Cisco SSL Appliance 2000-8200 Getting Started Guide

Version 3.8
November 11, 2014

Cisco Systems, Inc.
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.

Version 3.8
November 11, 2014 i

Introduction

Revised: June 23, 2014

Introduction

This guide describes how to get started using the Cisco 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 Cisco SSL Appliance is capable of inspecting both types of traffic.

Caution The embedded software contained within the Cisco SSL Appliance is subject to licensing terms and conditions imposed by Cisco, and third party software providers. You should only use the Cisco SSL Appliance if you agree to these licensing conditions; see the Cisco SSL2000 and SSL8200 Administration and 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 Cisco SSL Appliance is in accordance with any such legal or policy requirements.

The Administration & Deployment Guide for the platforms provide full details on all of the options available in the Cisco 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 SSL1500 Quick Start Guide; see for initial setup information

- Cisco SSL1500 Administration and Deployment Guide, Version 3.8.x and Cisco SSL2000 and SSL8200 Administration and Deployment Guide, Version 3.8.x; 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

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" indicating information warning the reader of potential bodily harm.**

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 Cisco SSL Appliance. Read the separate Safety Notice included in the Cisco 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.**

Unpacking the Cisco SSL2000 or SSL8200

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 Packing List

Part	Description	Quantity
Cisco SSL2000 or SSL8200 appliance	1U or 2U rack mountable device	1
2 x Power Cords	One for each redundant supply	2
Rack mounting rails	Rails to rack mount the device	1
Number of Components		4

SSL2000 and SSL8200 Specifications

Where hardware or software features differ between the two models the features for each product will be shown separately. Any features not explicitly identified as relating to only one model apply to both products, including Netmod information.

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 Cisco SSL Appliance Comparison

Measurement	SSL2000	SSL8200
Total Packet Processing Capacity	20 Gbps	40 Gbps
SSL Inspection Throughput	2.5 Gbps	4 Gbps
Cut through latency	<40 uS	<40 uS
Concurrent SSL flows being inspected	200000	400000
New full handshakes/Second 1024 bit key	10500	12500
New full handshake/Second 2048 bit key	3000	6000

Table 1-3 SSL2000 Specifications

Category	Description
Chassis Dimensions	17.2" (W) x 19.2" (D) x 1.73" (H) (433mm x 728mm x 44mm)
Weight	43.5 lbs (19.8 kg)
Processors	2 x Intel Xeon E5645 hex core CPUs
System memory	24 GB DDR3
Network Flow Engine (NFE)	1 x NFE-3240 card (NFP-3240 + 4 GB DDR3 + PCIe gen2 x8)
Network Module slots (Netmods)	3 x Netmod slots
Supported Netmod types	all Netmods have fail to wire/open capabilities 4 x 10/100/1000 fiber 2 x 10G fiber 4 x 10/100/1000 copper
Network Management interfaces	2 x 10/100/1000 copper interfaces on rear panel
Integrated Display	16 character by 2 line LCD on front panel
Power Supplies	2 x 750W redundant hot swap power supplies
Operating Temperature	5°C to 40°C
Storage Temperature	-10°C to 70°C
Cooling	Generates up to 2225 BTU/hour worst case
Air flow	210 ft3/min (6m3/min)

Table 1-4 SSL8200 Specifications

Category	Description
Chassis Dimensions	17.2" (W) x 19.0" (D) x 3.48" (H) (433mm x 735mm x 88.2mm)
Weight	58 lbs (26.4 kg)
Processors	2 x Intel Xeon E5645 hex core CPUs
System memory	48 GB DDR3

Table 1-4 SSL8200 Specifications

Category	Description
Network Flow Engine (NFE)	2 x NFE-3240 card (NFP-3240 + 4GB DDR3 + PCIe gen2 x8)
Network Module slots (Netmods)	7 x Netmod slots (recommended system limit is a total of 16 interfaces)
Supported Netmod types	all Netmods have fail to wire/open capabilities: 2 x 10G fiber 4 x 10/100/1000 fiber 4 x 10/100/1000 copper
Network Management interfaces	2 x 10/100/1000 copper interfaces on rear panel
Integrated Display	16 character by 2 line LCD on front panel
Power Supplies	2 x 750W redundant hot swap power supplies
Operating Temperature	5°C to 40°C
Storage Temperature	-10°C to 70°C Cooling generates up to 2225 BTU/hour worst case
Air flow	210 ft3/min (6m3/min)

SSL2000 Front Panel

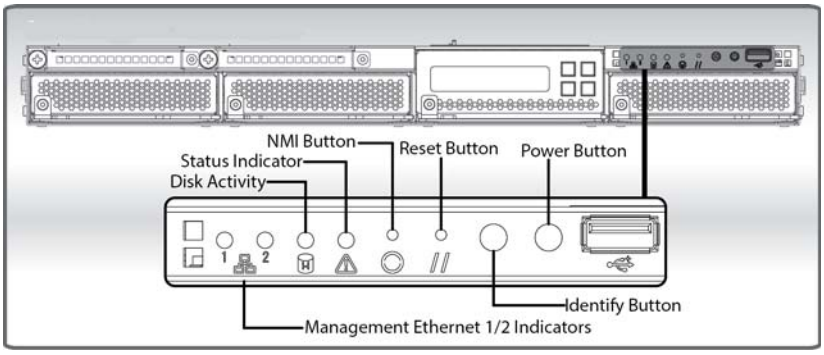
The SSL2000 has three front facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Up to 12 GigE or up to 6 10 GigE interfaces can be installed. See Front Panel LEDs, page 1-9 for information on LED indicators.

This example shows the front panel of an SSL2000 with 12 GigE copper interfaces.

The front panel has indicators, buttons, and an LCD display with keypad buttons corresponding to the rightmost locations on the LCD screen.

Figure 1-1 LCD and Keypad

Figure 1-2 Front Panel and Indicators

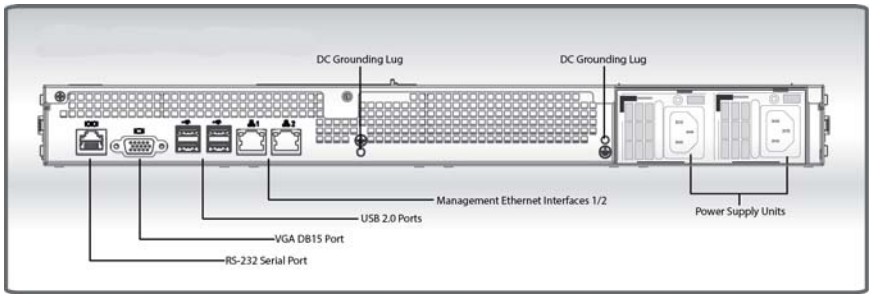


Netmods are docked into the remaining bays. See Netmods, page 1-11 for more information on working with Netmods.

Netmods are NOT hot swappable, and should only be swapped when the system is powered off.

SSL2000 Back Panel

The back panel connectors on the SSL2000 are shown next.



Ventilation holes on the back panel must not be blocked as free flow of air is essential for system cooling.

DB15

Connect to a VGA display

Serial Port

Access an SSH or serial console, to connect to the Command Line Diagnostic interface. See the Cisco SSL2000 and SSL8200 Administration and Deployment Guide for all of the commands. The serial RS-232 console has a male DB-9 connector.

USB Ports

Use to:

- Connect a USB keyboard to use with a VGA keyboard for console access
- Insert a USB drive with part of the key chain required to unlock the appliance during the boot sequence, if USB was selected in the bootstrap process.

Note You cannot save data from the appliance to a USB drive.

Power Supplies

The Cisco SSL Appliance 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).

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

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

SSL8200 Front Panel

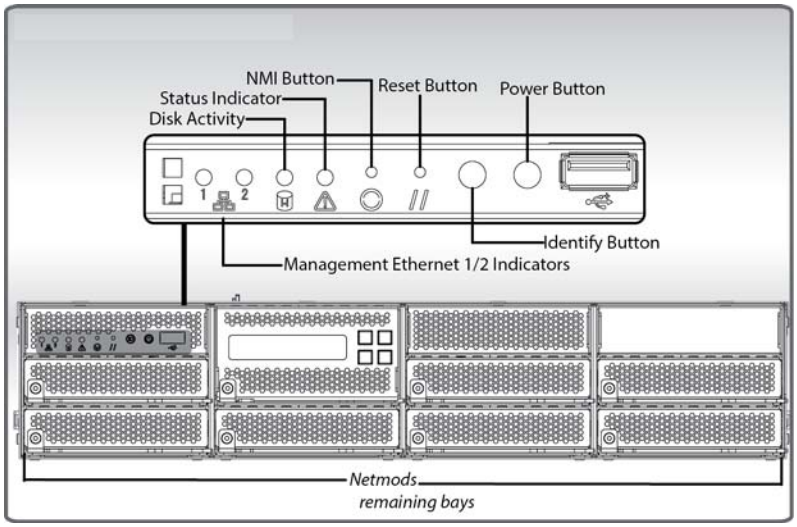
The SSL8200 has seven front facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the seven bays to configure the desired combination of interfaces.

Cisco recommends restricting an SSL8200 to supporting a maximum of 16 external interfaces. This means that if 4 x GigE Netmods are used a maximum of four can be installed in the system.

In this example, two of the Netmods each support 4 x GigE fiber interfaces, and the other two 4 x GigE copper interfaces. The front panel has indicators, buttons, and an LCD display with keypad buttons corresponding to the rightmost locations on the LCD screen.

Figure 1-3 LCD Screen and Keypad

Figure 1-4 Front Panel and Indicators



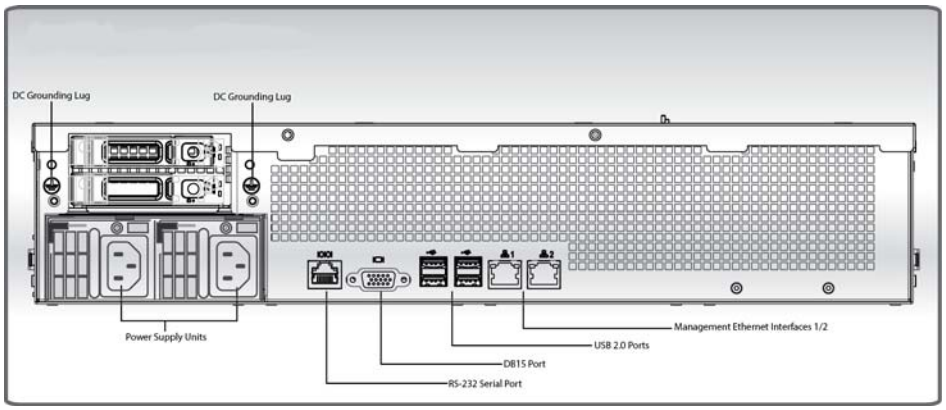
See Front Panel LEDs, page 1-9 for information on LED indicators.

Netmods are docked into the remaining bays. See Netmods, page 1-11 for more information on working with Netmods.

Netmods are NOT hot swappable, and should only be swapped when the system is powered off.

SSL8200 Back Panel

The back panel connectors on the SV800 are shown next. Ventilation holes on the back panel must not be blocked as free flow of air is essential for system cooling.



DB15

Connect to a VGA display

Serial Port

Access an SSH or serial console, to connect to the Command Line Diagnostic interface. See the Cisco SSL2000 and SSL8200 Administration and Deployment Guide for all of the commands. The serial RS-232 console has a male DB-9 connector.

USB Ports

Use to:

- Connect a USB keyboard to use with a VGA keyboard for console access
- Insert a USB drive with part of the key chain required to unlock the appliance during the boot sequence, if USB was selected in the bootstrap process.

Note You cannot save data from the appliance to a USB drive.

Power Supplies

The Cisco SSL Appliance 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).

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

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

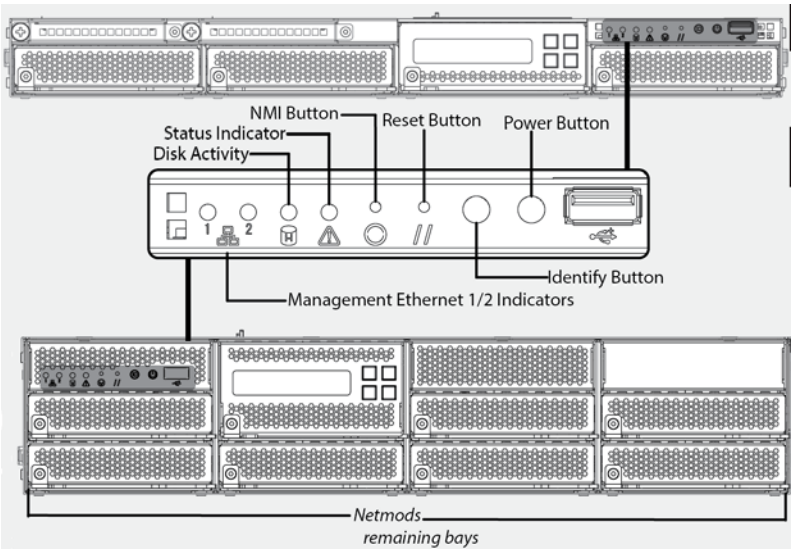
SSL2000 & SSL8200 Physical LEDs and Buttons

This section describes the LEDs and buttons on the front of the Cisco SSL Appliance.

Front Panel LEDs

The front panel LEDs for the rear panel Management Ethernet ports are green when the link is up, and flash amber/yellow to indicate traffic flowing over the link.

The two LEDs that are part of each Ethernet port on the rear panel indicate the operating speed of the link and if data is flowing over the link.



- The left LED viewed from the back of the unit is green if the link is up and flashes to indicate traffic flow.
- The right LED can be: off (10 Mbps connection), green (a 100 Mbps connection) or amber (a GigE connection).

The disk activity LED is green and flashes when there is any disk activity on a SATA port in the system.

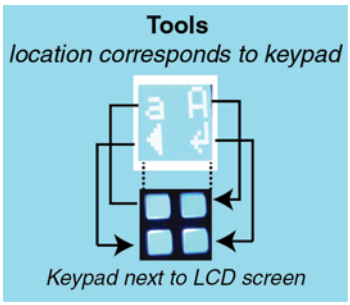
The system status LED is green/amber, and the various display options indicated different system states. The table shows the various system states that can be indicated by the system status LED on the front panel of the unit.

Table 1-5 SSL2000 & SSL8200 System Status Indications

Color	State	System Status	Meaning
Green	Solid	OK	System ready – no errors detected
Green	Blink	Degraded	Memory, fan, power supply or PCIe failures
Amber	Solid	Fatal	Alarm – system has failed and shut down
Amber	Blink	Non-Fatal	Alarm – system likely to fail – voltage/temp warnings
Green + Amber	Solid	OK	First 30 seconds after AC power connected
None	Off	Power off	AC or DC power is off

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 check mark and X (done/exit) appear in the inner/left positions.



The NMI and Reset buttons are recessed, requiring the use of a straight thin object to press the button.

- Reset: Reboot the appliance if required. Use this button rather than power cycle the appliance.
- NMI: Don't press NMI during normal operation as it may cause the system to halt. If the NMI button is used, this fact will be recorded in the system log file.
- ID: The ID button causes a blue LED on the rear panel to the left of the serial port to illuminate. The purpose of this LED is to make it easier to locate a system when it is racked in a stack with other systems.

Netmods

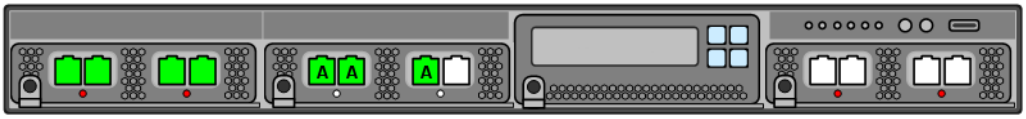
About Netmods

The SSL2000 and SSL8200 products have front facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the bays to configure the desired combination of interfaces, as shown on the SSL2000 front panel and the SSL8200 front panel. Netmod options are listed below. Other Netmod types may become available in the future:

- 4 x GigE copper (4 ports of 10/100/1000Base-T with bypass)
- 4 x GigE fiber (4 ports of 10/100/1000Base-SX with bypass)
- 2 x10Gig fiber (2 ports of 10GBase-SR with bypass)
- 2 x10Gig fiber (2 ports of 10GBase-LR with bypass)

Ports are numbered from left to right and top to bottom when facing the front of the device.

When a segment is configured and activated, the port numbers allocated to that segment are displayed on the management WebUI. Segment A is configured in the figure.



The relevant ports will need to be connected to the network and associated security appliance(s) using appropriate copper or fiber cabling.

Ports are grouped into pairs. Each odd numbered port is in a pair with the even numbered port. “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.

Changing Netmods

Netmods are NOT hot swappable and should only be swapped when the system is powered off.

When the power is off, a Network Module, or the blank plate covering an empty position, may be removed by removing the screw on the front panel (M3×4mm, T8 flat head, black) and pulling the lever out. There is a hole that can be used to pull on the ejector handle.

When the power is off, the Network Modules may be installed as follows:

Step 1 Power off the appliance.

Step 2 The Network Module ejector is held in by a screw; remove the screw.

Step 3 Pull out the ejector handle until it is approximately 25mm (1") from the front panel.

Step 4 Insert the Network Module into the empty slot until the protrusion on the right side touches the chassis.

Step 5 Gently press on the ejector handle where the screw normally is, and push the module into the chassis.

Step 6 Make sure the seating plane of the front of the network module is lined up with other modules. It may be necessary to push on the front of the module to fully seat it. If the module cannot be fully seated, try reinserting it, paying attention to the retention mechanism on the right side of the module.

Step 7 Install the screw.

SSL2000 and SSL8200 Installation

The Cisco 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

The Cisco SSL Appliance is equipped with pre-installed rack-mount brackets and supplied with rack mount rails allowing easy installation in a rack.

If the Cisco 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 specified for the appliance.
- 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.

SSL2000

- At least 1U rack space (deep enough for a 27" device); power and management ports at rear
- Phillips (cross-head) screwdriver
- Two available power outlets (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
- Cooling for an appliance with two 650W power supply units
- One RJ-45 CAT5e/CAT6 Ethernet cable to connect the Cisco SSL Appliance to the management network (or a local notebook/desktop computer which is used to manage the Cisco SSL Appliance)
- Appropriate copper or fiber cables to connect Netmods to the network and to associated security appliances
- The information sheet provided with the rails.

SSL8200

- At least 2U rack space (deep enough for a 27" device); power and management ports at rear
- Phillips (cross-head) screwdriver
- Two available power outlets (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
- Cooling for an appliance with two 750W power supply units
- One RJ-45 CAT5e/CAT6 Ethernet cable to connect the Cisco SSL Appliance to the management network (or a local notebook/desktop computer which is used to manage the Cisco SSL Appliance)
- Appropriate copper or fiber cables to connect Netmods 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 SSL2000 & SSL8200

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 back panel of the appliance. See SSL2000 Back Panel, page 1-6 and SSL8200 Back Panel, page 1-8.

Check that the LEDs on the port indicate that the link is up:

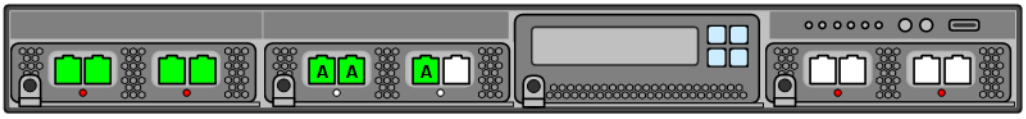
- To use the WebUI for the initial configuration, see Power On and Initial Configuration - WebUI, page 1-21.
- To use a console connection for the initial configuration, see Console Configuration, page 1-14.

Connect to the Network and Attached Appliances

The SSL2000 and SSL8200 products have front facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (“Netmods” on page 20) are installed in the bays to configure the desired combination of interfaces. See SSL2000 Front Panel, page 1-5 and SSL8200 Front Panel, page 1-7.

See the Cisco SSL2000 and SSL8200 Administration and Deployment Guide for deployment information.

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



Console Configuration

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

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

Step 1 Connect the Management Ethernet port. HTTPS access to the Cisco 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 - WebUI, page 1-21 to use the WebUI rather than a serial connection, and for more information about the bootstrap states and the master key mode.

Connecting to the Console

The console port on the Cisco 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 Diagnostic CLI which is also accessible via SSH.

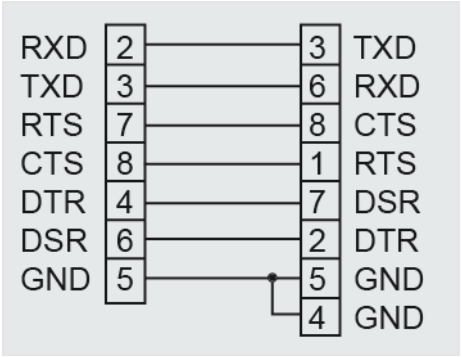
The serial connection on the appliance is configured as:

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

SSL2000/SSL8200 Pin-Outs

The console interface for the SSL2000 and SSL8200 requires a special cable that connects the console port to the DB9 communications port of a PC.

The pin-out for a serial cable is shown in the table.

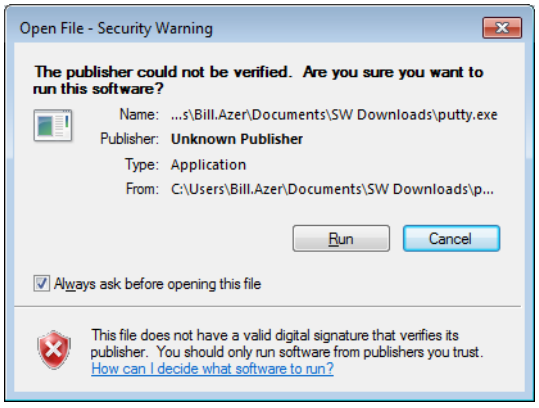


Configuring Putty for the Console Connection

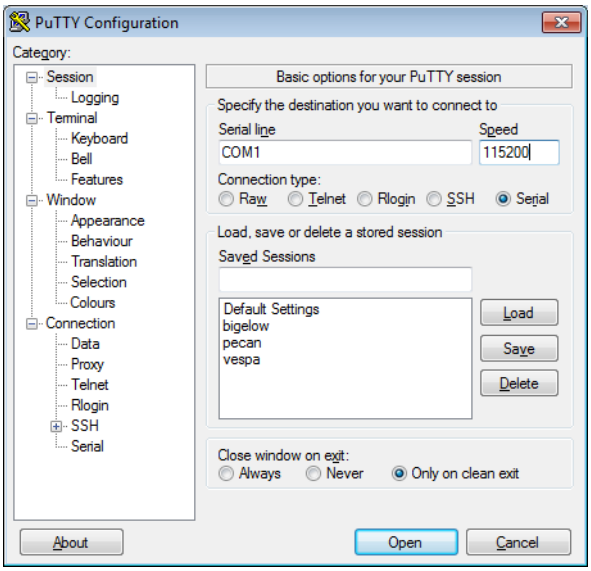
The following steps detail the console configuration as connection with the Putty client.

Step 1 Download Putty client (from the Putty download site).

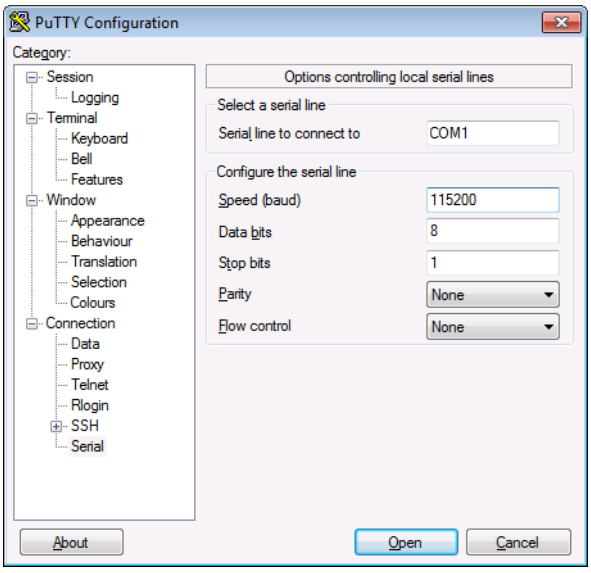
Step 2 Run the Putty Client.



Step 3 Configure Putty to use a serial connection at 1152300.



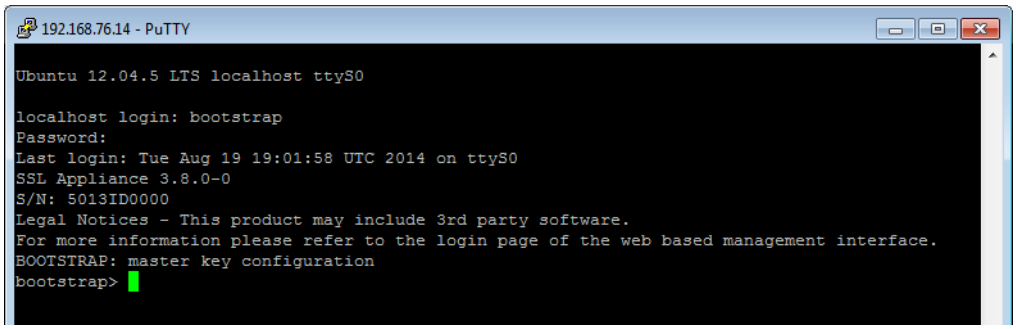
Step 4 Configure the serial connection to support the Cisco SSL Appliance's console speeds.



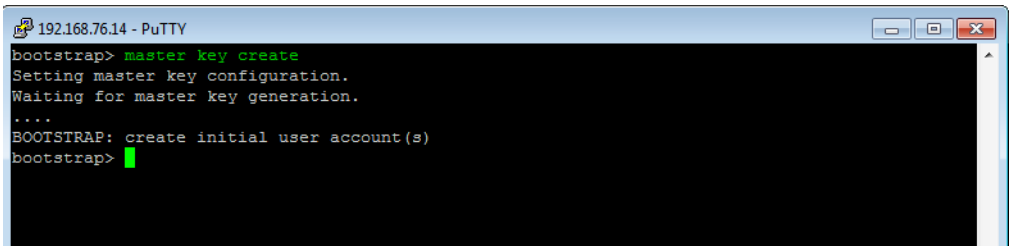
Configure the Cisco SSL Appliance

The SSLV 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).

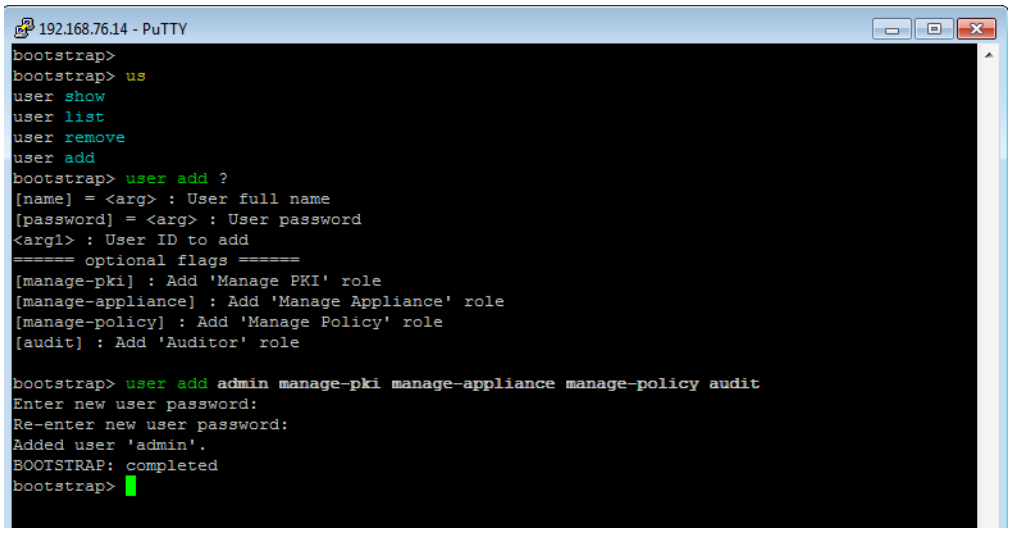
Step 1 Connect to the appliance, and login using the bootstrap user (the password is “bootstrap” as well).



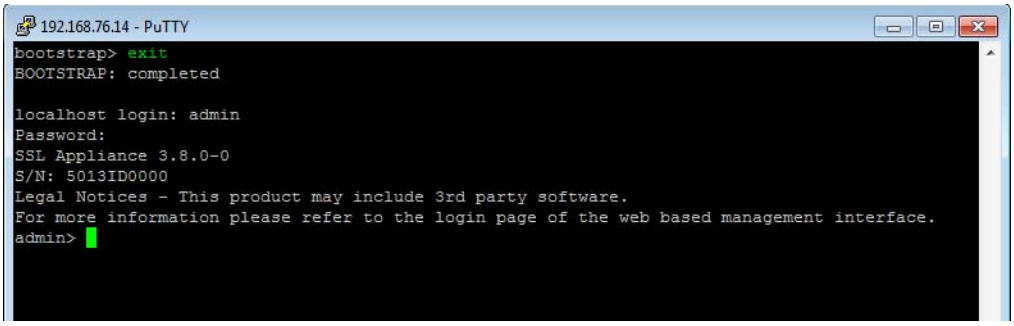
Step 2 Create the master key next. This example assumes that the master key is not being stored on a USB stick, and that no front panel password is required to unlock the secure store during boot. Commands are provided to allow one or both of these options to be set before the master key is created.



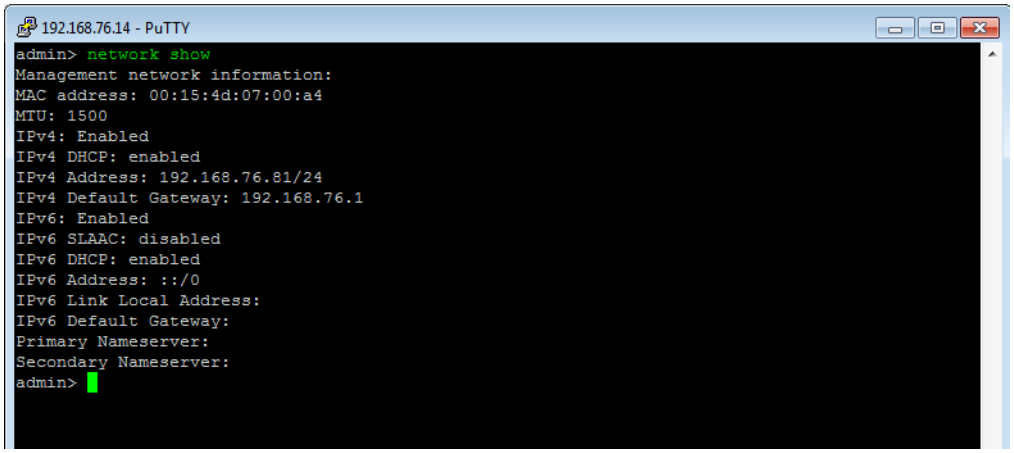
Step 3 Configure an Admin user with the administrator options, and enter the password when prompted. This example creates a single admin user account that has all four roles allocated to it. The only requirements for completing the bootstrap phase is that there is a user account with the Manage Appliance 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.



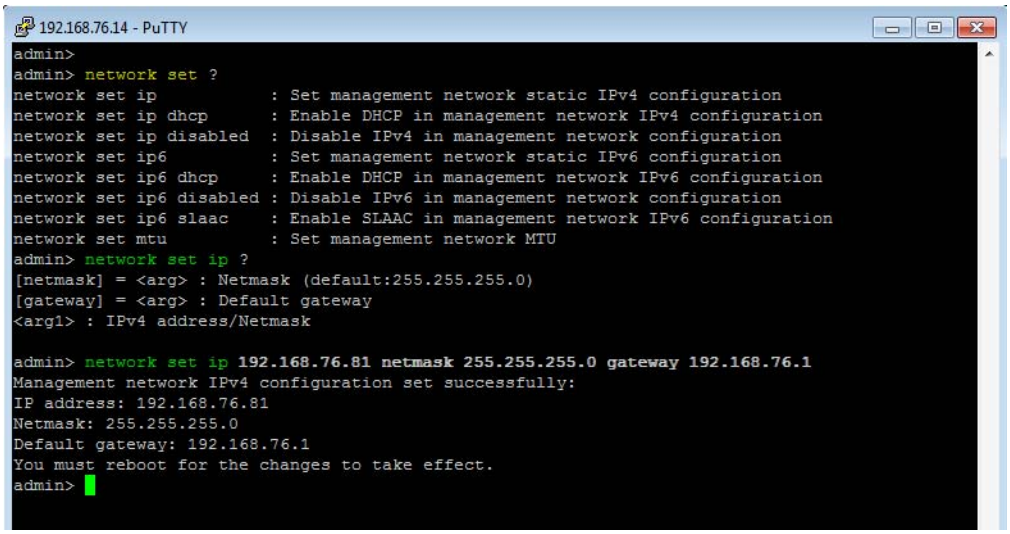
Step 4 Logout as the bootstrap user, then log back in as the newly created admin user.



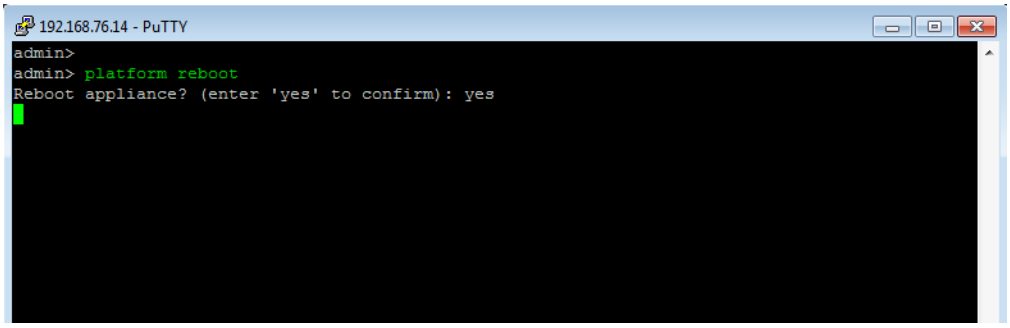
Step 5 The current (default) network setting is for DHCP. The settings are displayed by using the "network show" command.



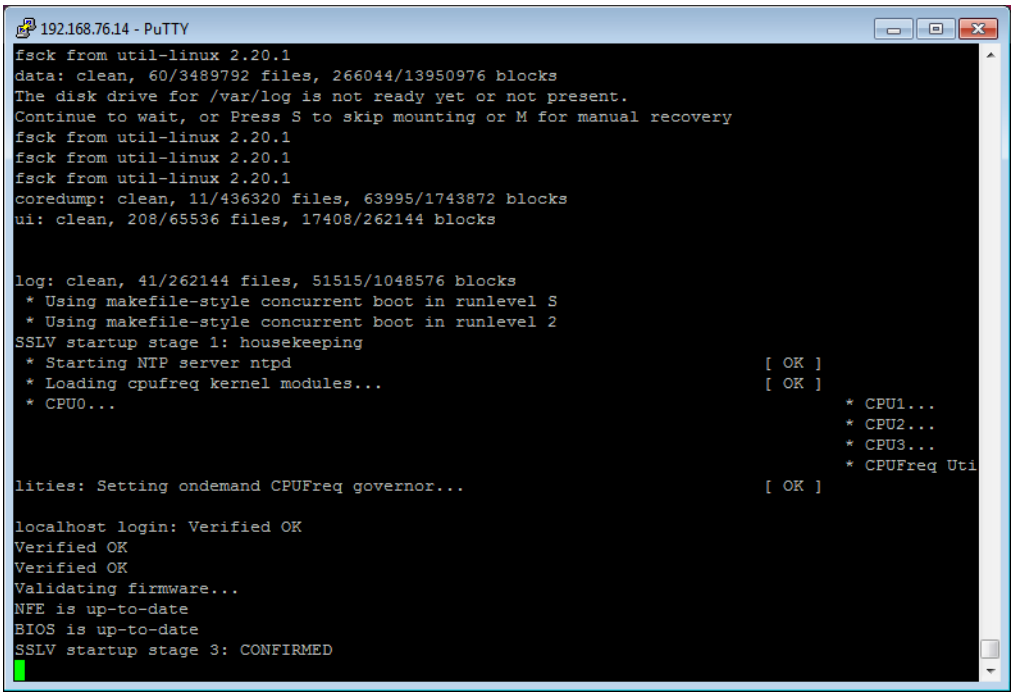
Step 6 To configure the network interface with a static IP address, use the "network set ip" command with applicable parameters. See also Update the IP Using a Serial Console, page 1-20.



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



Step 8 On reboot, confirm that the “SSLV startup stage 3: CONFIRMED” is displayed.



Step 9 Confirm that you can log in to the appliance via your browser. Log on via a web browser, using the format https://<ip address>. Log in with the username and password you created.

Update the IP Using a Serial Console

The Cisco SSL Appliance may be accessed through a serial console or SSH session as well as the WebUI. The Command Line Diagnostics (CLD) interface (see the Administration and Deployment Manual appropriate to your appliance for a full list of commands) is primarily used for diagnostics and monitoring purposes. It can also be used to configure static and/or IPv6 IP address.

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, page 1-14 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

Table 1-6 IPv4 Related Commands

Command	Description
network set ip	Set management network static IP configuration
network set ip dhcp	Enable DHCP management IP configuration
network show	Show network IP configuration

Step 1 Enter the command: network set ip, and press Enter.

Step 2 Enter the desired IP address, and press Enter.

Step 3 You will see an acceptance message.

Step 4 Log in to the appliance as usual.

Configure an IPv6 Address

Table 1-7 IPv6 Related Commands

Command	Description
network set ip6 <IP>[/mask bits] [gateway <gateway IP>]	Set management network static IP configuration
network set ip6 dhcp	Enable DHCP management IP configuration
network set ip6 slaac [stateless-dhcp]	Enable IPv6 SLAAC with stateless DHCP IP configuration

Step 1 Enter the command: network set ip6 <IP>, and press Enter.

Step 2 Enter the desired IP address, and press Enter.

Step 3 You will see an acceptance message

Step 4 Log in to the appliance as usual.

Power On and Initial Configuration - WebUI

A typical installation process for a new Cisco 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, page 1-14 to use a console connection instead.

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

Step 1 Connect the Management Ethernet port. HTTPS access to the Cisco 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 users

- 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, but that should already be installed.

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 Cisco SSL Appliance uses DHCP to acquire both IPv4 and IPv6 addresses from an attached network DHCP server. If you use DCHP, see Getting the DHCP IP Address from the LCD Screen, page 1-22.

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

You can also configure a static 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 Cisco SSL2000 and SSL8200 Administration and Deployment Guide 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 of two groups of four. For example:

- IP6 screen 1: Q 1-2: FD00:0AFD IP6 screen 2: Q 3-4: 0B00:0000
- IP6 screen 3: Q 5-6: 020C:29FF
- IP6 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.

Bootstrap States

Every time that the Cisco 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 Cisco 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 Cisco 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. **Note** 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.

The front panel keypad is arranged as follows.

0 1

2 3

Subsequent Startups

Whenever the Cisco 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.

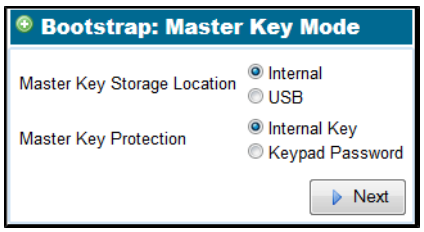
- If the master key is stored internally and no password is set for the master key, the bootstrap process becomes invisible, and the device will start up without any need for input from the administrator.
- If the master key is partly stored on a USB storage device, the USB device will need to be connected 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 Cisco 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.

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.

Create a Password

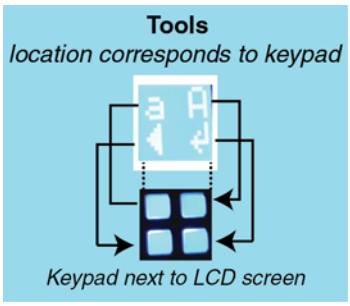
The password used to unlock the master key must be typed in on the front panel keypad after entering the code for PIN entry mode. See Bootstrap States, page 1-22. The password is only required if the master key mode chosen requires a PIN.

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, page 1-24.

Configuring a Password

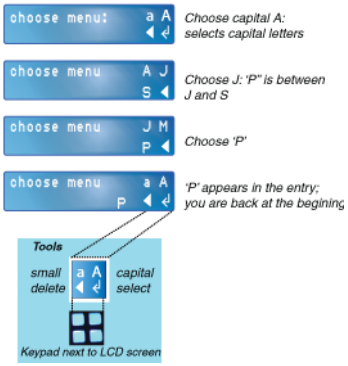
To configure a system password using the front LCD screen and keypad, enter the PIN entry mode as described in Bootstrap States, page 1-22 during start up.

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.

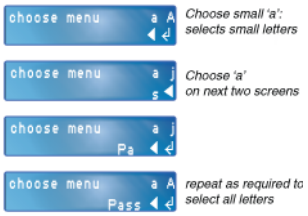


Step 1 Choose the capital 'A'; top right keypad button, to select capital letters.

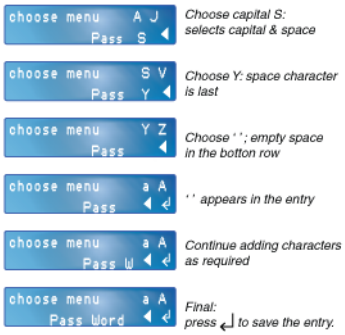
Step 2 Select 'J', top right button, as 'P' is between 'J' and 'S'.

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'.

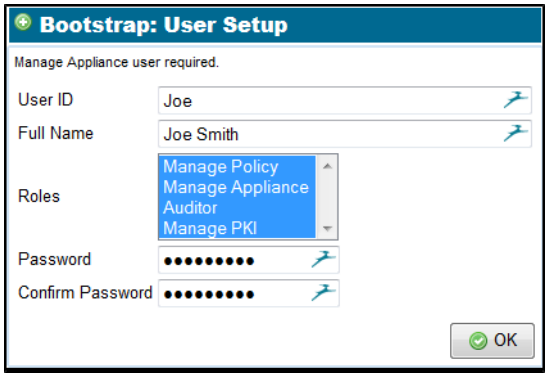
Step 10 Press OK (bottom right button) to confirm the entry.

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 the users 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.



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.

Configuring IP Addresses with the WebUI

The easiest way to use the Cisco 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 via a browser.

Once you are logged in, select (Platform Management) > Management Network, and edit the address(es) as required. The Cisco 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 Diagnostic Interface (see "Command Line Diagnostics Interface" in the Cisco SSL2000 and SSL8200 Administration and Deployment Guide) if this can be accessed directly from the console, or via the serial console.

Configuring a Static IP Address

This section describes how to set a Static address. Once the update is complete, 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: FE80:0000:0000:0000:0202:B3FF:FE1E:8329

  Collapsed: FE80::0202:B3FF:FE1E:8329

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.

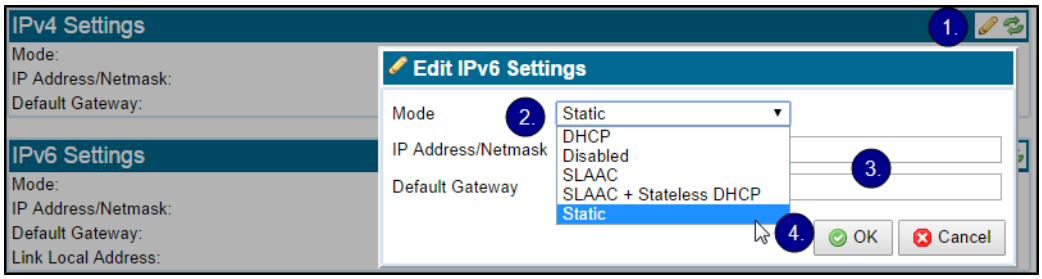
IPv6 Options

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

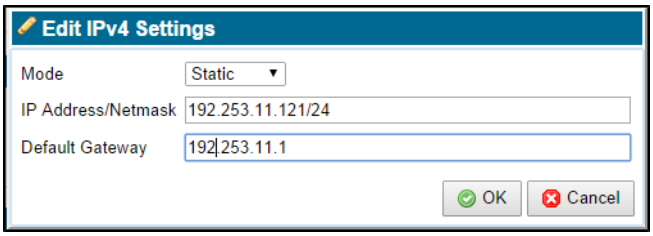
- When DHCP, SLAAC, or SLAAC + Stateless DHCP are selected, all other fields are grayed out.
- When Static is selected, enter the IP Address, Netmask, and Default Gateway addresses

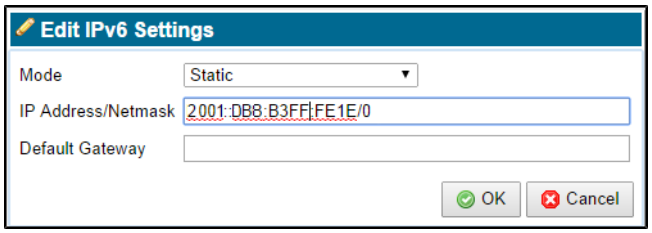
The Link Local Address, if applicable, is automatically generated, and is the last display item in the IPv6 Settings panel. See the Cisco SSL2000 and SSL8200 Administration and Deployment Guide for details on all of the settings.

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.

Configuring IPv4 Static with the LCD Screen

The easiest way to use the Cisco 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 Bootstrap States, page 1-22, 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 your 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:

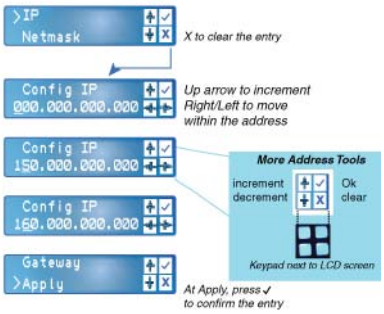
- IP address for the system

- 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

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



Step 1 Select the IP item, and press OK (the check mark).

Step 2 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 3 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 4 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 5 Once all the elements have been configured, click Apply; this is the last option in the list of menu items.

Completing 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.

Logging On

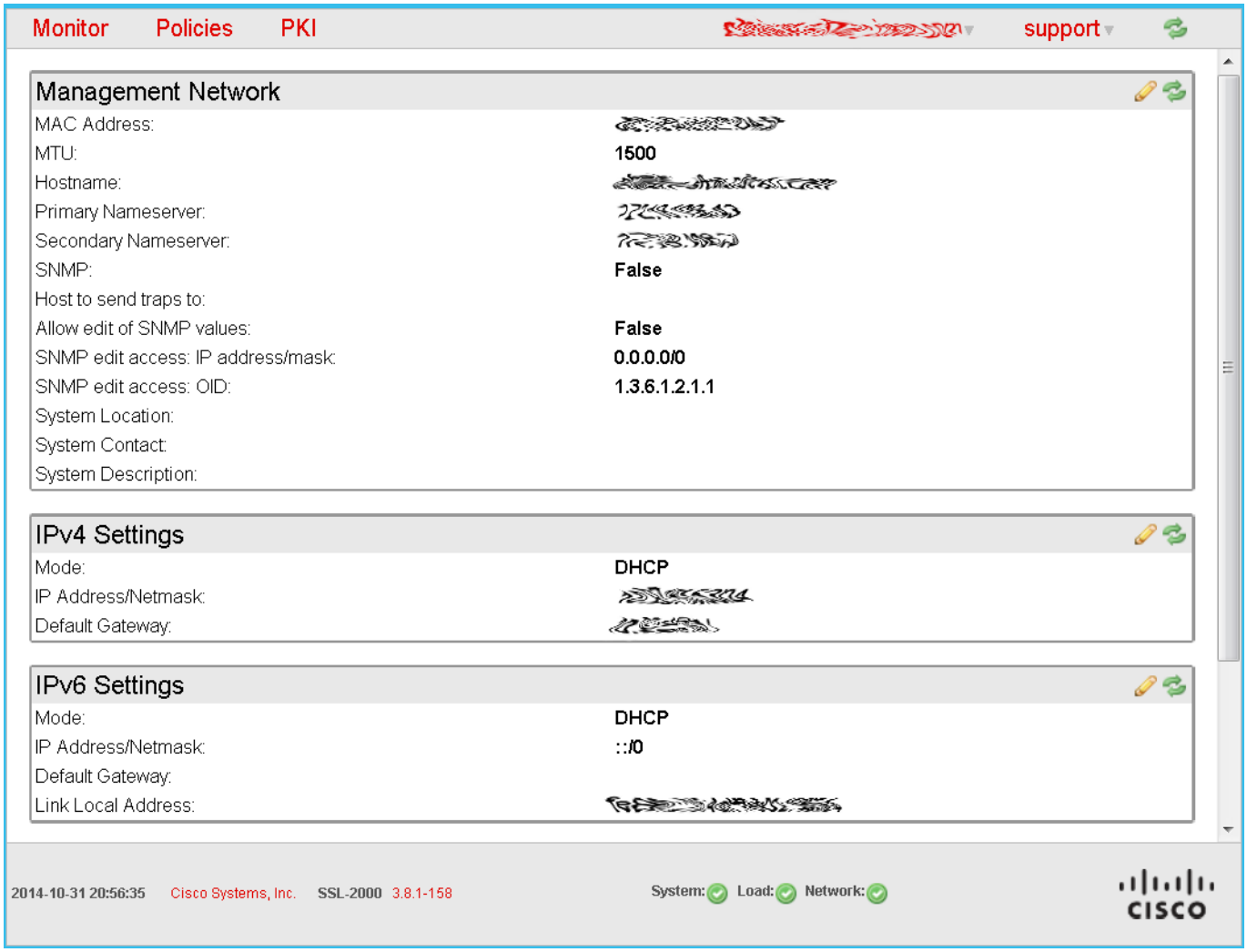
Once the bootstrap phase is complete the full WebUI is available and can be used to configure the system. The WebUI is described in detail in the Administration and Deployment Guide for your appliance. An HTTPS connection to the IP address assigned to the Cisco SSL Appliance management interface will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

The Cisco 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 Cisco SSL Appliance as a trusted device.

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

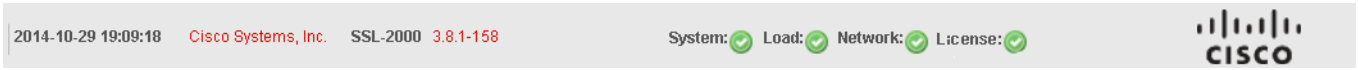
Use a web browser to login to the Cisco SSL Appliance at its IP address. For an IPv4 example, https://192.168.2.42. Once the administrator has logged on, the top and bottom of the initial management Dashboard screen present important information. The top of the screen contains menus along the top. The 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 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.

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 Cisco 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.

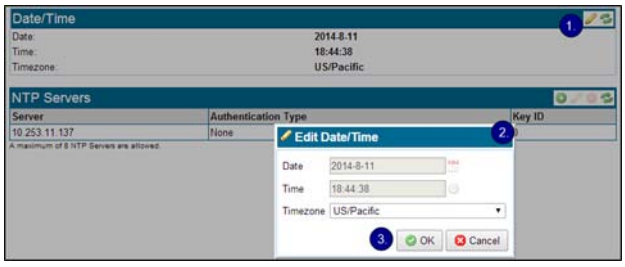
Table 1-9

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 unfail, connect
	Manually fail, 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 SSL2000 and SSL8200 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.

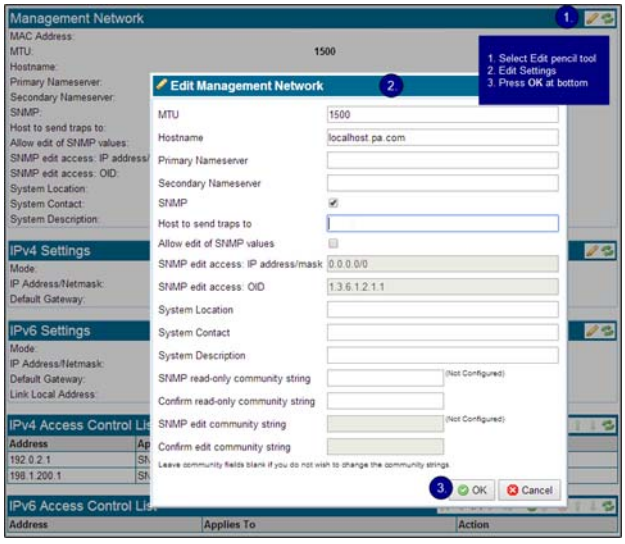
Step 4 If you have changed the date, time, NTP, or timezone, you must select Apply at the "Platform Config Changes" message which appears at the bottom of the screen.

Step 5 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.

Completing 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 (see Configuring IP Addresses with the WebUI, page 1-27, next) and SNMP settings, and so on. See the Cisco SSL2000 and SSL8200 Administration and Deployment Guide for your appliance 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.

Licensing

Each Cisco SSL Appliance has a pre-applied license which activates inspection.

Power Off

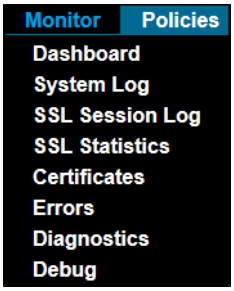
The Cisco SSL Appliance may be powered off several different ways:

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

Monitoring the System

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

The Monitor menu contains eight options that provide details on the operation of the system and that allow the collection of 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.



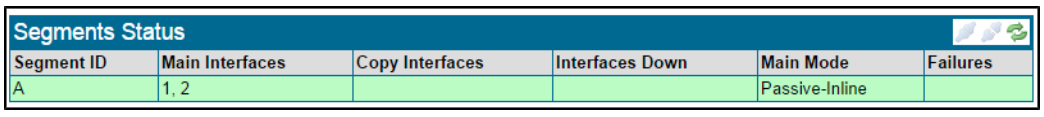
Dashboard: See the overall system status and the status of network links and active segments

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

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

Dashboard

The Dashboard displays several panels containing different types of information.



The Segment Status panel displays the status of currently active segments. 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.

The tools are available in addition to the Refresh button are:

Manually Unfail, which is normally grayed out. It will only be active if the segment is in a failure mode that requires manual intervention to clear the failure.

Manual Fail tool, which is active if a segment is selected. The Manual Fail icon allows a segment to be forced 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 tools provided for this panel are the Refresh tool and a Clear Counters tool.

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	19955571/14931583506	0
7	1G	Down	0/0	0/0	0
8	1G	Down	0/0	0/0	0

CPU Load % shows the current CPU utilization as a percentage of the total capacity of the CPU. The only tool provided for this panel is the Refresh button.

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 ºC)

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

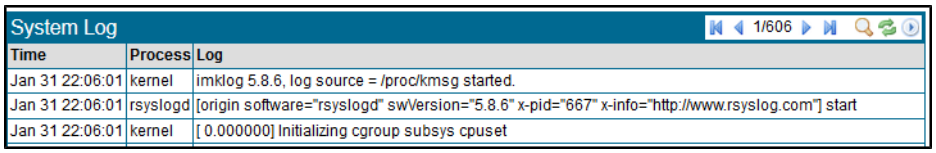
Thermal margin sensors are reported as negative values which when increased to 0 will cause CPU to throttle down or halt

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

Utilization %

Disk	Memory
51.0	6.0

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

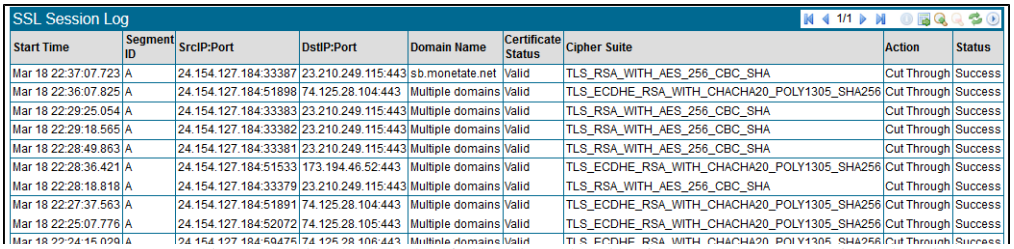

System Log 1/606

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

The SSL Session Log screen contains a single multipage panel enabling all entries in the last 64 pages of the SSL Session Log to be viewed. The panel has the standard multipage navigation tools in addition to the Refresh tool, an Export tool, and two filter 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.


SSL Session Log 1/1

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	24.154.127.184:59476	74.125.28.106:443	Multiple domains	Valid	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Cut Through	Success

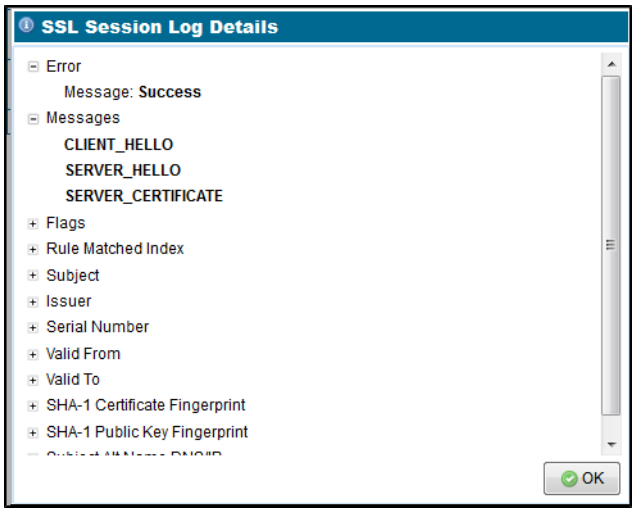
The SSL Session Log includes the following details for each SSL session that is recorded in the log:

- 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 Cisco SSL Appliance for this session
- Status for the session

Entries in the session log 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.

The Filter on Errors tool causes the session log to only display entries for flows that were not inspected successfully. The no filter tool causes the session log to revert to showing all entries.

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



SSL Statistics

The SSL Statistics screen contains a single multipage panel enabling all entries in the last 64 pages of the SSL Statistics log to be viewed. The panel has the standard multipage navigation tools, and a Clear Statistics tool.

SSL Statistics 1/64

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

The figure shows an example where page 1 out of the 64 pages of available statistics information is being displayed. Statistics are collected every second and each row in the table holds the data for a collection interval. Apart from the Detected and Decrypted columns, all the counts are cumulative. The Detected and Decrypted columns 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.

Configuring 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 56
- "Import Known Server Key" on page 57

Install a CA Cert for Certificate Resign

Before the Cisco 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 Cisco SSL Appliance and self signed or sent off for signing by another CA), or it can be imported. Management of Internal Certificate Authorities is done using the Resigning Certificate Authorities option on the PKI menu.

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 an 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.

Click  .

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.

Click the Generate self-signed CA button.

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.

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.

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.

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

Import Known Server Key

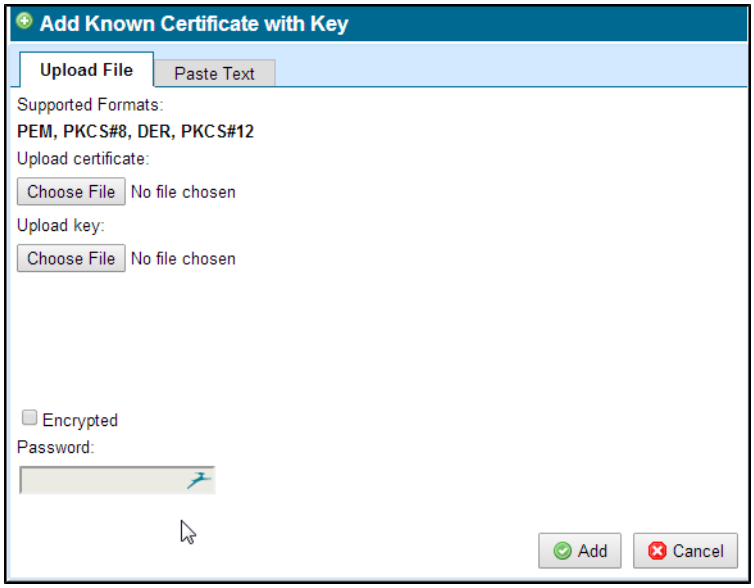
To inspect traffic to an internal SSL server, the easiest approach is to use known server key and certificate mode which requires that a copy of the server's SSL certificate and private key are loaded into the Cisco SSL Appliance.

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.

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

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



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.

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.

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

From here, use 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.

Sourcefire Support

If you are a new customer, please visit https://support.sourcefire.com/ to download the Sourcefire Support Welcome Kit, a document to help you get started with Sourcefire Support and set up your Customer Center account.

If you have any questions, want to download updated documentation, or require assistance with the Cisco SSL Appliance, please contact Sourcefire Support:

- Visit the Sourcefire Support site at https://support.sourcefire.com/.
- Email Sourcefire Support at support@sourcefire.com.
- Call Sourcefire Support at 410.423.1901 or 1.800.917.4134.

Cisco Support

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.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.