Sun™ Crypto Accelerator 1000 介面卡安裝與使用者指南

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

零件編號 816-4570-10
2002 年 3 月，版本 A

請將關於此文件的意見傳送到：docfeedback@sun.com

請進行
資源回收

Adobe PostScript

Declaration of Conformity

EMC

Compliance Model Number: DEIMOS
Product Family Name: Sun Crypto Accelerator 1000 (X6762A)

European Union

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

EN55022:1998/CISPR22:1997		Class A
EN55024:1998	Required Limits (as applicable):	
	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 60950:1999, 3rd Edition

Supplementary Information

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

/S/

Dennis P. Symanski DATE
Manager, Compliance Engineering
Sun Microsystems, Inc.
901 San Antonio Road, MPK15-102
Palo Alto, CA 94303-4900 U.S.A.
Tel: 650-786-3255
Fax: 650-786-3723

/S/

Peter Arkless DATE
Quality Manager
Sun Microsystems Scotland, Limited
Springfield, Linlithgow
West Lothian, EH49 7LR
Scotland, United Kingdom
Tel: 0506-670000 Fax: 0506-760011

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.

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

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

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。

目錄

1. 產品概述 1

硬體概述 1

產品特色 2

動態組態重設與高可用性考量 3

負載分擔 4

硬體與軟體需求 4

必需的修正程式 5

2. 安裝與移除 Sun Crypto Accelerator 1000 介面卡 7

操作介面卡 7

安裝介面卡 8

▼ 安裝硬體 8

安裝 Sun Crypto Accelerator 1000 軟體 9

▼ 安裝軟體 9

目錄與檔案 11

移除軟體 13

▼ 刪除領域 13

▼ 移除軟體 14

3. 啟動由 iPlanet 網站伺服器所使用的介面卡 15

密碼 15

新增與建立領域 16

▼ 新增與建立領域 16

啓動 iPlanet 網站伺服器概述 18

4. 安裝與設定 iPlanet 網站伺服器 4.1 組態 19

安裝 iPlanet 網站伺服器 4.1 19

▼ 安裝 iPlanet 網站伺服器 4.1 19

▼ 新增信任資料庫 20

▼ 產生伺服器憑證 22

▼ 安裝伺服器憑證 24

設定 iPlanet 網站伺服器 4.1 組態 26

▼ 設定 iPlanet 網站伺服器 4.1 組態 26

5. 安裝與設定 iPlanet 網站伺服器 6.0 組態 29

安裝 iPlanet 網站伺服器 6.0 29

▼ 安裝 iPlanet 網站伺服器 6.0 29

▼ 新增信任資料庫 30

▼ 產生伺服器憑證 32

▼ 安裝伺服器憑證 35

設定 iPlanet 網站伺服器 6.0 組態設定 36

▼ 設定 iPlanet 網站伺服器 6.0 組態 36

6. 啟用 Apache 網站伺服器 39

啓用 Apache 網站伺服器 39

▼ 啓用 Apache 網站伺服器 39

建立憑證 42

▼ 建立憑證 42

7. 診斷與疑難排解 47

SunVTS 診斷軟體 47

▼ 執行 dcatest 48

dcatest 測試參數選項 49

dcatest 命令列語法 50

對 Sun Crypto Accelerator 1000 進行疑難排解 51

A. 使用 iPlanet 網站伺服器管理 Sun Crypto Accelerator 1000 介面卡 53

概念與詞彙 53

領域、使用者與 iPlanet 網站伺服器 54

標記與插槽檔案 54

插槽檔案 55

使用 secadm 55

作業模式 56

使用 secadm 輸入命令 57

使用 secadm 進行驗證 58

取得命令說明 60

退出 secadm 程式 60

設定與管理領域 61

建立領域 61

設定目前工作中領域 62

列出領域 63

列出領域類別 63

刪除領域 63

設定與管理使用者帳號 64

建立使用者 64

列出使用者 64

變更使用者密碼 65

啓用或禁用使用者　65

刪除使用者　66

B.　手冊說明頁　67

C.　Apache 網站伺服器 SSL 組態指令行　69

D.　建立應用程式以搭配 Sun Crypto Accelerator 1000 介面卡使用　77

E.　Sun Crypto Accelerator 1000 介面卡規格　79

實體尺寸　79

介面規格　80

電源要求　80

環境規格　81

F.　Third-Party Licenses （協力廠商授權）　83

附表

表 1-1 支援的 SSL 演算法 3

表 1-2 硬體與軟體需求 4

表 1-3 Sun Crypto Accelerator 1000 軟體所必需的修正程式 5

表 1-4 Sun Crypto Accelerator 1000 軟體建議使用的修正程式 5

表 2-1 Sun Crypto Accelerator 1000 目錄 11

表 3-1 iPlanet 網站伺服器所需的密碼 15

表 7-1 `dcatest` 測試參數選項 49

表 7-2 `dcatest` 子測試 49

表 7-3 `dcatest` 命令列語法 50

表 A-1 `secadm` 選項 56

表 A-2 命令對照表 58

表 B-1 Sun Crypto Accelerator 1000 `man` 說明頁 67

表 C-1 SSL 通訊協定 70

表 C-2 可用 SSL 編碼器 71

表 C-3 SSL 別名 72

表 C-4 設定編碼器偏好組態用的特殊字元 73

表 C-5 SSL 檢查用戶端階層 74

表 C-6 SSL 記錄階層數值 75

表 C-7 可用 SSL 選項 76

表 E-1 實體尺寸 79

表 E-2 介面規格 80
表 E-3 電源要求 80
表 E-4 環境規格 81

前言

Sun Crypto Accelerator 1000 介面卡安裝與使用者指南 提供了 Sun™ Crypto Accelerator 1000 介面卡的功能說明、以及如何在系統上安裝及使用此介面卡。

本書假定您爲熟悉 Solaris 作業環境的系統管理者。

UNIX 指令的使用

本文件可能不包含關於基本 UNIX® 指令和程序（例如關閉系統、啓動系統和組態裝置）的資訊。

關於這些資訊，請參閱以下文件：

- *Solaris 硬體平台指南*
- Solaris™ 作業環境的 AnswerBook2™ 線上文件
- 系統附帶的其他軟體文件

排版慣例

字型	含義	範例
AaBbCc123	指令、檔案和目錄的名稱；電腦的螢幕輸出	編輯 .login 檔案。 使用 ls -a 列出所有檔案。 % You have mail。
AaBbCc123	您鍵入的內容，相對於電腦的螢幕輸出	% **su** Password:
AaBbCc123	書名、新詞或術語、需強調的詞彙	請閱讀*使用者指南* 的第 6 章。 這些稱爲*類別* 選項。 要執行此操作，您*必須* 是超級使用者 (superuser) 使用者。
	命令列變數；請使用實際名稱或數值替換	要刪除某個檔案，請輸入 rm *檔案名稱*。

Shell 提示符號

Shell	提示符號
C shell	*machine_name*%
C shell 超級使用者	*machine_name*#
Bourne shell 和 Korn shell	$
Bourne shell 和 Korn shell 超級使用者	#

存取線上 Sun 文件

您可以由下列網址取得各種 Sun 系統文件：

`http://www.sun.com/products-n-solutions/hardware/docs`

完整的 Solaris 文件與其他書籍可以在下列網址找到：

`http://docs.sun.com`

Sun 歡迎您提出意見

我們衷心希望提高文件品質，歡迎您提出意見和建議。請將您的建議透過電子郵件發送給我們，地址是：

`docfeedback@sun.com`

請將文件的編號 (816-4570-10) 寫在電子郵件的主題行中。

第 1 章

產品概述

本章說明 Sun Crypto Accelerator 1000 介面卡。

本章包含了下列幾個部份。

- 第 1 頁的「硬體概述」
- 第 4 頁的「硬體與軟體需求」

硬體概述

Sun Crypto Accelerator 1000 介面卡是一張短 PCI 介面卡，其功能是作爲編碼協同處理器，可以加速公開金鑰與對稱式編碼。本產品沒有外部介面。此介面卡與主機透過內部 PCI 匯流排介面連接。此介面卡的目的，在於加速電子商務應用程式中，安全通訊協定使用的各式電腦運算密集編碼演算法。

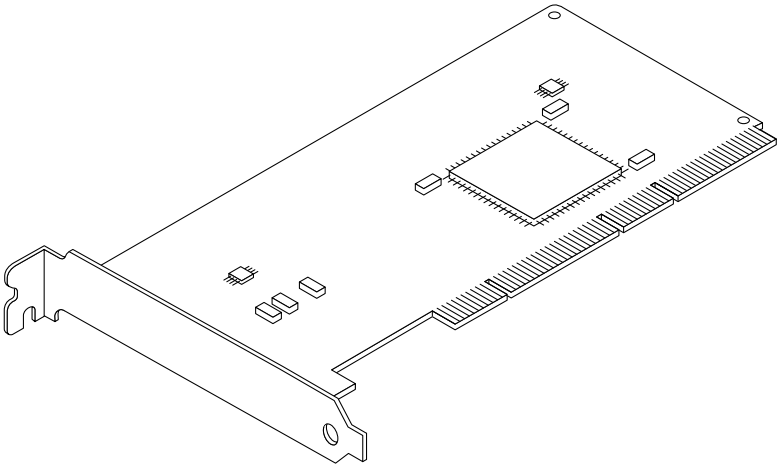


圖 1-1 Sun Crypto Accelerator 1000 介面卡

產品特色

Sun Crypto Accelerator 1000 是用來加強在 Sun 平台上 SSL 的編碼加速器介面卡。Sun Crypto Accelerator 1000 加速在硬體與軟體上的編碼演算。其複雜的原因在於加速編碼演算的成本，並非在所有的演算法中都是一致的。部份編碼演算法是特別設計用於硬體上的，而有些則是設計用於軟體上的。除硬體加速外，將使用者的資料從應用程式空間移到硬體加速裝置、再把運算完的結果放回使用者應用程式中，也會造成不小的效能損失。

請注意，部份編碼演算法（例如 ARCFOUR）可以經由高度微調的軟體執行，並且像在專用的硬體中一樣快。Sun Crypto Accelerator 1000 產品會測試所有的編碼要求，以及判定最好的加速位置（主機處理器或 Sun Crypto Accelerator 1000），以達成最大的處理量。負載分佈是根據編碼演算、目前工作負載、以及資料量來決定。

表 1-1 顯示哪一個加速演算法可以被卸載到硬體，以及哪一個軟體演算法可以提供給 iPlanet 與 Apache 網站伺服器使用。

表 1-1 支援的 SSL 演算法

	IPlanet 網站伺服器		Apache 網站伺服器	
演算法	**硬體**	**軟體**	**硬體**	**軟體**
RSA	X	X	X	X
DSA	X	X	X	X
Diffie-Hellman			X	X
DES	X	X	X	X
3DES	X	X	X	X
ARCFOUR		X		X

動態組態重設與高可用性考量

Sun Crypto Accelerator 1000 硬體及相關軟體提供在支援動態組態重設 (DR) 與熱插拔的 Sun 平台上能有效率運作的功能。例如當動態組態重設或熱插拔作業發生時，Sun Crypto Accelerator 1000 軟體層會自動地偵測出附加或移除的介面卡，並調整排序演算以配合硬體資源的變動。

爲達成高可用性 (HA) 組態，多個 Sun Crypto Accelerator 1000 可以同時安裝在一個系統或網域內，以確保硬體加速持續可用。Sun Crypto Accelerator 1000 幾乎不可能發生故障，倘若一旦出現這樣的情況，軟體層會偵測出故障，並將故障的介面卡從可用硬體編碼加速器清單上移除。Sun Crypto Accelerator 1000 調整排序演算以配合硬體資源的縮減。接著編碼要求會被排序到其餘的介面卡上。

此外，Sun Crypto Accelerator 1000 軟體庫提供在軟體上執行所有編碼作業的功能。這可以支援動態組態重設或熱拔差移除所有系統網裕中的 Sun Crypto Accelerator 1000 機板，但在功能上不會造成減損。在 Sun Crypto Accelerator 1000 硬體恢復組態之前會出現明顯的效能折損。

注意 Sun Crypto Accelerator 1000 硬體提供了高品質一致性以產生長期金鑰。如果網域或系統中的全部 Sun Crypto Accelerator 1000 介面卡都被移除，長期的金鑰產生將會以低品質一致性產生。

負載分擔

Sun Crypto Accelerator 1000 軟體會跨越 Solaris 網域或系統上所有安裝的介面卡分攤負載。收到的編碼要求會依據固定長度工作佇列，跨介面卡來做分配。這些要求會依佇列被送到第一個可以接受這一類型要求的可用介面卡上。序列機制是設計來最佳化輸出量，便於在介面卡上結合需求。

硬體與軟體需求

表 1-2 提供 Sun Crypto Accelerator 1000 介面卡硬體及軟體需求的摘要。

表 1-2 硬體與軟體需求

硬體與軟體	需求
硬體	Sun Blade™ 1000 Sun Enterprise™ 220R, 250, 420R, 450 Sun Fire™ 280R, V480, V880, 4800, 4810, 6800 Sun Netra™ T1 AC200/DC200, Netra 20, Netra t 1400/1405 Sun Ultra™ 60, 80
作業環境	Solaris 8 7/01 或後續相容版本
PCI 插槽	32 位元或 64 位元 33 MHz 或 66 MHz
軟體	iPlanet™ 網站伺服器 4.1 SP9、6.0 SP1，或 Apache 網站伺服器 1.3.12 所有執行 iPlanet 或 Apache 網站伺服器所必需的修正程式

注意 – 當提到 iPlanet 網站伺服器 4.1 或 6.0 時，代表的是已經安裝了這些編號的服務套件（SP9 或 SP1）。

必需的修正程式

當您在系統上執行 Sun Crypto Accelerator 1000 時可能需要下列的修正程式。Solaris 更新包含早期版本的修正程式。使用 `showrev -p` 指令來得知哪些選單上的修正程式已經被安裝過了。

必要的話，您可以從下列的網站上下載修正程式：`http://sunsolve.sun.com`。

安裝最新版的修正程式。破折號後面的數字（例如：-01）會隨著修正程式版本的更新而增加。如果網站上的版本較下列表格中的爲新，那麼它就是較新的版本。

如果您在 SunSolve℠ 上無法找到所需要的修正程式，請與當地銷售人員與服務代表連繫。

下列表格中列出搭配本產品使用所必需與建議的修正程式：表 1-3 列出並說明必需的修正程式。

表 1-3 Sun Crypto Accelerator 1000 軟體所必需的修正程式

修正程式識別碼	說明
110383-01	`libnvpair`
108528-05	`KU-05`（`nvpair` 支援）
112438-01	`/dev/random`

注意 – 如果您計劃使用 Apache 1.3.12 網站伺服器，您必需同時安裝修正程式識別碼 109234-02。

表 1-4 列出並說明建議的修正程式。

表 1-4 Sun Crypto Accelerator 1000 軟體建議使用的修正程式

修正程式識別碼	說明
108528-13	`KU-13`（`nvpair` 安全修正）

第 2 章

安裝與移除 Sun Crypto Accelerator 1000 介面卡

本章說明如果安裝 Sun Crypto Accelerator 1000 硬體與軟體。

本章包含了下列幾個部份

- 第 7 頁的「操作介面卡」
- 第 8 頁的「安裝介面卡」
- 第 11 頁的「目錄與檔案」

操作介面卡

所有的介面卡都包裝在特別的防靜電袋內，以在出貨與存放的過程中保護介面卡。爲了避免介面卡上對靜電極爲敏感的元件受損，在您的身體接觸介面卡前，請使用下列方法以減少身上的靜電：

- 觸碰電腦的金屬邊緣。
- 在手腕繫上防靜電腕帶，並接地至金屬表面上。

注意 – 爲了避免損壞介面卡上敏感的元件，握持介面卡時請穿戴防靜電腕帶，拿取介面卡時請握住邊緣，並將介面卡放置在防靜電表面上 （如隨卡附帶的塑膠袋）。

安裝介面卡

安裝程序包含 Sun Crypto Accelerator 1000 介面卡把介面卡插入系統，並載入軟體工具。硬體安裝說明只包含安裝介面卡的一般步驟。特定的安裝說明，請參考隨系統所附的文件。

▼ 安裝硬體

1. **請以超級使用者身份登入，並依說明關閉電腦、切斷電源、拔掉電源線，接著移除電腦外殼。**
2. **找出未使用的 PCI 插槽 （最好是 64 位元，66 MHz 插槽）。**
3. **將防靜電腕帶繫在您的手腕上，並將另一頭接地至金屬表面上。**
4. **使用十字型螺絲起子，將螺絲從 PCI 蓋板卸下。**

   將螺絲保留以備在步驟 5 中拴住支撐片。
5. **握住 Sun Crypto Accelerator 1000 介面卡的邊緣，將它從塑膠袋裡拿出來，然後插入 PCI 插槽內，接著鎖上背後支撐片的螺絲。**
6. **將電腦外殼蓋好，接上電源線，並將開啟系統電源。**
7. **在 `ok` 提示輸入 `show-devs` 指令以確認介面卡已安裝妥當：**

```
ok show-devs
. . .
/pci@1f,2000/pci108e,5455@1
/pci@1f,4000/pci108e,5455@5
. . .
```

`/pci@1f,2000/pci108e,5455@`*n* 這一行顯示介面卡已安裝，且已由系統辨識出來。

安裝 Sun Crypto Accelerator 1000 軟體

Sun Crypto Accelerator 1000 軟體包含在 *Sun Crypto Accelerator 1000* CD 中。您或許需要從 SunSolve 網站上下載修正程式。請參考第 5 頁的 「必需的修正程式」以取得更多的資訊。

▼ 安裝軟體

1. **將 *Sun Crypto Accelerator 1000* CD 放入與系統連接的 CD-ROM 光碟機中。**
   - 如果系統正在執行 Sun Enterprise Volume Manager™，則它會自動將 CD-ROM 掛入到 `/cdrom/cdrom0` 目錄中。
   - 如果系統沒有執行 Volume Manager，請依下列指示掛入 CD-ROM：

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

您將會在 /cdrom/cdrom0 目錄裡看到下列檔案與目錄。

檔案或目錄	內容
Copyright	英文著作權檔案
FR_Copyright	法文著作權檔案
Docs	Sun Crypto Accelerator 1000 使用者指南
Packages	包含 Sun Crypto Accelerator 1000 軟體套件： SUNWcrypr 編碼核心元件 SUNWcrypu 編碼管理公用程式與程式庫 SUNWcrysu Apache SSL 支援（選用） SUNWcrypm 編碼管理說明頁 SUNWdcar DCA 編碼加速器 (Root) SUNWdcamn DCA 編碼加速器說明頁 SUNWdcav DCA 編碼加速器 SunVTS 測試（選用） SUNWcrysl Apache SSL 發展工具與程式庫

如果您計劃使用 Apache 來做爲網站伺服器，您只需安裝 SUNWcrysu 套件。

如果您計劃重新連結到 Apache 網站伺服器的其他（未支援）版本，請安裝 SUNWcrysl 套件。

如果您計劃執行 SunVTS™ 測試，請安裝 SUNWdcav 套件。您必需先安裝 SunVTS 4.4、4.5、或 4.6，然後再安裝 SUNWdcav 套件。

2. 輸入下列指令以安裝軟體套件：

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

3. 要確認軟體已正確地安裝完成，請執行 pkginfo 指令。

```
# pkginfo SUNWcrypr SUNWcrypu SUNWcrysl SUNWcrysu SUNWcrypm SUNWdcar SUNWdcamn
SUNWdcav
system  SUNWcrypr   Cryptography Kernel Components
system  SUNWcrypu   Cryptographic Administration Utility and Libraries
system  SUNWcrysl   SSL Development Tools and Libraries
system  SUNWcrysu   SSL Support for Apache
system  SUNWcrypm   Cryptographic Administration Manual Pages
system  SUNWdcar    DCA Crypto Accelerator (Root)
system  SUNWdcamn   DCA Crypto Accelerator Manual Page
system  SUNWdcav    SunVTS Test of DCA Crypto Accelerator
```

4. （選用步驟）要確認已安裝驅動程式，請執行 `prtconf` 指令。

```
# prtconf
pci108e,5455, instance #0
pci108e,5455, instance #1
```

5. （選用步驟）執行 `modinfo` 指令來顯示已載入的模組。

```
# modinfo | grep Crypto
130 1033e946   6df0  79   1  cryptio (Cryptographic IOCTL v1.58)
131 1030240c   2d93   -   1  kcl (Cryptographic Library v1.64)
132 10313ac8   131e   -   1  kcpi (Crypto Provider Interface v1.27)
135 103178be   8684  82   1  dca (PCI Crypto Accelerator v1.156)
```

然而，`kcl` 及 `cryptio` 只有在實際使用 Sun Crypto Accelerator 1000 來執行編碼作業後，才會載入或顯示出來。

目錄與檔案

表 2-1 顯示由 Sun Crypto Accelerator 1000 軟體預設安裝時所建立的目錄。

表 2-1 Sun Crypto Accelerator 1000 目錄

目錄	內容
`/etc/opt/SUNWconn/crypto/realms`	領域與使用者資料
`/opt/SUNWconn/crypto/bin`	應用程式執行檔
`/opt/SUNWconn/crypto/lib`	應用程式庫
`/opt/SUNWconn/crypto/sbin`	靜態連結執行檔

圖 2-1 顯示這些階層的目錄與檔案。

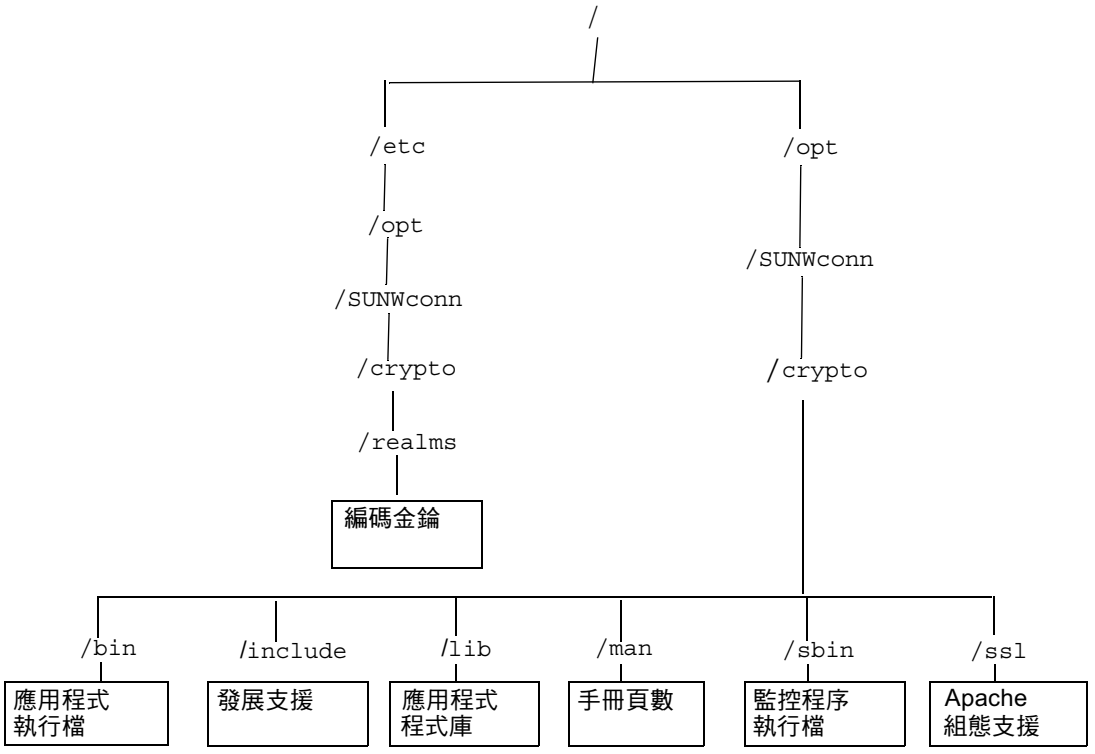


圖 2-1 Sun Crypto Accelerator 1000 目錄與檔案

移除軟體

如果您新增了領域，您必需在移除軟體前先刪除這些領域。如果您未新增領域，您可以放心地忽略下列程序。您可以刪除一個目前正在使用中的領域。要釋出領域，您必需關閉網站伺服器及（或）管理伺服器。

注意 – 在移除 Sun Crypto Accelerator 1000 軟體之前，您必需先關閉所有使用 Sun Crypto Accelerator 1000 介面卡的網站伺服器。如果沒有這麼做，會導致這些網站伺服器無法正常運作。

▼ 刪除領域

1. **以超級使用者的身份存取** `secadm` **公用程式：**

```
# /opt/SUNWconn/crypto/bin/secadm
secadm>
```

2. **使用** `secadm` **公用程式來刪除所有的領域。**

```
secadm> delete realm=realm-name
Delete realm realm-name? [Y/N]: Y
System Administrator Login Required
Login: root
Password:
Realm realm-name deleted successfully.
```

這會移除所有站台內特定的領域資料，包括金鑰資料。

▼ 移除軟體

- **如果只要移除所安裝的軟體套件，請以超級使用者 (superuser) 身份登入，並使用** `pkgrm` **指令來移除。**

  已安裝的套件必需依說明順序移除。沒有依序移除可能引起警告，且無法卸載核心模組。

  如果您已安裝所有的套件，您應該依照下列指示來移除這些套件：

```
# pkgrm SUNWcrysl SUNWdcav SUNWdcar SUNWcrysu SUNWcrypu SUNWcrypr
SUNWdcamn SUNWcrypm
```

注意 – 在安裝或移除了 Sun Crypto Accelerator 1000 的 SunVTS 測試 (`SUNWdcav`) 後，如果 SunVTS 已經在執行了，您也許需要由 SunVTS 來讓系統更新可用的測試。請參考 SunVTS 文件集來取得更多的資訊。

第 3 章

啓動由 iPlanet 網站伺服器所使用的介面卡

本章說明如何啓動使用在 iPlanet 網站伺服器上的 Sun Crypto Accelerator 1000 介面卡。

本章包含了下列幾個部份

- 第 15 頁的「密碼」
- 第 18 頁的「啓動 iPlanet 網站伺服器概述」
- 第 16 頁的「新增與建立領域」

密碼

在啓動 iPlanet 網站伺服器 (iWS) 的過程中，系統會要求您輸入幾個密碼。表 3-1 提供每一個步驟的說明。這些密碼會在本章做說明。如果對於該使用哪一組密碼有疑慮，請參考表 3-1。

表 3-1 iPlanet 網站伺服器所需的密碼

密碼類型	說明
iWS 管理伺服器	啓動 iPlanet 管理伺服器所需的密碼。這個密碼是在 iPlanet 安裝時所指派的。
網站伺服器信任資料庫	在安全模式中執行、要求認證、以及認證安裝完成時，啓動內部編碼模組所需的密碼。在 iPlanet 網站伺服器裡，這個密碼同時適用於金鑰組檔案密碼，與模組內部密碼。
系統管理者	在執行 `secadm` 特定作業時所需的密碼。這是 UNIX 主機密碼。
user@realm-name	在安全模式中執行時，啓動 Sun Crypto Accelator 1000 模組所需要的密碼。這個密碼是在使用 `secadm` 爲領域新增使用者時所指派的密碼。

新增與建立領域

在您於 iPlanet 網站伺服器上啓動使用此介面卡前，您必需先設定並建立領域。如果您尚未完成這個步驟，您必需至少設定一個領域以及一個使用者。請參閱附錄 A 以取得更多領域相關的資訊。

▼ 新增與建立領域

1. **如果您尚未完成這個步驟，請將 Sun Crypto Accelerator 1000 工具目錄放置在您的搜尋路徑裡，例如：**

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

2. **存取** `secadm` **公用程式：**

```
$ secadm
```

3. **使用** `secadm` **公用程式來新增領域：**

```
secadm> create realm=realm-name
System Administrator Login Required
Login: root
Password:
Realm realm-name created successfully.
```

4. 在網域中新增使用者。

這些使用者名稱僅能使用在 Sun Crypto Accelerator 1000 網域中，且不需與執行網站伺服器程序的 UNIX 使用者名稱一致。在新增使用者之前，請記得您必需先設定目前執行的領域，並以系統管理者身份登入。

在您新增使用者之前，您必需先設定將產生使用者的領域。

```
secadm> set realm=realm-name
secadm{realm-name}> su
System Administrator Login Required
Login: root
Password:
secadm{root@realm-name}#
```

a. 如果您只需要一個領域使用者，您可以使用 「nobody」這個使用者名稱來避免設定插槽檔案。(請參考第 55 頁的 「插槽檔案」以取得更多的資訊。)

```
secadm{root@realm-name}# create user=nobody
Initial password:
Confirm password:
User nobody created successfully.
```

在網站伺服器啓動驗證時，您必需使用這個密碼。這是 *user@realm-name* 密碼。

注意 – 您必需牢記所輸入的密碼。有了這個密碼，您才可以存取金鑰。沒有任何方法可以擷取失去的密碼。

5. 離開 secadm。

```
secadm> exit
```

啓動 iPlanet 網站伺服器概述

您必需完成下列的程序以啓動 iPlanet 網站伺服器，下面兩章會有更詳盡的說明。

1. 安裝 iPlanet 網站伺服器
2. 新增信任資料庫。
3. 要求認證。
4. 安裝認證。
5. 設定 iPlanet 網站伺服器組態。

注意 – 這些程序必需依下列指示順序完成。否則會導致不正確的組態設定。

- 如果您使用 iPlanet 網站伺服器 4.1，請參閱第 4 章。
- 如果您使用 iPlanet 網站伺服器 6.0，請參閱第 5 章。

第 4 章

安裝與設定 iPlanet 網站伺服器 4.1 組態

本章說明如何安裝及設定 iPlanet 網站伺服器 4.1 組態

本章包含了下列幾個部份

- 第 19 頁的「安裝 iPlanet 網站伺服器 4.1」
- 第 26 頁的「設定 iPlanet 網站伺服器 4.1 組態」

安裝 iPlanet 網站伺服器 4.1

下列幾個部份說明如何安裝及設定 iPlanet 4.1 網站伺服器組態。這些程序必需依指示順序完成。請參考 iPlanet 網站伺服器文件集以取得使用 iPlanet 網站伺服器的相關資訊。

▼ 安裝 iPlanet 網站伺服器 4.1

1. **安裝 iPlanet 網站伺服器 4.1 軟體。**

   您可以在下列的網址中找到網站伺服器軟體：

   `http://www.iplanet.com`

2. **安裝網站伺服器。**

   說明包含一個範例，您也可以決定爲網站伺服器設定不同的組態。伺服器的預設路徑名稱爲：`/usr/netscape/server4`

   在 iPlanet 網站伺服器安裝過程中接受預設路徑。本書參照這些預設路徑。如果您決定安裝在不同的位置，請留意您安裝在什麼路徑下。

3. **執行安裝程式。**

4. **回答在安裝指令碼中的提示。**

   除了依照提示操作外，您也可以接受預設值，輕鬆完成設定。

   a. **輸入** `yes` **以同意接受授權條款。**

   b. **輸入完整的** *hostname.domain* **。**

   c. **輸入兩次 iWS 管理伺服器密碼。**

   d. **出現提示時按下 Return。**

▼ 新增信任資料庫

1. **啟動管理伺服器。**

   - 要啓動 iPlanet 4.1 網站伺服器，請使用下列的指令（而非如安裝程式之要求，執行 `startconsole`）：

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

   回應訊息提供網址讓您連結以管理伺服器。

2. **開啟網頁瀏覽器並輸入下列文字以啟動 iPlanet 管理伺服器：**

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

   接著跳出式視窗會要求輸入使用者帳號及密碼。輸入您執行安裝程式時選擇的 iWS 管理伺服器使用者名稱及密碼。

注意 – 如果您在安裝 iPlanet 網站伺服器的過程中使用預設值，請在使用者帳號中輸入 `admin`，或 iWS 管理伺服器的使用者名稱。

---

3. **按一下「OK」。**

4. 為網站伺服器例項新增信任資料庫。

您也許想在一個以上的網站伺服器例項裡啓用安全功能。請在所有的網站伺服器例項上重複這些程序。

注意 – 如果您同時想要在管理伺服器上執行 SSL，設定信任資料庫的程序是類似的。請參考 iPlanet 相關文件以取得更多的資訊。

---

a. 在管理伺服器上按一下「Servers（伺服器）」標籤。

b. 選擇伺服器並按一下「Manage（管理）」按鈕。

c. 按一下本頁頂端的「Security（安全）」，並選擇「Create Database（建立資料庫）」選項。

d. 在兩個對話方塊中輸入密碼（網站伺服器信任資料庫）並按一下「OK」。

密碼設定最少八碼。當 iPlanet 網站伺服器在安全模式中執行時，這個密碼將用於啓動內部編碼模組。

5. 執行下列的指令碼以啟動 Sun Crypto Accelerator 1000 介面卡：

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

這個指令碼會提示您選擇一個網站伺服器。它會爲 iPlanet 網站伺服器或 Apache 網站伺服器安裝 Sun Crypto Accelerator 1000 編碼模組。指令碼皆下來會更新組態檔以啓動 Sun Crypto Accelerator 1000 介面卡。

6. 要使用 SSL，請輸入 `1` 來設定 iPlanet 網站伺服器組態，並按一下 Enter。

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

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit): 1
```

7. **當出現提示時，請輸入網站伺服器 root 目錄路徑並按一下 Enter。**

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

8. **如果要繼續程序，請在出現提示時輸入 y 並按一下 Enter。**

```
This script will update your iPlanet 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

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


<Press ENTER to continue>
```

9. **輸入 0 退出。**

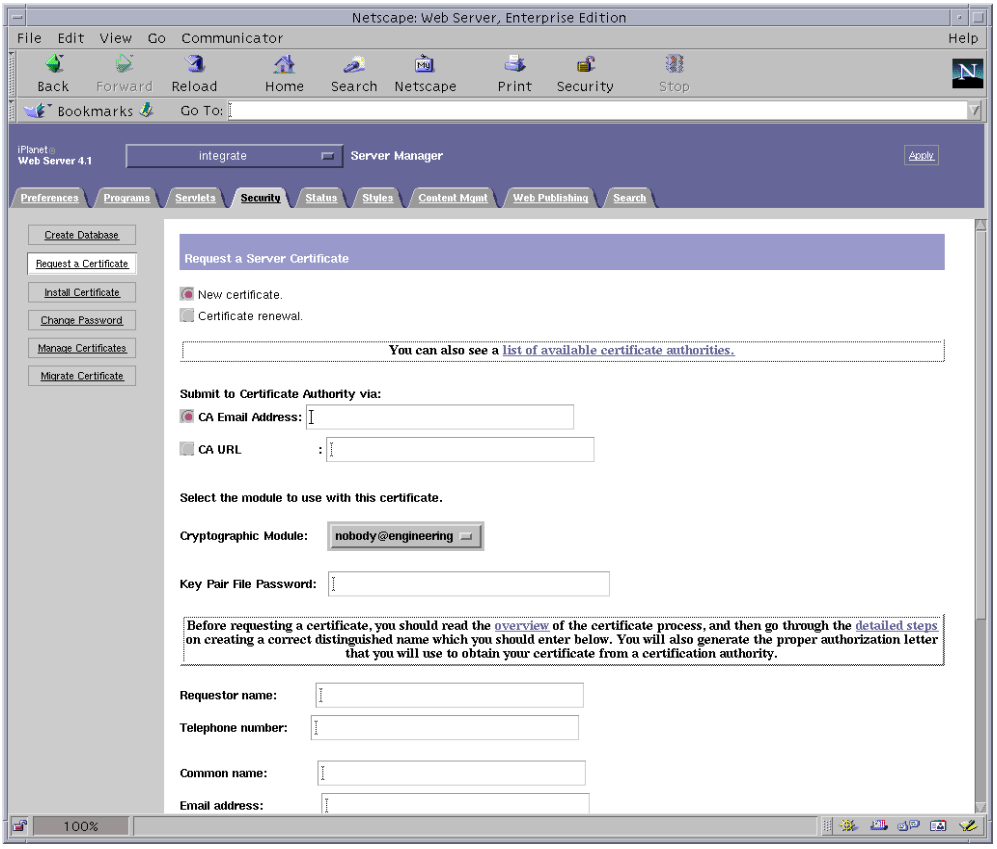
▼ 產生伺服器憑證

1. **輸入下列指令以重新啟動管理伺服器：**

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

2. **要求伺服器憑證，請按一下本頁頂端的「Security（安全）」標籤。**
   顯示新增信任資料庫的視窗。

3. **選擇本頁左側的要求憑證連結。**



4. **使用下列的資訊回答表格問題，以產生憑證要求：**

   a. **選擇「New Certificate （新憑證）」**

      如果您可以直接發佈您的憑證要求到有網路能力的憑證授權機構或註冊機構，請選擇 CA URL 選項。否則請選擇 CA Email Address，並選擇一個您希望接收憑證要求的郵件位址。

   b. **選擇要使用的「Cryptographic Module （編碼模組）」。**

      每個領域都在本下拉式功能表中有代表項目。確定選擇了正確的領域。要使用 Sun Crypto Accelerator 1000，您必需在 *user@realm-name* 表格中選擇某個模組。

   c. **在「Key Pair File Password （金鑰成對檔案密碼）」對話方塊中，為將擁有金鑰的 *user@realm-name* 設定密碼。**

d. 提供下列項目正確的資訊：

- Requestor Name（要求者名稱）：要求者連絡資訊
- Telephone Number（電話號碼）：要求者連絡資訊
- Common Name（通用名稱）：在參觀者的瀏覽器裡輸入的網站網域 *hostname.domain*
- Email Address（電子郵件地址）：要求者連絡資訊
- Organization（組織）：在憑證中代表組織加以聲明的數值
- Organizational Unit（組織單元）：（選用）在憑證中代表組織單位加以聲明的數值
- Locality（所在地）：（選用）在憑證中加以聲明的城市、郡或國家。
- State（州）：（選用）在本欄中填入完整的州名
- Country（國家）：代表國家的雙字母 ISO 碼，在憑證中會加以聲明，必填欄位

e. 輸入完成後，按一下「OK」按鈕來加以提交。

5. 透過憑證授權機構產生憑證。

- 如果您選擇發佈憑證要求至 CA URL，則憑證要求會在這裡自動發佈。
- 如果您選擇「CA Email Address（CA 電子郵件）」，請將寄送到您的信箱中的憑證要求連同檔頭複製一份，並將其送交憑證授權機構。

6. 在憑證產生後，請連同標頭一併複製貼到剪貼簿。

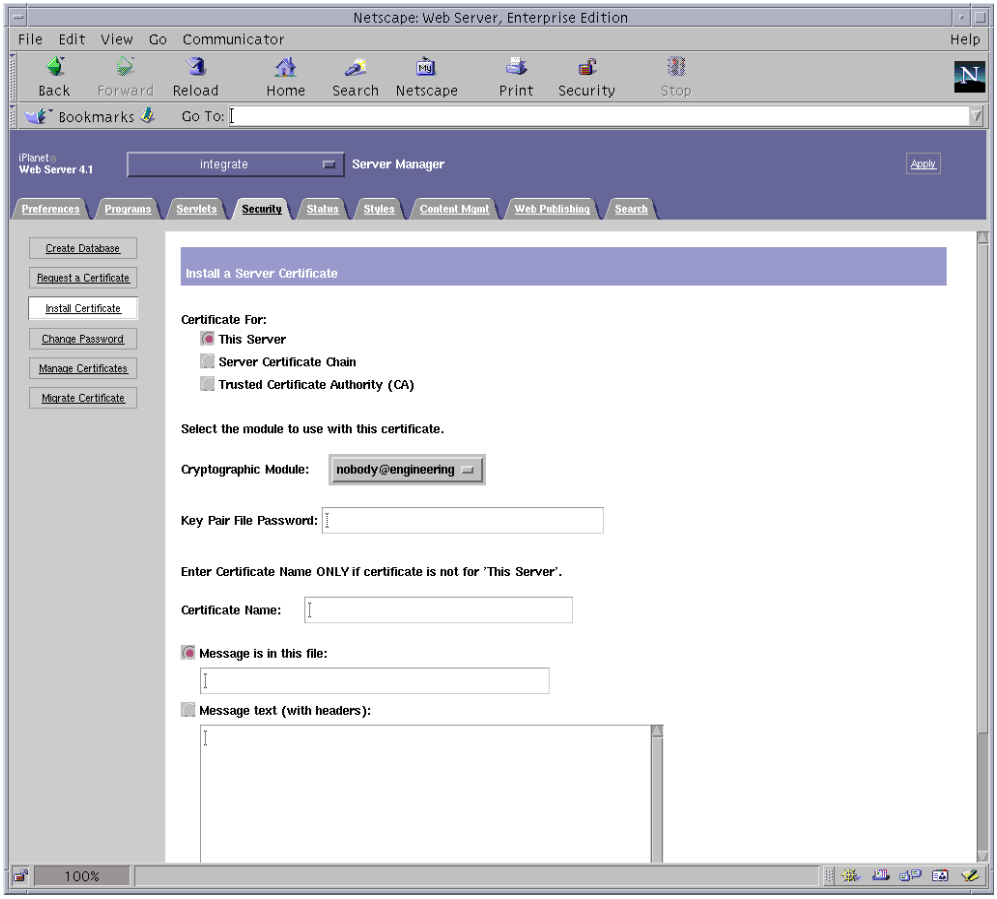
請留意憑證不同於憑證要求，且通常是以文字模式顯示。

▼ 安裝伺服器憑證

1. 請選擇在本頁面左側的安裝憑證連結。

一旦要求被憑證授權機構所接受且通過，您必需將它安裝在 iPlanet 網站伺服器上。

2. **請選擇「Security」標籤，然後在左側的窗格中選擇安裝憑證選項。**



3. **填妥表格以進行安裝憑證：**
   - Certificate For：本伺服器
   - Cryptographic Module：選擇適當的 *user@realm-name* 名稱。
   - Key Pair File Password：提供擁有稍早產生之金鑰的 *user@realm-name* 的密碼。
   - Certificate Name：在大多數的情況下，您可以將本欄留白。如果您選擇提供一個名稱，當在 SSL 支援下執行時，它將會變更網站伺服器用來存取憑證及金鑰的名稱。
4. **請選擇訊息文字 （含標頭）並將您稍早所複製的憑證貼上。**
5. **按一下在本頁下方的「OK」按鈕，將您從憑證授權機構上所複製的憑證貼到「Message （訊息）」方塊內。**

   系統會顯示一些關於憑證的基本資料。

6. **如果所有資料都正確，請按一下「Add Server Certificate（新增伺服器憑證）」按鈕。**

螢幕上的訊息會要求您重新啓動伺服器。這不是必要的，因爲網站伺服器已經完全被關閉。網站伺服器要使用 SSL，您也會被通知要這麼設定組態。使用下列的程序來爲網站伺服器設定組態。

設定 iPlanet 網站伺服器 4.1 組態

現在網站伺服器及伺服器憑證已安裝完成，您必需爲網站伺服器的 SSL 設定組態。

▼ 設定 iPlanet 網站伺服器 4.1 組態

1. **從主要管理畫面中，選擇想要執行的網站伺服器實體，並按一下「Manage（管理）」按鈕。**

根據預設值，您應該會在頁面頂端的「Preference（偏好設定）」標籤上。如果沒有，請按一下該標籤。

2. **按一下靠近頁面頂端的「Preference（偏好設定）」標籤。選擇在本頁左側的「Encryption（加密） On/Off」連結。將加密設定為「On」。**

對話方塊中的通訊埠應該更新爲預設 SSL 通訊埠號碼 443。如果有需要時請變更通訊埠號碼。

3. **按一下「OK」按鈕。**

4. **按一下「Save（儲存）」按鈕以套用這些變更。**

網站伺服器目前被設定爲在安全模式下執行。

5. **輸入下列指令來編輯** `/usr/netscape/server4/https-`*hostname*`/config/magnus.conf` **檔：**

```
CERTDefaultNickname user@realm-name:Server-Cert
```

其中 *hostname* 即是網站伺服器的名稱。

根據預設值，您在步驟 2 及步驟 3 所產生的憑證會被命名爲 `Server-Cert`。如果您的憑證有不同的名稱，請用憑證名稱來取代 `Server-Cert`。

6. **請選擇您想要管理的伺服器，然後按一下本頁右上角的「Apply（套用）」按鈕。**

這個動作會在管理伺服器上套用所有的變更。

7. 請按一下「Load Configuration Files（載入組態檔案）」按鈕來套用稍早在 `magnus.conf` 檔裡所做的變更。

當伺服器關閉時，如果按一下「Apply Change（套用變更）」按鈕，系統會顯示跳出式視窗並提示輸入密碼。這個視窗不可重設大小，且您有可能會在同意這些變更時發生問題。關於這個問題有兩個替代性解決方法：

- 按一下「Load Configuration Files（載入組態檔案）」按鈕。
- 先啓動網站伺服器，然後按一下「Apply Change（套用變更）」按鈕。

8. 在網站伺服器頁面裡，選擇在頁面左側的「On/Off」連結。輸入伺服器密碼並按一下「OK」按鈕。

接下來系統會提示您輸入一個或多個密碼。在內部模組提示下，請提供網站伺服器信任資料庫密碼。

在 *user@realm-name* 模組提示下，請輸入當您在 *realm-name* 使用 `secadm` 建立 *user* 時設定的密碼。

9. 請開啟瀏覽器連結至下列網址，以確認剛啟用的 SSL 網站伺服器：

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

請留意預設的 *server_port* 爲 443。

第 5 章

安裝與設定 iPlanet 網站伺服器 6.0 組態

本章說明如何啓動 Sun Crypto Accelerator 1000 介面卡以搭配使用 iPlanet 6.0 網站伺服器。

本章包含了下列幾個部份

- 第 29 頁的「安裝 iPlanet 網站伺服器 6.0」
- 第 36 頁的「設定 iPlanet 網站伺服器 6.0 組態設定」

安裝 iPlanet 網站伺服器 6.0

下列幾個部份說明如何安裝及設定 iPlanet 網站伺服器組態。這些程序必需依指示順序完成。請參考 iPlanet 網站伺服器文件集以取得使用 iPlanet 網站伺服器的相關資訊。

▼ 安裝 iPlanet 網站伺服器 6.0

1. **安裝 iPlanet 網站伺服器 6.0 軟體。**

   您可以在下列的網址中找到網站伺服器軟體：

   `http://www.iplanet.com`

2. **安裝網站伺服器。**

   說明包含一個範例，您也可以決定爲網站伺服器設定不同的組態。伺服器的預設路徑名稱爲：`/usr/iplanet/servers`

   在 iPlanet 網站伺服器安裝過程中接受預設路徑。本書參照這些預設路徑。如果您決定安裝在不同的位置，請留意您安裝在什麼路徑下。

3. **執行安裝程式。**

4. **回答在安裝指令碼中的提示。**

   除了依照提示操作外，您也可以接受預設值，輕鬆完成設定。

   a. **輸入** `yes` **以同意接受授權條款。**

   b. **輸入完整的** *hostname.domain* **。**

   c. **輸入兩次 iWS 管理伺服器密碼。**

   d. **出現提示時按下 Return。**

▼ 新增信任資料庫

1. **啟動管理伺服器。**

   要啓動 iPlanet 網站伺服器，請使用下列的指令（取代執行 `startconsole` 來做爲 `setup` 要求）：

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

   回應訊息提供網址讓您連結以管理伺服器。

2. **開啟網頁瀏覽器並輸入下列文字以啟動 iPlanet 管理伺服器：**

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

   接著跳出式視窗會要求輸入使用者帳號及密碼。輸入您執行安裝程式時選擇的 iWS 管理伺服器使用者名稱及密碼。

注意 – 如果您在安裝 iPlanet 網站伺服器的過程中使用預設值，請在使用者帳號中輸入 `admin`，或 iWS 管理伺服器的使用者名稱。

---

3. **按一下「OK」。**

4. 為網站伺服器例項新增信任資料庫。

您也許想在一個以上的網站伺服器例項裡啓用安全功能。請在所有的網站伺服器例項上重複這些程序。

注意 – 如果您同時想要在管理伺服器上執行 SSL，設定信任資料庫的程序是類似的。請參考 iPlanet 相關文件以取得更多的資訊。

---

a. 在管理伺服器上按一下「Servers（伺服器）」標籤。

b. 選擇伺服器並按一下「Manage（管理）」按鈕。

c. 按一下本頁頂端的「Security（安全）」，並選擇「Create Database（建立資料庫）」選項。

d. 在兩個對話方塊中輸入密碼（網站伺服器信任資料庫）並按一下「OK」。

密碼設定最少八碼。當 iPlanet 網站伺服器在安全模式中執行時，這個密碼將用於啓動內部編碼模組。

5. 執行下列的指令碼以啟動 Sun Crypto Accelerator 1000 介面卡：

```
# /opt/SUNWconn/crypto/bin/sslconfig
```

這個指令碼提示您選擇一個網站伺服器。它爲 iPlanet 網站伺服器或 Apache 網站伺服器安裝 Sun Crypto Accelerator 1000 編碼模組。指令碼皆下來會更新組態檔以啓動 Sun Crypto Accelerator 1000 介面卡。

6. 要使用 SSL，請輸入 1 來設定 iPlanet 網站伺服器組態，並按一下 Enter。

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

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys
Your selection (0 to quit): 1
```

7. **當出現提示時，請輸入網站伺服器 root 目錄路徑並按一下 Enter。**

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

8. **如果要繼續程序，請在出現提示時輸入 y 並按一下 Enter。**

```
This script will update your iPlanet 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

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


<Press ENTER to continue>
```

9. **輸入 0 退出。**

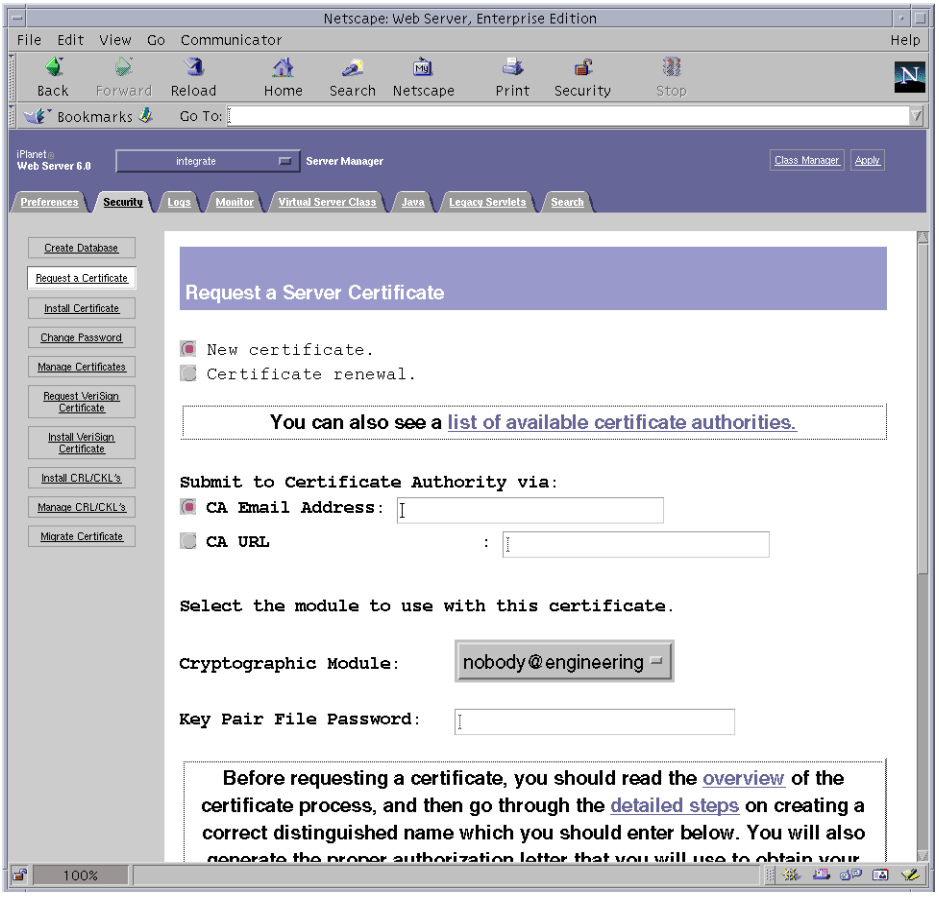
▼ 產生伺服器憑證

1. **輸入下列指令以重新啟動管理伺服器：**

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

2. **要求伺服器憑證，請按一下本頁頂端的「Security（安全）」標籤。**
   顯示新增信任資料庫的視窗。

3. **選擇本頁左側的要求憑證連結。**



4. **使用下列的資訊回答表格問題，以產生憑證要求：**

   a. **選擇「New Certificate（新憑證）」**

   如果您可以直接發佈您的憑證要求到有網路能力的憑證授權機構或註冊機構，請選擇 CA URL 選項。否則請選擇「CA Email Address（CA 電子郵件地址）」，並選擇一個您希望接收憑證要求的郵件位址。

   b. **選擇要使用的「Cryptographic Module（編碼模組）」。**

   每個領域都在本下拉式功能表中有代表項目。確定選擇了正確的領域。要使用 Sun Crypto Accelerator 1000，您必需在 *user@realm-name* 表格裡選擇一個模組。

   c. **在「Key Pair File Password（金鑰成對檔案密碼）」對話方塊中，為將擁有金鑰的 *user@realm-name* 設定密碼。**

d. 提供下列項目正確的資訊：

- Requestor Name：要求者連絡資訊
- Telephone Number：要求者連絡資訊
- Common Name：在參觀者的瀏覽器裡輸入的網站網域 *hostname.domain*
- Email Address：要求者連絡資訊
- Organization：在憑證中代表組織加以聲明的數值
- Organizational Unit：（選用）在憑證中代表組織單位加以聲明的數值
- Locality：（選用）在憑證中加以聲明的城市、郡或國家
- State：（選用）在本欄中填入完整的州名
- Country：用兩個字母代表國家的 ISO 碼，在憑證中聲明且是必填的欄位

e. 一旦您輸入完成，按一下「OK」按鈕來加以提交。

5. 透過憑證授權機構產生憑證。

- 如果您選擇發佈憑證要求至 CA URL，則憑證要求會在這裡自動發佈。
- 如果您選擇「CA Email Address（CA 電子郵件地址）」，請將寄送到您的信箱中的認證要求連同標頭文字複製一份，並將其送交認證授權。

6. 在憑證產生後，請連同標頭一併複製貼到剪貼簿。

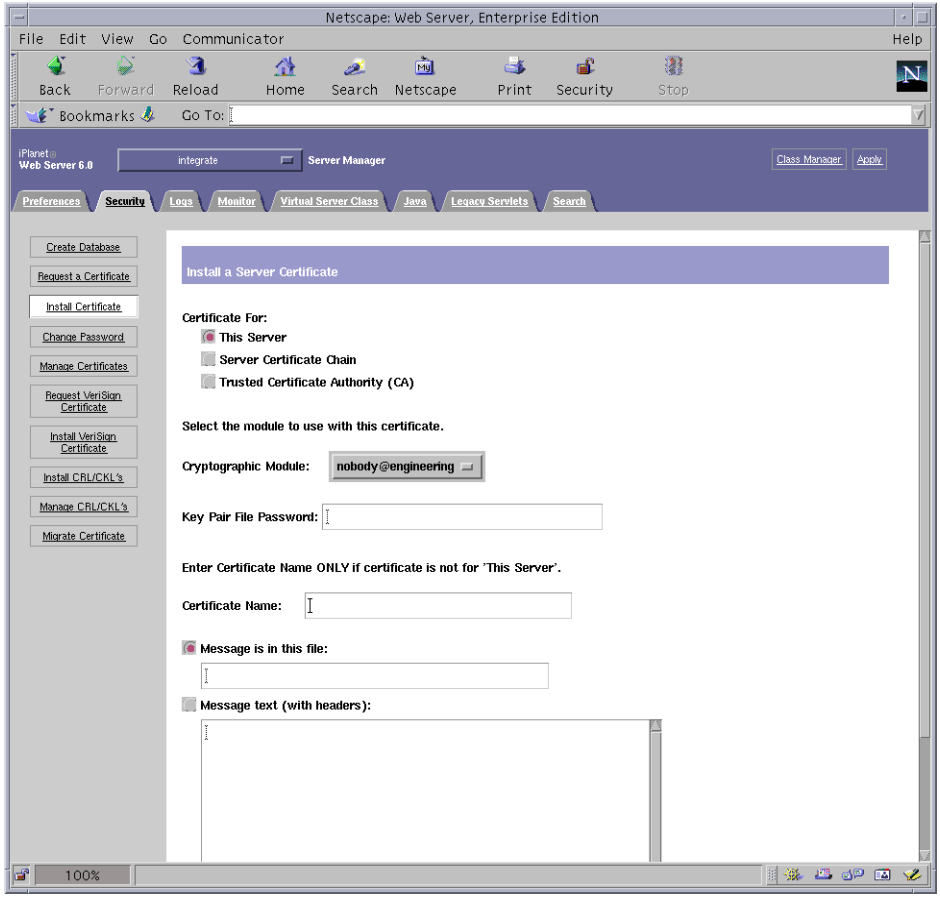
請留意憑證不同於憑證要求，且通常是以文字模式顯示。

▼ 安裝伺服器憑證

1. **請選擇在本頁面左側的安裝憑證連結。**

   一旦要求被憑證授權機構所接受且通過，您必需將它安裝在 iPlanet 網站伺服器上。

2. **請選擇 「Security」標籤，然後在左側的窗格中選擇安裝憑證選項。**



3. **填妥表格以進行安裝憑證：**

   - Certificate For （憑證標的）：本伺服器
   - Cryptographic Module （加密模組）：選擇適當的 *user@realm-name*。
   - Key Pair File Password （金鑰配對檔案密碼）：提供擁有稍早產生之金鑰的 *user@realm-name* 的密碼。
   - Certificate Name （憑證名稱）：在大多數的情況下，您可以將本欄留白。如果您選擇提供一個名稱，當在 SSL 支援下執行時，它將會變更網站伺服器用來存取憑證及金鑰的名稱。

4. **請選擇訊息文字（含標頭）並將稍早所複製的憑證貼上。**

5. **按一下在本頁下方的「OK」按鈕，將您從憑證授權機構上所複製的憑證貼到「Message（訊息）」方塊內。**

   系統會顯示部份憑證的相關基本資料。

6. **如果所有資料都正確，請按一下「Add Server Certificate（新增伺服器憑證）」按鈕。**

   螢幕上的訊息會要求您重新啓動伺服器。這不是必要的，因爲網站伺服器已經完全被關閉。網站伺服器要使用 SSL，您也會被通知要這麼設定組態。使用下列的程序來爲網站伺服器設定組態。

設定 iPlanet 網站伺服器 6.0 組態

現在網站伺服器及伺服器憑證已安裝完成，您必需爲網站伺服器的 SSL 設定組態。

▼ 設定 iPlanet 網站伺服器 6.0 組態

1. **按一下靠近頁面頂端的「Preference（偏好設定）」標籤。選擇在左側窗格的「Edit Listen Sockets（編輯聆聽插槽）」選項。**

   主要窗格會列出該網站伺服器例項的所有聆聽插槽。

   a. **變更下列欄位：**

      - Port（連接埠）：設定您將在啓動 SSL 的網站伺服器上的通訊埠（通常是通訊埠 443）。
      - Security（安全）：設定爲「On」。

   b. **按下「OK」按鈕來套用這些變更。**

      在「Edit Listen Sockets（編輯聆聽插槽）」頁面中的安全性欄位，現在應該有一個「Attributes（屬性）」連結。

2. **按一下「Attributes（屬性）」連結。**

3. **輸入** *user@realm-name* **密碼以驗證系統上的** *user@realm-name***。**

4. **從跳出式視窗中選擇 SSL 設定。**

   您可以選擇「Cipher Default」設定、「SSL2」、或「SSL3/TLS」。「Default」選項不會顯示預設的設定。另外兩個選項需要您選擇您想啓動的演算法。

5. **接下來選擇 *user@realm-name* 認證，請輸入 `:Server-Cert` （或您所選擇不同的名稱）。**

   只有適當的 *user@realm-name* 所擁有的金鑰會顯示在「Certificate Name（憑證名稱）」欄位中。

6. **當您已選擇了認證，並確認所有的安全性設定，請按下「OK」按鈕。**

7. **按一下右上角的「Apply（套用）」連結，在您啟動伺服器前套用這些變更。**

8. **按一下「Load Configuration Files（載入組態檔案）」連結以套用這些變更。**

   您會被導向到另一個頁面，讓您啓動網站伺服器例項。

   當伺服器關閉時，如果按一下「Apply Changes（套用變更）」按鈕，系統會顯示跳出式視窗並提示輸入密碼。這個視窗不可重設大小，且您有可能會在同意這些變更時發生問題。

   關於上述的問題有兩個替代性解決方法：

   - 按一下「Load Configuration Files（載入組態檔案）」按鈕。
   - 先啓動網站伺服器，然後按一下「Apply Changes（套用變更）」按鈕。

9. **在要求密碼的對話框內輸入密碼以啟動伺服器。**

   接下來系統會提示您輸入一個或多個密碼。在內部模組提示下，請提供網站伺服器信任資料庫密碼。

   在 *user@realm-name* 模組提示下，請輸入當您在 *realm-name* 使用 `secadm` 建立 *user* 時設定的密碼。

10. **請開啟瀏覽器連結至下列網址，以確認剛啟用的 SSL 網站伺服器：**

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

    請留意預設的 *server_port* 爲 443。

第 6 章

啓用 Apache 網站伺服器

本章說明了如何在 Apache 網站伺服器上啓用 Sun Crypto Accelerator 1000 介面卡。

本章包含了下列章節

- 第 39 頁的「啓用 Apache 網站伺服器」
- 第 42 頁的「建立憑證」

啓用 Apache 網站伺服器

Solaris 8 7/01 作業環境內附了 Apache 網站伺服器 1.3.12。下面的說明是專爲該版本的 Apache 網站伺服器而提供。請參閱 Apache 網站伺服器文件以取得更多與 Apache 網站伺服器使用相關的資訊。

▼ 啓用 Apache 網站伺服器

1. **建立** `httpd` **組態檔案。**

   對於 Solaris 系統，`httpd.conf-example` 檔案通常位於 `/etc/apache`。您可以使用本檔案做爲範本，依照下列方式加以複製：

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

   以 `ServerName` 置換伺服器名稱。

2. **啟動** `sslconfig`**。**

   ```
   # /opt/SUNWconn/crypto/bin/sslconfig
   ```

3. **選擇 2 以設定 Apache 網站伺服器組態來使用 SSL：**

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

Please select the type of web server you wish to configure
to use the Sun Crypto Accelerator:
------------------------------------------------------------
1. Configure iPlanet Web Server for SSL
2. Configure Apache for SSL
3. Work with iPlanet and Apache keys

Your selection (0 to quit):
```

4. **提供 Apache 二進位程式所在的目錄。**

   在 Solaris 系統上，該目錄通常是 /usr/apache。

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

5. **請提供 Apache 的組態檔案位置。**

   在 Solaris 系統上，該目錄通常是 /etc/apache。

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

6. **為系統建立 RSA 金鑰組。**

   如果您選擇不要這樣做，您必需在稍後回來使用 sslconfig 產生金鑰。

```
Do you wish to create a new RSA keypair and certificate request?
[Y/N]:
```

   如果您回答 No，請跳到第 42 頁的「建立憑證」。

7. **提供儲存金鑰的目錄。**

   如果目錄不存在，則會建立該目錄。

```
Where would you like the keys stored? [/etc/apache/keys]:
/etc/apache/keys
```

8. **選擇金鑰資料的基礎名稱。**

   該名稱會被附加上不同的字尾以識別金鑰檔案、憑證要求檔案與憑證檔案。

```
Please choose a base name for the key and request file:
```

9. **提供長度介於 512 到 2048 位元間的金鑰長度。**

   對於多數網站伺服器應用程式，1024 位元夠強了，但您可以選擇使用更強的金鑰。

```
What size would you like the RSA key to be [1024]? 1024
Generating RSA private key, 1024 bit long modulus
..........++++++
......++++++
e is 65537 (0x10001)
```

10. **建立 PEM 通行碼。**

    本通行碼是用來保護金鑰資料。請確定選擇夠強的通行碼，但記得牢記該通行碼。如果忘記密碼，您將無法存取金鑰。

```
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
```

警告 – 您必需記得輸入的通行碼。沒有通行碼，您將無法存取金鑰。沒有任何方法可以擷取失去的通行碼。

建立憑證

下列程序說明了如何建立在 Apache 網站伺服器使用 Sun Crypto Accelerator 1000 介面卡所需的憑證。

▼ 建立憑證

1. **使用您剛建立的金鑰建立憑證要求。**

   您必需先輸入密碼才能存取金鑰。然後在下列欄位提供合適資訊：

   - Country Name（國家名稱）：兩個字元構成的 ISO 代碼，憑證上會註明代碼，這是必要欄位
   - State or Province Name（州或省名稱）：（選用）在本欄位中輸入完整的州或省名稱（或者輸入「.」並按下 Return）
   - Locality（所在地）：（選用）城市、郡、所在地或國家，如果提供該項資訊，也會註明在憑證上
   - Organizational Name（機構名稱）：代表機構的數值，也會註明在憑證上
   - Organizational Unit Name（機構單位名稱）：（選用）代表機構單位的數值，也會註明在憑證上
   - SSL Server Name（SSL 伺服器名稱）：造訪者的瀏覽器中必需輸入的網站網域
   - Email Address（電子郵件地址）：要求者的聯絡資訊

```
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. 依照說明，修改 `/etc/apache/httpd.conf` **檔案。**

系統會顯示與金鑰及憑證相關的資訊。您也將學到如何修改 `/etc/apache/httpd.conf` 檔案以配合 Sun Crypto Accelerator 1000 使用。

```
The keyfile is stored in /etc/apache/keys/ap6-key.pem.
The certificate request is in /etc/apache/keys/ap6-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.1.3.12

In the AddModule section, add the following:

AddModule mod_ssl.c
```

3. **如果您選擇不要設立** VirtualHost**，您必需在** httpd.conf **中、** SSLPassPhraseDialog **指令行之上加入** SSLEngine、SSLCertificateFile **與** SSLCertificateKeyFile **指令行。**

```
You may need a virtual host directive similar to
what is shown below:

<VirtualHost _default_:443>
        SSLEngine on
        SSLCertificateFile /etc/apache/keys/ap6-cert.pem
        SSLCertificateKeyFile /etc/apache/keys/ap6-key.pem
</VirtualHost>

You must add the following line after all of your VirtualHost
definitions:

SSLPassPhraseDialog exec:/opt/SUNWconn/crypto/bin/sslpassword

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>
```

如果您對步驟 6 中的問題回答 no，您也將獲得稍後如何產生金鑰資料的進一步資訊。

```
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 iPlanet and Apache keys" from the
sslconfig main menu.
```

4. **完成** sslconfig **的操作後，選擇** 0**。**

5. **由** /etc/apache/keys/*base_name*-certreq.pem **（base_name 應該在步驟 8 中設定）複製您的憑證及檔頭，並交給憑證授權機構。**

6. **憑證產生後，請建立憑證檔案** `/etc/apache/keys/`*base_name*`-cert.pem` **並將您自己的憑證貼上到其中。**

7. **啟動 Apache 網站伺服器。**

   這會假定 Apache 二進位程式碼目錄是 `/usr/apache/bin`。如果這不是您的二進位程式碼目錄，請輸入正確目錄。

```
# /usr/apache/bin/apachectl start
```

8. **提示時，輸入 PEM 通行碼。**

9. **要檢查網站伺服器的 SSL 功能是否啟用，請使用瀏覽器造訪下列 URL：**

   `https://`*server_name*`:`*server_port*`/`

   注意預設的 *server_port* 是 443。

第 7 章

診斷與疑難排解

本章說明了 Sun Crypto Accelerator 1000 軟體的診斷測試與疑難排解。它包括了下列段落：

- 第 47 頁的「SunVTS 診斷軟體」
- 第 51 頁的「對 Sun Crypto Accelerator 1000 進行疑難排解」

SunVTS 診斷軟體

Sun Crypto Accelerator 1000 CD 的 `SUNWdcav` 套件中提供的 SunVTS 測試：`dcatest` 可以與 Solaris Supplement CD 上的 `SUNWvts` 與 `SUNWvtsx` 套件提供的核心 SunVTS 測試控制與使用者介面共同運作，以提供 Sun Crypto Accelerator 1000 介面卡的診斷功能。

請參閱 SunVTS 的文件，以取得執行與監控這些診斷測試的相關資訊。您可以在 Sun Hardware AnswerBook 上找到這些文件的 Solaris 版本；Sun Hardware AnswerBook 會依照您系統使用的 Solaris 版本，在 Solaris Supplement CD 上提供。

注意 – 僅有在安裝 Solaris Supplement CD 上的 SunVTS 套件後，您才能使用 SunVTS。

▼ 執行 dcatest

1. **以超級使用者 (superuser) 的身份，啟動 SunVTS。**

```
# /opt/SUNWvts/bin/sunvts
```

   請參閱 *SunVTS 使用者指南* 以取得 SunVTS 啓動上的詳細說明。

   下列說明假定您使用 CDE 使用者介面啓動 SunVTS。

2. **在 SunVTS Diagnostic 主視窗中，設定 System Map （系統映射圖）為 Logical （邏輯）模式。**

3. **清除所有核取方塊以禁用所有測試。**

4. **選擇 「OtherDevices （其他裝置）」旁的核取方塊，然後選擇 「OtherDevices （其他裝置）」的加號方塊，以顯示 「OtherDevices （其他裝置）」群組中的所有測試。**

5. **清除 OtherDevices 群組中、名稱不是 `dcatest` 的核取方塊。**

   - 如果 `dcatest` 被顯示出來，請跳到步驟 6。
   - 如果 `dcatest` 沒有被顯示，請由「Commands（命令）」下拉式功能表中選擇「Reprobe system（重新偵測系統）」，重新偵測系統。

   請參閱 SunVTS 文件以瞭解詳細的程序。偵測完成、顯示 `dcatest` 後，請繼續進行步驟 6。

6. **按一下 `dcatest` 例項之一，然後用右鍵按一下並拖拉，以顯示 「Test Parameter Options （測試參數選項）」。**

   這些選項僅適用於 `dcatest`；第 49 頁的「dcatest 測試參數選項」中會有詳細說明。

7. **完成所有選擇後，按一下 「Within Instance Apply （在例項內套用）」以變更選定的 `dcatest` 例項，或按一下 「Across All Instance Apply （跨越所有例項套用）」以變更 `dcatest` 所有選取的例項。**

   本動作會移除跳出式視窗，並將您送回 Sun Diagnostic 主視窗。

8. **按一下 `dcatest` 例項之一，然後右鍵按一下並拖拉以顯示 「Test Execution Options」。**

   另外一個顯示「Test Execution Options（測試執行選項）」的方法，是按一下「Options（選項）」跳出式視窗，然後按一下「Test Executions（測試執行）」。這些選項是通用 SunVTS 控制項，它們會影響所有測試。請參考 SunVTS 文件以獲得更多資訊。

9. **作完所有選擇後，請按一下 「Apply （套用）」以移除跳出式視窗，並回到 Sun Diagnostic 主視窗。**

10. **按一下 「Start （開始）」執行所有選定測試。**

11. **按一下 「Stop （停止）」停止所有測試。**

dcatest 測試參數選項

表 7-1 顯示了 dcatest 的測試參數選項，詳細說明在第 48 頁的「執行 dcatest」的步驟 6 中。被測試的機板類型，會顯示在跳出式視窗的「Configuration（組態）」區域中。

表 7-1 dcatest 測試參數選項

選項標籤	描述
Test_Sel	十進位數值，用於指定要執行的子測試組合。數值 0 會選擇所有測試。每個子測試都會有一個以 2 爲底的次方數字。您可以輸入指定給子測試的數字以選擇個別子測試。要選擇多個子測試，請輸入指定給所需子測試的數字的和。預設設定是 0。
Info_Print	啓用或禁用資訊（INFO 類型）訊息的列印。預設設定是「啓用」。

表 7-2 說明了各項 dcatest 子測試。

表 7-2 dcatest 子測試

測試名稱	號碼	描述
ALL	0	執行所有測試。
SHOWINFO	1	列印 INFO 類型資訊，在測試資訊下顯示供應器與裝置。
3DES	2	測試 3DES 大量加密。
RSA	4	測試 RSA 公開與私人金鑰。
DSA	32	測試 DSA 簽章驗證。
Random	64	測試亂數與虛擬亂數的產生。印出 INFO 類型訊息，顯示產生的數字。

子測試產生的訊息會被顯示在 SunVTS Diagnostic 主視窗的「Test Message（測試訊息）」區域。子測試產生的訊息會以類別分組：

- INFO 類型訊息：如果 info_Print 在「Test Parameters（測試參數）」跳出視窗中被啓用，則該類訊息會被列印到「Test Message（測試訊息）」區域，並記錄在「Information Log（資訊記錄）」中。INFO 類型訊息提供了非關鍵資訊。
- FATAL 錯誤類型訊息：永遠會被顯示，並會記錄在「Test Error Log（測試錯誤記錄）」與「Information Log（資訊記錄）」中。
- VERBOSE 類型訊息：只有在「Test Execution（測試執行）」跳出式視窗中啓用「VERBOSE（詳細）」選項時，才會顯示子測試的追蹤進度。VERBOSE 訊息不會被保留在任何記錄中。

  要選擇僅顯示與 dcatest FATAL 錯誤訊息的安靜模式，請禁用 VERBOSE 與 Info_Print 選項。

dcatest 命令列語法

如果您選擇由命令列而非 CDE 環境執行 dcatest，則所有的引數必須在命令列字串中指定。

在 32 位元模式中，dcatest 的路徑是 /opt/SUNWvts/bin/。在 64 位元模式中，dcatest 的路徑是 /opt/SUNWvts/bin/sparcv9/。

下面的範例顯示了 32 位元模式的語法：

```
/opt/SUNWvts/bin/dcatest -f [Standard Command-Line Arguments]
[-o [dev=dcan][,testsel=n][,infodis]]
```

請參閱 *SunVTS Test Reference Manual* 以取得標準命令列引數的定義。由於 dcatest 是一個功能模式測試，您必須加入 -f。加入 -u 以顯示使用方式訊息、或加入 -v 以顯示 VERBOSE 訊息。上面以方括號括住的項目，代表選擇性輸入項。略過選項或會產生該選項的預設動作，如表 7-3 中所示。

表 7-3 dcatest 命令列語法

引數	描述
dev=dca*n*	指定要測試的裝置例項，例如 dca0 或 dca2。如果不加入此引數，預設值是 dca0。
testsel=*n*	指定要執行的子測試，n 可以是 0 到 127 的數字。如果不加入此引數，預設值是 0。
infodis	如果要禁用 INFO 類型的訊息，請加入本引數。如果不加入本引數，預設爲 Info_Print Enabled。

對 Sun Crypto Accelerator 1000 進行疑難排解

要判斷 Sun Crypto Accelerator 1000 裝置是否列在系統中，請由 OpenBoot PROM (OBP) 提示，輸入 `show-devs` 以顯示裝置清單。您應該會看到幾行屬於 Sun Crypto Accelerator 1000 介面卡的裝置清單，範例如下：

```
ok show-devs
. . .
/pci@1f,0/pci@1/pci108e,5455@2
. . .
```

在上面的範例中，`pci108e,5455` 代表 Sun Crypto Accelerator 1000 介面卡的裝置路徑。介面卡上沒有韌體，因此沒有可用的 OBP 階層診斷。

Sun Crypto Accelerator 1000 不包含指示燈或顯示器，因而無法反應介面卡上的編碼活動。要判斷編碼工作要求是否真的是由介面卡處理，請使用 `kstat`(1M) 命令來顯示裝置使用情形：

```
# kstat -m dca -i 0 -n dca0

module: dca                             instance: 0
name:   dca0                        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
```

顯示 `kstat` 資訊以查看加密要求、也就是「jobs」是否有被傳送到 Sun Crypto Accelerator 1000 介面卡。「jobs」數值的逐漸變更，代表 Sun Crypto Accelerator 1000 介面卡正在加速傳送到其上的工作要求。如果編碼工作沒有被送到介面卡上，請依照網站伺服器的特定組態，檢查網站伺服器的組態。

您不一定總能判斷編碼要求是在何處被處理，視要求提出的時間子系統的負載，編碼要求可能會在不同位置進行。

不要嘗試解讀 `kstat`(1M) 送回的核心/驅動程式統計數值。驅動程式維持這些數值的目的，是爲便利進行現地支援。其意義和實際數值可能會隨時變更。

附錄 **A**

使用 iPlanet 網站伺服器管理 Sun Crypto Accelerator 1000 介面卡

本附錄提供了使用 iPlanet 網站伺服器管理 Sun Crypto Accelerator 1000 介面卡的安全功能摘要。

注意 – 要管理領域，您必需能夠存取電腦上的系統管理員帳號。

本附錄包含下列章節：

- 第 53 頁的「概念與詞彙」
- 第 61 頁的「設定與管理領域」
- 第 64 頁的「設定與管理使用者帳號」

概念與詞彙

對於透過 PKCS#11 介面與 Sun Crypto Accelerator 1000 通訊的應用程式如：iPlanet 網站伺服器，您必需建立領域及使用者。

Sun Crypto Accelerator 1000 內的使用者是加密金鑰資料的唯一擁有者。每個使用者都可以擁有多重金鑰。使用者可能會希望擁有多重金鑰以支援不同的組態，例如「production」與「development」金鑰（以反應使用者的不同機構）；或需要多重金鑰以便於建立高可用性 (HA) 組態。請注意「使用者」與「使用者帳號」指的是 Sun Crypto Accelerator 1000 使用者，而非傳統的 UNIX 使用者帳號。UNIX 使用者名稱與 Sun Crypto Accelerator 1000 使用者名稱間，並沒有固定對應。

領域是使用者與其金鑰資料間的邏輯分隔。領域提供了容納多重使用者的能力。使用領域分隔不同使用者的好處，是對於各個領域，都可以維持獨立的名稱空間。這可以讓您獨立管理領域內容。

一般的安裝，包含單一領域與單一使用者。舉例來說，該組態可能包括單一領域「webserver」與該領域的單一使用者「nobody」。這可以讓使用者「nobody」擁有並維護單一領域中的多個金鑰的存取控制權。

您將擁有建立額外領域的彈性，以便分隔使用者與金鑰資料。更複雜的組態可能包含多重領域、例如：「finance」、「legal」與「engineering」。每個領域都維持獨立的名稱空間。舉例來說，財務領域的使用者「webserv」、與工程領域的「webserv」是不同的使用者帳號。

您可以使用 `secadm` 管理工具來管理 Sun Crypto Accelerator 1000 領域與使用者。

領域、使用者與 iPlanet 網站伺服器

當 iPlanet 網站需要參照 Sun Crypto Accelerator 1000 管理的金鑰時，它會使用「標記名稱」來標明該金鑰是由硬體而非內部軟體資料庫管理。

Sun Crypto Accelerator 1000 使用「@」符號來結合使用者帳號與領域名稱，建立標記名稱。在上面的安裝範例中，我們建立了單一的領域「webserver」、以及單一的使用者「nobody」。iPlanet 網站伺服器會用來參照使用者「nobody」在「webserver」領域中擁有的金鑰的標記標籤是「nobody@webserver」。您必需使用使用者 nobody 的密碼（使用 `secadm` 建立使用者時設立的密碼）來要求憑證、安裝憑證、或驗證啓動 iPlanet 網站伺服器。

標記與插槽檔案

iPlanet 網站伺服器透過標記存取金鑰資料；這些標記也被稱爲插槽。插槽檔案是允許 Sun Crypto Accelerator 1000 管理員對特定應用程式選擇性僅呈現指定標記。

如果沒有插槽檔案存在，Sun Crypto Accelerator 1000 會呈送預設標記組給 iPlanet 網站伺服器。在此範例中會對每個領域呈送一個標記，標記名稱是 `nobody@`*`realm-name`*。

範例

系統上有三個領域：工程、財務與法律。下列標記會被呈現給 iPlanet 網站伺服器。

- nobody@engineering
- nobody@finance
- nobody@legal

然而，這些名稱要能夠使用，這些領域中都必需存在一個叫做「nobody」的使用者。

插槽檔案

要取代預設設定，系統上必需有插槽檔案。插槽檔案是包含一個或多個標記名稱的文字檔案，每個標記名稱一行。iPlanet 網站伺服器僅會呈現列在檔案中的標記。指定插槽檔案的方法如下（依序介紹）：

1. `$HOME/.SUNWconn_crypto_slots` 檔案

   該檔案必需存在於執行 iPlanet 網站伺服器的使用者的根目錄。iPlanet 網站伺服器可能會以沒有根目錄的 UNIX 使用者的身份執行，在此情況下則不能使用此方式。

2. `/etc/opt/SUNWconn/crypto/slots` 檔案

   `/etc/opt/SUNWconn/crypto/slots` 檔案是全域預設值，如果使用者的根目錄中沒有 `.SUNWconn_crypto_slots` 檔案，則會使用前者。

下面是插槽檔案的內容範例：

```
webserv@engineering
webserv@finance
```

如果找不到上述任一檔案，則第 54 頁的「標記與插槽檔案」中描述的預設模式會被使用。

請參閱第 3 章以取得更多標記名稱在 iPlanet 網站伺服器組態中的相關應用資訊。

使用 `secadm`

`secadm` 程式爲 Sun Crypto Accelerator 1000 提供了命令列介面。

要輕鬆存取 `secadm` 程式，請將 Sun Crypto Accelerator 1000 工具目錄放入搜尋路徑中，例如：

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

`secadm` 命令的語法如下：

`secadm` [`-h`]

`secadm` [`-y`] [`-f` *filename*]

`secadm` [`-y`] [`-r` *realm-name*] [`-u` *username* | `-s` *admin-name*] *command*

該命令的位置在 /opt/SUNWconn/crypto/bin/ 目錄。

表 A-1 顯示了 secadm 工具的選項

表 A-1 secadm 選項

選項	意義
-h	顯示 secadm 的命令說明並離開。
-f *filename*	由 *filename* 讀取一個或多個命令，並結束。
-r *realm-name*	僅在單一命令模式中使用。-r 選項會告訴 secadm 在領域 *realm-name* 中執行提供的命令。
-s *admin-name*	僅在單一命令模式中使用。-s 選項會告訴 secadm 使用 *admin-name* 作爲登入名稱、以系統管理員身份登入。*admin-name* 必需是 UID 0（零）UNIX 使用者（例如 root）。登入程序會在提供的命令被執行前先進行。
-u *username*	僅在單一命令模式中使用。-u 選項告訴 secadm 以 *username* 登入。登入程序會在提供的命令被執行前先進行。
-y	對於所有一般會提示要求確認的命令，強迫回答「yes」。

作業模式

secadm 可以在三種模式之一執行。這些模式的差異，在於命令如何傳送到 secadm。這三個模式是單一命令模式、檔案模式與互動模式。每個模式需要不同的密碼。

單一命令模式

在單一命令模式中，使用者會在 secadm 後指定所有命令列參數、然後指定要執行的命令。舉例來說，下列命令會顯示所有現有領域，並將使用者送回命令列 shell 提示。

```
$ secadm show realm
```

下列命令會以系統管理員身份進行登入，然後在「realm」領域中建立使用者「webserv」。

```
$ secadm -r engineering -s root create user=webserv
Password:
Initial password:
Confirm password:
User webserv created successfully.
```

注意在「Password:」提示後輸入的密碼必需是系統管理員密碼，而「Initial password:」與「Confirm password:」提示後輸入的密碼是新建立使用者的密碼。

所有單一命令模式的輸出，都會送往標準輸出串流。該輸出可以使用標準 UNIX shell 方式加以重導向。

檔案模式

在檔案模式中，使用者會指定一個檔案以供 `secadm` 讀取一個或多個命令。檔案必需是 ASCII 文字，每行包含一個命令。評語應該以「**#**」字元作開頭。如果設定了檔案模式選項，`secadm` 會忽略最後一個選項後所有的命令列參數。下面的範例會執行 `deluser.scr` 中的命令、並對所有提示進行確認回答：

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

互動模式

互動模式提供使用者與 `ftp`(1) 類似的介面，您可以一次輸入一個命令。互動模式不支援 `-y` 選項。

使用 `secadm` 輸入命令

`secadm` 程式擁有命令列語言，您必需加以使用才能與 Sun Crypto Accelerator 1000 介面卡互動。您可以使用命令詞彙的全部或部份字元（足以識別該命令爲限）進行輸入命令。使用「sh」取代「show」應該能夠正常動作，但「lo」可能會產生混淆，因爲這可能是「login」或「logout」。

下面的範例顯示了如何使用完整詞彙輸入命令：

```
secadm{root@engineering}# show user
User                                        Status
-----------------------------------------------------
webserv                                     enabled
alice                                       enabled
bob                                         enabled
-----------------------------------------------------
```

同樣的資訊也可以使用命令詞彙的部份字元獲得，例如：`sh`、`us`。

模糊的命令將會導致解說性的回應：

```
secadm{root@engineering}# lo
Ambiguous command: lo
```

使用 secadm 進行驗證

許多命令、特別是處理使用者帳號與金鑰的命令，會要求您驗證爲使用者管理員或使用者。系統管理員必需對 Sun Crypto Accelerator 1000 進行驗證，才能進行動作如：建立領域、建立使用者帳號、啓用或禁用使用者帳號、或刪除領域及使用者帳號。要變更使用者密碼、或列出使用者擁有的金鑰物件，驗證爲使用者是必需的。表 A-2 顯示了系統管理員可以使用哪些命令、使用者可以使用哪些命令。

表 A-2 命令對照表

命令	驗證	持有憑證	合乎驗證的使用者
`create user=`*username*	否	是	系統管理員
`create realm=`*realm-name*	是	否	系統管理員
`delete user=`*username*	否	是	系統管理員
`delete realm=`*realm-name*	是	否	系統管理員
`disable user=`*username*	否	是	系統管理員
`enable user=`*username*	否	是	系統管理員
`exit`	否	否	全部
`login`	是	否	使用者
`logout`	否	否	全部
`passwd`	是	是	使用者
`set realm=`*realm-name*	否	否	全部
`show class`	否	否	全部
`show key`	否	是	使用者
`show realm`	否	否	全部
`show user`	否	是	系統管理員
`su`	是	否	系統管理員
`quit`	否	否	全部
`unset realm`	否	否	全部

要驗證爲系統管理員，您必需提供 UID 0 的 UNIX 使用者名稱（例如 root 使用者），並在系統提示時輸入密碼。使用者將必需輸入建立使用者時爲他們設定的密碼。當以系統管理員或使用者的身份登入時，您必需先選擇某個領域。

要以使用者的身份登入，請鍵入：

```
secadm{realm-name}> login user=username
```

要以系統管理員的身份登入，請鍵入：

```
secadm{realm-name}> su
```

當以使用者或系統管理員身份登入時，secadm 提示會顯示目前登入的使用者。使用者登入與系統管理員登入可以由提示的最後一個字元辨別。使用者的符號是角括號 (>)，而系統管理員的是井字號 (#)。如果您目前是以使用者或系統管理員的身份登入、並嘗試登入爲其他使用者或系統管理員，新登入成功後，您目前的憑證將會失去。例如：

```
secadm> set realm=engineering
secadm{engineering}> login user=webserv
Password:
secadm{webserv@engineering}> su
System Administration Login Required
Login: root
Password:
secadm{root@engineering}# logout
secadm{engineering}>
```

取得命令說明

secadm 擁有內建說明功能。要取得說明，您必需輸入「?」字元，後面跟著要取得說明的命令。如果輸入命令時，命令列中包含了「?」字元，系統也會顯示該命令的語法，例如：

```
secadm> create ?
Usage: create {user=<username> | realm=<realm-name>}

secadm> show ?
Sub-Command                         Description
-----------------------------------------------------
class                               Show all realm classes
key                                 Show all key objects in a realm
realm                               Show all realms
user                                Show all system accounts
```

輸入「?」可以提供可用命令詞彙的清單，例如：

```
secadm> ?
Sub-Command                       Description
-----------------------------------------------------
create                            Create users and accounts
delete                            Delete users and accounts
disable                           Disable a user
enable                            Enable a user
exit                              Exit secadm
login                             Login as a user
logout                            Logout current session
passwd                            Change password for a user
set                               Set current working realm
show                              Show system settings
su                                Authenticate as the System Administrator
quit                              Exit secadm
unset                             Unset secadm operating parameters
```

如果您要在命令列模式中取得說明，您必需記得在某些情況下，「?」會被您所使用的 shell 解讀。請確定您在問號前使用了命令 shell 脫離字元。

退出 secadm 程式

有兩個命令可以用於脫離 secadm：quit 和 exit。CTRL-D 按鍵序列也可以由 secadm 中脫離。

設定與管理領域

領域是金鑰資料的儲存位置。與領域相關連的包括了管理員與使用者。領域不只提供儲存空間，也提供了使用者帳號持有金鑰物件的方式。這可以讓未以擁有者身份驗證的應用程式看不到金鑰。領域有兩個元件：

- 金鑰元件：這些是長期金鑰，並會儲存以供應用程式如 iPlanet 網站伺服器使用。
- 使用者帳號：這些帳號提供應用程式驗證與存取特定金鑰的方法。

雖然至少必需有一個領域，系統中可已有多個領域，每個領域可已有自己的使用者帳號組。舉例來說，如果應用程式驗證爲使用者 `webserv`、且必需存取領域中的金鑰，則使用者帳號 `webserv` 必需存在於領域中。

建立領域

建立領域會連帶建立儲存長期金鑰目標的目錄、檔案與其他必要資源。要建立領域，系統管理員必需使用 `create realm` 命令命提供要建立的領域名稱。不論目前持有憑證爲何，系統管理員必需經過驗證，命令才能順利完成。當提示輸入密碼時，請輸入 UNIX 系統管理員密碼。例如：

```
secadm> create realm=engineering
System Administrator Login Required
Login: root
Password:
Realm engineering successfully created.
```

您可以依照需要，將領域加以命名。舉例來說，您想爲不同的部門如：財務部門和工程部門，建立不同的領域。在此情況下，您應該將領域命名爲 `finance` 與 `engineering`。例如：

```
secadm> create realm=finance
System Administrator Login Required
Login: root
Password:
Realm finance successfully created
```

設定目前工作中領域

secadm 一次僅能管理單一領域中的金鑰或帳號。多數處理領域即使用者帳號的命令會要求您先選擇領域。要選擇領域，請發出 set realm 命令，範例如下：

```
secadm> set realm=finance
secadm{finance}>
```

選定領域後，secadm 會在 {} 括號中顯示領域名稱。

如果您不想繼續在目前的領域中工作，您可以將目前工作領域設定爲新數值、或取消設定領域。變更或取消設定目前工作領域也會自動登出該領域中目前經過驗證的所有使用者或系統管理員。例如：

```
secadm{finance}> set realm=engineering
secadm{engineering}> unset realm
secadm>
```

在領域中加入使用者

這些使用者名稱僅能使用在 Sun Crypto Accelerator 1000 網域中，且不需與執行網站伺服器程序的 UNIX 使用者名稱一致。在嘗試建立使用者之前，請記得您必需先選擇正確的領域，並以系統管理員的身份登入。例如：

```
secadm> set realm=engineering
secadm{engineering}> su
System Administrator Login Required
Login: root
Password:
secadm{root@engineering}#
```

如果您僅需要一個領域使用者，您可以使用領域名稱「nobody」，避免設定插槽檔案。下面範例在領域「engineering」中建立了使用者「nobody」，並爲「nobody@engineering」設定了密碼，其定義如表 3-1 中的 *user@realm-name*。

```
secadm{root@engineering}# create user=nobody
Initial password:
Confirm password:
User nobody successfully created.
```

網站伺服器啓動時，您必需使用此密碼進行驗證。

警告 – 您必需記住輸入的密碼。沒有密碼，您將無法存取金鑰。沒有任何方法可以擷取失去的密碼。

列出領域

您可以發出 `show realm=`*realm-name* 命令來列出領域上的資訊。

```
secadm> show realm
Realm Name
-----------------------------------------------------
engineering
finance
-----------------------------------------------------
```

列出領域類別

領域類別是金鑰管理模組，控制領域如何管理金鑰物件、使用者帳號、以及驗證資料。Sun Crypto Accelerator 1000 目前唯一支援的領域類別是 `SUNW_filesys` 領域類別。要列出所有支援的領域類別，請使用 `show class` 命令。

```
secadm> show class
Realm Class
-----------------------------------------------------
SUNW_filesys
-----------------------------------------------------
```

刪除領域

要刪除領域，請發出 `delete realm` 命令，並提供要刪除的領域名稱。發出本命令時，`secadm` 會發出「yes/no」訊息，要求您確認移除領域。建立領域後，系統管理員必需先加以驗證，命令才能被執行。此外，您不能刪除使用中的領域。要釋放對領域的參照，您可能必需關閉網站伺服器與（或）管理伺服器。

設定與管理使用者帳號

使用者帳號提供應用程式驗證 Sun Crypto Accelerator 1000 的方法，並允許在同一領域中分隔金鑰。某個使用者帳號擁有的金鑰將不能被未驗證使用者存取、或被以其他身份驗證到領域的使用者存取。對於所有這些命令，您必需選擇領域、且系統管理員必需使用 `secadm su` 命令登入該領域。

建立使用者

- **請發出** `create user` **命令以建立使用者。**

  本命令需要使用者名稱，格式如：`create user=`*username*。

```
secadm{root@engineering}# create user=username
Initial password:
Confirm password:
User username created successfully.
```

警告 – 您必需記住輸入的密碼。沒有密碼，您將無法存取金鑰。沒有任何方法可以擷取失去的密碼。

列出使用者

只有系統管理員才能列出領域中的使用者。系統管理員必需發出 `show user` 命令。本命令只會列出選定領域中的使用者。

- **發出** `show user` **命令。**

```
secadm{root@engineering}# show user
User                                        Status
-----------------------------------------------------------
webserv                                     enabled
alice                                       enabled
bob                                         enabled
-----------------------------------------------------------
```

變更使用者密碼

僅有使用 `secadm login` 命令個別登入的使用者，可以變更該使用者的密碼。您必需先知道目前的密碼，才能設定新密碼。

- **發出** `passwd` **命令。**

```
secadm{username@realm-name}> passwd
Enter current password:
Enter Password:
Confirm Password:
Password successfully changed for user username.
```

警告 – 您必需記住輸入的密碼。沒有密碼，您將無法存取金鑰。沒有任何方法可以擷取失去的密碼。

啓用或禁用使用者

僅系統管理員擁有啓用或禁用使用者的能力。根據預設，每個使用者都是使用啓用狀態建立的。

- **要禁用使用者帳號，請輸入** `disable user=`*username* **命令。**

```
secadm{root@engineering}# disable user=username
User is now disabled.
```

所有對禁用使用者帳號的驗證嘗試都會失敗。然而，所有金鑰都沒有被變更。當帳號被重新啓用時，所有該使用者擁有的金鑰都可以再次被認證應用程式存取。

- **要啟用帳號，請輸入** `enable user=`*username* **命令。**

```
secadm{root@engineering}# enable user=username
User is now enabled.
```

刪除使用者

- **發出** `delete user` **命令，指定要刪除的使用者。**

  系統管理員必需提供要刪除的使用者帳號名稱。

  發出該命令後，與使用者相關連的金鑰會被刪除。刪除使用者之前，`secadm` 會提示系統管理員進行 yes/no 的確認。

```
secadm{root@engineering}# delete user=username
Delete user webserv? [Y/N]: y
User username deleted successfully.
```

附錄 **B**

手冊說明頁

本附錄說明了 Sun Crypto Accelerator 1000 軟體內含的 man 說明頁。

說明頁可以使用下列命令加以檢視：

```
man -M /opt/SUNWconn/man page
```

表 B-1 列出並描述可用的 man 說明頁。

表 B-1 Sun Crypto Accelerator 1000 man 說明頁

man 說明頁	描述
cryptio(7d)	cryptio 裝置驅動程式爲下層硬體編碼加速器提供了存取控制功能。cryptio 驅動程式需要層級軟體的存在，應用程式與核心用戶端才能存取提供的服務。
dca(7d)	dca 裝置是 Sun 加密供應器 leaf 驅動程式，提供下層硬體加密加速器的存取控制功能。 dca 驅動程式需要層級軟體的存在，應用程式與核心用戶端才能存取提供的服務。
kcl(7d)	kcl 裝置驅動程式是多執行緒可載入核心模組，提供 Sun 加密供應器驅動程式支援。 kcl 驅動程式需要層級軟體的存在，應用程式與核心用戶端才能存取提供的服務。
kcpi(7d)	kcpi 裝置驅動程式是多執行緒可載入核心模組，提供 Sun 加密供應器驅動程式支援。 kcpi 驅動程式需要層級軟體的存在，應用程式與核心用戶端才能存取提供的服務。

表 B-1 Sun Crypto Accelerator 1000 man 說明頁

man 說明頁	描述
secadm(1m)	secadm 是 Sun Crypto Accelerator 的管理公用程式。secadm 命令是用來手動操控與 Sun Crypto Accelerator 相關連的組態、帳號、與金鑰資料庫。 secadm 處理敏感的加密金鑰資訊。
secd(1m)	secd 監控程序提供 secadm 應用程式的管理存取服務。
sslconfig(1m)	sslconfig 是 Sun Crypto Accelerator 1000 的組態公用程式。

附錄 C

Apache 網站伺服器 SSL 組態指令行

本附錄列出了設定 Apache 網站 SSL 支援組態以搭配 Sun Crypto Accelerator 1000 軟體使用的相關資訊。在 `http.conf` 檔案中設定指令行組態。請參考 Apache 文件以獲得更多資訊。

1. `SSLPassPhraseDialog exec:`*program*

   適用範圍：全域

   本指令行告知 Apache 網站伺服器、指定 *program* 應該被執行以蒐集密碼或金鑰檔案。*program* 應該將蒐集到的密碼列印到標準輸出。

   如果系統上有多重金鑰檔案、且有通用密碼，則 *program* 僅會被執行一次（每個被蒐集到的密碼在下次執行 *program* 前，都會被再試一次。）

   program 執行時有兩個引數：第一個是伺服器的名稱，格式如：*servername*:*port*，例如：`www.fictional-company.com:443`。（連接埠 443 是以 SSL 爲基礎的網站伺服器的典型連接埠。）第二個是金鑰檔案中的金鑰類型 (*keytype*)。*keytype* 可以是 RSA 或 DSA。

注意 – 由於本程式可以在系統啓動時執行，請確定加以設計已應付主控台並非 `tty` 裝置的情況（此時 `tty`(3c) 會傳回 false）。

   提供的程式 `/opt/SUNWconn/crypto/bin/sslpassword` 可以用於 *program* 執行檔。本程式會自動提示要求輸入密碼，且在密碼輸入時將不予顯示。

   提供的 `sslpassword` 程式也會自動由檔案中搜尋密碼 ，這可以用來在網站伺服器啓動時避免使用者互動。金鑰檔案的密碼會由檔案 `/etc/apache/`*servername*`:`*port*`.`*keytype*`.pass` 進行搜尋。如果找不到該檔案，則系統會使用 `/etc/apache/default.pass` 檔案。這些密碼檔案的內容僅包含未加密的密碼，每個密碼一行。

注意 – 密碼檔案應該使用權限加以保護，如此僅有執行網站伺服器的 UNIX 使用者可以讀取該檔案。這應該與使用標準 Apache `User` 指令行相同的使用者。

如果沒有特別指定，預設動作是使用內部的提示機制。Sun 建議客戶避免預設值，並使用提供的 `sslpassword` 程式加以取代，以避免在系統啓動時進行互動的麻煩。

2. `SSLEngine (on|off)`

   適用範圍：全域、虛擬主機

   本指令行是用於啓用 SSL 通訊協定。這一般是用來在虛擬主機上啓用伺服器子集的 SSL 功能。常用的型態之一是：

```
<VirtualHost _default_:443>
SSLEngine on
</VirtualHost>
```

對於聆聽連接埠 443（標準 HTTPS 連接埠）的所有伺服器，設定 SSL 使用上的組態。如果不存在，根據預設這會被關閉。

3. `SSLProtocol [+-]`*protocol*

   適用範圍：全域、虛擬主機

   本指令行會設定伺服器應該用於 SSL 交易的的通訊協定。

   可用的通訊協定會被會被列在表 C-1 中並加以詳細描述。

表 C-1 SSL 通訊協定

通訊協定	說明
`SSLv2`	來自 Netscape，原始的實質 SSL 標準
`SSLv3`	更新版本的 SSL 通訊協定，受到多數受歡迎網頁瀏覽器支援
`TLSv1`	`SSLv3` 的更新，目前正再進行 IETF 標準化，本文撰寫之時僅有極少的瀏覽器支援
`all`	啓用所有通訊協定

您可以使用加號 (+) 或減號 (-) 來新增或移除所有通訊協定。舉例來說，要禁用 SSLv2 支援，請使用下列指令行：

```
SSLProtocol all -SSLv2
```

這也等於：

```
SSLProtocol +SSLv3 +TLSv1
```

4. `SSLCipherSuite` *cipher-spec*

   適用範圍：全域、虛擬主機、目錄、`.htaccess`

   SSLCipherSuite 指令行是用於設定哪些 SSL 編碼器可供使用、以及他們的偏好設定。在全域或虛擬主機的情況下，它會在最初的 SSL handshake 中被使用。在單一目錄的情況下，它會強迫 SSL 協議使用指名的編碼器。協議會在要求被讀取後、回應被傳送前進行。

   cipher-spec 是一個用冒號分隔的編碼器清單，編碼器詳細資料如表 C-2。

表 C-2 可用 SSL 編碼器

Cipher-Tag	通訊協定	金鑰交換	驗證	加密	MAC	類型
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES（168 位元）	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES（168 位元）	MD5	
RC4-SHA	SSLv3	RSA	RSA	ARCFOUR（128 位元）	SHA1	
RC4-MD5	SSLv3	RSA	RSA	ARCFOUR（128 位元）	MD5	
RC4-MD5	SSLv2	RSA	RSA	ARCFOUR（128 位元）	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	ARCTWO（128 位元）		
DES-CBC-SHA	SSLv3	RSA	RSA	DES（56 位元）	SHA1	
RC4-64-MD5	SSLv2	RSA	RSA	ARCFOUR（64 位元）	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES（56 位元）	MD5	
EXP-DES-CBC-SHA	SSLv3	RSA（512 位元）	RSA	DES（40 位元）	SHA1	匯出
EXP-RC2-CBC-MD5	SSLv2	RSA（512 位元）	RSA	ARCTWO（40 位元）	SHA1	匯出
EXP-RC2-CBC-MD5	SSLv3	RSA（512 位元）	RSA	ARCTWO（40 位元）	SHA1	匯出
EXP-RC4-MD5	SSLv3	RSA（512 位元）	RSA	ARCFOUR（40 位元）	MD5	匯出
EXP-RC4-MD5	SSLv2	RSA（512 位元）	RSA	ARCFOUR（40 位元）	MD5	匯出
NULL-SHA	SSLv3	RSA	RSA	無	SHA1	
NULL-MD5	SSLv3	RSA	RSA	無	MD5	

表 C-2 可用 SSL 編碼器

Cipher-Tag	通訊協定	金鑰交換	驗證	加密	MAC	類型
ADH-DES-CBC3-SHA	SSLv3	DH	無	3DES（168 位元）	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	無	DES（56 位元）	SHA1	
ADH-RC4-MD5	SSLv3	DH	無	ARCFOUR（128 位元）	MD5	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES（168 位元）	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES（168 位元）	SHA1	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES（56 位元）	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES（56 位元）	SHA1	
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH（512 位元）	RSA	DES（40 位元）	SHA1	匯出
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH（512 位元）	DSS	DES（40 位元）	SHA1	匯出
EXP-ADH-DES-CBC-SHA	SSLv3	DH（512 位元）	無	DES（40 位元）	SHA1	匯出
EXP-ADH-RC4-MD5	SSLv3	DH（512 位元）	無	ARCFOUR（40 位元）	MD5	匯出

在表 C-2 中，DH 指的是 Diffie-Hellman，DSS 指的是 Digital Signature Standard。表 C-3 列出並說明了提供類似巨集之分組功能的別名。

表 C-3 SSL 別名

別名	說明
SSLv2	所有 SSL 2.0 版編碼器
SSLv3	所有 SSL 3.0 版編碼器
EXP	所有匯出等級編碼器
EXPORT40	所有 40 位元匯出編碼器
EXPORT56	所有 56 位元匯出編碼器
LOW	較低強度編碼器（DES，40 位元 RC4）
MEDIUM	全部 128 位元編碼器
HIGH	所有編碼器使用三重 DES
RSA	所有編碼器使用 RSA 金鑰交換
DH	所有編碼器使用 Diffie-Hellman 金鑰交換
EDH	所有編碼器使用 Ephemeral Diffie-Hellman 金鑰交換

表 C-3 SSL 別名

別名	說明
ADH	所有編碼器使用匿名 Diffie-Hellman 金鑰交換
DSS	所有編碼器使用 DSS 驗證
NULL	所有編碼器都不使用加密

您可以使用表 C-4 中列出並詳細說明的特殊字元來設定編碼器偏好組態。

表 C-4 設定編碼器偏好組態用的特殊字元

字元	說明
< 無 >	新增編碼器到清單
!	由清單中完全移除編碼器 — 編碼器將不能再次被加入
+	新增編碼器到清單中，並放到目前位置（可能會將它降階）
-	由清單中移除編碼器（可以在稍後重新加入到清單中）

cipher-spec 的預設值是

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
```

預設值會設定所有編碼器的組態，但匿名（未經驗證） Diffie-Hellman 除外，ARCFOUR 之使用優於 RSA，且高等級的加密優於低等級的加密。

5. `SSLCertificateFile` *file*

   適用範圍：全域、虛擬主機

   本指令行會指定本伺服器中 PEM 編碼之 X.509 憑證檔案的所在位置。

6. `SSLCertificateKeyFile` *file*

   適用範圍：全域、虛擬主機

   本指令行會指定本伺服器中 PEM 編碼之私人金鑰檔案的所在位置，對應於使用 `SSLCertificateFile` 指令行設定組態的憑證。

7. `SSLCertificateChainFile` *file*

   適用範圍：全域、虛擬主機

   本指令行會指定包含構成伺服器憑證路徑的 PEM 編碼之憑證的位置。當伺服器的憑證並非由用戶端認識的授權機構直接簽署時，這可以用於協助用戶端檢查伺服器的憑證。

   當使用用戶端驗證 (`SSLVerifyClient`) 時，對於用戶端驗證，鍊結中的憑證也被假定爲有效。

8. `SSLCACertificateFile` *file*

   適用範圍：全域、虛擬主機

   本指令行會指定包含用於用戶端驗證之憑證授權機構 (CA) 的憑證連鎖檔案的所在位置。

9. `SSLCARevocationFile` *file*

   適用範圍：全域、虛擬主機

   本指令行會指定包含用於用戶端驗證之憑證授權機構憑證授權機構 (CA) 之憑證撤銷連鎖檔案。

10. `SSLVerifyClient` *level*

    適用範圍：全域、虛擬主機、目錄、`.htaccess`

    本指令行設定了用戶端對伺服器的驗證組態。（注意：對於電子商務應用而言一般並不需要此項設定，但在其他應用中有作用。）

    level 的數值列在表 C-5，並有詳細說明。

表 C-5 SSL 檢查用戶端階層

層級	說明
`none`	不需要用戶端憑證
`optional`	用戶端可以提出有效憑證
`require`	用戶端*必需*提出有效憑證
`optional_no_ca`	用戶端可能會提出憑證，但憑證不一定必需有效

一般來說，您可以使用 `none` 或 `require`。預設值是 `none`。

11. `SSLVerifyDepth` *depth*

    適用範圍：全域、虛擬主機、目錄、`.htaccess`

    本指令行會指定伺服器在用戶端憑證上允許的最大憑證鍊結深度。數值 0 代表只有自行簽署的憑證有效，而數值 1 代表用戶端必需被伺服器直接認知的 CA （透過 `SSLCACertificateFile`）簽署。更大的數值允許 CA 的代理。

12. `SSLLog` *filename*

適用範圍：全域、虛擬主機

本指令行會指定記錄 SSL 專屬資訊的記錄檔。如果沒有加以指定（預設值），則沒有任何 SSL 特定資訊將會被記錄。

13. `SSLLogLevel` *level*

適用範圍：全域、虛擬主機

本指令行指定記錄在 SSL 記錄檔中的資訊的詳細度。*level* 的數值列在表 C-6，並有詳細說明。

表 C-6 SSL 記錄階層數值

數值	說明
`none`	不記錄，但錯誤訊息依然會被傳送到標準 Apache 錯誤記錄
`warn`	包含警告訊息
`info`	包含資訊訊息
`trace`	包含追蹤訊息
`debug`	包含除錯訊息

14. `SSLOptions` [`+-`] *option*

適用範圍：全域、虛擬主機、目錄、`.htaccess`

本指令行會設定 SSL 專屬選項的組態。要將選項新增到目前組態中，請在前方加上加號 (+)；要移除，請在前方加上減號 (-)。如果沒有加號或減號，則最接近的選項組會被使用。

選項與其描述被列在表 C-7 中。

表 C-7 可用 SSL 選項

選項	說明
`StdEnvVars`	建立標準的 SSL 相關環境變數組—這會導致性能衰減。
`ExportCertData`	導致匯出 `SSL_SERVER_CERT`、`SSL_CLIENT_CERT` 與 `SSL_CLIENT_CERT_CHAIN`*n* (*n* = 0, 1, ...) 環境變數。這些變數包含 PEM 編碼的用戶端與伺服器憑證。
`FakeBasicAuth`	用戶端憑證的「Distinguished Name (DN)」會被轉譯爲 HTTP 基本驗證使用者名稱 (Basic Authentication Username)，且會「假裝」爲有驗證。這可以在 SSL 用戶端認證上使用標準的 Apache 存取控制機制，而不提示使用者輸入密碼。 這些使用者在 Apache 密碼檔案中的項目必需使用加密密碼 `xxj31ZMTZzkVA`，這是「password」這個字的加密型態 (`crypt`(3c))。
`StrictRequire`	強制在 `SSLRequireSSL` 被拒絕時禁止存取，即使其他可能覆蓋本指令行的指令行如 `Satisfy Any` 存在。

15. `SSLRequireSSL`

適用範圍：目錄、`.htaccess`

本指令行會禁止對特定目錄進行存取，除非使用的是 HTTPS 這可以用來防止錯誤的組態造成目錄的內容被未經驗證或未加密存取。

附錄 **D**

建立應用程式以搭配 Sun Crypto Accelerator 1000 介面卡使用

本附錄討論隨 Sun Crypto Accelerator 1000 提供的軟體，它們可以用來建立某些 OpenSSL 相容應用程式、以利用 Sun Crypto Accelerator 的編碼加速功能。

注意 – 本項建立應用程式建立以使用 Sun Crypto Accelerator 1000 軟體與硬體的資訊係以其「現狀」提供，且並非本產品的正式支援部份。提供本資訊的目的是希望有所幫助，但本項資訊並不提供任何擔保。如果您需要 Sun 支援的解決方案，請與 Sun Professional Services 聯繫，查看有哪些選擇。

您必需先安裝 `SUNWcrysl` 套件，其中包含必要的檔頭檔與程式庫。

應用程式組態必需包含 `/opt/SUNWconn/crypto/include` 的 OpenSSL 檔頭，例如編譯旗標。

```
-I /opt/SUNWconn/crypto/include
```

此外，連結器必需包含通往正確程式庫的參照。多數 OpenSSL 相容的應用程式會參照 `libcrypto.a` 與 `libssl.a` 程式庫之一、或兩者皆參照。您也必需加入 Sun 加密程式庫。下列的連結器旗標可以用來達成目的：

```
-L/opt/SUNWconn/crypto/lib -R/opt/SUNWconn/crypto/lib \
-lcrypto -lssl -lcryptography -lnvpair
```

注意並非所有 OpenSSL 應用程式都會由這樣的編譯中獲益（相對於使用原本的 OpenSSL 程式庫建立而言；該程式庫可以由 `www.openssl.org` 下載）。

附錄 **E**

Sun Crypto Accelerator 1000 介面卡規格

本章概略敘述 Sun Crypto Accelerator 1000 介面卡的各種規格。

本附錄包含了下列幾個部份：

- 第 79 頁的「實體尺寸」
- 第 80 頁的「介面規格」
- 第 80 頁的「電源要求」
- 第 81 頁的「環境規格」

實體尺寸

表 E-1 實體尺寸

尺寸	英制度量	公制度量
長度	6.875 英吋	174.625 公釐
寬度	4.2 英吋	106.680 公釐

介面規格

表 E-2 介面規格

功能	規格
PCI 時脈	33 MHz 或 66 MHz
主機介面	支援 33 MHz 或 66 MHz 時脈率及 3.3 V 或 5 V 電壓的 PCI 2.1。
PCI 匯流排寬度	32 位元或 64 位元

電源要求

表 E-3 電源要求

規格	測量
最大電源消耗量	10W @ 5V 700mW @ 3.3V
電源公差	5V +/- 5% 3.3V +/- 5%
操作電流	2A @ 1.8V 150mA @ 3.3V

環境規格

表 E-4 環境規格

條件	操作規格	蓄電規格
溫度	0° 至 70° C、32° 至 160° F	-65° 至 +150° C、-85° 至 300° F
相關溼度	5 至 85% 非凝結	0 至 95% 非凝結

附錄 **F**

Third-Party Licenses（協力廠商授權）

Some portions of Software are provided with notices and/or licenses from other parties which govern the use of those portions.

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.

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.

索引

A

Apache SSL 指令行，69

D

dcatest，48
  命令列語法，50
  參數選項，49
dcatest 子測試，49

R

RSA 金鑰組，40

S

secadm，55
SunVTS，47

U

URL
  iPlanet 軟體，19, 29
  openssl，77

五劃

目錄
  層級，11

七劃

伺服器憑證，22, 32

八劃

使用者，53
  列表，64
  刪除，66
  建立，64
  啓用或禁用，65
使用者密碼
  變更，65
金鑰長度，41

九劃

負載平衡，4

十劃

修正程式
- 建議，5
- 需求，5

高可用性，3

十一劃

動態組態重設，3

密碼
- iPlanet 網站伺服器需要清單，15

啓用
- Apache 網站伺服器，39
- iPlanet 網站伺服器，15

統計數值，52

軟體套件，10

十二劃

插槽檔案，54

診斷測試，47

十四劃

演算法，3

管理 iPlanet 網站伺服器，53

需求
- 軟體，4
- 硬體，4

領域，53
- 列表，63
- 刪除，63
- 建立，61
- 設定，62

十五劃

熱拔插，3

十七劃

檔案與目錄，10