



## **Cisco SSL Appliance 1500 Getting Started Guide**

Version 3.9.2  
November 23, 2015

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.



Version 3.9.2  
November 20, 2015

---

**CHAPTER 1**

<b>Introduction</b>	<b>1-1</b>
Introduction	1-1
Related Documents	1-1
Document Conventions	1-2
Safety	1-2
Unpack the SSL1500	1-3
SSL1500 Specifications	1-3
SSL1500 Front Panel	1-4
Back of the SSL1500	1-7
SSL1500 Installation Requirements Checklist	1-8
Rack Mounting	1-8
Connect to the Management Network and Appliances	1-9
Connect to the Management Network	1-9
Connect to the Network and Attached Appliances	1-9
Console Configuration	1-9
Connect to the Console	1-10
Configuring Putty for the Console Connection	1-10
Configure the SSL Appliance	1-12
Update the IP Address Using a Serial Console	1-15
Setting up the Console	1-15
Configure a Static IPv4 Address	1-15
Configure an IPv6 Address	1-15
Power On and Initial Configuration - WebUI	1-16
Power On	1-17
Get the IP Address	1-17
Bootstrap States	1-18
Bootstrap: Master Key Mode	1-19
Configure a Password	1-20
Bootstrap: Management User Setup	1-21
Configure IP Addresses with the WebUI	1-22

- Configuring IPv4 Static with the LCD Screen 1-24
- Complete System Configuration 1-25
  - Log On 1-26
  - Tool Icons 1-28
  - Date and Time 1-28
  - Complete System Settings 1-29
- Power Off 1-30
- Monitor the System 1-31
  - Dashboard 1-31
  - SSL Session Log 1-33
  - SSL Statistics 1-35
- Configure PKI 1-35
  - Install a CA Cert for Certificate Resign 1-35
  - Import Known Server Key 1-37
- Getting Help 1-38



# Introduction

---

Revised: November 23, 2015,

## Introduction

This guide describes how to get started using the SSL Appliance. It provides a physical overview of each appliance and discusses rack mounting. It shows how to configure the minimum set of system options and gets you ready to deploy your appliance.

Throughout this document the term SSL is used to mean both SSL and TLS, unless explicitly indicated. Secure Socket Layer (SSL) has been largely replaced by Transport Layer Security (TLS) which is the more up to date standard derived from SSL. Both SSL and TLS traffic are present in networks today and the SSL Appliance is capable of inspecting both types of traffic.



### Caution

---

The embedded software contained within the SSL Appliance is subject to licensing terms and conditions imposed by Cisco and third party software providers. You should only use the SSL Appliance if you agree to these licensing conditions; see the Cisco Administration & Deployment Guide for licensing details.

---



### Note

---

The act of “inspecting” SSL traffic may be subject to corporate policy guidelines and/or national legislation. It is your responsibility to ensure that your use of the SSL Appliance is in accordance with any such legal or policy requirements

---

The Cisco Administration & Deployment Guide for the platforms provide full details on all of the options available in the SSL Appliance, and should be consulted for more complex configurations and deployment examples.

## Related Documents

Other documentation for the Cisco SSL Appliance line of products is available.

- *Cisco SSL2000 and SSL8200 Quick Start Guide*; see for initial setup information
- *Cisco SSL Appliance Administration and Deployment Guide*, Version 3.9.x a; see for deployment and configuration information

- *Cisco SSL Appliance Release Notes*; see for software updates, fixes, issues

Use the current Cisco FireSIGHT System documentation roadmap to access current Cisco SSL Appliance documentation:

[www.cisco.com/documentation/pubs/SSL%20Visibility](http://www.cisco.com/documentation/pubs/SSL%20Visibility)

## Document Conventions

The following conventions are used throughout this document.



### Note

This style indicates a “note” providing additional information that the reader may be interested in.



### Caution

This style indicates a “caution” providing additional information that the reader needs to pay attention to.



### Warning

**This style indicates a “warning” that alerts the reader to potential physical injury.**



### Tip

This style indicates a helpful hint.

Many procedures have the “Select Menu > Action” format, where the > means “then select.” A selection in the Platform Management menu is often shown as (Platform Management) > Feature, as the name you actually see will be that of your appliance.

## Safety

Adhere to the warnings and cautions listed in this document when installing or working with the SSL Appliance. Read the separate Safety Notice included in the SSL Appliance packaging.

Read all the installation instructions carefully before connecting the appliance to its power source.

## Ventilation

The Cisco SSL Appliance vents (on the front panel) and the fan openings (on the back panel) are provided for ventilation and reliable operation of the product and to protect it from overheating. These openings must not be blocked or covered. This product must not be placed in a built-in installation unless proper ventilation is provided.

## Power Cords



### Caution

The power supply cords are used as the main disconnect device. Ensure that the socket outlet is located or installed near the equipment and is easily accessible. The SSL1500, SSL2000, and SSL8200 have a dual redundant power supply that is powered by two separate power cords. Always disconnect BOTH cords to remove power from the unit. Disconnect power cables carefully.



### Warning

**To reduce the risk of electrical shock, do not disassemble this product. Return it to Cisco when service or repair work is required. Opening or removing covers may expose the user to dangerous voltage or other risks. Incorrect assembly can cause electric shock when this appliance is subsequently used.**

## Unpack the SSL1500



### Warning

**Take electrostatic discharge control measures before unpacking or installing the appliance.**

Carefully unpack the Cisco SSL Appliance. Compare the actual contents with the table to ensure that you have received all ordered components.

The package also includes the Software License Agreement, a Safety and Regulatory Compliance Guide, and the Quick Start Guide.

**Table 1-1 SSL1500 Packing List**

Part	Description	Quantity
Cisco SSL1500 appliance	1U rack mountable device	1
2 x Power Cords	One for each redundant supply	2
Rack mounting rails	Rack to mount the device	1
Number of Components		4

## SSL1500 Specifications

The specifications shown in each table may change over time, any changes will be reflected in new versions of this documentation which may be downloaded from the Cisco Support site.

**Table 1-2 SSL Appliance Summary**

Specification	SSL1500-C/-F
Total Packet Processing Capacity	8 Gbps
SSL Inspection Throughput	1.5 Gbps

**Table 1-2** *SSL Appliance Summary*

Specification	SSL1500-C/-F
Concurrent SSL Flows being inspected	100,000
New full handshakes/Second 1024 bit key	7500
New full handshakes/Second 2048 bit key	3000
New full handshakes/Second ECDHE256	3500

**Table 1-3** *SSL1500 Specifications*

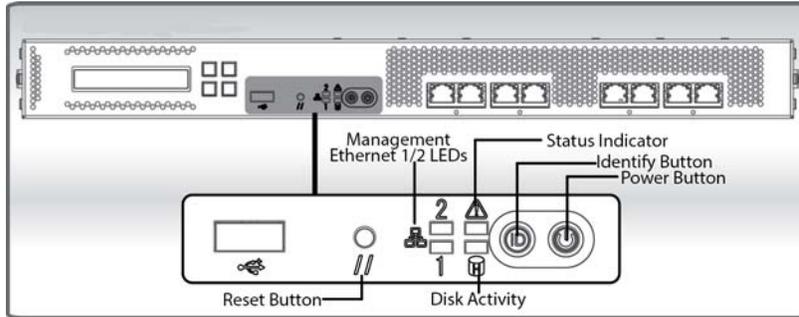
Chassis Dimensions	17.5" (W) x 19.5" (D) x 1.75" (H) (444.5mm x 495.3mm x 44.5mm)
Weight	29 lbs (13.15 kg)
Interfaces	8 x 10/100/1000 copper interfaces
Management Interface	1 x 10/100/1000 management Ethernet interface
Integrated Display	16 character by 2 line LCD on front panel
Power Supplies	2 x 450W power supply
Operating Temperature	5°C to 40°C (41°F to 104°F)
Storage Temperature	-10°C to 70°C (14°F to 158°F)
Cooling	Generates up to 1200 BTU/hour worst case
Air flow	210 ft <sup>3</sup> /min (6m <sup>3</sup> /min)

## SSL1500 Front Panel

This section describes the front and back of the SSL1500. The SSL1500 has eight copper (-C) or fiber (-F) interfaces on the front panel, for connecting to the network and other appliances, as well as an Ethernet management interface.



The front panel has indicators, buttons, an LCD display and a USB port.



## LEDs

**Management Port:** The front panel status LEDs for the management Ethernet interfaces (located on the back) are green when the link is up and flash to indicate traffic flowing over the link. These indicators can be on even when the box is powered off.

**HD Activity:** The hard disk activity LED is green and flashes when there is any internal disk activity.

**System Status:** The system status LED is red while booting, then goes off. The disk activity LED is green and flashes when there is any disk activity on the internal hard drive.

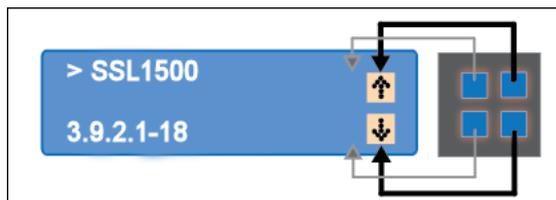
The table shows the various system states that can be indicated by the system status LED on the front panel of the unit. For details on management ports' LEDs, see “Connecting to the Management Network and Appliances” on page 24.

**Table 1-4**

Color	State	System Status	Meaning
None	Off	OK	System ready – no errors detected
Red	Solid	Fault	AC power supply (single) failure AC power cord not present AC power supply module not present

## Buttons

**Keypad:** There are four icon positions at the right side of the LCD screen, corresponding to the display. If you see only an up and down arrow, use the corresponding right side two keypad keys to move through the screens with the arrows. Other icons, such as checkmark and X (done/exit) appear in the inner/left positions.



**Reset:** Reboot the appliance if required. The Reset button is recessed and requires the use of a straight thin object to press the button. Use this button rather than power cycle the appliance.

**ID:** The ID button, if pressed, will cause a blue LED on the rear panel to the left of the serial port to illuminate. This LED is located behind the back panel, so it is visible through the ventilation holes. The purpose of this LED is to make it easier to locate a system when it is racked in a stack with other systems.

## Ports

The SSL1500 has eight copper or fiber interfaces on the front panel. These ports are used to connect the appliance to the monitored network and to other appliances. “Fail to wire” (FTW) hardware directly connects the two ports in a pair together whenever the port pair are in FTW mode. All port pairs enter FTW mode when the appliance is powered off.



### Note

FTW is the default setting but can be disabled if desired.

**Figure 1-1** *Copper Interfaces and LEDs*



Each port has Activity and Link Up LEDs. Each pair of ports has a single FTW LED.

**Table 1-5**

Color	State	Link Speed
None	Off	No link
Green	Solid	1000 Mbps link established
Amber	Solid	10/100 Mbps link established

The LED to the top right of each port indicates activity on the port. It blinks green when there is activity on the link.

Below each pair of interfaces is a Fail To Wire (FTW) LED that indicates the current FTW status for that pair of interfaces.

**Table 1-6** *Copper & Fiber Interface FTW LED States*

Color	State	FTW Status
None	Off	Power off FTW disabled
Green	Solid	Active state with armed watchdog
Amber	Solid	Commanded FTW state change
Amber	Flashing	Forced FTW

**Figure 1-2** *Fiber Interfaces and LEDs*

Each fiber interface has two LEDs arranged vertically.

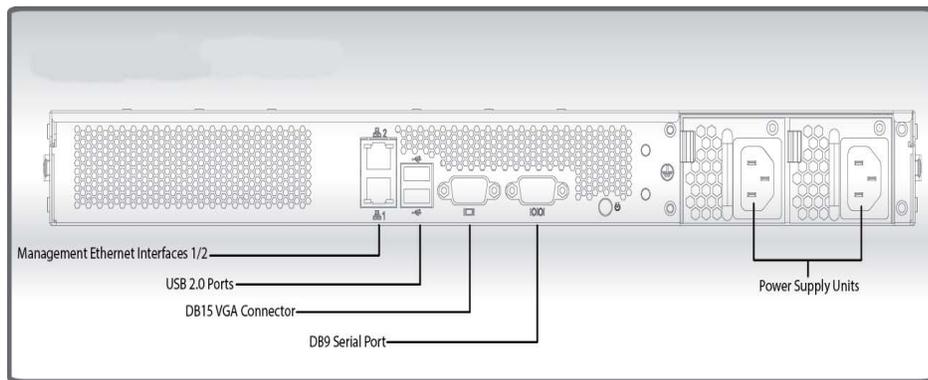
- The top LED indicates link activity and
- The bottom LED indicates link state.

Link state can be: off, meaning no link is established, or solid green indicating a 1000 Mbps link is established.

Each pair of fiber ports has a FTW indicator LED that indicates FTW status as shown in the table above.

## Back of the SSL1500

The rear panel connectors on the SSL1500 are shown next. Ventilation holes on the rear panel must not be blocked as free flow of air is essential for system cooling.



1	Management Ethernet 1	4	USB port
2	Management Ethernet 2	5	VGA display connector
3	USB port	6	Serial port

- LEDs for the management ports are located on the front of the appliance.
- For enhanced security, the management port is isolated from inspected network traffic going through the network ports.
- Two 4x15 mm lugs are provided on the rear panel to allow connection of the chassis to earth ground.

## Power Supplies

The SSL1500 is equipped with two independent power supply units, either of which can power the appliance. The power supply units feature IEC-320 (that is, standard server/PC style) connectors. Normally both units should be attached to an uninterruptible power supply or other power outlet (110 or 220/240 Volt AC).



### Note

The power supplies are hot swappable and can be replaced while the SSL Appliance is powered on and operating.



### Caution

Replacement must be done with units supplied by Cisco Systems Inc. Use of other units will void any warranty and may damage the system.

The power supplies have a bi-color LED indicator. The table shows the conditions indicated by the LED.

**Table 1-7 LED Power Supply Indicators**

LED Color	State	Power Supply Condition
Green	Flashing	AC connected but not turned on; standby
Green	Solid	Powered on and working fine
Red	Flashing	AC not connected
Red	Solid	Fault condition

## SSL1500 Installation Requirements Checklist

The SSL Appliance operates in a 5°C to 40°C environment with an operating humidity of 5-85% non-condensing. It requires sufficient space around the appliance to ensure adequate cooling. The unit may be installed on a firm surface that supports the width, depth and weight of the complete assembly. Edge-only shelves may also be used. Don't use a too-short shelf, with the unit cantilevered off the front or back.

### Rack Mounting

If the SSL Appliance is to be installed in an equipment rack, please follow these precautions:

- Ensure that the ambient temperature around the appliance (which may be higher than the room temperature) is within the operational limits.
- Ensure that there is sufficient airflow around the unit.
- Ensure that the electrical circuits are not overloaded; consider the nameplate ratings of all the connected equipment and ensure that sufficient over current protection is available.
- Ensure that the equipment is properly grounded.
- Never place any objects on top of the appliance.

The SSL1500 is equipped with pre-installed rack-mount brackets and supplied with rack mount rails allowing easy installation in a rack. The following will be required:

- At least 1U rack space (deep enough for a 27" device) – power and management ports at rear
- Phillips (cross head) screwdriver
- Two available power outlet (110 VAC or 220-240 VAC)
- Two IEC-320 power cords (normal server/PC power cords) should the supplied power cords not be suitable for your environment
- Adequate cooling for all devices in the environment
- One RJ-45 CAT5e/CAT6 Ethernet cable for connecting the SSL Appliance to the management network (or a local notebook/desktop computer which is used to manage the SSL Appliance)
- An appropriate copper or fiber cables to connect the SSL1500 to the network and to associated security appliances
- The information sheet provided with the rails.

Follow the procedures in the information sheet provided with the rails kit to install the appliance.

# Connect to the Management Network and Appliances

## Connect to the Management Network

The WebUI management interface is accessed via Management Ethernet 1. Plug a cable into the Ethernet port identified as Management Ethernet 1 on the SSL1500 Front Panel. See Power On and Initial Configuration for additional information. Check that the LEDs on the port indicate that the link is up.

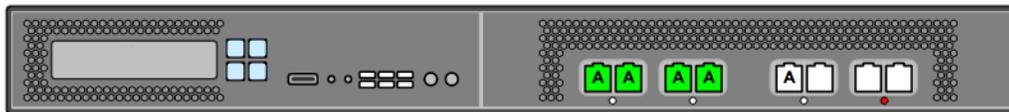
See the Cisco SSL1500 Administration and Deployment Guide for deployment information and examples.

- To use the WebUI for the initial configuration, see Power On and Initial Configuration for configuration information.
- To use a console connection for the initial configuration, see Console Configuration.

## Connect to the Network and Attached Appliances

Connect to the network/other appliance via the front network interfaces.

When a segment is configured and activated, port numbers allocated to that segment are displayed on the management WebUI. The relevant ports must be connected to the network and associated appliance(s) using the appropriate cabling.



Log into the SSL Appliance to configure policy, observe statuses, and so on.

## Console Configuration

Follow this section to connect to and initially configure your SSL Appliance using a serial console and the Command Line Diagnostics (CLD) interface. See the *Administration and Deployment Guide* for a list of CLD commands.

The first time you turn on your SSL Appliance, you need to:

- 
- Step 1** Connect the Management Ethernet port. HTTPS access to the SSL Appliance is via this separate interface, which should be connected to a secure network used by administrators to manage security appliances.
  - Step 2** Power on: ensure the required power cables are connected, and press the power button.  
The System Status Indicator will be solid green, and after a minute or so the LCD display will illuminate and display an appliance name and software version message.
  - Step 3** Get an IP address (required to manage the appliance).
  - Step 4** Go through the bootstrap process, setting up the required users.

See Power On and Initial Configuration to use the WebUI rather than a serial connection, and for more information about the bootstrap states and the master key mode.

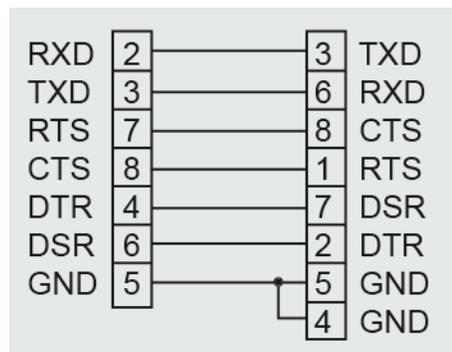
## Connect to the Console

The console port on the SSL Appliance allows the user direct access to the management interface during the initial configuration phase. In the initial configuration, you will configure the IP Address, user accounts, and roles.

After initial configuration is complete, the console port can be used to access the Command Line Diagnostics (CLD) interface, which is also accessible via SSH.

The serial connection on the appliance is configured as:

- 115200 baud rate
- 8 data bits
- 1 stop bit
- no parity
- no hardware flow control.



### SSL1500 Serial Port Pin Outs

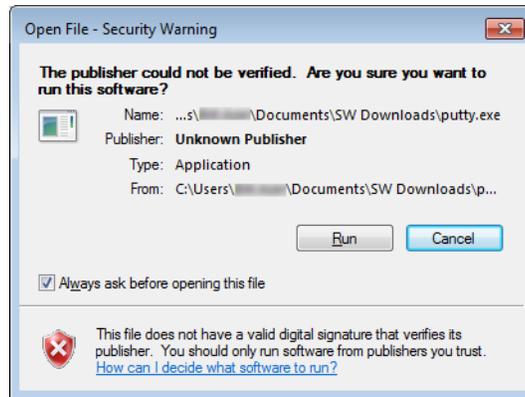
The console cable required for the SSL1500 follows the wiring in a straight-through serial cable (DB9 to DB9). The pin-out for a serial cable is shown next.

1	DCD (Data Carrier Detect)	6	DSR (Data Set Ready) Input
2	RXD (Received Data) Input	7	RTS (Request To Send)
3	TXD (Transmit Data) Output	8	CTS (Clear To Send)
4	DTR (Data Terminal Ready)	9	RI (Ring Indication)
5	Ground		

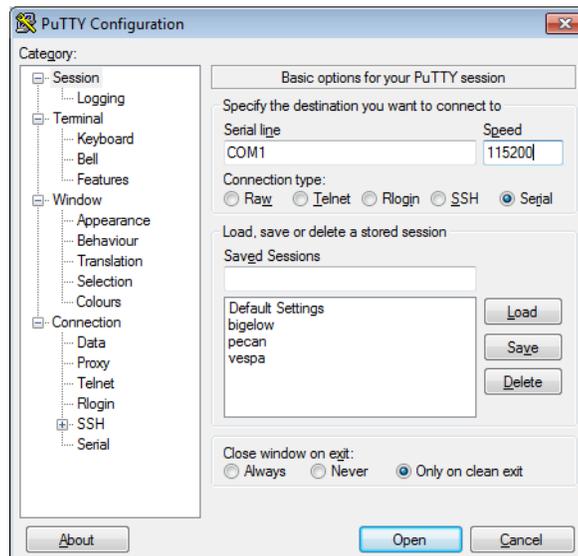
## Configuring Putty for the Console Connection

The following example describes the console configuration using the Putty client on a Windows system.

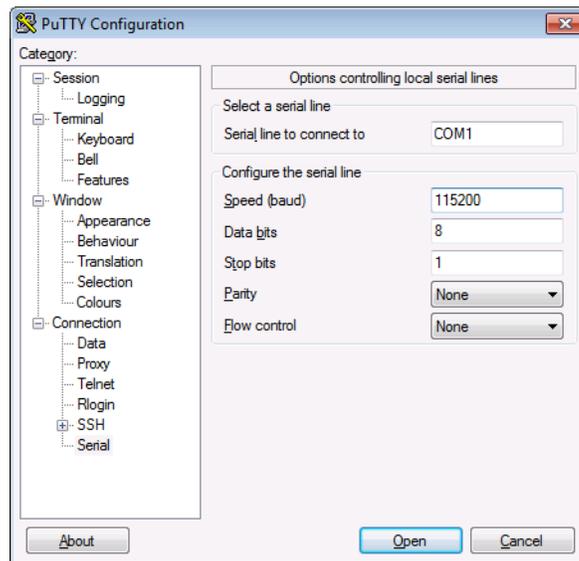
- Step 1** Download Putty client (from the Putty download site).
- Step 2** Run the Putty Client.



- Step 3** Configure Putty to use a serial connection at 115200.



**Step 4** Configure the serial connection to support the SSL Appliance's console speeds.



## Configure the SSL Appliance

The SSL Appliance bootstrap settings can be configured via the CLD interface upon initial boot. Logging on to the console and via the “bootstrap” user, you will configure the management interface for access via the Web User Interface (WebUI).

**Step 1** Connect to the appliance, and login using the bootstrap user (the password is “bootstrap” as well).

```

192.168.76.14 - PuTTY
Ubuntu 12.04.5 LTS localhost ttyS0

localhost login: bootstrap
Password:
Last login: Tue Aug 19 19:01:58 UTC 2014 on ttyS0
SSL Appliance 3.8.0-0
S/N: 5013ID0000
Legal Notices - This product may include 3rd party software.
For more information please refer to the login page of the web based management interface.
BOOTSTRAP: master key configuration
bootstrap>

```

**Step 2** Create the master key next. This example assumes that the master key is not being stored on a USB stick, and that no front panel password is required to unlock the secure store during boot. Commands are provided to allow one or both of these options to be set before the master key is created.

```

192.168.76.14 - PuTTY
bootstrap> master key create
Setting master key configuration.
Waiting for master key generation.
....
BOOTSTRAP: create initial user account(s)
bootstrap>

```

- Step 3** Configure an Admin user with the administrator options, and enter the password when prompted. This example creates a single admin user account that has all four roles allocated to it. The only requirements for completing the bootstrap phase is that there is a user account with the Manage Appliance role, and a user account with the Manage PKI role. These may be the same or different accounts. In most cases, creating a single account with all four roles is the simplest approach.

```

192.168.76.14 - PuTTY
bootstrap>
bootstrap> us
user show
user list
user remove
user add
bootstrap> user add ?
[name] = <arg> : User full name
[password] = <arg> : User password
<arg1> : User ID to add
===== optional flags =====
[manage-pki] : Add 'Manage PKI' role
[manage-appliance] : Add 'Manage Appliance' role
[manage-policy] : Add 'Manage Policy' role
[audit] : Add 'Auditor' role

bootstrap> user add admin manage-pki manage-appliance manage-policy audit
Enter new user password:
Re-enter new user password:
Added user 'admin'.
BOOTSTRAP: completed
bootstrap>

```

- Step 4** Log out as the bootstrap user, then log back in as the newly created admin user. Once the bootstrap mode is complete, the bootstrap user account is no longer present and cannot be used.

```

192.168.76.14 - PuTTY
bootstrap> exit
BOOTSTRAP: completed

localhost login: admin
Password:
SSL Appliance 3.8.0-0
S/N: 5013ID0000
Legal Notices - This product may include 3rd party software.
For more information please refer to the login page of the web based management interface.
admin>

```

- Step 5** The current (default) network setting is for DHCP. The settings are displayed by using the “network show” command.

```

192.168.76.14 - PuTTY
admin> network show
Management network information:
MAC address: 00:15:4d:07:00:a4
MTU: 1500
IPv4: Enabled
IPv4 DHCP: enabled
IPv4 Address: 192.168.76.81/24
IPv4 Default Gateway: 192.168.76.1
IPv6: Enabled
IPv6 SLAAC: disabled
IPv6 DHCP: enabled
IPv6 Address: ::/0
IPv6 Link Local Address:
IPv6 Default Gateway:
Primary Nameserver:
Secondary Nameserver:
admin>

```

- Step 6** To configure the network interface with a static IP address, use the “network set ip” command with applicable parameters. See also “Update the IP Using a Serial Console” on page 32.

```

192.168.76.14 - PuTTY
admin>
admin> network set ?
network set ip          : Set management network static IPv4 configuration
network set ip dhcp    : Enable DHCP in management network IPv4 configuration
network set ip disabled : Disable IPv4 in management network configuration
network set ip6        : Set management network static IPv6 configuration
network set ip6 dhcp   : Enable DHCP in management network IPv6 configuration
network set ip6 disabled : Disable IPv6 in management network configuration
network set ip6 slaac  : Enable SLAAC in management network IPv6 configuration
network set mtu        : Set management network MTU
admin> network set ip ?
[netmask] = <arg> : Netmask (default:255.255.255.0)
[gateway] = <arg> : Default gateway
<arg1> : IPv4 address/Netmask

admin> network set ip 192.168.76.81 netmask 255.255.255.0 gateway 192.168.76.1
Management network IPv4 configuration set successfully:
IP address: 192.168.76.81
Netmask: 255.255.255.0
Default gateway: 192.168.76.1
You must reboot for the changes to take effect.
admin>

```

- Step 7** Reboot the system for the changes to take effect (confirm that you wish to reboot).

```

192.168.76.14 - PuTTY
admin>
admin> platform reboot
Reboot appliance? (enter 'yes' to confirm): yes

```

- Step 8** When the web interface on the appliance starts, confirm that you can log in to the appliance using your browser. Log on using the format `https://<ip address>`. Log in with the username and password you created.



  
 User ID   
 Password

# Update the IP Address Using a Serial Console

The SSL Appliance may be accessed through a serial console or SSH session as well as the WebUI. The Command Line Diagnostics (CLD) interface (refer to the “Command Line Diagnostics Interface” in the Administration and Deployment Guide for a list of commands) is primarily used for diagnostics and monitoring purposes. It can also be used to configure static IPv4 and/or IPv6 IP addresses.

Following the examples, see lists of related commands.

## Setting up the Console

- 
- Step 1** Provide the hostname or IP address information for the SSLV you want to control to your serial or SSH console. See “Console Configuration” for a complete explanation.
  - Step 2** Enter the user name and password for the Manage Appliance user on the appliance.
  - Step 3** To see a list of CLD commands, enter “?”.
- 

## Configure a Static IPv4 Address

- 
- Step 1** Enter the command: `network set ip`, supplying desired IPv4 address, and the netmask and gateway parameters, and press Enter.
  - Step 2** You will see an acceptance message.
  - Step 3** Log in to the appliance as usual.
- 

### IPv4 Related Commands

<code>network set ip &lt;IP&gt;[/mask bits] [gateway &lt;default gateway IP&gt;]</code>	Set management network static IP configuration
<code>network set</code>	Enable DHCP management IP configuration
<code>network show</code>	Show network IP configuration

## Configure an IPv6 Address

- 
- Step 1** Enter the command: `network set ip6`, supplying desired IPv6 address, and the netmask and gateway parameters, and press Enter.
  - Step 2** You will see an acceptance message
  - Step 3** Log in to the appliance as usual.
-

**IPv6 Related Commands**

<code>network set ip6 &lt;IP&gt;[/mask bits] [gateway &lt;default gateway IP&gt;]</code>	Set management network static IP configuration
<code>network set ip6 dhcp</code>	Enable DHCP management IP configuration
<code>network set ip6 slaac [stateless-dhcp]</code>	Enable IPv6 SLAAC, optionally with stateless DHCP IP configuration
<code>network show</code>	Show network IP configuration

**Note**


---

To configure a DNS nameserver IP address, use the Platform Management (system name) > Management Network option in the WebUI.

---

## Power On and Initial Configuration - WebUI

A typical installation process for a new SSL Appliance is to install the system in a rack in the equipment room, then power it up perform the initial configuration. Follow this section to perform the initial configuration using the WebUI (graphical user interface). See “Console Configuration” to use a console connection instead.

The first time you turn on your SSL Appliance, you need to:

- 
- Step 1** Connect the Management Ethernet port. HTTPS access to the SSL Appliance is via this separate interface, which should be connected to a secure network used by administrators to manage security appliances.
  - Step 2** Power on.
  - Step 3** Get an IP address (required to manage the appliance).
  - Step 4** Go through the bootstrap process, setting up the required parameters:
    - Bootstrap States
    - Master Key Mode
    - Management Users
  - Step 5** Using the WebUI, set the appliance date and time, and verify or update the management settings (including the IP address).

You also have the option to install an SSL Inspection license, which you will need to do in order to execute SSL inspection policy.

The next several sections of this document will guide you through the process options.

## Power On

Ensure that the one or two power supplies are connected to power using appropriate cabling. To turn the unit on press the front panel power button. If all is well, the System Status Indicator will be solid green, and after a minute or so the LCD display will illuminate and display an appliance name and software version message. After several startup, booting, and validating messages, the appliance/version message appears again, with up and down arrow keys.

## Get the IP Address

You must have the IP address on hand to perform initial configuration. By default, the SSL Appliance uses DHCP to acquire both IPv4 and IPv6 addresses from an attached network DHCP server. If you use DHCP, see “Getting the DHCP IP Address from the LCD Screen” on page 34

If the appliance can't get the IP address via DHCP, you can use a serial console to connect. You may:

- Set a static IPv4 address
- Set a DHCP IPv6 address
- Set a static IPv6 address

**Note**

---

You can also configure a static IPv4 or IPv6 address via the WebUI after initially logging in.

---

For IPv4 or IPv6 management, the appliance can most easily be configured using the WebUI Management Network > Mode setting to use either a Static (fixed) IP address, or to acquire an IP address automatically using DHCP or a SLAAC method (IPv6 only). See Management Network in the Blue Administration and Deployment Guide for your appliance for details on all of the IP address options.

## Getting the DHCP IP Address from the LCD Screen

Press the down arrow on the LCD screen to scroll to the Network screen.

There, press the top left (check mark) button to bring up the sub-menu; select the required IP address option. Make a note of this address.

An IPv6 address displays over multiple screens. An IPv6 address is displayed in sets as four groups of two quads. For example:

- IPv6 screen 1: Q 1-2: FD00:0AFD
- IPv6 screen 2: Q 3-4: 0B00:0000
- IPv6 screen 3: Q 5-6: 020C:29FF
- IPv6 screen 4: Q 7-8: FE3F:7772

You may also want to use the serial console to set or retrieve the IP address, or the LCD screen to set a static IPv4 address; see the next sections, then continue on with the bootstrapping process.

**Note**

---

To configure a DNS nameserver IP address, use the Platform Management (system hostname) > Management Network option in the WebUI.

---

## Bootstrap States

Every time that the SSL Appliance is powered on or re-booted it goes through a number of stages before reaching the fully operational state, these stages are termed the “bootstrap” phase.

As soon as the SSL Appliance is powered on, it can be forced into one of three states by typing in the correct sequence on the front panel keypad.

To enter factory default reset mode, the key sequence must be typed within five seconds of seeing the “Appliance Startup Loading” message on the LCD screen. Key sequences for other states can be typed at any time.

Table 1-8 SSL Appliance Power On Key Sequences

Sequence	State Entered	Description
031203	Factory default reset	May be used before system enters bootstrap mode. Resets appliance, erasing all configuration and other data; returns to factory state  Important: The factory default sequence only works after the LCD turns on and says “Loading...” on the second line. You have 5 seconds to enter the sequence at this point.
01320132	IP configuration mode	Use to configure a static IP address (default is DHCP).
01230123	PIN entry mode	Enter a password PIN when master key mode with PIN has been selected.

## Keypad Layout

The front panel keypad is arranged as follows.

3

0 1

2 3

## Subsequent Startups

Whenever the SSL Appliance is powered on or forced to do a factory default reset, the bootstrap phase will run before the device becomes fully functional. Depending on how the device is configured, the administrator may need to provide input to enable the bootstrap phase to complete allowing the device to become operational again.

- If the master key is stored internally and no password is set for the master key, the bootstrap process becomes invisible, and the device will start up without any need for input from the administrator.
- If the master key is partly stored on a USB storage device, the USB device will need to be connected to the system before the bootstrap phase can complete.
- If the master key is protected by a password, the password will have to be entered using the front panel keypad before the bootstrap phase can complete.

- If the master key is partly stored on a USB storage device and is protected by a password, the password will have to be entered using the front panel keypad, and the USB storage device will have to be connected before the bootstrap phase can complete.

## Bootstrap: Master Key Mode

If the SSL Appliance has not been previously set up, you will see the Bootstrap: Master Key Mode window on first accessing the appliance via the WebUI. The Master Key can be stored internally, with an internal key.

For security, part of the Master Key can be stored on an external USB memory device and can be password protected; this means that the USB memory device will need to be present when the device is powered on, and the password must be input on the front panel keypad in order to make the device operational.

See an internal setup example:



Once the master key mode is configured, the appliance will scan the internal, and if required, external, persistent storage device, for the master key, and if not found, create the master key.

If the master key is protected by a password, the user must first enter the password on the keypad before the master key can be unlocked or created. While in this state the GUI will display a screen with a “spinner” and without any buttons or links.



### Note

The password can be entered into the device prior to the WebUI bootstrap phase, in which case it will be retrieved and used when this point in the bootstrap sequence is reached.

Once the master key is unlocked the secure store can be opened or created, enabling normal operation.

## Create a Password

The password used to unlock the master key must be typed in on the front panel keypad after entering the code for PIN entry mode. See “SSL Appliance Power On Key Sequences “ on page 35. The password is only required if the master key mode chosen requires a PIN.

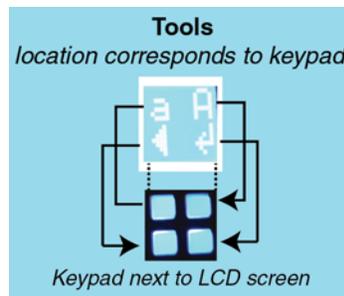
The password is a minimum of 8 characters long. The user has to select each character from a set of 4 characters that are displayed on the LCD, using the corresponding keypad buttons. Passwords can include upper and lower case characters, and the space character. The mechanism used to enter a password is shown in “Configuring a Password” on page 38

## Configure a Password

To configure a system password using the front LCD screen and keypad, enter the PIN entry mode “SSL Appliance Power On Key Sequences” on page 35 during start up.

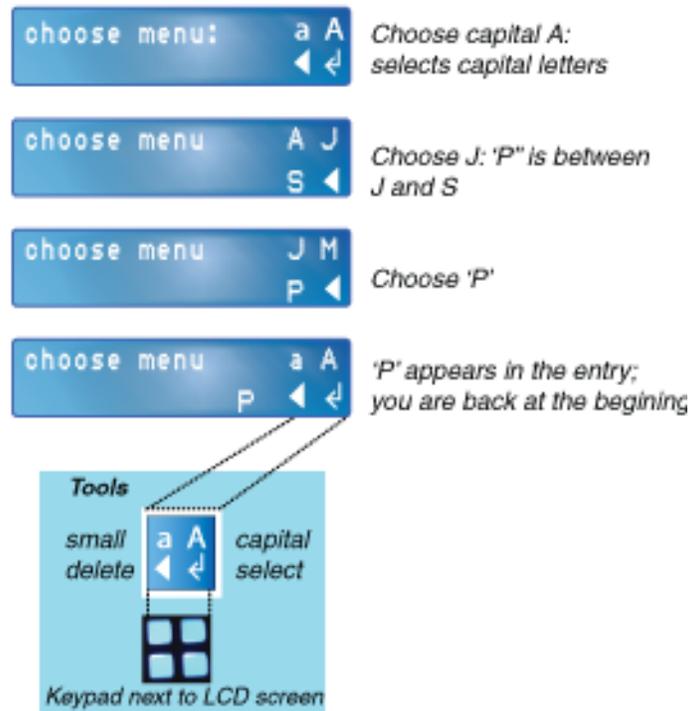
Passwords must be a minimum of 8 characters long. It is good practice to always use at least one non-alphabetic character, at least one uppercase letter, one lowercase letter, and one digit.

The next figure shows the correspondence between the tool graphics on the LCD, and the physical keypad.

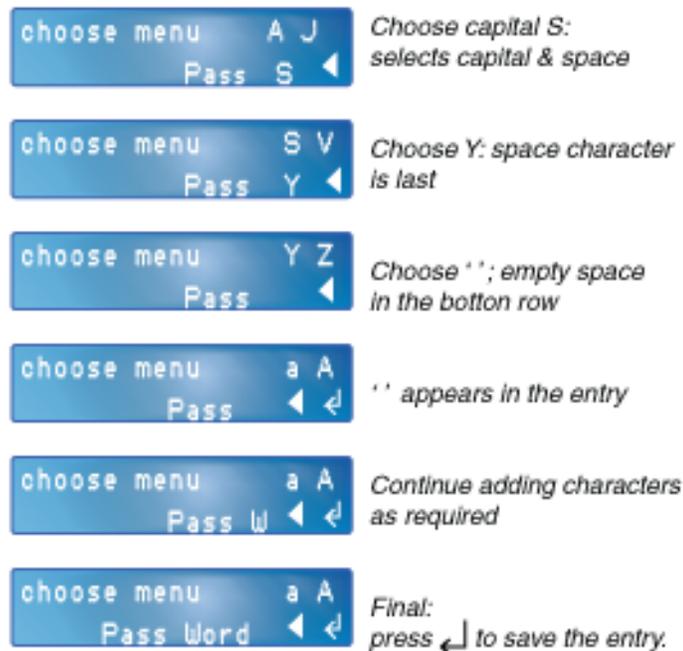


In the example figures, the password “Pass Word” is being created.

Start by entering the first half of the password. Follow the steps, illustrated in the graphic.



- 
- Step 1** Choose the capital 'A'; top right keypad button, to select capital letters.
- Step 2** Select 'J', top right button, as 'P' is between 'J' and 'S'.
- Step 3** Select the character 'P'; it appears in the entry, which puts you back at the start, to choose the next capital or small group of letters.
- Step 4** Repeat the process, narrowing the fields until you select each letter, continuing until you have "Pass"  
Next, you will need to enter a space, ' ', and then finish the password entry.



- Step 5** At the start screen, select capital letters.
- Step 6** Select 'S'; this select the last letters in the alphabet, and the space character.
- Step 7** Select 'Y'; this will bring up the space character.
- Step 8** Select the space character (bottom left button); a space will appear in the password entry.
- Step 9** Continue adding the rest of the password; the characters 'Word'.
- Step 10** Press OK (bottom right button) to confirm the entry.
- 

## Bootstrap: Management User Setup

The final stage of the bootstrap process is user setup. At least one user with the Manage Appliance role and at least one with the Manage PKI role must be created, either one user with both roles, or two users. As soon as these user roles are created the system will exit bootstrap mode.

If the system has previously been configured, and already has at least one user with the Manage Appliance role and one with the Manage PKI role, this step will be skipped.

Create new user accounts on the system using the Users option on the (Platform Management) menu. Click the + icon to add a new user to the system.

**Bootstrap: User Setup**

Manage Appliance user required.

User ID: Joe

Full Name: Joe Smith

Roles: Manage Policy, Manage Appliance, Auditor, Manage PKI

Password: [masked]

Confirm Password: [masked]

OK

Assign one or more roles to the user being created in the Roles section.

To assign more than one role, click on the first role, which will highlight the role, then hold down the CTRL key (Command key, for Mac users), and click on a second role, which will also be highlighted. Repeat this process until all the roles you wish the new user to have are highlighted. Click OK to create and add the new user to the system.

A user can change their own password at any time by logging on to the system and using the Change Password option on the User menu. The user menu is the menu at the top right of the screen under the user name.

## Configure IP Addresses with the WebUI

The easiest way to use the SSL Appliance is to allocate it a management IP address using DHCP. However, if a static or IPv6 address is required, you can configure it using the WebUI, once you have completed the bootstrap phase and accessed the appliance using a browser.

Once you are logged in, select (Platform Management) > Management Network, and edit the address(es) as required.

The SSL Appliance supports simultaneous access by both IPv4 and IPv6. If both IPv4 and IPv6 are disabled (Mode > Disable), access is only possible through the Command Line Diagnostics Interface (refer to “Command Line Diagnostics Interface” in the Cisco Administration and Deployment Guide) if this can be accessed directly from the console, or using the serial console.

### Configure a Static IP Address

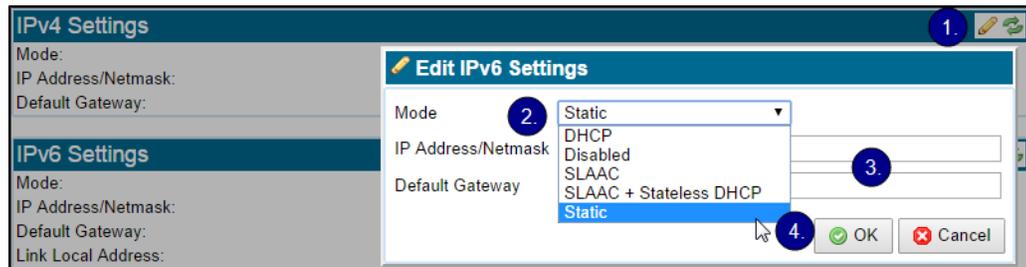
This section describes how to set a Static address. Once the update is complete, and the appliance has restarted, click Refresh in the page header to view the changes.

IP Address Format Notes

- Use the IP address/mask bits (CIDR) format to enter the IP address and netmask for all IP addresses.
  - IPv4 Example: 192.0.2.0/24

- IPv6 Example: 2001:db8::/24
- IPv6 addresses may be entered in full or collapsed form:
  - Full: FE80:0000:0000:0202:B3FF:FE1E:8329
  - Collapsed: FE80::0202:B3FF:FE1E:8329

Start at (Platform Management) > Management Network. Here is an overview of the process.



**Step 1** Click Edit (the pencil icon) on the appropriate IPvX Settings panel. The Edit IPvX Settings window opens.

**Step 2** On the Edit IPvX Settings window, select Static as the Mode.

**Step 3** Fill in the addresses.

**Step 4** Click OK. The window closes.

**Step 5** Click Apply on the Management Network window.

**Step 6** The appliance will restart.

### IPv4 Options

DHCP, Disabled, and Static are the IPv4 Mode options.

- When DHCP is selected, all other fields are grayed out.
- When Static is selected, enter the IP Address, Netmask, and Default Gateway addresses.

### IPv6 Options

DHCP, Disabled, SLAAC, SLAAC with stateless DHCP, and Static are the IPv6 Mode options.

- When DHCP, SLAAC, or SLAAC + Stateless DHCP are selected, all other fields are grayed out.
- When Static is selected, enter the IP Address, Netmask, and Default Gateway addresses.

The Link Local Address, if applicable, is automatically generated, and is the last display item in the IPv6 Settings panel.

Refer to the Cisco Administration and Deployment Guide for details on all of the settings.

## Configuring IPv4 Static with the LCD Screen

The easiest way to use the SSL Appliance is to allocate it a management IP address using DHCP. However, if a static IPV4 address is required, it can be configured by interrupting the start up sequence using the keypad sequence described in the Bootstrap States table, and then using the front panel keypad and LCD to configure the desired address. To configure a static IPv6 address, use a serial console or the WebUI once you are connected to it.

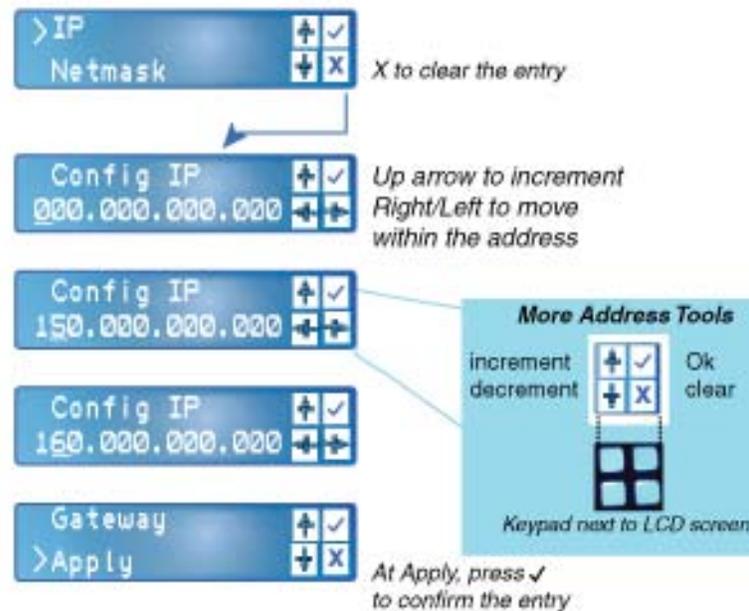
Once the IP Management screen appears, as shown in the figure, use the up and down arrows to select the item to be configured, then press the top right (check mark) button on the keypad to edit that item. You can see and edit the:

- IP address for the system
- IP Netmask for the system
- Gateway IP address for the system

After selecting an item to edit, use the left and right arrows to move within the configuration item. Use the up arrow to increment the value at the point where the cursor is located.

## Enter an IPv4 Address with the LCD Screen

**Step 1** Using the arrow keys, scroll to the IP screen to get started.



**Step 2** Select the IP item, and press OK (the check mark).

**Step 3** On the Config IP screen, you can press the X (lower left button) to clear the IP address, or you may simply start making changes. On entry to this screen the cursor is located under the leftmost digit in the address. The left/right arrow buttons will move the cursor.

**Step 4** The second screen in the figure shows the screen after the right arrow key has been used to move the cursor to underneath the numeral. Pressing the up arrow button at this point will cause the number above the cursor to be incremented, and the display will then appear as shown in the third screen.

**Step 5** Once all the changes to the IP address are complete, press the top right button (check mark) to exit back to the previous level in the menu, where you can select another element, such as Netmask, to configure.

**Step 6** Once all the elements have been configured, click Apply; this is the last option in the list of menu items.

## Complete System Configuration

The following steps are commonly performed once the system is out of the bootstrap phase:

**Step 1** Logging on.

**Step 2** Configuring the date and time.

**Step 3** Reviewing the system setup.

## Log On

Once the bootstrap phase is complete the full WebUI is available and can be used to configure the system. The WebUI is described in detail in the Administration and Deployment Guide. An HTTPS connection to the IP address assigned to the SSL Appliance management interface will produce the standard login box.

The SSL Appliance uses a self signed SSL server certificate which may result in a warning message from the browser when connecting to the WebUI. The warning can be prevented by adding this self signed certificate to your browser as a trusted device. Consult your browser documentation for details on how to add the SSL Appliance as a trusted device.

A screenshot of the Cisco login interface. At the top center is the Cisco logo, consisting of a stylized bridge icon above the word "CISCO". Below the logo are two input fields: "User ID" and "Password". Below the "Password" field is a "Login" button with a small icon of a person.

Log on using the username and password created in the initial configuration.

Use a web browser to login to the SSL Appliance at its IP address. IPv4 example: <https://192.168.2.42>.

Once you have logged on, see the top and bottom of the initial management Dashboard screen for important information. The top of the screen contains menus. The two menus on the right side have names that depend on the device name and the username.

For example your appliance might have a device name of “SSLAppliance.example.com,” and a username of the connected user of “support.”

The screenshot displays the configuration interface for a Cisco SSL Appliance. The top navigation bar includes 'Monitor', 'Policies', and 'PKI'. The user is logged in as 'admin' on the 'localhost' device. The interface is divided into several sections:

- Management Network:**
  - MAC Address: 00: [redacted]
  - MTU: 1500
  - Hostname: localhost
  - Primary Nameserver:
  - Secondary Nameserver:
- IPv4 Settings:**
  - Mode: DHCP
  - IP Address/Netmask: 192. [redacted] /24
  - Default Gateway: 192. [redacted]
- IPv6 Settings:**
  - Mode: DHCP
  - IP Address/Netmask: ::/0
  - Default Gateway:
  - Link Local Address: fe80::215:4dff:fe03:9f45/64
- IPv4 Access Control List:** A table with columns 'Address', 'Applies To', and 'Action'. It shows 1/1 entries.
- IPv6 Access Control List:** A table with columns 'Address', 'Applies To', and 'Action'. It shows 1/1 entries.

The footer of the interface displays the following information:

- Date and Time: 2015-11-02 20:44:20
- Software Version: 3.9.2.1-11
- Status Indicators: System: [green checkmark], Load: [green checkmark], Network: [green checkmark], License: [green checkmark]

The bottom of the screen (footer) contains status information on the device and shows:

- current date and time
- version of software running on the device
- status indicators for System, Load, Network, and License

The status indicators will change color if there are problems. The License status icon will be green. See “Licensing” on page 50 for further information.

As part of an initial configuration the following are typically configured:

- management settings
- time zone and use of NTP
- additional user accounts with relevant roles assigned to the user

See the next sections.

## Tool Icons

The SSL Appliance WebUI offers a number of tools in most WebUI windows, shown by icons or buttons in the upper right of the active window. Refer to this list if necessary when setting up the initial configuration.

Some tools are used to perform different but related functions in different screens. Here are the mostly commonly available tools.

**Table 1-9**      **Tool Icons**

Icon	Function
	Add; a new rule, list, or similar
	Generate a new Certificate
	Export; data, a certificate, a file, and so on
	Delete highlighted item
	Error
	Start; begin a download, install a certificate, and so on
	Refresh
	Move to the first/last/next/previous page
	OK, approve
	Manually unplug, connect
	Manually plug, disconnect

## Date and Time

To configure the system date and time, use the Date/Time item in the device (Platform Management)> menu. Initially, this menu will be labeled “localhost.localdomain”.

Click the Edit pencil icon at the top right of the Date/Time window to edit these settings.



- 
- Step 1** Click Edit in the header. The Edit Date/Time window pops up.
  - Step 2** Enter the correct data for your time and location.
  - Step 3** Click OK.
- 

If NTP is enabled, the Date and Time fields will be disabled, as these values are being set by the Network Time Protocol (NTP). In order for NTP to operate you need to configure a primary NTP server and ideally a secondary NTP server. Up to eight NTP servers may be configured. See the Cisco Administration and Deployment Guide for details on setting up NTP servers.

Once the settings are configured and OK is clicked to save the settings, the screen will refresh.

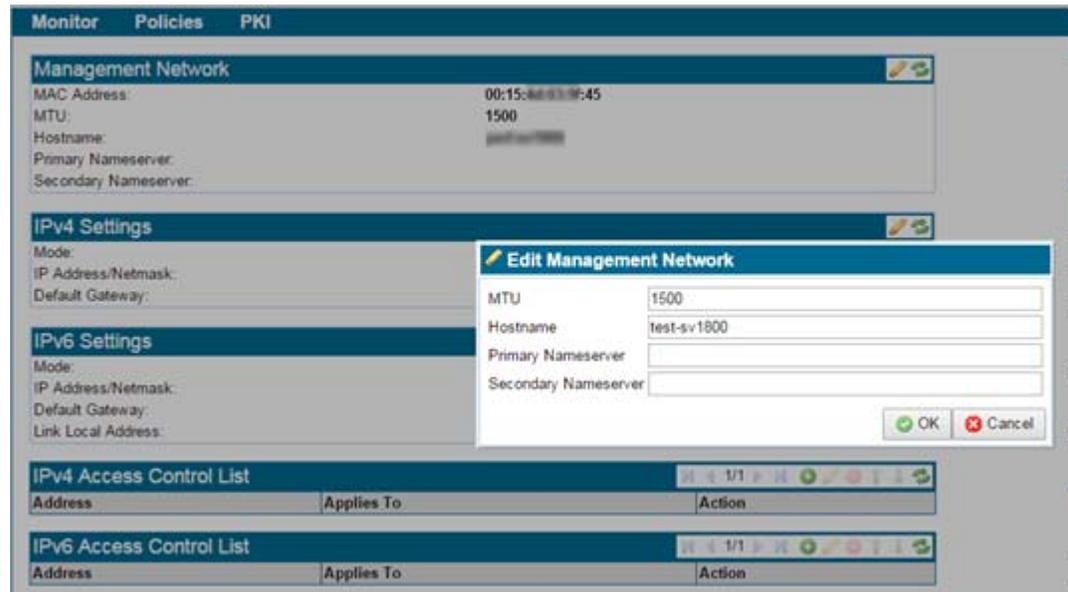
If you have changed the date, time, NTP, or timezone, you must select Apply at the “Platform Config Changes” message which appears at the bottom of the screen.

When you make changes to the Date or Time settings, click Reboot on the Date/Time window in order to reboot the appliance and apply the changes.

## Complete System Settings

Once you have logged on and configured the date and time, you will want to review and possibly update the system settings.

To configure system settings, use the (Platform Management) (system name) > Management Network menu. Change the name (hostname) of the system, edit the IP address (see “Configure IP Addresses with the WebUI”) and so on. Refer to the Cisco Administration and Deployment Guide for details on all of the settings.



**Step 1** Click Edit in the Management Network header. The Edit Management Network window opens.

**Step 2** Make your changes.

**Step 3** Click OK.



**Note**

If you need to configure SNMP, refer to the Cisco SSL Appliance Administration & Deployment Guide for details.

## Power Off

The SSL Appliance may be powered off several different ways:

- Use the CLD command `platform halt`.
- Use the WebUI process: (Platform) > Halt/Reboot > Halt.
- Hold down power button for 3 to 5 seconds.
- Unplug the power cable.



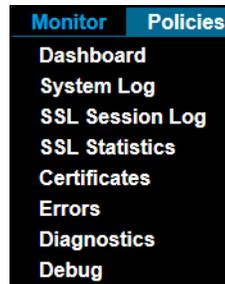
**Note**

Wait at least five seconds between disconnecting and reconnecting power supply cables.

# Monitor the System

Once you have configured the system and logged in, you can perform all of the SSL Appliance functions. Use the Monitor menu, on the left side of the header in the WebUI, to see how the system is performing as well as collect diagnostic and debug information.

Only the Dashboard, SSL Session Log and SSL Statistics are described in this document. For more details on monitoring options (and segments and rules) consult the Cisco Administration and Deployment Guide.



**Dashboard:** View the overall system status and the status of network links and active segments.

**SSL Session Log:** View details of SSL traffic that is passing through the SSL Appliance using the session log.

**SSL Statistics:** View statistics on SSL traffic that is passing through the SSL Appliance.

## Dashboard

The Dashboard displays several panels containing different types of information.

The **Front Panel** shows the appliance model and the status of configured interfaces, including their Segment IDs.



View the status of currently active segments on the **Segment Status** panel.

Segment ID	Main Interfaces	Copy Interfaces	Interfaces Down	Main Mode	Failures
A	1, 2	3		Passive-Inline	
B	5, 6	4		Passive-Inline	

The **Segment ID** is a unique identifier that enables this segment to be distinguished from other segments that may be present in the system. The Interface numbers identify the physical ports that are being used by this segment. If any of the interfaces being used by the segment are currently down, the interface numbers will show in the Interfaces Down column. Main Mode indicates the operating mode of the segment, and the Failures column will record any failure details.

## Dashboard Tools

These tools are available in addition to Refresh.

Manually Unfail: Usually unavailable. It is active if the segment is in a failure mode that requires manual intervention to clear the failure.

Manual Fail tool: Active when a segment is selected. Use to force a segment into a failed state.

The Network Interfaces panel has a row for every interface installed in the system. Each row shows the interface Type and the speed it is operating at, along with transmit and receive statistics. The Refresh tool and Clear Counters tools are available.

Network Interfaces					
Port	Type	Link State	RX Packets/Bytes	TX Packets/Bytes	RX Drops
1	1G	1G	18864475/15662763383	19085341/14955569986	0
2	1G	1G	18967611/14946890174	18755544/15616215820	0
3	1G	Down	0/0	0/0	0
4	1G	Down	0/0	0/0	0
5	1G	1G	19955564/14931573650	15165425/15282183930	0
6	1G	1G	15165425/15282183930	19955571/14931563506	0
7	1G	Down	0/0	0/0	0
8	1G	Down	0/0	0/0	0

The possible statuses are:

- OK: Appears in green; working as expected.
- No Power: Appears in yellow. Verify the supply is plugged in.
- Failed: Appears in red. The causes may be... OVER\_TEMPERATURE, FAN\_FAILURE, OVER\_VOLTAGE, UNDER\_VOLTAGE...

CPU Load % shows the current CPU utilization as a percentage of the total capacity of the CPU. The Refresh tool is available.

CPU Load %																
cpu	cpu0	cpu1	cpu2	cpu3	cpu4	cpu5	cpu6	cpu7	cpu8	cpu9	cpu10	cpu11	cpu12	cpu13	cpu14	cpu15
0.2	1.2	0	2.9	0	0	0	0	0	0	0	0	0	0	0	1	0

The Fan Speed (RPM) panel shows the current speed values for the various fans in the system. The Refresh tool is available.

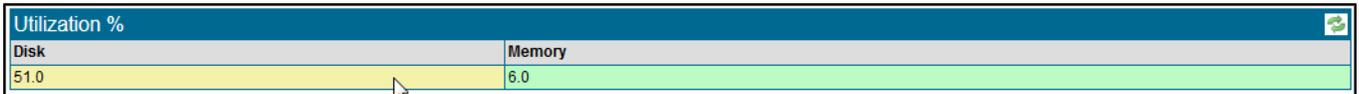
Fan Speed (RPM)						
Fan Mod 1 Inlet	Fan Mod 1 Outlet	Fan Mod 2 Inlet	Fan Mod 2 Outlet	Fan Mods 3 to 5	Left Power Supply Fan	Right Power Supply Fan
13276	11860	13876	11592	7237	13157	13157

The Temperatures panel includes details of temperatures and thermal margins for components within the system. The Refresh tool is available.

Temperatures (Degrees °C)									
Baseboard Temp	Front Panel Temp	IOH Therm Margin	Mem P1 Thrm Mrgn	Mem P2 Thrm Mrgn	P1 Therm Margin	P2 Therm Margin	NFP0 Temp	Left Power Supply Temp	Right Power Supply Temp
31	25	-43	-35	-48	-53	-60	54	37	41

Thermal margin sensors are reported as negative values which when increased to 0 will cause CPU to throttle down or halt

The Utilization panel shows the percentage utilization of system memory and disk space. The Refresh tool is available.



The System Log panel contains the most recently generated system log entries; this panel automatically refreshes.

Time	Process	Log
Jan 31 22:06:01	kernel	imklog 5.8.6, log source = /proc/kmsg started.
Jan 31 22:06:01	rsyslogd	[origin software="rsyslogd" swVersion="5.8.6" x-pid="667" x-info="http://www.rsyslog.com"] start
Jan 31 22:06:01	kernel	[ 0.000000] Initializing cgroup subsys cpuset

## SSL Session Log

View the last 64 pages of the SSL Session Log on the **SSL Session Log** window. The window offers an Export tool, and two filter tools, as well as the standard multipage navigation and Refresh tools.

The session log can be enabled on a per segment basis. Make sure that it is enabled on the segment you are trying to see details for.



**Note**

You must configure a segment in order for the SSL Session Log to be populated with session data. Refer to the SSL Appliance Administration & Deployment Guide for information about configuring segments.



**Note**

The Session Log can be enabled on a per segment basis. Make sure that it is enabled on the segment you want to inspect.

Start Time	Segment ID	SrcIP:Port	DstIP:Port	Domain Name	Certificate Status	Cipher Suite	Action	Status
Mar 18 22:37:07.723	A	24.154.127.184:33387	23.210.249.115:443	sb.monetate.net	Valid	TLS_RSA_WITH_AES_256_CBC_SHA	Cut Through	Success
Mar 18 22:36:07.825	A	24.154.127.184:51898	74.125.28.104:443	Multiple domains	Valid	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Cut Through	Success
Mar 18 22:29:25.054	A	24.154.127.184:33383	23.210.249.115:443	Multiple domains	Valid	TLS_RSA_WITH_AES_256_CBC_SHA	Cut Through	Success
Mar 18 22:29:18.565	A	24.154.127.184:33382	23.210.249.115:443	Multiple domains	Valid	TLS_RSA_WITH_AES_256_CBC_SHA	Cut Through	Success
Mar 18 22:28:49.863	A	24.154.127.184:33381	23.210.249.115:443	Multiple domains	Valid	TLS_RSA_WITH_AES_256_CBC_SHA	Cut Through	Success
Mar 18 22:28:36.421	A	24.154.127.184:51533	173.194.46.52:443	Multiple domains	Valid	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Cut Through	Success
Mar 18 22:28:18.818	A	24.154.127.184:33379	23.210.249.115:443	Multiple domains	Valid	TLS_RSA_WITH_AES_256_CBC_SHA	Cut Through	Success
Mar 18 22:27:37.563	A	24.154.127.184:51891	74.125.28.104:443	Multiple domains	Valid	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Cut Through	Success
Mar 18 22:25:07.776	A	24.154.127.184:52072	74.125.28.105:443	Multiple domains	Valid	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Cut Through	Success
Mar 18 22:24:15.029	A	24.154.127.184:59475	74.125.28.106:443	Multiple domains	Valid	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Cut Through	Success

The SSL Session Log includes the following details for each SSL session that is recorded in the log:

- Start date and time
- Segment ID for the segment the SSL session occurred on
- IP source and destination address and port number
- Domain details from the server certificate used during the session

- Status of the server certificate
- Cipher Suite that was used for the session
- Action taken by the SSL Appliance for this session
- Status for the session

Entries in the **SSL Session Log** are ordered from most recent to oldest. Hence, the first row on page 1/64 is the most recent entry, and the last row on page 64/64 is the oldest entry.

Use the Filter on Errors tool to have the log display only entries for flows that were not inspected successfully. Use the No Filter tool to revert the log to showing all entries.

The View Details tool ( ) is only active when a row in the SSL Session Log panel has been selected. Clicking the View Details tool will open up a dialog box showing more details for the selected session.



## SSL Statistics

View the last 64 pages of the SSL Statistics log on this window. The panel has the standard multipage navigation tools as well as a Clear Statistics tool.

SSL Statistics								
Timestamp	#Detected	#Done	#Ignored	#Decrypt	#Decrypt Done	#Error	Detected	Decrypt
Feb 12 14:19:05	13361	13301	809	11474	11418	18	60	56
Feb 12 14:19:04	13361	13300	809	11473	11417	18	61	56
Feb 12 14:19:03	13359	13299	809	11472	11416	18	60	56
Feb 12 14:19:02	13357	13297	809	11470	11414	18	60	56
Feb 12 14:19:01	13357	13297	809	11470	11414	18	60	56
Feb 12 14:19:00	13356	13296	808	11470	11414	18	60	56
Feb 12 14:18:59	13352	13294	808	11466	11412	18	58	54
Feb 12 14:18:58	13351	13293	808	11465	11411	18	58	54
Feb 12 14:18:57	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:56	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:55	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:54	13351	13277	808	11465	11395	18	74	70
Feb 12 14:18:53	13350	13276	808	11464	11394	18	74	70
Feb 12 14:18:52	13349	13275	808	11463	11393	18	74	70
Feb 12 14:18:51	13349	13275	808	11463	11393	18	74	70
Feb 12 14:18:50	13349	13275	808	11463	11393	18	74	70

In this example, page 1 of the 64 pages of statistics information is displayed. Statistics are collected each second, and each row in the table holds the data for a collection interval. All counts are cumulative, except for in the **Detected** and **Decrypted** columns, which show the instantaneous number of sessions in each category at the point the data was collected. This is not the total number of sessions that may have been in that category over the one second period.

Entries in the Statistics panel are ordered from most recent to oldest. So, the first row on page 1/64 is the most recent entry, and the last row on page 64/64 is the oldest entry.

## Configure PKI

This section details how to set up a known server key and certificate on the system. It is assumed that a local SSL server is available, and that a copy of the private key and SSL server certificate are available.

- “Install a CA Cert for Certificate Resign” on page 57
- “Import Known Server Key” on page 59

## Install a CA Cert for Certificate Resign

Before the SSL Appliance can be used to inspect traffic using Certificate Resign mechanisms, it must have at least one CA certificate and private key installed to do the resigning. A CA can either be created by the SSL Appliance and self signed or sent off for signing by another CA), or it can be imported. Use the Resigning Certificate Authorities option on the PKI menu for the management of INternal Certificate Authorities.

It is assumed in this process that a local SSL server is available, and that a copy of the private key and SSL server certificate are available.

The icons at the top right of the window allow you to:

Generate a new Resigning Certificate Authority



Add a Resigning Certificate Authority by importing an existing CA and key.



Export a Certificate



## Generate a Resigning Self Signed Certificate

The simplest approach is to generate a self signed CA certificate. Here is a panel before any certificates have been added.



**Step 1** Click.



**Step 2** The Generate Certificate window appears. Use it to input the basic data required in a CA, as well as specify the key size and validity period.

**Step 3** Click the Generate self-signed CA button.

**Step 4** As this CA is self-signed, it will not be trusted by a client system until it has been exported and added to the list of trusted CAs on the client system.

**Step 5** Click the OK button, and the certificate is saved and installed. An entry in the Internal Certificate Authorities table appears with an indication that no CSR has been generated for this certificate.

**Step 6** To download the CA certificate so you can install it on the client system, click to select the entry, then click on the Export certificate button.

**Step 7** Consult your browser documentation for details on how to add this CA to the browsers list of trusted CAs.

## Import Known Server Key

To inspect traffic to an internal SSL server, the easiest approach is to use known server key and certificate mode which requires that a copy of the server's SSL certificate and private key are loaded into the SSL Appliance.

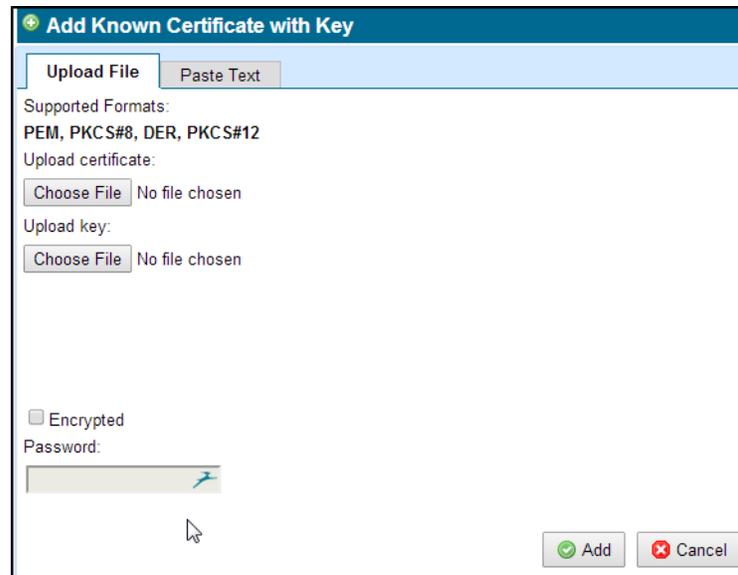
Known server certificates and keys are imported into the all-known-certificates-with-keys list. The Known Certificates and Keys option on the PKI menu is used to import new certificates and keys.

There are two panels, one for choosing the list that is to be operated on, and the other to manipulate the contents of that list. In this example the key/certificate will be added to the all-known-certificates-with-keys list.

**Step 1** Load the key/certificate for each local SSL server that you wish to inspect traffic to.



**Step 2** Click to select the all-known-certificates-with-keys list, then click the Add button. The Add Known Certificate with Key window opens.



**Step 3** You can then either specify the file to import (Upload File) or paste in the key and certificate details (Paste Text), and then click the Add button.

**Step 4** If the key and certificate are valid then a message confirming that the Certificate has been added will appear with a button that allows you to view the details of the imported certificate. You will also see that the key now appears as a row in the Known Certificate with Keys window.

**Step 5** Click Apply to save the imported certificates and keys to the secure store.



**Step 6** From here, use the See the Cisco Administration & Deployment Guide for information on deployments and all appliance functions. Download the manual from BlueTouch Online.

## Getting Help

Thank you for choosing the Cisco SSL Appliance.

Thank you for choosing the Cisco SSL Appliance.

### Cisco Support

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco SSL Appliances, see **What's New in Cisco Product Documentation** at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to **What's New in Cisco Product Documentation**, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions or require assistance with the Cisco SSL Appliance, you can also contact Cisco Support:

- Visit the Cisco Support site at <http://support.cisco.com/>.
- Email Cisco Support at [tac@cisco.com](mailto:tac@cisco.com).
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.