accelerator 4000 board for use with Sun ONE Web Servers. This chapter includes the following sections:

Note – The Sun ONE Web Servers described in this manual were previously named iPlanet™ Web Servers.

Administering Security for Sun ONE Web Servers

This section provides an overview of the security features of the Sun Crypto Accelerator 4000 board as it is administered with Sun ONE Web Servers.

Note – To manage keystores, you must have access to the system administrator account for your system.

Concepts and Terminology

Keystores and users must be created for applications that communicate with the Sun Crypto Accelerator 4000 board through a PKCS#11 interface, such as the Sun ONE Web Server.

Users, within the context of the Sun Crypto Accelerator 4000, are owners of cryptographic keying material. Each key is owned by a single user. Each user may own multiple keys. A user may want to own multiple keys to support different configurations, such as a `production` key and a `development` key (to reflect the organizations the user is supporting).

Note – The term *user* or *user account* refers to Sun Crypto Accelerator 4000 users created in `vcaadm`, not traditional UNIX user accounts. There is no fixed mapping between UNIX user names and Sun Crypto Accelerator 4000 user names.

A keystore is a repository for key material. Associated with a keystore are security officers and users. Keystores not only provide storage, but a means for key objects to be owned by user accounts. This allows keys to be hidden from applications that do not authenticate as the owner. Keystores have three components:

- **Key objects –** Long-term keys that are stored for applications such as the Sun ONE Web Server.
- **User accounts –** These accounts provide applications a means to authenticate and access specific keys
- **Security officer accounts –** These accounts provide access to key management functions through `vcaadm`.

Note – A single Sun Crypto Accelerator 4000 board must have exactly one keystore. Multiple Sun Crypto Accelerator 4000 boards can be configured to collectively work with the same keystore to provide additional performance and fault-tolerance.

A typical installation contains a single keystore with a single user. For example, such a configuration might consist of a single keystore *web_server* and a single user within that keystore, *web_admin*. This would allow the user *web_admin* to own and maintain access control of the server keys within that single keystore.

An administrative tool, `vcaadm`, is used to manage Sun Crypto Accelerator 4000 keystores and users. Refer to “Managing Keystores With vcaadm” on page 69.

Tokens and Token Files

Keystores appear to Sun ONE Web Servers as *tokens*. Token files are a technique for Sun Crypto Accelerator 4000 administrators to selectively present only specific tokens to a given application.

Example

There are three keystores, *engineering*, *finance*, and *legal*. The following tokens are presented to the Sun ONE Web Server:

- `engineering`
- `finance`
- `legal`

Token Files

To override the default case, a token file must exist. Some applications cannot handle multiple tokens. Token files are text files that contain one or more token names, one per line.

Note – Token names and keystore names are the same.

A Sun ONE Web Server presents only the tokens listed in the token file. The methods of specifying token files are as follows (in order of precedence):

1. The file named by the environment variable `SUNW_PKCS11_TOKEN_FILE`

   Some application software suppresses environment variables, in which case this approach might not be feasible.

2. The file `$HOME/.SUNWconn_cryptov2/tokens`

   This file must exist in the home directory of the UNIX user that the Sun ONE Web Server runs as. The Sun ONE Web Server may run as a UNIX user who has no home directory, in which case this approach might not be feasible.

3. The file `/etc/opt/SUNWconn/cryptov2/tokens`

If no token file exists, the Sun Crypto Accelerator 4000 software presents all tokens to Sun ONE Web Servers.

The following is an example of the contents in a token file:

```
================================
# This is an example token file

engineering # Comments are acceptable on the same line

legal

# Because the finance keystore is not listed, the Sun Crypto
# Accelerator will not present it to the Sun ONE Web Server.

...
================================
```

Note – Comments are preceded by a pound sign (#) and empty lines are acceptable.

If none of the files described in this subsection are found, then the default method described in "Tokens and Token Files" on page 87 is used.

Enabling and Disabling Bulk Encryption

The bulk encryption feature for SunONE server software is disabled by default. You may want to enable this feature for securely transferring primarily large files.

To enable Sun ONE server software to use bulk encryption on the Sun Crypto Accelerator 4000 board, you simply create an empty file in the `/etc/opt/SUNWconn/cryptov2/` directory named `sslreg`, and restart the server software.

```
# touch /etc/opt/SUNWconn/cryptov2/sslreg
```

To disable the bulk encryption feature, you must delete the `sslreg` file and restart the server software.

```
# rm /etc/opt/SUNWconn/cryptov2/sslreg
```

Configuring Sun ONE Web Servers

This section describes the following:

Passwords

You are asked for several passwords in the course of enabling a Sun ONE Web Server. TABLE 5-1 provides a description of each. These passwords are referred to throughout this chapter. If there is any confusion about which password to use, refer to TABLE 5-1.

TABLE 5-1 Passwords Required for Sun ONE Web Servers

Type of Password	Description
Sun ONE Web Server Administration Server	Required to start up the Sun ONE Web Server Administration Server. This password was assigned during the Sun ONE Web Server setup.
Web Server Trust Database	Required to start the internal cryptographic module when running in secure mode. This password was assigned when creating a trust database through the Sun ONE Web Server Administration Server. This password is also required when requesting and installing certificates into the internal cryptographic module.
Security Officer	Required when performing `vcaadm` privileged operations.
username:*password*	Required to start the Sun Crypto Accelerator 4000 module when running in secure mode. This password is also required when requesting and installing certificates into the internal cryptographic module (*keystore_name*). This password consists of the *username* and *password* of a keystore user that was created in `vcaadm`. The keystore *username* and *password* are separated by a colon (:).

Populating a Keystore

Before you can enable the board for use with a Sun ONE Web Server, you must first initialize the board and populate the board's keystore with at least one user. The keystore for the board is created during the initialization process. You can also initialize Sun Crypto Accelerator 4000 boards to use an existing keystore. Refer to "Initializing the Sun Crypto Accelerator 4000 Board With vcaadm" on page 65.

Note – Only one keystore per Sun Crypto Accelerator 4000 board can be configured and you must configure one keystore per board. You can configure multiple Sun Crypto Accelerator 4000 boards to collectively work with the same keystore to provide additional performance and fault-tolerance.

▼ To Populate a Keystore

1. **If you have not already done so, place the Sun Crypto Accelerator 4000 tools directory in your search path, for example**:

```
$ PATH=$PATH:/opt/SUNWconn/bin
$ export PATH
```

2. **Access the** `vcaadm` **utility with the** `vcaadm` **command or enter** `vcaadm -h` *hostname* **to connect** `vcaadm` **to a board on a remote host.**

   Refer to "Using vcaadm" on page 55.

```
$ vcaadm -h hostname
```

3. **Populate the board's keystore with users.**

   These user names are known only within the domain of the Sun Crypto Accelerator 4000 board and do not need to be identical to the UNIX user name that the web server process is using. Before attempting to create the user, remember that you must first log in as a `vcaadm` security officer.

4. **Create a user with the** `create user` **command.**

```
vcaadm{vcaN@hostname, sec_officer}> create user username
Initial password:
Confirm password:
User username created successfully.
```

The *username* and *password* created here collectively make the *username:password* (See TABLE 5-1). You must use this password when authenticating during a web server startup. This is the keystore password for a single user.

Caution – Users must remember this *username:password*. Without this password, users cannot access their keys. There is no way to retrieve a lost password.

5. **Exit** `vcaadm`**.**

```
vcaadm{vcaN@hostname, sec_officer}> exit
```

Overview for Enabling Sun ONE Web Servers

To enable Sun ONE Web Servers you must complete the following procedures, which are explained in detail in the next two sections.

- Install the Sun ONE Web Server
- Create a trust database.
- Request a certificate.
- Install the certificate.
- Configure the Sun ONE Web Server.

Caution – These procedures must be followed in the order given. Failure to do so may result in an incorrect configuration.

- If you are using Sun ONE Web Server 4.1, go to “Installing and Configuring Sun ONE Web Server 4.1” on page 92.
- If you are using Sun ONE Web Server 6.0, go to “Installing and Configuring Sun ONE Web Server 6.0” on page 101.

Installing and Configuring Sun ONE Web Server 4.1

This section explains how to install and configure Sun ONE Web Server 4.1. This chapter includes the following sections:

Installing Sun ONE Web Server 4.1

You must perform these procedures in order. Refer to the Sun ONE Web Server documentation for more information about using Sun ONE Web Servers.

▼ To Install Sun ONE Web Server 4.1

1. **Download the Sun ONE Web Server 4.1 software.**

   You can find the web server software at the following URL:
   `http://www.sun.com/`

2. **Install the web server.**

   This section includes instructions for one example, you may decide to configure your Sun ONE Web Server differently. The default path name for the server is: `/usr/netscape/server4`

   Accept the default path during the Sun ONE Web Server installation. This document refers to the default paths. If you decide to install the web server software in a different location, be sure to note where you installed it.

3. **Run the `setup` program.**

4. **Answer the prompts in the installation script.**

   Except for the following prompts, you can accept the default for ease of use.

   a. **Agree to accept the license terms by typing `yes`.**

   b. **Enter a fully qualified *hostname.domain*.**

   c. **Enter the Sun ONE Web Server 4.1 Administration Server password twice.**

   d. **Press Return when prompted.**

▼ To Create a Trust Database

1. **Start the Sun ONE Web Server 4.1 Administration Server.**

   Instead of running `startconsole` as `setup` requests, start a Sun ONE Web Server 4.1 Administration Server, use the following command:

   ```
   # /usr/netscape/server4/https-admserv/start
   SunONE-WebServer-Enterprise/4.1SP9 BB1-08/23/2001 05:50
   startup: listening to http://hostname.domain, port 8888 as root
   ```

   The response provides the URL for connecting to your servers.

2. **Start the Administration graphical user interface (GUI) by opening up a web browser and typing:**

   ```
   http://hostname.domain:admin_port
   ```

   In the authentication dialog box enter the Sun ONE Web Server 4.1 Administration Server user name and password you selected while running `setup`.

   Note – If you used the default settings during the Sun ONE Web Server setup, type `admin` for the User ID or the Sun ONE Web Server 4.1 Adminstration Server user name.

   ---

3. **Select OK.**

   The Sun ONE Web Server 4.1 Administration Server server window is displayed.

4. **Create the trust database for the web server instance.**

   a. **Select the Servers tab in the Sun ONE Web Server 4.1 Administration Server window.**

   b. **Select a server and select the Manage button.**

   c. **Select the Security tab near the top of the page and select the Create Database link.**

   d. **Enter a password (web server trust database; see** TABLE 5-1**) in the two dialog boxes and select OK.**

      Choose a password of at least eight characters. You will use this password to start the internal cryptographic modules when the Sun ONE Web Server runs in secure mode.

      You might want to enable security on more than one web server instance. If so, repeat Step 1 through Step 4 for each web server instance.

Note – If you want to run Secure Socket Layer (SSL) on the Sun ONE Web Server 4.1 Administration Server server as well, the process of setting up a trust database is similar. Refer to the *iPlanet Web Server, Enterprise Edition Administrator's Guide* at `http://docs.sun.com` for more information.

5. **Execute the following script to enable the Sun Crypto Accelerator 4000 board:**

```
# /opt/SUNWconn/bin/iplsslcfg
```

This script prompts you to choose a web server. It installs the Sun Crypto Accelerator 4000 cryptographic modules for the Sun ONE Web Server. The script then updates the configuration files to enable the Sun Crypto Accelerator 4000 board.

6. **Type `1` to configure your Sun ONE Web Server to use SSL and press Return.**

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

7. **Enter the path of the web server root directory when prompted and press Return.**

```
Please enter the full path of the web server
root directory [/usr/netscape/server4]: /usr/netscape/server4
```

8. **Type** `y` **and press Return when prompted, if you want to proceed.**

```
This script will update your Sun ONE Web Server installation
in /usr/netscape/server4 to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/netscape/server4/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/netscape/server4 has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **Type** `0` **to quit.**

▼ To Generate a Server Certificate

1. **Restart the Sun ONE Web Server 4.1 Administration Server by typing the following commands:**

```
# /usr/netscape/server4/https-admserv/stop
# /usr/netscape/server4/https-admserv/start
```

The response provides the URL for connecting to your servers.

2. **Start the Administration GUI by opening up a web browser and typing:**

```
http://hostname.domain:admin_port
```

In the authentication dialog box, enter the Sun ONE Web Server 4.1 Administration Server user name and password you selected while running `setup`.

Note – If you used the default settings during Sun ONE Web Server setup, type `admin` for the User ID or the Sun ONE Web Server 4.1 Administration Server user name.

---

3. **Select OK.**

The Sun ONE Web Server 4.1 Administration Server window is displayed.

4. **To request the server certificate, select the Security tab near the top of the Sun ONE Web Server 4.1 Administration Server window (**FIGURE 5-1**).**

   The Create Trust Database page is displayed.

5. **Select the Request a Certificate link on the left pane** (FIGURE 5-1)**.**

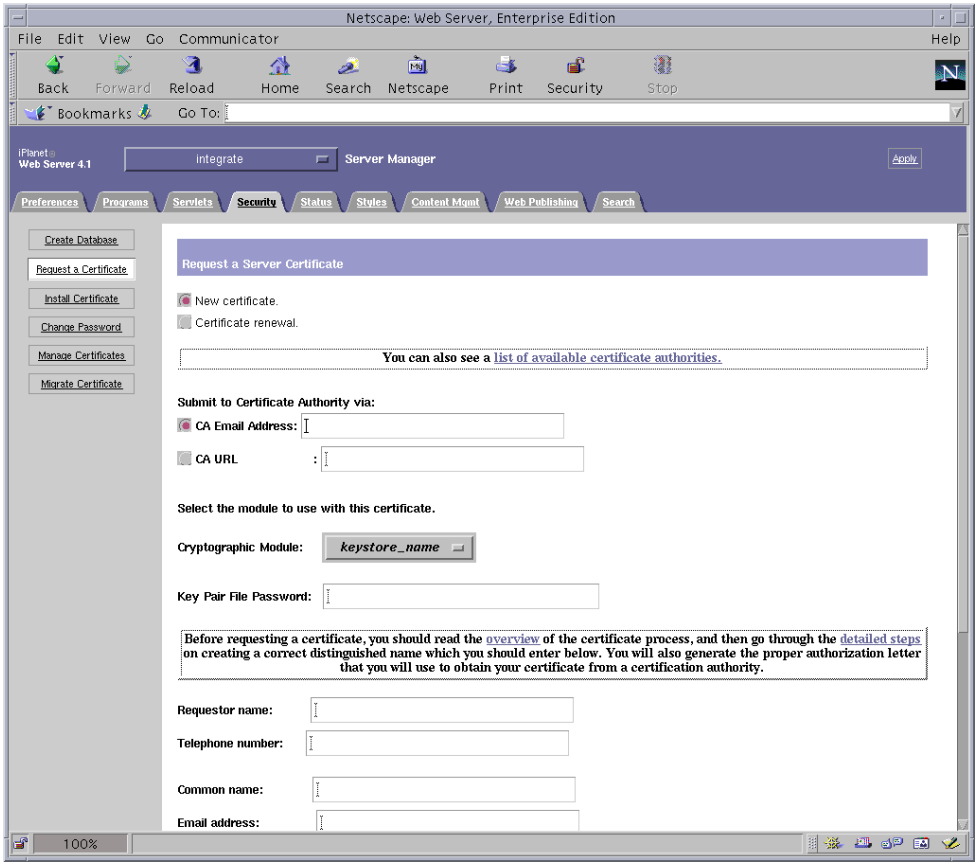

FIGURE 5-1 Request a Server Certificate Page of the Sun ONE Web Server 4.1 Administration Server

6. **Fill out the form to generate a certificate request, using the following information:**

   a. **Select a New Certificate.**

      If you can directly post your certificate request to a web-capable certificate authority or registration authority, select the CA URL link. Otherwise, select CA Email Address and enter an email address where you would like the certificate request to be sent.

b. Select the Cryptographic Module you want to use.

Each keystore has its own entry in this pull-down menu. Be sure that you select the correct keystore. Do not select SUNW acceleration only.

c. In the Key Pair File Password dialog box, provide the password for the user that will own the key.

This password is the *username:password* (TABLE 5-1).

d. Provide the appropriate information for the following requestor information fields:

TABLE 5-2 Requestor Information Fields

Field	Description
Requestor Name	Contact information for the requestor
Telephone Number	Contact information for the requestor
Common Name	Web site Domain that is typed in a visitor's browser *hostname.domain*
Email Address	Contact information for requestor
Organization	A value for the organization to be asserted on the certificate
Organizational Unit	(Optional) A value for the organizational unit that will be asserted on the certificate
Locality	(Optional) City, county, principality, or country, which is also asserted on the certificate if provided
State	(Optional) The full name of the state
Country	The two-letter ISO code for the country (for example, the United States is US)

e. Select the OK button to submit the information.

7. Use a certificate authority to generate the certificate.

- If you choose to post your certificate request to a CA URL, the certificate request is automatically posted there.
- If you choose the CA Email Address, copy the certificate request that was emailed to you with the headers and hand it off to your certificate authority.

8. Once the certificate is generated, copy it, along with the headers, to the clipboard.

Note – The certificate is different from the certificate request and is usually presented to you in text form. Keep this data on the clipboard for Step 5 of the following section.

▼ To Install the Server Certificate

1. **Select the Install Certificate link on the left side of the Sun ONE Web Server 4.1 Administration Server window.**

   Once your request has been approved by a certificate authority and a certificate has been issued, you must install the certificate in the Sun ONE Web Server.

2. **Select the Security tab.**

3. **On the left pane, choose the Install Certificate link.**

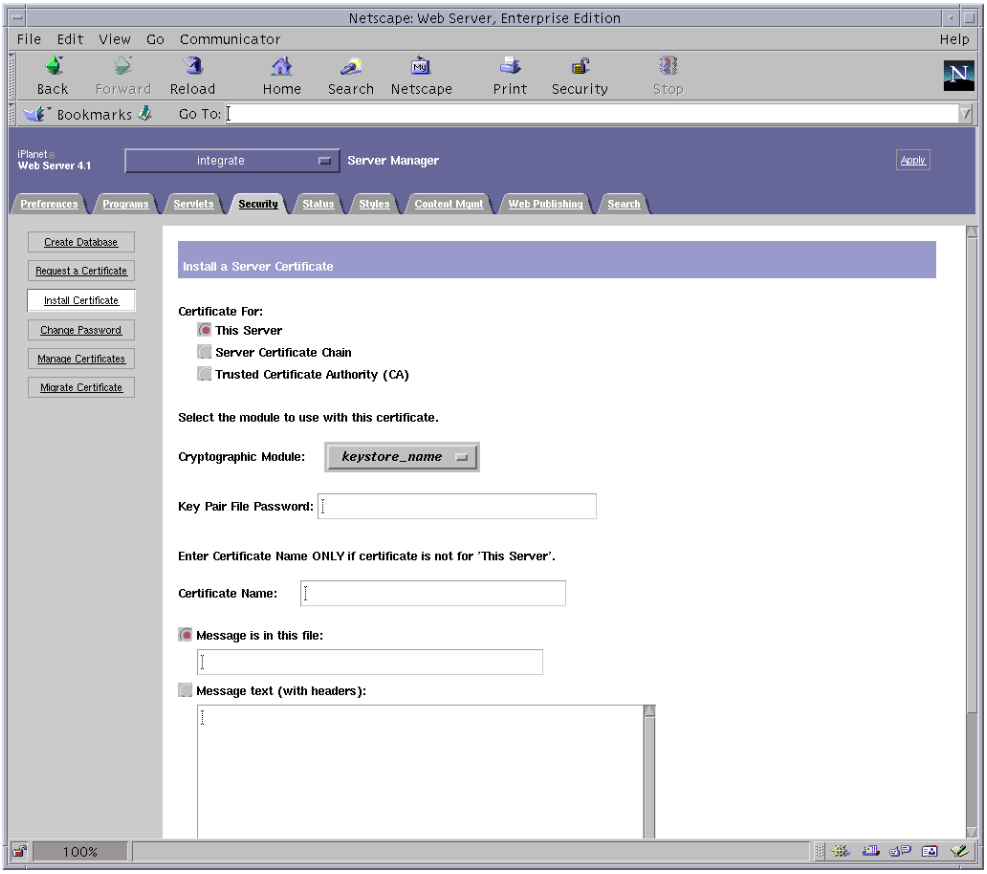

FIGURE 5-2 The Install a Server Certificate Page of the Sun ONE Web Server 4.1 Administration Server

4. **Fill out the form to install your certificate:**

TABLE 5-3 Fields for the Certificate to Install

Fields	Description
Certificate For	This server
Cryptographic Module	Each keystore has its own entry in this pull-down menu. Be sure to select the correct keystore name. To use the Sun Crypto Accelerator 4000, you must select a module with the same name you assigned the keystore.
Key Pair File Password	This password is the *username:password* (TABLE 5-1).
Certificate Name	In most cases, you can leave this blank. If you provide a name, it will alter the name the web server uses to access the certificate and key when running with SSL support. The default for this field is `Server-Cert`.

5. **Paste the certificate you copied from the certificate authority (in Step 8 of the "To Generate a Server Certificate" on page 95) into the Message box.**

   You are shown some basic information about the certificate.

6. **Select the OK button at the bottom of the page.**

7. **If everything looks correct, select the Add Server Certificate button.**

   On-screen messages tell you to restart the server. This is not necessary because the web server instance has been shut down the entire time.

   You are also notified that in order for the web server to use SSL, the web server must be configured to do so. Use the following procedure to configure the web server.

Configuring Sun ONE Web Server 4.1 for SSL

Now that your web server and the server certificate are installed, you must configure the web server for SSL.

▼ To Configure the Sun ONE Web Server 4.1

1. **From the main Sun ONE Web Server 4.1 Administration Server page, select the web server instance you want to work with and select Manage.**

2. **If the Preferences tab is not selected at the top of the page, select the Preferences tab.**

3. **Select the Encryption On/Off link on the left side of the page.**

4. **Set encryption to On.**

   The Port field in the dialog box should update to the default SSL port number 443. Alter the port number if necessary.

5. **Select the OK button.**

6. **Apply these changes by selecting the Save button.**

   The web server is now configured to run in secure mode.

7. **Edit the** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **file (***hostname* **is the name of the web server) by adding the following line:**

   ```
   CERTDefaultNickname keystore_name:Server-Cert
   ```

   By default, the certificate you generated is named `Server-Cert`. If your certificate has a different name, be sure to use the name you chose instead of `Server-Cert`.

8. **Select the server you want to administer and select the Apply button in the far upper right corner of the page.**

   This selection applies the changes through the Sun ONE Web Server 4.1 Administration Server.

9. **Select the Load Configuration Files button to apply the changes you just made to the** `magnus.conf` **file.**

   You are redirected to a page that enables you to start your web server instance.

   If you select the Apply Changes button when the server is off, an authentication dialog box prompts you for the *username:password*. This window is not resizable, and you might have a problem submitting the change.

   There are two workarounds for this problem:

   - Select the Load Configuration Files instead.
   - Start up the web server first, and select the Apply Changes button.

10. **In the Sun ONE Web Server 4.1 Administration Server window, select the On/Off link on the left side of the window.**

11. **Enter the passwords for the servers and select the OK button.**

    You are prompted for one or more passwords. At the Module Internal prompt, provide the password for the web server trust database.

    At the Module *keystore_name* prompt, enter the *username:password* for that keystore.

    Enter the *username:password* for other keystores as prompted.

12. **Verify the new SSL-enabled web server at the following URL:**

    `https://`*hostname.domain*`:`*server_port*`/`

Note – The default *server_port* is 443.

Installing and Configuring Sun ONE Web Server 6.0

This section explains how to enable the Sun Crypto Accelerator 4000 board for use with Sun ONE 6.0 Web Servers. This section includes the following:

Installing Sun ONE Web Server 6.0

You must perform these procedures in order. Refer to the Sun ONE Web Server documentation for more information about using Sun ONE Web Servers.

▼ To Install Sun ONE Web Server 6.0

1. **Download the Sun ONE Web Server 6.0 software.**

   You can find the web server software at the following URL:

   `http://www.sun.com/`

2. **Install the web server.**

   This section includes instructions for one example, you may decide to configure your Sun ONE Web Server differently. The default path name for the server is: `/usr/iplanet/servers`

   Accept the default path during the Sun ONE Web Server installation. This book refers to the default paths. If you decide to install the software in a different location, be sure to note where you installed it.

3. **Run the** `setup` **program.**

4. **Answer the prompts in the installation script.**

   Except for the following prompts, you can accept the defaults for ease of use:

   a. **Agree to accept the license terms by typing** `yes`**.**

   b. **Enter a fully qualified** *hostname.domain***.**

c. Enter the Sun ONE Web Server 6.0 Administration Server password twice.

d. Press Return when prompted.

▼ To Create a Trust Database

1. **Start the Sun ONE Web Server 6.0 Administration Server.**

   To start a Sun ONE Web Server 6.0 Administration Server, use the following command (instead of running `startconsole` as `setup` requests):

   ```
   # /usr/iplanet/servers/https-admserv/start
   SunONE-WebServer-Enterprise/6.0SP1 B08/20/2001 00:58
   warning: daemon is running as super-user
   [LS ls1] http://hostname.domain/port 8888 ready to accept requests
   startup: server started successfully
   ```

   The response provides the URL for connecting to your servers.

2. **Start the Administration GUI by opening up a web browser and typing**:

   ```
   http://hostname.domain:admin_port
   ```

   In the authentication dialog box, enter the Sun ONE Web Server 6.0 Administration Server user name and password you selected while running `setup`.

   Note – If you used the default settings during Sun ONE Web Server setup, enter `admin` for the User ID or the Sun ONE Web Server 6.0 Administration Server user name.

   ---

3. **Select OK.**

   The Sun ONE Web Server 6.0 Administration Server window is displayed.

4. **Create the trust database for the web server instance.**

   You might want to enable security on more than one web server instance. If so, repeat Step 1 through Step 4 for each web server instance.

   Note – If you want to run SSL on the Sun ONE Web Server 6.0 Administration Server as well, the process of setting up a trust database is similar. Refer to the *iPlanet Web Server, Enterprise Edition Administrator's Guide* at `http://docs.sun.com` for more information.

   ---

a. **Select the Servers tab in the Sun ONE Web Server 6.0 Administration Server window.**

b. **Select a server and select the Manage button.**

c. **Select the Security tab near the top of the page and select the Create Database link.**

d. **Enter a password (web server trust database [**TABLE 5-1**]) in the two dialog boxes and select OK.**

   Choose a password of at least eight characters. This will be the password used to start the internal cryptographic modules when the Sun ONE Web Server runs in secure mode.

5. **Execute the following script to enable the Sun Crypto Accelerator 4000 board:**

```
# /opt/SUNWconn/crypto/bin/iplsslcfg
```

This script prompts you to choose a web server. It installs the Sun Crypto Accelerator 4000 cryptographic modules for the Sun ONE Web Server. The script then updates the configuration files to enable the Sun Crypto Accelerator 4000 board.

6. **Type `1` to configure your Sun ONE Web Server to use SSL and press Return.**

```
Sun Crypto Accelerator Sun ONE Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Sun ONE Products.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Sun ONE Web Server for SSL
2. Configure Sun ONE Application Server for SSL
3. Export Sun ONE Web Server keys to PKCS#12 format
4. Import keys from PKCS#12 format for Sun ONE Web Server

Your selection (0 to quit): 1
```

7. **Enter the path of the web server root directory when prompted and press Return.**

```
Please enter the full path of the web server
root directory [/usr/iplanet/servers]: /usr/iplanet/servers
```

8. **Type** `y` **and press Return when prompted, if you want to proceed.**

```
This script will update your Sun ONE Web Server installation
in /usr/iplanet/servers to use the Sun Crypto Accelerator
You will need to restart your admin server after this has
completed.
Ok to proceed? [Y/N]: y

Using database directory /usr/iplanet/servers/alias...
Module "Sun Crypto Accelerator 4000" added to database.
/usr/iplanet/servers has been configured to use
the Sun Crypto Accelerator.


<Press ENTER to continue>
```

9. **Type** `0` **to quit.**

▼ To Generate a Server Certificate

1. **Restart the Sun ONE Web Server 6.0 Administration Server by typing the following commands:**

```
# /usr/iplanet/servers/https-admserv/stop
# /usr/iplanet/servers/https-admserv/start
```

The response provides the URL for connecting to your servers.

2. **Start the Administration GUI by opening up a web browser and typing:**

```
http://hostname.domain:admin_port
```

In the authentication dialog box enter the Sun ONE Web Server 6.0 Administration Server user name and password you selected while running `setup`.

Note – If you used the default settings during Sun ONE Web Server setup, enter `admin` for the user ID or the Sun ONE Web Server 6.0 Administration Server user name.

---

3. **Select OK.**

The Sun ONE Web Server 6.0 Administration Server window is displayed.

4. **To request the server certificate, select the Security tab near the top of Sun ONE Web Server 6.0 Administration Server window.**

   The Create Trust Database window is displayed.

5. **Select the Request a Certificate link on the left pane of the Sun ONE Web Server 6.0 Administration Server window.**

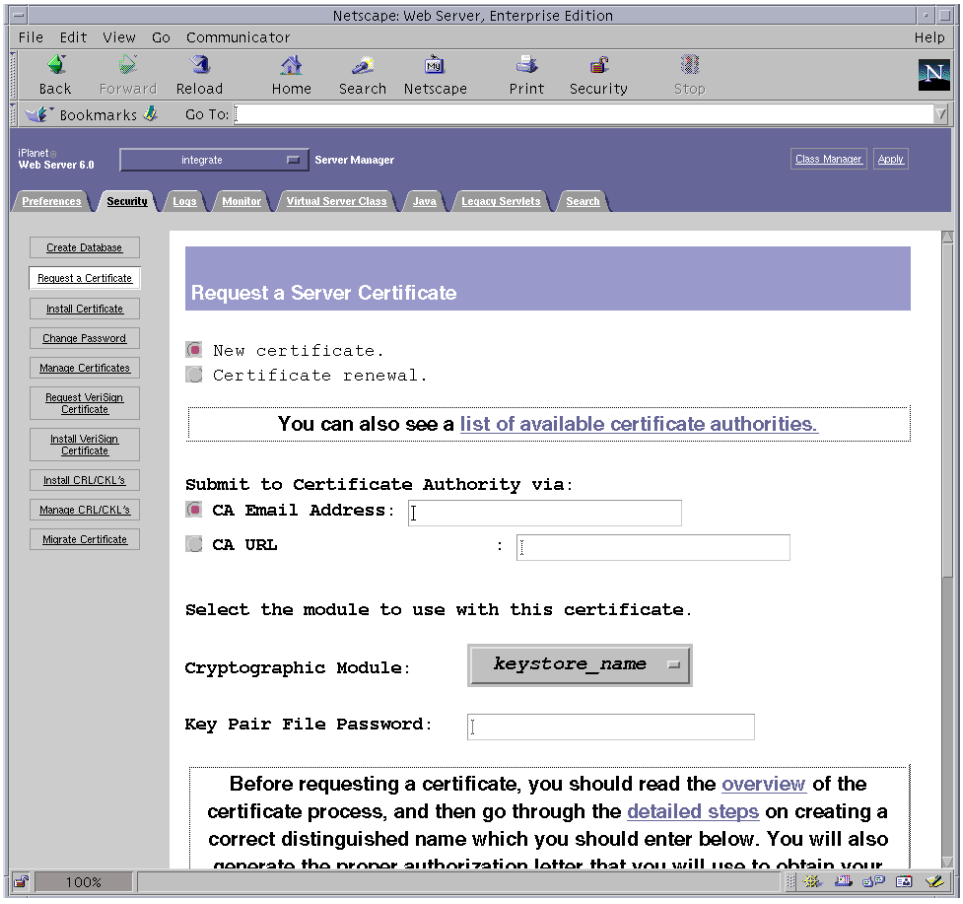

FIGURE 5-3 Request a Server Certificate Page of the Sun ONE Web Server 6.0 Administration Server

6. **Fill out the form to generate a certificate request, using the following information:**

   a. **Select a New Certificate.**

      If you can directly post your certificate request to a web-capable certificate authority or registration authority, select the CA URL link. Otherwise, select CA Email Address and enter an email address where you would like the certificate request to be sent.

b. Select the Cryptographic Module you want to use.

Each keystore has its own entry in this pull-down menu. Be sure that you select the correct keystore. Do not select SUNW acceleration only.

c. In the Key Pair File Password dialog box, provide the password for the user that will own the key.

This password is the *username:password* (TABLE 5-1).

d. Provide the appropriate information for the following requestor information fields:

TABLE 5-4 Requestor Information Fields

Field	Description
Requestor Name	Contact information for the requestor
Telephone Number	Contact information for the requestor
Common Name	Website Domain that is typed in a visitor's browser *hostname.domain*
Email Address	Contact information for requestor
Organization	A value for the organization to be asserted on the certificate
Organizational Unit	(Optional) A value for the organizational unit that will be asserted on the certificate
Locality	(Optional) City, county, principality, or country, which is also asserted on the certificate if provided
State	(Optional) The full name of the state
Country	The two-letter ISO code for the country (for example, the United States is US)

e. Select the OK button to submit the information.

7. Use a certificate authority to generate the certificate.

- If you choose to post your certificate request to a CA URL, the certificate request is automatically posted there.
- If you choose the CA Email Address, copy the certificate request that was emailed to you with the headers and hand it off to your certificate authority.

8. Once the certificate is generated, copy it, along with the headers, to the clipboard.

Note – The certificate is different from the certificate request and is usually presented to you in text form. Keep this data on the clipboard for Step 5 of the "To Install the Server Certificate" on page 107.

▼ To Install the Server Certificate

1. **Select the Install Certificate link on the left side of the Sun ONE Web Server 6.0 Administration Server window.**

   Once your request has been approved by a certificate authority and a certificate has been issued, you must install the certificate in the Sun ONE Web Server.

2. **Select the Security tab.**

3. **On the left pane, choose the Install Certificate link.**

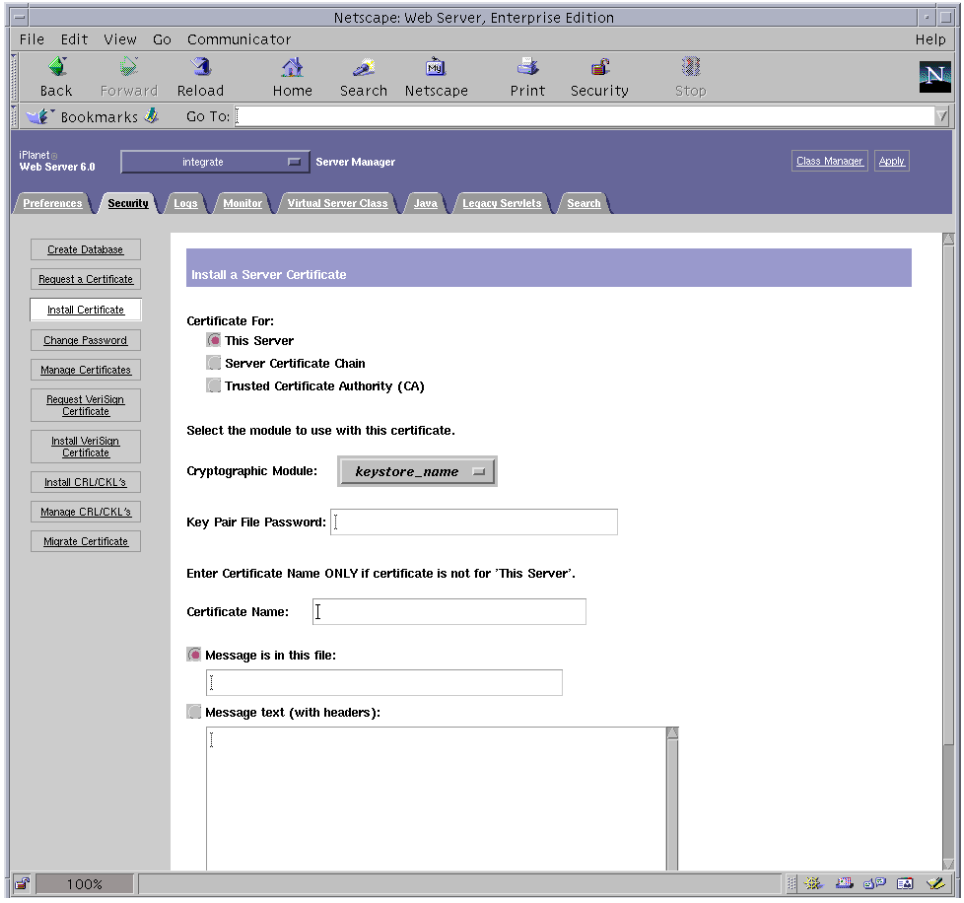

FIGURE 5-4 Install a Server Certificate Page of the Sun ONE Web Server 6.0 Administration Server

4. **Fill out the form to install your certificate:**

TABLE 5-5 Fields for the Certificate to Install

Fields	Description
Certificate For	This server
Cryptographic Module	Each keystore has its own entry in this pull-down menu. Be sure that you select the correct keystore name. To use the Sun Crypto Accelerator 4000, you must select a module in the form of *keystore_name*.
Key Pair File Password	This password is the *username:password* (TABLE 5-1).
Certificate Name	In most cases, you can leave this blank. If you provide a name, it will alter the name the web server uses to access the certificate and key when running with SSL support. The default for this field is `Server-Cert`.

5. **Paste the certificate you copied from the certificate authority (in Step 8 of the "To Generate a Server Certificate" on page 104) into the Message text box.**

   You are shown some basic information about the certificate.

6. **Select the OK button at the bottom of the page.**

7. **If everything looks correct, select the Add Server Certificate button.**

   On-screen messages tell you to restart the server. This is not necessary because the web server instance has been shut down the entire time.

   You are also notified that in order for the web server to use SSL, the web server must be configured to do so. Use the following procedure to configure the web server.

Configuring Sun ONE Web Server 6.0 for SSL

Now that your web server and the Server Certificate are installed, you must configure the web server for SSL.

▼ To Configure the Sun ONE Web Server 6.0

1. **Select the Preferences tab near the top of the page.**

2. **Select the Edit Listen Sockets link on the left pane.**

   The main pane lists all the listen sockets set for the web server instance.

   a. **Alter the following fields:**

- **Port**: Set to the port on which you will be running your SSL-enabled web server (usually this is port 443).
- **Security**: Set to On.

b. Select the OK button to apply these changes.

In the security field of the Edit Listen Sockets page, there should now be an Attributes link.

3. **Select the Attributes link.**
4. **Enter the** *username:password* **to authenticate to the keystore on the system.**
5. **If you want to change the default set of ciphers, select the cipher suites under the Ciphers heading.**

   A dialog box is displayed for changing cipher settings. You can select either Cipher Default settings, SSL2, or SSL3/TLS (Transmission Layer Security). If you select the Cipher Default, you are not shown the default settings. The other two choices require you to select the algorithms you want to enable in a pop-up dialog box. Refer to your Sun ONE documentation on cipher selection.

6. **Select the certificate for the keystore followed by**: `Server-Cert` **(or the name you chose if it is different).**

   Only keys that the appropriate keystore user owns appear in the Certificate Name field. This keystore user is the user that is authenticated with the *username:password*.

7. **When you have chosen a certificate and confirmed all the security settings, select the OK button.**
8. **Select the Apply link in the far upper right corner to apply these changes before you start your server.**
9. **Select the Load Configuration Files link to apply the changes.**

   You are redirected to a page that allows you to start your web server instance.

   If you select the Apply Changes button when the server is off, an authentication dialog box prompts you for the *username:password*. This window is not resizable, and you might have a problem submitting the change.

   There are two workarounds for this problem:

   - Select the Load Configuration Files instead.
   - Start up the web server first, and select the Apply Changes button.

10. **In the Sun ONE Web Server 6.0 Administration Server window, select the On/Off link on the left side of the window.**
11. **Enter the passwords for the servers and select the OK button.**

    You are prompted for one or more passwords. At the Module Internal prompt, provide the password for the web server trust database.

At the Module *keystore_name* prompt, enter the *username:password*.

Enter the *username:password* for other keystores as prompted.

12. **Verify the new SSL-enabled web server at the following URL**:
`https://`*hostname.domain:server_port*`/`

Note – The default *server_port* is 443.

CHAPTER 6

Configuring Apache Web Servers for Use With the Sun Crypto Accelerator 4000 Board

This chapter explains how to configure the Sun Crypto Accelerator 4000 board for use with Apache Web Servers. This chapter includes the following sections:

Caution – Do not configure Apache Web Server for use with the Sun Crypto Accelerator 1000 board and the Sun Crypto Accelerator 4000 at the same time. If both boards are configured to use the Apache Web Server at the same time, Apache will not work correctly.

If you plan to use the Apache Web Server, you must also install Patch 109234-09. Once the `SUNWkcl2a` package is added, the system will be configured with Apache Web Server mod_ssl 1.3.26.

Note – The bulk encryption feature for Apache Web Server software is enabled by default and cannot be disabled.

Enabling the Board for Apache Web Servers

This section provides an overview of how to enable the Sun Crypto Accelerator 4000 board for use with Apache Web Servers.

Enabling Apache Web Servers

Apache Web Server 1.3.26 or later is required for use with the Sun Crypto Accelerator 4000 board. The following instructions are for the 1.3.26 release of Apache Web Server. Refer to the Apache Web Server documentation for more information about using Apache Web Servers.

▼ To Enable the Apache Web Server

1. **Create an** `httpd` **configuration file.**

   For Solaris systems, the `httpd.conf-example` file is usually in `/etc/apache`. You can use this file as a template and copy it as follows:

   ```
   # cp /etc/apache/httpd.conf-example /etc/apache/httpd.conf
   ```

2. **Replace** `ServerName` **with your server name in the** `httpd.conf` **file.**

3. **Start** `apsslcfg`**.**

   ```
   # /opt/SUNWconn/cryptov2/bin/apsslcfg
   ```

4. **Select `1` to configure your Apache Web Server to use SSL:**

```
Sun Crypto Accelerator Apache Installation
------------------------------------------------------------
This script will install the Sun Crypto Accelerator
cryptographic modules for Apache.

Please select what you wish to do:
------------------------------------------------------------
1. Configure Apache for SSL
2. Work with Apache keys

Your selection (0 to quit): 1
```

5. **Provide the directory where the Apache binaries exist.**

   On Solaris systems, this is usually `/usr/apache`.

```
Please enter the directory where the Apache
binaries and libraries exist [/usr/apache]: /usr/apache
```

6. **Provide the location of the configuration files for Apache.**

   On Solaris systems, this is usually `/etc/apache`.

```
Please enter the directory where the Apache configuration files exist
[/etc/apache]: /etc/apache
```

7. **Create an RSA keypair for your system.**

   If you choose not to create a keypair, you must go back later and use `apsslcfg` to generate keys.

```
Do you wish to create a new RSA keypair and certificate request? [Y/N]:
```

   If you answer No to this question, skip to "To Create a Certificate" on page 115.

8. **Provide the directory for storing the keys.**

   If this directory does not exist, it is created.

```
Where would you like the keys stored? [/etc/apache/keys]: /etc/apache/keys
```

9. **Choose a base name for the key material.**

   This name is appended with different suffixes to distinguish key files, certificate request files and later on, certificate files from one another.

```
Please choose a base name for the key and request file: base_name
```

10. **Provide a key length between 512 and 2048 bits.**

    For most web server applications, 1024 bits is sufficiently strong, but you can choose stronger keys if preferred.

```
What size would you like the RSA key to be [1024]? 1024
Using configuration from /opt/SUNWconn/cryptov2/ssl/openssl.cnf
Generating a 1024 bit RSA private key
........++++++
.....................................................++++++
writing new private key to /etc/apache/keys/base_name
```

11. **Create your PEM pass phrase.**

    This pass phrase protects the key material. Be sure to select a strong pass phrase, but one that you can remember. If you forget the pass phrase, you will be unable to access your keys.

```
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
```

Caution – You must remember the pass phrase you enter. Without the pass phrase, you cannot access your keys. There is no way to retrieve a lost pass phrase.

Creating a Certificate

The following procedure describes how to create the certificate required to enable Apache Web Servers to use the Sun Crypto Accelerator 4000 board.

▼ To Create a Certificate

1. **Create a certificate request using the keys you created in "To Enable the Apache Web Server" on page 112.**

   You must first enter the password to access your keys. Then provide the appropriate information for the following fields:

   - Country Name: The two-letter ISO code for the country, which is asserted on the certificate and is a required field (for example, the United States is US)
   - State or Province Name: (Optional) The full name of the state in this field (or type a dot character (.) and press Return).
   - Locality: (Optional) City, county, principality, or country, which is also asserted on the certificate if provided
   - Organization Name: A value for the organization to be asserted on the certificate
   - Organizational Unit Name: (Optional) A value for the organizational unit to be asserted on the certificate
   - SSL Server Name: Website domain that is typed in a visitor's browser
   - Email Address: Contact information for requestor

   The following is an example of how the certificate fields are entered:

```
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated into
your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:US
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) []: Fictional Company, Inc.
Organizational Unit Name (eg, section) []: Online Sales Division
SSL Server Name (eg, www.company.com) []:www.fictional-company.com
Email Address []:admin@fictional-company.com
```

2. **Modify the** `/etc/apache/httpd.conf` **file as directed.**

   You are shown information concerning your key and certificate files. You are also instructed on how to modify the `/etc/apache/httpd.conf` file for use with the Sun Crypto Accelerator 4000 software.

```
The keyfile is stored in /etc/apache/keys/base_name-key.pem.
The certificate request is in /etc/apache/keys/base_name-certreq.pem.

You will need to edit /etc/apache/httpd.conf for the following items:

You must specify the ports that Apache will listen to for
SSL connections, as well as for non-SSL connections.  One
way to accomplish this is to add the following lines in
the Listen section:

Listen 80
Listen 443

In the LoadModule section, add the following:

LoadModule ssl_module /usr/apache/libexec/mod_ssl.so.version-number

In the AddModule section, add the following:

AddModule mod_ssl.c
```

Note – The correct *version-number* will be displayed for your configuration.

3. **If you chose not to set up a** `VirtualHost`**, you must place the** `SSLEngine`**,** `SSLCertificateFile`**, and** `SSLCertificateKeyFile` **directives in the** `httpd.conf` **file, just above the** `SSLPassPhraseDialog` **directive.**

```
You may need a virtual host directive similar to
what is shown below:

<VirtualHost _default_:443>
        SSLEngine on
        SSLCertificateFile /etc/apache/keys/base_name-cert.pem
        SSLCertificateKeyFile /etc/apache/keys/base_name-key.pem
</VirtualHost>

You must add the following line after all of your VirtualHost
definitions:

SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass

Other SSL-related directives and their explanations
can be found in the Sun Crypto Accelerator documentation.

Other Apache-related directives may need to be configured
in order to start your Apache Web Server.  Please refer
to your Apache documentation.

<Press ENTER to continue>
```

If you answered no to the question in Step 7 of "To Enable the Apache Web Server" on page 112, you will also be given additional information on how to generate key material later:

```
Since you did not create keys, you will need to
make sure that you have a key file and a certificate
file in place before enabling SSL for Apache.

You can create a new key file and certificate request
by selecting the "Generate a keypair and request a
certificate for Apache" option after choosing
"Work with Sun ONE and Apache keys" from the
apsslcfg main menu.
```

4. **Select** `0` **to quit when you finish with** `apsslcfg`**.**

5. **Copy your certificate request with the headers from** `/etc/apache/keys/`*base_name*`-certreq.pem` **(where** *base_name* **was set in Step 9 of "To Enable the Apache Web Server" on page 112) and hand it off to your certificate authority.**

6. **Once the certificate is generated, create the certificate file** `/etc/apache/keys/`*base_name*`-cert.pem` **and paste your certificate into it.**

7. **Start the Apache Web Server.**

   This assumes your Apache binary directory is `/usr/apache/bin`. If this is not your binary directory, type in the correct directory.

```
# /usr/apache/bin/apachectl start
```

8. **Enter your PEM pass phrase when prompted for it.**

9. **Verify the new SSL-enabled web server with a browser by going to the following URL:**

   `https://`*server_name*:*server_port*`/`

   Note that the default *server_port* is 443.

CHAPTER 7

Diagnostics and Troubleshooting

This chapter describes diagnostic tests and troubleshooting for the Sun Crypto Accelerator 4000 software. This chapter includes the following sections:

SunVTS Diagnostic Software

The core SunVTS wrapper provides test control and a user interface to a suite of tests. Some of those tests are delivered in packages `SUNWvts` and `SUNWvtsx` along with the core to make up a bundle that is contained on the Solaris 8/9 Software Supplement CD. Other, unbundled, tests that use the SunVTS core are packaged with the driver software of the device tested.

The Sun Crypto Accelerator 4000 board can be tested by three SunVTS tests. Two of those tests, `nettest` and `netlbtest` are bundled with the core SunVTS software beginning with the release of SunVTS 5.1 Patch Set (PS) 2. These tests operate on the Ethernet circuitry of the board.

The third SunVTS test, `vcatest`, is delivered in the `SUNWvcav` package on the Sun Crypto Accelerator 4000 CD and operates with the core SunVTS wrapper to provide diagnostics of the cryptographic circuitry of the board.

Installing SunVTS `netlbtest` and `nettest` Support for the `vca` Driver

TABLE 7-1 shows the method of updating installed SunVTS software to provide SunVTS `netlbtest` and `nettest` support for the `vca` driver.

TABLE 7-1 SunVTS `netlbtest` and `nettest` Required Software for the `vca` Driver

Base Solaris Software	Base SunVTS Software	Required Replacement Package	Required Overlay Patch
Solaris 8 7/01	SunVTS4.4		111854-04
Solaris 8 10/01	SunVTS4.5		112250-04
Solaris 8 2/02	SunVTS4.6	SunVTS5.1ps2	
Solaris 9 5/02	SunVTS5.0	SunVTS5.1ps2	
Solaris 9 9/02	SunVTS5.1		113614-11
Solaris 8 HW 12/02	SunVTS5.1ps1		113614-11
Solaris 9 12/02	SunVTS5.1ps1		113614-11
Solaris 8 HW 5/03	SunVTS5.1ps2		
Solaris 9 4/03	SunVTS5.1ps2		

SunVTS software is delivered on the Solaris Software Supplement CD that is distributed with each Solaris release. The version of SunVTS software listed in the Base SunVTS Software column of TABLE 7-1 is distributed on the Solaris Software Supplement CD included in the Solaris release identified on the same line.

Entries in TABLE 7-1 that begin with “SunVTS” identify the version of a set of SunVTS packages. Within each SunVTS package set, the `SUNWvts` and `SUNWvtsx` packages must be installed.

The Required Replacement Packages column in TABLE 7-1 lists the SunVTS package sets that must replace the previously installed SunVTS package set. You must remove the previously installed SunVTS packages before adding the SunVTS replacement packages. The previously installed SunVTS packages must be removed with the same method you installed them. For example, if you used the `pkgadd` command to install the packages, use the `pkgrm` command to remove the packages.

If an entry is shown in the Required Overlay Patch column in TABLE 7-1, you must use the `patchadd` command to install that patch over the SunVTS packages shown in the Base SunVTS Software column. Do not remove the previously installed SunVTS packages before adding the required patch.

Using the `patchadd` command to install patch 113614-11 is the equivalent of replacing the previously installed SunVTS packages with the SunVTS5.1ps2 packages.

The replacement packages are available at:
`http://www.sun.com/oem/products/vts/`

The overlay patches are available at:
`http://sunsolve.sun.com/`

Note – The required SunVTS packages and any required patches must be installed before the `SUNWvcav` package is installed. The `SUNWvcav` package contains the SunVTS test `vcatest`.

Using SunVTS Software to Perform `vcatest`, `nettest`, and `netlbtest`

Refer to the SunVTS test reference manual, user's guide, and quick reference card for instructions on how to perform and monitor these diagnostics tests. These documents are available on the Solaris on Sun Hardware Documentation Set at `http://docs.sun.com`. These documents are also provided on the Solaris Software Supplement CD that is distributed with the Solaris release on your system.

Note – SunVTS can be used only if you have installed the required SunVTS packages and any required SunVTS patches.

▼ To Perform `vcatest`

1. **As superuser, start SunVTS.**

```
# /opt/SUNWvts/bin/sunvts
```

Refer to the SunVTS user's guide for detailed instructions on starting SunVTS.

The following instructions assume that you have started SunVTS using the CDE user interface.

2. **On the SunVTS Diagnostic main window, set the System Map to Logical mode.**

Note – Physical mode is supported; however, this procedure assumes you are using Logical mode.

3. **Disable all tests by clearing their check boxes.**
4. **Select the check box for Cryptography, then select the plus box for Cryptography to display all tests in the Cryptography group.**
5. **Clear check boxes in the Cryptography group that are not named** `vcatest`**.**
   - If a `vcatest` is displayed, then go to Step 6.
   - If a `vcatest` is not displayed, probe the system to find it by selecting Reprobe system in the Commands drop-down menu.

   Refer to the SunVTS user's guide for the exact procedure. When the probe completes and a `vcatest` is displayed, continue to Step 6.
6. **Select one of the instances of** `vcatest` **then right-click and drag to display the Test Parameter Options dialog box.**

   These options, which only pertain to the `vcatest`, are described in "Test Parameter Options for vcatest" on page 123.
7. **After you have made all selections, select Apply from the Within Instance drop-down menu to change the selected instance of** `vcatest`**, or select Apply from the Across All Instances drop-down menu to change all checked instances of** `vcatest`**.**

   This action removes the dialog box and returns you to the SunVTS Diagnostic main window.
8. **Select one of the instances of** `vcatest` **then right-click and drag to display the Test Execution Options dialog box.**

   An alternate method of displaying Test Execution Options dialog box is to select the Options drop-down main menu; then select Test Executions. These options are generic SunVTS controls that affect all tests. Refer to the SunVTS user's guide for detailed information.
9. **When you have made all selections, select Apply to remove the dialog box and return to the SunVTS Diagnostic main window.**
10. **Select Start to perform the selected tests.**
11. **Select Stop to stop all tests.**

Test Parameter Options for vcatest

TABLE 7-2 describes the vcatest subtests.

TABLE 7-2 vcatest Subtests

Test Name	Description
CDMF	Tests CDMF bulk encryption.
DES	Tests DES bulk encryption.
3DES	Tests 3DES bulk encryption
RSA	Tests RSA public and private keys
DSA	Tests DSA signature verification
MD5	Tests MD5 Message Digest/Digital Signature.
SHA1	Tests SHA1 Digest Key Creation.
RNG	Test random number generation

vcatest Command-Line Syntax

If you choose to perform vcatest from the command line instead of the CDE interface, then all arguments must be specified in the command-line string.

In 32-bit mode, the path to vcatest is /opt/SUNWvts/bin/. In 64-bit mode, the path to vcatest is /opt/SUNWvts/bin/sparcv9/.

All SunVTS standard options are supported from the command-line interface for vcatest. Test-specific options are specified with the -o argument.

Refer to the SunVTS test reference manual for a definition of the standard command-line arguments. The vcatest is a Functional mode test; therefore, -f must be included. Include -u to display a usage message, or -v for VERBOSE messages. Items enclosed in square brackets denote optional entries.

The following is an example of invoking vcatest in 32-bit mode as a standalone program. The following command performs all subtests on vca0:

```
# /opt/SUNWvts/bin/vcatest -f -o dev=vca0,tl=all
```

The following is an example of invoking `vcatest` in 64-bit mode from the SunVTS infrastructure. The following command tests RSA, DSA, and MD5 on `vca2`:

```
# /opt/SUNWvts/bin/sparcv9/vcatest -f -o dev=vca2,tl=RSA+DSA+MD5
```

When performing `vcatest` from the command line, omission of an option produces the default behavior for that option, as stated in TABLE 7-3.

TABLE 7-3 `vcatest` Command-Line Syntax

Option	Description
`dev=vca`*N*	Specifies the instance of the device to test such as `vca0` or `vca2`. Defaults to `vca0` if not included. Note that *N* specifies the placement of the instance number of the device being tested.
`tl=`*testlist*	Specifies the list of subtests to be performed. The subtests for `tl` are separated by the + (plus) character. The supported subtests are CDMF, DES, 3DES, DSA, RSA, MD5, SHA1, and RNG, so `tl=CDMF+DES+3DES+DSA+RSA+MD5+SHA1+RNG` enables all subtests. You can also insert `tl=all` which performs all tests. Defaults to `all` if no subtests are specified.

▼ To Perform `netlbtest`

1. **As superuser, start SunVTS.**

```
# /opt/SUNWvts/bin/sunvts
```

Refer to the SunVTS user's guide for detailed startup instructions.

The following instructions assume that SunVTS was started using the CDE user interface.

2. **On the SunVTS Diagnostic main window, set the System Map to Logical mode.**

Note – Physical mode is also supported; however, this procedure assumes you are using Logical mode.

---

3. **Disable all tests by clearing their check boxes.**
4. **Select the check box for Network, then select the plus box for Network to display all tests in the Network group.**

5. **Clear check boxes in the Network group that are not named** `vca`*N*`(netlbtest)`**. Note that** *N* **specifies the placement of the instance number of the device under test.**

   - If a `vca`*N*`(netlbtest)` is displayed, then go to Step 6.
   - If a `vca`*N*`(netlbtest)` is not displayed, probe the system to find it by selecting Reprobe system in the Commands drop-down menu.

   Refer to the SunVTS user's guide for the exact procedure. When the probe completes and a `vca`*N*`(netlbtest)` is displayed, continue to Step 6.

6. **Select the Intervention Mode button. Select one of the instances of** `vca`*N*`(netlbtest)`**, then right-click and drag to display the Test Parameter Options dialog box.**

   These options, which only pertain to `netlbtest`, are described in the SunVTS test reference manual.

7. **After you have made all selections, select Apply from the Within Instance drop-down menu to change the selected instance of** `vca`*N*`(netlbtest)`**, or select Apply from the Across All Instances drop-down menu to change all checked instances of** `vca`*N*`(netlbtest)`**.**

   This action removes the dialog box and returns you to the SunVTS Diagnostic main window.

8. **Select one of the instances of** `vca`*N*`(netlbtest)` **then right-click and drag to display the Test Execution Options dialog box.**

   An alternate method of displaying the Test Execution Options dialog box is to select the Options drop-down main menu; then select Test Executions. These options are generic SunVTS controls that affect all tests. Refer to the SunVTS user's guide for detailed information.

9. **When you have made all selections, select Apply to remove the dialog box the return to the SunVTS Diagnostic main window.**

10. **Select Start to perform the selected tests.**

11. **Select Stop to stop all tests.**

▼ To Perform `nettest`

1. **As superuser, start SunVTS.**

```
# /opt/SUNWvts/bin/sunvts
```

Refer to the SunVTS user's guide for detailed startup instructions.

The following instructions assume that SunVTS was started using the CDE user interface.

2. **On the SunVTS Diagnostic main window, set the System Map to Logical mode.**

Note – Physical mode is also supported; however, this procedure assumes you are using Logical mode.

---

3. **Disable all tests by clearing their check boxes.**
4. **Select the check box for Network, then select the plus box for Network to display all tests in the Network group.**
5. **Clear check boxes in the Network group that are not named** `vca`*N*`(nettest)`**. Note that** *N* **specifies the placement of the instance number of the device under test.**
   - If a `vca`*N*`(nettest)` is displayed, then go to Step 6.
   - If a `vca`*N*`(nettest)` is not displayed, enter `ifconfig -a` in another window on the server containing the `vca`*N* board. There should be an entry listed as follows:

```
vcaN up inet ip-address plumb
```

   If the preceding `ifconfig` entry is not listed, the `nettest` probe will not consider the device testable, and you should follow the `ifconfig` online manual page instructions for bringing an interface online.

   Once the `ifconfig -a` produces the preceding entry, return to the SunVTS Diagnostic main window and probe the system to find `vca` by selecting Reprobe system in the Commands drop-down menu.

   Refer to the SunVTS user's guide for the exact procedure. When the probe completes and a `vca0(nettest)` is displayed, continue to Step 6.

6. **Select one of the instances of** `vca`*N*`(nettest)`**, then right-click and drag to display the Test Parameter Options dialog box.**

   These options, which only pertain to `nettest`, are described in the SunVTS test reference manual.

7. **After you have made all selections, select Apply from Within Instance drop-down menu to change the selected instance of** `vca`*N*`(nettest)`**, or select Apply from the Across All Instances drop-down menu to change all checked instances of** `vca`*N*`(nettest)`**.**

This action removes the dialog box and returns you to the SunVTS Diagnostic main window.

8. **Select one of the instances of** `vca`*N*`(nettest)`**, then right-click and drag to display the Test Execution Options dialog box.**

   An alternate method of displaying Test Execution Options dialog box is to select the Options drop-down main menu; then select Test Executions. These options are generic SunVTS controls that affect all tests. Refer to the SunVTS user's guide for detailed information.

9. **When you have made all selections, select Apply to remove the dialog box, then return to the SunVTS Diagnostic main window.**

10. **Select Start to perform the selected tests.**

11. **Select Stop to stop all tests.**

Note – Do not select `nettest` and `netlbtest` to be performed simultaneously.

Using `kstat` to Determine Cryptographic Activity

The Sun Crypto Accelerator 4000 board does not contain lights or other indicators to reflect cryptographic activity on the board. To determine whether cryptographic work requests are actually being performed on the board, use the `kstat`(1M) command to display the device usage:

```
# kstat vca:0
module: vca                     instance: 0
name:   vca0                    class:    misc
        3desbytes               3040
        3desjobs                5
        crtime                  65.342725895
        dsasign                 0
        dsaverify               0
        rngbytes                10592
        rngjobs                 187
        rngsha1bytes            16328
        rngsha1jobs             327
        rsaprivate              9
        rsapublic               0
        snaptime                106956.467004482
```

Note – In the previous example, `0` is the instance number of the `vca` device. This number should reflect the instance number of the board for which you are performing the `kstat` command.

Displaying the `kstat` information indicates whether cryptographic requests or "jobs" are being sent to the Sun Crypto Accelerator 4000 board. A change in the *jobs* values over time indicates that the board is accelerating cryptographic work requests sent to the Sun Crypto Accelerator 4000 board. If cryptographic work requests are not being sent to the board, verify your web server configuration per the web server specific configuration.

Do not attempt to interpret the kernel / driver statistic values returned by `kstat`(1M). These values are maintained within the driver to facilitate field support. The meanings and actual names may change over time.

Note – If the `nostats` property is defined in the `/kernel/drv/vca.conf` file, the capture and display of statistics will be disabled. This property may be used to help prevent traffic analysis.

Using the OpenBoot PROM FCode Self-Test

The following tests are available to help identify problems with the adapter if the system does not boot.

You can invoke the FCode self-test diagnostics by using the OpenBoot PROM (OBP) `test` or `test-all` commands. If you encounter an error while performing diagnostics, appropriate messages will be displayed. Refer to the *OpenBoot Command Reference Manual* for more information on the `test` and `test-all` commands.

The FCode self-test exercises most functionality subsection by subsection and ensures the following:

- Connectivity during adapter board installation
- Verification that all components required for a system boot are functional

▼ Performing the Ethernet FCode Self-Test Diagnostic

To perform the Ethernet diagnostics, you must first bring the system to a stop at the OBP prompt after issuing a reset. If you do not reset the system, the diagnostic tests might cause the system to hang.

For more information about the OpenBoot commands in this section, refer to the *OpenBoot Command Reference Manual*.

1. **Shut down the system.**

   Use the standard shutdown procedures described in the *Solaris Handbook for Sun Peripherals*.

2. **At the OBP prompt, set the `auto-boot?` configuration variable to `false`.**

```
ok setenv auto-boot? false
```

3. **Reset the system.**

```
ok reset-all
```

4. **Type** `show-nets` **to display the list of devices and enter a selection:**

   You should see a list of devices, similar to the example below, specific to the adapter:

```
ok show-nets
a) /pci@8,600000/network@1
b) /pci@8,700000/network@5,1
q) NO SELECTION
Enter Selection, q to quit: a
/pci@8,600000/network@1 has been selected.
Type ^Y ( Control-Y ) to insert it in the command line.
e.g. ok nvalias mydev ^Y for creating devalias mydev for
/pci@8,600000/network@1
```

Note – To perform the following self-test with the `test` command, the Ethernet port must be connected to a network.

---

5. **Perform the self-test using the** `test` **command:**

   The following tests are performed when the `test` command is executed:

   - `vca` register test (happens only when `diag-switch?` is true)
   - Internal loopback test
   - link up / down test

Note – The Sun Crypto Accelerator 4000 UTP adapter self-test for a 1000 Mbps connection is not supported for use with an external loopback cable because the link-clock cannot be reconciled. For this test, the local and remote ports must reconcile as clock master and clock slave. If an external loopback cable is used, both the local and remote ports are identical. Hence, the single port cannot be both a clock master and a clock slave, which causes the PHY link-up to always fail. For a Sun Crypto Accelerator 4000 UTP adapter self-test for a 1000 Mbps connection to work, a remote 1000Base-T port must be connected.

Type the following:

```
ok test device_path
```

If the `test` passes, you see the following messages:

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: 100 Mbps half duplex link up
```

If the board is not connected to a network, you see the following messages:

```
ok test /pci@8,600000/network@1
Testing /pci@8,600000/network@1
Register tests: passed
Internal loopback test: passed
/pci@8,600000/network@1: link down
```

6. **After testing the adapter, type the following to return the OBP interface to standard operating mode:**

```
ok setenv diag-switch? false
```

7. **Set the** `auto-boot?` **configuration parameter to** `true`**.**

```
ok setenv auto-boot? true
```

8. **Reset and reboot the system.**

Troubleshooting the Sun Crypto Accelerator 4000 Board

This section describes the commands available at the OBP level for troubleshooting the board. Refer to the *OpenBoot Command Reference Manual* for more information on the commands described in the following subsections.

show-devs

To determine whether the Sun Crypto Accelerator 4000 device is listed in the system: from the OBP prompt, type `show-devs` to display the list of devices. You should see lines in the list of devices, similar to the examples below, specific to the Sun Crypto Accelerator 4000 board:

```
ok show-devs
.
.
/chosen
/packages
/upa@8,480000/SUNW,ffb@0,0
/pci@8,600000/network@1
/pci@8,600000/SUNW,qlc@4
/pci@8,600000/SUNW,qlc@4/fp@0,0
.
.
```

In the preceding example, the `/pci@8,600000/network@1` entry identifies the device path to the Sun Crypto Accelerator 4000 board. There will be one such line for each board in the system.

.properties

To determine whether the Sun Crypto Accelerator 4000 device properties are listed correctly: from the OBP prompt, type `.properties` to display the list of properties.

```
ok .properties
assigned-addresses       82000810 00000000 00102000 00000000 00002000
                          81000814 00000000 00000400 00000000 00000100
                          82000818 00000000 00200000 00000000 00200000
                          82000830 00000000 00400000 00000000 00100000
d-fru-len                00 00 00 00
d-fru-off                00 00 e8 00
d-fru-dev                eeprom
s-fru-len                00 00 08 00
s-fru-off                00 00 e0 00
s-fru-dev                eeprom
compatible               70 63 69 38 30 38 36 2c 62 35 35 35 2e 31 30 38
reg                      00000800 00000000 00000000 00000000 00000000
                          02000810 00000000 00000000 00000000 00002000
                          02000814 00000000 00000000 00000000 00000100
                          02000818 00000000 00000000 00000000 00200000
                          02000830 00000000 00000000 00000000 00100000
address-bits             00 00 00 30
max-frame-size           00 00 40 00
network-interface-type   ethernet
device_type              network
name                     network
local-mac-address        08 00 20 aa bb cc
version                  Sun PCI Crypto Accelerator 4000 1000Base-T Code
2.11 02/10/31
phy-type                 mif
board-model              501-6039
model                    SUNW,pci-vca
fcode-rom-offset         00000000
66mhz-capable
fast-back-to-back
devsel-speed             00000001
class-code               00100000
interrupts               00000001
latency-timer            00000040
cache-line-size          00000010
max-latency              00000040
min-grant                00000040
subsystem-id             00003de8
subsystem-vendor-id      0000108e
revision-id              00000002
device-id                0000b555
vendor-id                00008086
```

watch-net

To monitor a network connection: from the OBP prompt, type the `apply watch-net` command with the device path:

```
ok apply watch-net /pci@8,600000/network@1
/pci@8,600000/network@1: 1000 Mbps full duplex link up
Watch ethernet packets
'.' is a good packet and 'X' is a bad packet
Press any key to stop
.....X...X......X.....
```

The system monitors network traffic, displaying "." each time it receives an error-free packet and "X" each time it receives a packet with an error that can be detected by the network hardware interface.

APPENDIX **A**

Specifications

This appendix lists the specifications for the Sun Crypto Accelerator 4000 MMF and UTP adapters. It contains the following sections:

Sun Crypto Accelerator 4000 MMF Adapter

This section provides the specifications for the Sun Crypto Accelerator 4000 MMF adapter.

Connectors

FIGURE A-1 shows the connector for the Sun Crypto Accelerator 4000 MMF adapter.

FIGURE A-1 Sun Crypto Accelerator 4000 MMF Adapter Connector

TABLE A-1 lists the characteristics of the SC connector (850 nm).

TABLE A-1 SC Connector Link Characteristics (IEEE P802.3z)

Characteristic	62.5 Micron MMF	50 Micron MMF
Operating range	Up to 260 meters	Up to 550 meters

Physical Dimensions

TABLE A-2 Physical Dimensions

Dimension	Measurement	Metric Measurement
Length	12.283 inches	312.00 mm
Width	4.200 inches	106.68 mm

Performance Specifications

TABLE A-3 Performance Specifications

Feature	Specification
PCI clock	33/66 MHz max
PCI data burst transfer rate	Up to 64-byte bursts
PCI data/address width	32/64-bit
PCI modes	Master/slave
1 Gbps, 850 nm	1000 Mbps (full duplex)

Power Requirements

TABLE A-4 Power Requirements

Specification	Measurement
Maximum power consumption	6.25 W @ 5V 12.75 W @ 3.3V
Voltage tolerance	5V +/- 5% 3.3V +/- 5%

Interface Specifications

TABLE A-5 Interface Specifications

Feature	Specification
PCI clock	33 MHz or 66 MHz
Host interface	PCI 2.1 with support for 33 MHz or 66 MHz clock rate and 3.3V or 5V power.
PCI bus width	32 bits or 64 bits

Environmental Specifications

TABLE A-6 Environmental Specifications

Condition	Operating Specification	Storage Specification
Temperature	0° to +55° C, +32° to +131° F	-40° to +75° C, -40° to +167° F
Relative humidity	5 to 85% noncondensing	0 to 95% noncondensing

Sun Crypto Accelerator 4000 UTP Adapter

This section provides the specifications for the Sun Crypto Accelerator 4000 UTP adapter.

Connectors

FIGURE A-1 shows the connector for the Sun Crypto Accelerator 4000 UTP adapter.

FIGURE A-2 Sun Crypto Accelerator 4000 UTP Adapter Connector

TABLE A-7 lists the characteristics of the Cat-5 connector used by the Sun Crypto Accelerator 4000 UTP adapter.

TABLE A-7 Cat-5 Connector Link Characteristics

Characteristic	Description
Operating range	Up to 100 meters

Physical Dimensions

TABLE A-8 Physical Dimensions

Dimension	Measurement	Metric Measurement
Length	12.283 inches	312.00 mm
Width	4.200 inches	106.68 mm

Performance Specifications

TABLE A-9 Performance Specifications

Feature	Specification
PCI clock	33/66 MHz max
PCI data burst transfer rate	up to 64-byte bursts
PCI data/address width	32/64-bit
PCI modes	Master/slave
1 Gbps, 850 nm	1000 Mbps (full duplex)

Power Requirements

TABLE A-10 Power Requirements

Specification	Measurement
Maximum power consumption	6.25 W @ 5V 12.75 W @ 3.3V
Voltage tolerance	5V +/- 5% 3.3V +/- 5%

Interface Specifications

TABLE A-11 Interface Specifications

Feature	Specification
PCI clock	33 MHz or 66 MHz
Host interface	PCI 2.1 with support for 33 MHz or 66 MHz clock rate and 3.3V or 5V power
PCI bus width	32 bits or 64 bits

Environmental Specifications

TABLE A-12 Environmental Specifications

Condition	Operating Specification	Storage Specification
Temperature	0° to +55° C, +32° to +131° F	-40° to +75° C, -40° to +167° F
Relative humidity	5 to 85% noncondensing	0 to 95% noncondensing

APPENDIX **B**

SSL Configuration Directives for Apache Web Servers

This appendix lists directives for using Sun Crypto Accelerator 4000 software to configure SSL support for Apache Web Servers. Configure directives in your `http.conf` file. Refer to the Apache Web Server documentation for more information.

1. `SSLPassPhraseDialog exec:`*program*

   Context: Global

   This directive informs the Apache Web Server that the specified *program* should be executed to collect the password for key file. *program* should print the collected password to standard output.

   If multiple key files are present, and have common passwords, then *program* will only be executed once (each collected password is tried before running *program* again.)

   program is executed with two arguments, the first is the name of the server, in the form *servername*:*port*, for example, `www.fictional-company.com:443`. (Port 443 is the typical port for SSL based web servers.) The second argument is the type of key in the key file (*keytype*). *keytype* can be either RSA or DSA.

Note – Because this program can be executed during system startup, be sure to design it to cope with the situation where the console is not a `tty` device (that is, a `tty`(3c) returns false).

   The supplied program `/opt/SUNWconn/cryptov2/bin/apgetpass` can be used for the *program* executable. This program automatically prompts for the password, suppressing the display of the password as it is entered.

   The supplied `sslpassword` program also automatically searches for passwords in files, which can be used to avoid user interaction when the web server starts up. Passwords for key files are searched for in files named

`/etc/apache/`*servername*:*port*.*keytype*`.pass`. If this file is not present, then the file `/etc/apache/default.pass` is used. These password files contain only the unencrypted password on a line by itself.

Note – Password files should be protected by permissions so that only the UNIX user that the web server runs as can read the file. This user should be the same user as configured with the standard Apache `User` directive.

If not specified, the default behavior uses an internal prompting mechanism. Do not use the default; use the supplied `sslpassword` program instead, to avoid problems with interaction at system startup.

2. `SSLEngine` (`on|off`)

   Context: Global, virtual host

   This directive enables the SSL protocol. It is typically used in a virtual host to enable SSL on a subset of servers. One form commonly used is:

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

This statement configures the use of SSL for any servers listening on port 443 (the standard HTTPS port). If not present, this protocol is turned off by default.

3. `SSLProtocol [+-]`*protocol*

   Context: global, virtual host

   This directive configures the protocol(s) that the server should use for SSL transactions. The available protocols are listed and described in TABLE B-1:

TABLE B-1 SSL Protocols

Protocol	Description
`SSLv2`	Original standard SSL protocol from Netscape
`SSLv3`	Updated version of the SSL protocol, supported by most popular web browsers
`TLSv1`	Update to `SSLv3` currently undergoing IETF standardization, with minimal browser support
`all`	Enable all protocols

Using the plus (+) or minus (-) signs, protocols can be added or removed. For example, to disable support for SSLv2, the following directive could be used:

```
SSLProtocol all -SSLv2
```

The preceding statement is equivalent to:

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   Context: Global, virtual host, directory, `.htaccess`

   The SSLCipherSuite directive is used to configure which SSL ciphers are available for use and their preference. In global context or virtual host context, directive is used during the initial SSL handshake. In per-directory context, it forces an SSL renegotiation to use the named ciphers. The renegotation takes place after the request is read, but before the response is sent.

   The *cipher-spec* is a colon-delimited list of the ciphers described in TABLE B-2. In TABLE B-2, DH refers to Diffie-Hellman and DSS refers to the Digital Signature Standard.

TABLE B-2 Available SSL Ciphers

Cipher-Tag	Protocol	Key Exchange	Auth.	Encryption	MAC	Type
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES (168-bit)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES (168-bit)	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR (128-bit)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR (128-bit)	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR (128-bit)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO (128-bit)		
DES-CBC-SHA	SSLv3	RSA	RSA	DES (56-bit)	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR (64-bit)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES (56-bit)	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA (512 bit)	RSA	DES (40-bit)	SHA1	export
EXP-RC2-CBC-MD5	SSLv2	RSA (512 bit)	RSA	ARCTWO (40-bit)	SHA1	export
EXP-RC2-CBC-MD5	SSLv3	RSA (512 bit)	RSA	ARCTWO (40-bit)	SHA1	export
EXP-RC4-MD5	SSLv3	RSA (512 bit)	RSA	ARCFOUR (40-bit)	MD5	export

TABLE B-2 Available SSL Ciphers *(Continued)*

Cipher-Tag	Protocol	Key Exchange	Auth.	Encryption	MAC	Type
EXP-RC4-MD5	SSLv2	RSA (512 bit)	RSA	ARCFOUR (40-bit)	MD5	export
NULL-SHA	SSLv3	RSA	RSA	None	SHA1	
NULL-MD5	SSLv3	RSA	RSA	None	MD5	
ADH-DES-CBC3-SHA	SSLv3	DH	None	3DES (168-bit)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	None	DES (56-bit)	SHA1	
ADH-RC4-MD5	SSLv3	DH	None	ARCFOUR (128-bit)	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES (168-bit)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES (168-bit)	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES (56-bit)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES (56-bit)	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512 bit)	RSA	DES (40-bit)	SHA1	export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH (512 bit)	DSS	DES (40-bit)	SHA1	export
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512 bit)	None	DES (40-bit)	SHA1	export
EXP-ADH-RC4-MD5	SSLv3	DH (512 bit)	None	ARCFOUR (40-bit)	MD5	export

TABLE B-3 lists and describes the aliases that provide macro-like groupings.

TABLE B-3 SSL Aliases

Alias	Description
SSLv2	All SSL version 2.0 ciphers
SSLv3	All SSL version 3.0 ciphers
EXP	All export-grade ciphers
EXPORT40	All 40-bit export ciphers
EXPORT56	All 56-bit export ciphers
LOW	Lower strength ciphers (DES, 40-bit RC4)
MEDIUM	All 128-bit ciphers
HIGH	All ciphers using Triple DES
RSA	All ciphers using RSA key exchange
DH	All ciphers using Diffie-Hellman key exchange
EDH	All ciphers using Ephemeral Diffie-Hellman key exchange

TABLE B-3 SSL Aliases *(Continued)*

Alias	Description
ADH	All ciphers using anonymous Diffie-Hellman key exchange
DSS	All ciphers using DSS authentication
NULL	All ciphers using no encryption

The preference of ciphers can be configured using the special characters listed and described in TABLE B-4.

TABLE B-4 Special Characters to Configure Cipher Preference

Character	Description
<none>	Add cipher to list
!	Remove a cipher from the list entirely—it cannot be added again
+	Add cipher to list, and pull to current location (possibly demoting it)
-	Remove cipher from list (can be added later in list)

The default value of *cipher-spec* is

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

The default configures all ciphers except anonymous (unauthenticated) Diffie-Hellman, giving preference to ARCFOUR and RSA, and then higher grades of encryption over the lower grades.

5. `SSLCertificateFile` *file*

   Context: Global, virtual host

   This directive specifies the location of the PEM-encoded X.509 certificate file for this server.

6. `SSLCertificateKeyFile` *file*

   Context: Global, virtual host

   This directive specifies the location of the PEM-encoded private key file for this server, corresponding to the certificate configured with the `SSLCertificateFile` directive.

7. `SSLCertificateChainFile` *file*

   Context: Global, virtual host

   This directive specifies the location of a file containing the PEM-encoded certificates making up the certification path of the server. You can use the directive to assist clients in verifying the server's certificate when the server's certificate is not directly signed by an authority that the client recognizes.

Certificates in the chain are assumed to be valid for client authentication as well, when client authentication (`SSLVerifyClient`) is used.

8. `SSLCACertificateFile` *file*

   Context: Global, virtual host

   This directive specifies the location of a file containing the concatenation of the certificates for certification authorities (CAs) used for client authentication.

9. `SSLCARevocationFile` *file*

   Context: Global, virtual host

   This directive specifies the location of a file containing the concatenation of the certificate revocation lists of CAs used for client authentication.

10. `SSLVerifyClient` *level*

    Context: Global, virtual host, directory, `.htaccess`

    This directive configures the authentication of clients to the server. (Note that this is not normally needed for e-commerce applications, but has use in other applications.)

    Values for *level* are listed and described in TABLE B-5.

TABLE B-5 SSL Verify Client Levels

Level	Description
`none`	No client certificate is required
`optional`	Client may present a valid certificate
`require`	Client *must* present a valid certificate
`optional_no_ca`	Client may present a certificate, but it need not be valid

Typically either `none` or `require` is used. The default is `none`.

11. `SSLVerifyDepth` *depth*

    Context: Global, virtual host, directory, `.htaccess`

    This directive specifies the maximum certificate chain depth that the server will allow for client certificates. A value of 0 means that only self-signed certificates are eligible, whereas a value of 1 means that client certificates must be signed by a CA known directly to the server (through the `SSLCACertificateFile`). Larger values permit delegation of the CA.

12. `SSLLog` *filename*

    Context: Global, virtual host

This directive specifies a log file where SSL-specific information will be logged. If not specified (default), then no SSL-specific information will be logged.

13. `SSLLogLevel` *level*

Context: Global, virtual host

This directive specifies the verbosity of the information logged in the SSL log file. Values for *level* are listed and described in TABLE B-6.

TABLE B-6 SSL Log Level Values

Value	Description
`none`	no logging, but error messages are still sent to the standard Apache error log
`warn`	Include warning messages
`info`	Include information messages
`trace`	Include trace messages
`debug`	Include debugging messages

14. `SSLOptions` [`+-`] *option*

Context: Global, virtual host, directory, `.htaccess`

This directive configures SSL runtime options on a per-directory basis. Options can be added to the current configuration by prefixing them with a plus sign (+), or removed using a minus sign (-). If multiple options could apply to a directory, the most restrictive option is used; the options are not merged.

Options are listed and described in TABLE B-7.

TABLE B-7 Available SSL Options

Options	Description
`StdEnvVars`	Standard set of SSL-related CGI/SSI environment variables are created—there is a performance penalty for this.
`ExportCertData`	Causes the `SSL_SERVER_CERT`, `SSL_CLIENT_CERT` and `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...) environment variables to be exported. These variables contain PEM-encoded certificates for the client and server.
`FakeBasicAuth`	Distinguished Name (DN) of the client certificate is translated into an HTTP Basic Authentication Username, and is "faked" to have authentication. This allows the use of standard Apache access control mechanisms with SSL client authentication without prompting the user for a password. Entries for these users in the Apache password files must use the encrypted password `xxj31ZMTZzkVA`, which is just an encrypted form (`crypt`(3c)) of the word "password."
`StrictRequire`	Forces a forbidden access due to `SSLRequireSSL` to be denied, even in the presence of other directives, such as `Satisfy Any`, which might override this.

15. `SSLRequireSSL`

Context: Directory, `.htaccess`

This directive forbids access in a given directory unless HTTPS is used. Use the directive to guard against misconfigurations that might otherwise leave a directory's contents available to unauthenticated and unencrypted accesses.

APPENDIX **C**

Building Applications for Use With the Sun Crypto Accelerator 4000 Board

This appendix describes the software supplied with the Sun Crypto Accelerator 4000, which can be used to build OpenSSL-compatible applications to take advantage of the cryptographic acceleration features of the Sun Crypto Accelerator 4000 board. Not all OpenSSL applications will benefit from being compiled in this fashion (as opposed to being built with the stock OpenSSL library, which can be downloaded from `www.openssl.org`).

Note – This information on building applications to use the Sun Crypto Accelerator 4000 software and hardware is provided strictly as-is, and is not an officially supported part of this product. This information is provided in the hope it may be useful, but without any warranty. If you require a Sun-supported solution, please contact Sun Professional Services to learn about your options.

You must first install the `SUNWkcl2o` package, which contains the required header files and libraries.

Your application must be configured to include OpenSSL headers from `/opt/SUNWconn/cryptov2/include`, such as with the compiler flag:

```
-I/opt/SUNWconn/cryptov2/include
```

Additionally, the linker must be directed to include references to the appropriate libraries. Most OpenSSL-compatible applications reference either or both of the `libcrypto.a` and `libssl.a` libraries. The Sun cryptographic libraries must also be included. The following linker attributes will accomplish this:

```
-L/opt/SUNWconn/cryptov2/lib -R/opt/SUNWconn/cryptov2/lib \
-lcrypto -lssl -lkcl
```

APPENDIX **D**

Software Licenses

This appendix provides the Sun Binary Code License Agreement and third-party software notices and licenses.

Note – The third-party licenses and notices provided in this appendix are included exactly as they are provided by the owners of the software licenses and notices.

Sun Microsystems, Inc.

Binary Code License Agreement

READ THE TERMS OF THIS AGREEMENT AND ANY PROVIDED SUPPLEMENTAL LICENSE TERMS COLLECTIVELY "AGREEMENT") CAREFULLY BEFORE OPENING THE SOFTWARE MEDIA PACKAGE. BY OPENING THE SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF THE SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT.

1. LICENSE TO USE. Sun grants you a non-exclusive and non-transferable license for the internal use only of the accompanying software and documentation and any error corrections provided by Sun (collectively "Software"), by the number of users and the class of computer hardware for which the corresponding fee has been paid.

2. RESTRICTIONS Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Except as specifically authorized in any Supplemental License Terms, you may not make copies of Software, other than a single copy of Software for archival purposes. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Software is not designed,

licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

3. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software.

4. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, 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 THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

5. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose.

6. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Upon Termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

8. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

9. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

10. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

11. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

For inquiries please contact: Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054

(Form ID#011801)

Sun Microsystems, Inc.

Supplemental Terms for Sun Crypto Accelerator 4000

These Supplemental Terms for the Sun Crypto Accelerator 4000 supplement the terms of the Binary Code License Agreement ("BCL"). Capitalized terms not defined herein shall have the meanings ascribed to them in the BCL. These Supplemental Terms will supersede any inconsistent or conflicting terms in the BCL. Use of the Software constitutes acceptance of the BCL as supplemented hereby.

1. THIRD PARTY LICENSE TERMS. Some portions of Software are provided with notices and/or licenses from other parties which govern the use of those portions.

Third Party License Terms

OPENSSL LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE

OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

``Ian Fleming was a UNIX fan!
How do I know? Well, James Bond
had the (license to kill) number 007,
i.e. he could execute anyone."
-- Unknown

MOD_SSL LICENSE

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2000 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

APPENDIX **E**

Manual Pages

This appendix provides descriptions of the Sun Crypto Accelerator 4000 board commands and lists the online manual pages for each. The commands in this appendix are included with the Sun Crypto Accelerator 4000 software.

The online manual pages can be viewed with the following command:

```
man -M /opt/SUNWconn/man page
```

TABLE E-1 lists and describes the available online manual pages.

TABLE E-1 Sun Crypto Accelerator 4000 Online Manual Pages

man page	Description
vca(7d)	The vca device driver is a leaf driver that provides access control to the underlying hardware cryptographic accelerator. The vca driver requires the presence of layered software for applications and kernel clients to access the provided services.
vcad(1m)	The vcad daemon provides keystore services.
vcaadm(1m)	vcaadm is the administration program for the Sun Crypto Accelerator 4000. The vcaadm command is used to manually manipulate the configuration, account, and keying databases associated with the Sun Crypto Accelerator 4000 board. vcaadm handles sensitive cryptographic key information.
vcadiag(1m)	vcadiag is a utility that allows root users to reset Sun Crypto Accelerator 4000 boards and to zeroize key material. This utility also allows root users to perform basic diagnostics.
kcl2(7d)	kcl2 is a kernel module that provides support for cryptographic hardware drivers.

TABLE E-1 Sun Crypto Accelerator 4000 Online Manual Pages *(Continued)*

man page	Description
kcl2(7d)	The kcl2 device driver is a multithreaded loadable kernel module providing support for Sun cryptographic provider drivers. The kcl2 driver requires the presence of layered software for applications and kernel clients to access the provided services.
apsslcfg(1m)	apsslcfg is the configuration utility for Apache Web Servers.
iplsslcfg(1m)	iplsslcfg is the configuration utility for Sun ONE Web Servers.

APPENDIX **F**

Zeroizing the Hardware

This appendix describes how to zeroize the Sun Crypto Accelerator 4000 board to the factory state which is the `failsafe` mode for the board.

Caution – You should use the procedures described in this appendix only if it is absolutely necessary. The `zeroize` command in `vcaadm` is appropriate if you need to remove all key material. Refer to “Zeroizing a Sun Crypto Accelerator 4000 Board” on page 80 for details on the `zeroize` command. Also refer to the online manual pages for `vcadiag`(4) for removing all key material.

Note – The procedures described in this appendix remove the Sun Crypto Accelerator 4000 firmware. You will have to reinstall the firmware which is provided with the Sun Crypto Accelerator 4000 software.

Zeroizing the Sun Crypto Accelerator 4000 Hardware to the Factory State

In some situations, it may become necessary to return a board to `failsafe` mode, and clear it of all key material and configuration information. This can only be done by using the hardware jumper attached to the board.

Note – You can use the `zeroize` command with the `vcaadm` utility to remove all key material from a Sun Crypto Accelerator 4000 board. However, the `zeroize` command leaves any updated firmware intact. See “Zeroizing a Sun Crypto Accelerator 4000 Board” on page 80. Also refer to the `vcadiag` online manual pages.

▼ To Zeroize the Sun Crypto Accelerator 4000 Board With the Hardware Jumper

1. **Power off the system.**

Note – For some systems, you can use dynamic reconfiguration (DR) to remove and replace the board as necessary for this procedure instead of powering off the system. Refer to the documentation delivered with your system for the correct DR procedures.

Caution – The board must not receive any electrical power while adjusting the jumper.

---

2. **Remove the computer cover to get access to the jumper located at the top middle of the board.**

3. **Place the jumper on pins 0 and 1 of the jumper block.**

   Pins 0 and 1 are the pins closest to the bracket and labeled with a “Z.” There are four sets of two pins and the jumper should only be placed on the 0 and 1 pin set as shown in FIGURE F-1.

Caution – You cannot use the Sun Crypto Accelerator 4000 board with the jumper on pins 0 and 1.

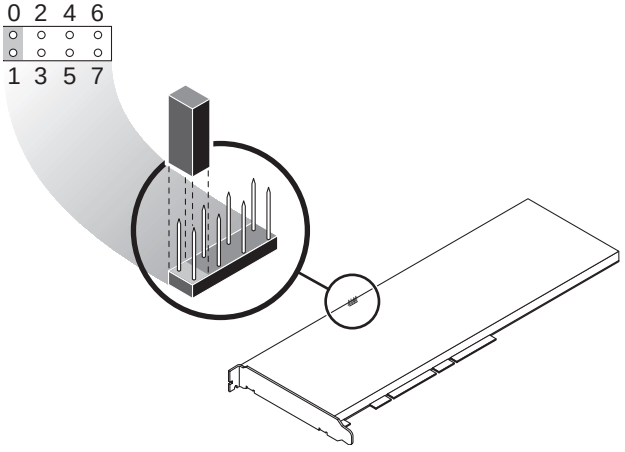

FIGURE F-1 Sun Crypto Accelerator 4000 Board Jumper Block Pins

4. **Power on the system.**

Caution – When you power on the system after adjusting the Sun Crypto Accelerator 4000 board jumper, all firmware, key material, and configuration information is deleted. This process returns the board to the factory state and places the board in `failsafe` mode.

5. **Power off the system.**
6. **Remove the jumper from pins 0 and 1 of the jumper block and store the jumper in the original location.**
7. **Power on the system.**
8. **Connect to the Sun Crypto Accelerator 4000 board with** `vcaadm`.

   `vcaadm` prompts you for a path to upgrade the firmware.

9. **Type** `/opt/SUNWconn/cryptov2/firmware/sca4000fw` **as the path for installing the firmware.**

   The firmware is automatically installed and you are logged out of `vcaadm`.

10. **Reconnect to Sun Crypto Accelerator 4000 board with** `vcaadm`**.**

    `vcaadm` prompts you to either initialize the board with a new keystore, or initialize the board to use an existing keystore. See "Initializing the Sun Crypto Accelerator 4000 Board With vcaadm" on page 65.

APPENDIX **G**

Frequently Asked Questions

How Do I Configure the Web Server to Startup Without User Interaction on Reboot?

You can enable both Sun ONE and Apache Web Servers to perform an unattended startup at reboot with an encrypted key.

▼ To Create an Encrypted Key for Automatic Startup of Apache Web Servers on Reboot

1. **Verify that the following entry exists in the `httpd.conf` file:**

```
SSLPassPhraseDialog exec:/opt/SUNWconn/cryptov2/bin/apgetpass
```

This directive retrieves a password from a protected password file in the `/etc/apache` directory.

2. **Create a password file that contains only the password in the `/etc/apache` directory with the following file name convention:**

server_name`:`*port*`.`*KEYTYPE*`.pass`

- *server_name* – The value that you put in the “ServerName” directive in the `httpd.conf` file.
- *port* – The port that this SSL server will run on (for example, 443)
- *KEYTYPE* – Either `RSA` or `DSA`

Example: For a server named `webserv101` running SSL on port 443 with an RSA key, you create the following file in `/etc/apache`:

```
webserv101:443.RSA.pass
```

It is recommended to change the permissions and ownership of the password file as follows:

```
# chmod 400 server_name:port.KEYTYPE.pass
# chown root server_name:port.KEYTYPE.pass
```

Refer to the mod_SSL and OpenSSL documentation for more information.

▼ To Create an Encrypted Key for Automatic Startup of Sun ONE Web Servers on Reboot

1. **Navigate to the `config` subdirectory for your Sun ONE Web Server instance—for example, `/usr/iplanet/servers/https-`*webserver_instance_name*`/config`.**
2. **Create a `password.conf` file with only the following lines (See** TABLE 5-1 **for password definitions):**

```
internal:trust_db_password
keystore_name:username:password
```

3. **Set the file ownership of the password file to the UNIX user ID that the web server runs as, and set the file permissions to be readable only by the owner of the file:**

```
# chown web_server_UNIX_user_ID password.conf
# chmod 400 password.conf
```

How Do I Assign Different MAC Addresses to Multiple Boards Installed in the Same Server?

There are two methods to assign different MAC addresses to multiple boards in a single server. The first method is at the operating environment level, and the second is at the OpenBoot PROM (OBP) level.

▼ To Assign Different MAC Addresses From a Terminal Window

1. **Enter the following command:**

```
# eeprom "local-mac-address?"=true
```

Note – With the "`local-mac-address?`" parameter set to `true`, all nonintegrated network interface devices use the local MAC address assigned to the product at the manufacturing facility.

---

2. **Reboot the system.**

▼ To Assign Different MAC Addresses From the OpenBoot PROM Level

1. **Enter the following command at the OBP prompt:**

```
ok setenv local-mac-address? true
```

Note – With the "`local-mac-address?`" parameter set to `true`, all nonintegrated network interface devices use the local MAC address assigned to the product at the manufacturing facility.

---

2. **Boot the operating environment.**

How Can I Configure the Sun Crypto Accelerator 1000 for Use With Apache After I Have Installed the Sun Crypto Accelerator 4000 Software?

Once the `SUNWkcl2a` software package is installed, the system will be configured with Apache Web Server mod_ssl 1.3.26.

If you want to configure Sun Crypto Accelerator 1000 with Apache, you must have the following patches.

To configure the Sun Crypto Accelerator 1000 for use with Apache 1.3.26 on a Solaris 8 system with the `SUNWkcl2a` package installed, you need the following patches:

- For Apache 1.3.26 – Patch ID 109234-09 or later

- For Sun Crypto Accelerator 1000 version 1.0 software – Patch ID 112869-02
- For Sun Crypto Accelerator 1000 version 1.1 software – Patch ID 113355-01

To configure the Sun Crypto Accelerator 1000 for use with Apache 1.3.26 on a Solaris 9 system with the `SUNWkcl2a` package installed, you need the following patches:

- For Apache 1.3.26 – Patch ID 113146-01 or later
- For Sun Crypto Accelerator 1000 version 1.1 software – Patch ID 113355-01

How Do I Self-Sign a Certificate for Testing?

Refer to the mod_SSL and OpenSSL documentation for this procedure.

Index

B

C

D

E

F

G

H

I

P

Q

R

S

T

U

V

W

Z