Installation and User's Guide

iSD-SSL™ 2.0

Secure Sockets Layer Offload Device

Part Number: 050125, Revision B, April 2001

AlteonWebSystems
Web Speed for e-Business

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

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.

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 (eay@cryptsoft.com).

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

See Appendix E, "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 Règlements 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

This *Installation and User's Guide* describes the Alteon WebSystems Integrated Service Director (iSD-SSL) with SSL offload software. This document introduces the major features of the iSD-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 and IP addressing.

How This Book Is Organized

The chapters in this book are organized as follows:

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

Chapter 2, "Installing the iSD-SSL Hardware" describes how to mount the iSD-SSL, connect network cables, and attach power.

Chapter 3, "Initial Setup" describes how to perform minimal start-up configuration on the iSD-SSL and how to upgrade and reinstall its software.

Chapter 4, "Upgrading the iSD-SSL Software" describes how to upgrade the iSD-SSL software for a minor release upgrade, major release upgrade, or comprehensive upgrade from software version 1.0 to version 2.0.

Chapter 5, "The Command Line Interface" describes how to connect to the iSD-SSL and access the information and configuration menus.

Chapter 6, "iSD-SSL Command Reference" provides an overview of the iSD-SSL menu system and details of all menus and options.

Chapter 7, “Public Key Infrastructure and SSL” provides a general overview of basic concepts behind Secure Socket Layer (SSL) transactions.

Chapter 8, “iSD-SSL Sample Applications” provides basic scenarios and configuration examples for using the iSD-SSL for Web server acceleration, content intelligent switching for secure sessions, and in redundant active-standby configurations.

Chapter 9, “Managing Certificates and Client Authentication” describes how to generate and prepare keys and certificates for use with the iSD-SSL.

Chapter 10, “Using the Quick Server Setup Wizard” describes how to use the Quick Server Setup wizard.

Chapter 11, “Configuring the iSD-SSL to Rewrite Client Requests” describes how to configure the iSD-SSL to rewrite client requests for the HTTPS service in case the client browser does not meet the required cipher strength.

Chapter 12, “Using the iSD-SSL as a Web Server Accelerator” describes how to set up the iSD-SSL as a stand-alone Web server accelerator, without using a Web switch.

Chapter 13, “Troubleshooting the iSD-SSL” provides suggestions for troubleshooting basic problems.

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

Appendix B, “Command Translation Table” provides information about the Web OS commands used for iSD-SSL version 1.0, and their equivalents in the built in command line interface of the iSD-SSL version 2.0.

Appendix C, “iSD-SSL 2.0 SNMP Agent” provides information about the SNMP agent on the iSD-SSL, and which MIBs (Management Information Bases) are supported.

Appendix D, “Specifications” describes the physical characteristics of the iSD-SSL.

Appendix E, “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.	View the `readme.txt` file.
	It also depicts on-screen computer output and prompts.	`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.	To establish a Telnet session, enter: `host#` **`telnet`** *<IP address>*
	This also shows book titles, special terms, or words to be emphasized.	Read your *User's Guide* 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 that are under warranty or covered by a maintenance contract.

- E-mail access:

  support@alteon.com

  E-mail access to Alteon WebSystems Customer Support is available to accounts that are 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 iSD-SSL

The Integrated Service Director (iSD-SSL) is a peripheral Secure Socket Layer (SSL) offload platform that attaches to an Alteon Web switch or a comparable switch from another vendor. The iSD-SSL performs a TCP three-way handshake with the client through the Web switch and performs all the SSL encryption and decryption for the session. Combined with the load balancing features of the Web switch, the iSD-SSL offloads SSL encryption/decryption functions from back-end servers.

The iSD-SSL is delivered on two different hardware platforms:

- iSD100-SSL
- iSD310-SSL

For detailed technical specifications of the respective hardware platform, see “Specifications” on page 219.

Feature Summary

iSD100-SSL

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

iSD310-SSL

- High-speed network interface controllers (NIC), which provide an Ethernet interface.
  - Model iSD310-SSL-X—dual integrated Intel PRO/100+ copper port NICs for Ethernet or Fast Ethernet.
  - Model iSD310-SSL-F—3Com Gigabit fiber-optic port NIC for Gigabit Ethernet, in addition to the dual integrated Intel PRO/100+ NICs.
- 1U height, rack-mountable chassis.
- Local console port (DCE) at the back panel for system diagnostics and configuration.
- TFTP download to hard disk for software updates and upgrades.

iSD-SSL 2.0 Software (Common to Both Hardware Platforms)

- Accelerates SSL processing—offloads SSL encryption and decryption from the back end server pool.
- Supports SSL version 2.0 and 3.0, plus TLS version 1.0.
- Supports SMTPS, POP3S, and IMAPS in addition to the standard HTTPS.
- Supports up to 400 SSL transactions per second and per iSD-SSL.
- Supports up to 256 virtual SSL servers, and an unlimited number of certificates.
- Supports certificate and key management—private keys generated in Apache, OpenSSL, Stronghold, WebLogic, and Microsoft IIS 4.0 can be imported.
- Supports SNMP version 1 and SNMP version 2c.
- Provides dynamic scalability—up to 256 iSD-SSLs can be added to each cluster.
- Provides a single system image (SSI)—all iSD-SSLs in a given cluster are configured as a single system.
- Provides dynamic plug and play—iSD-SSLs can be added to or removed from a cluster dynamically without disrupting network traffic.

New and Enhanced Software Features in iSD-SSL 2.0

- Extended support of key import without using conversion tools. Private keys generated in WebLogic and Microsoft IIS 4.0 can now be imported using TFTP, in addition to keys from Apache, OpenSSL and Stronghold.
- Support for validating private keys and certificates via the command line interface.
- Support for generating a certificate signing request (CSR) via the command line interface.
- Support for creating test certificates (self-signed) via the command line interface, for instant testing of SSL features.
- Support for client authentication, generation of client certificates, and revocation of client certificates.
- Support for SNMP via the SNMP menu on the iSD-SSL.
- Support for creating multiple virtual SSL servers, whereby other secure services than HTTPS can be put to use by the same virtual server IP address on the Web switch.

- The user can customize the SSL protocol version that a specific virtual SSL server should use. Choices include:
  - □ SSL 2.0 only
  - □ TLS 1.0 only
  - □ Both SSL 3.0 and TLS 1.0
  - □ All three protocols
- Support for rewriting client requests, whereby customized error messages can be sent to the client's Web browser in case the browser is unable to perform the required cipher strength. Without this feature, the client request would simply be rejected during the SSL handshake.
- Ability to transmit extra SSL information to the back end servers, such as the negotiated cipher suit and client certificate information (in case client certificates were required by the virtual SSL server). The information is conveyed by configuring the virtual SSL server to add an extra SSL header to the client's request.
- Works with the Alteon 708 Web switches, as well as with comparable switches from other vendors.
- Stand-alone configuration via built-in command line interface with Alteon look and feel, accessible via both Telnet and Secure Shell.
- Ability to control remote access via Telnet and Secure Shell down to specific machines.
- Ability to create multiple clusters of iSD-SSLs, each capable of serving its own group of real servers.
- High level of redundancy in the master/slave cluster design: even if three master iSD-SSLs in a cluster fail, additional slave iSD-SSLs would still be operational and could accept configuration changes.

iSD100-SSL Physical Description

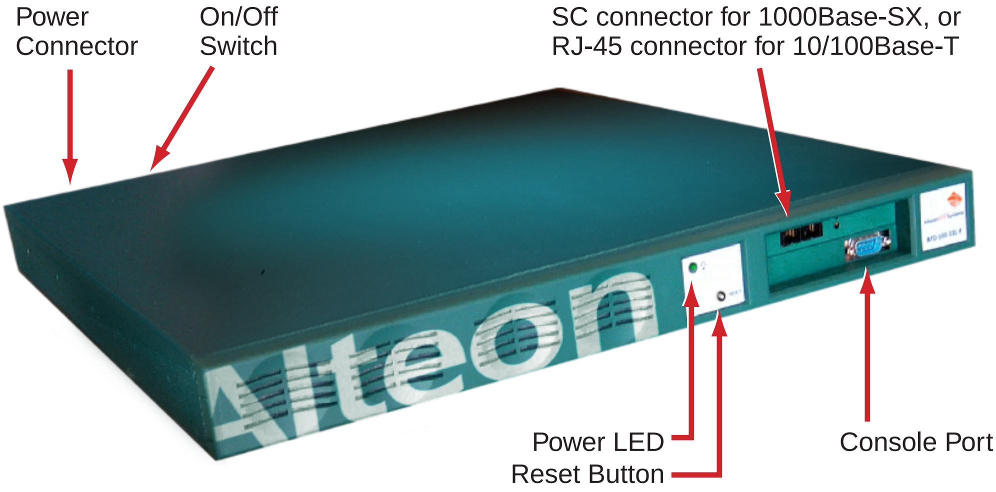

Power Connector
On/Off Switch
SC connector for 1000Base-SX, or RJ-45 connector for 10/100Base-T
Power LED
Reset Button
Console Port

Figure 1-1 Physical Layout of the iSD-SSL

Front Panel

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

  See Table 2-1 on page 29 and Table 2-3 on page 30 for LED state information.
- Console port

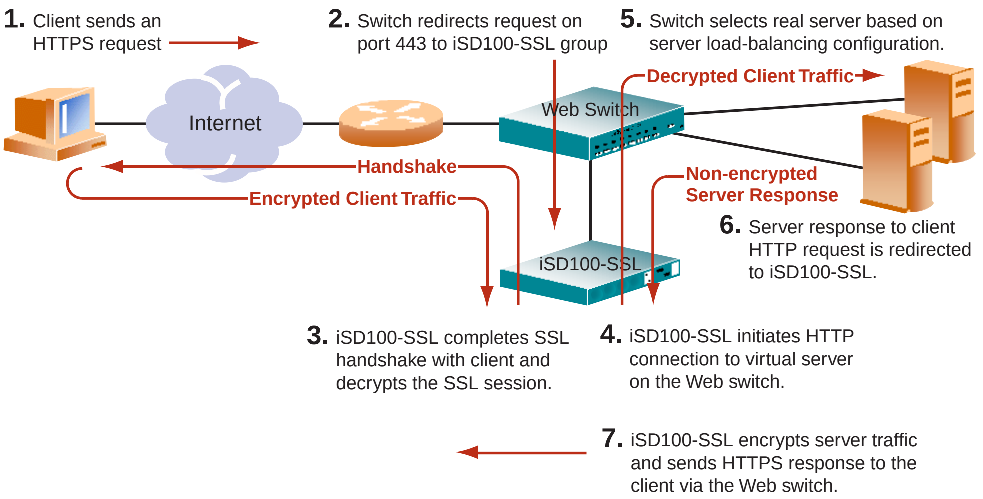
  The female DB-9 serial connector, labeled "Console," is used for connecting to the iSD-SSL during the initial setup, or when reinstalling software. It can also be used for trouble-shooting purposes, should the iSD-SSL become inaccessible via Telnet or SSH connection.
- Power LED lights up to indicate that the iSD-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 iSD-SSL operation. For an overview of encryption systems in general, see Chapter 7, "Public Key Infrastructure and SSL."


1. Client sends an HTTPS request

2. Switch redirects request on port 443 to iSD100-SSL group

3. iSD100-SSL completes SSL handshake with client and decrypts the SSL session.

4. iSD100-SSL initiates HTTP connection to virtual server on the Web switch.

5. Switch selects real server based on server load-balancing configuration.

6. Server response to client HTTP request is redirected to iSD100-SSL.

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

Figure 1-2 Basic iSD-SSL Offload Operation

1. **Client requests secure information via HTTPS.**

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

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

   The Web switch recognizes HTTPS traffic on port 443 and redirects the request to an iSD-SSL device. This form of application redirection is described in detail in your *Web OS Application Guide* (provided for buyers of Alteon Web switches).

3. **The iSD-SSL completes the SSL handshake and decrypts the session.**

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

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

   The iSD-SSL receives the client's encrypted SSL traffic via the Web switch. The iSD-SSL decrypts the secure traffic and forwards it as a regular HTTP request to a virtual server on the Web switch. The iSD-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 iSD-SSL device.

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

CHAPTER 2

Installing the iSD-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 iSD-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 iSD-SSL
- A user’s manual

Installation involves the following tasks:

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

System Requirements

The iSD-SSL can be attached either to an Alteon Web switch running Web OS 8.0 (or higher) software, or to a comparable switch from another manufacturer.

Preparing for Installation

Before installing the iSD-SSL:

1. **Unpack the iSD-SSL 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 iSD-SSL:

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

Avoid overloading your electrical supply circuits. Electrical ratings are printed on the nameplates 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 iSD-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 iSD-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 2-1, connect the two mounting brackets to the iSD-SSL using the supplied screws.**

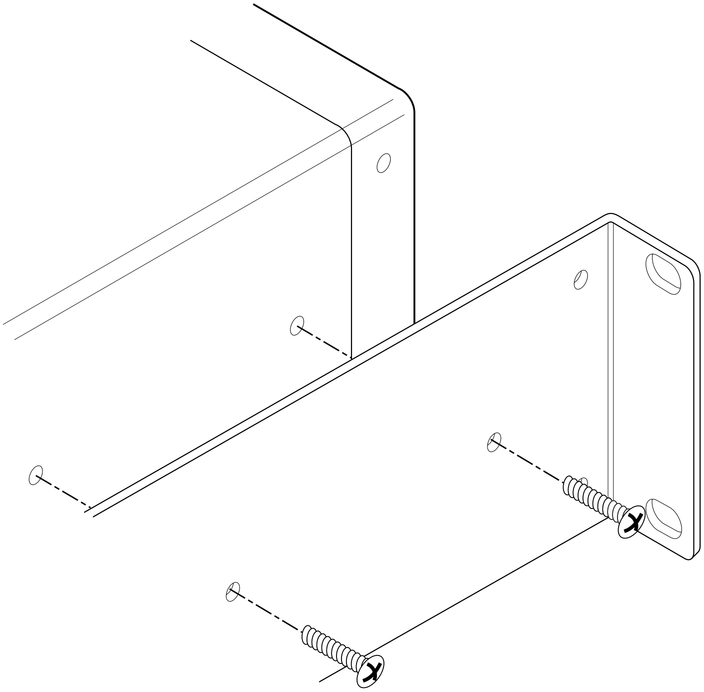


Figure 2-1 Position Mounting Brackets for Rack Mount

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

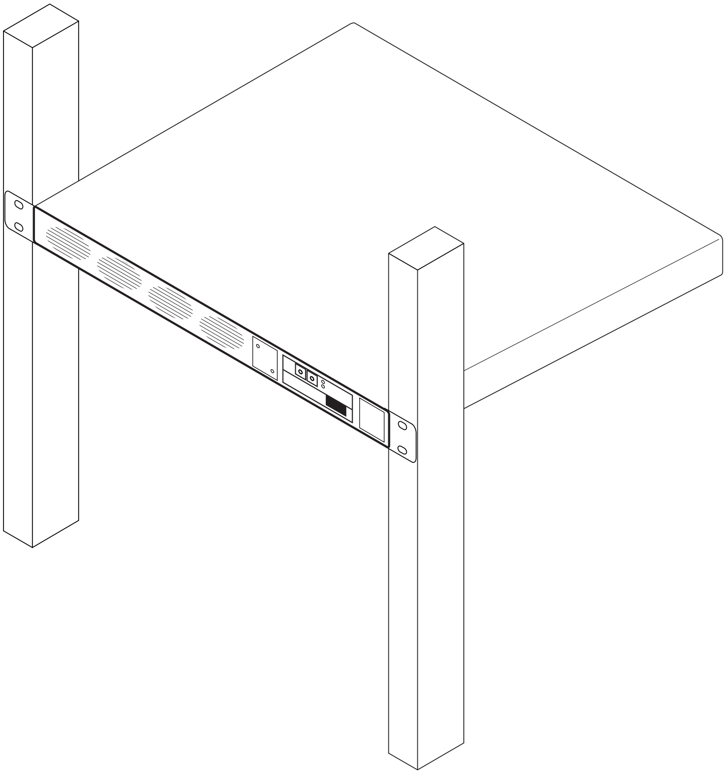


Figure 2-2 Rack-Mounted iSD-SSL 2.0

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 iSD-SSL high-speed uplink port must be connected to an Alteon Web switch running Web OS 8.0 (or higher) software, or to the appropriate port of a comparable switch. The type and method of cabling depends on your particular model of iSD-SSL:

- Model iSD-SSL-C1A has one 10/100Base-T port for copper Ethernet or Fast Ethernet.
- Model iSD-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 iSD-SSL-C1A)

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

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

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

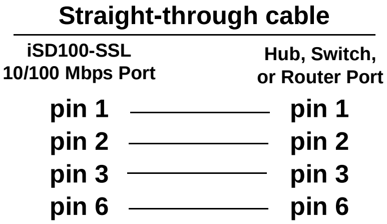


Figure 2-3 Pin assignments for 10/100 Mbps port cables

Table 2-1 describe the states of the uplink LEDs.

Table 2-1 iSD-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 iSD-SSL-F2A)

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

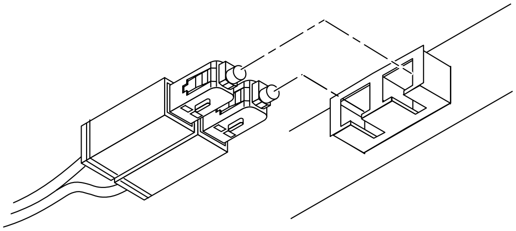


Figure 2-4 Fiber Optic Connector for the iSD-SSL-F2A

The 1000Base-SX port is designed to operate with multi-mode fiber-optic cables. Table 2-2 lists the cable characteristics for this port.

Table 2-2 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 2-3 describes the states of the uplink LEDs.

Table 2-3 iSD-SSL-F2A Uplink Port LEDs

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

Power

Connecting the Power Cord

1. **Verify that the iSD-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 2.0.**
3. **Plug the cord into a properly fused outlet.**

⚠ **CAUTION—**The iSD-SSL uses a 3A/250V fast-acting fuse. For continued protection against risk of fire, replace only with the same type and rating fuse. French: *Attention–Utilisé un fusible de rechange de même type.*

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 iSD-SSL is on and receiving proper power.

CHAPTER 3

Initial Setup

This chapter covers the basic setup and initialization process for the iSD-SSL. It introduces the concept of iSD-SSL *clusters*, and provides detailed instructions for reinstalling the iSD-SSL software, should it become necessary.

About iSD-SSL Clusters

All iSD-SSLs are members of a *cluster*. A cluster is a group of iSD-SSLs that share the same configuration parameters. There can be more than one iSD-SSL cluster in the network, each with its own set of parameters and services to be used with different real servers. Every cluster has a Management IP (MIP) address, which is an IP alias to one of the iSD-SSLs in the cluster. The MIP address identifies the cluster and is used when making configuration changes via a Telnet or SSH connection.

The configuration parameters are stored in a database, which is replicated among the iSD-SSLs designated as masters in a cluster. By default, the first four iSD-SSLs in one given cluster are set up as masters. Additional iSD-SSLs are automatically set up as slaves, which means they depend on a master iSD-SSL in the cluster for proper configuration. However, even if three of the masters fail, the remaining iSD-SSL(s) are still operational and can have configuration changes made to them.

Each time you perform an initial setup of an iSD-SSL and select **`new`** in the Setup menu, you create a new cluster which initially only has one single member. You can add one or more iSD-SSLs to any existing cluster by performing an initial setup and select **`join`** in the Setup menu.

When using an Alteon Web switch, all iSD-SSL in a cluster can form a Real Server Group. Traffic intended for the iSD-SSL cluster can then be load balanced by the Web switch.

Configuration at Boot Up

When starting an iSD-SSL the very first time, you need to:

- Mount the iSD-SSL chassis.
- Connect the iSD-SSL uplink port to a compatible port on the Web switch.
- Connect a terminal to the console port.
  For more information, see "Connecting to the iSD-SSL" on page 52.
- Press the power-on button.
- Wait until you get a login prompt.
- Log in as `user`: *admin*, `password`: *admin*

When you log in after having started the iSD-SSL the first time, you will automatically enter the setup utility menu (see Figure 3-1). You will be prompted for the minimum information required to make the iSD-SSL operational.

```
[Setup Menu]
join    - Join an existing iSD cluster
new     - Initialize iSD as a new installation
boot    - Boot Menu
```

Figure 3-1 The Setup Menu

The amount of information you need to provide will depend on whether you are installing the iSD-SSL to join an existing cluster of iSD-SSLs, or if you are installing it as a single iSD-SSL that is connected to the Web switch. If joining an existing cluster less information is needed because the iSD-SSL will fetch most of the configuration from the other iSD-SSL(s) in the cluster. In either case you must provide an IP address for the iSD-SSL itself and the gateway address, as well as provide the network mask. You will also be asked to provide a Management IP address. Note that when you select **`new`** in the Setup menu, you actually assign a new Management IP address to a new cluster, even though the cluster only contains a single iSD-SSL to start with. When you select **`join`** in the Setup menu, the Management IP address that is already assigned to an existing cluster will be used.

CAUTION—Each iSD-SSL cluster in the network must have a *unique* MIP address. The MIP address you assign to a cluster when selecting **`new`** in the Setup menu must be different from all other IP addresses used on your network, including the IP address you assign to each particular iSD-SSL in the cluster.

Installing a Single iSD-SSL

To install an iSD-SSL as a single device connected to the Web switch, or to install an iSD-SSL as the first member in a new cluster, choose **new** from the Setup menu.

Provide answers to the requested information in order to perform the initial configuration and network access of the iSD-SSL. Make sure that the IP address you assign to the machine and the Management IP address you assign to the cluster (a new cluster is actually created, even though it only contains a single iSD-SSL to start with) are unique on your network, and that they are within the same network range. The gateway IP address you specify must also be within the same network range as the machine IP address and the Management IP address. If not, a built-in control function in the Setup utility will detect the erroneous configuration and ask you to check your network settings before trying again.

In order to maintain a high level of security when accessing the iSD-SSL via a SSH connection, it is also recommended that you accept the default choice to generate new SSH host keys.

```
>> Setup# new
Setup will guide you through the initial configuration of the iSD.

Enter IP address for this machine: <IP address>
Enter network mask: <IP subnet mask>
Enter gateway IP address: <gateway IP address>
Enter a timezone or ’select’ [select]: <Press ENTER to select>
Select a continent or ocean: <Continent or ocean by number>
Select a country: <Country by number>
Select a region: <Region by number>
Selected timezone: <Suggested timezone, based on your selections>
Enter the current date (YYYY-MM-DD) [2001-02-05]: <Press ENTER if correct>
Enter the current time (24-hour, HH:MM:SS) [09:26:16]: <Press ENTER if
correct>
Enter NTP server address (or blank to skip): <IP address>
Enter DNS server address (or blank to skip): <IP address>
Generate new SSH host keys (yes/no) [yes]: <Press ENTER to accept>
This may take a few seconds...
Enter a password for the “admin” user:
Re-enter to confirm:
Enter the Management IP (MIP) address: <IP address>
```

Figure 3-2 Installing the first iSD-SSL

The setup utility is now finished, and after a short while you will get a login prompt as shown in Figure 3-3.

```
........
Setup successful, relogin to configure.
login:
```

Figure 3-3 Finishing the Initial Setup Utility

Log in as Administrator, and the Main menu is displayed. You can now continue the configuration of the iSD-SSL using the command line interface (CLI). For more information about the CLI, see "The Command Line Interface" on page 51.

Joining an Existing Cluster

Performing a **`join`** via the setup utility menu is the only way to add a new iSD-SSL to an existing cluster. Trying to do a **`new`** setup and give the same Management IP address will not work. The reason to this is that **`new`** indicates creating a new cluster, and each cluster must have a unique Management IP address.

NOTE – All the iSD-SSLs in a cluster must run the same software version. To adjust a new iSD-SSL to the same software version as on the iSD-SSLs in the cluster before performing a join setup, see "Reinstalling the iSD-SSL Software" on page 38.
Or, to upgrade a cluster to the same software version as on the new iSD-SSL, see "Performing Minor/Major Release Upgrades" on page 42. You can check the currently installed software version by typing the command **`/boot/cur`**.

After having installed the first iSD-SSL, additional iSD-SSLs may be added to the same cluster by specifying the Management IP (MIP) address that identifies the cluster. To check the Management IP of an existing cluster, connect to the cluster and use the command **`/cfg/sys/cur`**. Among various other system information, the Management IP address of the cluster is listed.

Add iSD-SSLs to an existing cluster by selecting **`join`** from the Setup menu in the new iSD-SSL, after it has booted.

```
>> Setup# join
Setup will guide you through the configuration of the iSD.

Enter IP address for this iSD: <IP address>

The system is initialized by connecting to the management server
on an existing iSD, which must be operational and initialized.
Enter the Management IP (MIP) address: <IP address>
Enter the existing admin user password:
Enter the type of this iSD (master/slave) [master]:
```

Figure 3-4 Adding an Extra iSD-SSL

Assign a unique IP address to the device and provide the Management IP address of the (existing) cluster to which you want to add the iSD-SSL. Make sure that the IP address you assign to the device is within the same network range as the Management IP address of the cluster. If not, a built-in control function in the Setup utility will detect the error and ask you to check your configuration before trying again.

Type the correct Administrator password for the cluster whose Management IP address you provided.

When adding up to three additional iSD-SSLs to a cluster containing a single iSD-SSL, you may configure each additional iSD-SSL as either master or slave. For up to three additional iSD-SSLs, the default setting is **`master`**. When adding one or more iSD-SSLs to a cluster that already contains four iSD-SSLs, each additional iSD-SSL is automatically configured as **`slave`**. It is recommended that there are 2-4 master iSD-SSLs in each cluster, so in most cases there is no need to change the default setting. If needed, you can always reconfigure an iSD-SSL by changing the Type setting after the initial setup. For more information, see the **`type`** command under "iSD Host Configuration Menu" on page 96.

The setup utility is now finished. The iSD-SSL that was joined will automatically pick up all other configuration data from one of the already installed iSD-SSLs in the cluster. After a short while you will get a login prompt as shown in Figure 3-5.

```
.......
Setup successful, relogin to configure.
login:
```

Figure 3-5 Finishing the Initial Setup Utility

Log in as Administrator, and the Main menu is displayed. You can now continue the configuration of the iSD-SSL using the command line interface (CLI). For more information about the CLI, see "The Command Line Interface" on page 51.

Reinstalling the iSD-SSL Software

Reinstalling the software is seldom required except in case of serious malfunction. When adding a new iSD-SSL to an existing cluster, and the software version of the new iSD-SSL is different from the iSD-SSLs in the cluster, you will also need to reinstall the software.

When you log in as the *boot* user and perform a reinstall of the software, the iSD-SSL is reset to its factory default configuration. All configuration data and current software is wiped out, including old software image versions or upgrade packages that may be stored in the flash memory card or on the hard disk. Also note that a reinstall must be performed on each iSD-SSL via a console connection.

NOTE – As a reinstall wipes out all configuration data (including network settings), it is a good idea to first save all configuration data to a file on a TFTP server. Using the **`ptcfg`** command, installed keys and certificates are included in the configuration data, and can later be restored by using the **`gtcfg`** command. For more information about these commands, see the respective command under "Configuration Menu" on page 73. If you would prefer to make backup copies of your keys and certificates separately, you can use the **`export`** or **`tftpexport`** command. For more information about these commands, see the respective command under "Certificate Management Menu" on page 77.

To reinstall an iSD-SSL you will need the following:

- Access to the iSD-SSL via a console connection.
- An install image, loaded on a TFTP server on your network.
- The host name or IP address of the TFTP server.
- The name of the install image.
- Log in as `user:` *boot*, `password:` *ForgetMe*

NOTE – Configure DNS parameters if you will be specifying host names. See "DNS Servers Menu" on page 95.

When performing a reinstallation of the iSD-SSL software, access to the iSD-SSLs must be accomplished via the console port. Log in as the *boot* user and provide the required information. Example:

```
login: boot
Password:
Enter IP address for this iSD [192.168.128.185]: <Press ENTER if the IP
address displayed within square brackets is correct.>
Enter network mask [255.255.255.0]: <Press ENTER if correct.>
Enter gateway IP address [192.168.128.1]: <Press ENTER if correct.>
Enter TFTP server address: 10.0.0.1
Enter file name of boot image: isdssl-boot.img
Downloading boot image...
Installing new boot image...
Done
Restarting...
Restarting system.

Login:
```

Figure 3-6 Reinstalling the iSD-SSL Software

If the iSD-SSL has not been configured for network access previously, you must provide information about network settings such as IP address, network mask, and gateway IP address. After the new boot image has been installed, the iSD-SSL will reboot and you can log in again when the login prompt appears. This time, log in as the *admin* user to enter the Setup menu. For more information about the choices in the Setup menu, see page 34 and onwards.

CHAPTER 4

Upgrading the iSD-SSL Software

The iSD-SSL software image is the executable code running on the iSD-SSL. A version of the image ships with the iSD-SSL, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your iSD-SSL. Before upgrading, please check the accompanying release notes for any specific actions to take for the particular software upgrade package or install image.

There are three types of upgrades:

- **Minor release upgrade:** This is typically a bug fix release. Usually this kind of upgrade can be done without the iSD-SSL rebooting. Thus, the normal operation and traffic flow is maintained. All configuration data is retained. When performing a minor upgrade, you should connect to the Management IP address of the cluster you want to upgrade.
- **Major release upgrade:** This kind of release may contain both bug fixes as well as feature enhancements. The iSD-SSL may automatically reboot after a major upgrade, since the operating system may have been enhanced with new features. All configuration data is retained. When performing a major upgrade, you should connect to the Management IP address of the cluster you want to upgrade.
- **Upgrading from software version 1.0 to software version 2.0:** This comprehensive upgrade is performed from an Alteon Web switch, and wipes the current configuration of all iSD-SSLs. After the upgrade is complete, you will need to perform an initial setup on each upgraded iSD-SSL.

Upgrading the software on your iSD-SSL requires the following:

- Loading the new software upgrade package or install image onto a TFTP server on your network.
- Downloading the new software from the TFTP server to your iSD-SSL.

Performing Minor/Major Release Upgrades

The following description applies to a minor or a major release upgrade.

To upgrade the iSD-SSL you will need the following:

- Access to one of your iSD-SSLs via a remote connection (Telnet or SSH), or a console connection.
- The software upgrade package (typically a compressed tar-file), loaded on a TFTP server on your network.
- The host name or IP address of the TFTP server. If you choose to specify the host name, please note that the DNS parameters must have been configured. For more information, see "DNS Servers Menu" on page 95.
- The name of the software upgrade package.

It is important to realize that the set of installed iSD-SSLs you are running in a cluster are cooperating to give you a single system view. Thus, when performing a minor or a major release upgrade, you only need to be connected to the Management IP address of the cluster. The upgrade will automatically be executed on all the iSD-SSLs in operation at the time of the upgrade. All configuration data is retained. For a minor upgrade, normal operations are usually unaffected, whereas a major upgrade may cause the iSD-SSL to reboot.

Access to the Management IP address can be accomplished via a Telnet connection or SSH (Secure Shell) connection. Note however that Telnet and SSH connections to the iSD-SSL are disabled by default, after the initial setup has been performed. For more information about enabling Telnet and SSH connections, see "Connecting to the iSD-SSL" on page 52. When you have gained access to the iSD-SSL, use the following procedure.

1. **At the Main menu prompt, enter:**

```
>> Main# boot/tftp
```

2. **Enter the host name or IP address of the TFTP server.**

```
Enter TFTP server host: <host name or IP address>
```

3. **Enter the name of the new software file on the TFTP server.**

```
Enter filename on server: <filename.tar.gz>
Received 13056048 bytes in 27.2 seconds

ok

>> Boot#
```

The exact form of the name will vary by TFTP server. However, the file location is normally relative to the TFTP directory (usually `/tftpboot`).

Activating the Software Upgrade Package

The iSD-SSL can hold up to two versions of the same major software release simultaneously (version 2.0 and version 2.1 for example, but not version 1.0 and version 2.0). When a new version of the software is downloaded to the iSD-SSL, the software package is decompressed automatically and marked as *unpacked*. After you *activate* the unpacked software version (which may cause the iSD-SSL to reboot), the software version is marked as *permanent*. The software version previously marked as *permanent* will then be marked as *old*.

For minor and major releases, the software change will take part synchronously among the set of iSD-SSLs in a cluster. If one or more iSD-SSLs are not operational when the software is upgraded, they will automatically pick up the new version when they are started.

NOTE – If *more than one* software upgrade has been performed to a cluster while an iSD-SSL has been out of operation, the iSD-SSL must be reinstalled with the software version currently in use in that cluster. For more information about how to perform a reinstall, see "Reinstalling the iSD-SSL Software" on page 38.

When you have downloaded the software upgrade package, you can inspect its status with the **`cur`** command.

1. **At the `Boot#` prompt, enter:**

```
>> Boot# cur
2.0.1 unpacked
2.0 permanent
```

The downloaded software upgrade package is indicated with the status `unpacked`. The software versions can be marked with one out of four possible status values. The meaning of these status values are:

- **unpacked** means that the software upgrade package has been downloaded and automatically decompressed.
- **permanent** means that the software is operational and will survive a reboot of the system.
- **old** means the software version has been permanent but is not currently operational. If a software version marked *old* is available, it is possible to switch back to this version by *activating* it again.
- **current** means that a software version marked as *old* has been activated. As soon as the system has performed the necessary health checks, the *current* status changes to *permanent*.

To activate the unpacked software upgrade package, use the **`activate`** command.

2. **At the `Boot#` prompt, enter:**

```
>> Boot# activate 2.0.1
Confirm action 'activate'? [y/n]: y
Activate ok, relogin                                  <you are logged out here>
Restarting system.

login:
```

As a result of running the **`activate`** command, you will be logged out and have to log in again. The reason for this is the command line interface (CLI) software may be upgraded as well. Wait until the login prompt appears again, which may take up to 2 minutes depending on your type of hardware platform and whether the system reboots.

3. **After having logged in again, enter the following command:**

```
>> Main# boot/cur
2.0.1 permanent
2.0 old
```

In this example version 2.0.1 is now operational and will survive a reboot of the system, while the software version previously indicated as *permanent* now is marked as *old*.

NOTE – If you encounter serious problems while running the new software version, you can revert to the previous software version (now indicated as *old*). To do this, *activate* the software version indicated as *old*. When you log in again after having activated the *old* software version, its status is indicated as *current* for a short while. After about one minute, when the system has performed the necessary health checks, the *current* status is changed to *permanent*.

Upgrading iSD-SSLs from Software Version 1.0 to Software Version 2.0

If you have one or more iSD-SSLs running software version 1.0, you need to upgrade them to software version 2.0 in order to run them in the same cluster as iSD-SSLs with software version 2.0.

To upgrade an iSD-SSL from software version 1.0 to software version 2.0, the iSD-SSL must be connected to an Alteon Web switch. Because version 1.0 is controlled via the Alteon Web switch, you will start the upgrade by issuing the **`update`** command on the Web switch. After the upgrade is complete, all configuration is performed directly on the iSD-SSL via the built-in command line interface. This is a major difference from version 1.0, where all configuration was made through the Web switch.

NOTE – Upgrading from version 1.0 to version 2.0 wipes all configuration data (including network settings). You should therefore dump your current configuration to a TFTP server for your own reference. You should also make sure that you have backups of the certificates and keys currently in use. Preferably, place the backup files of certificates and keys on a TFTP server, from which they can be downloaded and installed after the upgrade is complete. Also note the starting IP address for the iSD-SSLs, in case you want to assign the same range of IP addresses to the upgraded iSD-SSLs.

Upgrading an iSD-SSL from software version 1.0 to version 2.0 requires the following:

- Log in access rights as *admin* user on the Web switch.
- An install image, loaded on a TFTP or FTP server on your network.
- The IP address of the TFTP or FTP server on which the install image is loaded.
- Access to the upgraded iSD-SSLs via a console connection.

1. **On the Web switch, access the SSL Offload Application menu by entering:**

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

2. **On the Web switch, initiate the upgrade process by entering:**

```
>> SSL Offload Application# update
Enter IP address of remote server: <IP address>
TFTP (t) or Anonymous FTP (f)? <t for TFTP or f for FTP>
Waiting a maximum of 10 minutes per iSD for <number of iSDs>
iSD(s).........

iSD(s) updated successfully. Rebooting iSD(s).

Command succeeded as iSD.
```

Wait until all the iSDs in the cluster have been upgraded.The message “iSD(s) updated successfully” only indicates that the install image was downloaded and unpacked successfully to each iSD-SSL in the cluster. The actual upgrading of the iSD(s) has not begun when this message is displayed.

Upgrading one iSD-SSL should take approximately 10 minutes. If there are more than one iSD-SSL in the cluster, add approximately 90 seconds for each additional iSD-SSL. This is the time it takes to download and unpack the new software image, after which the iSD-SSLs in the cluster are upgraded in parallel.

The upgrade process is finished when the login prompt is displayed in the terminal window of an upgraded iSD-SSL, to which you have connected via a console connection. It is important that the process is not discontinued before it is finished, as this may disrupt the flash memory card (when upgrading an iSD100-SSL). Do not proceed with the following steps until you have made sure that all iSD-SSLs in the cluster are upgraded.

3. **On the Web switch, turn off iSD-SSL processing.**

```
# /cfg/isd/off
```

4. **On the Web switch, disable the IP address assignment for a range of iSD units.**

```
# /cfg/isd/ipnum 0
```

In software version 2.0, the assignment of IP addresses is made directly on the iSD-SSL. Therefore, IP address assignment should be disabled on the Web switch.

5. **On the Web switch, remove the starting IP address for iSD-SSL units.**

   ```
   # /cfg/isd/ipstart 0.0.0.0
   ```

   For the same reason as above, the starting IP address for iSD-SSL units should be reset to 0.0.0.0

6. **On the Web switch, remove real server group 256 that was automatically assigned to the iSD-SSL(s) when first set up.**

   ```
   # /cfg/slb/group 256/del
   ```

7. **On the Web switch, apply and save the configuration changes.**

   ```
   # apply
   # save
   ```

8. **On the upgraded iSD-SSL, connect via the console port and enter the Setup menu.**

   After having connected to an upgraded iSD-SSL via the console port, press ENTER until the login prompt appears. Log in as `user:` *admin*, `password:` *admin* and the Setup menu is displayed.

9. **Perform the initial setup on the iSD-SSL(s).**

   ```
   [Setup Menu]
   join    - Join an existing iSD-SSL cluster
   new     - Initialize iSD-SSL as a new installation
   boot    - Boot Menu
   ```

   Install the first iSD-SSL by using the **`new`** command, and each subsequent iSD-SSL by using the **`join`** command to install them in the same cluster.

   Note that you must establish a new console connection to each upgraded iSD-SSL before you can access the Setup menu. After having established a console connection, follow the instructions on page 35 and onwards.

10. **Make configuration changes on an upgraded iSD-SSL.**

    After all the iSD-SSLs are members of a cluster, configuration changes need only be made to one iSD-SSL in the cluster. The changes made to one member of the cluster are distributed to all members automatically. After the initial setup is complete, you may also connect to an iSD-SSL via a Telnet or SSH connection rather than via a console connection in order to make configuration changes. Note however that Telnet and SSH connections to the iSD-SSL are disabled by default, after the initial setup has been performed. For more information about enabling Telnet and SSH connections, see “Connecting to the iSD-SSL” on page 52.

11. **On the Web switch, assign a real server group number to the upgraded iSD-SSL(s).**

    On the Web switch, real server group number 256 was automatically assigned to the iSD-SSL(s) running software version 1.0 when first set up. After the upgrade to software version 2.0 however, you need to assign a real server group number for the iSD-SSL(s) manually on the Web switch. You can choose to assign real server group number 256 to the upgraded iSD-SSL(s), and thereby continue to use your redirect filters without changing them.

    Or, you can assign a new server real group number to the upgraded iSD-SSL(s). If you prefer to do so, you must also change the group number in filters where there is an **`action redir`** instruction pointing to real server group number 256.

12. **Add the certificates and keys that were in use before the upgrade.**

    Before taking the upgraded iSD-SSL(s) into operation, you must also add the certificates and keys that were in use before the upgrade. For more information about different methods to accomplish this, see “Adding Certificates to the iSD-SSL” on page 156.

CHAPTER 5

The Command Line Interface

This chapter explains how to access the iSD-SSL via the command line interface (CLI).

The iSD-SSL version 2.0 software included in your iSD-SSL provides means for accessing, configuring, and viewing information and statistics about the iSD-SSL. By using the built-in, text-based command line interface and menu system, you can access and configure the iSD-SSL either via a local console connection (using a computer running terminal emulation software), or via a remote session using either a Telnet client or an SSH client.

When using a Telnet client or SSH client to connect to a cluster of iSD-SSLs, always connect to the IP address of the MIP (Management IP). Configuration changes are automatically propagated to all members of the cluster. However, when using the commands **`halt`**, **`reboot`**, or **`teardown`** (available in the Boot menu), you should connect to the IP address of the particular iSD-SSL on which you want to perform these commands, or connect to that iSD-SSL via a console connection.

Connecting to the iSD-SSL

You can access the command line interface in two ways:

- Using a console connection via the console port
- Using a Telnet connection or SSH connection over the network

Establishing a Console Connection

A console connection is required when performing the initial setup, and when reinstalling the iSD-SSL software as the *boot* user. When logging in as *root* user for advanced troubleshooting purposes, a console connection is also required.

Requirements

To establish a console connection with the iSD-SSL, you will need the following:

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

Table 5-1 Console Configuration Parameters

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

- A standard serial cable with a male DB9 connector (for specifics, see "Connecting a Terminal to the iSD-SSL" on page 192).

Procedure

1. **Connect the terminal to the Console port using the serial cable.**
2. **Power on the terminal.**
3. **To establish the connection, press ENTER on your terminal.**

   You will next be required to enter a password for access to the iSD-SSL. (For more information, see "Installing a Single iSD-SSL" on page 35).

Establishing a Telnet Connection

A Telnet connection offers the convenience of accessing the iSD-SSL from any workstation connected to the network. Telnet access provides the same options for user access and administrator access as those available through the console port.

To configure the iSD-SSL for Telnet access, you need to have a device with Telnet client software located on the same network as the iSD-SSL. The iSD-SSL must have an IP address and a Management IP address. If you have already performed the initial setup by selecting **new** or **join** in the Setup menu, the assignment of IP addresses is complete.

When making configuration changes to a cluster of iSD-SSLs via Telnet, it is recommended that you connect to the IP address of the MIP. However, if you want to halt or reboot a particular iSD-SSL in a cluster, or reset all configuration to the factory default settings, you must connect to the IP address of the particular iSD-SSL. This also applies when using an SSH connection instead of a Telnet connection. To view the IP addresses of all iSD-SSLs in a cluster, use the command **`/info/isdlist`**.

Running Telnet

Once the IP parameters on the iSD-SSL are configured, you can access the CLI using a Telnet connection. To establish a Telnet connection with the iSD-SSL, run the Telnet program on your workstation and issue the Telnet command, followed by the iSD-SSL IP address.

```
telnet <IP address>
```

You will then be prompted to enter a valid password. For more information about different access levels and initial passwords, see "Accessing the iSD-SSL" on page 55.

Enabling and Restricting Telnet Access

Telnet access to the iSD-SSL is disabled by default, for security reasons. However, depending on the severity of your security policy, you may want to enable Telnet access. You may also restrict Telnet access to one or more specific machines.

For more information on how to enable Telnet access, see the **`telnet`** command under "System Configuration Menu" on page 93. For more information on how to restrict Telnet access to one or more specific machines, see the **`add`** command under "Access List Menu" on page 97.

Establishing a Connection Using SSH (Secure Shell)

When accessing the iSD-SSL from a workstation connected to the network using a Telnet connection, it is important to keep in mind that the communication channel is not secure. All data flowing back and forth between the Telnet client and the iSD-SSL is sent unencrypted (including the password), and there is no server host authentication.

By using an SSH client to establish a connection over the network, the following benefits can be achieved:

- Server Host Authentication
- Encryption of Management Messages
- Encryption of Passwords for User Authentication

Running an SSH Client

Connecting to the iSD-SSL using a SSH client is similar to connecting via Telnet. As with Telnet, the IP parameters on the iSD-SSL need to be configured in advance. After providing your user name and password, the command line interface in the iSD-SSL is accessible the same way as when using a Telnet client. However, since a secured and encrypted communication channel is set up even before the user name and password is transmitted, all management messages are encrypted.

During the initial setup of the iSD-SSL, you are provided with the choice to generate new SSH host keys. It is recommended that you do so, in order to maintain a high level of security when connecting to the iSD-SSL using a SSH client. If you fear that your SSH host keys have been compromised, you can create new host keys any time by using the command **`/cfg/sys/gensshkey`**. When reconnecting to the iSD-SSL after having generated new host keys, your SSH client will display a warning that the host identification (or host keys) has been changed.

For more information about different access levels and initial passwords, see Accessing the iSD-SSL.

Enabling and Restricting SSH Access

SSH access to the iSD-SSL is disabled by default. However, depending on the severity of your security policy, you may want to enable SSH access. You may also restrict SSH access to one or more specific machines.

For more information on how to enable SSH access, see the **`ssh`** command under "System Configuration Menu" on page 93. For more information on how to restrict SSH access to one or more specific machines, see the **`add`** command under "Access List Menu" on page 97.

Accessing the iSD-SSL

To enable better iSD-SSL management and user accountability, four categories of users can access the iSD-SSL:

- The Operator is only granted read access to the menus and information appropriate to this user access level. The Operator cannot make any changes to the configuration.
- The Administrator can make any changes to the iSD-SSL configuration. Thus, the Administrator has read and write access to all menus, information and configuration commands in the iSD-SSL.
- The Boot user can only perform a reinstallation. For security reasons, it is only possible to log in as the Boot user via the console port using terminal emulation software.
- The Root user is granted full access to the underlying Linux operating system. For security reasons, it is only possible to log in as the Root user via the console port using terminal emulation software. Root user access should mainly be reserved for advanced troubleshooting purposes, under guidance from the Alteon WebSystems customer support.

  For more information, see "Contacting Alteon WebSystems" on page 16.

Access to the iSD-SSL command line interface and settings is controlled through the use of four predefined user accounts and passwords. Once you are connected to the iSD-SSL via a console connection or remote connection (Telnet or SSH), you are prompted to enter a user account and the corresponding password. The user account and default password for each access level are listed in the following table.

NOTE – The default Administrator password can be changed during the initial configuration (see "Installing a Single iSD-SSL" on page 35). For the Operator user, the Boot user, and the Root user however, the default passwords are used even after the initial configuration. It is therefore recommended that you change the default iSD-SSL passwords soon after the initial configuration, and as regularly as required under your network security policies. For more information about how to change a user account password, see "User Password Menu" on page 101.

Table 5-2 User Access Levels

User Account	Access Level Description	Default Password
oper	The Operator is allowed read access to some of the menus and information.	`oper`
admin	The Administrator is allowed both read and write access to all menus, information and configuration commands.	`admin`
boot	The boot user can only perform a reinstallation of the software, and only via a console connection.	`ForgetMe`
root	The root user has full access to the underlying Linux operating system, but only via a console connection.	`ForgetMe`

CLI vs. Setup

Once the administrator password is verified, you are given complete access to the iSD-SSL. If the iSD-SSL is still set to its factory default configuration, the system will run Setup (see "Installing a Single iSD-SSL" on page 35), a utility designed to help you through the first-time configuration process. If the iSD-SSL has already been configured, the Main menu of the CLI is displayed instead.

The following figure shows the Main menu with administrator privileges.

```
[Main Menu]
      info        - Information Menu
      stats       - Statistics Menu
      cfg         - Configuration Menu
      boot        - Boot Menu
      diff        - Show pending config changes   [global command]
      apply       - Apply pending config changes  [global command]
      revert      - Revert pending config changes [global command]
      help        - Show command help Menu        [global command]
      exit        - Exit [global command, always available]
```

Figure 5-1 Administrator Main Menu

Command Line History and Editing

For a description of global commands, shortcuts, and command line editing functions, see Chapter 6, "iSD-SSL Command Reference".

Idle Timeout

The iSD-SSL will disconnect your local console connection or remote connection (Telnet or SSH) after 10 minutes of inactivity. This value is fixed and cannot be changed.

CHAPTER 6

iSD-SSL Command Reference

This chapter describes how to use the command line interface on the iSD-SSL. The chapter also provides explanations of all available commands.

Menu Basics

The iSD-SSL command line interface (CLI) is used for viewing iSD-SSL information and statistics. In addition, the administrator can use the CLI for configuring all levels of iSD-SSL.

The various CLI commands are grouped into a series of menus and sub-menus. Each menu displays a list of commands and/or sub-menus that are available, along with a summary of what each command will do. Below each menu is a prompt where you can enter any command appropriate to the current menu.

This chapter describes the Main menu commands, and provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

If you have previously had one or more iSD-SSLs running software version 1.0 connected to an Alteon Web switch equipped with Web OS 8.1 or higher, you will recall that all configuration of the iSD-SSLs was made through the command line interface of the Web switch. Even when using iSD-SSLs running software version 2.0 together with an Alteon Web switch, commands such as **`/cfg/isd`** and **`/info/isd`** still remain in the Web switch menu system. However, you cannot use Web OS commands to configure iSD-SSLs running software version 2.0. All configuration is done through the built-in command line interface of the iSD-SSLs. For a translation table covering iSD-SSL version 1.0 commands performed on the Web switch, and the corresponding commands now performed on the iSD-SSL 2.0, see “Command Translation Table” on page 207.

Global Commands

Some basic commands are recognized throughout the menu hierarchy. These commands are useful for obtaining online help, navigating through menus, and for applying and saving configuration changes:

Table 6-1 Global Commands

Command	Action
`help`	Display a summary of the global commands.
`.`	Display the current menu.
`..`	Go up one level in the menu structure.
`up`	Go up one level in the menu structure.
`/`	If placed at the beginning of a command, go to the Main menu. Otherwise, this is used to separate multiple commands placed on the same line.
`diff`	Show any pending configuration changes.
`apply`	Apply pending configuration changes.
`revert`	Remove pending configuration changes between "apply" commands. Use this command to restore configuration parameters set since last "apply" command.
`paste`	Lets you restore a saved configuration that includes private keys. Before pasting the configuration, you need to provide the password phrase you specified when selecting to include the private keys in the configuration dump. For more information, see the **dump** command under the Configuration Menu on page page 73.
`exit`	Exit from the command line interface and log out.
`quit`	Same as Exit.
`CTRL, ^`	Exit from the command line interface in case the iSD-SSL has stopped responding. This command should only be used when connected to a specific iSD-SSL via a console connection, not when connected to the Management IP of the cluster via a Telnet or SSH connection.
`ping`	Use this command to verify station-to-station connectivity across the network. The format is as follows: **ping <***address* [*tries* [*delay*]]> Where *address* is the host name or IP address of the device, *tries* (optional) is the number of attempts (1-32), and *delay* (optional) is the number of milliseconds between attempts. The DNS parameters must be configured if specifying host names (see "DNS Servers Menu" on page 95).

Table 6-1 Global Commands

Command	Action
`traceroute`	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: **`traceroute <`***address* [*max-hops* [*delay*]]> Where *address* is the host name or IP address of the target station, *max-hops* (optional) is the maximum distance to trace (1-16 devices), and *delay* (optional) is the number of milliseconds for wait for the response. As with `ping`, the DNS parameters must be configured if specifying host names.
`nslookup`	Use this command to find the IP address or host name of a machine. In order to use this command, you must have configured the iSD-SSL to use a DNS server. If you did not specify a DNS server during the initial setup procedure, you can add a DNS server at any time by using the command **`/cfg/sys/dns/add`**.
`pwd`	Display the command path used to reach the current menu.
`lines` *n*	Set the number of lines (*n*) that is displayed on the screen at one time. The default value is 24 lines. When used without a value, the current setting is displayed.
`verbose` *n*	Sets the level of information displayed on the screen: **`0`** =Quiet: Nothing appears except errors—not even prompts. **`1`** =Normal: Prompts and requested output are shown, but no menus. **`2`** =Verbose: Everything is shown. The default level is 2. When used without a value, the current setting is displayed.

Command Line History and Editing

Using the command line interface, you can retrieve and modify previously entered commands with just a few keystrokes. The following options are available globally at the command line:

Table 6-2 Command Line History and Editing Options

Option	Description
`history`	Display a numbered list of the last 10 previously entered commands.
`!!`	Repeat the last entered command.
`!`*n*	Repeat the n^{th} command shown on the history list.

Table 6-2 Command Line History and Editing Options

Option	Description
pushd	“Bookmarks” your current position in the menu structure. After moving to another level or command in the menu structure, you can easily return to the bookmarked position by typing the **popd** command. The **pushd** command can be combined with command stacking, as in this example: >> Information# **`pushd /cfg/ssl/server 1/ssl`** >> SSL Settings for Server 1# When you issue the **popd** command, you are immediately taken back to the prompt from where you issued the **pushd** command, the Information prompt in this example.
popd	Takes you back to a position in the menu structure that has been “bookmarked” by using the **pushd** command.
<Ctrl-p>	(Also the up arrow key.) Recall the *previou*s command from the history list. This can be used multiple times to work backward through the last 10 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n>	(Also the down arrow key.) Recall the *next* command from the history list. This can be used multiple times to work forward through the last 10 commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the *end* of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor *back* one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor *forward* one position to the right.
<Backspace>	(Also the Delete key.) Erase one character to the left of the cursor position.
<Ctrl-d>	*Delete* one character at the cursor position.
<Ctrl-k>	*Kill* (erase) all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redraw the screen.
<Ctrl-c>	Abort an on-going transaction and display the current menu.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

Command Line Interface Shortcuts

Command Stacking

You can type multiple commands separated by forward slashes (`/`) on a single line in order to access a submenu and one of the related menu options. Type as many commands as required to access the desired submenu and menu option. For example, the keyboard shortcut to access the **`list`** command in the NTP Servers menu from the Main menu prompt is as follows:

```
>> Main# cfg/sys/ntp/servers/list
```

You can also use command stacking to go up one level in the menu system and then go directly to another submenu and one of the related menu options. For example, to go up one level from the NTP Servers menu to the NTP Settings menu, and then directly to the **`cur`** command you would type:

```
>> NTP Servers# ../cur
```

Command Abbreviation

Most commands can be abbreviated by entering the first characters which distinguish the command from the others in the same menu or sub-menu. For example, the command shown in the first example above could also be entered as follows:

```
Main# c/sy/n/s/l
```

Tab Completion

By typing the first letter of a command at any menu prompt and pressing TAB, all commands in that menu beginning with the letter you typed is displayed. By typing additional letters, you can further refine the list of commands or options displayed. If only one command matches the letter(s) you typed, that command is supplied on the command line when pressing TAB. You can then execute the command by pressing ENTER. If the TAB key is pressed without any input on the command line, the currently active menu is displayed.

The Main Menu

The Main menu appears after a successful connection and login. Figure 6-1 shows the Main menu as it appears when logged in as Administrator. Note that some of the commands are not available when logged in as Operator.

```
[Main Menu]
      info         - Information Menu
      stats        - Statistics Menu
      cfg          - Configuration Menu
      boot         - Boot Menu
      maint        - Maintenance Menu
      diff         - Show pending config changes   [global command]
      apply        - Apply pending config changes  [global command]
      revert       - Revert pending config changes [global command]
      help         - Show command help Menu        [global command]
      exit         - Exit [global command, always available]
```

Figure 6-1 Administrator Main Menu

Menu Summary

- **Information menu**

  Provides sub-menus for displaying information about the current status of the iSD-SSL. For more information, see page 65.

- **Statistics menu**

  Provides sub-menus for displaying iSD-SSL performance statistics. For more information, see page 68.

- **Configuration menu**

  Provides sub-menus for configuring the iSD-SSL. Some of the commands in the Configuration menu are available only from the administrator login. For more information, see page 73.

- **Boot menu**

  Is used for upgrading iSD-SSL software and for rebooting, if necessary. The Boot menu is only accessible when logged in as Administrator. For more information, see page 107.

- **Maintenance menu**

  Is used for sending a technical support dump to a TFTP server. For more information, see page 109.

/info
Information Menu

```
[Information Menu]
      servers     - Show configured SSL servers
      certs       - Show configured certificates
      isdlist     - Show all iSDs and their operational status
      events      - Inspect events Menu
      dump        - Dump all information
```

The Information menu is used for viewing information and events for the iSD-SSLs that are in a cluster.

Table 6-3 Information Menu Options (/info)

Command Syntax and Usage
`servers` Displays the current SSL server settings, including SSL specific settings for each configured virtual SSL server.
`certs` Displays the certificate name, serial number, expiration date, and key size for each installed certificate. Information related to the subject of the certificate is also displayed.
`isdlist` Displays the IP addresses, master/slave assignments, CPU usage, memory usage, and operational status for all the iSD-SSLs in the cluster. An asterisk (*) in the MIP column indicates which iSD-SSL in the cluster is currently is control of the Management IP. An asterisk (*) in the Local column indicates the particular iSD-SSL to which you have connected. For an example screen output, see page 66.
`events` Displays the Events menu. To view menu options, see page 66.
`dump` Displays all information for each menu option in the Information menu, including pending alarms from the Events menu. For an example screen output, see page 67.

/info/events

Events Menu

```
[Events Menu]
      alarms     - List all pending alarms
      download   - Download the event log file
```

The Events menu is used for viewing active alarms and events that have been logged.

Table 6-4 Events Menu Options (/info/events)

Command Syntax and Usage
`alarms` Displays all alarms in the active alarm list by their main attributes: severity level, alarm ID number, date and time when triggered, alarm name, sender, and cause.
`download` *<host name or IP address> <file name on host>* Lets you download the event log file from the iSD-SSL cluster to a file on a TFTP server. You need to specify the IP address or host name of the TFTP server, as well as a file name.

/info/isdlist

iSD List Command

```
>> Information# isdlist
IP addr           type     MIP   local  cpu(%)   mem(%)    op
192.168.128.122   master    *           1        14        up
192.168.128.123   master           *    1        14        up
192.168.128.124   master                1        14        up
192.168.128.125   slave                                  down
```

/info/dump

Information Dump Command

```
Information:
  Server 1:
    Server name = test_server
    IP addr of SSL server = 192.168.128.187
    Listen port of SSL server = 443 (https)
    Real server IP = 0.0.0.0
    Real server port = 81
    Type (generic/http) = generic
    Transparent proxy mode (on/off) = on
    Enable SSL server = enabled
      SSL Settings for Server 1:
        Server certificate = 1
        SSL cache size = 8000
        SSL cache timeout = 5m
        List of accepted signers of client certificates =
        List of CA chain certificates =
        Protocol version = ssl3
        Certificate verification level = none
        Cipher list = ALL
  Certificate 1:
    Certificate name = test_cert
    Serial number:  0 (0x0)
    Expire:  Mar  7 09:08:12 2002 GMT
    Certificate subject:
       C=US
       ST=Oaklafornia
       L=Testing
       O=Test Inc.
       OU=test dept
       CN=www.dummyssltesting.com/Email=tester@dummyssltesting.com
    Validate: key and certificate match.
    Key is of size 1024.
  IP addr           type     MIP   local  cpu(%)   mem(%)    op
  192.168.128.122   master    *           1        14        up
  192.168.128.123   master          *     1        14        up
  192.168.128.124   master                1        14        up
  192.168.128.125   slave                                  down
  Events:
    ** (alarm) Active Alarm List *********************************
    Severity Id Time Name Sender Cause Misc
    -------- -- ---- ---- ------ ----- ----
```

/stats
Statistics Menu

```
[Statistics Menu]
      ssl         - SSL Server statistics
      activesess  - Number of currently active request sessions
      totalsess   - Total completed request sessions
      clear       - Clear all statistics for all IPs
      dump        - Dump all information
```

The Statistics menu is used for viewing various iSD-SSL performance statistics.

Table 6-5 Statistics Menu Options (/stats)

Command Syntax and Usage
`ssl` *<virtual SSL server number (1-256)>* Displays the SSL statistics menu for a specific virtual SSL server. To view menu options, see page 69.
`activesess` Displays the number of currently active request sessions.
`totalsess` Displays the total number of completed request sessions.
`clear` Resets all statistics to zero.
`dump` Displays all statistics. For details, see page 72.

`/stats/ssl` *<virtual SSL server number>*

SSL Statistics Menu

```
[SSL Statistics (1) Menu]
      accept      - SSL accept
      renegotiat  - SSL renegotiate requests
      handshakeg  - SSL handshakes completed
      cachemisses - SSL cache misses
      cachetimeo  - SSL cache timeout
      cachefull   - SSL cache full
      cachehits   - SSL cache hits
      revocation  - Client cert revocations
      cipherrewr  - HTTP weak cipher rewrites
      becnctfail  - Failed backend server connects
      tps         - SSL transactions/sec
      dump        - Dump all stats
```

The SSL Statistics menu is used for viewing various statistics for a virtual SSL server, specified by its index number.

Table 6-6 SSL Statistics Menu Options (/stats/ssl #)

Command Syntax and Usage
`accept` Displays the number of initiated SSL client connections.
`renegotiate` Displays the number of times clients have requested a renegotiation of the SSL connection.
`handshakegood` Displays the number of successfully completed SSL handshakes. The number of failed SSL handshakes equals the sum of the **`accept`** and **`renegotiate`** numbers, minus the **`handshakegood`** numbers.

Table 6-6 SSL Statistics Menu Options (/stats/ssl #)

Command Syntax and Usage

`cachemisses`

Displays the number of times clients have made requests to reuse a particular session ID, and that session ID was not found in the SSL cache.

If there is a high number of cache misses in combination with a high value for **`cachefull`**, you may consider increasing the SSL cache size of the virtual SSL server. Type the command **`/cfg/ssl/server`**, specify the appropriate virtual SSL server by index number, and then type the command **`ssl/cachesize`**. The default cache size is 8000 items.

If there is a high number of cache misses in combination with a low value for **`cachefull`**, you may consider increasing the **`cachettl`** value. Type the command **`/cfg/ssl/server`**, specify the appropriate virtual SSL server by index number, and then type the command **`ssl/cachettl`**.

The default SSL cache timeout value is 5 minutes.

`cachetimeout`

Displays the number of reuse attempts on SSL sessions still in the cache, and whose timeouts were initiated.

If there is a high number of cache timeouts, you may consider increasing the **`cachettl`** value for the virtual SSL server. Type the command **`/cfg/ssl/server`**, specify the appropriate virtual SSL server by index number, and then type the command **`ssl/cachettl`**.

The default SSL cache timeout value is 5 minutes.

`cachefull`

Displays the number of times when a new client session could not be cached due to the cache being full. If the **`cachefull`** value is high, you may consider increasing the SSL cache size of the virtual SSL server.

`cachehits`

Displays the number of times clients have made requests to reuse a particular session ID, and that session ID was found in the SSL cache.

`revocation`

Displays the number of revoked client certificates.

`cipherrewr`

Displays the number of HTTP weak cipher rewrites.

Table 6-6 SSL Statistics Menu Options (/stats/ssl #)

Command Syntax and Usage
`becnctfail` Displays the number of failed connections to backend servers.
`tps` Displays the number of SSL transactions per second.
`dump` Displays all statistics for the current virtual SSL server. For details, see page 72.

/stats/dump

Statistics Dump Command

```
Statistics:
  Number of currently active request sessions =
    1 (192.168.128.185:443) = 0
  Total completed request sessions =
    1 (192.168.128.185:443) = 7047

    SSL statistics (1):
      192.168.128.185 SSL accept = 467780
      192.168.128.185 SSL renegotiate requests = 0
      192.168.128.185 SSL handshakes completed = 467792
      192.168.128.185 SSL cache misses = 0
      192.168.128.185 SSL cache timeout = 0
      192.168.128.185 SSL cache full = 452039
      192.168.128.185 SSL cache hits = 3
      192.168.128.185 Client cert revocations = 0
      192.168.128.185 HTTP weak cipher rewrites = 0
      192.168.128.185 Failed backend server connects = 0
      192.168.128.185 SSL transactions/sec = 18
```

/stats/ssl *<virtual SSL server number>*/dump

SSL Statistics Dump Command

```
SSL statistics (1):
  192.168.128.185 SSL accept = 467780
  192.168.128.185 SSL renegotiate requests = 0
  192.168.128.185 SSL handshakes completed = 467792
  192.168.128.185 SSL cache misses = 0
  192.168.128.185 SSL cache timeout = 0
  192.168.128.185 SSL cache full = 452039
  192.168.128.185 SSL cache hits = 3
  192.168.128.185 Client cert revocations = 0
  192.168.128.185 HTTP weak cipher rewrites = 0
  192.168.128.185 Failed backend server connects = 0
  192.168.128.185 SSL transactions/sec = 18
```

/cfg
Configuration Menu

```
[Configuration Menu]
      ssl         - SSL Offload Menu
      sys         - System-wide Parameter Menu
      snmp        - SNMP Menu
      ptcfg       - Backup current configuration to TFTP server
      gtcfg       - Restore current configuration from TFTP server
      dump        - Dump configuration on screen for copy-and-paste
      paste       - Restore saved config with key [global command]
      cur         - Current settings
```

The Configuration menu is used for performing SSL and system-wide configuration, as well as for saving and restoring iSD-SSL configurations to and from a TFTP server.

Table 6-7 Configuration Menu Options (/cfg)

Command Syntax and Usage
`ssl` Displays the SSL Offload Configuration menu. To view menu options, see page 76.
`sys` Displays the System Configuration menu. To view menu options, see page 93.
`snmp` Displays the SNMP menu. To view menu options, see page 103.
`ptcfg` *<TFTP server> <file name>* Saves the current configuration, including private keys and certificates, to a TFTP server. The information is saved in a gzip compressed tar file, and can later be restored by using the **`gtcfg`** command. You are required to specify a password phrase before the information is sent to the TFTP server, and the password phrase you specify applies to all included private keys. If you restore the configuration by using the **`gtcfg`** command, you will be prompted for the password phrase you have specified.
`gtcfg` *<TFTP server> <file name>* Restores a configuration, including private keys and certificates, from a TFTP server. You need to provide the password phrase you specified when saving the configuration to the TFTP server.

Table 6-7 Configuration Menu Options (/cfg)

Command Syntax and Usage
`dump` Dumps the current configuration on screen in a format that allows you to restore the configuration without using a TFTP server. Save the configuration to a text file by performing a copy-and-paste operation to a text editor. The configuration can later be restored by pasting the contents of the saved text file at any command prompt in the command line interface. When pasted, the content is batch processed by the iSD-SSL. To view the pending configuration changes resulting from the batch processing, use the **`diff`** command. To apply the configuration changes, use the **`apply`** command. If you choose to include private keys in the configuration dump, you are required to specify a password phrase. The password phrase you specify applies to all private keys. When restoring a configuration that includes private keys, use the global **`paste`** command. Before pasting the configuration, you will be prompted for the password phrase you have specified.
`paste` Lets you restore a saved configuration that includes private keys. Before pasting the configuration, you need to provide the password phrase you specified when selecting to include the private keys in the configuration dump.
`cur` Displays the current settings. The **`cur`** command can only be used for viewing the current configuration on screen. In order to save the configuration for a possible restore later on, use the command **`dump`** or **`ptcfg`**.

Viewing, Applying and Removing Changes

As you use the configuration menus to set iSD-SSL parameters, the changes you make do not take effect immediately. All changes are considered "pending" until you explicitly apply them.

While configuration changes are in the pending state, you can do the following:

- View the pending changes
- Apply the pending changes
- Remove the pending changes

Viewing Pending Changes

You can view all pending configuration changes by entering **diff** at the menu prompt.

```
# diff
```

Applying Pending Changes

To make your configuration changes active, you must apply them. To apply pending configuration changes, enter **apply** at the menu prompt.

```
# apply
```

Removing Pending Changes

To remove your pending configuration changes before they have been applied, you enter the command **revert** at the menu prompt.

```
# revert
```

NOTE – The `diff`, `apply` and `revert` commands are global commands. Therefore, you can enter these commands at any menu prompt in the command line interface.

/cfg/ssl
SSL Main Menu

```
[SSL Menu]
      cert        - Certificate Menu
      server      - SSL Server Menu
      test        - Create test server and certificate
      quick       - Quick server setup wizard
      cur         - Current settings
```

The SSL Offload Configuration menu is used for configuring SSL certificates and virtual SSL servers. There are also menu options for viewing the current settings, and for creating a test server and a test certificate

Table 6-8 SSL Configuration Menu Options (/cfg/ssl)

Command Syntax and Usage
`cert` *<certificate number (1-256)>* Displays the Certificate menu, after you have typed the number of an existing certificate or a new certificate. To view menu options, see page 77.
`server` *<virtual SSL server number (1-256)>* Displays the SSL Server menu, after you have typed the number of an existing virtual SSL server or a new server. To view menu options, see page 83.
`test` *<virtual server IP address of virtual SSL test server>* Creates a test SSL server using the first available virtual SSL index number. The default name of the test server is `test_server`. A test certificate and key is also created for the test SSL server. When executing the **`test`** command, you are asked to specify the IP address of a virtual server (defined on the Web switch). The virtual server you specify will then make use of the services the test SSL server provides (HTTPS offload by default).
`quick` Starts the Quick Server Setup Wizard. For more information about using the Quick Server Setup Wizard, see "Using the Quick Server Setup Wizard" on page 175.
`cur` Displays the current settings for all certificates and virtual SSL servers.

/cfg/ssl/cert *<certificate number>*

Certificate Management Menu

```
[Certificate 1 Menu]
      name       - Set certificate name
      cert       - Set certificate
      key        - Set private key
      revoke     - Revocation Menu
      genkey     - Generate private key
      genclient  - Generate signed client certificate
      genserver  - Generate signed server certificate
      tftpcert   - TFTP certificate from remote machine
      tftpkey    - TFTP key from remote machine
      test       - Generate test certificate+key
      request    - Generate certificate request
      export     - Export certificate and key
      tftpexport - Export certificate and key with TFTP
      show       - Show certificate information
      info       - Show certificate subject information
      validate   - Check if key and certificate match
      keysize    - Show key size
      del        - Remove certificate
      cur        - Current settings
```

The Certificate menu is used for managing private keys and certificates. When accessing the Certificate menu, you are requested to specify the index number of the certificate you want to work with. To view basic information about all certificates, type the **/cfg/ssl/cur** command.

Table 6-9 Certificate Menu Options (/cfg/ssl/cert #)

Command Syntax and Usage
name *<certificate name>* Lets you assign a name to the certificate. The assigned name is mainly for your own reference.
cert Lets you paste the contents of a certificate file from a text editor. If the certificate file contains both the private key and the certificate, you can paste the entire contents at the menu prompt. In this case, you will not need to paste the private key separately using the **key** command. If the key has been password protected, you are prompted for the correct password phrase.

Table 6-9 Certificate Menu Options (/cfg/ssl/cert #)

Command Syntax and Usage

`key`

Lets you paste the contents of a key file from a text editor. Make sure the key file corresponds to the public key contained in the related certificate file. If the key has been password protected, you are prompted for the correct password phrase.

After you have added the private key you should use the **`validate`** command to ensure that the private key matches the public key in the current certificate.

`revoke`

Displays the Revocation menu. To view menu options, see page 82.

`genkey` <*Key size* [512|1024|2048]>

Lets you generate a PEM (Privacy Enhanced Mail) encrypted private key. After specifying a key length (512, 1024, or 2048 bits, with 1024 bits being the default key length), the key is generated immediately. Note that existing keys in the current certificate number are overwritten when you execute the **`apply`** command.

To save the key to a file, use the **`export`** command to display the encrypted key on-screen. You can then perform a copy-and-paste operation to a text editor and save the key to a file. When using the **`export`** command, you also have the option of protecting the key with a password by specifying a password phrase.

`genclient` <*country code*> <*state or province*> <*locality*> <*organization*> <*organizational unit*> <*common name*> <*e-mail address*> <*validity period*> <*key size*> <*serial number*> <*pass phrase*>

Generates a client certificate which is signed using the private key that relates to the current certificate. In order to authenticate a client using the generated certificate, you must also specify the current certificate as a CA certificate to the virtual SSL server handling authentication for the intended service. Specify CA certificates used for client authentication by typing the command **`/cfg/ssl/server`**. After specifying the desired SSL server, type the command **`ssl`** to access the SSL settings menu. Then type the command **`cacerts`** and specify the desired CA certificate by its index number.

Note: Only certificates that have the basic constraints CA:TRUE can be used to generate client certificates. For more information about generating client certificates, see "Generating Client Certificates in the iSD-SSL" on page 166.

Table 6-9 Certificate Menu Options (/cfg/ssl/cert #)

Command Syntax and Usage
`genserver` *<country code> <state or province> <locality> <organization> <organizational unit> <common name> <e-mail address> <validity period> <key size> <serial number> <pass phrase>* Generates a server certificate which is signed using the private key that relates to the current certificate. The generated server certificate is provided with key use options that are appropriate for server usage.The server certificate also contains the basic constraint CA:TRUE, which means the server certificate can be used for generating client certificates. However, in order to successfully validate those client certificates, the server certificate still must be specified as a CA certificate for the appropriate virtual SSL server.
`tftpcert` *<TFTP server> <file name>* Lets you install a certificate by downloading it from a TFTP server. If the certificate file contains both the private key and the certificate, you will not need to use the **`tftpkey`** command. If the private key has been password protected, you are prompted for the correct password phrase. Note that an existing certificate in the current certificate number is overwritten when you execute the **`apply`** command.
`tftpkey` *<TFTP server> <file name>* Lets you install a private key by downloading it from a TFTP server. If the key has been password protected, you are prompted for the correct password. Note that an existing key in the current certificate number is overwritten when you execute the **`apply`** command.
`test` *<country code> <state or province> <locality> <organization> <organizational unit> <common name> <e-mail address> <validity period> <key size>* Lets you generate a self-signed certificate and private key for testing purposes. After providing the requested information, the certificate and key are generated immediately. However, to activate the test certificate and key, you need to execute the **`apply`** command. **Note:** If a certificate and key already exist for the current certificate index number, they are overwritten when you execute the **`apply`** command. You should therefore always choose an unused certificate index number before creating a test certificate. To check if a certificate and key already exist for the current index number, type the command **`info`**.

Table 6-9 Certificate Menu Options (/cfg/ssl/cert #)

Command Syntax and Usage
`request` *<country code> <state or province> <locality> <organization> <organizational unit> <common name> <e-mail address> <key size> <request CA certificate>* Generates a certificate signing request (CSR), which can be further processed by a certificate authority (CA) such as VeriSign, Entrust, or any other CA. During the process of generating a CSR, you are asked whether to generate a new private key. The default answer is *Yes*. However, if you want to generate a CSR using the existing private key, you should answer *No*. If your existing certificate is reaching its expiration date and you only want to renew it, you should keep using the existing private key and answer *No*. For more information about how to generate a CSR, see "Generating and Submitting a CSR Using the CLI" on page 152.
`export` *<pass phrase>* Lets you export the current key and certificate to a file in the PEM format. When executing the **`export`** command, you are provided with the option to protect the private key with a password phrase. This adds an extra layer of security and is recommended. You can perform a cut-and-paste operation on the key section into a text editor, and save the private key to a file with the `.PEM` extension. Repeat the cut-and-paste operation on the certificate section and save it to a file with the `.PEM` extension. You may also save both the key and the certificate to the same file, again using the `.PEM` extension.
`tftpexport` *<TFTP server> <export file format* [pem|der|net|pkcs12]*>* Exports the current key and certificate to a TFTP server in the specified format. Keys and certificates can be stored in four different formats: PEM, DER, NET, or PKCS12. These formats have different capabilities regarding private key encryption and the ability to save the private key and the certificate in separate files. Only the DER format does not offer private key encryption. The DER format and the NET format lets you store the private key and the certificate in separate files. The PEM format and the PKCS12 format always combine the private key and the certificate in the same file. Most Web browsers allow importing a combined key and certificate file in the PKCS12 format.
`show` Displays detailed information related to the certificate, except the certificate name.
`info` Displays the serial number, the expiration date, and information related to the subject of the current certificate.
`validate` Validates that the private key matches the public key in the current certificate.
`keysize` Displays the keysize of the private key in the current certificate.

Table 6-9 Certificate Menu Options (/cfg/ssl/cert #)

Command Syntax and Usage
`del` Removes the current certificate and key.
`cur` Displays the certificate name, the serial number, the key size, whether the key and certificate match, and information related to the subject of the current certificate.

/cfg/ssl/cert *<certificate number>*/revoke

Certificate Revocation Menu

```
[Revocation for Cert 1 Menu]
      add          - Add serial number to revocation list
      del          - Cancel revocation for a serial number
      list         - List revoked certificates
      tftp         - TFTP revocation list from remote machine
```

The Certificate Revocation menu is used for revoking client certificates.

Table 6-10 Certificate Revocation Menu Options (/cfg/ssl/cert #/revoke)

Command Syntax and Usage
add *<serial number>* Lets you type the serial number of the client certificate you want to revoke. The certificate is then added to the current revocation list.
del *<serial number>* Lets you type the serial number of the client certificate you want to remove from the current revocation list. This will cancel the revocation of the specified certificate.
list Lists the serial numbers of client certificates that will be revoked on client authentication.
tftp *<TFTP server> <file name>* Lets you install a certificate revocation list in PEM, DER or ASCII format by using TFTP. The revocation list is used to revoke client certificates issued by a particular certificate authority (CA). The currently selected certificate index number (Cert 1, for example) should hold the CA certificate of the same CA as from which you obtained the certificate revocation list. To view information about the currently selected certificate, type the command **/cfg/ssl/cert** #**/show**. If your organization has issued its own client certificates, it may as well have created its own certificate revocation list in ASCII format. Such a list can also be downloaded and added to the certificate that was used in order to generate the client certificates.

`/cfg/ssl/server` *<SSL server number (1-256)>*

SSL Server Menu

```
[Server 1 Menu]
      name       - Set server name
      vip        - Set IP addr of SSL server
      port       - Set listen port of SSL server
      rip        - Set Real server IP
      rport      - Set Real server port
      type       - Set type (generic/http)
      proxy      - Set transparent proxy mode (on/off)
      ssl        - SSL Settings Menu
      http       - HTTP Settings Menu
      del        - Remove server
      ena        - Enable SSL server
      dis        - Disable SSL server
      cur        - Current settings
```

The SSL Server menu is used for configuring various attributes of a particular virtual SSL server. When accessing the SSL Server menu, you are requested to specify the index number of the virtual SSL server you want to work with. To view information about all configured SSL servers, type the command **`/cfg/ssl/cur`**.

Table 6-11 SSL Server Configuration Menu Options (/cfg/ssl/server #)

Command Syntax and Usage
`name` *<SSL server name>* Lets you assign a name to the virtual SSL server. The assigned name is mainly for your own reference.
`vip` *<virtual server IP address>* Lets you specify the virtual server IP address (on the Web switch), to which the virtual SSL server is mapped.
`port` *<TCP port number>* Lets you specify the TCP port number to which the virtual SSL server listens. The default is port 443 for all virtual SSL servers. The port setting on the iSD-SSL must be accompanied by a redirect filter (on the Web switch) in which the **`dport`** value corresponds to the **`port`** value (on the iSD-SSL).

Table 6-11 SSL Server Configuration Menu Options (/cfg/ssl/server #)

Command Syntax and Usage

`rip` *<real server IP address>*

Lets you specify the IP address of the real server to which the virtual SSL server should connect when initiating requests. When using the iSD-SSL in conjunction with a Web switch, the real server IP address (RIP) should be the set to 0.0.0.0 (the default setting). This setting instructs the iSD-SSL to use the destination IP address found in the received packets, when initiating requests to the virtual server on the Web switch to which the virtual SSL server has been mapped.

`rport` *<TCP port number>*

Lets you specify the TCP port to which the virtual SSL server connects. The default **`rport`** value for all virtual SSL servers that are created is 81. If you are setting up your iSD-SSL as a Web server accelerator, the iSD-SSL will use this port to send and receive decrypted HTTP information to and from the real Web servers. Note that both the virtual server (on the Web switch) and the real servers must also be configured to listen for iSD-SSL traffic on port 81.

`type generic|http`

Lets you specify the virtual SSL server type. If the server type is set to **`http`**, the content is parsed as HTTP requests and responses, and you can use the HTTP configuration options on the non-encrypted contents. If the server type is set to **`generic`**, the contents will be treated as generic data and will not be parsed.

The default value is **`generic`**.

For more information about HTTP configuration options, see page 89.

`proxy on|off`

Lets you specify whether to use Transparent proxy mode. If **`proxy`** is set to **`on`**, the client’s real IP address is used when the iSD-SSL forwards client requests to the real servers. Consequently, it is the client’s IP address that is logged on the real servers, and not the iSD-SSL’s IP address (which is “transparent” to the real servers). In order to use the Transparent proxy mode, you need to make sure all client traffic is routed back to the clients through the Web switch. The iSD-SSL real server group defined on the Web switch must use the hash algorithm for server load balancing, and FWLB (Firewall Load Balancing) must be enabled in the appropriate redirect filter on the Web switch.

If **`proxy`** is set to **`off`**, the IP address assigned to the iSD-SSL is used when client requests are forwarded to the real servers. If a real Web server is logging the client IP address, it will log the iSD-SSL’s IP address instead of the real client’s IP address. When **`proxy`** is set to **`off`**, the iSD-SSL works in non-transparent proxy mode, that is. When using non-transparent proxy mode, firewall redirect hash method must not be applied to any real ports on the Web switch.

The default proxy mode value is **`on`**.

Table 6-11 SSL Server Configuration Menu Options (/cfg/ssl/server #)

Command Syntax and Usage
`ssl` Displays the SSL Settings Server menu. To view menu options, see page 86.
`http` Displays the HTTP Settings Server menu. To view menu options, see page 89.
`del` Removes the current virtual SSL server.
`ena` Enables the current virtual SSL server.
`dis` Disables the current virtual SSL server.
`cur` Displays all settings for the current virtual SSL server.

`/cfg/ssl/server` *<SSL server number>* **`/ssl`**

SSL Server Settings Menu

```
[SSL Settings for Server 1 Menu]
     cert        - Set server certificate
     cachesize   - Set SSL cache size
     cachettl    - Set SSL cache timeout
     cacerts    - Set list of accepted signers of client certificates
     cachain     - Set list of CA chain certificates
     protocol    - Set protocol version
     verify      - Set certificate verification level
     ciphers     - Set cipher list
     cur         - Current settings
```

The SSL Settings Server menu is used for configuring SSL-specific settings for a particular virtual SSL server.

Table 6-12 SSL Settings for Server # Menu (/cfg/ssl/server #/ssl)

Command Syntax and Usage

`cert` *<certificate index number>*

Lets you specify which server certificate is used by the current virtual SSL server. To view basic information about available certificates, use the command **`/cfg/ssl/cur`**. To add a new certificate, see "Adding Certificates to the iSD-SSL" on page 156.

Note that each virtual SSL server may only use one server certificate.

`cachesize` *<number of SSL sessions>*

Lets you specify the size of the SSL cache. The default value is 8000 cached sessions. If you notice that there are many cache misses, the **`cachesize`** value can be increased for better performance.

To view the number of cache misses for a virtual SSL server, use the command **`/stats/ssl`** #**`/cachemisses`** (where # is replaced by the index number of the desired virtual SSL server).

`cachettl` *<maximum Time To Live value in minutes>*

Lets you specify the maximum Time To Live (TTL) value for items in the SSL cache, before they are discarded. The default TTL value is 5 minutes.

Table 6-12 SSL Settings for Server # Menu (/cfg/ssl/server #/ssl)

Command Syntax and Usage
`cacerts` *<certificate index number>* Lets you specify which of the available CA certificates to use for client authentication. CA certificates are added the same way as an SSL server certificate—either via a cut-and-paste operation, or via TFTP from a remote host. Both actions are performed from the Certificate menu. You can get an overview over available certificates by using the command **`/cfg/ssl/cur`**. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified CA certificates, press ENTER when asked to enter the certificate numbers, then answer **`yes`** to the question if you want to clear the list. Note: If you are using one of the available certificates to generate your own client certificates, you must specify it as a CA certificate in order to successfully authenticate clients.
`cachain` *<certificate index number>* Lets you specify the CA certificate chain of the server certificate. The chain starts with the issuing CA certificate of the server certificate, and can range up to the root CA certificate. This command explicitly constructs the server certificate chain, which is sent to the browser in addition to the server certificate. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified chain certificates, press ENTER when asked to enter the certificate numbers, then answer **`yes`** to the question if you want to clear the list.
`protocol ssl2|ssl3|ssl23|tls1` Lets you specify the protocol to use when establishing an SSL session with a client. Valid options are: ■ **`ssl2`**: Only accept SSL 2.0. ■ **`ssl3`**: Accept SSL 3.0 and TLS 1.0. ■ **`ssl23`**: Accept SSL 2.0, SSL 3.0, and TLS 1.0. ■ **`tls1`**: Only accept TLS 1.0. The default protocol value is **`ssl3`**.

Table 6-12 SSL Settings for Server # Menu (/cfg/ssl/server #/ssl)

Command Syntax and Usage
`verify none|optional|require` Lets you specify the level of client authentication to use when establishing an SSL session. Valid options are: ■ **`none`**: No client certificate is required. ■ **`optional`**: A client certificate is requested, but the client need not present one. ■ **`require`**: The client must present a valid certificate in order to establish a session. The default verify value is **`none`**.
`ciphers` *<cipher list>* Lets you change the default cipher preference list, which corresponds to `ALL`. For more information about cipher lists, see “Cipher List Formats” on page 203.
`cur` Displays all SSL-specific settings for the current virtual SSL server.

/cfg/ssl/server *<SSL server number>***/http**

SSL Server HTTP Settings Menu

```
[HTTP Settings for Server 1 Menu]
      redirect     - Set handle SSL redirect
      rewrite      - SSL Triggered Rewrite Menu
      sslheader    - Set add SSL header
      addxfor      - Set add X-Forwarded-For header
      addvia       - Set add Via header
      cur          - Current settings
```

The HTTP Settings Server menu is used for configuring HTTP-specific settings for a particular virtual SSL server.

NOTE – The HTTP Settings menu is only available if the virtual SSL server has been defined as being of the HTTP type. For more information about virtual SSL server types, see "SSL Server Menu" on page 83.

Table 6-13 HTTP Settings for Server # Menu (/cfg/ssl/server #/http)

Command Syntax and Usage

`redirect on|off|all`

When redirect is set to **`on`**, a client HTTP request that matches the domain name of the virtual server IP address to which the virtual SSL server is mapped, is rewritten from `http://` to `https://`. This function is designed to enhance a Web server’s built-in redirect functionality, as illustrated by the example below.

With redirect set to **`off`**, the client request

```
GET /top_page HTTP/1.0
Host: www.testserver.com
```

may first be redirected by the Web server to

```
HTTP/1.0 302 Moved Temporarily
Date: Thu, 01 Mar 2001 16:27:51 GMT
Server: inets/2.5.3
Location: http://www.testserver.com/login
```

With redirect set to **`on`**, the iSD-SSL rewrites `http://` to `https://` according to the following pattern:

```
HTTP/1.0 302 Moved Temporarily
Date: Thu, 01 Mar 2001 16:27:51 GMT
Server: inets/2.5.3
Location: https://www.testserver.com/login
```

When **`redirect`** is set to **`all`**, all redirects are rewritten to `https://`, regardless of the protocol and domain name in the original client request. Use this setting with caution.

The default **`redirect`** value is **`on`**.

`rewrite`

Displays the SSL Rewrite menu. To view menu options, see page 92.

Table 6-13 HTTP Settings for Server # Menu (/cfg/ssl/server #/http)

Command Syntax and Usage

`sslheader on|off`

Lets you configure the virtual SSL server to make use of an extra SSL header. Valid options for the **`sslheader`** command are:

- **`on`**: An extra SSL header is added to the client request. This extra SSL header contains information about the particular cipher suite that was used during the SSL session—information that can be logged on the Web servers. The information can also be used for Web application logical decisions concerning which cipher suites should be accepted. Such a decision would then override the default cipher suite setting for a virtual SSL server in the iSD-SSL.
  Example of an added SSL header:
  `X-SSL: decrypted=true, ciphers="TLSv1/SSLv3 RC4-MD5"`
  In case you have configured the virtual SSL server to require client certificates, information about the certificate issuer and the certificate subject is extracted from the client certificate and added to the encryption information in the SSL header.
- **`off`**: No extra SSL header is added to the client request.

The default value for the **`sslheader`** setting is **`on`**.

`addxfor on|off|anonymous|remove`

Lets you configure the virtual SSL server to make use of an extra X-Forwarded-For HTTP header. Valid options for the **`addxfor`** command are:

- **`on`**: The peer IP address of the current client connection is added to the X-Forwarded-For header. This information can be used for enhanced logging purposes.
- **`off`**: No action whatsoever is taken regarding the X-Forwarded-For header.
- **`anonymous`**: The peer IP address of the current client connection is hidden.
- **`remove`**: The X-Forwarded-For heading is removed (if present) from the current client request.

The default value for the **`addxfor`** setting is **`off`**.

Note: If there are more than one iSD-SSL in a cluster and transparent proxy is set to **`off`**, then firewall load balancing (on the Web switch) must also be set to **`off`** for the **`addxfor`** feature to work.

`addvia on|off|anonymous|remove`

Lets you configure the virtual SSL server to make use of an extra Via HTTP header. Valid options for the **`addvia`** command are:

- **`on`**: The IP address of the virtual server on the Web switch is added to the Via header.
- **`off`**: No action whatsoever is taken regarding the Via header.
- **`anonymous`**: The IP address of the virtual server is hidden.
- **`remove`**: The Via header is removed (if present) from the current client request.

The default value for the **`addvia`** setting is **`on`**.

`cur`

Displays the current values for all HTTP settings.

/cfg/ssl/server <#>/http/rewrite

SSL Server HTTP Rewrite Menu

```
[Rewrite Menu for Server 1 Menu]
      rewrite     - Set SSL triggered rewrite
      ciphers     - Set accepted ciphers
      response    - Set source of response
      URI         - Set URI with the weak cipher alert
      cur         - Current settings
```

The SSL Server Rewrite menu is used for enabling and configuring the HTTP rewrite functionality for a particular virtual SSL server.

Table 6-14 SSL Rewrite Menu Options (/cfg/ssl/server #/http/rewrite)

Command Syntax and Usage
`rewrite on|off` Enables the rewrite functionality for the specified virtual SSL server. When you enable the rewrite functionality, a customized error message can be sent back to the client’s Web browser in case the browser is unable to perform the required cipher strength. If the rewrite functionality is not enabled in such a scenario, the client request is simply rejected during the SSL handshake. For more information about how to configure an SSL server to use the rewrite functionality, see page 181.
`ciphers` *<cipher list>* Lets you change the cipher list used when the SSL rewrite function is enabled. The default cipher list used when the rewrite function is **not** enabled corresponds to `ALL`. When the rewrite function is enabled, the default rewrite cipher list is `HIGH`. If you change the default rewrite cipher list from `HIGH` when having the rewrite function enabled, remember that the rewrite cipher strength must always be higher than the cipher strength specified by using the command **`/cfg/ssl/server`** #**`/ssl/ciphers`** (where the default cipher list is `ALL`). For more information about supported ciphers and cipher list formats, see page 201.
`response iSD|WebServer` Lets you specify whether the iSD-SSL or a Web server should handle the response message sent back to the client.
`URI` Lets you specify the URI pointing to a resource that provides the response message.
`cur` Displays the current settings.

/cfg/sys

System Configuration Menu

```
[System Menu]
      date        - Set system date
      time        - Set system time
      tzone       - Set Timezone
      dns         - DNS Servers Menu
      host        - iSD Hosts Menu
      mip         - Set management IP (MIP) address
      netmask     - Set network mask
      telnet      - Set telnet CLI access
      ssh         - Set SSH CLI access
      gensshkeys  - Generate new SSH host keys
      accesslist  - Access List Menu
      gateway     - Set gateway address
      syslog      - Syslog Servers Menu
      ntp         - Configure NTP settings
      user        - User access control menu (passwords)
      cur         - Current settings
```

The System Configuration menu is used for configuring system-wide parameters on a per cluster basis.

Table 6-15 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
`date` <*date (YYYY-MM-DD)*> Sets the system date according to the specified format.
`time` <*time (HH:MM:SS)*> Sets the system time using a 24-hour clock format.
`tzone` Lets you specify a timezone by selecting a continent or ocean, a country, and a region (if applicable).
`dns` Displays the DNS Servers menu. To view menu options, see page 95.
`host` Displays the iSD Host menu. To view menu options, see page 96.

Table 6-15 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
`mip` *<Management IP address>* Lets you change the Management IP (MIP) address. The MIP address identifies the cluster, and each MIP address must be unique on the network. For more information about clusters and MIP addresses, see "About iSD-SSL Clusters" on page 33.
`netmask` *<IP subnet mask>* Lets you change the network mask for all iSD-SSLs in the cluster.
`telnet on|off` Lets you specify whether or not Telnet access should be allowed. When set to **`on`** and not having added machine(s) via the **`/cfg/sys/accesslist/add`** command, all Telnet connections are allowed. When set to **`on`** and having added machine(s) via the **`/cfg/sys/accesslist/add`** command, only the specified machine(s) are allowed Telnet access. When set to **`off`**, all Telnet connections are rejected, including connections from machine(s) added via the **`/cfg/sys/accesslist/add`** command. To view **`accesslist`** menu options, see page 97. The default Telnet setting is **`off`**.
`ssh on|off` Lets you specify whether or not SSH access should be allowed. When set to **`on`** and not having added machine(s) via the **`/cfg/sys/accesslist/add`** command, all SSH connections are allowed. When set to **`on`** and having added machine(s) via the **`/cfg/sys/accesslist/add`** command, only the specified machine(s) are allowed SSH access. When set to **`off`**, all SSH connections are rejected, including connections from machine(s) added via the **`/cfg/sys/accesslist/add`** command. To view **`accesslist`** menu options, see page 97. The default SSH setting is **`off`**.
`gensshkeys` Lets you generate new SSH host keys.
`accesslist` Displays the Access List menu. To view menu options, see page 97.
`gateway` *<default gateway IP address>* Lets you change the default gateway IP address for all iSD-SSL in the cluster.

Table 6-15 System Configuration Menu Options (/cfg/sys)

Command Syntax and Usage
`syslog` Displays the Syslog Servers menu. To view menu options, see page 98.
`ntp` Displays the NTP Server menu. To view menu options, see page 99.
`user` Displays the User Access Control menu. To view the options, see page 101.
`cur` Displays the current settings. For an example screen output, see page 102.

/cfg/sys/dns

DNS Servers Menu

```
[DNS Servers Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
```

The DNS Servers menu is used for adding and deleting IP addresses of DNS servers accessible to the iSD-SSL.

Table 6-16 DNS Server Configuration Menu Options (/cfg/sys/dns)

Command Syntax and Usage
`list` Displays all DNS servers by their index number and IP address.
`del` *<index number>* Deletes a DNS server by index number. Use the **`list`** command to display the index numbers and IP addresses of added DNS servers.
`add` *<IP address of DNS server>* Adds a new DNS server.

`/cfg/sys/host` *<iSD host number (1-256)>*

iSD Host Configuration Menu

```
[iSD Host 1 Menu]
      type         - Set type of the iSD
      ip           - Set IP address
      del          - Deletes the iSD from the system
      cur          - Current settings
```

The iSD Host menu is used for configuring basic TCP/IP properties for a particular iSD host in a cluster, as well as setting the iSD host to either master or slave. To view the host number for each iSD-SSL in the cluster, use the command **`/cfg/sys/cur`**.

Table 6-17 iSD Host Menu Options (/cfg/sys/host #)

Command Syntax and Usage

`type master|slave`

Lets you set the currently selected iSD-SSL host as master or slave. When installing an iSD-SSL in a new cluster (by selecting **`new`** in the Setup menu), it is automatically configured as master. When adding up to three additional iSD-SSLs to the same cluster (by selecting **`join`** in the Setup menu), you are provided with the option to configure them as either master or slave. The default setting, however, for up to three additional iSD-SSL in one given cluster is master. This means that in a cluster containing four iSD-SSLs, all four are configured as masters provided you accepted the default settings during the initial setup.

When adding one or more iSD-SSL(s) to a cluster that already contains four master iSD-SSLs, the added iSD-SSL(s) is automatically configured as slave (without the option to change this during the initial setup).

Normally, you will only need to change the **`type`** configuration when you have removed one or more master iSD-SSLs in a cluster, in which there are also iSD-SSLs configured as slaves. In this case, you may want to promote one of the slaves to become a master. Depending on the total number of iSD-SSLs in a cluster and the desired level of redundancy, it is recommended that 2-4 iSD-SSLs are configured as masters.

To view the status and current master/slave configuration of the iSD-SSLs in a cluster, use the command **`/info/isdlist`**. To view the host number of each iSD-SSL in a cluster, use the command **`/cfg/sys/cur`**.

`ip` *<iSD host IP address>*

Lets you change the IP address of the currently selected iSD-SSL host. Changing the IP address of a specific iSD-SSL host does not affect the Management IP address (which defines the cluster itself, and not an individual iSD-SSL host). To change the Management IP address, use the command **`/cfg/sys/mip`**.

Table 6-17 iSD Host Menu Options (/cfg/sys/host #)

Command Syntax and Usage
`del` Lets you remove the currently selected iSD-SSL host from the cluster, and wipes the configuration database. Any other iSD-SSLs in the cluster are unaffected. To ensure that you remove the intended iSD-SSL, view the current settings by using the **`cur`** command first. To view information about all iSD-SSLs in a cluster and their respective configuration, use the command **`/info/isdlist`**. To view the host number of each iSD-SSL in a cluster, use the command **`/cfg/sys/cur`**.
`cur` Displays the current settings regarding type, IP address, network mask, and gateway address for the selected iSD-SSL host.

/cfg/sys/accesslist

Access List Menu

```
[Access List Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
```

The Access List menu is used for controlling Telnet and SSH access to the iSD-SSL. The access control rules can be applied to individual machines, or to all machines on a specific network.

Table 6-18 Access List Menu Options (/cfg/sys/accesslist)

Command Syntax and Usage
`list` Displays all entries in the list by index number, network address, and network mask.
`del` *<index number>* Lets you delete an entry in the list by specifying the index number.
`add` *<IP address> <IP subnet mask>* Lets you specify a single machine, or a range of machines on a specific network, that are allowed to access the iSD-SSL via a Telnet or SSH connection (provided Telnet or SSH connections, or both, are enabled). To enable Telnet or SSH connections, see the **`telnet`** and **`ssh`** commands under “System Configuration Menu” on page 93.

/cfg/sys/syslog

Syslog Servers Menu

```
[Syslog Servers Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
```

The Syslog Servers menu is used to configure Syslog servers. The iSD-SSL software can send log messages to the specified Syslog hosts.

Table 6-19 Syslog Server Configuration Menu Options (/cfg/sys/syslog)

Command Syntax and Usage
`list` Displays all configured syslog servers by their index number, IP address, and facility number.
`del` *<index number>* Lets you delete a syslog server from the configuration by specifying the server’s index number.
`add` *<syslog server IP address> <local facility number>* Lets you add a new syslog server. When adding a syslog server you will be prompted for both the IP address and the local facility number. The facility number can be used to uniquely identify syslog entries. For more information, see the man page for `syslog.conf` under UNIX.

/cfg/sys/ntp

NTP Settings Menu

```
[NTP Settings Menu]
      servers     - Enter NTP servers menu
      cur         - Current settings
```

The NTP Settings menu is used for configuring NTP servers, and viewing the current NTP settings.

Table 6-20 NTP Settings Menu Options (/cfg/sys/ntp)

Command Syntax and Usage
`servers` Displays the NTP Servers menu. To view menu options, see page 100.
`cur` Displays the current NTP settings.

/cfg/sys/ntp/servers

NTP Servers Menu

```
[NTP Servers Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
```

This menu enables you to list the configured NTP servers, delete NTP servers, or add a new NTP server.

Table 6-21 NTP Servers Menu Options (/cfg/sys/ntp/servers)

Command Syntax and Usage
`list` Lists all configured NTP servers by their index number and IP address.
`del` *<index number>* Lets you delete an NTP server from the configuration by specifying the server's index number. Use the **`list`** command to display the index numbers and IP addresses of added NTP servers.
`add` *<IP address>* Lets you add a Network Time Protocol (NTP) server. The NTP server you add is used by the NTP client on the iSD-SSL to synchronize its clock. NTP should have access to a number of servers (at least three) in order to compensate for any discrepancies in the servers.

/cfg/sys/user

User Password Menu

```
[User Menu]
      admpw      - Set administrator password (admin)
      operpw     - Set operator password (oper)
      rootpw     - Set root password (root)
```

The User Password menu is used to change the passwords for the **`admin`** user account, the **`oper`** user account, and the **`root`** user account. Only the Administrator can change these passwords.

The password for the **`boot`** user cannot be changed. The reason for this is that if you would lose both the **`admin`** password and the **`boot`** password, there would be no way to restore the default passwords by performing a reinstallation of the software (only the **`boot`** user can do this). For more information about different user accounts and related access levels, see "Accessing the iSD-SSL" on page 55.

Table 6-22 User Configuration Menu Options (/cfg/sys/user)

Command Syntax and Usage
`admpw` *<administrator password> <new password> <confirm new password>* Lets the administrator change the Administrator user password.
`operpw` *<administrator password> <new password> <confirm new password>* Lets the administrator change the Operator user password.
`rootpw` *<administrator password> <new password> <confirm new password>* Lets the administrator change the Root user password.

/cfg/sys/cur

Current System Settings Command

```
System:
  System date = 2001-04-15
  System time = 18:00:00
  Timezone = Europe/Stockholm
  Management IP (MIP) address = 192.168.51.100
  Network mask = 255.255.255.0
  Telnet CLI access = off
  SSH CLI access = on
  Gateway address = 192.168.51.1

    DNS Servers:
       1: 192.168.128.1

    iSD Host 1:
      Type of the iSD = master
      IP address = 192.168.51.20

    iSD Host 2:
      Type of the iSD = master
      IP address = 192.168.51.21

    Access list:
      No items configured

    Syslog Servers:
       1:+192.168.51.1, 1

    NTP Servers
       1: 192.168.128.1
```

/cfg/snmp

SNMP Menu

```
[SNMP Menu]
      snmpv2-mib - SNMPv2-MIB Menu
      community  - SNMP Community Menu
      target     - Notification Targets Menu
      cur        - Current settings
```

The SNMP menu is used for configuring the network monitoring of your iSD-SSLs.

Table 6-23 SNMP Menu Options (/cfg/snmp)

Command Syntax and Usage
`snmpv2-mib` Displays the SNMPv2-MIB menu. To view menu options, see page 104.
`community` Displays the SNMP Community menu. To view menu options, see page 105.
`target` Displays the Notification Targets menu. To view menu options, see page 106.
`cur` Displays the current SNMP settings.

/cfg/snmp/snmpv2-mib

SNMPv2-MIB Menu

```
[SNMPv2-MIB Menu]
      sysDescr    - Set sysDescr
      sysContact  - Set sysContact
      sysName     - Set sysName
      sysLocatio  - Set sysLocation
      snmpEnable  - Set snmpEnableAuthenTraps
      cur         - Current settings
```

The SNMPv2-MIB menu is used for configuring parameters in the standard SNMPv2 Management Information Base (MIB) for the system.

Table 6-24 SNMPv2-MIB Menu Options (/cfg/snmp/snmpv2-mib)

Command Syntax and Usage
`sysDescr` Lets you add a textual description of the managed iSD-SSL cluster.
`sysContact` Lets you specify a contact person for the managed iSD-SSL cluster, together with information on how to contact this person.
`sysName` Lets you add an adminstratively-assigned name for the managed iSD-SSL cluster.
`sysLocatio` Lets you add a description of the physical location of the managed iSD-SSL cluster.
`snmpEnable disabled|enabled` Lets you specify whether the managed iSD-SSL is permitted to generate authentication failure traps. The default snmpEnable value is **`disabled`**.
`cur` Displays the current SNMPv2-MIB settings.

/cfg/snmp/community

SNMP Community Menu

```
[SNMP Community Menu]
      read       - Set read community string
      write      - Set write community string
      trap       - Set trap community string
      cur        - Current settings
```

The SNMP Community menu is used for configuring the community aspects of the SNMP monitoring.

Table 6-25 SNMP Community Menu Options (/cfg/snmp/community)

Command Syntax and Usage
`read` Lets you specify the monitor community name that grants read access to the Management Information Base (MIB). If no monitor community name is specified, read access is not granted. The default monitor community name is **`public`**.
`write` Lets you specify the control community name that grants read and write access to the Management Information Base (MIB). If no control community name is specified, neither write nor read access is granted.
`trap` Lets you specify the trap community name that accompanies trap messages sent to the SNMP manager. If no trap community name is specified, the sending of trap messages is disabled. The default trap community name is **`trap`**.
`cur` Displays the current SNMP community settings.

/cfg/snmp/target *<notification target number>*

SNMP Notification Target Menu

```
[Notification Target 1 Menu]
        ip     - Set target IP
        port   - Set target port
        vsn    - Set SNMP version
        del    - Remove target
        cur    - Current settings
```

The SNMP Notification Targets menu is used for configuring the notification target aspects of SNMP monitoring.

Table 6-26 SNMP Notification Targets Menu Options (/cfg/snmp/target)

Command Syntax and Usage
`ip` *<SNMP manager IP address>* Lets you specify the IP address of the SNMP manager, to which trap messages are sent.
`port` *<TCP port [162]>* Lets you change the TCP port used by the SNMP manager. The default value is port number 162.
`vsn v1|v2c` Lets you specify the SNMP version used by the SNMP manager. The default SNMP version is **`v2c`**.
`del` Removes the current SNMP manager from the configuration.
`cur` Displays the current SNMP notification target settings.

/boot
Boot Menu

```
[Boot Menu]
      cur          - Display current software status
      activate     - Select software version to run
      tftp         - Download a new software image via TFTP
      del          - Remove downloaded (unpacked) releases
      halt         - Halt the iSD
      reboot       - Reboot the iSD
      teardown     - Tear down all configuration on this iSD
```

The Boot menu is used for managing software versions, and to shutdown, reboot, or reset the configuration of a particular iSD-SSL.

Table 6-27 Boot Menu Options (/boot)

Command Syntax and Usage
`cur` Displays the software status of the particular iSD-SSL to which you have connected via Telnet, SSH, or a console connection. For more information about software status values, see "Activating the Software Upgrade Package" on page 43.
`activate` *<software version>* Lets you activate a downloaded and unpacked software upgrade package. If serious problems occur while running the new software version, you may switch back to the previous version by activating the software version indicated as `old`. Note that you will be logged out upon confirming the **`activate`** command.
`tftp` *<host name or IP address> <file name>* Lets you download a software upgrade package from a TFTP server, in order to perform a minor or major upgrade. You need to provide the host name or IP address of the TFTP server, as well as the file name of the software upgrade package.
`del` Lets you remove a software image that has been downloaded by using the **`tftp`** command, in case you do not want to activate the software image.

Table 6-27 Boot Menu Options (/boot)

Command Syntax and Usage
`halt` Stops the particular iSD-SSL to which you have connected via Telnet, SSH, or a console connection. If you are using Telnet or SSH, only use this command when you have connected to the iSD-SSL's individually assigned IP address. Do not use the **`halt`** command when you are connected via Telnet or SSH to the Management IP address (MIP).
`reboot` Reboots the particular iSD-SSL to which you have connected via Telnet, SSH or a console connection. If you are using Telnet or SSH, only use this command when you have connected to the iSD-SSL's individually assigned IP address. Do not use the **`reboot`** command when you have connected via Telnet or SSH to the Management IP address (MIP).
`teardown` Wipes the configuration of the particular iSD-SSL to which you have connected via Telnet, SSH, or a console connection, and resets the iSD-SSL to its factory default configuration. The software itself will remain intact. After having performed a **`teardown`**, you must log in as Administrator to access the Setup menu. If the iSD-SSL is member of a cluster, you should remove it by using the command **`del`** from the iSD Host menu. For more information about the iSD Host menu options, see page page 96.

/boot/cur

Current Software Status Command

```
2.0.1       permanent
2.0         old
```

This command displays information about the software version that is currently operational (`permanent`), and the software version that preceded the currently operational version (`old`).

/maint
Maintenance Menu

```
[Maintenance Menu]
      tsdmp    - Tech support dump to tftp server
```

The **`tsdmp`** command in the Maintenance menu is used to send information collected from one or all iSD-SSLs to a TFTP server for technical support purposes.

Table 6-28 Maintenance Menu Options (/maint)

Command Syntax and Usage
`tsdmp` *<TFTP server> <file name>* Collects system log file information from the iSD-SSL you are connected to or optionally, all iSD-SSLs in the cluster, and sends the information to a file in the gzip compressed tar format on a TFTP server. The information can then be used for technical support purposes.

CHAPTER 7

Public Key Infrastructure and SSL

This chapter describes some of the fundamentals behind the iSD-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 7-1 shows the time required to break the encryption of a message based on the key length.

Table 7-1 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.

When sending encrypted messages using public key encryption, digital signatures are used to ensure that the message originated with the person sending it, and that the message was not tampered with after the signature was applied.

Digital signatures are also used in digital certificates, where the certificate owner’s public key is digitally signed with the private key of a certificate authority. A server certificate, along with other data, is sent to the client during the SSL handshake. The client then uses this information, along with the public key of the certificate authority, in order to authenticate the server.

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:

- Register 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.

Certificate Authorities

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.

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.

Secure Sockets Layer (SSL)

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.

Example of an SSL Transaction

The steps involved in an SSL transaction can be done with an iSD-SSL (or an SSL-enabled server). The steps are summarized as follows:

1. The client sends the following information to the iSD-SSL: SSL version number, cipher settings, randomly generated data, and other information that the server needs to communicate with the SSL client.
2. The iSD-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 iSD-SSL to authenticate the iSD-SSL. If the iSD-SSL is not authenticated, the user is warned of the problem and informed that an encrypted and authenticated connection cannot be established. If the iSD-SSL is successfully authenticated, the client goes on to Step 4.
4. The client (with the cooperation of the iSD-SSL, depending on the cipher being used) creates the premaster secret for the session, encrypts it with the iSD-SSL’s public key (obtained from the iSD-SSL’s certificate, sent in Step 2), and sends the encrypted premaster secret to the iSD-SSL.
5. If the iSD-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 the iSD-SSL. In this case the client sends both the signed data and the client's own certificate to the iSD-SSL along with the encrypted premaster secret.

6. If the iSD-SSL has requested client authentication, the iSD-SSL attempts to authenticate the client. If the client is not authenticated, the session is terminated. If the client can be successfully authenticated, the iSD-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 iSD-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 iSD-SSL 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 iSD-SSL informs the client that future messages will be encrypted with the session key. It then sends the client a separate (encrypted) message indicating that the iSD-SSL portion of the handshake is finished.

10. The SSL handshake is now complete, and the SSL session begins. The client and the iSD-SSL use the session keys to encrypt and decrypt the data they send to each other and to verify data integrity.

Figure 7-1 depicts an outline of the steps above.

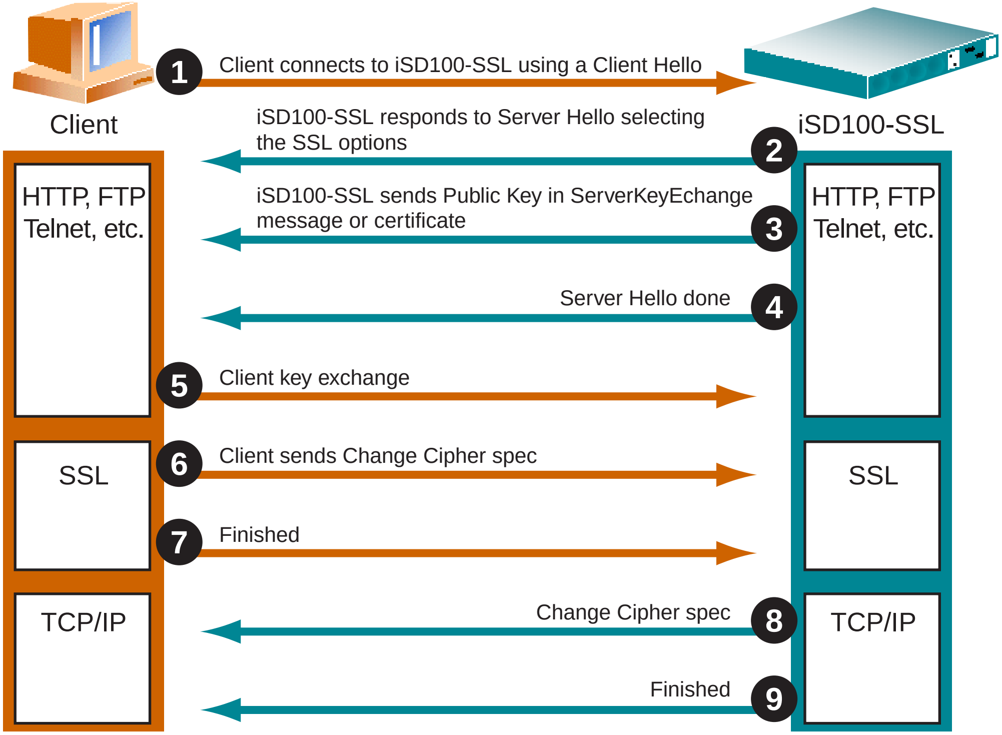

Client
iSD100-SSL
1 Client connects to iSD100-SSL using a Client Hello
2 iSD100-SSL responds to Server Hello selecting the SSL options
3 iSD100-SSL sends Public Key in ServerKeyEchange message or certificate
4 Server Hello done
5 Client key exchange
6 Client sends Change Cipher spec
7 Finished
8 Change Cipher spec
9 Finished
HTTP, FTP Telnet, etc.
SSL
TCP/IP
HTTP, FTP Telnet, etc.
SSL
TCP/IP

Figure 7-1 SSL Handshake Procedure

CHAPTER 8

iSD-SSL Sample Applications

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

- Web Server Accelerator, using two or more load-balanced iSD-SSLs for SSL offload, on page 118.
- Content-Intelligent Switching for Secure Sessions, using single or multiple iSD-SSLs for SSL offload with cookie processing, on page 130.
- Redundant Active-Standby Configuration, using multiple iSD-SSLs for high-availability scenarios, on page 131.
- Mail Server Accelerator, using two or more load-balanced iSD-SSLs for SSL offload, on page 137.

The sample configurations discussed are merely recommendations and are not required. The first three examples are based on the configuration described in "Web Server Accelerator" on page 118. Therefore, it is recommended that you read this chapter in sequence, and modify the base configuration as noted in each subsequent example.

In the Mail Server Accelerator example it is assumed that Web server accelerating has not been set up. However, it is possible to use mail server accelerating in parallel with Web server accelerating using the same group of iSD-SSLs.

Web Server Accelerator

Figure 8-1 illustrates the most common network configuration for the iSD-SSL. This configuration example consists of two iSD-SSLs, an Alteon Web switch and two servers.

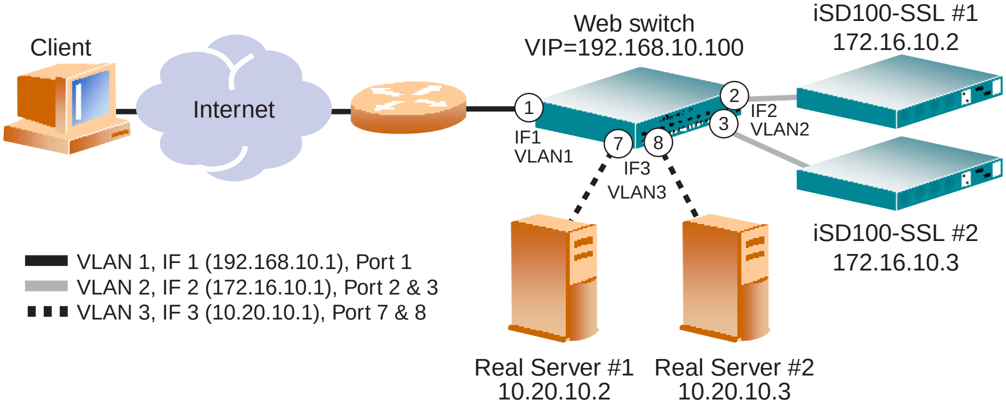


Figure 8-1 Sample Web Server Accelerator Network Using Multiple iSD-SSLs

Initial Setup

First do the initial setup of the two iSD-SSLs as described in Chapter 3, "Initial Setup'' using the IP addresses shown in Figure 8-1. Then connect to one of the iSD-SSLs to add a certificate.

On the iSD-SSL, Add a Server Certificate

This step presumes that you have a server certificate, signed by a certificate authority (CA), and a private key. The process for obtaining the required certificate files is covered in "Generating and Submitting a CSR Using the CLI" on page 152."

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

```
# /cfg/ssl/cert
Enter certificate number: (1-) 1
Creating Certificate 1
>> Certificate 1# cert
Paste the certificate, press Enter to create a new line, and then
type "..."(without the quotation marks) to terminate.
```

The example above assumes that the certificate signing request (CSR) was generated from certificate number 1, which implies that the private key that corresponds to the public key in the certificate is already in place.

When prompted for the certificate, follow the instructions. Use Notepad or any other text editor to display the certificate. Then copy and paste the text of the certificate into the terminal window. For more detailed information about how to add certificates and keys to the iSD-SSL, see "Adding Certificates to the iSD-SSL" on page 156.

Important—*Once you have pasted the entire contents of the certificate file, press ENTER to create a new empty line and then type three periods (`...`). Press ENTER again to complete the installation of the certificate.*

NOTE – Under Microsoft Windows, HyperTerminal may be slow to complete the copy-and-paste operation.

On the iSD-SSL, Configure the Parameters

Connect to the MIP of the iSD-SSLs to configure them. The configuration changes will be distributed automatically to all members in the cluster.

1. **Create a virtual SSL server.**

```
# /cfg/ssl/server
Enter virtual server number: (1-) 1
Creating new server 1
>> Server 1#
```

This creates a new virtual SSL server on the iSD-SSL. Each virtual SSL server listens to a specific TCP port and is connected to a Virtual Server IP address on the Web switch.

2. **Define a name for virtual SSL server 1.**

```
>> Server 1# name
Current value: ""
Enter new SSL server name: HTTPS
```

This step lets you specify a name, by which you can identify SSL server 1. To view the numbers and related names of all configured SSL servers, use the command **`/cfg/ssl/cur`**. The name you specify is mainly intended for your own reference, and is not critical for the configuration itself. As the example above suggests, the name can indicate the service for which the SSL server was created.

3. **Set listen TCP port for SSL server 1.**

```
>> Server 1# port
>> Current value: 443 (https)
>> Enter listen port number: 443
```

Each time you create a new SSL server, the listen port is automatically set to 443. Since you are setting up the iSD-SSL for HTTPS offload purposes in this example, it is not really necessary to configure the SSL server to listen port to 443. However, for using the iSD-SSL for any protocol other than HTTPS, a new virtual SSL server must be configured to listen to the TCP port of the intended service.

4. **Connect the SSL server to the desired Virtual Server IP address on the Web switch.**

```
>> Server 1# vip
Current value: <not set>
Enter IP address: 192.168.10.100
```

This step connects SSL Server 1 to the IP address of the desired virtual server on the Web switch.

5. **Set the Real Server IP address to which SSL Server 1 should connect when initiating requests.**

```
>> Server 1# rip
Current value: 0.0.0.0
Enter IP address to connect to: 0.0.0.0
```

Preserve the current value of the Real Server IP address, which should be 0.0.0.0. At first glance this configuration may perhaps seem odd. However, by specifying 0.0.0.0 as the Real Server IP address, the SSL server is instructed to use the destination IP address (in the received packets) when initiating requests sent to the virtual server. Since the destination IP address in the received packets corresponds to the IP address of the virtual server, the requests will always reach the correct Virtual Server IP address.

6. **Set the server port to which SSL server 1 should connect when initiating requests.**

```
>> Server 1# rport
Current value: 0 [81]
Enter port to connect to: 81
```

This step sets the TCP port, to which SSL Server 1 connects when initiating requests.

NOTE – The real Web servers must also be set to listen for iSD-SSL traffic on port 81.

---

7. **Specify the certificate to be used by SSL Server 1.**

```
>> Server 1# ssl
>> SSL Settings for server 1# cert
Current value: <not set>
Enter certificate number: (1-) 1
```

You are prompted to type the index number of an existing certificate. To view all certificates currently added to the iSD-SSL by index number and name, use the command **`/cfg/ssl/cur`**. For more information about how to add a certificate, see "Adding Certificates to the iSD-SSL" on page 156.

NOTE – If the certificate you specify is a chained certificate, you need to first add the CA certificates up to and including the root CA certificate, and then specify the CA certificate chain of the server certificate. For more information on how to construct the server certificate chain, see the **`cachain`** command under "SSL Server Settings Menu" on page 86.

---

8. **Apply the changes.**

```
>> SSL Settings for Server 1# apply
Changes applied successfully.
```

On the Web Switch, 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 iSD-SSL units, and VLAN 3 for the real servers. Since VLAN 1 is the default, only VLAN 2 and VLAN 3 require additional configuration. Note that all the sample configuration changes that follow are performed on the Web switch.

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

```
# /cfg/vlan 2
>> VLAN 2# add 2
Port 2 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# add 3
Port 3 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# ena
```

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

```
# /cfg/vlan 3
>> VLAN 3# add 7
Port 7 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 3# add 8
Port 8 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 3# ena
```

3. **Disable Spanning Tree Protocol (STP) for the iSD-SSL ports 2 and 3 and real server ports 7 and 8.**

   STP will not function across multiple VLANs.

```
# /cfg/stp/port 2
>> Spanning Tree Port 2# off
>> Spanning Tree Port 2# ../port 3
>> Spanning Tree Port 3# off
>> Spanning Tree Port 3# ../port 7
>> Spanning Tree Port 7# off
>> Spanning Tree Port 7# ../port 8
>> Spanning Tree Port 8# off
```

On the Web Switch, Configure One IP Interface for Each VLAN

NOTE – If you prefer, you can reverse the order of the first two commands (**`addr`** and **`mask`**) in the example below. By entering the mask first, the Web switch will automatically calculate the correct broadcast address for you. The calculated broadcast address is displayed immediately after you provide the IP address of the interface, and will be applied together with the other settings when you execute the **`apply`** command.

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

```
# /cfg/ip/if 1
>> IP Interface 1# addr 192.168.10.1
>> IP Interface 1# mask 255.255.255.0
>> IP Interface 1# broad 192.168.10.255
>> IP Interface 1# vlan 1
>> IP Interface 1# ena
```

2. **Configure an IP interface for iSD-SSL traffic with VLAN 2.**

```
# /cfg/ip/if 2
>> IP Interface 2# addr 172.16.10.1
>> IP Interface 2# mask 255.255.0.0
>> IP Interface 2# broad 172.16.255.255
>> IP Interface 2# vlan 2
>> IP Interface 2# ena
```

3. **Configure an IP interface for the real server traffic with VLAN 3.**

```
# /cfg/ip/if 3
>> IP Interface 3# addr 10.20.10.1
>> IP Interface 3# mask 255.255.255.0
>> IP Interface 3# broad 10.20.10.255
>> IP Interface 3# vlan 3
>> IP Interface 3# ena
```

4. **Enable global IP forwarding between the configured IP interfaces.**

```
# /cfg/ip/frwd
>> IP Forwarding# on
Current status: OFF
New status:     ON
```

5. **Apply the changes.**

```
# apply
```

NOTE – Make sure the iSD-SSLs are configured to use the IP address of IP interface 2 on VLAN 2 as their default gateway. For more information about gateway configuration, see the **`gateway`** command under "iSD Host Configuration Menu" on page 96. Likewise, the Web servers must be configured to use the IP address of IP interface 3 on VLAN 3 as their default gateway.

On the Web Switch, Configure Web Server Load Balancing Parameters

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

```
# /cfg/slb/real 1
>> Real Server 1# rip 10.20.10.2
>> Real Server 1# ena
>> Real Server 1# ../real 2
>> Real Server 2# rip 10.20.10.3
>> Real Server 2# ena
```

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

```
# /cfg/slb/group 1
>> Real server group 1# add 1
>> Real server group 1# add 2
```

3. **Set and enable the IP address for Virtual Server 1, enable service on port 81, and connect real server group 1 to the virtual server.**

```
# /cfg/slb/virt 1
>> Virtual Server 1# vip 192.168.10.100
>> Virtual Server 1# ena
>> Virtual Server 1# service 81
>> Virtual Server 1 81 Service# group 1
>> Virtual Server 1 81 Service# ../service http
>> Virtual Server 1 http Service# group 1
>> Virtual Server 1 http Service# apply
```

Enable service on port 81 for unencrypted communication between the iSD-SSLs and the real Web servers. Recall that the real Web servers must also be configured to listen for iSD-SSL traffic on port 81. The step above also connects the real Web servers in server group 1 to the enabled virtual server. The HTTP service on port 80 for non-SSL Web traffic from clients to the real Web servers in real server group 1 is also enabled. Thus, the load balancing scheme for real server group 1 includes traffic on port 80 and 81.

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

```
# /cfg/slb/port 1/client ena
```

5. **Enable client processing on ports 2 and 3 leading to iSD-SSLs.**

```
# /cfg/slb/port 2
>> SLB Port 2# client ena
>> SLB Port 2# ../port 3
>> SLB Port 3# client ena
```

6. **Enable server processing on ports 7 and 8 leading to real servers.**

```
# /cfg/slb/port 7
>> SLB Port 7# server ena
>> SLB Port 7# ../port 8
>> SLB Port 8# server ena
```

7. **Turn on Layer 4 processing.**

```
# /cfg/slb/on
```

On the Web Switch, Configure iSD-SSL Load Balancing Parameters

Set and enable the IP addresses of the iSD-SSLs, and create a group in the switch for load balancing.

1. **For each iSD-SSL create a Real Server IP address on the Web switch**

```
# /cfg/slb/real 3
>> Real server 3# rip 172.16.10.2
>> Real server 3# ena
>> Real server 3# ../real 4
>> Real server 4# rip 172.16.10.3
>> Real server 4# ena
```

2. **Create a Real Server Group and add the Real Servers (the iSD-SSLs in this case)**

```
# /cfg/slb/group 2
>> Real server group 2# add 3
>> Real server group 2# add 4
```

3. **Set the load balancing metric and health check type for real server group 2.**

```
# /cfg/slb/group 2
>> Real server group 2# metric hash
>> Real server group 2# health tcp
```

4. **Apply the changes.**

```
# apply
```

On the Web Switch, Configure Filters

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

```
# /cfg/slb/filt 100
>> Filter 100# proto tcp
>> Filter 100# dport https
>> Filter 100# action redir
>> Filter 100# group 2
>> Filter 100# rport https
>> Filter 100# adv/fwlb e
>> Filter 100 Advanced# ../ena
```

When this filter is added to the switch port leading to the Internet, incoming HTTPS traffic is redirected to the iSD-SSLs in real server group 2. Firewall redirect hash method is also enabled, using redirection based on hashing on both the source IP and the destination IP of the packets.

The HTTPS traffic filter should be given a high number (a lower priority), such as 100, so as not to interfere with other filters.

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

```
# /cfg/slb/filt 3
>> Filter 3# proto tcp
>> Filter 3# dport 81
>> Filter 3# action deny
>> Filter 3# ena
```

This filter, when placed on the client port leading to the Internet, blocks all incoming traffic destined for port 81. This is required to ensure that traffic from clients outside your trusted network does not gain access to non-encrypted content on your real Web servers (content that would have been encrypted, had you not used the iSD-SSL for SSL offload purposes).

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

```
# /cfg/slb/filt 224
>> Filter 224# sip any
>> Filter 224# dip any
>> Filter 224# proto any
>> Filter 224# action allow
>> Filter 224# ena
```

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

```
# /cfg/slb/port 1
>> SLB Port 1# add 100
>> SLB Port 1# add 3
>> SLB Port 1# add 224
>> SLB Port 1# filt ena
```

This step adds the HTTPS redirect filter, the port 81 deny filter, and the default allow filter to the client port leading to the Internet.

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

```
# /cfg/slb/filt 150
>> Filter 150# action allow
>> Filter 150# sip 192.168.10.100
>> Filter 150# smask 255.255.255.255
>> Filter 150# dip 10.20.10.1
>> Filter 150# dmask 255.255.255.255
>> Filter 150# proto tcp
>> Filter 150# sport 81
>> Filter 150# dport any
>> Filter 150# ena
```

The health check filter should be given a smaller number (higher priority) than the redirection filter set in Step 6. on page 128.

The source IP (SIP) must be the virtual server IP (VIP) address of the switch. The destination IP (DIP) must be the IP address of the switch interface number 3, which is connected to server ports 7 & 8 leading to the real Web servers.

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

```
# /cfg/slb/filt 200
>> Filter 200# proto tcp
>> Filter 200# sport 81
>> Filter 200# action redir
>> Filter 200# group 2
>> Filter 200# adv/fwlb e
>> Filter 200 Advanced# ../ena
```

This filter, when added to the switch ports leading to the real Web servers, will redirect TCP traffic from port 81 back to the iSD-SSLs in group 2.

Firewall redirect hash method is also enabled, and the redirection is based on hashing using both the source IP and the destination IP of the packets. The return packets hash to the same IP address of the iSD-SSL in real server group 2, as from which the packets originated.

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

```
# /cfg/slb/port 7
>> SLB Port 7# add 150
>> SLB Port 7# add 200
>> SLB Port 7# add 224
>> SLB Port 7# filt ena
>> SLB Port 7# ../port 8
>> SLB Port 8# add 150
>> SLB Port 8# add 200
>> SLB Port 8# add 224
>> SLB Port 8# filt ena
```

On the Web Switch, Apply, Save, and Verify the Configuration

1. **Apply and save the configuration changes.**

```
# apply
# save
```

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 Alteon Web switch to combine cookie-based persistence in the cookie rewrite mode with SSL offload through the iSD-SSL. These steps assume that the network is already configured as described in “Web Server Accelerator” on page 118.

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.**

```
# /cfg/slb/virt 1/service 81
>> Virtual Server 1 Service 81# pbind
Enter client|cookie|sslid|disable persistence mode: cookie
Enter passive|rewrite cookie persistance mode [p/r]: rewrite
Enter Cookie Name: AlteonSession
Enter the number of bytes to be extract: 8
Look for cookie in URL [e|d]: d
```

Active cookie mode (cookie rewrite mode) only works for cookies defined in the HTTP cookie header, not cookies defined in the URI. In Web OS 8.3 and higher, the switch can be configured to look for the cookie to rewrite in up to 16 server response packets in a TCP connection. This ensures that active cookie mode works well with HTTP 1.1, where multiple HTTP GET requests happen within the same TCP connection and the cookie may therefore not be present in the first server response packet. In Web OS versions previous to 8.3, the switch could only rewrite a cookie if it was present in the first server response packet in a TCP connection.

4. **Apply and save the changes.**

```
# apply
# save
```

Redundant Active-Standby Configuration

The following steps are used for configuring a redundant active-standby configuration with two Alteon Web switches and two iSD-SSLs, as illustrated below. It is assumed that the first Web switch is configured as in the example for "Web Server Accelerator" on page 118.

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

NOTE – Port 3 on VLAN 2, and port 8 on VLAN 3 (configured in "Web Server Accelerator" on page 118) are not required for this example.

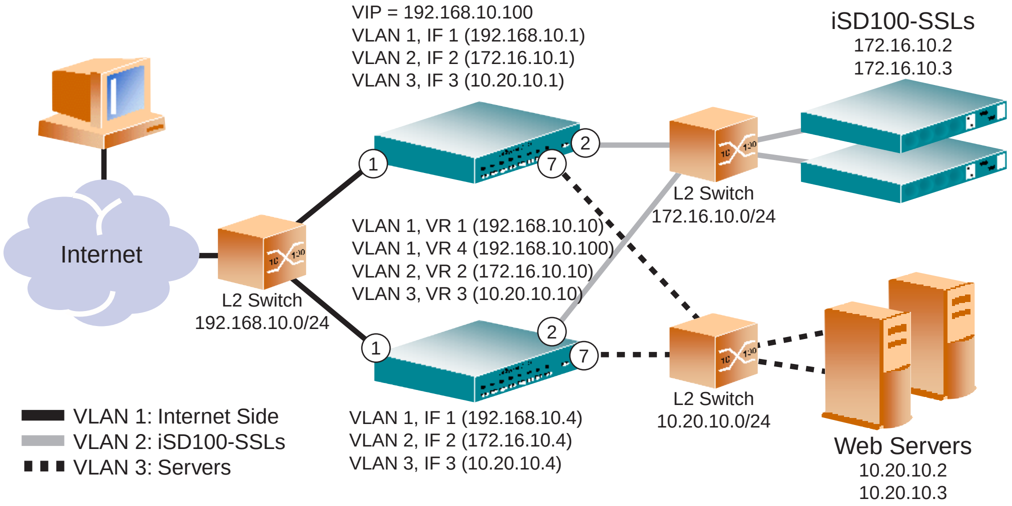

VIP = 192.168.10.100
VLAN 1, IF 1 (192.168.10.1)
VLAN 2, IF 2 (172.16.10.1)
VLAN 3, IF 3 (10.20.10.1)
iSD100-SSLs
172.16.10.2
172.16.10.3
1
2
7
L2 Switch
172.16.10.0/24
Internet
L2 Switch
192.168.10.0/24
VLAN 1, VR 1 (192.168.10.10)
VLAN 1, VR 4 (192.168.10.100)
VLAN 2, VR 2 (172.16.10.10)
VLAN 3, VR 3 (10.20.10.10)
1
2
7
L2 Switch
10.20.10.0/24
VLAN 1: Internet Side
VLAN 2: iSD100-SSLs
VLAN 3: Servers
VLAN 1, IF 1 (192.168.10.4)
VLAN 2, IF 2 (172.16.10.4)
VLAN 3, IF 3 (10.20.10.4)
Web Servers
10.20.10.2
10.20.10.3

Figure 1 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

Create the Necessary VLANs (Web Switch 2)

In this configuration, there will be three VLANs: VLAN 1 for the Web switch, VLAN 2 for the iSD-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, log in as the administrator.**

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

```
# /cfg/vlan 2
>> VLAN 2# add 2
Port 2 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# ena
```

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

```
# /cfg/vlan 3
>> VLAN 3# add 7
Port 7 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 3# ena
```

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

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

```
# /cfg/stp/port 2
>> Spanning Tree Port 2# off
>> Spanning Tree Port 2# ../port 7
>> Spanning Tree Port 7# off
```

Configure IP Interfaces for Each VLAN (Web Switch 2)

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

```
# /cfg/ip/if 1
>> IP Interface 1# addr 192.168.10.4
>> IP Interface 1# mask 255.255.255.0
>> IP Interface 1# ena
```

2. **Configure an IP interface for iSD-SSL traffic.**

```
# /cfg/ip/if 2
>> IP Interface 2# addr 172.16.10.4
>> IP Interface 2# mask 255.255.255.0
>> IP Interface 2# vlan 2
>> IP Interface 2# ena
```

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

```
# /cfg/ip/if 3
>> IP Interface 3# addr 10.20.10.4
>> IP Interface 3# mask 255.255.255.0
>> IP Interface 3# vlan 3
>> IP Interface 3# ena
```

4. **Enable global IP forwarding between the configured IP interfaces.**

```
# /cfg/ip/frwd
>> IP Forwarding# on
Current status: OFF
New status:     ON
```

5. **Apply the changes.**

```
# apply
```

Prepare to Receive Synchronization (Web Switch 2)

Synchronize the configuration between two Web switches.

1. **Configure the synchronization parameters.**

```
# /cfg/slb/sync
>> Config Synchronization# prios d
>> Config Synchronization# peer 1
>> Peer Switch 1# addr 192.168.10.1
>> Peer Switch 1# ena
```

Set the Web switch 1 IP interface as peer 1 and disable synchronization of VRRP priorities.

2. **Apply the configuration.**

```
# apply
```

Configure VRRP (Web Switch 1)

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

1. **On Web switch 1, log in as the administrator.**

2. **Globally turn on the VRRP.**

```
# /cfg/vrrp/on
```

3. **Configure virtual router 1.**

```
# /cfg/vrrp/vr 1
>> VRRP Virtual Router 1# vrid 1
>> VRRP Virtual Router 1# addr 192.168.10.10
>> VRRP Virtual Router 1# if 1
>> VRRP Virtual Router 1# prio 101
>> VRRP Virtual Router 1# share dis
>> VRRP Virtual Router 1# track/l4pts e
>> VRRP Virtual Router 1 Priority Tracking# ../ena
```

4. **Configure virtual router 2.**

```
# /cfg/vrrp/vr 2
>> VRRP Virtual Router 2# vrid 2
>> VRRP Virtual Router 2# addr 172.16.10.10
>> VRRP Virtual Router 2# if 2
>> VRRP Virtual Router 2# prio 101
>> VRRP Virtual Router 2# share dis
>> VRRP Virtual Router 2# track/14pts e
>> VRRP Virtual Router 2 Priority Tracking# ../ena
```

5. **Configure virtual router 3.**

```
# /cfg/vrrp/vr 3
>> VRRP Virtual Router 3# vrid 3
>> VRRP Virtual Router 3# addr 10.20.10.10
>> VRRP Virtual Router 3# if 3
>> VRRP Virtual Router 3# prio 101
>> VRRP Virtual Router 3# share dis
>> VRRP Virtual Router 3# track/14pts e
>> VRRP Virtual Router 3 Priority Tracking# ../ena
```

6. **Configure virtual router 4, which is the virtual server router.**

```
# /cfg/vrrp/vr 4
>> VRRP Virtual Router 4# vrid 4
>> VRRP Virtual Router 4# addr 192.168.10.100
>> VRRP Virtual Router 4# if 1
>> VRRP Virtual Router 4# prio 101
>> VRRP Virtual Router 4# share dis
>> VRRP Virtual Router 4# track/14pts e
>> VRRP Virtual Router 4 Priority Tracking# ../ena
```

NOTE – Make sure the iSD-SSLs are configured to use the IP address of Virtual Router 2 on VLAN 2 as their default gateway. For more information about gateway configuration, see the **`gateway`** command under “iSD Host Configuration Menu” on page 96. Likewise, the Web servers must be configured to use the IP address of Virtual Router 3 on VLAN 3 as their default gateway.

Prepare and Send Synchronization (Web Switch 1)

1. **Configure the Synchronization parameters.**

```
# /cfg/slb/sync
>> Config Synchronization# prios d
>> Config Synchronization# peer 1
>> Peer Switch 1# addr 192.168.10.4
>> Peer Switch 1# ena
```

2. **Apply and save the configuration changes.**

```
# apply
# save
```

3. **Synchronize server load balancing configuration on peers.**

```
# /oper/slb/sync
Synchronizing VRRP, FILT, PORT and SLB configuration
to 192.168.10.4

Confirm synchronizing the configuration to 192.168.10.4 [y/n]: y
```

CAUTION—The **`/oper/slb/sync`** command will synchronize the current filter, port, and server load balancing configuration between the two switches, besides the VRRP configuration.

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.

Mail Server Accelerator

Figure 8-1 illustrates the same network configuration for the iSD-SSL as in the Web server accelerator example, using an Alteon Web switch. However, this configuration example describes how to use the iSD-SSLs for mail server accelerator purposes.

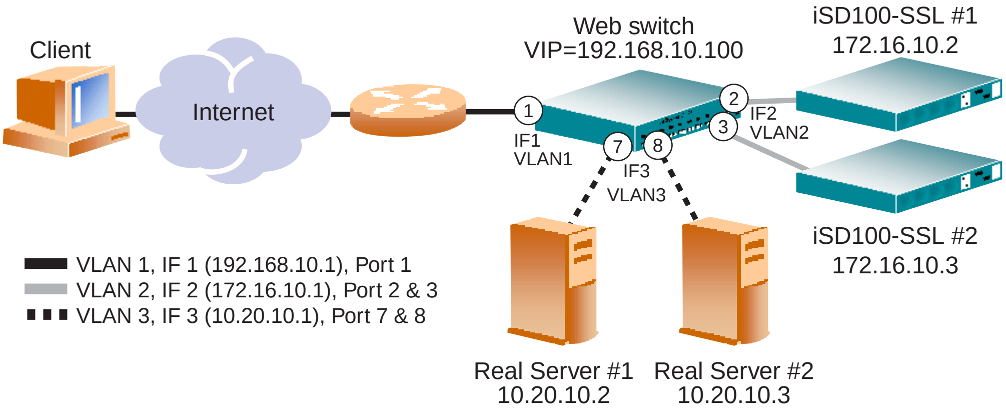


Figure 2 Sample Mail Server Accelerator Network Using Multiple iSD-SSLs

Initial Setup

First do the initial setup of the two iSD-SSLs as described in Chapter 3, “Initial Setup’’using the IP addresses shown in Figure 8-1. Then connect to one of the iSD-SSLs to add a certificate.

On the iSD-SSL, Add a Server Certificate

This step presumes that you have a server certificate, signed by a certificate authority (CA), and a private key. The process for obtaining the required certificate file is covered in “Generating and Submitting a CSR Using the CLI” on page 152.

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

```
# /cfg/ssl/cert
Enter certificate number: (1-) 1
Creating Certificate 1
>> Certificate 1# cert
Paste the certificate, press Enter to create a new line, and then
type "..."(without the quotation marks) to terminate.
```

The example above assumes that the certificate signing request (CSR) was generated from certificate number 1, which implies that the private key that corresponds to the public key in the certificate is already in place.

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 certificate into the terminal window. For more detailed information about how to add certificates and keys to the iSD-SSL, see "Adding Certificates to the iSD-SSL" on page 156.

Important—*Once you have pasted the entire contents of the certificate file, press ENTER to create a new empty line and then type three periods (`...`). Press ENTER again to complete the installation of the certificate.*

NOTE – Under Microsoft Windows, HyperTerminal may be slow to complete the copy-and-paste operation.

Configure iSD-SSL Parameters

Connect to the MIP of the iSD-SSLs to configure them. The configuration changes will be distributed automatically to all members in the cluster.

On the iSD-SSL, Create a Virtual SSL Server for SMTPS

1. **Create the necessary virtual SSL server for SMTPS.**

```
# /cfg/ssl/server
Enter virtual server number: (1-) 1
Creating new server 1
>> Server 1#
```

This step creates a new virtual SSL server in the iSD-SSL. Each virtual SSL server listens to a specific TCP port and is mapped to a virtual server on the Web switch. If you have already created a virtual SSL server for HTTPS services, you must create additional virtual servers for SMTPS and POP3S mail services. Each virtual SSL server must be assigned a unique number.

2. **Define a name for virtual SSL server 1.**

```
>> Server 1# name
Current value: ""
Enter new SSL server name: SMTPS
```

This step lets you specify a name, by which you can identify SSL server 1. To view the numbers and related names of all configured SSL servers, use the command **`/cfg/ssl/cur`**. The name you specify is mainly intended for your own reference, and is not critical for the configuration itself. As the example above suggests, the name can indicate the service for which the SSL server was created.

3. **Set listen TCP port for virtual SSL server 1.**

```
>> Server 1# port
Current value: 443 (https)
Enter listen port number: 465
```

Each time you create a new SSL server, the listen port is automatically set to 443. Since you are setting up the iSD-SSL for secure mail offload purposes, configure the listen port to 465, which is the TCP port used by SMTPS.

4. **Connect virtual SSL server 1 to the desired Virtual Server IP address on the Web switch.**

```
>> Server 1# vip
Current value: <not set>
Enter IP address: 192.168.10.100
```

This step connects SSL server 1 to the IP address of the desired virtual server on the Web switch.

5. **Set the Real Server IP address to which SSL Server 1 should connect when initiating requests.**

```
>> Server 1# rip
Current value: 0.0.0.0
Enter IP address to connect to: 0.0.0.0
```

Preserve the current value of the Real Server IP address, which should be 0.0.0.0. At first glance this configuration may perhaps seem a bit odd. However, by specifying 0.0.0.0 as the Real Server IP address, the SSL server is instructed to use the destination IP address (in the received packets) when initiating requests sent to the Virtual Server IP address. Because the destination IP address in the received packets corresponds to the IP address of the virtual server, the requests will always reach the correct Virtual Server IP address.

6. **Set the server port to which SSL server 1 should connect when initiating requests.**

```
>> Server 1# rport
Current value: 0 [81]
Enter port to connect to: 25
```

This step sets the TCP port to which SSL Server 1 connects when initiating requests.

7. **Specify the certificate to be used by virtual SSL Server 1.**

```
>> Server 1# ssl
>> SSL Settings for Server 1# cert
Current value: <not set>
Enter certificate number: (1-) 1
```

Note that you are prompted to type the number of an existing certificate, not the name assigned to a certificate. To view all certificates currently added to the iSD-SSL, use the command **`/cfg/ssl/cur`**. For more information about how to add a certificate, see "Adding Certificates to the iSD-SSL" on page 156.

On the iSD-SSL, Create the Virtual SSL Server for POP3S

1. **Create the necessary virtual SSL server for POP3S.**

```
# /cfg/ssl/server
Enter virtual server number: (1-) 2
Creating new server 2
>> Server 2#
```

This creates a virtual SSL server intended for POP3S services. Recall that each virtual SSL server must be assigned a unique number.

2. **Define a name for virtual SSL server 2.**

```
>> Server 2# name
Current value: ""
Enter new SSL server name: POP3S
```

3. **Set listen TCP port for virtual SSL server 2.**

```
>> Server 2# port
Current value: <not set> [443 (https)]
Enter listen port number: 995
```

This step sets the listen port of virtual SSL server 2 to 995, which is the TCP port used by POP3S.

4. **Map SSL server 2 to the Virtual Server IP address on the Web switch.**

```
>> Server 2# vip
Current value: <not set>
Enter IP address: 192.168.10.100
```

This step maps SSL server 2 to the same Virtual Server IP address on the Web switch as the one to which you mapped SSL server 1.

5. **Set the Real Server IP address to which SSL Server 2 should connect when initiating requests.**

```
>> Server 1# rip
Current value: 0.0.0.0
Enter IP address to connect to: 0.0.0.0
```

As for virtual SSL server 1, preserve the current value of 0.0.0.0 for virtual SSL server 2.

6. **Set the server port to which SSL server 2 should connect when initiating requests.**

```
>> Server 2# rport
Current value: 0 [81]
Enter port to connect to: 110
```

This step sets the TCP port, to which the SSL Server 2 connects when initiating requests.

As you will see further ahead, the virtual server will have services enabled on both port 25 (SMTP) and 110 (POP3) to match the settings on virtual SSL server 1 and 2 respectively.

7. **Specify the certificate to be used by virtual SSL Server 2.**

```
>> Server 2# ssl
>> SSL Settings for Server 2# cert
Current value: <not set>
Enter certificate number: (1-) 1
```

Specify the same certificate number as you did for virtual SSL server 1.

8. **Apply the changes.**

```
>> SSL Settings for Server 2# apply
```

On the Web Switch, 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 iSD-SSL units, and VLAN 3 for the real mail servers. Since VLAN 1 is the default, only VLAN 2 and VLAN 3 require additional configuration. Note that all the sample configuration changes that follow are performed on the Web switch.

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

```
# /cfg/vlan 2
>> VLAN 2# add 2
Port 2 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# add 3
Port 3 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# ena
```

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

```
# /cfg/vlan 3
>> VLAN 3# add 7
Port 7 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 3# add 8
Port 8 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 3# ena
```

3. **Disable Spanning Tree Protocol (STP) for the iSD-SSL ports 2 and 3 and real server ports 7 and 8.**

   STP will not function across multiple VLANs.

```
# /cfg/stp/port 2
>> Spanning Tree Port 2# off
>> Spanning Tree Port 2# ../port 3
>> Spanning Tree Port 3# off
>> Spanning Tree Port 3# ../port 7
>> Spanning Tree Port 7# off
>> Spanning Tree Port 7# ../port 8
>> Spanning Tree Port 8# off
```

On the Web Switch,Configure One IP Interface for Each VLAN

NOTE – If you prefer, you can reverse the order of the first two commands (**`addr`** and **`mask`**) in the example below. By entering the mask first, the Web switch will automatically calculate the correct broadcast address for you. The calculated broadcast address is displayed immediately after you provide the IP address of the interface, and will be applied together with the other settings when you execute the **`apply`** command.

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

```
# /cfg/ip/if 1
>> IP Interface 1# addr 192.168.10.1
>> IP Interface 1# mask 255.255.255.0
>> IP Interface 1# broad 192.168.10.255
>> IP Interface 1# vlan 1
>> IP Interface 1# ena
```

2. **Configure an IP interface for iSD-SSL traffic with VLAN 2.**

```
# /cfg/ip/if 2
>> IP Interface 2# addr 172.16.10.1
>> IP Interface 2# mask 255.255.0.0
>> IP Interface 2# broad 172.16.255.255
>> IP Interface 2# vlan 2
>> IP Interface 2# ena
```

3. **Configure an IP interface for the real server traffic with VLAN 3.**

```
# /cfg/ip/if 3
>> IP Interface 3# addr 10.20.10.1
>> IP Interface 3# mask 255.255.255.0
>> IP Interface 3# broad 10.20.10.255
>> IP Interface 3# vlan 3
>> IP Interface 3# ena
```

4. **Apply the changes.**

```
# apply
```

On the Web Switch,Configure Mail Server Load Balancing Parameters

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

```
# /cfg/slb/real 1
>> Real Server 1# rip 10.20.10.2
>> Real Server 1# ena
>> Real Server 1# ../real 2
>> Real Server 2# rip 10.20.10.3
>> Real Server 2# ena
```

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

```
# /cfg/slb/group 1
>> Real server group 1# add 1
>> Real server group 1# add 2
```

3. **Set and enable the IP address for Virtual Server 1, enable services for SMTP and POP3, and connect real server group 1 to the Virtual Server.**

```
# /cfg/slb/virt 1
>> Virtual Server 1# vip 192.168.10.100
>> Virtual Server 1# ena
>> Virtual Server 1# service smtp
>> Virtual Server 1 smtp Service# group 1
>> Virtual Server 1 smtp Service# ../service pop3
>> Virtual Server 1 pop3 Service# group 1
>> Virtual Server 1 pop3 Service# apply
```

Enable services for SMTP and POP3 on Virtual Server 1 for communication between the iSD-SSLs and the real mail servers. This step also connects the real mail servers in server group 1 to the enabled virtual server.

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

```
# /cfg/slb/port 1/client ena
```

5. **Enable client processing on ports 2 and 3 leading to iSD-SSLs.**

```
# /cfg/slb/port 2
>> SLB Port 2# client ena
>> SLB Port 2# ../port 3
>> SLB Port 3# client ena
```

6. **Enable server processing on ports 7 and 8 leading to real servers.**

```
# /cfg/slb/port 7
>> SLB Port 7# server ena
>> SLB Port 7# ../port 8
>> SLB Port 8# server ena
```

7. **Turn on Layer 4 processing.**

```
# /cfg/slb/on
```

8. **Apply the changes.**

```
# apply
```

On the Web Switch,Configure iSD-SSL Load Balancing Parameters

Set and enable the IP addresses of the iSD-SSLs, and create a group in the switch for load balancing.

1. **For each iSD-SSL create a Real Server IP address in the switch**

```
# /cfg/slb/real 3
>> Real server 3# rip 172.16.10.2
>> Real server 3# ena
>> Real server 3# ../real 4
>> Real server 4# rip 172.16.10.3
>> Real server 4# ena
```

2. **Create a Real Server Group and add the Real Servers (the iSD-SSLs in this case)**

```
# /cfg/slb/group 2
>> Real server group 2# add 3
>> Real server group 2# add 4
```

3. **Set the load balancing metric and the health check type for Real Server Group 2.**

```
# /cfg/slb/group 2
>> Real server group 2# metric hash
>> Real server group 2# health tcp
```

4. **Apply the changes.**

```
# apply
```

On the Web Switch, Configure Filters

1. **Create a filter to redirect client SMTPS traffic intended for port 465.**

```
# /cfg/slb/filt 110
>> Filter 110# proto tcp
>> Filter 110# dport 465
>> Filter 110# action redir
>> Filter 110# group 2
>> Filter 110# rport 465
>> Filter 110# adv/fwlb e
>> Filter 110 Advanced# ../ena
```

When this filter is added to the switch port leading to the Internet, all incoming SMTPS traffic is redirected to the iSD-SSLs in real server group 2. Firewall redirect hash method is also enabled, using redirection based on hashing on both the source IP and the destination IP of the packets.

The SMTPS traffic filter should be given a high number (a lower priority), such as 110, so as not to interfere with other filters.

2. **Create a filter to redirect client POP3S traffic intended for port 995.**

```
# /cfg/slb/filt 120
>> Filter 120# proto tcp
>> Filter 120# dport 995
>> Filter 120# action redir
>> Filter 120# group 2
>> Filter 120# rport 995
>> Filter 120# adv/fwlb e
>> Filter 120 Advanced# ../ena
```

When this filter is added to the switch port leading to the Internet, all incoming POP3S traffic is redirected to the iSD-SSLs in real server group 2. Firewall redirect hash method is also enabled, using redirection based on hashing on both the source IP and the destination IP of the packets.

The POP3S traffic filter should be given a high number (a lower priority), such as 120, so as not to interfere with other filters.

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

```
# /cfg/slb/filt 224
>> Filter 224# sip any
>> Filter 224# dip any
>> Filter 224# proto any
>> Filter 224# action allow
>> Filter 224# ena
```

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

```
# /cfg/slb/port 1
>> SLB Port 1# add 110
>> SLB Port 1# add 120
>> SLB Port 1# add 224
>> SLB Port 1# filt ena
```

This step adds the SMTPS and POP3S redirect filters and the default deny filter to the client port leading to the Internet.

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

```
# /cfg/slb/filt 160
>> Filter 160# action allow
>> Filter 160# sip 192.168.10.100
>> Filter 160# smask 255.255.255.255
>> Filter 160# dip 10.20.10.1
>> Filter 160# dmask 255.255.255.255
>> Filter 160# proto tcp
>> Filter 160# sport smtp
>> Filter 160# dport any
>> Filter 160# ena
```

The health check filter should be given a smaller number (higher priority) than the redirection filters set for the real server responses back to the iSD-SSLs.

The source IP (SIP) must be the virtual server IP (VIP) address of the switch. The destination IP (DIP) must be the IP address of the switch interface number 3, which is connected to server ports 7 & 8 leading to the real mail servers.

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

```
# /cfg/slb/filt 210
>> Filter 210# proto tcp
>> Filter 210# sport 25
>> Filter 210# action redir
>> Filter 210# group 2
>> Filter 210# adv/fwlb e
>> Filter 210 Advanced# ../ena
```

This filter, when added to the switch ports leading to the real mail servers, will redirect TCP traffic from port 25 back to the iSD-SSLs in group 2.

Firewall redirect hash method is also enabled, which means the packets are hashed based on both the source IP and the destination IP. This makes the return packets hash to the same IP address of the iSD-SSL in real server group 2, as from which the packets originated.

7. **Create a filter to redirect real server responses back to the iSD-SSL.**

```
# /cfg/slb/filt 220
>> Filter 220# proto tcp
>> Filter 220# sport 110
>> Filter 220# action redir
>> Filter 220# group 2
>> Filter 220# adv/fwlb e
>> Filter 220 Advanced# ../ena
```

This filter, when added to the switch ports leading to the real Web servers, will redirect TCP traffic from port 110 back to the iSD-SSLs in group 2.

Firewall redirect hash method is also enabled, which means the packets are hashed based on both the source IP and the destination IP. This makes the return packets hash to the same IP address of the iSD-SSL in real server group 2, as from which the packets originated.

8. **Add the real server filters to the real server ports.**

```
# /cfg/slb/port 7
>> SLB Port 7# add 160
>> SLB Port 7# add 210
>> SLB Port 7# add 220
>> SLB Port 7# add 224
>> SLB Port 7# filt ena
>> SLB Port 7# ../port 8
>> SLB Port 8# add 160
>> SLB Port 8# add 210
>> SLB Port 7# add 220
>> SLB Port 8# add 224
>> SLB Port 8# filt ena
```

On the Web Switch, Save the Configuration

1. **Apply and save the configuration changes.**

```
# apply
# save
```

You also need to instruct the intended users of the service that they need to enable secure e-mail in their mail client application. If this feature is not supported, they may need to upgrade to a newer version.

CHAPTER 9
Managing Certificates and Client Authentication

This chapter describes common tasks involving certificates and client authentication. The chapter also provides detailed step-by-step instructions for generating certificate signing requests, adding certificates to the iSD-SSL, generating and revoking client certificates, as well as configuring the iSD-SSL to require client certificates.

The iSD-SSL accelerator supports certificates in the PEM, NET, DER and PKCS12 formats. 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 using the command line interface in the iSD-SSL are:

- Generate a Certificate Signing Request (CSR) and send it to a Certificate Authority (CA, such as Entrust or VeriSign) for certification.
- Add the signed certificate to the iSD-SSL.

NOTE – Even though the iSD-SSL supports keys and certificates created by using Apache-SSL, OpenSSL, or Stronghold SSL, the preferred method from a security point of view is to create keys and generate certificate signing requests from within the iSD-SSL by using the command line interface. This way, the encrypted private key never leaves the iSD-SSL, and is invisible to the user.

Generating and Submitting a CSR Using the CLI

1. **Initiate requesting a certificate signing request (CSR), and provide the necessary information.**

```
>> Main# cfg/ssl/cert
Enter certificate number (1-): <certificate number>
Creating Certificate 1
>> Certificate 1# request
The combined length of the following parameters may not exceed 225
bytes.
Country Name (2 letter code):
State or Province Name (full name):
Locality Name (e.g., city):
Organization Name (e.g., company):
Organizational Unit Name (e.g., section):
Common Name (e.g., your name or your server's hostname):
Email Address:
Generate new key pair (y/n) [y]:
Key size [1024]:
Request a CA certificate (y/n) [n]:
```

Note – When specifying a certificate number, make sure not to use a number currently used by an existing certificate. To view information about configured certificates, type the command **`/cfg/ssl/cur`** and press ENTER. The information displayed lists all configured certificates by their main attributes, including the certificate number (such as "Certificate 1").

Explanations for the requested units of information:

- Country Name: The two-letter ISO code for the country where the Web server is located.
- State or Province Name: 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 Name: The name of the city where the head office of the organization is located.
- Organization Name: 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 Name: 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.
- Email Address: Enter the user’s e-mail address.
- Generate new key pair [y]: In most cases you will want to generate a new key pair for a CSR. However, if a configured certificate is approaching its expiration date and you want to renew it without replacing the existing key, answering no (n) is appropriate. The CSR will then be based on the existing key (for the specified certificate number) instead.
- Key size [1024]: Specify the key length of the generated key. The default value is 1024.
- Request a CA certificate (y/n) [n]: Lets you specify whether to request a CA certificate to use for client authentication. The default value is to not request a CA certificate.

2. **Generate the CSR.**

   Press ENTER after you have provided the requested information. The CSR is generated and displayed on screen:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB+jCCAWMCAQAwgZQxCzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0x
DjAMBgNVBAcTBUtpc3RhMREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9j
dTEZMBcGA1UEAxMQd3d3LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9y
Ympvcm5AYmx1ZXRhaWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX
2rSY81cgKJODuUreGF3ZnK7RvlRqSV/TIMS4UerqXPKpTjfMAWDjBG77hjIAOOZO
FQKFB5x/Zs9kNMBUmPBokA1/GXghomOvBhMIJBZBiUVtJNGmv2sjeqNXxsUg5XfJ
iwV2LjUvw65EzCLpq5dhq6ZPEx7tAgqB2Wgu8MolwQIDAQABoCUwIwYJKoZIhvcN
AQkHMRYTFEEgY2hhbGxlbmdlIHBhc3N3b3JkMA0GCSqGSIb3DQEBBAUAA4GBACem
SJr8Xuk9PQZPuIPV7iCDG+eWneU3HH3F3DigW3MILCLNqweljKw5pZdAr9HbDwU+
2iQGbTSH0nVeoqn4TJujq96XpIrbiAFdE1tR7Lmf6oGdrwG8ypfRpp3PmfId6lp+
HJ2fUGliPYyNtd/94AL6wW8un208+icCHq/S0yjz
-----END CERTIFICATE REQUEST-----
```

3. **Save the CSR to a file.**

   Copy the entire CSR, including the “`-----BEGIN CERTIFICATE REQUEST-----`” and “`-----END CERTIFICATE REQUEST-----`” lines, and paste it into a text editor. Save the file with a **.csr** extension. The name you define can indicate the server on which the certificate is to be used.

4. Save the private key to a file.

NOTE – Provided you intend to use the same certificate number when adding the certificate returned to you (after the CSR has been processed by a certificate authority), this step is only necessary if you want to create a backup copy of the private key. When generating a CSR, the private key is created and stored (encrypted) transparently to the user, and you need only add the received certificate that contains the corresponding public key.

First, type the **`apply`** command and press ENTER.

```
>> Certificate # apply
Changes applied successfully.
```

Then, type the **`export`** command and press ENTER. Specify a password phrase to protect the private key, and make sure to remember the password phrase.

```
>> Certificate 1# export
Enter export pass phrase:
Reconfirm export pass phrase:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,27C89CBC65615F06

5cZBjjKAVoYRdtLYFa0zBpKQhK3yAJ+qSXxkrNCaRlSzuX2iClaAHtsSueGvJg7o
HNHcZVZCCxZtSLIsBTvDK0xY5ZomlqAU+JdWn0zc4hilf9KjLRBzk2p7azQUCMqW
jVJ5x9oFeuurfm3e6kqdCvnPweYJmZGp5A33Y7EV7TY5v30lZWnZrmD0tTfvljq7
rAfavlfWFgeBRG5kcdOgeb1hIHF2X16YMcp7YQUWGBccA1R7FvsVuvFuva9icCN1
++bF1GjfIMcSdpFt6Rkyq/CXBy3LVCAX0rfdPjaniO8G6sARa+qbkpnOvsA2eMc4
MXDHxc7+EavNBOIxAPL8PXunns53MYiWx5INWiQPh38gkjhi+n+75PJQi/J1Ab5p
iOpqHDUfcUBwdrkp/+3SKMAbc4VIaBnbGpfv2hNrr0Q/LyJilhjEPX+LIizkhWKo
QcdeqY3KyJGDugnqJBfybkNysKpPMDtd5Q7Yki5HdRe1RXenowDpiQlxToLlz9Bl
XDwFj2Ag7IfUk3Kwin2dn5KKSM35+a6Ateb4WjctIZGRlsi9JqQN8GOZf4uwj/Wg
nkzQeQ1rExpLbGTfiuRfVAstvo8bUIjm5xDY5HSmKx1FA2O2W2E/mB02Q9ZckG7I
hjB3ku2Wnvzv91qiCq6ljPN+hl4/zVmo6c/v2+pzubAxbOF5/NfQWwyogx0quCgN
4LaxsUXb0kpak4OLXNoqPVEDysYKD1zGCnrb3rgQ8hyhgoVHcRt6Rtsi4/6UzCkT
wtRtiyR96OEmVVA+x/8jsrU3LLCPYsswP0zje87mphh1PwiSRIMB6Q==
-----END RSA PRIVATE KEY-----
```

Copy the private key, including the "`-----BEGIN RSA PRIVATE KEY-----`" and "`-----END RSA PRIVATE KEY-----`" lines, and paste it into a text editor. Save the file with a **.key** extension. Preferably, use the same file name that you defined for the **.csr** file, so the connection between the two files becomes obvious. The name you define can indicate the server on which the certificate and the corresponding private key is to be used.

After you have received the processed CSR from a CA, make sure to create a backup copy of the certificate as well.

5. **Open and copy the CSR.**

   In a text editor, open the **.csr** file you created in Step 3. It should appear similar to the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB+jCCAWMCAQAwgZQxCzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0x
DjAMBgNVBAcTBUtpc3RhMREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9j
dTEZMBcGA1UEAxMQd3d3LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9y
Ympvcm5AYmx1ZXRhaWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX
2rSY81cgKJODuUreGF3ZnK7RvlRqSV/TIMS4UerqXPKpTjfMAWDjBG77hjIAOOZO
FQKFB5x/Zs9kNMBUmPBokA1/GXghomOvBhMIJBZBiUVtJNGmv2sjeqNXxsUg5XfJ
iwV2LjUvw65EzCLpq5dhq6ZPEx7tAgqB2Wgu8MolwQIDAQABoCUwIwYJKoZIhvcN
AQkHMRYTFEEgY2hhbGxlbmdlIHBhc3N3b3JkMA0GCSqGSIb3DQEBBAUAA4GBACem
SJr8Xuk9PQZPuIPV7iCDG+eWneU3HH3F3DigW3MILCLNqweljKw5pZdAr9HbDwU+
2iQGbTSH0nVeoqn4TJujq96XpIrbiAFdE1tR7Lmf6oGdrwG8ypfRpp3PmfId6lp+
HJ2fUGliPYyNtd/94AL6wW8un208+icCHq/S0yjz
-----END CERTIFICATE REQUEST-----
```

   Copy the entire CSR, including the "`-----BEGIN CERTIFICATE REQUEST-----`" and "`-----END CERTIFICATE REQUEST-----`" lines.

6. **Submit the CSR to Verisign, Entrust, 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 added into the iSD-SSL.

Adding Certificates to the iSD-SSL

Using the encryption capabilities of the iSD-SSL requires adding a key and certificate that conforms to the X.509 standard to the iSD-SSL. If you have more than one iSD-SSL in a cluster, the key and certificate need only be added to one of the devices. As with configuration changes, the information is automatically propagated to all other devices in the cluster.

There are two ways to install a key and certificate into the iSD-SSL:

- Copy-and-paste the key/certificate.
- Download the key/certificate from a TFTP server.

The iSD-SSL supports the following certificate and key formats:

- PEM
- NET
- DER
- PKCS12 (also known as PFX)

Besides these, the iSD-SSL also supports keys in the PKCS8 format (used in WebLogic) and the KEY format (used in MS IIS 4.0).

Keys from Netscape Enterprise Server or iPlanet Server can also be added to the iSD-SSL. However, these keys require that you first use a conversion tool. For more information about the conversion tool, contact Alteon WebSystems Customer Support. See "Contacting Alteon WebSystems" on page 16 for contact information.

NOTE – When performing a copy-and-paste operation to add a certificate or key, you must always use the PEM format.

Using a Copy-and-Paste Operation to Add Certificates

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

1. **Type the following command from the Main menu prompt on the iSD-SSL to start adding a certificate.**

```
>> Main# cfg/ssl/cert
Enter certificate number: (1-) <number of the certificate you want to configure>
>> Certificate 1# cert
Paste the certificate, press Enter to create a new line, and then
type "..." (without the quotation marks) to terminate.
>
```

In most cases you should specify the same certificate number as the certificate number you used when generating the CSR. By doing so, you do not have to add the private key because this key remains connected to the certificate number that you used when you generated the CSR.

If you have obtained a key and a certificate by other means than generating a CSR using the **`request`** command on the iSD-SSL, specify a certificate number not used by a configured certificate before pasting the certificate. If the private key and the certificate are not contained in the same file, use the **`key`** or **`tftpkey`** command to add the corresponding private key.

To view information about configured certificates, type the command **`/cfg/ssl/cur`** and press ENTER. The information displayed lists all configured certificates by their main attributes.

2. **Copy the contents of your certificate file.**

Open the certificate file you have received from a CA in a text editor and copy the entire contents. Make sure the selected text includes the "`-----BEGIN CERTIFICATE-----`" and "`-----END CERTIFICATE-----`" lines.

3. **Paste the contents of the certificate file at the command prompt.**

Now, paste the certificate at the command line interface prompt, press ENTER to create a new empty line, and then type "**`...`**" (without the quotation marks). Press ENTER again to complete the installation of the certificate.

Your screen output should now resemble the following example:

```
>> Certificate 1# cert
Paste the certificate, press Enter to create a new line, and then
type "..." (without the quotation marks) to terminate.
> -----BEGIN CERTIFICATE-----
> MIIDTDCCArWgAwIBAgIBADANBgkqhkiG9w0BAQQFADB9MQswCQYDVQQGEwJzZTEO
> MAwGA1UECBMFa2lzdGExEjAQBgNVBAcTCXN0b2NraG9sbTEMMAoGA1UEChMDZG9j
> MQ0wCwYDVQQLEwRibHVlMRIwEAYDVQQDEwl3d3cuYS5jb20xGTAXBgkqhkiG9w0B
> CQEWCnR0dEBjY2MuZG4wHhcNMDAxMjIyMDkxOTI0WhcNMDExMjIyMDkxOTI0WjB9
> MQswCQYDVQQGEwJzZTEOMAwGA1UECBMFa2lzdGExEjAQBgNVBAcTCXN0b2NraG9s
> bTEMMAoGA1UEChMDZG9jMQ0wCwYDVQQLEwRibHVlMRIwEAYDVQQDEwl3d3cuYS5j
> b20xGTAXBgkqhkiG9w0BCQEWCnR0dEBjY2MuZG4wgZ8wDQYJKoZIhvcNAQEBBQAD
> gY0AMIGJAoGBALXym9cIVfHZUZFE1MFi+xefDviIEvilnJAQSSPITnZa69fzGcL3
> vpQv0NLxNffs1jEw4RPDMKu2rQ9N02EiiJcrCHnaSNZPdwGoX39IkEUkANzm3mh2
> DlP1RfW4ejpNKsG5Tme/e1vFYWXeXXI1oRtdPIaVGxK8pvqBEHDXCcJlAgMBAAGj
> gdswgdgwHQYDVR0OBBYEFJBM3K0KB03fpCOVrQCC34hovwM8MIGoBgNVHSMEgaAw
> gZ2AFJBM3K0KB03fpCOVrQCC34hovwM8oYGBpH8wfTELMAkGA1UEBhMCc2UxDjAM
> BgNVBAgTBWtpc3RhMRIwEAYDVQQHEwlzdG9ja2hvbG0xDDAKBgNVBAoTA2RvYzEN
> MAsGA1UECxMEYmx1ZTESMBAGA1UEAxMJd3d3LmEuY29tMRkwFwYJKoZIhvcNAQkB
> Fgp0dHRAY2NjLmRuggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEA
> m/GKwEyDKCm2qdPt8+pz1znSGNaRTxfK1R0mjtnDGFb0qk+Bv7d9YlX+1QTZhxnZ
> Z4JXuWPJS36kAwiirVbOIaIforIVa+IUlo8HUjMvxzIqCYPiiDwBcBi3NsvjlFM7
> i24Q+lvDLE/Ko+x/YEnNukfp3SBXiJqZ8WZIvbTCyT4=
> -----END CERTIFICATE-----
> ...
Certificate added.
```

NOTE – Depending on the type of certificate the CA generates (registered 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.

4. **Apply your changes.**

```
>> Certificate 1# apply
Changes applied successfully.
```

If you have used the **`request`** command in the iSD-SSL to generate a CSR, and have specified the same certificate number as the CSR when pasting the contents of the certificate file, your certificate is now fully installed.

If you have obtained a certificate by other means, however, you must also add the corresponding private key.

Using a Copy-and-Paste Operation to Add a Private Key

1. **Type the following command from the Main menu prompt on the iSD-SSL to start adding a private key.**

   ```
   >> Main# cfg/ssl/cert
   Enter certificate number: (1-) <number of the certificate you want to configure>
   >> Certificate 1# key
   Paste the key, press Enter to create a new line, and then type "..."
   (without the quotation marks) to terminate.
   >
   ```

   Make sure you specify the same certificate number as when pasting the certificate.

2. **Copy the contents of your private key file.**

   Locate the file containing your private key. Make sure the key file corresponds with the certificate file you have received from a CA. The public key contained in the certificate works in concert with the related private key when handling SSL transactions.

   Open the key file in a text editor and copy the entire contents. Make sure the selected text includes the “`-----BEGIN RSA PRIVATE KEY-----`” and “`-----END RSA PRIVATE KEY-----`” lines.

3. **Paste the contents of the key file at the command prompt.**

   Now, paste the private key at the command line interface prompt. Press ENTER to create a new row, and then type “`...`” (without the quotation marks). Press ENTER again to complete the installation of the key.

   You may be prompted for a password phrase after having completed the paste operation. The password phrase you are requested to type is the one you specified when creating (or exporting) the private key.

Your screen output should now resemble the following example.

```
>> Certificate 1# key
Paste the key, press Enter to create a new line, and then type "..."
(without the quotation marks) to terminate.
> -----BEGIN RSA PRIVATE KEY-----
> Proc-Type: 4,ENCRYPTED
> DEK-Info: DES-EDE3-CBC,2C60C89FEB57A853
>
> MbbLDYlwdbNfXUGHFm10nfRlI+KTnx2Bdx750EaG8HSVV7KrtnsNF/Fsz1jFvO/j
> nKhZfs4zsVrsstrVlqfP1uatg19VyJSEug1ZcCamH59Dcy+UNocFWCzR56PHpyZK
> GXX66jS+6twYdiXQk58URIudkmGXGTYMvBRuVjV22ZRLyJk41Az5nA6HiDz6GGs6
> vkCaPFGm263KxmXjy/okNgSJl9QTqJfSq7Eh1cIslBReAE9HXGl0Eubb6gVJu+sR
> mGhS/yGx4vMx98wiMjL37gRtXBfDWlu6u0HOPeJxs6fH05fYzmnpwAHj592TDFds
> Ji5pmrY0NhAeXfuG8mF/T9nEz02ZA8iQGJsaUPfkeBxbZS+umY/R65Okwt1k2RN4
> RlFnmRWqvhHMrHzJuegez/806YazHBv74sOg3KgETRH92z5yvwbgFwmffgb+hai0
> RlRtZgQ4A5kSAFYW37KDq6eJBsZ/m3Que1buMbh8tRxdGpo54+bGqu5b12iLanLn
> Rk57ENQGTgzxOD/1RZIJHqObCY7VDLkK7WZM/LPa0k+bTeAysmZa7fu7gvELJF0i
> vszs3nzm7zT1y0mJ0QX9u9eoW8wpASCAdCC2r2LZt8o9+IWLSZWh5UCIr8qFKGiL
> rUIx8coIhxSpx/PqEV8KhSRV+0taq0N7pJa3TLmO3o80t5966VSFKc3Y35fx9Yk8
> G+RlSzo4CxooY4bCKsfchnJ957SJx5vUyh6jjztnuU4iAfeTVCUdF0LXd+NlQ7T7
> IMFsjjx9SZuuHPZTF0KD/WYLx7FfIFIBHDumu6scraYZOaWaJKI5Pw==
> -----END RSA PRIVATE KEY-----
> ...
Enter pass phrase:
Key added
```

4. **Apply your changes.**

```
>> Certificate 1# apply
Changes applied successfully.
```

Your certificate and private key is now fully installed and ready to be taken into use by a virtual SSL server. To view information about configured certificates and SSL servers, type the command **`/cfg/ssl/cur`** and press ENTER.

Using TFTP to Add Certificates and Keys

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

1. **Put the certificate file and key file on your TFTP server.**

NOTE – You may arrange to include your private key in the certificate file. When the specified certificate file is retrieved from the TFTP server, the iSD-SSL software will analyze the contents and automatically add the private key, if present (the screen output displays "Certificate added" and "Key added" in this case). If the private key is included, you do not have to perform step 3.

---

2. **Initiate the process of adding a certificate using TFTP.**

Type the command **`/cfg/ssl/cert`** and press ENTER. Specify an unused certificate index number, and then type the command **`tftpcert`**.

```
>> Main# cfg/ssl/cert
Enter certificate number: (1-) <number of the certificate you want to configure>
>> Certificate 1# tftpcert
Enter host name or IP address of TFTP server: <TFTP server>
Enter name of file on TFTP server: <filename.crt>
Retrieving filename.crt from TFTP server
```

Make sure to specify a certificate number not in use by an existing certificate. To view information about configured certificates, type the command **`/cfg/ssl/cur`** and press ENTER.

Provided the operation was successful, your screen output should resemble the following example:

```
>> Certificate 1# tftpcert
Enter host name or IP address of TFTP server: 192.168.128.58
Enter name of file on TFTP server: VIP_1.crt
Retrieving VIP_1.crt from 192.168.128.58
Certificate added.
```

3. **Add your private key using TFTP.**

   Type the command **`tftpkey`** and press ENTER. Provide the required information. You may be prompted for a password phrase (if specified when creating or exporting the private key).

   ```
   >> Certificate 1# tftpkey
   Enter host of IP address of TFTP server: <TFTP server>
   Enter name of file on TFTP server: <filename.key>
   Retrieving filename.key from TFTP server
   Enter pass phrase:
   ```

   Provided the operation was successful, your screen output should resemble the following example:

   ```
   >> Certificate 1# tftpkey
   Enter host of IP address of TFTP server: 192.168.128.58
   Enter name of file on TFTP server: VIP_1.key
   Retrieving VIP_1.key from 192.168.128.58
   Enter pass phrase:
   Key added.
   ```

4. **Apply your changes.**

   ```
   >> Certificate 1# apply
   Changes applied successfully.
   ```

   Your certificate and private key is now fully installed and ready to be taken into use by a virtual SSL server. To view information about configured certificates and SSL servers, type the command **`/cfg/ssl/cur`** and press ENTER.

Importing an Existing Key/Certificate from an Apache Server

You can import an existing key/certificate pair from an Apache server. The iSD-SSL accelerator supports keys created with Apache-SSL, or the Apache interface to OpenSSL.

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 iSD-SSL. For more information, see "Using a Copy-and-Paste Operation to Add Certificates" on page 157.**

Apache-SSL Certificate

1. **Change directory to** `$APACHESSLROOT/conf/httpd.comf` **for location of the** `*.cert` **file**
2. **Apache-SSL, defaults to** `$APACHESSLROOT/certs/*.cert`
3. **Copy and paste the certificate file into the iSD-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 iSD-SSL. For more information, see "Using a Copy-and-Paste Operation to Add Certificates" on page 157.**

OpenSSL Certificate (Apache interface)

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

Configuring a Virtual SSL Server for Client Authentication

In each iSD-SSL cluster, you can create up to 256 virtual SSL servers. Each virtual SSL server is mapped to a virtual server on the Web switch, and can handle a specific service such as HTTPS, SMTPS, IMAPS, or POP3S. Each virtual SSL server is configured to use a server certificate to authenticate itself towards the clients. Besides, a virtual SSL server can be configured to require client certificates in order to authenticate clients before granting access to the requested service.

When a virtual SSL server is set to require client certificates, a CertificateRequest message is sent from the server to the client during the SSL handshake. The client responds by sending its public key certificate in a Certificate message. After that, the client will send a CertificateVerify message to the server. The CertificateVerify message is signed by using the client’s private key, and contains important information about the SSL session known to both the client and the server. Upon receiving the CertificateVerify message, the virtual SSL server will use the public key from the client certificate to authenticate the client’s identity.

The virtual SSL server will also check if the certificate the client presents is signed by an accepted certificate authority. Accepted certificate authorities are defined by the CA certificates you have specified in the virtual SSL server. The certificate you use for generating client certificates must therefore also be specified as a CA certificate in the virtual SSL server.

The virtual SSL server also checks if the client certificate should be revoked, by comparing the serial number of the presented client certificate with entries in the certificate revocation list.

The following steps demonstrate how to configure a virtual SSL server to require client certificates for authentication purposes.

1. **Display information about current virtual SSL servers.**

```
>> Main# cfg/ssl/cur
```

This command displays information about all certificates and virtual SSL servers on the iSD-SSL, including their current configurations. Based on the information displayed, decide which virtual SSL server to configure for client authentication.

2. Configure the chosen virtual SSL server to require client certificates.

```
>> SSL# server 1
>> Server 1# ssl
>> SSL Settings for Server 1# verify
Current value: none
Certificate verification (none/optional/require): require
```

This requires the client to send its client certificate to the virtual SSL server during the SSL handshake. If the client does not have a certificate, the client will respond with a NoCertificateAlert message. At that point, the session will be terminated.

3. Specify which CA certificates to use for client authentication.

```
>> SSL Settings for Server 1# cacerts
Current value: ""
Enter certificate numbers (separated by comma): <CA certificates by index
                                               number>
```

Specify which CA certificates you want the virtual SSL server to use for authenticating client certificates. Only those client certificates that are issued by a certificate authority whose CA certificate you specify, will be accepted. Note that the CA certificates you specify by index number, first must have been added from the Certificate menu by using the **`cert`** command.

In order to authenticate client certificates issued within your own organization, the server certificate used for generating client certificates must be specified as a CA certificate.

To view information about all certificates currently added, type the command **`/cfg/ssl/cur`** and press ENTER.

4. Apply your settings.

```
>> SSL Settings for Server 1# apply
Changes applied successfully.
```

Generating Client Certificates in the iSD-SSL

Before issuing client certificates, you should establish the means of validating the identities of the users. The credentials users need to present in order to obtain a client certificate may vary, depending on the type of service, the size of your organization etc.

1. **Specify a server certificate by index number, to use for generating a client certificate.**

```
>> Main# cfg/ssl/cert
Enter certificate number: (1-) 1
>> Certificate 1# genclient
The combined length of the following parameters may not exceed 225
bytes.
Country Name (2 letter code):
State or Province Name (full name):
Locality Name (e.g., city):
Organization Name (e.g., company):
Organizational Unit Name (e.g., section):
Common Name (e.g., your name or your server's hostname):
Email Address:
```

In this example certificate number 1 is specified for generating a client certificate. It is actually the private key that corresponds with the public key in the certificate you specify, that is used for signing the client certificate. To view basic information about available certificates, type the command **`/cfg/ssl/cur`** and press ENTER.

NOTE – Only certificates having the basic constraint CA:TRUE can be used for generating client certificates. When generating a client certificate, the iSD-SSL automatically checks that the current certificate has this constraint. To perform this check yourself, type the command **`show`** and look for a line containing the text "X509v3 Basic Constraints:" in the screen output.

2. **When prompted, provide the following information about the subject to include in the client certificate:**

   - Country Name (2 letter code): The ISO code for the country in which the subject resides. With subject is meant the person for whom the client certificate is created.
   - State or Province Name (full name): The full name of the state or province in which the subject resides.
   - Locality Name (e.g., city): The name of the city or town where the subject resides.
   - Organization Name (e.g., company): The registered name of the organization to which the subjects belongs. Do not abbreviate the organization name and do not use the following characters: `< > ~ ! @ # $ % ^ * / \ ( ) ?`
   - Organizational Unit Name (e.g., section): The unit name of the organization to which the subject belongs.
   - Common Name (e.g., the subject’s name): The full name of the subject.
   - E-mail address: The full e-mail address of the subject.

3. **Specify the validity period, key size, and serial number.**

```
>> Certificate 1#
Valid for days [365]:
Key size (512 or 1024) [512]:
Serial number of client certificate [1]:
```

After having provided information about the subject, you are now ready to specify information relating to the client certificate itself.

Decide how many days the client certificate should be valid. By default, each new client certificate is set to be valid for 365 days.

Decide which key size should be used. The default key size is set to 512 bits, which is appropriate in most cases. Note that export versions of MS Internet Explorer 4.x (40-bit encryption) and MS Internet Explorer 5 (56-bit encryption) can not import client certificates with a larger key size than 512.

Assign a serial number to the client certificate, or accept the suggested number. When generating a new client certificate, the lowest available serial number is displayed in square brackets and will be used unless you specify a different number. As you generate more client certificates, the proposed serial number is incremented automatically.

4. **Decide whether to save the client certificate and define a pass phrase.**

```
>> Certificate 1#
Save client certificate (yes/no) [yes]:
Select cert no. to save to [2]:
Enter export pass phrase:
Reconfirm export pass phrase:
Creating new cert 2
Use ’apply’ to save client key and certificate.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5B2BFB839B4A9524

ErcHmgvzyLuaGn9WXrkZgn/EY6CcrgluO7d4fh/a3YuCBFPgiE5NKs7HtqJ6RPfb
K/Uinv7MaRSmRzIIbojOaOk6jZUsP1U7d+60Hy/kgfnMI7mI2oByHFvJ1IfZ5Dfs
SyJFmbMYSfG7MPtobaUjuTedmBw5Vo5JnpmfYqnd0uvMMT4H8HM6PgEHggJctBoJ
iaENDtCEbhaUX6B6+7qzXBpcUx6GJoQ3P8b07YrGhkfY9KWGT4DglKBHJiT4Wgua
+voUZ2WPebSC5XCfR6bnIFykxNrFPWMV+2FwxNs6to6QPY2sARwym8/pK2CQFW5b
mojNTWtW9U9UObAvV1TUCSUauARy3aVAMtY7bi7HX93Yypk5FXFVn75RoTMB7CIZ
jxwL3R7kZFsEmHe/NE4LkiLHRFd+ZxbbRdNC1Zw47qw=
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDyjCCAzOgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBqjELMAkGA1UEBhMCVVMx
FDASBgNVBAgTC09ha2xhZm9ybmlhMRAwDgYDVQQHEwdUZXN0aW5nMRIwEAYDVQQK
EwlUZXN0IEluYy4xEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UEAxMXd3d3LmR1
bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3RlckBkdW1teXNz
bHRlc3RpbmcuY29tMB4XDTAxMDIyNzEyMzAzMFoXDTAyMDIyNzEyMzAzMFowgZQx
CzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0xDjAMBgNVBAcTBUtpc3Rh
MREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9jdTEZMBcGA1UEAxMQd3d3
LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9yYmpvcm5AYmx1ZXRhaWwu
Y29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALNjbwor//Gz3CsugRPJvcw36tm1
09BuZ81g2NTahrXJKKotRb947c7YJgTZYFnlaOHV7tpRUnp5yASCzBHBt0MCAwEA
AaOCAVYwggFSMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgWgMAsGA1UdDwQE
AwIF4DAsBglghkgBhvhCAQ0EHxYdaVNELVNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNh
dGUwHQYDVR0OBBYEFDdbxK9VEsti/nS/1cTxp9eMYVfdMIHXBgNVHSMEgc8wgcyA
FIZ96B3BhM12d8GJl/GrC+Shs5gtoYGwpIGtMIGqMQswCQYDVQQGEwJVUzEUMBIG
A1UECBMLT2FrbGFmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxEjAQBgNVBAoTCVRl
c3QgSW5jLjESMBAGA1UECxMJdGVzdCBkZXB0MSAwHgYDVQQDExd3d3cuZHVtbXlz
c2x0ZXN0aW5nLmNvbTEpMCcGCSqGSIb3DQEJARYadGVzdGVyQGR1bW15c3NsdGVz
dGluZy5jb22CAQAwDQYJKoZIhvcNAQEEBQADgYEAlEIbixeNQqSUIiRJ28ty8vQW
TqpEP7B9dGGqPnGXTQQ5QqjHaaGppYDAUZAceFGWHG94fIS7OtRqX40zrsCO51bn
2kMMz/XVj78Z3/nr+mv4Rm1ZGXmAEhVo2XjvVFChOF74XcMyAz0Qp3UVvTVsFULK
A1qnT20SWno9T8xR0lU=
-----END CERTIFICATE-----
Use ’apply’ to save incremented certificate serial number.
```

You should save the client certificate and assign a certificate index number to it. The lowest available index number available is displayed in square brackets and will be used unless you specify a different number.

The requested pass phrase is a word or code which protects the encrypted key against illegitimate use. When the intended user installs the client certificate into a Web browser or e-mail client, the correct pass phrase is required to unlock the certificate.

By saving the certificate, you can later easily access the certificate by specifying the assigned index number at the `cert` prompt. After having specified the assigned index number, you can use the commands **`export`** or **`tftpexport`** in order to prepare for the transfer of the client certificate to the subject. By typing the command **`/cfg/ssl/cur`** and pressing ENTER, you can view information about all saved certificates.

If you choose not to save the client certificate by assigning an index number to it, you will need to save the private key and the certificate to a file by performing a copy-and-paste operation to a text editor. The private key and the certificate are displayed on screen as soon as you reconfirm the chosen password phrase. The private key and the certificate are combined and saved in the PEM format when using a copy-and-paste operation.

5. **Verify that the certificate you use for generating client certificates is specified as a CA certificate.**

```
>> Main# cfg/ssl/server
Enter virtual server number: (1-) 1
>> Server 1# ssl
>> SSL Settings for Server 1# cacerts
Current value: 1
Enter certificate numbers (separated by comma):
```

In order to successfully validate the client certificate on authentication, you need to verify that the certificate you used for generating the client certificate is also specified as a CA certificate. In the example screen output above, the certificate has already been defined as a CA certificate to use for client authentication (evident by the line `Current value: 1`, where number 1 is the index number of the certificate that was used for generating the client certificates). In most cases, you will arrange for specifying the CA certificate(s) when configuring a virtual SSL server to require client authentication.

If the certificate number representing the certificate you used for generating client certificates is not listed by `Current value`, type the certificate index number and apply your changes.

If the certificate index number is listed by `Current value`, press ENTER and answer **`no`** to the question if you want to clear the list.

6. **Transmit the private key and certificate to the user.**

   Before you transfer the private key and client certificate to the subject, save the key and the certificate to a file by using either the **`export`** command or the **`tftpexport`** command from the Certificate menu. The **`tftpexport`** command is recommended, as this provides you with the option to select the PKCS12 file format (also known as PFX). Most Web browsers accept importing a combined key and certificate file in the PKCS12 format. For more information, see the **`export`** and **`tftpexport`** commands under "Certificate Management Menu" on page 77.

   Transmit the client certificate and the pass phrase protected private key to the user in a secure manner. Never send the password phrase in an e-mail message.

   The user will then need to import the received client certificate into his or her Web browser or e-mail program. For more information about importing certificates, refer to the help system of the destination Web browser or e-mail program.

Managing Revocation of Client Certificates

Certificate revocation lists (CRL) are maintained by certificate authorities to recall client certificates that are no longer considered trustworthy. The reasons for this can be that the client certificate was issued by mistake, or that the subject accidentally has revealed the private key.

By keeping a certificate revocation list on your SSL server, client certificates sent to the server are checked against the CRL. If a match is found, the SSL session is terminated. This mode of operation requires, first of all, that you have configured the virtual SSL server to always require client certificates. You must also regularly check with the certificate authorities you trust for their latest CRLs.

Moreover, if you take on the role of a certificate authority by issuing your own client certificates, you will also need to maintain your own certificate revocation lists. This can be done by listing the serial numbers of the client certificates you want to revoke in an ASCII file. You may also specify the serial number of a particular client certificate directly in the command line interface by using the **`add`** command in the Revocation menu.

Revoking Client Certificates Issued by an External CA

1. **Specify the CA certificate, to which you want to add a CRL.**

```
>> Main# cfg/ssl/cert
Enter certificate number: (1-) 1 (example)
>> Certificate 1# revoke
```

The certificate you specify must be a CA certificate from the same certificate authority that published the CRL you are about to add. To view basic information about available certificates, use the command **`/cfg/ssl/cur`** and press ENTER.

2. **Download and add a CRL from a TFTP server.**

```
>> Revocation for Cert 1# tftp
Enter host or IP address of TFTP server: 192.168.128.20 (example)
Enter name of file on TFTP server (PEM, DER or ASCII format): crl.der
Retrieving crl.der from 192.168.128.20
Received 12628 bytes in 0.1 seconds

Certificate revocation list found in der format
Revocation list added.
Use 'apply' to activate changes.
```

Specify the host name or IP address of the TFTP server, and provide the file name of the CRL. The CRL is retrieved and added to Certificate 1 (used as an example).

3. **Apply your changes.**

```
>> Revocation for Cert 1# apply
Changes applied successfully.
```

Revoking Client Certificates Issued Within Your own Organization

1. **Specify the CA certificate, to which you want to add a CRL.**

```
>> Main# cfg/ssl/cert
Enter certificate number: (1-) 1 (example)
>> Certificate 1# revoke
```

Specify the certificate number that represents the CA certificate of the certificate used for generating the client certificate you want to revoke. To view basic information about available certificates, use the command **`/cfg/ssl/cur`** and press ENTER.

2. **Add the serial number of a specific client certificate to revoke.**

```
>> Revocation for Cert 1# add
Enter serial number to revoke:
```

Repeat this step for each serial number you want to add. To show the serial number (along with subject information) for a saved client certificate, use the command **`/cfg/ssl/cur`** and press ENTER.

Or, download and add your own CRL in ASCII format from a remote machine.

```
>> Revocation for Cert 1# tftp
Enter host or IP address of TFTP server: 192.168.128.20 (example)
Enter name of file on TFTP server (PEM, DER or ASCII format):
crl.ascii
Retrieving crl.ascii from 192.168.128.20
Received 12628 bytes in 0.1 seconds

Certificate revocation list found in ascii format
Revocation list added.
Use 'apply' to activate changes.
```

If you have added serial numbers for particular client certificates by using the **`add`** command prior to using the **`tftp`** command, you will be asked if you want to merge those serial numbers to the CRL in ASCII format. If the CRL does not already include those serial numbers, choose to merge them. However, make sure that you update the original CRL with the merged serial numbers before the next download, as you will otherwise lose them. For more information about how to build your own CRL, see "Creating Your Own Certificate Revocation List" on page 173.

3. **Verify that the serial numbers of the client certificates you want to revoke have been added.**

```
>> Revocation for Cert 1# list
Revoked certificates:
```

4. **Apply your changes.**

```
>> Revocation for Cert 1# apply
Changes applied successfully.
```

Creating Your Own Certificate Revocation List

You can easily build and manage certificate revocation lists for client certificates issued within your own organization. The CRL can then be added by using TFTP. For more information about how to accomplish this, see “Revoking Client Certificates Issued Within Your own Organization” on page 172.

1. **Open a text editor and create a new file.**
2. **Decide if you want to add serial numbers in decimal form, or in hexadecimal form.**
3. If you choose to add serial numbers for client certificates to revoke in decimal form, add a paragraph in the text document that reads:

```
ASCII revocation
```

Or, if you choose to add serial numbers in hexadecimal form, add a paragraph in the text document that reads:

```
HEX ASCII revocation
```

NOTE – You can add comments to a CRL ASCII file by preceeding your comments with the # character. Each new line of comments must begin with the # character. Comments can be used for providing information about the date of issue or last update, for example. You can cancel the revocation of a client certificate by inserting the # character at the beginning of the line containing the desired serial number.

4. **Add the serial numbers of the client certificates you want to revoke.**

For a CRL in decimal format, simply list the serial numbers below the ASCII revocation paragraph. For example:

```
# CRL for CA certificate 1
# Issued first: 2001-01-01
# Last update: 2001-02-01

ASCII revocation

500
501
590
```

Or, for a CRL in hexadecimal format, list the serial numbers by their hexadecimal values below the HEX ASCII revocation paragraph. For example:

```
# CRL for CA certificate 1
# Issued first: 2001-01-01
# Last update: 2001-02-01

HEX ASCII revocation

1F4
1F5
24E
```

5. **Save the file, and upload it to a TFTP server that can be accessed from your iSD-SSL(s).**

CHAPTER 10

Using the Quick Server Setup Wizard

The Quick Server Setup Wizard provides a way to quickly configure and enable a working virtual SSL server for the service you specify. Before using the Quick Server Setup Wizard, you must have obtained a server certificate in the PEM format that the virtual SSL server can use.

Note that even if the wizard provides an easy way to create and configure a virtual SSL server, you still must configure the Web switch accordingly. The extent of configuration changes to filters etc. needed on the Web switch depend on your current setup and services. For detailed examples of virtual SSL server implementations in conjunction with an Alteon Web switch, see “iSD-SSL Sample Applications” on page 117.

1. **Start the Quick Server Setup Wizard and define a server name.**

```
>> Main# cfg/ssl/quick
Name of server: HTTPS Offload
```

Define a name for the virtual SSL server you are creating. The name is mainly for your own reference, and could indicate the service for which the virtual SSL server is created, or the virtual server on the Web switch to which you bind the virtual SSL server. In this example, the name **`HTTPS Offload`** is used.

2. **Specify the IP address of an existing virtual server.**

```
IP address of SSL server: 192.168.128.100
```

Specify the IP address of an existing virtual server (on the Web switch) in order to bind the virtual SSL server to the desired virtual server.

3. Set the listen TCP port.

```
Listen port of SSL server [443]:
```

In this example, the virtual SSL server is created for HTTPS offload purposes and the listen TCP port suggested by the wizard ([443]) need not be changed. Simply press ENTER to preserve the TCP port value. However, if you want to set up the virtual SSL server to handle IMAPS for example, you would set the listen TCP port to 993.

4. Define the SSL server type.

```
Type of server (http/generic) [http]:
```

Again, as the virtual SSL server is created for HTTPS offload purposes in this example, the server type suggested by the wizard ([http]) need not be changed. Simply press ENTER to preserve the server type.

NOTE – When the SSL server type is set to HTTP, the virtual SSL server is automatically configured to use built-in features such as automatic SSL redirect and the adding of extra headers. For more information about these advanced HTTP-specific features, see “SSL Server HTTP Settings Menu” on page 89.

5. Set the real server IP address.

```
Real server IP [192.168.128.100]:
```

The real server IP address defines to which server the virtual SSL server should connect when it initiates requests. Since the requested real server IP address usually corresponds to the virtual server IP address you specified in step number 1, the Quick Server Setup wizard suggests this IP address.

Press ENTER to accept the suggested real server IP address.

6. **Set the real server TCP port.**

```
Real server port [81]:
```

The real server port defines the TCP port to which the virtual SSL server connects. When setting up a virtual SSL server for HTTPS offload purposes, the default real server port is 81. The virtual SSL server will use this port to send and receive decrypted HTTP information to and from the real Web servers.

NOTE – The real Web servers must also be configured to listen for iSD-SSL traffic on port 81. For security reasons it is also important to define a filter on the Web switch that blocks all incoming client traffic destined for port 81.

7. **Paste the certificate you want the virtual SSL server to use.**

```
Paste the certificate, press Enter to create a new line,
and then type "..." (without the quotation marks)
to terminate.
>
```

Locate the certificate you want to use, make sure the certificate file is in the PEM format (which combines both the private key and the certificate in the same file), open the file in a text editor and copy the entire content. Make sure your text selection includes the "-----BEGIN PRIVATE KEY-----" and "-----END CERTIFICATE-----" lines.

Now, paste the content at the command line interface prompt, press ENTER to create a new empty line, and then type "`...`" (without the quotation marks). Press ENTER again to complete the installation of the certificate. If the private key has been password protected, you will be asked to provide the correct pass phrase.

8. Your screen output should now resemble the following example:

```
Paste the certificate, press Enter to create a new line,
and then type "..." (without the quotation marks)
to terminate.
> -----BEGIN RSA PRIVATE KEY-----
> Proc-Type: 4,ENCRYPTED
> DEK-Info: DES-EDE3-CBC,A869F45E9CC45F52
>
> 7Px2H7TG/9omI8juY96FKTY3+8ID6J2KGMMutWBT7ug6dVzKD+K0yd6Lza20xivk
> JVWXU7+ry448vcHVw2ApSb3qvlg7FRdN7oFYutZZESozlZrZzbKDxv4LH/lqW2x+
> Ngb2qjFsP6jKtlc4TNkdFLYkzVxXC6h+hSdG7C0H4taylxoP1RdY8SZwoT0PLaC6
> 8aZGCdfYZ+RsVDoGeP3QyenlXTrMls/d2+SWOG4xjEAfEHunI/z7W1lIBmipmvnz
> wjbD2PNmzx2k8JuYA4gclbAfJYKoeT1O4N9tzJrv0GLkG1Hq8XAvHXzs4W8WUfln
> sCmu1kKDGCfl6EOCt1le4oDzK8EuBZF2y0ZmQYEXuf9oFUN3xiu/rShzEPFCoADv
> a8ZV+jvFH1j/ozvTmRXaNz1I8dHkbrFz8ViELfqXr6k=
> -----END RSA PRIVATE KEY-----
>
> -----BEGIN CERTIFICATE-----
> MIICXjCCAgigAwIBAgIBADANBgkqhkiG9w0BAQQFADBbMQswCQYDVQQGEwJTRTEK
> MAgGA1UECBMBZzEKMAgGA1UEBxMBZzEKMAgGA1UEChMBZzEKMAgGA1UECxMBZzEK
> MAgGA1UEAxMBZzEQMA4GCSqGSIb3DQEJARYBZzAeFw0wMDExMTQxNzQ0NTBaFw0w
> MTExMTQxNzQ0NTBaMFsxCzAJBgNVBAYTAlNFMQowCAYDVQQIEwFnMQowCAYDVQQH
> EwFnMQowCAYDVQQKEwFnMQowCAYDVQQLEwFnMQowCAYDVQQDEwFnMRAwDgYJKoZI
> hvcNAQkBFgFnMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMM1w/CGs5lLh3Thrns6
> HW2s8YT0ujIq3chDHppNSQQskeM4EN4GIRbBmPmuMmqFzmC1CVARm4wJQu+/Xnnv
> s6sCAwEAAaOBtjCBszAdBgNVHQ4EFgQUMeRJwoUki4m4moHPCgvhbNgCgacwgYMG
> A1UdIwR8MHqAFDHkScKFJIuJuJqBzwoL4WzYAoGnoV+kXTBbMQswCQYDVQQGEwJT
> RTEKMAgGA1UECBMBZzEKMAgGA1UEBxMBZzEKMAgGA1UEChMBZzEKMAgGA1UECxMB
> ZzEKMAgGA1UEAxMBZzEQMA4GCSqGSIb3DQEJARYBZ4IBADAMBgNVHRMEBTADAQH/
> MA0GCSqGSIb3DQEBBAUAA0EALUQqocsBBMd7Y9b2PnMoc/U9yzcunxH3cwSK+oLE
> NuykQRO72vie+n1uztXTJxugTnFO9MGoIxEy19zFklUrLQ==
> -----END CERTIFICATE-----
> ...
Enter pass phrase:
Do you require chain certificates (yes/no) [no]:
```

9. **If the server certificate you just added is a chain certificate, add your chain certificate(s) as well.**

   You need to repeat the pasting of chain certificates until the root CA certificate has been added. This constructs the server certificate chain, which is sent to the client’s browser in addition to the server certificate.

   When you have added your root CA certificate, answer **no** to the question if you require (additional) chain certificates. The following message is then displayed:

   ```
   Do you require more chain certificates (yes/no) [no]: no
   Creating new server 2
   Creating new cert 2
   Server certificate added as cert 2
   Creating new cert 3
   Adding chain certificate as cert 3
   Use apply to activate the new server.
   ```

10. **Apply your settings.**

    ```
    >> SSL# apply
    ```

11. **Verify your settings.**

    ```
    >> SSL# cur
    ```

    According to the example above, information relating to the added virtual SSL server and added certificates can be reviewed under the following main entries in the screen output, after you have issued the `cur` command:

    - Certificate 2
    - Certificate 3
    - Server 2

CHAPTER 11

Configuring the iSD-SSL to Rewrite Client Requests

If the client’s web browser is not capable of meeting the cipher list requirement you have specified for a virtual SSL server on the iSD-SSL, you can enable the rewrite functionality in order to let the Web server display a customized error message. Without this functionality, the SSL session between the client and the iSD-SSL would simply be terminated during the SSL handshake.

Setting up Rewrite of Weak Cipher Client Requests

This example assumes that you already have configured a virtual SSL server for the HTTPS service, as described in the Web Server Accelerator example on page 118.

1. **Decide which virtual SSL server to configure.**

```
>> Main# cfg/ssl
>> SSL# cur
```

View the displayed information about certificates and virtual SSL servers. If you have configured more than one virtual SSL server, identify the server used for HTTPS by verifying that the Listen port value is set to 443 (HTTPS). In this example virtual SSL server 1 is used as an example for the configuration changes.

2. **Examine the current settings for the chosen virtual SSL server.**

```
>> SSL# server
Enter virtual server number: (1-) 1 (example)
>> Server 1# cur
```

Examine the settings and make sure that the virtual SSL server is enabled. Take special notice of the SSL settings and the current cipher list, which denotes the cipher strength. If you have not modified the cipher list, it should correspond to the default value of `ALL`.

3. **Set the SSL server type to HTTP.**

```
>> Server 1# type
Current value: generic
Type (generic/http): http
```

In order to make use of high-level HTTP capabilities, such as rewriting client requests, the virtual SSL server type needs to be changed to **`http`**. Also, without changing the type to **`http`**, the HTTP Settings menu and Rewrite menu are not even activated.

4. **Access the HTTP menu and the Rewrite menu, then enable the rewrite functionality.**

```
>> Server 1# http
>> HTTP Settings for Server 1# rewrite
>> Rewrite Menu for Server 1# rewrite
Current value: off
Enable rewrite (on/off): on
```

5. **Specify which cipher list to accept.**

```
>> Rewrite Menu for Server 1# ciphers
Current value: HIGH
Enter cipher list: RC4:ALL:!EXPORT:!DH
```

Specify the cipher list (in uppercase letters) that you actually require here, or accept the default rewrite cipher list (`HIGH`). The cipher strength that you actually require must always be *higher* than the cipher strength provided by the cipher list specified under the SSL Settings menu (you viewed these settings in step 2). This way, clients using a Web browser that does not meet the actual cipher strength requirements can still establish an SSL session and get a customized error message from the Web server (or a default error message from the iSD-SSL), even if the actual requirements are not met.

The rewrite function is only triggered when a client browser can perform the (lower) cipher strength specified under the SSL Settings menu, but is unable to perform the (higher) cipher strength you specify in this step. When both cipher requirements are met, the SSL session is established transparently without the involvement of the rewrite function.

Again, verify that the cipher list you specify in this step provides higher cipher strength than the cipher list you took note of in step 2. For more information about ciphers, see "Supported Ciphers" on page 201. If you find that you need to change the cipher list specified under the SSL Settings menu, use the command **/cfg/ssl/server**, specify the desired virtual SSL server, and then type the command **ssl/ciphers**.

6. **Configure the SSL server to let the Web server handle the client response.**

```
>> Rewrite Menu for Server 1# response
Current value: iSD
Enter the source of response (iSD/WebServer): WebServer
```

In this example, configure the SSL server to let the Web server handle the response sent back to the client browser when the rewrite function is triggered. This configuration also requires specifying a valid URI, pointing to a resource on the Web server (described in the next step).

If you choose to let the iSD-SSL handle the response, it returns a predefined error message to the client browser if the required cipher strength is not met. An example of such a predefined error message emanating from the iSD-SSL can be:

```
www.foo.com requires stronger cryptography support of your browser.
   Your browser used TLSv1/SSLv3, with the cipher suite RC4-MD5,
          which is not one of the accepted ones: NULL-SHA
```

7. **Specify the URI to add when rewriting the client request.**

```
>> Rewrite Menu for Server 1# URI
Current value: /cgi-bin/weakcipher
Enter the URI address (WebServer response only): /cipheralert.asp
```

Specify a URI pointing to a resource on the Web server to which the client made its initial request. The URI can point to a static HTML page, or to a server-side script generating a dynamic error message. A dynamic error message can be based on the session specific information that the rewrite function automatically adds to the modified request passed on to the Web server.

If you specify **`MEDIUM`** as the cipher list (used only as an example) and **`/cipheralert.asp`** for the URI, the rewritten client request sent on to the Web server would look similar to this:

```
"GET /cipheralert.asp?c=TLSv1/SSLv3:RC4-MD5&cs=MEDIUM HTTP/1.0"
```

Where *c* stands for client, and *cs* stands for (required) cipher suite.

8. **Apply your settings.**

```
>> Rewrite Menu for Server 1# apply
Changes applied successfully.
```

CHAPTER 12
Using the iSD-SSL as a Web Server Accelerator

The following example configures the iSD-SSL to be used as a stand-alone Web server accelerator, without requiring any interoperability with a Web switch. The example configuration can be used in a network environment with low traffic flows, and where there is no demand for the redundancy, scalability, and advanced load balancing features offered by a Web switch.

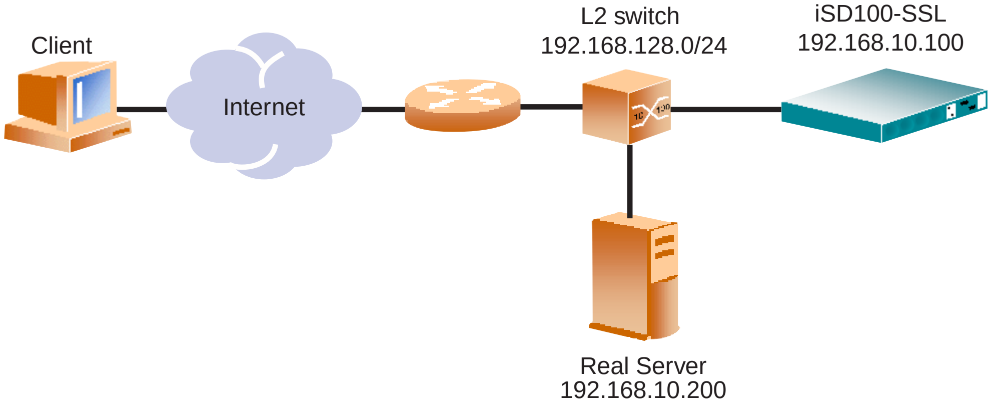


Figure 12-1 Sample Web Server Accelerator Network Using a Stand-Alone iSD-SSL

Initial Setup

First do the initial setup of the iSD-SSL as described in Chapter 3, "Initial Setup'' using the IP address shown in Figure 12-1. Then connect to the iSD-SSL to add a certificate.

Add a Server Certificate

This step presumes that you have a server certificate, signed by a certificate authority (CA), and a private key. The process for obtaining the required certificate files is covered in "Generating and Submitting a CSR Using the CLI" on page 152."

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

```
# /cfg/ssl/cert
Enter certificate number: (1-) 1
Creating Certificate 1
>> Certificate 1# cert
Paste the certificate, press Enter to create a new line, and then
type "..."(without the quotation marks) to terminate.
```

The example above assumes that the certificate signing request (CSR) was generated from certificate number 1, which implies that the private key that corresponds to the public key in the certificate is already in place.

When prompted for the certificate, follow the instructions. Use Notepad or any other text editor to display the certificate. Then copy and paste the text of the certificate into the terminal window. For more detailed information about how to add certificates and keys to the iSD-SSL, see "Adding Certificates to the iSD-SSL" on page 156.

Important—*Once you have pasted the entire contents of the certificate file, press ENTER to create a new empty line and then type three periods (`...`). Press ENTER again to complete the installation of the certificate.*

NOTE – Under Microsoft Windows, HyperTerminal may be slow to complete the copy-and-paste operation.

Configure the Virtual SSL Server Parameters

Connect via Telnet or SSH to the management IP address (MIP) of the iSD-SSL.

1. **Create a virtual SSL server.**

```
# /cfg/ssl/server
Enter virtual server number: (1-) 1
Creating new server 1
>> Server 1#
```

This step creates a new virtual SSL server on the iSD-SSL. Each virtual SSL server listens to a specific TCP port, and is mapped to a virtual server IP address.

2. **Define a name for virtual SSL server 1.**

```
>> Server 1# name
Current value: ""
Enter new SSL server name: HTTPS
```

This step lets you specify a name, by which you can identify SSL server 1. The name you specify is mainly intended for your own reference, and is not critical for the configuration itself. As the example above suggests, the name can indicate the service for which the virtual SSL server is created.

3. **Disable transparent proxy mode.**

```
>> Server 1# proxy
Current value: on
Proxy mode (on/off): off
```

Transparent proxy mode is currently only supported when the iSD-SSL is used together with a Web switch configured with the appropriate filters and load balancing algorithm. For a Web server accelerator configuration example that includes using an Alteon Web switch, see "Web Server Accelerator" on page 118.

4. **Set the listen TCP port for SSL server 1.**

```
>> Server 1# port
>> Current value: 443 (https)
>> Enter listen port number: 443
```

Enter the listen port number 443, which is the default value used for HTTPS connections.

5. **Connect the virtual SSL server to a Virtual Server IP address.**

```
>> Server 1# vip
Current value: <not set>
Enter IP address: 192.168.10.100
```

This step creates a binding between virtual SSL Server 1 and the listen IP address (the virtual server IP address). Normally, one or more virtual server IP addresses are defined on a Web switch, and the virtual SSL server is then mapped to one of these virtual server IP addresses. However, since no Web switch is involved in this stand-alone configuration example, the virtual server IP address is set to the IP address of the iSD-SSL itself.

6. **Set the Real Server IP address to which SSL Server 1 should connect when initiating requests.**

```
>> Server 1# rip
Current value: 0.0.0.0
Enter IP address to connect to: 192.168.10.200
```

This step instructs the iSD-SSL to initiate requests to the real Web server.

7. **Set the server port to which SSL server 1 should connect when initiating requests.**

```
>> Server 1# rport
Current value: 0 [81]
Enter port to connect to: 80
```

When using the iSD-SSL together with a Web switch for Web server accelerating purposes, the **`rport`** value is normally set to TCP port 81. In that case, normal HTTP traffic uses TCP port 80, while HTTPS requests are redirected to the iSD-SSL(s) by the Web switch. The iSD-SSL(s) then use TCP port 81 to send and receive decrypted HTTP information to and from the real Web servers (via the Web switch).

When using the iSD-SSL as a stand-alone device, however, you are restricted to using HTTPS for all requests to the Web server. Therefore, you might just as well use the standard TCP port 80, which does not require you to reconfigure the real Web server.

8. Specify the certificate to be used by SSL Server 1.

```
>> Server 1# ssl
>> SSL Settings for server 1# cert
Current value: <not set>
Enter certificate number: (1-) 1
```

You are prompted to type the index number of an existing certificate. To view all certificates currently added to the iSD-SSL by index number and name, use the command **`/cfg/ssl/cur`**. For more information about how to add a certificate, see "Adding Certificates to the iSD-SSL" on page 156.

NOTE – If the certificate you specify is a chained certificate, you need to first add the CA certificates up to and including the root CA certificate, and then specify the CA certificate chain of the server certificate. For more information on how to construct the server certificate chain, see the **`cachain`** command under "SSL Server Settings Menu" on page 86.

---

9. Apply the changes.

```
>> SSL Settings for Server 1# apply
Changes applied successfully.
```

CHAPTER 13
Troubleshooting the iSD-SSL

The iSD-SSL is built to be easily installed. However, in the unlikely event that it cannot be installed properly, this chapter provides troubleshooting tips for the following problems:

- The iSD-SSL does not boot.
- No connection can be established via the console port.
- Cannot connect to the iSD-SSL via Telnet or SSH.
- Cannot ad the iSD-SSL to an existing cluster.
- The iSD-SSL stops responding.
- A user password is lost.

The chapter also provides a section on performing system diagnostics.

The iSD-SSL Does Not Boot

If nothing at all seem to happen when you switch on the iSD-SSL it may have been damaged during transport. Things to check:

Q: Have you connected the power to the iSD-SSL?

If not, connect the power cord of the iSD-SSL to a power source. Also, make sure the power source really provides enough voltage.

Q: Have you switched on the iSD-SSL?

If not, turn on the iSD-SSL.

Q: When switching on the iSD-SSL, can you hear any noise (e.g. from the built-in fan)?

If not, the iSD-SSL's power supply is probably broken. Replace the iSD-SSL.

Q: Can you see boot messages but not the console prompt?

Refer to “Connecting a Terminal to the iSD-SSL” on page 192.

If none of the suggested problems applies to you, contact Alteon support. See “Contacting Alteon WebSystems” on page 16 for details.

Connecting a Terminal to the iSD-SSL

The iSD-SSL has a console port for system diagnostics and configuration. This chapter explains how to connect a terminal to the console port.

To establish a console (DCE) connection with an Alteon iSD-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:

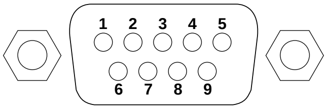
Table 13-1 Console Configuration Parameters

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

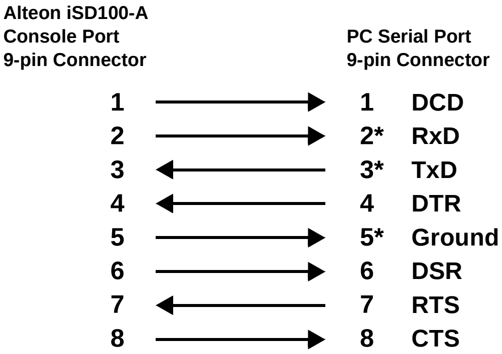
- Console Cable (shipped with the iSD-SSL)

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

Table 13-2 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

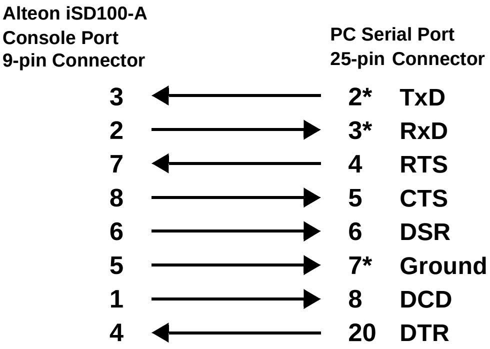
The following figures show the pin assignments for the console to use to configure serial cables to terminal connectors with 9-pin or 25-pin connectors.



Alteon iSD100-A Console Port 9-pin Connector		PC Serial Port 9-pin Connector	
1	→	1	DCD
2	→	2*	RxD
3	←	3*	TxD
4	←	4	DTR
5	→	5*	Ground
6	→	6	DSR
7	←	7	RTS
8	→	8	CTS

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

Figure 13-1 9-pin to 9-pin Connector Pin Assignments



Alteon iSD100-A Console Port 9-pin Connector		PC Serial Port 25-pin Connector	
3	←	2*	TxD
2	→	3*	RxD
7	←	4	RTS
8	→	5	CTS
6	→	6	DSR
5	→	7*	Ground
1	→	8	DCD
4	←	20	DTR

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

Figure 13-2 9-pin to 25-pin Connector Pin Assignments

NOTE – Console cables are not intended for permanent installation and should be disconnected from the console port after configuring the iSD-SSL.

Establishing a Console Connection

1. **Connect the terminal to the console port using the serial cable that is included with your iSD-SSL.**
2. **Power on the terminal.**
3. **To establish the connection, press ENTER on your terminal.**

   You should now see the login prompt as explained in "Installing a Single iSD-SSL" on page 35.

Cannot Connect via Telnet or SSH

It is important that the IP addresses of the iSD-SSL are configured correctly and that they are reachable from where you try to connect to the iSD-SSL.

Q: Can you ping the iSD-SSL?

If not, you have either not configured the correct IP addresses on the iSD-SSL, or you have a routing problem. Try to run **`traceroute`**, **`tcpdump`** or some other network analysis tool to locate the problem. Also, make sure you ping the real IP address of the iSD-SSL, not the management IP (MIP) of the cluster in which the iSD-SSL may be a member.

Q: You can ping the iSD-SSL, but not connect using Telnet or SSH?

Try to run some network analysis tool to really make sure the traffic enters the iSD-SSL.

If this does not help you to solve the problem, contact Alteon support. See "Contacting Alteon WebSystems" on page 16.

Cannot add an iSD-SSL to a Cluster

When trying to add an iSD-SSL to a cluster by selecting **`join`** in the Setup menu, you may receive an error message stating that the system is running an incompatible software version. The incompatible software version referred to in the error message is the software that is running on the iSD-SSL you are trying to join. This error message is displayed whenever the iSD-SSL you are trying to join has a different software version from the iSD-SSL(s) in the cluster. In this situation you need to do one of the following:

- Make sure the software version on the iSD-SSL you are trying to add is the same version as on the iSD-SSL(s) in the cluster. You can verify the current software version by using the command **`/boot/cur`**, where the active version is indicated as `permanent`. Adjusting the software version implies either an upgrade to a newer software version, or reverting to an older software version. In either case you will need to perform the steps described in "Reinstalling the iSD-SSL Software" on page 38. After having adjusted the software version, log in as *admin* user and select **`join`** from the Setup menu.
- Upgrade the software version running on the iSD-SSL(s) in the cluster to the same version as running on the iSD-SSL you want to add. Provided the difference between the software versions is limited (for example: version 2.0 is running in the cluster, but version 2.0.1 or version 2.1 is installed on the iSD-SSL you want to add), perform the steps described in "Performing Minor/Major Release Upgrades" on page 42. Then add the iSD-SSL by selecting **`join`** from the Setup menu.

  If software version 1.x is running in the cluster, and software version 2.x is installed on the iSD-SSL you want to join, perform the steps described in "Upgrading iSD-SSLs from Software Version 1.0 to Software Version 2.0" on page 46. If there is still a difference in software versions after this, you need to adjust the software version on the iSD-SSL you want to add as well. After having upgraded the software version in the cluster, log in to the iSD-SSL you want to add as *admin* and select **`join`** from the Setup menu.

The iSD-SSL Stops Responding

Telnet or SSH Connection to the Management IP Address

When you are connected to a cluster of iSD-SSLs via a Telnet or SSH connection to the Management IP address, your connection to the cluster can be maintained as long as at least one master iSD-SSL in the cluster is up and running. However, if the particular iSD-SSL that currently is in control of the Management IP stops responding while you are connected, you need to close down your Telnet or SSH connection and reconnect to the Management IP address.

After doing so, you can view the operational status of all iSD-SSLs in the cluster by using the command **`/info/isdlist`**. If you find that one of the iSD-SSL's operational status is indicated as `down`, you can reboot that machine by pressing the Reset button on the front panel. Insert a straightened paperclip through the hole labeled RESET, and press the Reset button gently. Log in as the Administrator user when the login prompt appears and check the operational status again.

Console Connection

If you are connected to a particular iSD-SSL via a console connection, and that iSD-SSL stops responding, you should first try pressing the key combination CTRL, ^. This will take you back to the login prompt. Log in as the Administrator user and check the operational status of the iSD-SSL. Use the command **`/info/isdlist`** and see if the operational status is indicated as `up`. If the operational status is `up`, the iSD-SSL should continue to process SSL traffic without the need of a reboot.

If the operational status of the iSD-SSL is indicated as `down`, try rebooting the iSD-SSL by using the command **`/boot/reboot`**. You will be asked to confirm your action before the actual reboot is performed. Log in as the Administrator user and check if the operational status of the iSD-SSL now is indicated as `up`.

If the operational status of the iSD-SSL still is indicated as `down`, reboot the iSD-SSL by pressing the Reset button. Insert a straightened paperclip through the hole labeled RESET on the front panel, and press the Reset button gently. Log in as the Administrator user when the login prompt appears.

A User Password is Lost

Administrator User Password

If you have lost the Administrator user password there is only one way to regain access to the iSD-SSL as the Administrator user: reinstalling the software via a console connection as the Boot user.

For more information, see "Reinstalling the iSD-SSL Software" on page 38.

Operator User Password

In case you have lost the Operator user password, log in as the Administrator user and define a new Operator user password. Only the Administrator user can change the Operator user password.

For more information, see the **`operpw`** command under "User Password Menu" on page 101.

Root User Password

If you have lost the Root user password, log in as the Administrator user and define a new Root user password. Only the Administrator user can change the Operator password. For more information, see the **`rootpw`** command under "User Password Menu" on page 101.

Boot User Password

The default Boot user password cannot be changed, and can therefore never really be "lost". If you have forgotten the Boot user password, see "Accessing the iSD-SSL" on page 55.

If the Boot user password could be changed but you had lost both the Administrator password and the Boot user password, the iSD100-SSL would be rendered completely inaccessible to all users except the Operator, whose access level does not permit any changes being made to the configuration of the iSD-SSL.

The fact that the Boot user password cannot be changed should not imply a security issue, since the Boot user can only access the iSD-SSL via a console connection using a serial cable, and the iSD-SSL presumably is set up in a server room with restricted access.

System Diagnostics

A few system diagnostics can be performed on the iSD-SSL.

Installed Certificates and Virtual SSL Servers

To view the currently installed certificates and SSL servers, type the following command:

```
/cfg/ssl/cur
```

The screen output also provides information about which certificate is used by which SSL server.

To view detailed information for a specific certificate, access the Certificate menu by typing the following commands:

```
/cfg/ssl/cert
Enter certificate number: (1-) <certificate number by index>
>> Certificate 1# show
```

Network Diagnostics

To check various network settings for a specific iSD-SSL, access the iSD Host menu by typing the following commands:

```
/cfg/sys/host
Enter host number: (1-) <iSD host by index number>
>> iSD Host 1# cur
```

The screen output provides information about the type of iSD (master or slave), IP address, network mask, and gateway address for the iSD-SSL you have specified (by host number).

To check general network settings related to the cluster to which you have connected, type the following command:

```
/cfg/sys/cur
```

The screen output provides information about the management IP address (MIP) of the iSD-SSL cluster, DNS servers, iSD hosts in the cluster, Syslog servers, and NTP servers.

To check if the iSD-SSL(s) is getting network traffic, type the following command:

```
/stats/dump
```

The screen output provides information about currently active request sessions, total completed request sessions, as well as SSL statistics for configured virtual SSL servers.

To check if a virtual server (on the Web switch) is working, type the following command at any menu prompt:

```
ping <IP address of virtual server>
```

Active Alarms and the Events Log File

To view an alarm that has been triggered and is active, type the following command:

```
/info/events/alarms
```

In the current software version of the iSD-SSL, an alarm is only triggered when a hardware failure in an SSL accelerator card is detected.

To save the events log file to a TFTP server, type the following command:

```
/info/events/download
```

You need to provide the IP address or host name of the TFTP server, as well as a file name. After the events log file has been saved, connect to the TFTP server and examine the contents of the file.

Error Log Files

Provided you have configured the iSD-SSL to use a Syslog server, the iSD-SSL will send log messages to the specified Syslog server. For more information on how to configure a UNIX Syslog daemon, see the Syslog manpages under UNIX. For more information on how to configure the iSD-SSL to use a Syslog server, see the "Syslog Servers Menu" on page 98.

Appendix A
Supported Ciphers

The iSD-SSL supports SSL version 2.0, SSL version 3.0, and TLS version 1.0. All ciphers covered in these versions of SSL are supported, except the IDEA ciphers and the FORTEZZA ciphers.

Table A-1 Supported Ciphers

Cipher Name	SSL Protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
DHE-DSS-RC4-SHA	SSLv3	DH, DSS	RC4(128)	SHA1
EXP1024-DHE-DSS-RC4-SHA	SSLv3	DH (1024), DSS	RC4(56)	SHA1 EXPORT
EXP1024-RC4-SHA	SSLv3	RSA(1024), RSA	RC4 (56)	SHA1 EXPORT
EXP1024-DHE-DSS-DES-CBC-SHA	SSLv3	DH (1024), DSS	DES (56)	SHA1 EXPORT
EXP1024-DES-CBC-SHA	SSLv3	RSA (1024), RSA	DES (56)	SHA1 EXPORT
EXP1024-RC2-CBC-MD5	SSLv3	RSA (1024), RSA	RC2 (56)	MD5 EXPORT
EXP1024-RC4-MD5	SSLv3	RSA (1024), RSA	RC4 (56)	MD5 EXPORT
EDH-RSA-DES-CBC3-SHA	SSLv3	DH, RSA	3DES(168)	SHA1
EDH-RSA-DES-CBC-SHA	SSLv3	DH, RSA	DES (56)	SHA1
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512), RSA	DES (40)	SHA1 EXPORT
EDH-DSS-DES-CBC3-SHA	SSLv3	DH, DSS	3DES (168)	SHA1
EDH-DSS-DES-CBC-SHA	SSLv3	DH, DSS	DES (56)	SHA1
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH (512), DSS	DES (40)	SHA1 EXPORT

Table A-1 Supported Ciphers

Cipher Name	SSL Protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
DES-CBC3-SHA	SSLv3	RSA, RSA	3DES (168)	SHA1
DES-CBC-SHA	SSLv3	RSA, RSA	DES (56)	SHA1
EXP-DES-CBC-SHA	SSLv3	RSA (512), RSA	DES (40)	SHA1 EXPORT
EXP-RC2-CBC-MD5	SSLv3	RSA (512), RSA	RC2 (40)	MD5 EXPORT
RC4-SHA	SSLv3	RSA, RSA	RC4 (128)	SHA1
RC4-MD5	SSLv3	RSA, RSA	RC4 (128)	MD5
EXP-RC4-MD5	SSLv3	RSA (512), RSA	RC4 (40)	MD5 EXPORT
ADH-DES-CBC3-SHA	SSLv3	DH, NONE	3DES (168)	SHA1
ADH-DES-CBC-SHA	SSLv3	DH, NONE	DES (56)	SHA1
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512), None	DES (40)	SHA1 EXPORT
ADH-RC4-MD5	SSLv3	DH, None	RC4 (128)	MD5
EXP-ADH-RC4-MD5	SSLv3	DH (512), None	RC4 (40)	MD5 EXPORT
RC4-64-MD5	SSLv2	RSA, RSA	RC4 (64)	MD5
DES-CBC3-MD5	SSLv2	RSA, RSA	3DES (168)	MD5
DES-CBC-MD5	SSLv2	RSA, RSA	DES (56)	MD5
RC2-CBC-MD5	SSLv2	RSA, RSA	RC2 (128)	MD5
EXP-RC2-CBC-MD5	SSLv2	RSA (512), RSA	RC2 (40)	MD5 EXPORT
RC4-MD5	SSLv2	RSA, RSA	RC4 (128)	MD5
EXP-RC4-MD5	SSLv2	RSA (512), RSA	RC4 (40)	MD5 EXPORT

Cipher List Formats

The cipher list you specify for a virtual SSL server consists of one or more cipher strings separated by colons (e.g. RC4:+RSA:+ALL:!NULL:!DH:!EXPORT@STRENGTH). Lists of ciphers can be combined using a logical **and** operation (+) (e.g. SHA1+DES represents all cipher suites containing the SHA1 and the DES algorithms).

In the colon-separated list, any cipher string can be preceded by the characters !, - or +. These characters serve as modifiers, with the following meanings:

- ! permanently deletes the ciphers from the list (e.g. !RSA).
- - deletes the ciphers from the list, but the ciphers can be added again by later options.
- + moves the ciphers to the end of the list. This option doesn't add any new ciphers it just moves matching existing ones.
- @STRENGTH is placed at the end of the cipher list, and sorts the list in order of encryption algorithm key length.

The default cipher list used for all virtual SSL servers in the iSD-SSL is `ALL`.

A cipher list consisting of the string RC4:ALL:!DH translates into a preferred list of ciphers that begins with all ciphers using RC4 as the encryption algorithm, followed by all cipher suites except the eNULL ciphers (ALL). The final !DH string means that all cipher suites containing the DH (Diffie-Hellman) cipher are removed from the list. (None of the major Web browsers support these ciphers.)

Modifying a Default Cipher List

An example of a slightly modified cipher list can be:
RC4:ALL:!EXPORT:!DH

This example will remove all EXPORT ciphers, besides the DH related cipher suites. Removing the EXPORT ciphers means that all ciphers using either 40 or 56 bits symmetric ciphers are removed from the list. This means that browsers running export controlled crypto software cannot access the server.

Using the OpenSSL command line tool (on a UNIX machine), it is possible to check which cipher suites a particular cipher list corresponds to. The example above yields the following output:

```
# openssl ciphers -v ’RC4:ALL:!EXPORT:!DH
RC4-SHA         SSLv3 Kx=RSA     Au=RSA    Enc=RC4(128)    Mac=SHA1
RC4-MD5         SSLv3 Kx=RSA     Au=RSA    Enc=RC4(128)    Mac=MD5
RC4-64-MD5      SSLv2 Kx=RSA     Au=RSA    Enc=RC4(64)     Mac=MD5
RC4-MD5         SSLv2 Kx=RSA     Au=RSA    Enc=RC4(128)    Mac=MD5
DES-CBC3-SHA    SSLv3 Kx=RSA     Au=RSA    Enc=3DES(168)   Mac=SHA1
DES-CBC-SHA     SSLv3 Kx=RSA     Au=RSA    Enc=DES(56)     Mac=SHA1
IDEA-CBC-SHA    SSLv3 Kx=RSA     Au=RSA    Enc=IDEA(128)   Mac=SHA1
DES-CBC3-MD5    SSLv2 Kx=RSA     Au=RSA    Enc=3DES(168)   Mac=MD5
DES-CBC-MD5     SSLv2 Kx=RSA     Au=RSA    Enc=DES(56)     Mac=MD5
IDEA-CBC-MD5    SSLv2 Kx=RSA     Au=RSA    Enc=IDEA(128)   Mac=MD5
RC2-CBC-MD5     SSLv2 Kx=RSA     Au=RSA    Enc=RC2(128)    Mac=MD5
```

Supported Cipher Strings and Meanings

Table A-2 Cipher Strings and Meanings

Cipher String Aliases	Meaning
DEFAULT	The default cipher list, which corresponds to ALL.
ALL	All cipher suites except the eNULL ciphers, which must be explicitly enabled.
HIGH	Cipher suites with key lengths larger than 128 bits.
MEDIUM	Cipher suites using 128 bit encryption.
LOW	Includes cipher suites using 64 or 56 bit encryption, but excludes export cipher suites.
EXPORT	Includes cipher suites using 40 and 56 bit encryption.
EXPORT40	Cipher suites using 40 bit export encryption only.
EXPORT56	Cipher suites using 56 bit export encryption only.
eNULL, NULL	Cipher suites that do not offer any encryption at all. Since the use of such ciphers pose a security threat, they are disabled unless explicitly included.
aNULL	Cipher suites that do not offer authentication, like anonymous DH algorithms. The use of such cipher suites is not recommended, since they facilitate man-in-the-middle attacks.
kRSA, RSA	Cipher suites using RSA key exchange.
kEDH	Cipher suites using ephemeral Diffie-Hellman key agreement.
aRSA	Cipher suites using RSA authentication, which implies that the certificates carry RSA keys.
aDSS, DSS	Cipher suites using DSS authentication, which implies that the certificates carry DSS keys.
SSLv3, SSLv2	SSL version 3.0 and SSL version 2.0 cipher suites, respectively.

Table A-2 Cipher Strings and Meanings

DH	Cipher suites using DH encryption algorithms, including anonymous DH.
ADH	Cipher suites using anonymous DH encryption algorithms.
3DES	Cipher suites using triple DES encryption algorithms.
DES	Cipher suites using DES encryption algorithms, but not triple DES.
RC4	Cipher suites using RC4 encryption algorithms.
RC2	Cipher suites using RCS encryption algorithms.
MD5	Cipher suites using MD5 encryption algorithms.
SHA1, SHA	Cipher suites using SHA1 encryption algorithms.

Appendix B
Command Translation Table

This appendix explains the differences in menu commands between iSD-SSL 1.0 and iSD-SSL 2.0.

Web OS Commands and iSD-SSL 2.0 Commands

One of the main objectives behind developing the iSD-SSL version 2.0 was the ability to run the iSD-SSL together with the other Alteon Web switches. As a result, the iSD-SSL version 2.0 is less tightly integrated with the Web switch. Thus, a main difference between iSD-SSL version 1.0 and version 2.0 is that the initial setup and all configuration is now performed directly on the iSD-SSL itself via the command line interface.

To ease the transition from iSD-SSL version 1.0 to version 2.0, this appendix provides tables containing iSD-SSL commands previously performed on an Alteon Web switch running Web OS 8.1 or higher, and their current equivalents on the iSD-SSL version 2.0. Note that most of the Web OS commands used in iSD-SSL 1.0 units are still available in the command line interface of the Web OS also when using iSD-SSL 2.0 units. When executed in the Web OS, however, these iSD-SSL 1.0 commands will not function.

iSD Menu Options

Table B-1 iSD Menu Options

iSD-SSL v1.0 Web OS Commands	iSD-SSL v2.0 iSD Commands
`/cfg/isd/ssl` This Web OS command displayed the SSL Offload Application menu.	For information about the corresponding menu commands in iSD-SSL 2.0, see "SSL Offload Application Menu Options" on page 211.
`/cfg/isd/ipstrt` This Web OS command was used to set the starting IP address for iSD-SSL units.	On the iSD-SSL 2.0, you assign a unique IP address to each iSD-SSL manually at the time of the initial setup, regardless of whether you select **`new`** or **`join`** in the Setup menu. To change the IP address of a particular iSD-SSL after the initial setup, see the **`ip`** command under "iSD Host Configuration Menu" on page 96. To view information about which IP addresses that are currently assigned to the available iSD hosts, use the command **`/cfg/sys/cur`**. On the iSD-SSL 2.0, you also assign an IP address to each new cluster. Each time you perform an initial setup on an iSD-SSL 2.0 and select **`new`** in the Setup menu, you are requested to specify a unique management IP address (MIP). By doing so, a new cluster is created, even though it initially only consists of a single iSD-SSL. In order to change the management IP address of an existing cluster, use the command **`/cfg/sys/mip`**. For more information, see the **`mip`** command under "System Configuration Menu" on page 93.

Table B-1 iSD Menu Options

iSD-SSL v1.0 Web OS Commands	iSD-SSL v2.0 iSD Commands
`/cfg/isd/ipnum` This Web OS command was used to specify the number of iSD-SSL units attached to the Web switch. Starting from the **`ipstart`** value, the Web switch would then automatically assign IP addresses in sequence to the specified number of iSD-SSL units.	On the iSD-SSL 2.0, you assign a unique IP address to each iSD-SSL manually at the time of the initial setup. **`/cfg/sys/host #/ip`** To change the IP address of a particular iSD-SSL after the initial setup, use the **`ip`** command. For more information, see the **`ip`** command under "iSD Host Configuration Menu" on page 96.
`/cfg/isd/vrnum` This Web OS command was used to specify the virtual router number that the iSD-SSL 1.0 connected to on the Web switch in case you had a redundant active-standby configuration.	**`/cfg/sys/gateway`** On the iSD-SSL 2.0, when having a redundant active-standby configuration, you set the gateway IP address to the IP address of the virtual router. If you have an active-standby configuration when performing the initial setup of the iSD-SSL 2.0, specify the IP address of the appropriate virtual router as the gateway IP address. To change the gateway IP address for all iSD hosts in a cluster after the initial setup, use the command **`/cfg/sys/gateway`**. For more information, see the **`gateway`** command under "System Configuration Menu" on page 93. To view information about which gateway IP address that is currently assigned to the available iSD hosts in a cluster, use the command **`/cfg/sys/cur`**.
`/cfg/isd/on` This Web OS command was used to globally turn on all iSD-SSL processing.	On the iSD-SSL 2.0, the iSD-SSL processing is performed stand-alone from the Web switch, and a cluster of iSD-SSLs provides you with a single system image through the Management IP (MIP).

Table B-1 iSD Menu Options

iSD-SSL v1.0 Web OS Commands	iSD-SSL v2.0 iSD Commands
/cfg/isd/off This Web OS switch command was used to globally turn off all iSD-SSL processing.	On the iSD-SSL 2.0, there is no command to turn of iSD-SSL processing for all iSD hosts in a cluster. However, to temporarily remove a single iSD-SSL 2.0 from operation, you can connect to the particular iSD-SSL either via a remote connection (Telnet or SSH) or a console connection, and use the command **/boot/halt**. For more information, see the **halt** command under "Boot Menu" on page 107. Note: To bring a halted iSD-SSL back into operation, you need to press the Reset button on the front panel.
/cfg/isd/cur This Web OS command was used to display the iSD-SSL configuration regarding starting IP address, number of iSD-SSL units, virtual router number, and iSD-SSL processing.	**/cfg/sys/cur** On the iSD-SSL 2.0, you can use the **cur** command to view information about IP address and type of iSD (master or slave) on a per host basis. System information and network information common for all iSD hosts in the cluster is also displayed. **/info/isdlist** To view information about memory usage and CPU usage, as well as the operational status of all iSD-SSLs in a cluster, you can use the **isdlist** command.

SSL Offload Application Menu Options

Table B-2 SSL Offload Application Menu Options

iSD-SSL v1.0 Web OS Commands	iSD-SSL v2.0 iSD Commands

`/cfg/isd/ssl/addcrt`
This Web OS command was used to add a certificate using a cut-and-paste operation, and to bind the certificate to a virtual server IP address.
	`/cfg/ssl/cert #/cert`
	`/cfg/ssl/cert #/key`
	On the iSD-SSL 2.0, you can add certificates and keys separately or combined (if both are contained in the same file) by using a cut-and-paste operation.
	For more information, see the **`cert`** and the **`key`** commands under "Certificate Management Menu" on page 77.

`/cfg/isd/ssl/tftpcrt`
This Web OS command was used to add a certificate by downloading the certificate file from a TFTP server, and to bind the certificate to a Virtual Server IP address.
	`/cfg/ssl/cert #/tftpcert`
	`/cfg/ssl/cert #/tftpkey`
	On the iSD-SSL 2.0, you can add certificates and keys separately or combined (if both are contained in the same file) by using TFTP.
	For more information, see the **`tftpcert`** and **`tftpkey`** commands under "Certificate Management Menu" on page 77.

`/cfg/isd/ssl/remcrt` This Web OS command was used to remove a certificate.	**`/cfg/ssl/cert #/del`** On the iSD-SSL 2.0, you can remove a certificate and the corresponding private key by using the **`del`** command. For more information, see the **`del`** command under "Certificate Management Menu" on page 77.

Table B-2 SSL Offload Application Menu Options

iSD-SSL v1.0 Web OS Commands	iSD-SSL v2.0 iSD Commands
/cfg/isd/ssl/lstcrt This Web OS command was used to display the contents of a certificate.	**/cfg/ssl/cert #/show** On the iSD-SSL 2.0, you can display the contents of a certificate by using the **show** command. **/cfg/ssl/cert #/info** To only view the serial number, expiration date and information related to the owner or subject of the certificate, use the **info** command. For more information, see the **show** and **info** commands under "Certificate Management Menu" on page 77.
/cfg/isd/ssl/lstip This Web OS command was used to list the virtual IP addresses for which certificates had been configured.	**/cfg/ssl/cur** On the iSD-SSL 2.0, you can display information about all added certificates and configured SSL servers by using the **cur** command. The command also shows information about which certificate is being used by a particular SSL server. For more information, see the **cur** command under "SSL Main Menu" on page 76.
/cfg/isd/ssl/setport This Web OS command was used to set the TCP port for communication between the iSD-SSLs and the real Web servers via plain HTTP.	**/cfg/ssl/server #/rport** On the iSD-SSL 2.0, you configure the TCP port for communication between the iSD-SSL and the real servers by using the **rport** command. For more information, see the **rport** command under "SSL Server Menu" on page 83.

Table B-2 SSL Offload Application Menu Options

iSD-SSL v1.0 Web OS Commands	iSD-SSL v2.0 iSD Commands
`/cfg/isd/ssl/lstport` This Web OS command was used to display the TCP port set for communication between the iSD-SSLs and the real Web servers via plain HTTP.	**`/cfg/ssl/server #/cur`** On the iSD-SSL 2.0, you can display all settings for a specific virtual SSL server by using this command. The Real server port value indicates the TCP port used for communication between the iSD-SSL and the real servers. To display information about all certificates and virtual SSL servers, use the command **`/cfg/ssl/cur`**.
`/cfg/isd/ssl/update` This Web OS command was used to update or upgrade all iSD-SSL software via TFTP.	**`/boot/tftp`** On the iSD-SSL 2.0, you can perform an upgrade of the software that runs on all iSD-SSLs in a cluster by using the **`tftp`** command. For more information, see “Performing Minor/Major Release Upgrades” on page 42.
`/cfg/isd/ssl/shutdn` This Web OS command was used to either shutdown or reboot a particular iSD-SSL or all iSD-SSLs.	**`/boot/halt`** On the iSD-SSL 2.0, you can use the **`halt`** command to shut down the particular iSD-SSL to which you have connected. **`/boot/reboot`** To reboot the iSD-SSL, you can use the **`reboot`** command. Note: You should connect to the particular iSD-SSL you want to halt or reboot via a remote connection (Telnet or SSH) or a console connection, and not via a remote connection to the Management IP address (MIP). For more information, see the **`halt`** and **`reboot`** commands under “Boot Menu” on page 107.

iSD Information Command

Table B-3 iSD Information Commands

iSD-SSL v1.0 Web OS Commands	iSD-SSL v2.0 iSD Commands
`/info/isd` For the iSD-SSL 1.0, this Web switch command was used to display switch information regarding all iSD-SSL devices.	**`/info/isdlist`** On the iSD-SSL 2.0, you can use the **`isdlist`** command to display information about IP address, master or slave assignment, operational status, CPU and memory usage for all iSD-SSLs in the cluster. **`/info/localisd`** To view information only for the particular iSD-SSL to which you are connected via a remote connection or console connection, you can use the **`localisd`** command. If you are connected to the Management IP address (MIP) via a remote connection when using this command, the information displayed refers to the iSD-SSL in the cluster that currently is in control of the MIP. For more information, see the **`isdlist`** and **`localisd`** commands under "Information Menu" on page 65.

APPENDIX C
iSD-SSL 2.0 SNMP Agent

There is one SNMP agent in each iSD-SSL cluster, and the agent listens to the MIP (Management IP address) of the cluster. The SNMP agent supports SNMP version 1 and version 2c. Notification targets (the SNMP managers receiving trap messages sent by the agent) can be configured to use either SNMP v1 or SNMP v2c (with the default being SNMP v2c). Users may specify any number of notification targets on the iSD-SSL.

For more information on how to configure the SNMP agent in a cluster, see "SNMP Menu" on page 103 (and the following pages).

For detailed information about the MIB (Management Information Base) definitions that are currently implemented for the iSD-SSL 2.0 SNMP agent, see "Contacting Alteon WebSystems" on page 16.

Supported MIBs

The iSD-SSL supports the following MIBs:

- SNMPv2-MIB
- ALTEON-ISD-PLATFORM-MIB
- ALTEON-ISD-SSL-MIB

The SNMPv2 MIB

The SNMPv2-MIB is a standard MIB which all agents implements, and it contains the following groups and objects:

- System group, which is a collection of objects common to all managed systems.
- SNMP group, which is a collection of objects providing basic instrumentation and control of an SNMP entity.

The Alteon iSD Platform MIB

The ALTEON-ISD-PLATFORM-MIB contains the following groups and objects:

- Cluster group, whose objects provide information about the operational status of each iSD-SSL, IP address assignment, master/slave assignment, and the iSD host number.
- Performance group, whose objects provide information about CPU and memory utilization.
- Current Alarm group, whose objects provide information about the number of active alarms, alarm IDs, alarm severity levels, alarm cause, and the time when the alarm was triggered.
- Event group, whose objects provide information about the time when the event was generated, as well as a description of the event.

The Alteon iSD-SSL MIB

The ALTEON-ISD-SSL-MIB contains objects for monitoring the SSL gateways. The objects provide information about the following:

- Number of SSL transactions per second.
- Number of initiated client SSL connections.
- Number of renegotiated client SSL connections.
- Number of successfully completed SSL handshakes.
- Number of client requests for a session ID found in the SSL cache.
- Number of client requests for a session ID not found in the SSL cache.
- Number of times a session ID could not be cached because the SSL cache was full.
- Number of client requests for a session ID that was found in the SSL cache, but inaccessible due to the fact that the Time To Live value for the session was exceeded.

Supported Traps

The following SNMP traps are supported in the iSD-SSL 2.0:

Table C-1 Traps supported in the iSD-SSL 2.0

Trap Name	Description
alteonISDSSLHwFail	Signifies that the SSL accelerator hardware failed. The iSD-SSL will continue to handle traffic, but with severely degraded performance.
alteonISDDown	Signifies that an iSD-SSL in the cluster is down and out of service.
alteonISDSingleMaster	Signifies that only one master iSD-SSL in the cluster is up and operational. Only having one master in a cluster means that the fault tolerance level is severely degraded—if the last master fails, the system cannot be reconfigured. This trap is only sent if more than two iSD-SSLs in the cluster defined as masters.

Appendix D
Specifications

iSD100-SSL Specifications

iSD100-SSL 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 Celeron 500 MHz
SDRAM memory	256 MB, expandable up to 1 GB
L2 Cache (Internal)	256KB ECC 64-bit wide
Flash Memory Card	64 MB
Drive Bay (available)	One or two 3.5" hard disks
Communications	On model iSD100-SSL-C1A, one 10/100Base-T port for copper Ethernet/Fast Ethernet at half or full duplex. On model iSD100-SSL-F2A, one 1000Base-SX port for fiber-optic Gigabit Ethernet.
Expansion cards (installed)	Two CryptoSwift PCI Rainbow cards, 200 TPS, and one Network Interface Controller—Ethernet/Fast Ethernet or Gigabit Ethernet, depending on the model.
Expansion Slot (available)	No expansion slots available on either the iSD100-SSL-C1A or the iSD100-SSL-F2A.

iSD100-SSL 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)

iSD100-SSL 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 50 micron multimode fiber	 2 to 275 meters (6.5 to 902 feet) 2 to 550 meters (6.5 to 1804 feet)
Console (DCE)	Female DB-9	RS-232C (serial)	25 meters (80 feet)

iSD100-SSL Power Requirements

Specification		Measurement
AC Power	Power Supply	150W Max.
	Input	100-240 VAC, 50/60 Hz, 2/1A

iSD100-SSL 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	

iSD100-SSL Certifications

Category	Compliance
EMC	CISPR22, CISPR24 FCC CFR 47, Part 15, Class A VCCI, Class A ICES, 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

iSD310-SSL Specifications

iSD310-SSL Physical Characteristics

Characteristic	Measurement
Height	43.2 mm (1.7 inches), 1U
Width	447.3 mm (17.61 inches)
Depth	609.6 mm (24 inches)
Weight	9.9 kg (22 pounds) minimum 11.80 kg (26 pounds) maximum
Processor	Intel Pentium III 866 MHz
SDRAM (ECC) memory	256 MB PC 133, expandable up to 2 GB
Level 2 Cache (internal)	256KB
Video type	ATI RAGE XL PCI video controller; VGA connector
Vide memory (standard)	4 MB SDRAM
SCSI hard-disk drive	One 1-inch hot-pluggable 18 GB HDD, expandable up to three using formatted capacities ranging from 9 GB to 36 GB
SCSI devices	Internal hot-pluggable with RAID controller, termination and automatic configuration for up to three drives. Integrated Adaptec Ultra3 AIC-7899 SCSI host adapter
Diskette drive	3.5 inch, 1.44-MB diskette drive
CD-ROM drive	IDE CD-ROM drive
Communications	On model iSD310-SSL-X, dual integrated Intel PRO/100+ Network Interface Controller (NIC). On model iSD310-SSL-F, one 3Com Gigabit NIC for fiber-optic Gigabit Ethernet, in addition to the dual integrated Intel PRO/100+ NICs.
Expansion cards (installed)	On model iSD310-SSL-X, one CryptoSwift PCI Rainbow card, 600 TPS. On model iSD310-SSL-F, one CryptoSwift PCI Rainbow card, 600 TPS, and one 3COM 1GB Fiber NIC PCI card.
Expansion slots (available)	On model iSD310-SSL-X, one PCI slot (64-bit, 66 MHz) available. On model iSD310-SSL-F, no extra PCI slots available due to the 3COM 1GB Fiber NIC.

iSD310-SSL 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)

iSD310-SSL Port Specifications

Port	Connector	Media	Maximum Distance
Rear:			
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 50 micron multimode fiber	 2 to 275 meters (6.5 to 902 feet) 2 to 550 meters (6.5 to 1804 feet)
Console (DCE)	Female DB-9	RS-232C (serial)	25 meters (80 feet)
USB	two 4-pin	USB cable	5 meters (20 feet)
Video	15-pin	Standard cable	N/A
PS/2-style keyboard	6-pin mini-DIN	Standard cable	N/A
PS/2-compatible mouse	6-pin mini-DIN	Standard cable	N/A
Front:			
Video	15-pin	Standard cable	N/A
PS/2-style keyboard/mouse	6-pin mini-DIN, keyboard default (mouse optional with combination Y cable)		N/A

iSD310-SSL Power Requirements

Specification		Measurement
AC Power	Wattage	240 W Max.
	Voltage	100-240 VAC, 3.6-1.8 A, 60-50 Hz
System battery		CR2032 3-V lithium coin cell

iSD310-SSL Environmental Specifications

Condition	Operating Specification	Storage Specification
Temperature	+10°C to +35°C (50°F to 95°F)	-40°C to +65°C (-40°F to 149°F)
Relative humidity	8% to 80% (noncondencing) with a humidity gradation of 10% per hour	5% to 95% (noncondencing)
Altitude	-16 meters to 3048 meters (-50 to 10,000 feet)	-16 meters to 10,600 meters (-50 to 35,000 feet)
Shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 41 G for 2 ms	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for 2 ms
Vibration	0.25 G (half-sine wave) at a sweep of 3 to 200 Hz for 15 minutes	0.5 G at 3 to 200 Hz for 15 minutes

iSD310-SSL Certifications

Category	Compliance
EMC	CISPR22, CISPR24 FCC CFR 47, Part 15, Class A VCCI, Class A ICES, 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

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

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with 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.

Index