



Sun™ Crypto Accelerator 1000

보드 버전 1.1 릴리스 노트

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

부품 번호 816-4573-10
2002년 7월, 개정판 A

이 문서에 대한 의견은 다음 주소로 보내 주십시오. docfeedback@sun.com

Copyright 2002 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

이 제품 또는 문서는 사용, 복사, 배포, 역컴파일 등에 대한 제한 사항이 수록된 라이선스 계약에 따라 배포됩니다. Sun 및 Sun 인가자의 사전 서면 승인 없이는 어떠한 수단으로도 이 제품 또는 문서를 복사할 수 없습니다. 글꼴 기술을 포함한 타사 소프트웨어는 Sun 공급업체로부터 저작권 및 라이선스를 받은 것입니다.

제품의 일부는 캘리포니아 대학으로부터 라이선스를 받은 BSD 버전일 수 있습니다. UNIX는 미국 및 기타 국가에 등록된 상표이며 X/Open Company, Ltd로부터 독점 라이선스를 받은 제품입니다.

Sun, Sun Microsystems, Sun 로고, SunVTS, AnswerBook2, docs.sun.com, iPlanet, Sun Enterprise, Sun Enterprise Volume Manager, Solaris는 미국 및 기타 국가에 등록된 상표, 등록 상표, Sun Microsystems, Inc의 서비스 상표입니다. 모든 SPARC 상표는 라이선스 계약에 따라 사용되며 미국 및 기타 국가에 등록된 SPARC International, Inc의 상표 또는 등록 상표입니다. SPARC 상표를 부착한 제품은 Sun Microsystems, Inc가 개발한 아키텍처에 기초하며, Netscape는 Netscape Communications Corporation의 상표 또는 등록 상표입니다. 이 제품에는 OpenSSL Toolkit(<http://www.openssl.org/>)에서 사용하기 위해 OpenSSL Project가 개발한 소프트웨어가 포함되어 있습니다. 이 제품에는 Eric Young(eay@cryptsoft.com)이 작성한 암호화 소프트웨어가 포함되어 있습니다. 이 제품에는 mod_ssl 프로젝트(<http://www.modssl.org/>)에서 사용하기 위해 Ralf S. Engelschall <rse@engelschall.com>이 개발한 소프트웨어가 포함되어 있습니다.

OPEN LOOK 및 Sun™ Graphical User Interface는 Sun Microsystems, Inc.가 사용자와 피인가자를 위해 개발하였습니다. Sun은 컴퓨터 산업에서 비주얼 또는 그래픽 사용자 인터페이스 개념을 연구 및 개발에 Xerox가 아낌없이 보여준 선구적 노력에 큰 감사를 드립니다. Sun은 Xerox Graphical User Interface에 대해 Xerox로부터 비독점적 라이선스를 받았으며 이 라이선스는 OPEN LOOK GUI를 구현하거나 Sun의 서면 라이선스 계약을 준수하는 Sun의 피인가자에게도 적용됩니다.

이 문서는 "있는 그대로" 제공되며, 상품성, 특정 목적에 대한 적합성, 비침해성 등에 대한 묵시적 보증을 비롯한 명시적 또는 묵시적 조건, 진술, 보증 등에 대해 어떠한 책임을 지지 않습니다. 단, 이러한 책임 제한은 법적으로 허용된 범위 내에서만 적용됩니다.



재활용
가능



Adobe PostScript

Sun Crypto Accelerator 1000 보드 버전 1.1 릴리스 노트

본 릴리스 노트에서는 *Sun Crypto Accelerator 1000 보드 버전 1.1 설치 및 사용자 설명서*가 완성된 시점에는 알려지지 않았던 정보를 제공합니다.

iPlanet 웹 서버의 알려진 문제

1. iPlanet 4.x 또는 6.x 관리 서버는 실행 중이고 관리 웹 서버는 실행 중이 아닐 경우, 토큰 암호를 묻는 대화 상자가 여러 번 나타납니다. 글꼴 파일 크기가 너무 크거나 토큰이 많아서 암호 입력 행이 여러 줄로 표시되는 경우, 대화 상자의 크기가 고정되어 있으므로 패널 하단의 단추가 표시되지 않습니다. 대화 상자의 크기를 조정할 수 없으므로 패널 하단의 [Accept(동의)] 단추를 선택하고 변경 사항을 전송할 수 없습니다.

이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

- [GUI Preference(GUI 등록 정보)]를 [On/Off(설정/해제)]로 설정하여 명령행 또는 관리에서 웹 서버를 먼저 시작합니다.
- [Apply(적용)]와 [Load Configuration Files(구성 파일 로드)]를 차례로 눌러 서버를 시작하지 않고 구성을 적용합니다.

참조 버그: 4532645

2. 하나 이상의 영역이 존재하거나 여러 웹 서버에 여러 사용자가 사용되도록 구성되어 있으면 iPlanet 웹 서버가 작동되지 않습니다.

이 문제는 다음 두 가지 방법으로 해결할 수 있습니다.

- 각 웹 서버에 대해 하나 이상의 영역 및 사용자를 구성하지 않습니다.

- 여러 UNIX 사용자로 iPlanet 웹 서버의 여러 인스턴스를 실행할 수 있으며, 각 사용자에게 대해 \$HOME/.SUNWconn_crypto_slots를 구성합니다. 슬롯 파일에 대한 자세한 내용은 *Sun Crypto Accelerator 1000 보드 버전 1.1 설치 및 사용자 설명서*를 참조하십시오.

참조 버그: 4532941 및 4593111

3. iPlanet 제공 유틸리티인 pk12util은 내부(소프트웨어) 데이터베이스에서 인증서 및 키를 내보낸 다음 외부(하드웨어) 데이터베이스로 가져옵니다. 외부 데이터베이스에서는 인증서 또는 키를 내보내지 않습니다.

```
% cd /usr/iplanet/servers/alias
% pk12util -o temp.p12 -n "Our Token:Server-Cert" -d .
Enter Password or Pin for "Our Token":
Enter password for PKCS12 file:
Re-enter password:
pk12util: add cert and key failed: Unable to export. Private Key
could not be located and exported.
```

참조 버그: 4620283

4. iPlanet 웹 서버 6.0을 구성할 때 [Cipher Default(암호 기본값)] 설정을 선택하고, 인증서를 선택하고, [OK(확인)] 단추를 눌러 오른쪽 상단 모서리의 [Apply(적용)]를 선택하여 암호를 적용한 후, *Sun Crypto Accelerator 1000 보드 버전 1.1 설치 및 사용자 설명서*에 나와 있는 순서대로 정확히 실행하지 않으면 `user@realm-name` 항목이 제거될 수 있습니다.

웹 서버가 Sun Crypto Accelerator 1000 보드와 함께 올바르게 시작하려면 이 항목이 필요합니다. 다음 순서에 따라 단계를 실행하면 웹 서버가 시작됩니다.

- [Cipher Default(암호 기본값)]를 [SSL2] 암호 또는 [SSL3] 암호로 선택합니다.
- [OK(확인)]를 누릅니다.
- [Apply(적용)]를 누릅니다.
- [Load Configuration(구성 로드)]을 누릅니다.

상기 단계를 완료한 후에도 웹 서버가 올바르게 시작되지 않으면 다음 해결 방법을 사용합니다.

- 파일을 편집합니다.

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

- 다음으로 시작되는 행을 찾습니다.

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

- 같은 행에서 Server-Cert 앞에 `user@realm-name:`를 삽입하여 변경된 행이 다음과 같이 나타나게 합니다.

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

- 웹 서버를 다시 시작합니다.

참조 버그: 4607112

지원되는 아파치 웹 서버 버전

Sun Crypto Accelerator 1000 는 Solaris 8 기반 Apache 1.3.12 와 1.3.26 에서 사용할 수 있을 뿐만 아니라 ,Solaris 8 기반 Apache 1.3.22 와 1.3.26 에서도 사용할 수 있습니다. 이 정보는 Solaris 나 Sun 패치와 함께 제공되는 Apache 버전에만 적용됩니다.

아파치 웹 서버의 알려진 문제

1. 아파치(/etc/rc3.d/S50apache) 및 dtlogin(/etc/rc2.d/S99dtlogin)에 대한 시작 파일 실행을 명령하면 시스템 부팅시에 명령이 제대로 실행되지 않습니다. 이로 인해 시스템 시작 시 콘솔에서 아파치 암호 정보를 가져오지 못할 수 있습니다. 이 문제를 해결하려면 루트 상태에서 다음 명령을 실행하여 아파치 웹 서버 시작 명령을 다시 실행하십시오.

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

Sun Crypto Accelerator 1000 버전 1.1 소프트웨어의 알려진 문제

1. Solaris 8에서는 Sun Crypto Accelerator 1000 버전 1.1 소프트웨어를 설치하기 전에 112438-01 패치를 먼저 설치해야 합니다. 이 패치는 제품 CD의 patches 하위 디렉토리에 들어 있습니다. <http://sunsolve.sun.com>에서도 다운로드할 수 있습니다.

참조 버그: 4470196

2. 키 추출을 위한 소프트웨어 도구는 iPlanet 웹 서버 6.x과 함께 제공되므로 iPlanet 웹 서버 4.x에서는 제공되지 않습니다.

소프트웨어(내부) 데이터베이스 키 추출에 대해 다음 두 가지 해결 방법이 있습니다.

- <http://www.ipplanet.com/downloads>에서 NSPR 4.12 및 NSS 3.3 이상 릴리스를 다운로드합니다.
설치한 후 pk12util을 실행하여 소프트웨어(내부) 데이터베이스에서 정확한 인증서 및 키를 추출합니다.
- Netscape Communicator 4.x 또는 6.x를 사용하여 소프트웨어(내부) 데이터베이스에서 정확한 키를 추출합니다.

현재로서는 Sun Crypto Accelerator 1000 보드를 사용하여 키를 추출할 수 있는 방법이 없습니다.

참조 버그: 4621453

3. prtdiag 유틸리티 및 Open Boot PROM가 다른 플랫폼에서 구현되었으므로 prtdiag(1M)를 사용하면 Sun Crypto Accelerator 1000 보드가 다르게 나타나거나 전혀 나타나지 않을 수 있습니다. 예를 들어, Enterprise 450에서는 Sun Crypto Accelerator 1000 보드가 다음과 같이 나타납니다.

```
SYS PCI 66 4 pciclass,100000
```

참조 버그: 4343467 및 4526901

4. 이 문서를 작성한 시점에서는 Sun Crypto Accelerator I에서 키 및 인증 자료를 추출하기 위한 메커니즘이 없었습니다. <http://sunsolve.sun.com>의 패치 데이터베이스에서 이 문제 해결을 위한 패치가 있는지 확인하십시오.

참조 버그: 4630250

5. Sun Crypto Accelerator 1000 보드는 Solaris 9 기반 Sun Fire™ V880 시스템 66MHz 슬롯의 PCI 핫플러그 기능과 호환되지 않습니다. 그러나, Solaris 8 기반 시스템에서는 이 문제가 발생하지 않습니다. 이 문제를 해결할 수 있는 패치가 제공될 것으로 보입니다.

Solaris 9에서는 시스템이 꺼진 상태에서 보드가 설치될 수 있으므로 66MHz 슬롯 사용이 가능할 수 있으며, 33MHz 슬롯에서 핫플러그가 가능할 수 있습니다.

참조 버그: 4698278