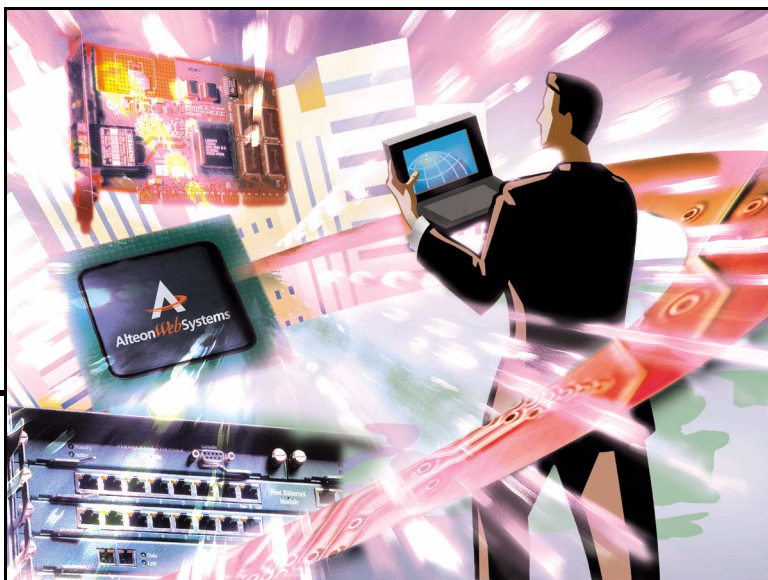


Installation and User's Guide



iSD100-SSLTM

Secure Sockets Layer Offload Device

Part Number: 050125, Revision A, September 2000



50 Great Oaks Boulevard
San Jose, California 95119
408-360-5500 Main
408-360-5501 Fax
www.alteonwebsystems.com

Copyright 2000 Alteon WebSystems, Inc., 50 Great Oaks Boulevard, San Jose, California 95119, USA. All rights reserved. Part Number: 050125, Revision A.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Alteon WebSystems, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov 1995).

Alteon WebSystems, Inc. reserves the right to change any products described herein at any time, and without notice. Alteon WebSystems, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Alteon WebSystems, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Alteon WebSystems, Inc.

iSD100-SSL and Web OS are trademarks of Alteon WebSystems, Inc. in the United States and certain other countries. Any other trademarks appearing in this manual are owned by their respective companies.

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

See [Appendix F, “License Information,”](#) for more information.

Regulatory Compliance

FCC Class A Notice. The equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: 1) The device may not cause harmful interference, and 2) This equipment must accept any interference received, including interference that may cause undesired operation.

The 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 in a residential installation. The 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. Operation of this equipment in a residential area is likely to cause harmful interference. In such a case, the user will be required to correct the interference at his own experience.

Do not make mechanical or electrical modifications to the equipment.

Industry Canada: This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil Numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI Class A Notice: This is a Class A product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur. In such a case, the user may be required to take corrective actions.

Japanese VCCI Class A Statement

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。

Taiwan EMC Statement

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。

CE Notice: The CE mark on this equipment indicates that this equipment meets or exceeds the following technical standards: EN50082-1, EN55022, EN60555-2, EN61000-4-1, EN61000-4-2, EN61000-4-3, EN61000-4-4, and EN61000-4-5.

Safety Information

Caution—The management processor module in this product contains a Lithium Battery. Batteries are not customer replaceable parts. They may explode if mishandled. Do not dispose of the battery in fire. Do not disassemble or recharge.

Caution—Alteon WebSystems products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electric shock, do not plug Alteon WebSystems products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.

Caution—Not all power cords have the same ratings. Household extension cords do not have overload protection and are not meant for use with computer systems. Do not use household extension cords with your Alteon WebSystems product.

Caution—Your Alteon WebSystems product is shipped with a grounding type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

Nordic Lithium Battery Cautions

(Norge) ADVARSEL—Litiumbatteri - Eksplosjonsfare. Ved utskifting benyttes kun batteri som anbefalt av apparatfabrikanten. Brukt batteri returneres apparatleverandøren.

(Sverige) VARNING—Explosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

(Danmark) ADVARSEL! Litiumbatteri - Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage til leverandøren.

(Suomi) VAROITUS—Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan laitevalmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mukaisesti.



Contents

Preface 9

- Who Should Use This Book 9
- How This Book Is Organized 9
- Typographic Conventions 10
- Contacting Alteon WebSystems 11
- Warranty 11

Chapter 1: Introducing the iSD100-SSL 13

- Feature Summary 13
 - Hardware 13
 - Software 14
- Physical Description 15
 - Front Panel 15
 - Rear Panel 15
- Basic Operation 16

Chapter 2: Installing the iSD100-SSL Hardware 19

- System Requirements 20
- Preparing for Installation 20
- Mounting the iSD100-SSL 21
 - Rack-Mounting the Unit 21
 - Table-Mounting the Unit 22
- Connecting Network Cables 23
 - 10/100Base-T Port (Model iSD100-SSL-C1A) 23
 - 1000Base-SX Port (Model iSD100-SSL-F2A) 24
- The Console Port 25
- Power 25
 - Connecting the Power Cord 25
 - Turning Power On/Off 25

Chapter 3: Initial Setup 27

Initializing the iSD100-SSL 27

Updating the Software 30

Chapter 4: iSD100-SSL Command Reference 31

Accessing the Menu System 31

iSD Menu 32

SSL Offload Application Menu 33

iSD Information Command 35

Chapter 5: iSD100-SSL Sample Applications 37

Web Server Accelerator 38

 Create the Necessary VLANs 38

 Configure One IP Interface for Each VLAN 39

 Configure Server Load Balancing Parameters 40

 Configure Basic iSD100-SSL Parameters 41

 Add a Certificate to the iSD100-SSL 43

 Configure Filters 44

 Apply, Save, and Verify the Configuration 46

Content-Intelligent Switching for Secure Sessions 47

Redundant Active-Standby Configuration 48

 On Web Switch 2, Create the Necessary VLANs 49

 Configure IP Interfaces for Each VLAN (Web Switch 2) 50

 Set Basic iSD100-SSL Parameters (Web Switch 2) 50

 Prepare to Receive Synchronization (Web Switch 2) 51

 On Web Switch 1, Configure VRRP 51

 Update VRRP Parameters for iSD100-SSL (Web Switch 1) 52

 Prepare and Send Synchronization (Web Switch 1) 53

 On Web Switch 2, Update VRRP Parameters for iSD100-SSL 53

 Verify failover 54

Appendix A: Theory of Operation 55

Encryption 55

Public Key Encryption 56

Digital Signatures 56

Certificates 57

 Register Certificates 57

 Chain Certificates 57

Example SSL Transaction 58

Appendix B: Supported Ciphers 61**Appendix C: Building Keys and Certificates 63**

Creating a Public/Private Key Pair 63

Generating and Submitting a CSR to a CA 64

Adding Certificates to the iSD100-SSL 66

Using Copy and Paste to Add Certificates and Keys 66

Using TFTP to Add Certificates 68

Importing an Existing Key/Certificate from a Server 69

Appendix D: Troubleshooting 71

Basic Solution Checklists 71

Console Diagnostics 72

Connecting a Terminal to the iSD100-SSL 72

System Diagnostics 74

Appendix E: Specifications 75

Physical Characteristics 75

Supported Standards 76

Port Specifications 76

Power Requirements 76

Environmental Specifications 77

Certifications 77

Appendix F: License Information 79



Preface

This *Installation and User's Guide* describes the Alteon WebSystems Integrated Service Director (iSD100-SSL) with SSL offload software. This document introduces the major features of the iSD100-SSL and explains how to perform system configuration and maintenance.

Who Should Use This Book

This *Installation and User's Guide* is intended for network installers and system administrators engaged in configuring and maintaining a network. It assumes that you are familiar with Ethernet concepts, IP addressing, the IEEE 802.1d Spanning Tree Protocol (STP), and SNMP configuration parameters.

How This Book Is Organized

The chapters in this book are organized as follows:

Chapter 1, “Introducing the iSD100-SSL,” provides an overview of the major features of the iSD100-SSL, including its physical layout and the basic concepts of its operation.

Chapter 2, “Installing the iSD100-SSL Hardware,” describes how to mount the iSD100-SSL, connect network cables, and attach power.

Chapter 3, “Initial Setup,” describes how to perform minimal start-up configuration on the iSD100-SSL and how to update and upgrade its software.

Chapter 4, “iSD100-SSL Command Reference,” explains how to access the iSD100-SSL menus on the Web switch and provides details about all available commands and options.

Chapter 5, “iSD100-SSL Sample Applications,” provides basic scenarios and configuration examples for using the iSD100-SSL for Web server acceleration, content intelligent switching for secure sessions, and in redundant active-standby configurations.

Appendix A, “Theory of Operation,” provides a general overview of basic concepts behind Secure Socket Layer (SSL) transactions.

Appendix B, “Supported Ciphers,” provides a list of ciphers supported in this product.

Appendix C, “Building Keys and Certificates,” describes how to generate and prepare keys and certificates for use with the iSD100-SSL.

Appendix D, “Troubleshooting,” provides solutions to basic problems and explains how to use the iSD100-SSL console port for system diagnostics.

Appendix E, “Specifications,” describes the physical characteristics of the iSD100-SSL.

Appendix F, “License Information,” provides licensing information for the software used in this product.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	This type is used for names of commands, files, and directories used within the text. It also depicts on-screen computer output and prompts.	View the <code>readme.txt</code> file. Main#
AaBbCc123	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	Main# sys
<AaBbCc123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets. This also shows book titles, special terms, or words to be emphasized.	To establish a Telnet session, enter: host# telnet <IP address> Read your <i>User's Guide</i> thoroughly.
[]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	host# ls [-a]

Contacting Alteon WebSystems

Use the following information to access Alteon WebSystems' support and sales.

- URL for Alteon WebSystems Online:

<http://www.alteonwebsystems.com>

This website includes product information, software updates, release notes, and white papers. The website also includes access to Alteon WebSystems Customer Support for accounts under warranty or covered by a maintenance contract.

- E-mail access:

support@alteonwebsystems.com

E-mail access to Alteon WebSystems Customer Support is available for accounts under warranty or covered by a maintenance contract.

- Telephone access to Alteon WebSystems Customer Support:

1-888-Alteon0 (or 1-888-258-3660)
1-408-360-5695

Telephone access to Alteon WebSystems Customer Support is available to accounts that are under warranty or covered by a maintenance contract. Normal business hours are 8 a.m. to 6 p.m. Pacific Standard Time.

- Telephone access to Alteon WebSystems Sales:

1-888-Alteon2 (or 1-888-258-3662), and press 2 for Sales
1-408-360-5600, and press 2 for Sales

Telephone access is available for information regarding product sales and upgrades.

Warranty

Alteon WebSystems provides a limited warranty on all its switches for a period of one year from the date of shipment. Free technical support and free replacement of hardware is provided for the first 90 days after shipment. You may choose to purchase additional service and support from Alteon WebSystems. Please contact your local sales representative for more information.



CHAPTER 1

Introducing the iSD100-SSL

The Integrated Service Director (iSD100-SSL) is a peripheral Secure Socket Layer (SSL) off-load platform that attaches to an Alteon WebSystems switch. The iSD100-SSL performs a TCP three-way handshake with the client through the Web switch and does all the SSL encryption and decryption for the session. This allows the switch to utilize load balancing features with encryption capabilities and to offload SSL encryption/decryption functions from servers.

Feature Summary

Hardware

- High-speed uplink port for non-intrusive integration with an Alteon WebSystems switch
 - Model iSD100-SSL-C1A—one 10/100Base-T port for copper Ethernet or Fast Ethernet at half or full duplex
 - Model iSD100-SSL-F2A—one 1000Base-SX port for fiber-optic Gigabit Ethernet
- 1U height, rack-mountable chassis
- Local console port (DCE) for system diagnostics
- TFTP download to Flash disk for software updates and upgrades

Software

- Accelerates SSL processing—works with the Web switch to offload SSL encryption and decryption from the server pool
- Supports SSL v3.0
- Supports up to 400 SSL transactions per second
- Supports certificate and key management—supports keys generated by Apache, Stronghold, and OpenSSL
- Supports up to 256 certificates
- Provides dynamic scalability—connect additional iSD100-SSLs to the Web switch to increase capacity
- Each Alteon WebSystems switch with Web OS software release 8.1 or higher supports up to 32 iSD100-SSL units, for a maximum of 12,800 SSL sessions per second
- Provides automatic failover of switch and SSL offload device
 - Supports TCP health checks
 - N+1 availability
- Intelligent Setup—The iSD100-SSL's self-configuration negotiates its IP address from the Web switch for simplified system integration.
- Dynamic Plug and Play—Once configured, a group of iSD100-SSLs can be dynamically connected or disconnected from an Alteon switch without disrupting network traffic.
- Seamless Management—The iSD100-SSL is configured through the Web switch Command Line Interface (CLI). This provides one central interface to configure and monitor both devices.
- Secure Management—The iSD100-SSL can be accessed only through the Web switch. The iSD100-SSL also performs access authentication, which validates authorization by administrators and system engineers, and accepts only authorized CLI commands.

Physical Description

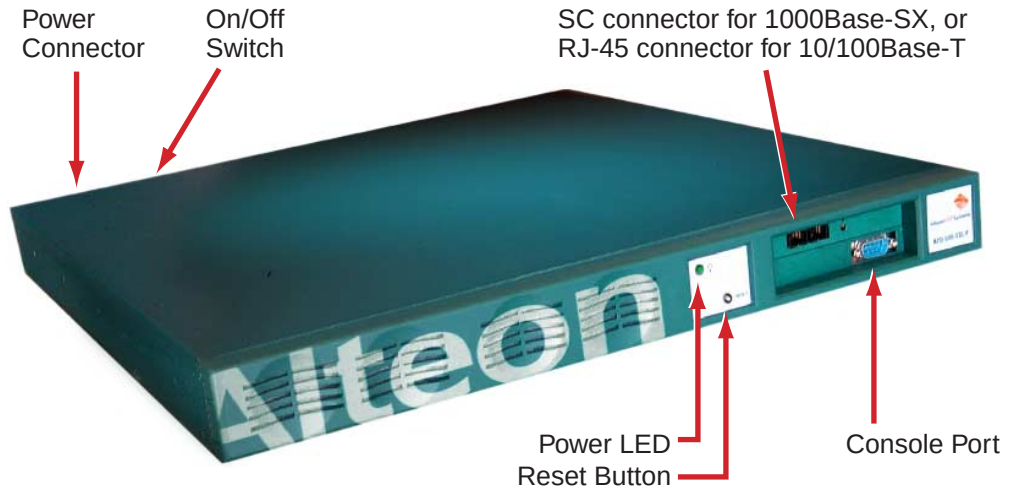


Figure 1 Physical Layout of the iSD100-SSL

Front Panel

- Network uplink port
 - Model iSD100-SSL-C1A—one 10/100Base-T port for copper (RJ-45 connector) Ethernet/Fast Ethernet at half or full duplex
 - Model iSD100-SSL-F2A—one 1000Base-SX port for fiber-optic (SC connector) Gigabit Ethernet
- LEDs for uplink port

See [Table 2 on page 23](#) and [Table 4 on page 24](#) for LED state information.
- Console port

The female DB-9 serial connector, labeled “Console,” can be used for DCE access to system diagnostics.
- Power LED lights up to indicate that the iSD100-SSL is on and receiving power.
- Reset button
- Air vents

Rear Panel

- Power on/off switch
- A/C power connector

Basic Operation

The following diagram and steps describe basic iSD100-SSL operation. For an overview of encryption systems in general, see [Appendix A, “Theory of Operation.”](#)

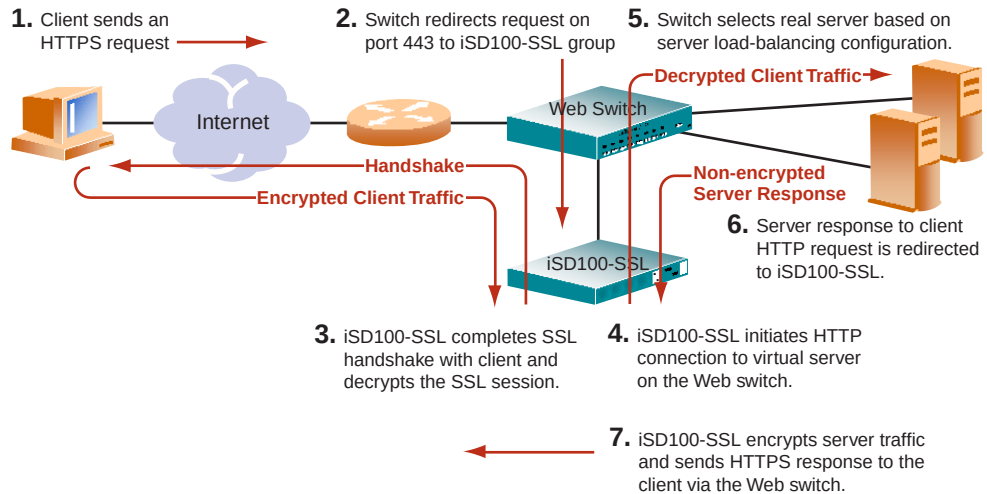


Figure 2 Basic iSD100-SSL Offload Operation

1. Client requests secure information via HTTPS.

When the client requires secure information, their Web browser sends a Hypertext Transfer Protocol Secure (HTTPS) request on TCP port 443. This request arrives at the Web switch connected to the server containing the desired information.

2. The Web switch redirects the request to the iSD100-SSL group.

The Web switch recognizes HTTPS traffic on port 443 and redirects the request to an iSD100-SSL device. This form of application redirection is described in detail in your *Web OS Application Guide*.

3. The iSD100-SSL completes the SSL handshake and decrypts the session.

The iSD100-SSL responds to the client's HTTPS request via the Web switch and starts the SSL session.

4. The iSD100-SSL initiates HTTP connection to the virtual server.

The iSD100-SSL receives the client's encrypted SSL traffic via the Web switch. The iSD100-SSL decrypts the secure traffic and forwards it as a regular HTTP request to a virtual server on the Web switch. The iSD100-SSL ensures that the source IP address of the client is preserved.

5. The Web switch selects a real server based on configured load-balancing options.

Based on criteria such as server health status and configured load-balancing distribution metrics, the Web switch selects a real server and forwards the client's decrypted HTTP traffic.

6. The server processes the HTTP request and replies to the client.

The server sends the requested non-encrypted HTTP information intended for the client's IP address. The Web switch redirects this traffic to the iSD100-SSL device.

7. The iSD100-SSL encrypts the server traffic and sends the HTTPS response to the client via the Web switch.



CHAPTER 2

Installing the iSD100-SSL Hardware

This chapter describes the physical installation of the iSD100-SSL. It provides step-by-step directions to rack mount or table mount the iSD100-SSL.

The iSD100-SSL is shipped with the following items:

- A/C power cord
- Console cable
- Two mounting brackets for rack mounting
- Six Phillips screws for installing the mounting brackets
- Four rubber feet for tabletop placement of the iSD100-SSL
- A user's manual

Installation involves the following tasks:

- Unpacking the iSD100-SSL
- Mounting the iSD100-SSL
- Connecting the iSD100-SSL to the Alteon WebSystems switch
- Connecting the power cord and plugging it into a power outlet
- Powering on the device

System Requirements

The iSD100-SSL is not a stand-alone device. To operate properly, it requires an Alteon Web-Systems switch running Web OS 8.1 (or higher) software.

Preparing for Installation

Before installing the iSD100-SSL:

1. **Unpack the unit from the shipping box.**
2. **Turn the power switch to the OFF (O) position.**
3. **Choose a suitable location to install the unit.**



CAUTION—Observe the following precautions when selecting a site and installing the iSD100-SSL:

Make sure the device is properly grounded electrically and power connections are safe, particularly when using power strips.

Avoid overloading your electrical supply circuits. Electrical ratings are printed on the name-plates of all your equipment. Be sure that your supply circuits and wiring can support the rated power draw of whatever equipment is used.

The ambient temperature of an operating iSD100-SSL must not exceed 40°C. When installing the device in a closed or multi-unit rack assembly, please consider that the operating ambient temperature of the equipment may be higher than the ambient temperature of the room. Take appropriate steps to ensure that the device does not overheat.

For proper air circulation, the vents on the front, back, and sides of the device should not be blocked or obstructed by cables, panels, rack frames, or other materials.

Do not place or rack-mount the device in any way which would exceed the maximum weight-bearing capacity of the surface or rack or cause potentially hazardous uneven mechanical loading.

Mounting the iSD100-SSL

Always observe the precautions outlined in the manuals for this and all other equipment you are installing.

Determine whether the unit will be mounted into an equipment rack or placed free-standing on a shelf or tabletop. The following sections detail each type of installation.

Rack-Mounting the Unit

NOTE – Do not use the included rubber feet for a rack installation.

1. As shown in [Figure 3](#), connect the two mounting brackets to the iSD100-SSL using the supplied screws.

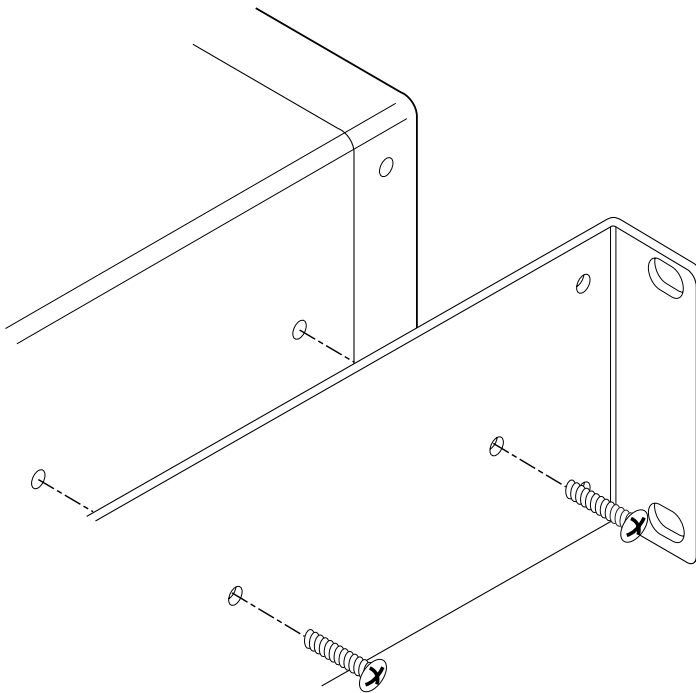


Figure 3 Position Mounting Brackets for Rack Mount

2. Mount the iSD100-SSL, as shown in [Figure 4](#), using the appropriate screws for your rack-mount system (four 10-32, 12-24, M5X.8-6H, or M6X1-6H type screws are suggested).

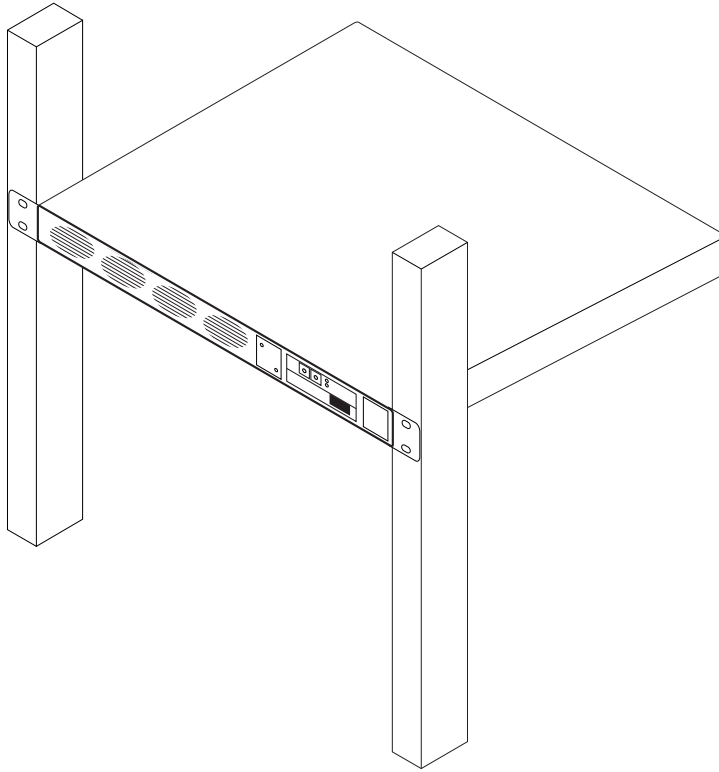


Figure 4 Rack-Mounted iSD100-SSL

Table-Mounting the Unit

1. Attach the four rubber feet and screws to the bottom of the switch.
2. Place the switch on a level tabletop or equipment shelf.

Connecting Network Cables

The iSD100-SSL high-speed uplink port must be connected to an Alteon WebSystems switch running Web OS 8.1 (or higher) software. The type and method of cabling depends on your particular model of iSD100-SSL:

- Model iSD100-SSL-C1A has one 10/100Base-T port for copper Ethernet or Fast Ethernet.
- Model iSD100-SSL-F2A has one 1000Base-SX port for fiber-optic Gigabit Ethernet.

Cable connections for both models are described below.

10/100Base-T Port (Model iSD100-SSL-C1A)

Model iSD100-SSL-C1A uses an RJ-45 copper connector for 10/100 Mbps (Fast Ethernet).

This port is auto-negotiating and supports half- and full-duplex operation. It is designed to operate with UTP Category 5 cables.

Use a straight-through cable when connecting the iSD100-SSL to a Web switch, hub, or router.

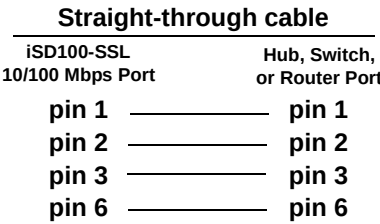


Figure 5 Pin assignments for 10/100 Mbps port cables

[Table 2](#) describe the states of the uplink LEDs.

Table 2 iSD100-SSL-C1A Uplink Port LEDs

LED	State	Description
Data	Blinking Off	Data is detected on the port. No data is detected on the port.
10	On Off	Good 10 Mbps Ethernet link established. No 10 Mbps link established (possible link at different speed, possible bad cable, bad connector, or configuration mismatch).
100	On Off	Good 100 Mbps Fast Ethernet link established. No 100 Mbps link established (possible link at different speed, possible bad cable, bad connector, or configuration mismatch).

1000Base-SX Port (Model iSD100-SSL-F2A)

Model iSD100-SSL-F2A uses an SC fiber-optic connector for 1000 Mbps (Gigabit Ethernet). The figure below illustrates an SC-type connector:

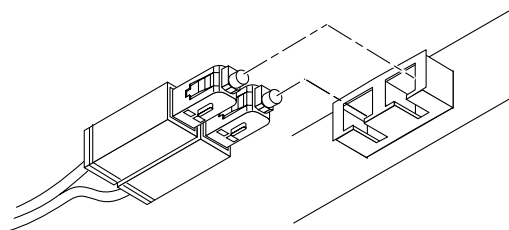


Figure 6 Fiber Optic Connector for the iSD100-SSL-F2A

The 1000Base-SX port is designed to operate with multi-mode fiber-optic cables. [Table 3](#) lists the cable characteristics for this port.:

Table 3 1000Base-SX Link Characteristics

Description	62.5 Micron	50 Micron
	Shortwave (850 nm multimode fiber)	
Operating Range	2-260 meters	2-550 meters (in compliance with IEEE 802.3z)

[Table 4](#) describe the states of the uplink LEDs.

Table 4 iSD100-SSL-F2A Uplink Port LEDs

LED	State	Description
Data	Blinking	Data is detected on the port.
	Off	No data is detected on the port.
Link	On	Good link established.
	Off	No link established (possible bad cable or bad connector).
	Blinking	Port has been disabled by software.

The Console Port

The iSD100-SSL console port is used only for system diagnostics and does not accept iSD100-SSL configuration commands. For information on gathering system diagnostics, see [“Console Diagnostics” on page 72](#).

Configuration for the iSD100-SSL is performed through the Web switch to which the unit is attached. For more information, see [Chapter 3, “Initial Setup”](#) and [Chapter 4, “iSD100-SSL Command Reference.”](#)

Power

Connecting the Power Cord

1. **Verify that the iSD100-SSL power switch (on back of the unit) is in the OFF (O) position.**
2. **Connect the power cord to the A/C power connector on the back of the unit.**
3. **Plug the cord into a properly fused outlet.**

Turning Power On/Off

Power is off when the power switch (on back of the unit) is in the O position.

To turn power on, move the power switch to the | position. The power LED lights up to indicate that the iSD100-SSL is on and receiving proper power.



CHAPTER 3

Initial Setup

This chapter covers the basic setup and initialization process for the iSD100-SSL and provides detailed instructions for updating the iSD100-SSL software when necessary.

Initializing the iSD100-SSL

The initialization process requires configuring an Alteon WebSystems switch to work with its attached iSD100-SSL units. The configuration steps are described below:

- 1. Verify the proper installation of the iSD100-SSL and Web switch hardware.**

The iSD100-SSL hardware must be installed and connected to an operating Alteon WebSystems switch. This installation includes:

- Mounting the iSD100-SSL chassis
- Connecting the iSD100-SSL uplink port to a compatible port on the Web switch
- Turning on power to the iSD100-SSL

For details on installing the iSD100-SSL hardware, see [Chapter 2](#) in this manual. For information on installing the required Alteon WebSystems switch, see your Web switch manuals.

- 2. Access the Web switch Command Line Interface (CLI).**

See your Web switch manuals for connecting to the Web switch and accessing the CLI.

- 3. From the CLI, assign an IP interface for communication between the Web switch and iSD100-SSL(s).**

```
# /cfg/ip/if <interface number [1-256]>  
> IP Interface# addr <IP address>
```

NOTE – The IP address for the IP interface must be on the same subnet as the IP addresses for the iSD100-SSL units configured in the following steps.

4. Enter the starting IP address (`ipstrt`) for the iSD100-SSL unit(s).

```
# /cfg/isd/ipstrt <IP address>
```

Specify the IP address to be assigned to the first iSD100-SSL unit. This IP address must be on the same subnet as the IP interface configured in the previous step. For example, if the IP interface was configured for 10.1.1.1, the iSD100-SSL `ipstrt` could be set to 10.1.1.10.

5. Set the number of iSD100-SSLs (`ipnum`) attached to the Web switch.

```
> isd# ipnum <number of iSD100-SSL units (0-32)>
```

Up to 32 iSD100-SSL units may be assigned per Web switch. Each iSD100-SSL will be automatically assigned the next highest IP address defined by `ipstart`.

For example, if `ipnum` is set to 2 and `ipstrt` is set to 10.1.1.10, the switch automatically assigns consecutive IP addresses for the two iSD100-SSL units to 10.1.1.10 and 10.1.1.11.

If only one iSD100-SSL is attached to the switch, `ipnum` will be 1, and the IP address assigned with `ipstrt` will be used as the default IP address of the iSD100-SSL unit.

NOTE – All IP addresses generated using `ipnum` must be on the same subnet as the IP interface configured for communication between the Web switch and iSD100-SSL units.

6. Turn on the iSD feature and apply the settings.

```
> isd# on
> isd# apply
```

Turning the iSD100-SSL on through the CLI executes the iSD100-SSL bootstrap code. The bootstrap code on each iSD100-SSL requests an IP address from the switch. The Alteon-specific Bootp server on the Web switch then assigns an IP address to each iSD100-SSL.

Once IP addresses have been assigned to the iSD100-SSL(s), the switch automatically performs the following functions:

- Automatically assigns a real server number for each iSD100-SSL, starting backwards from 255 (for example, for two iSD100-SSLs, real server numbers 255 and 254 are used)
- Automatically assigns real server group number 256 to the iSD100-SSLs
- Dynamically checks the system health
- Assigns a metric to balance the load among the iSD100-SSLs in the group
- Creates a table entry to track iSD100-SSLs in the group

7. **Ensure that the maximum number of connections (maxcon) for each iSD100-SSL is less than 7,500.**

Each iSD100-SSL can process up to 7,500 sessions per second. Make sure that all iSD100-SSL units assigned to real server numbers are configured with a **maxcon** limit of less than 7,500.

For example, if two iSD100-SSLs are used, real server numbers 255 and 254 are assigned, and **maxcon** limits would need to be configured as follows:

```
# /cfg/slb/real 255/maxcon 7450      (Set limit for first iSD100-SSL)
> Real Server 255# ../real 254/maxcon 7450 (Set limit for next iSD100-SSL)
```

8. **Apply and save the settings.**

```
# apply
# save
```

For further details about iSD100-SSL menu commands, see [Chapter 4, “iSD100-SSL Command Reference.”](#) For examples on configuring the iSD100-SSL to meet specific network needs, see [Chapter 5, “iSD100-SSL Sample Applications.”](#)

Updating the Software

The iSD100-SSL software is stored in compact Flash, making it easy to update and upgrade software via TFTP.

Updating the iSD100-SSL software requires a valid iSD100-SSL software image stored on a TFTP server. All iSD100-SSL units attached to an Alteon WebSystems switch are updated simultaneously using the following CLI commands:

1. **On the Web switch CLI, access the iSD100-SSL configuration menu.**

```
# /cfg/isd/ssl
```

2. **Initiate a software update for the iSD100-SSLs.**

```
# update
```

3. **When prompted, enter the IP address of the TFTP server where the iSD100-SSL software image is stored.**

For example:

```
Enter IP address of remote TFTP server: 169.172.21.184
```

4. **The iSD100-SSLs will finish downloading the software update and automatically reboot.**

CHAPTER 4

iSD100-SSL Command Reference

This chapter describes how to use the Web switch Command Line Interface (CLI) for making, viewing, and saving iSD100-SSL configuration changes.

For details on configuring other Web switch features (such as server load balancing, filters, and application redirection), see the *Web OS Command Reference* and *Web OS Application Guide*.

Accessing the Menu System

The iSD100-SSL has no user interface of its own and cannot be configured through its console port. Instead, iSD100-SSL configuration is performed using the standard CLI on the Alteon WebSystems switch, which is connected to the iSD100-SSL.

This documentation assumes that the administrator has access to the Web switch CLI prompt. For details on how to access the Web switch CLI, see your *Web OS Command Reference*.

When first logged in to the Web switch, the administrator will see the Main Menu and prompt:

```
[Main Menu]
  info      - Information Menu
  stats     - Statistics Menu
  cfg       - Configuration Menu
  oper      - Operations Command Menu
  boot      - Boot Options Menu
  maint     - Maintenance Menu
  diff      - Show pending config changes [global command]
  apply     - Apply pending config changes [global command]
  save      - Save updated config to FLASH [global command]
  revert    - Revert pending or applied changes [global command]
  exit      - Exit [global command, always available]
```

```
>> Main #
```

The iSD100-SSL menus can be accessed through the switch `info` menu (see [page 35](#)) and the `cfg` menu (see [page 32](#)).

/cfg/isd

iSD Menu

The iSD Menu is used for setting basic parameters for all iSD100-SSL devices. Once you have logged in as an administrator, this menu can be accessed using the following command:

```
# /cfg/isd
```

The iSD Menu is displayed below:

```
[isd Menu]
ssl      - SSL Offload Menu
ipstrt   - Set starting IP address for isd servers
ipnum    - Set number of isd servers
vrnum    - Set VRRP virtual interface router number to bind with
on       - Turn IP address assignment ON
off      - Turn IP address assignment OFF
cur      - Display current isd server configuration
```

Table 5 explains the available configuration options and parameters:

Table 5 iSD Menu Options (/cfg/isd)

Command Syntax and Usage

ssl

Displays the SSL Offload Application Menu. To view menu options, refer to [page 33](#).

ipstrt <IP address (eg, 192.4.17.101)>

Set the starting IP address for iSD100-SSL units.

ipnum <number (0-32), 0 to disable the IP address assignment for iSD units>

Set the number of iSD100-SSL units. If **ipstrt** is set at 192.4.17.101 and **ipnum** is 3, then the iSD100-SSLs attached to the switch will be numbered 192.4.17.101, 192.4.17.102, and 192.4.17.103.

vrnum <1-256>

Set the virtual router number to bind with the Web switch. This number must correspond to the virtual router of the Web switch that connects to the iSD100-SSL. For more information about virtual routers, see the **/cfg/vrrp/vr** command in the *Web OS Command Reference*.

Table 5 iSD Menu Options (/cfg/isd)**Command Syntax and Usage****on**

Globally turns on all iSD100-SSL processing. This enables the switch to assign IP addresses automatically and manage the iSD100-SSL units.

off

Globally turn all iSD100-SSL processing off. When iSD100-SSL processing is turned off, HTTPS traffic will be forwarded to the real Web server without being redirected to an iSD100-SSL. However, the real Web server must be configured to listen to HTTPS traffic on port 443.

cur

Display current iSD100-SSL configuration.

/cfg/isd/ssl

SSL Offload Application Menu

The SSL Offload Application Menu is used for configuring SSL certificates and iSD100-SSL ports, upgrading iSD100-SSL software, and resetting iSD100-SSL devices.

This menu can be accessed from the Web switch CLI prompt using the following command:

```
# /cfg/isd/ssl
```

The SSL Offload Application Menu is displayed below:

```
[SSL Offload Application Menu]
addcrt  - Add certificate for a virtual IP address
tftpcrt - Tftp certificate from remote machine
remcrt  - Remove certificate for a virtual IP address
lstcrt  - List certificate for a virtual IP address
lstip   - List all configured virtual IP addresses
setport - Set port for isd-server communication
lstport - List port for isd-server communication
update  - Update the isd software
shutdn  - Shutdown (halt or reboot) isd
```

Table 6 explains the available configuration options and parameters.

Table 6 iSD Configuration Menu Options (/cfg/isd/ssl)

Command Syntax and Usage

addcrt

Add a virtual IP address of a certificate to the iSD100-SSLs. Enter the virtual IP address of the certificate, then cut and paste the contents of the certificate at the prompt. Finally, type three periods (. . .) on a new line to denote the end of the certificate.

tftpport

Get a certificate using TFTP. Enter an IP address of a TFTP server that has the certificate you want. Then, enter the virtual IP address of the certificate filename.

remcrt

Remove a certificate from the iSD100-SSLs. Enter the virtual IP address of the certificate you want to remove.

lscrt

Display a certificate by entering the virtual IP address for the certificate. The contents of the certificate are displayed.

lstip

List all virtual IP addresses for which certificates have been configured on the group of iSD100-SSLs.

setport

Set the port for communication between the iSD100-SSLs and the real Web servers. Enter the port number (usually port 81) at which the iSD100-SSLs contact the real Web servers via plain HTTP. All the real Web servers and iSD100-SSLs should be configured to the same port. This command can be used for security against direct access to secure Web pages.

lstport

List the port for communication between the iSD100-SSL and the real Web server. This shows the port that was set using the **setport** command (usually port 81).

update

Update or upgrade all iSD100-SSL software via TFTP. Enter the IP address of the remote TFTP server where the iSD100-SSL software image is stored. This command will upgrade all iSD100-SSLs that are connected to the Web switch.

shutdn <IP address of iSD100-SSL | **all**>

Shutdown/Reboot one or more iSD100-SSLs that are connected to the Web switch.

/info/isd

iSD Information Command

To display switch information regarding all iSD100-SSL devices, enter the following command at the switch CLI prompt:

```
# /info/isd
```

The iSD information is displayed below:

```
Current isd server configuration:
  10.0.1.10, 1, 0, ON
isd BOOTP server: ON
isd master IP: 10.0.1.10
Network interface for isd: 2
Current isd servers:
state   isd IP       mac_addr      life
-----
  2     10.0.1.10   00:01:02:08:4d:1c  8676

isd system status:
  Total Memory:    264507392
  Free Memory:     252874752
  Buffer Memory:    335872
  Blocks Written:   0
  Blocks Read:      0
  Interrupts:       108
  Context Switches: 20
  User Time:        0
  System Time:      1
  Idle Time:        99
  System status averaged over 3 seconds

isd free disk space:
  total disk size: 50685K
  free disk size: 21671K

SSL app status:
  total connections   = 0
  running threads     = 7
  current connections = 0
  maximum connections = 0
```

Figure 7 iSD100-SSL Information

Table 7 describes the iSD100-SSL information output:

Table 7 /info/isd Output

Parameter	Description
Current isd server configuration	This line contains the following data about basic iSD100-SSL configuration: ■ Starting IP address (<code>ipstart</code>) of the iSD100-SSL units ■ Number of iSD100-SSL units (<code>ipnum</code>) configured on the switch ■ Virtual router number (<code>vrnum</code>) ■ State of Web switch iSD100-SSL processing, on or off.
isd BOOTP server	State of the BOOTP server which assigns IP addresses to the iSD100-SSL: on or off.
isd master IP	IP address of the Master iSD100-SSL.
Network interface for isd	The IP interface configured for communication between the Web switch and the iSD100-SSL.
Current isd servers	There is one line for each configured iSD100-SSL, with the following data: ■ <code>state</code> 2 means that IP address has been assigned. ■ <code>isd IP</code> The IP address assigned to the iSD100-SSL. ■ <code>mac_addr</code> The MAC address of the iSD100-SSL. ■ <code>life</code> This represents the number of milliseconds since the iSD100-SSL sent a signal to the Web switch. If <code>life</code> exceeds 120,000 ms, the switch considers the iSD100-SSL to be down, and no further traffic will be directed to that iSD100-SSL until it comes back up. If the down iSD100-SSL is a Master, the switch will select another Master iSD100-SSL. If no other iSD100-SSL units are up and available, HTTPS traffic will be sent directly to the real Web servers on port 443.
isd system status	Memory and time usage characteristics averages over three seconds.
isd free disk space	Total and available disk space available on the iSD100-SSL.
SSL app status	SSL connection and thread information.



CHAPTER 5

iSD100-SSL Sample Applications

This chapter describes some basic network applications that make use of the iSD100-SSL:

- Web Server Accelerator, using two or more load-balanced iSD100-SSLs for SSL offload
- Content-Intelligent Switching for Secure Sessions, using single or multiple iSD100-SSLs for SSL offload with cookie processing
- Redundant Active-Standby Configuration, using multiple iSD100-SSLs for high-availability scenarios

The sample configurations discussed are merely recommendations and are not required. However, each example is based on the configuration described in [“Web Server Accelerator” on page 38](#). Therefore, it is recommended that you read this chapter in sequence, and modify the base configuration as noted in each subsequent example.

Because all iSD100-SSL configuration is performed through the Web switch, the procedures outlined in this chapter presume that you are connected to the Web switch and have access to the Command Line Interface (CLI) prompt. For detailed information about accessing the CLI prompt, refer to the *Web OS Command Reference*.

Web Server Accelerator

Figure 8 illustrates the most common network configuration for the iSD100-SSL. This configuration example consists of two iSD100-SSLs, a Web switch and two servers.

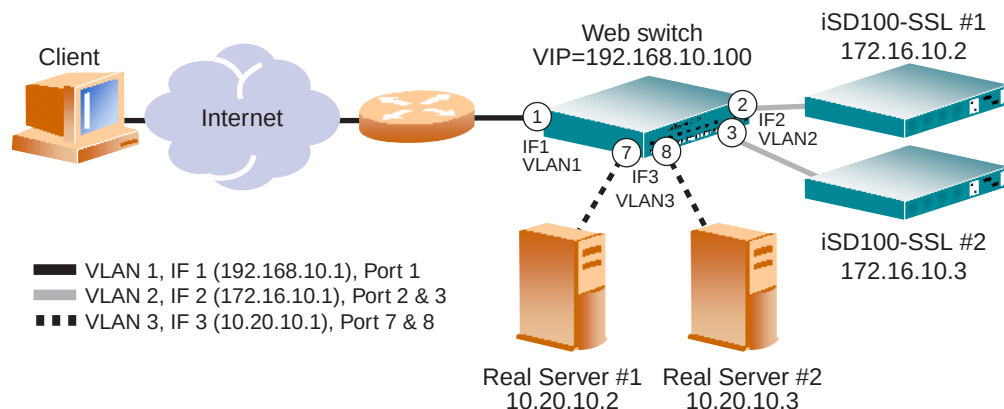


Figure 8 Sample Web Server Accelerator Network Using Multiple iSD100-SSLs

Create the Necessary VLANs

In this configuration, there will be three VLANs: VLAN 1 for the Web switch that connects to the Internet, VLAN 2 for the iSD100-SSL units, and VLAN 3 for the real servers. Since VLAN 1 is the default, only VLAN 2 and VLAN 3 require additional configuration.

1. **Configure VLAN 2 to include Web switch ports leading to the iSD100-SSL units.**

<code>/cfg/vlan 2</code>	<i>(Select VLAN 2)</i>
<code>add 2</code>	<i>(Add the port for the first iSD100-SSL)</i>
<code>y</code>	<i>(Enter y to confirm adding port 2)</i>
<code>add 3</code>	<i>(Add the port for the second iSD100-SSL)</i>
<code>y</code>	<i>(Enter y to confirm adding port 3)</i>
<code>ena</code>	<i>(Enable VLAN 2)</i>

2. Configure VLAN 3 to include Web switch ports leading to the real servers.

<code>/cfg/vlan 3</code>	<i>(Select VLAN 3)</i>
<code>add 7</code>	<i>(Add the port for the first real server)</i>
<code>y</code>	<i>(Enter y to confirm adding port 7)</i>
<code>add 8</code>	<i>(Add the port for the second real server)</i>
<code>y</code>	<i>(Enter y to confirm adding port 8)</i>
<code>ena</code>	<i>(Enable VLAN 3)</i>

3. Disable Spanning Tree Protocol (STP) for the iSD100-SSL and real server ports.

STP will not function across multiple VLANs.

<code>/cfg/stp/port 2</code>	<i>(Select STP port 2 menu for iSD100-SSL 1)</i>
<code>off</code>	<i>(Turn STP off for port 2)</i>
<code>../port 3</code>	<i>(Select STP port 3 menu for iSD100-SSL 2)</i>
<code>off</code>	<i>(Turn STP off for port 3)</i>
<code>../port 7</code>	<i>(Select STP port 7 menu for real server 1)</i>
<code>off</code>	<i>(Turn STP off for port 7)</i>
<code>../port 8</code>	<i>(Select STP port 8 menu for real server 2)</i>
<code>off</code>	<i>(Turn STP off for port 8)</i>

Configure One IP Interface for Each VLAN

1. Configure an IP interface for client traffic on the Web switch.

The subnet mask for IP interface 1 will be automatically assigned.

<code>/cfg/ip/if 1</code>	<i>(Select IP interface 1 for client traffic)</i>
<code>addr 192.168.10.1</code>	<i>(Set the IP address for IP interface 1)</i>
<code>ena</code>	<i>(Enable IP interface 1)</i>

2. Configure an IP interface for iSD100-SSL traffic.

The subnet mask for IP interface 2 will be automatically assigned.

<code>/cfg/ip/if 2</code>	<i>(Select IP interface 2 for iSD100-SSLs)</i>
<code>addr 172.16.10.1</code>	<i>(Set the IP address for IP interface 2)</i>
<code>vlan 2</code>	<i>(Set the iSD100-SSL VLAN number)</i>
<code>ena</code>	<i>(Enable IP interface 2)</i>

3. Configure an IP interface for the real server traffic.

<code>/cfg/ip/if 3</code>	<i>(Select IP interface 3 for real servers)</i>
<code>addr 10.20.10.1</code>	<i>(Set the IP address for IP interface 3)</i>
<code>mask 255.255.255.0</code>	<i>(Set the subnet mask for IP interface 3)</i>
<code>vlan 3</code>	<i>(Set the real server VLAN number)</i>
<code>ena</code>	<i>(Enable IP interface 3)</i>

4. Apply the changes.

<code>apply</code>	<i>(Make your changes active)</i>
--------------------	-----------------------------------

Configure Server Load Balancing Parameters

1. Set and enable the IP addresses of the real servers.

<code>/cfg/slb/real 1</code>	<i>(Select real server 1)</i>
<code>rip 10.20.10.2</code>	<i>(Set the IP address for real server 1)</i>
<code>ena</code>	<i>(Enable real server 1)</i>
<code>../real 2</code>	<i>(Select real server 2)</i>
<code>rip 10.20.10.3</code>	<i>(Set the IP address for real server 2)</i>
<code>ena</code>	<i>(Enable real server 2)</i>

2. Add real servers 1 and 2 to real server group 1.

<code>/cfg/slb/group 1</code>	<i>(Select real server group 1)</i>
<code>add 1</code>	<i>(Add real server 1 to the group)</i>
<code>add 2</code>	<i>(Add real server 2 to the group)</i>

3. Set and enable the virtual IP address for virtual server 1 (the Web switch).

<code>/cfg/slb/virt 1</code>	<i>(Select virtual server 1)</i>
<code>vip 192.168.10.100</code>	<i>(Set the virtual IP address for virtual server 1)</i>
<code>ena</code>	<i>(Enable virtual server 1)</i>
<code>service 81</code>	<i>(Enable service on port 81, for communication between the iSD100-SSL, the virtual server, and the real server)</i>
<code>apply</code>	<i>(Make your changes active)</i>

4. Enable client processing on port 1 leading to the Internet.

<code>/cfg/slb/port 1</code>	<i>(Select port 1 leading to the Internet)</i>
<code>client ena</code>	<i>(Enable client processing on port 1)</i>

5. Enable client processing on ports leading to iSD100-SSLs.

<code>/cfg/slb/port 2</code>	<i>(Select SLB port 2 for iSD100-SSL 1)</i>
<code>client ena</code>	<i>(Enable client processing on port 2)</i>
<code>../port 3</code>	<i>(Select SLB port 3 for iSD100-SSL 2)</i>
<code>client ena</code>	<i>(Enable client processing on port 3)</i>

6. Enable server processing on ports leading to real servers.

<code>/cfg/slb/port 7</code>	<i>(Select port 7 for real server 1)</i>
<code>server ena</code>	<i>(Enable server processing on port 7)</i>
<code>../port 8</code>	<i>(Select port 8 for real server 2)</i>
<code>server ena</code>	<i>(Enable server processing on port 8)</i>

7. Turn on Layer 4 processing.

<code>/cfg/slb/on</code>	<i>(Activate Layer 4 software)</i>
--------------------------	------------------------------------

Configure Basic iSD100-SSL Parameters

1. Set the basic IP address information for the iSD100-SSL units.

<code>/cfg/isd</code>	<i>(Select the iSD100 configuration menu)</i>
<code>ipstrt 172.16.10.2</code>	<i>(Set the start IP address for iSD100-SSLs)</i>
<code>ipnum 2</code>	<i>(Set the number of iSD100-SSL servers)</i>
<code>on</code>	<i>(Turn on iSD100-SSL address assignment)</i>

2. Check that the iSD100-SSLs are active.

<code>/info/isd</code>	<i>(Display information about iSD100-SSLs)</i>
------------------------	--

The iSD100-SSLs should show state 2 when active.

```

Current isd server configuration:
  172.16.10.2, 2, 0, ON
isd BOOTP server: ON
isd master IP: 172.16.10.2
Network interface for isd: 2
Current isd servers:
  state   isd IP           mac_addr           life
  ----   -
      2    172.16.10.2      00:01:02:08:70:cd    7636
      2    172.16.10.3      00:01:02:08:4d:1c   8148320

isd system status:
  Total Memory:      264507392
  Free Memory:       235876352
  Buffer Memory:     16990208
  Blocks Written:    0
  Blocks Read:       0
  Interrupts:        116
  Context Switches:  113
  User Time:         0
  System Time:       1
  Idle Time:         98
  System status averaged over 3 seconds

isd free diskspace:
  total disk size: 15351K
  free disk size:  15084K

SSL app status:
  total connections   = 0
  running threads     = 7
  current connections = 0
  maximum connections = 0

```

NOTE – The first time you type in `info/isd`, you may see a refused connection because the switch may not yet be communicating with the iSD100-SSL. It takes 10 to 15 seconds before the iSD100-SSL is ready.

3. Define a TCP port number for iSD100-SSL traffic.

```
/cfg/isd/ssl/setport 81
```

(Set port 81 for iSD100-SSL traffic to the real web server)

This defines the port (81) that is used by the iSD100-SSL to send and receive decrypted HTTP information to and from the Web switch. This port must be different from ports used by other services.

NOTE – As in [Step 3. on page 40](#), the real web server must also be set up to listen for iSD100-SSL traffic on port 81.

4. Apply the changes.

```
apply
```

(Make your changes active)

Add a Certificate to the iSD100-SSL

This step presumes that you have a Certificate Authority (CA) signed certificate with a private key. The process for obtaining the required certificate files is covered in [Appendix C, “Building Keys and Certificates.”](#)

Once you have the appropriate certificates, use the following procedure to add the certificate to the iSD100-SSL.

1. Initiate the certificate addition command.

```
/cfg/isd/ssl/addcrt
```

2. When prompted, enter the filename of the certificate. The certificate should be named with the virtual IP address assigned to the virtual server in [Step 3. on page 40](#).

```
192.168.10.100
```

(Filename of certificate)

3. Follow the onscreen instruction and perform a “copy and paste” to add the certificate.

When prompted for the certificate, follow the instructions on the screen. Use notepad or any other text editor to display the certificate. Then copy and paste the text of the private key and certificate into the terminal window.

Important—Once the paste function is completed, hit <Enter>, then enter three periods (. . .) on a new line. Then press <Enter> to exit the paste screen and complete the process.

NOTE – Under Microsoft Windows, hyperterminal may be slow to complete the copy and paste process.

Configure Filters

1. Create a filter to redirect client HTTPS traffic intended for port 443.

<code>/cfg/slb/filt 100</code>	<i>(Select filter 100)</i>
<code>proto tcp</code>	<i>(For TCP traffic)</i>
<code>dport https</code>	<i>(To an HTTPS destination port)</i>
<code>action redir</code>	<i>(Perform redirection)</i>
<code>group 256</code>	<i>(To the group reserved for iSD100-SSLs)</i>
<code>rport https</code>	<i>(And redirect to the HTTPS port)</i>
<code>adv/fwlb e</code>	<i>(Enable the firewall redirect hash method)</i>
<code>.. /ena</code>	<i>(Enable filter 1)</i>

This filter, when placed on the client port, intercepts incoming HTTPS traffic and redirects it to the iSD100-SSL group. The HTTP traffic filter should be given a high number, such as 100, so as not to interfere with other filters.

NOTE – Real server group 256 is reserved for iSD100-SSLs and is configured automatically.

2. Create a filter to deny client traffic intended for port 81.

<code>/cfg/slb/filt 3</code>	<i>(Select filter 3)</i>
<code>proto tcp</code>	<i>(For TCP traffic)</i>
<code>dport 81</code>	<i>(For traffic to destination port 81)</i>
<code>action deny</code>	<i>(Deny matching traffic)</i>
<code>ena</code>	<i>(Enable filter 3)</i>

This filter, when placed on the client port, blocks all incoming traffic destined for port 81. This is required to ensure that traffic from iSD100-SSL units outside your trusted network do not gain non-encrypted access to your real servers.

3. Create a default filter to allow all other traffic.

/cfg/slb/filt 224	<i>(Select filter 224)</i>
sip any	<i>(For traffic from any source IP address)</i>
dip any	<i>(To any destination IP address)</i>
proto any	<i>(Of any protocol)</i>
action allow	<i>(Allow matching traffic to pass)</i>
ena	<i>(Enable filter 224)</i>

4. Add the client filters to the port leading to the Internet.

/cfg/slb/port 1	<i>(Select the SLB port menu for port 1)</i>
add 1	<i>(Add the HTTPS redirect filter)</i>
add 3	<i>(Add the port 81 deny filter)</i>
add 224	<i>(Add the default allow filter)</i>
filt ena	<i>(Enable filtering on port 1)</i>

5. Add an additional filter to allow for real server health checks.

The health check filter should be given a smaller number (higher priority) than the redirection filter set in [Step 6. on page 46](#).

/cfg/slb/filt 150	<i>(Select filter 150)</i>
ena	<i>(Enable filter 150)</i>
action allow	
sip 192.168.10.100	<i>(Source IP must be the virtual IP address of the switch)</i>
smask 255.255.255.255	<i>(Set the source IP mask)</i>
dip 10.20.10.1	<i>(Destination IP must be the switch interface)</i>
dmask 255.255.255.255	<i>(Set the destination IP mask)</i>
proto tcp	<i>(For TCP traffic)</i>
sport 81	<i>(Set the switch to receive real server health checks on port 81)</i>
dport any	<i>(Set destination port to "any", because client traffic may enter on any port)</i>

6. Create a filter to redirect real server responses back to the iSD100-SSL.

/cfg/slb/filt 200	<i>(Select filter 200)</i>
proto tcp	<i>(For TCP traffic)</i>
sport 81	<i>(From source port 81)</i>
action redir	<i>(Perform redirection)</i>
group 256	<i>(To the group reserved for iSD100-SSLs)</i>
adv/fwlb e	<i>(Enable the firewall redirect hash method)</i>
../ena	<i>(Enable filter 2)</i>

7. Add the real server filter to the real server ports.

/cfg/slb/port 7	<i>(Select the SLB port menu for port 7)</i>
add 200	<i>(Add the redirect filter 200)</i>
add 224	<i>(Add the allow filter)</i>
filt ena	<i>(Enable filtering on port 1)</i>
../port 8	<i>(Select the SLB port menu for port 8)</i>
add 200	<i>(Add the redirect filter 200)</i>
add 224	<i>(Add the allow filter)</i>
filt ena	<i>(Enable filtering on port 1)</i>

Apply, Save, and Verify the Configuration

1. Apply and save the configuration changes.

apply	<i>(Make your changes active)</i>
save	<i>(Make your changes survive reboot)</i>

2. Verify SSL Offload is working.

Open a Web-browser from the client side of the network. Access the following URLs:

- **http://192.168.10.100**
- **https://192.168.10.100**

The second URL should prompt a security alert message.

Content-Intelligent Switching for Secure Sessions

The following example configures the Web switch to combine cookie-based persistence in the cookie rewrite mode with SSL offload through the iSD100-SSL. These steps assume that the network is already configured as described in [“Web Server Accelerator” on page 38](#).

1. **Connect to the Web switch CLI.**
2. **Enable Direct Access Mode for the Web switch.**

```
/cfg/slb/adv/direct ena
```

3. **Configure cookie options for the HTTP service on TCP port 81.**

<code>/cfg/slb/virt 1/service 81</code>	<i>(Select iSD100-SSL/server traffic)</i>
<code>pbind</code>	<i>(Set for persistent binding)</i>
<code>cookie</code>	<i>(Set for cookies)</i>
<code>rewrite</code>	<i>(Set for cookie rewrite mode)</i>

4. **Enter cookie name: *AlteonSession***
5. **Enter number of bytes to extract: 8**
6. **Look for cookie in URL e|d: dis**
7. **Apply the changes.**

<code>apply</code>	<i>(Make your changes active)</i>
<code>save</code>	<i>(Make your changes survive reboot)</i>

Redundant Active-Standby Configuration

The following steps are used for configuring a redundant active-standby configuration with two Web switches and two iSD100-SSLs, as illustrated below. It is assumed that the first Web switch is configured as in the example for “[Web Server Accelerator](#)” on page 38.

This configuration requires each iSD100-SSL to be connected to two Web switches. Because each iSD100-SSL has only one uplink port, a Layer 2 switch or hub must be placed between iSD100-SSLs and the Web switches. A Layer 2 switch or hub should also be placed between the real servers and web switches, and also between web switches and client.

Also note that port 3 on VLAN 2, and port 8 on VLAN 3 (configured in “[Web Server Accelerator](#)” on page 38) are not required for this example.

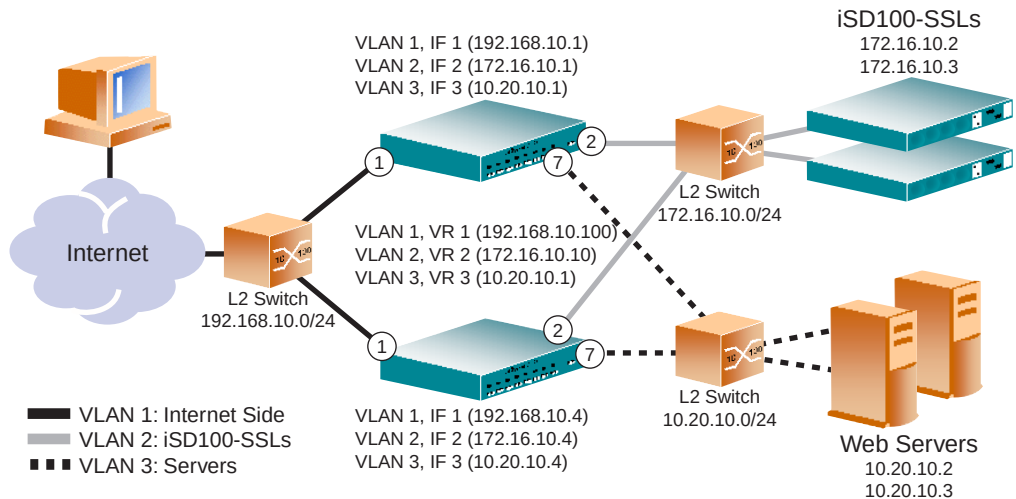


Figure 9 Redundant Active-Standby Configuration

In this process, the following tasks are performed:

- Create three IP interfaces on the second Web switch, each in a separate VLAN
- Enable VRRP and SLB on the Second switch
- Configure the SLB sync peer

On Web Switch 2, Create the Necessary VLANs

In this configuration, there will be three VLANs: VLAN 1 for the Web switch, VLAN 2 for the iSD100-SSL units, and VLAN 3 for the real servers. Since VLAN 1 is the default, only VLAN 2 and VLAN 3 require additional configuration.

1. **On the second switch, login as the administrator.**
2. **Configure VLAN 2 to include Web switch ports leading to the iSD100-SSL units.**

<code>/cfg/vlan 2</code>	<i>(Select VLAN 2)</i>
<code>add 2</code>	<i>(Add the port for the first iSD100-SSL)</i>
<code>add 3</code>	<i>(Add the port for the second iSD100-SSL)</i>
<code>ena</code>	<i>(Enable VLAN 2)</i>

3. **Configure VLAN 3 to include Web switch ports leading to the real servers.**

<code>/cfg/vlan 3</code>	<i>(Select VLAN 3)</i>
<code>add 7</code>	<i>(Add the port for the first real server)</i>
<code>add 8</code>	<i>(Add the port for the second real server)</i>
<code>ena</code>	<i>(Enable VLAN 3)</i>

4. **Disable Spanning Tree Protocol (STP) for the iSD100-SSL and real server ports.**

STP prevents loops in network topologies by removing redundant links. In active/standby configurations, STP would eventually kill all links between the iSD100-SSLs and Web switches. Therefore it must be disabled.

<code>/cfg/stp/port 2</code>	<i>(Select STP port 2 menu for iSD100-SSL 1)</i>
<code>off</code>	<i>(Turn STP off for port 2)</i>
<code>../port 7</code>	<i>(Select STP port 7 menu for real server 1)</i>
<code>off</code>	<i>(Turn STP off for port 7)</i>

Configure IP Interfaces for Each VLAN (Web Switch 2)

1. Configure an IP interface for client traffic on the Web switch.

<code>/cfg/ip/if 1</code>	<i>(Select IP interface 1 for client traffic)</i>
<code>addr 192.168.10.4</code>	<i>(Set the IP address for IP interface 1)</i>
<code>mask 255.255.255.0</code>	<i>(Set the subnet mask for IP interface 1)</i>
<code>ena</code>	<i>(Enable IP interface 1)</i>

2. Configure an IP interface for iSD100-SSL traffic.

<code>/cfg/ip/if 2</code>	<i>(Select IP interface 2 for iSD100-SSLs)</i>
<code>addr 172.16.10.2</code>	<i>(Set the IP address for IP interface 2)</i>
<code>mask 255.255.255.0</code>	<i>(Set the subnet mask for IP interface 2)</i>
<code>vlan 2</code>	<i>(Set the iSD100-SSL VLAN number)</i>
<code>ena</code>	<i>(Enable IP interface 2)</i>

3. Configure an IP interface for the real server traffic.

<code>/cfg/ip/if 3</code>	<i>(Select IP interface 3 for real servers)</i>
<code>addr 10.20.10.4</code>	<i>(Set the IP address for IP interface 3)</i>
<code>mask 255.255.255.0</code>	<i>(Set the subnet mask for IP interface 3)</i>
<code>vlan 3</code>	<i>(Set the real server VLAN number)</i>
<code>ena</code>	<i>(Enable IP interface 3)</i>

4. Apply the changes.

<code>apply</code>	<i>(Make your changes active)</i>
--------------------	-----------------------------------

Set Basic iSD100-SSL Parameters (Web Switch 2)

Set the basic IP address information the iSD100-SSL units.

<code>/cfg/isd</code>	<i>(Select the iSD100 configuration menu)</i>
<code>ipstrt 172.16.10.2</code>	<i>(Set the start IP address for iSD100-SSLs)</i>
<code>ipnum 2</code>	<i>(Set the number of iSD100-SSL servers)</i>
<code>off</code>	<i>(Turn off iSD100-SSL address assignment)</i>

Prepare to Receive Synchronization (Web Switch 2)

Synchronize the configuration between two Web switches.

1. Configure the synchronization parameters.

<code>/cfg/slb/sync</code>	<i>(Select the synchronization menu)</i>
<code>prios d</code>	<i>(Disable sync of VRRP priorities)</i>
<code>peer 1</code>	<i>(Select peer 1)</i>
<code>addr 192.168.10.1</code>	<i>(Set Web switch 1 IP interface as peer 1)</i>
<code>ena</code>	<i>(Enable the peer switch)</i>

2. Apply the configuration.

<code>apply</code>	<i>(Make your changes active)</i>
--------------------	-----------------------------------

On Web Switch 1, Configure VRRP

VRRP is configured for failover (redundancy) between two Web switches, in the event one of the Web switches fails.

1. On the second switch, login as the administrator.
2. Globally turn on the VRRP.

<code>/cfg/vrrp/on</code>

3. Configure virtual router 1.

<code>/cfg/vrrp/vr 1</code>	<i>(Select virtual router 1)</i>
<code>addr 192.168.10.100</code>	<i>(Set the IP address for virtual router 1)</i>
<code>if 1</code>	<i>(Set the IP interface number)</i>
<code>prio 101</code>	<i>(Set the priority to 101)</i>
<code>share dis</code>	<i>(Disable sharing)</i>
<code>track/14pts e</code>	<i>(Set the tracking option)</i>
<code>../ena</code>	<i>(Enable virtual router 1)</i>

4. Configure virtual router 2.

/cfg/vrrp/vr 2	<i>(Select virtual router 2)</i>
vrid 2	<i>(Set the virtual router ID)</i>
addr 172.16.10.10	<i>(Set the IP address for virtual router 2)</i>
if 2	<i>(Set the IP interface number)</i>
prio 101	<i>(Set the priority to 101)</i>
share dis	<i>(Disable sharing)</i>
track/14pts e	<i>(Set the tracking option)</i>
../ena	<i>(Enable virtual router 2)</i>

5. Configure virtual router 3.

/cfg/vrrp/vr 3	<i>(Select virtual router 3)</i>
vrid 3	<i>(Set the virtual router ID)</i>
addr 10.20.10.10	<i>(Set the IP address for virtual router 3)</i>
if 3	<i>(Set the IP interface number)</i>
prio 101	<i>(Set the priority to 101)</i>
share dis	<i>(Disable sharing)</i>
track/14pts e	<i>(Set the tracking option)</i>
../ena	<i>(Enable virtual router 2)</i>

Update VRRP Parameters for iSD100-SSL (Web Switch 1)**1. Turn on IP address assigning for the iSD100-SSL on Web switch 1.**

/cfg/isd/on

2. Set the Virtual Router Number.

/cfg/isd/vrnum 2	<i>(Set the virtual router number)</i>
-------------------------	--

3. Apply and save the configuration changes.

apply	<i>(Make your changes active)</i>
save	<i>(Make your changes survive reboot)</i>

Prepare and Send Synchronization (Web Switch 1)

1. Configure the Synchronization parameters.

/cfg/slb/sync	<i>(Select the synchronization menu)</i>
prios d	<i>(Disable sync of VRRP priorities)</i>
peer 1	<i>(Select peer 1)</i>
addr 192.168.10.4	<i>(Set Web switch 1 IP interface as peer 1)</i>
ena	<i>(Enable the peer switch)</i>

2. Apply and save the configuration changes.

apply	<i>(Make your changes active)</i>
save	<i>(Make your changes survive reboot)</i>

3. Synchronize server load balancing configuration on peers.

/oper/slb/sync	<i>(Initiate synchronization)</i>
-----------------------	-----------------------------------

At the prompt, enter IP address: **192.168.10.4**

On Web Switch 2, Update VRRP Parameters for iSD100-SSL

1. Turn on IP address assigning for the iSD100-SSL on Web switch 2.

/cfg/isd/on

2. Set the Virtual Router Number (VRN).

/cfg/isd/vrnum 2	<i>(Set the virtual router number)</i>
-------------------------	--

3. Apply and save the configuration changes.

apply	<i>(Make your changes active)</i>
save	<i>(Make your changes survive reboot)</i>

Verify failover

1. **Check for the master switch.**

```
/info/vrrp
```

Check secure connection on client. Disconnect link on master and verify failover to backup switch.

2. **Verify connectivity to iSD100-SSLs.**

```
/info/isd
```

Test secure connections on client again.



APPENDIX A

Theory of Operation

This appendix describes some of the fundamentals behind iSD100-SSL.

Encryption

Encryption and decryption allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder. Because of the number of possible combinations that can be formed out of the 128 bits, it is extremely difficult for a third party to intercept and decrypt the messages being sent. [Table 8](#) shows the time required to break the encryption of a message based on the key length.

Table 8 Statistical Time Required to Break Encryption

Key Length	Number of Possible Keys	Approximate Time to Break the Encryption
40 Bits (Exportable RC2/RC4)	1 Trillion	3.5 Hours
56 Bits (DES)	72 Quadrillion	2 Months
128 Bits (RC2/RC4)	340 Decillion	1.6 Trillion Years

Public Key Encryption

Public key encryption (also called asymmetric encryption) involves a pair of keys—a public key and a private key—associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key.

Public key cryptography facilitates the following tasks:

- Tamper detection allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message will be detected.
- Authentication allows the recipient of information to determine its origin—that is, to confirm the sender's identity.
- Non-repudiation prevents the sender of information from later claiming that the information was never sent.

Digital Signatures

It is possible to use a private key for encryption and a public key for decryption. Although this is not desirable when encrypting sensitive information, it is a crucial part of digitally signing any data. Instead of encrypting the data itself, the signing software creates a one-way hash of the data and then uses a private key to encrypt the hash. The encrypted hash, along with other information, such as the hashing algorithm, is known as a digital signature.

Certificates

A certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. A certificate provides recognized proof of a person's identity. Public key cryptography uses certificates to address the problem of impersonation. There are two kinds of certificates:

- **Regular Certificates:** certificates that have been authenticated by an authenticating service, such as a certificate authority
- **Chain Certificates:** certificates that have been authenticated by other certificates that have been authenticated by an authenticating service

A Certificate Authority (CA) is an entity that validates identities and issues certificates. They are issued by either independent third parties or independent organizations operating their own certificate-issuing server software (such as Netscape Certificate Server). The methods used to validate an identity vary, depending on the policies of a given CA. In general, before issuing a certificate, the CA must use its published verification procedures for that type of certificate to ensure that an entity requesting a certificate is authentic.

Register Certificates

The certificate issued by the CA binds a particular public key to the name of the entity that the certificate identifies (such as the name of an employee or a server). Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key, which is held by the entity identified by the certificate.

In addition to a public key, a certificate always includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The digital signature of the issuing CA allows the certificate to function as a “letter of introduction” for users who know and trust the CA.

Chain Certificates

Chain certificate allows a chain of trust to be created. Each certificate in the chain attests to the identity of the previous certificate. The final certificate will be a certificate that has been authenticated by a trusted CA. For example, client A trusts the CA, and the CA trusts client B, therefore, client A trusts client B.

Example SSL Transaction

The steps involved in an SSL transaction can be done with a server or an iSD100-SSL. They are summarized as follows:

1. The client sends the following information to the server or iSD100-SSL: SSL version number, cipher settings, randomly generated data, and other information that the server needs to communicate with the SSL client.
2. The server or iSD100-SSL sends the following information to the client: SSL version number, cipher settings, randomly generated data, and other information needed to communicate with the server over SSL. The server also sends its own certificate and, if the client is requesting a server resource that requires client authentication, requests the client's certificate.
3. The client uses some of the information sent by the server or iSD100-SSL to authenticate the server or iSD100-SSL. If the server or iSD100-SSL is not authenticated, the user is warned of the problem and informed that an encrypted and authenticated connection cannot be established. If the server or iSD100-SSL is successfully authenticated, the client goes on to Step 4.
4. The client (with the cooperation of the server or iSD100-SSL, depending on the cipher being used) creates the premaster secret for the session, encrypts it with the server's or iSD100-SSL's public key (obtained from the server's or iSD100-SSL's certificate, sent in Step 2), and sends the encrypted premaster secret to the server or iSD100-SSL.
5. If the server or iSD100-SSL has requested client authentication (an optional step in the handshake), the client also signs another piece of data that is unique to this handshake and is known by both the client and server or iSD100-SSL. In this case the client sends both the signed data and the client's own certificate to the server or iSD100-SSL along with the encrypted premaster secret.
6. If the server or iSD100-SSL has requested client authentication, the server or iSD100-SSL attempts to authenticate the client. If the client is not authenticated, the session is terminated. If the client can be successfully authenticated, the server or iSD100-SSL uses its private key to decrypt the premaster secret, then performs a series of steps (which the client also performs, starting from the same premaster secret) to generate the master secret.
7. Both the client and the server or iSD100-SSL use the master secret to generate the session key, which is a symmetric key. It is used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity—that is, to detect any change in the data between the time it was sent and the time it is received over the SSL connection.
8. The client informs the server that future messages from the client will be encrypted with the session key. The client then sends a separate (encrypted) message indicating that the client portion of the handshake is finished.

9. The server or iSD100-SSL informs the client that future messages from the server will be encrypted with the session key. It then sends the client a separate (encrypted) message indicating that the server or iSD100-SSL portion of the handshake is finished.
10. The SSL handshake is now complete, and the SSL session begins. The client and the server or iSD100-SSL use the session keys to encrypt and decrypt the data they send to each other and to verify data integrity.

Figure 10 illustrates these steps as performed by the iSD100-SSL.

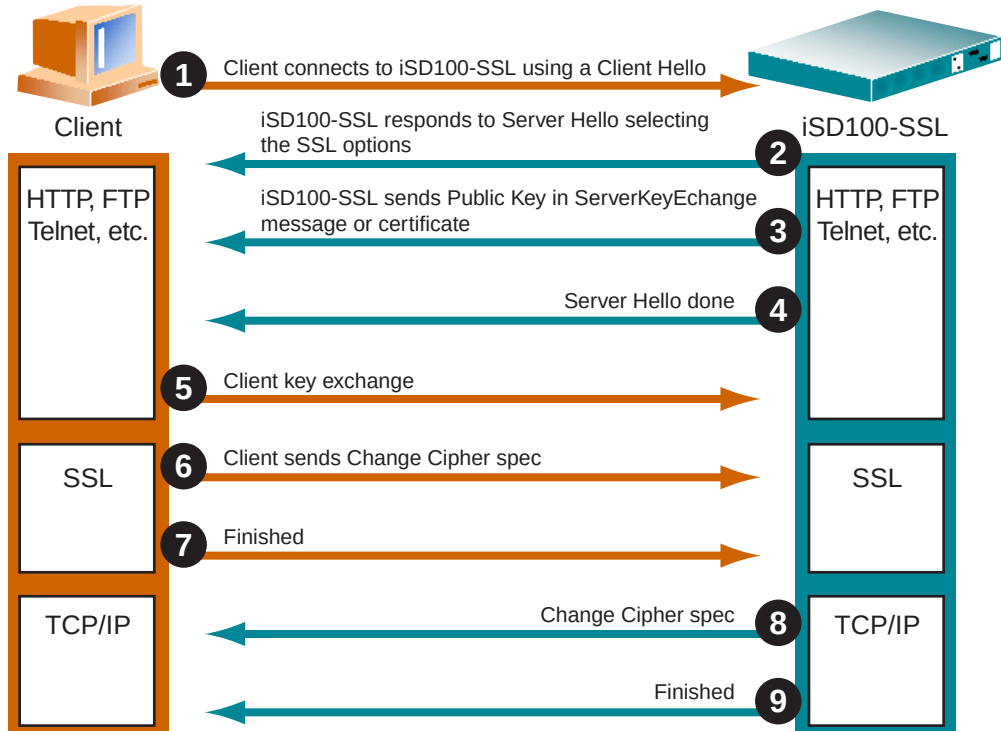


Figure 10 SSL Handshake Procedure

APPENDIX B

Supported Ciphers

The iSD100-SSL supports only RSA key exchange under SSL version 3.0. [Table 9](#) lists the ciphers supported by this product.

Table 9 Supported Ciphers

Name	Protocol	Key Exchange Authentication	Encryption	MAC
DES-CBC3-SHA	SSLv3	RSA	3DES	SHA1
IDEA-CBC-SHA	SSLv3	RSA	IDEA(128)	SHA1
RC4-SHA	SSLv3	RSA	RC4(128)	SHA1
RC4-MD5	SSLv3	RSA	RC4(128)	MD5
DES-CBC-SHA	SSLv3	RSA	DES(56)	SHA1
EXP-DES-CBC-SHA	SSLv3	RSA	DES(40)	SHA1
EXP-RC2-CBC-MD5	SSLv3	RSA	RC2(40)	MD5
EXP-RC4-MD5	SSLv3	RSA	RC4(40)	MD5

APPENDIX C

Building Keys and Certificates

The Secure Sockets Layer (SSL) protocol runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client. The client then authenticates itself to the server, and both machines establish an encrypted connection. This chapter provides steps for using the iSD100-SSL for SSL transactions.

The iSD100-SSL accelerator only supports certificates created using Apache-SSL, OpenSSL or Stronghold SSL. The certificates must conform to the X.509 standard. You can create a new certificate, or use an existing certificate. The basic steps to create a new certificate are:

- Create a private/public key pair using Apache-SSL or the Apache interface to OpenSSL (`mod_ssl`)
- Generate a Certificate Signing Request (CSR) and send it to a Certificate Authority (such as Entrust or Verisign) for certification
- Input the signed certificate with the private key into the iSD100-SSL

Creating a Public/Private Key Pair

NOTE – It is assumed that you will be creating the paired keys on a UNIX-based server.

This process will differ depending on the Certificate Authority (CA). There are a number of utilities that assist in making public/private keys. It is recommended that you contact the CA to see what utility is supported.

In the following example, generate the key pair and CSR using a utility named OpenSSL, which is installed when building Apache-SSL:

1. **Create three files on the hard drive of your UNIX-based Web server, named F1, F2 and F3.**
2. **Generate a 1024-bit RSA key pair and store it in the file *servername.key*:**

```
openssl genrsa -rand F1:F2:F3 1024 >servername.key
```

Generating and Submitting a CSR to a CA

1. **Generate the CSR. At the UNIX server shell prompt, enter:**

```
openssl req -new -key servername.key -out servername.csr
```

2. **When prompted, enter the information to include in your Web server Distinguished Name (DN), as follows:**
 - **Country code:** The two-letter ISO abbreviation for the country where the Web server is located.
 - **State or Province:** This is the name of the state or province where the head office of the organization is located. Enter the full name of the state or province.
 - **Locality:** The name of the city where the head office of the organization is located.
 - **Organization:** The registered name of the organization. This organization must own the domain name that appears in the common name of the Web server. Do not abbreviate the organization name and do not use any of the following characters:

< > ~ ! @ # \$ % ^ * / \ () ?
 - **Organizational unit:** The name of the department or group that uses the secure Web server.
 - **Common name:** The name of the Web server as it appears in the URL. This name must be the same as the domain name of the Web server that is requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse a secure connection with your site. Do not enter the protocol specifier (`http://`) or any port numbers or pathnames in the common name. Wildcards (such as `*` or `?`) and IP address are not allowed.
3. **The CSR is created and stored in a file with a `.csr` extension.**

4. Open and copy the CSR.

In a text editor, open the *servername.CSR* file that contains the CSR. It should appear similar to the following:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIISD0IulkmIsRRlksllskjauASKJlaloSISLKjwBgN
VBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZS
Bub3duMRQwEgYDVQKKEwtPchBvcnR1bml0aTEYMBYGA
1UECXMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3
d3cuZm9yd2FyZC5jby56YTBA0GCSqGSib3DQEBAQU
AAklmLKSuljsOIjsfBWu5WLHD/G4BJ+PobiC9d7S6p
DvAjuyC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh
2V7diuuPLHDAgEDoAAwDQYJKoZIhvcNAQEEBQADQQBf
8LSLKknlsklSSLlworr334ZmXD1AvUjuDPCWzFupRe
iq7UR8Z0wiJUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END NEW CERTIFICATE REQUEST-----
```

Copy the entire CSR, **including** the “-----BEGIN NEW CERTIFICATE REQUEST-----” and “-----END NEW CERTIFICATE REQUEST-----” lines.

5. Submit the CSR to Entrust, Verisign, or any other CA.

The process for submitting the CSR varies with each CA. Use your Web browser to access your CA's Web site and follow the online instructions. When prompted, paste the CSR into the space provided on the CA's online request process.

The CA will return the signed certificate for installation. The certificate is then ready to be entered into the iSD100-SSL.

Adding Certificates to the iSD100-SSL

Using the encryption capabilities of the iSD100-SSL requires installing a key and certificate that conforms to the X.509 standard into the iSD100-SSL. This process is expedited by displaying the desired key/certificate in a text editor and using the “copy and paste” method. Complete the certificate by entering three periods in a row (...). This signals the iSD100-SSL that the certificate is complete and ready for installation. There are three ways to install a certificate into the iSD100-SSL:

- Copy and paste the key/certificate
- TFTP the key/certificate
- Import an existing key/certificate from a server

Using Copy and Paste to Add Certificates and Keys

The following steps demonstrate how to add a certificate using the copy and paste method.

1. **On the Web switch CLI, access the SSL Offload Application Menu:**

```
# /cfg/isd/ssl
```

2. **Enter the following command to initiate adding a certificate:**

```
>> SSL Offload Application# addcert
```

3. **Enter the Virtual IP (VIP) address for the certificate when prompted.**

```
Enter VIP address: <virtual IP address>
```

4. **Paste the certificate into the Web switch prompt.**

Open the certificate in a text editor and copy the entire contents. Then, paste the contents into the Web switch prompt.

NOTE – The iSD100-SSL does not support IIS private keys or encrypted private keys.

5. Finally, enter three dots (. . .) on a new line at the end of the pasted certificate to signal the end of the certificate/key pair. For example:

```

-----BEGIN PRIVATE KEY-----
MIISDOIUlkmIsRRlkSllskjauASKJlaLOSISLKjwBgN
VBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZS
BUb3duMRQwEgYDVQKEwtPcHBvcnR1bml0aTEYMBYGA
1UECxMPT25saw5lIFNlcnZpY2VzMRowGAYDVQQDExF3
d3cuZm9yd2FyZC5jby56YTBA0GCSqGSIb3DQEBAQU
AAAKlmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6p
DvAjuyC+dPanL0d91tXdm2j190D1kgDoSp5ZyGSgwJh
2V7diuuPLHDAgEdoAAwDQYJKoZIhvcNAQEEBQADQQBf
8LSLKknlsklSSLlworr334ZmXD1AvUjuDPCwzFupRe
iq7UR8Z0wiJUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE -----
MIISDOIUlkmIsRRlkSllskjauASKJlaLOSISLKjwBgN
VBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZS
BUb3duMRQwEgYDVQKEwtPcHBvcnR1bml0aTEYMBYGA
1UECxMPT25saw5lIFNlcnZpY2VzMRowGAYDVQQDExF3
d3cuZm9yd2FyZC5jby56YTBA0GCSqGSIb3DQEBAQU
AAAKlmLKSuljSOIjsfBWu5WLHD/G4BJ+PobiC9d7S6p
DvAjuyC+dPanL0d91tXdm2j190D1kgDoSp5ZyGSgwJh
2V7diuuPLHDAgEdoAAwDQYJKoZIhvcNAQEEBQADQQBf
8LSLKknlsklSSLlworr334ZmXD1AvUjuDPCwzFupRe
iq7UR8Z0wiJUUsllkfq/IuuIlz6oCq6htdH7/tvKhh
-----END CERTIFICATE -----
. . .

```

NOTE – Depending on the type of certificate the CA generates (register or chain), your certificate may appear substantially different from the one shown above. Be sure to copy and paste the entire contents of the certificate file.

Using TFTP to Add Certificates

The following is an example of how to input a certificate into the iSD100-SSL using TFTP.

1. Put the certificate file onto your TFTP server.

NOTE – The certificate must be stored in a file named for the virtual server IP address where the certificate will be used. For example, “192.168.10.100”.

2. On the Web switch CLI, access the SSL Offload Application Menu:

```
# /cfg/isd/ssl
```

3. Enter the following command to initiate adding a certificate via TFTP:

```
>> SSL Offload Application# tftpcrt
```

4. Enter the IP address of the TFTP server that contains the certificate.

```
Enter IP address of tftp server: <TFTP server IP address>
```

5. Enter the virtual IP address for the certificate being added.

```
Enter certificate filename (as virtual IP address):
```

The iSD100-SSL is now ready to start SSL transactions.

Importing an Existing Key/Certificate from a Server

You can import an existing key/certificate pair from a server. The iSD100-SSL accelerator only supports keys created with Apache-SSL, or the Apache interface to OpenSSL. Keys created with Netscape Server cannot be moved to another device.

NOTE – Keys created for IIS have to be transformed before they can be moved to another device. This process is error prone and does not work very smoothly.

Apache-SSL Key

1. **Change directory to \$APACHESSLROOT/conf/httpd.conf**
2. **Look for mod_ssl defaults in \$APACHESSLROOT/certs/*.key**
3. **Copy and paste the key file into the iSD100-SSL. For more information, see [“Using Copy and Paste to Add Certificates and Keys”](#) on page 66.**

Apache-SSL Certificate

1. **Change directory to \$APACHESSLROOT/conf/httpd.conf for location of the *.cert file**
2. **Apache-SSL, defaults to \$APACHESSLROOT/certs/*.cert**
3. **Copy and paste the certificate file into the iSD100-SSL, after the key file.**

OpenSSL Key (Apache interface)

1. **Change directory to \$APACHEROOT/conf/httpd.conf**
2. **Look for mod_ssl defaults in \$APACHEROOT/conf/ssl.key**
3. **Copy and paste the key file into the iSD100-SSL. For more information, see [“Using Copy and Paste to Add Certificates and Keys”](#) on page 66.**

OpenSSL Certificate (Apache interface)

1. **Change directory to \$APACHEROOT/conf/httpd.conf for location of the *.crt file**
2. **Look for mod_ssl defaults to \$APACHEROOT/conf/ssl.crt/*.crt**
3. **Copy and paste the certificate into iSD100-SSL, after the key file.**



APPENDIX D

Troubleshooting

This chapter lists probable causes and defines possible solutions for basic problems that may occur with the iSD100-SSL. This chapter also provides a section on performing diagnostics through the iSD100-SSL console.

Basic Solution Checklists

Offload Server Management Problems

- Cannot ping an iSD100-SSL IP interface
- Switch cannot discover the iSD100-SSL

Possible Causes

- Incorrect switch IP interface configuration
- Link state connection of the port pinging station is down
- Switch IP interface address is used by some other device in the network

Actions

- Check `/cfg/ip/cur` for IP interface address, subnet mask, and default gateway configuration
- Check that the IP interfaces are enabled
- Check `/info/link` to verify that the management port link is “up”
- Check for duplicate IP addresses

Console Diagnostics

The console port is used for diagnostics on the iSD100-SSL. Although connected in the same manner as any Alteon WebSystems switch, the console port will not accept iSD100-SSL configuration commands.

Connecting a Terminal to the iSD100-SSL

To establish a console (DCE) connection with an iSD100-SSL, the following is required:

- An ASCII terminal or a computer running ASCII terminal emulation software set to the parameters shown in the table below:

Table 10 Console Configuration Parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1

- Console Cable

The switch console port accepts a straight-through serial cable with a male DB9 connector.

Table 11 Pinouts for DB9 Serial Connector

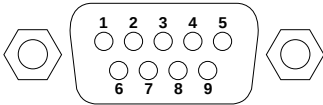
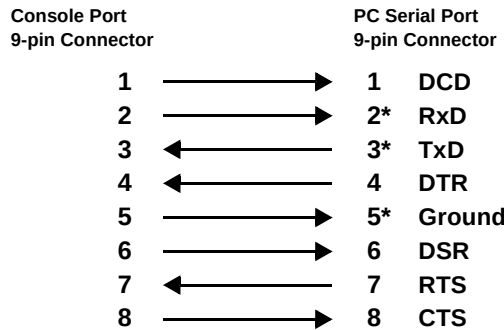
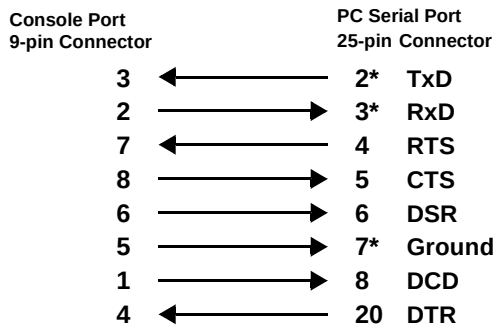
DB9 Serial Connector	Pin	Description
	1	DCD
	2	RxD
	3	TxD
	4	DTR
	5	Ground
	6	DSR
	7	RTS
	8	CTS
	9	Not used

Figure 11 and Figure 12 show the pin assignments for the console to use to configure serial cables to terminal connectors with 9-pin or 25-pin connectors.



* Only the pins for RxD, TxD, and Ground are required.

Figure 11 9-pin to 9-pin Connector Pin Assignments



* Only the pins for RxD, TxD, and Ground are required.

Figure 12 9-pin to 25-pin Connector Pin Assignments

NOTE – Console cables are not intended for permanent installation and should be disconnected when not in use.

Establishing a Console Connection

1. Connect a terminal to the Console port using the serial cable included with the unit.
2. Power on the terminal.
3. To establish the connection, press <Enter> on your terminal.
4. Enter the password when prompted (the default root password is alteon).

System Diagnostics

Perform the following diagnostics once logged in on the console port:

■ SSL Offload Hardware Diagnostic

```
csdiag -i <0 or 1 for the card number>
```

■ Certificates

This will show if the certificate is installed in the iSD100-SSL.

```
cat /home/ssl-proxy/config/<virtual IP address>
```

■ Network Diagnostics

To check if the iSD100-SSL has a IP address:

```
ifconfig eth0
```

To check if the virtual server is working:

```
ping <virtual IP address>
```

To check for error messages:

```
cat /var/log/ssllogfile
```

To check if the iSD100-SSL is getting network traffic:

```
ipchains -L -v
```

■ General Diagnostics

Enter the following command:

```
/usr/local/bin/isddiag.sh <IP1> <IP2>
```

Where <IP1> is the IP address of the iSD100-SSL, and <IP2> is the address to ping and the default route for the iSD100-SSL.

NOTE – The iSD100-SSL will reboot after this command.



APPENDIX E

Specifications

Physical Characteristics

Characteristic	Measurement
Height	44.45 mm (1.75 inches), 1U
Width	431.8 mm (17 inches)
Depth	457.2 mm (18 inches)
Weight	4.1 kg (9 pounds)
Processor	Intel Pentium III–Low Power–Up to 500MHz
SDRAM (ECC) memory	Up to 1GB
L2 Cache (Internal)	256KB ECC 64-bit wide
Compact Flash Disk	Up to 192 MB
Drive Bay	One or two 3.5" hard disks
Expansion Slot (available)	2 full-size PCI 1x half-size PCI

Supported Standards

- Logical Link Control (IEEE 802.2)
- 10Base-T/100Base-TX (IEEE 802.3, 802.3u)
- 1000Base-SX (IEEE 802.3z)
- IP
- TFTP (RFC 783)

Port Specifications

Port	Connector	Media	Maximum Distance
10Base-T	RJ-45	Cat. 3, 4, or 5 UTP	100 meters (328 feet)
100Base-T	RJ-45	Cat. 5 UTP	100 meters (328 feet)
1000Base-SX	SC full-duplex	Shortwave (850 nm):	
		62.5 micron multimode fiber	2 to 275 meters (6.5 to 902 feet)
		50 micron multimode fiber	2- to 550 meters (6.5 to 1804 feet)
Console (DCE)	Female DB-9	RS-232C (serial)	25 meters (80 feet)

Power Requirements

Specification		Measurement
AC Power	Power Supply	ATX150W AC
	Input Voltage	90-260VAC auto-switch 47-63Hz
DC Power	Power Supply	ATX150W DC-48
	Input Voltage	-42 to -56VDC (-48VDC nominal)

Environmental Specifications

Condition	Operating Specification	Storage Specification
Temperature	0° to +45°C (32°F to 133°F)	-40°C to +70°C (-40°F to 158°F)
Relative humidity	5-95% @ 40° (5-95% @ 104°F)	0-95% @ 40°C (0-95% @ 104°F)
Altitude	up to 3,048 meters (10,000 feet)	up to 9,114 meters (30,000 feet)
Shock	15G, 11ms duration (half-sinus / 6-axis)	30G, 11ms duration (half-sinus / 6-axis)
Vibration	1G, +/- .15mm, 10-58Hz (sinus / 6-axis)	2G, +/- .3mm, 10-500 Hz (sinus / 6-axis)
Acoustic Noise	<50dB at 1m in front of the system at full load	

Certifications

Category	Compliance
Emissions (EMC)	FCC CFR 47, Part 15, Class A VCCI, Class A Industry Canada, Class A CE EN-55022, EN-55024, EN-61000-4-2, EN-61000-4-3, EN-61000-4-4, EN-61000-4-5, EN-61000-4-6, EN-61000-4-8, EN-61000-4-11 BSMI CNS 13438 Class A AS/NZS 3548 Class A
Safety	UL 1950 CSA 22.2 No. 950 IEC 60950, with all NCB Member Differences* EN 60950 IEC 60825-1

*NCB (National Certified Bodies) Member countries: Austria, Australia, Belgium, Canada, Switzerland, China, Czech Republic, Germany, Denmark, Spain, Finland, France, United Kingdom, Greece, Hungary, Ireland, Israel, India, Italy, Japan, Republic of Korea, The Netherlands, Norway, Poland, Russia, Sweden, Singapore, Slovenia, Slovakia, United States of America, South Africa



APPENDIX F

License Information

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. Both licenses are actually BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License Copyright © 1998-1999 The OpenSSL Project. 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 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 (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (ey@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscape SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered 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 routines 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 publicly available version or derivative of this code cannot be changed. That is, this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

GNU General Public License

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work that contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program," below, refers to any such program or work. A "work based on the Program" means either the Program or any derivative work under copyright law: that is, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification.") Each licensee is addressed as "you."

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1, above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

- b) You must cause any work that you distribute or publish in whole or in part that contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it (when started running for such interactive use in the most ordinary way) to print or display an announcement, including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty), and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: If the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to the work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2, above, provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party (for a charge no more than your cost of physically performing source distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2, above, on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accordance with Subsection b, above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute, or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment, or allegation of patent infringement, or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system. It is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version,” you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs in which distribution conditions are different, write to the author for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING, THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

12. IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

Notes

