QUICK START GUIDE

Cisco S690 Web Security Appliance

1 Welcome

Thank you for choosing the Cisco S690 Web Security Appliance (WSA). The Web Security Appliance helps organizations secure and control web traffic.

This guide describes how to physically install the Cisco S690 appliance and use the System Setup Wizard to configure basic settings for the appliance. You can also refer to the *AsyncOS for Cisco Web Security Applicance User Guide* for information about how to configure appliance settings.

2 Before You Begin

Before you begin the installation, make sure that you have the items you need. The following items are included with the Cisco S690 Web Security Appliance:

- Slide rail kit
- Power cables (2)
- Ethernet cable for connecting the appliance to your network
- RJ45 to DB9 cable for connecting a computer to the console port
- Cisco Content Security documentation pointer card

> **Note** Two locking keys are included with the locking faceplate version of the Cisco S690 appliance. Keep these keys safe because you will need the 4-digit key code to replace missing keys.

You will need to provide the following items yourself:

- Rack cabinet enclosure (if rack-mounting the appliance)
- 10/100/1000 Base-TX TCP/IP LAN
- Desktop or laptop computer
- Web browser (or SSH and terminal software)
- Network and administrator information for the "Document Network Settings" section on page 3

3 Document Network Settings

Before you begin, write down the following information about your network and administrator settings.

Deployment Options	
Web Proxy: • **Transparent with L4** • **Switch Transparent with WCCP Router** • **Explicit Forward Proxy**	L4 Traffic Monitor: • Simplex tap/Span port • Duplex tap/Span port
Network Context	
Is there another proxy on the network:	
Other Proxy IP Address:	
Other Proxy Port:	
Network Settings	
Default System Hostname:	
DNS Servers:	Use the Internet root DNS servers. Use the DNS servers (maximum 3): 1. 2. 3.
Network Time Protocol (NTP) Server:	
Time Zone Region:	
Time Zone Country:	
Time Zone GMT Offset:	

Interface Settings	
Management Port	
IP Address:	
Network Mask:	
Hostname:	
Data Port (Optional, see Note)	
IP Address:	
Network Mask:	
Hostname:	

Note The Web Proxy can share the management interface. If configured separately, the Data interface IP address and the management interface IP address cannot share the same subnet.

Routes	
Internal Routes for Management	
Default Gateway:	
Static Route Name:	
Static Route Destination Network:	
Static Route Gateway:	
Internal Routes for Data	
Default Gateway:	
Static Route Name:	
Static Route Destination Network:	
Static Route Gateway:	

Transparent Routing Device	

Device Type:	• Layer 4 Switch or No Device
	• WCCP Router
	   – Enable standard service ID (web-cache).
	   – Router Addresses:
	    _____
	   – Enable router security.
	    Password:
	    _____

✎

Note When you connect the appliance to a WCCP router, you might need to configure the Web Security appliance to create WCCP services after you run the System Setup Wizard.

Administrative Settings	
Administrator Password:	
Email System Alerts To:	
SMTP Relay Host:	(Optional)
AutoSupport:	Enable
SenderBase Network Participation:	Enable • Limited • Standard

| Security Services	
L4 Traffic Monitor:	• Monitor only • Block
Acceptable Use Controls:	Enable • Cisco IronPort Web Usage Controls
Web Reputation Filters:	Enable
Malware and Spyware Scanning:	• Enable Webroot • Enable McAfee • Enable Sophos
Action for Detected Malware:	• Monitor only • Block
IronPort Data Security Filtering:	Enable
Locking Faceplate	
4-digit code (for the S690-LKFP appliance)	

4 Plan the Installation

Decide how you are going to configure the Cisco S690 Web Security Appliance within your network.

The Cisco S690 is typically installed as an additional layer in the network between clients and the Internet. Depending on how you deploy the appliance, you may or may not need a Layer 4 (L4) switch or a WCCP router to direct client traffic to the appliance.

Deployment options include:

- Transparent Proxy – Web proxy with an L4 switch
- Transparent Proxy – Web proxy with a WCCP router
- Explicit Forward Proxy – Connection to a network switch
- L4 Traffic Monitor – Ethernet or Fiber Optic tap (simplex or duplex). The following illustration shows a model with Ethernet ports. For more information about models with Fiber Optic ports, see the first note on the next page.

    - Simplex Mode: Port T1 receives all outgoing traffic, and port T2 receives all incoming traffic.

   - Duplex Mode: Port T1 receives all incoming and outgoing traffic.
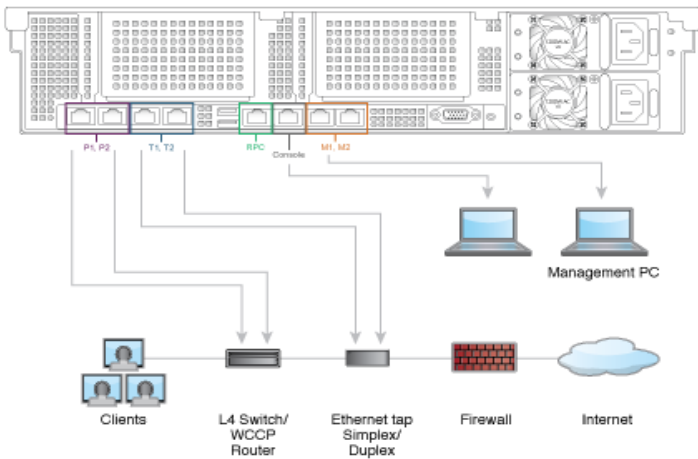
Note To monitor true client IP addresses, the L4 traffic monitor should always be configured inside the firewall and before NAT (Network Address Translation).

If your installation includes multiple Cisco Web Security Appliances (S-Series) or Cisco Email Security Appliances (C-Series)), you may want to also use a Cisco Content Security Management Appliance (M-Series) to manage them, as show in the following network diagram:

Outer DMZ

Cisco C-Series   Cisco S-Series

Inner DMZ

Cisco M-Series

Firewall

Internal Users
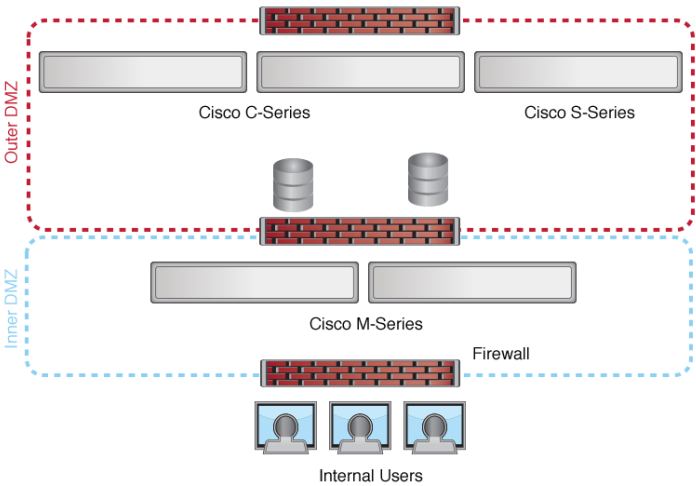
5   Install the Appliance in a Rack

Install the Cisco S690 Web Security Appliance using the slide rails supplied. For information about installing the appliance in a rack, see the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*.

Appliance Placement

- Ambient Temperature—To prevent the appliance from overheating, do not operate it in an area that exceeds an ambient temperature of 104°F (40°C).

- Air Flow—Be sure that there is adequate air flow around the appliance.

- Mechanical Loading—Be sure that the appliance is level and stable to avoid any hazardous conditions.

6   Plug In the Appliance

Plug the female end of each straight power cable into the redundant power supplies on the back panel of the appliance.

Plug the male end(s) into an electrical outlet.

7   Temporarily Change Your IP Address for Remote Access

To remotely configure the Cisco S690 using the network connection, you must temporarily change the IP address of your computer. Alternatively, you can use the serial console to configure the Cisco S690, without changing the IP address. If you use the serial console, proceed to section 8 below.

Note   Make a note of your current IP configuration settings as you will need to revert to these settings after you finish the configuration.

For Windows

Step 1 Connect your laptop to the Management port using the Ethernet cable included in the system box. The Cisco S690 appliance uses the Management port only. See "Plan the Installation" section on page 7.

Step 2 Go to the Start menu and choose **Control Panel**.

Step 3 Double-click **Network and Sharing Center**.

Step 4 Click **Local Area Connection** and then click **Properties**.

Step 5 Select **Internet Protocol** (**TCP/IP**) and then click **Properties**.

Step 6 Select **Use the Following IP Address**.

Step 7 Enter the following changes:

– IP Address: **192.168.42.43**

– Subnet Mask: **255.255.255.0**

– Default Gateway: **192.168.42.1**

**Step 8** Click **OK** and **Close** to exit the dialog box.

For Mac

Step 1 Launch the Apple menu and choose **System Preferences**.

Step 2 Click **Network.**

Step 3 Click lock icon to allow changes.

Step 4 Select the Ethernet network configuration with the green icon. This is your active connection. Then click **Advanced**.

Step 5 Click the TCP/IP tab and from Ethernet settings, choose **Manually** from the drop-down list.

Step 6 Enter the following changes:

– IP Address: **192.168.42.43**

– Subnet Mask: **255.255.255.0**

– Router: **192.168.42.1**

Step 7   Click **OK**.

8   Connect to the Appliance

Plug the Ethernet cables into the appropriate ports on the back panel of the Cisco S690 appliance.

- The proxy ports are labeled P1 and P2.
    - P1 only enabled: When only P1 is enabled, connect it to the network for both incoming and outgoing traffic.
    - P1 and P2 enabled: When both P1 and P2 are enabled, you must connect P1 to the internal network and P2 to the Internet.
- The traffic monitor ports are labeled T1 and T2.
    - Simplex tap: Ports T1 and T2; one cable for all packets destined for the Internet (T1) and one cable for all packets coming from the Internet (T2).
    - Duplex tap: Port T1; one cable for all incoming and outgoing traffic.
- Connect your laptop to the Management Port using the Ethernet cable included in the system box. The S-Series appliance uses the M1 Management Port only.
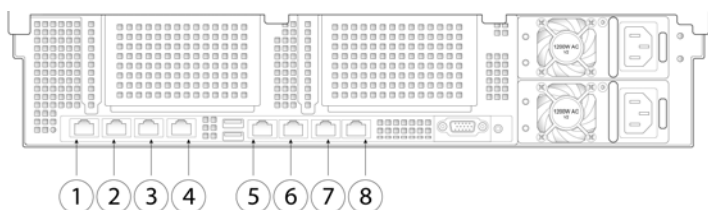
The illustration above shows a model with Ethernet ports. For models with Fiber Optic ports (S690-1G and S690-10G), call-outs 1 through 4, 7,and 8 are replaced with six Fiber Optic ports. These ports are located above the Ethernet ports shown in the illustration, and the Ethernet ports are not present. For details, see the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*.

The top two Fiber Optic ports are used as proxy ports in the same way as the Ethernet proxy ports described in the following table. The middle two Fiber Optic ports are used as traffic ports. The bottom two Fiber Optic ports are used as Management ports.

⚠️

Caution   Use only the transceiver modules supplied with the 10-Gigabit fiber optic interfaces. The use of any other transceiver modules may damage the fiber optic interface card.

Item	Port	Description
1	Proxy port 1	Connect proxy port P1 to the network for both incoming and outgoing traffic.
2	Proxy port 2	When both proxy ports P1 and P2 are enabled, you must connect P1 to the internal network and P2 to the Internet. P1 and P2 can connect to L4 switch, WCCP router, or network switch.
3	Traffic Monitor port 1	Traffic monitor port T1 for Duplex Ethernet tap: One cable for all incoming and outgoing traffic.
4	Traffic Monitor port 2	Traffic monitor port for Simplex Ethernet tap: One cable for all packets destined for the internet (T1), and one cable for all packets coming from the Internet (T2).
5	Remote Power Cycle	The port that is used for Remote Power Cycle (RPC).
6	Console	Indicates the console port that directly connects a computer to the appliance.

Item	Port	Description
7	Management interface 1	Indicates the Gigabit Ethernet interface that is restricted to management use only.
8	Management interface 2	Indicates the secondary Management Port. This port cannot be used.

9 Power Up the Appliance

Power up the appliance by pressing the On/Off switch on the front panel of the Cisco S690. You must wait 10 minutes for the system to initialize each time you power up the system. After the machine powers up, a solid green light indicates that the appliance is operational.

Note If turned on quickly after connecting power to the appliance, the appliance powers up, the fans spin and the LEDs turn on. Within 30-60 seconds, the fans stop and all LEDs turn off. The appliance powers on 31 seconds later. This behavior is by design to allow the system firmware and controller to synchronize.

Wait at least 10 minutes for the system to complete the power up sequence and the LEDs to turn green. If you turn the power off before the initialization is complete, the appliance will NOT reach an operational state and must be returned to Cisco.

10 Log In to the Appliance

You can log into the Cisco S690 using one of two interfaces: the web-based interface or the command line interface.

Web-Based Interface

Step 1   For web browser access via the Ethernet port (see the "Connect to the Appliance" section on page 11), go to the appliance management interface by entering the following URL in a web browser:

http://192.168.42.42:8080

Step 2   Enter the following login information:

- Username: **admin**
- Password: **ironport**

✎

Note   The hostname parameter is assigned during system setup. Before you can connect to the management interface using a hostname (http://hostname:8080), you must add the appliance *hostname* and IP address to your DNS server database.

Step 3   Click **Login**.

Command-Line Interface

Step 1   Access the command-line interface locally or remotely:

- To access the CLI locally, set up a terminal to connect to the serial port using 9600 bits, 8 bits, no parity, 1 stop bit (**9600, 8, N, 1**) and flow control set to Hardware. To physically connect the terminal, see the "Connect to the Appliance" section on page 11).

- To access the CLI remotely, initiate an SSH session to the IP address **192.168.42.42**.

Step 2   Log in as **admin** with the password **ironport**.

11 **Run the System Setup Wizard**

Run the System Setup Wizard to configure basic settings and
enable a set of system defaults. Navigate to System Administration >
System Setup Wizard to start the system setup wizard when you
access the appliance through the web-based interface. The end user
license agreement (also known as the EULA) is displayed.

Step 1   Accept the end user license agreement.

Step 2   Enter information from the "Document Network
Settings" section on page 3.

If you need additional information about the settings,
choose **Help and Support > Online Help**.

Step 3   Review the configuration summary page.

Step 4   Click **Install this Configuration**.

Step 5   The appliance may not appear to have accepted your
configuration or be performing the installation. This is
because you have changed the IP address, but the
installation is underway.

Step 6   If you temporarily changed the IP address of your
computer as described above, change the IP address
settings back to the original values.

Step 7   Ensure that your laptop and the appliance are
connected to the network.

Step 8   Log in to the appliance again, at the hostname or IP
address that you noted in the "Plan the Installation"
section on page 7. Use the username **admin** and the new
password that you entered in the wizard.

The Cisco M390 Content Security Management
Appliance uses a self-signed certificate that may trigger
a warning from your web browser. You can simply
accept the certificate and ignore this warning.

Step 9   Be sure to keep your new administrator password in a
safe place.

---

12 Check for Available Upgrades

After logging in to the appliance, look at the top of the web browser window for an upgrade notification (or for a notice in the command-line interface.) If an upgrade is available, evaluate whether you should install it.

Details about each release are available in the release notes for that Async OS version.

13 Configure Network Settings

Depending on your network configuration, your firewall may need to be configured to allow access using the following ports. SMTP and DNS services must have access to the Internet.

The web security appliance must be able to listen on the following ports:

- FTP: port 21, data port TCP 1024 and higher
- HTTP: port 80
- HTTPS: port 443
- Management access: ports 8443 (HTTPS) and 8080 (HTTP)
- SSH: port 22

The web security appliance must be able to make an outbound connection on the following ports:

- DNS: port 53
- FTP: port 21, data port TCP 1024 and higher
- HTTP: port 80
- HTTPS: port 443
- LDAP: port 389 or 3268
- LDAP over SSL: port 636
- LDAP with SSL for global catalog queries: port 3269
- NTP: port 123
- SMTP: port 25

> ✎
>
> **Note** If you do not open port 80 and port 443, you cannot download feature keys.

For details, and to open additional ports needed for the functionality you will use, see firewall information in the online help or user guide for your AsyncOS release.

14 Configuration Summary

Item	Description
Management	You can manage the web security appliance from the management port (Management port) by entering http://192.168.42.42:8080 or using the IP address assigned to the management interface after you have completed the System Setup Wizard.
	If you reset your configuration to factory default settings (for example, by re-running the System Setup Wizard), you can access the management interface only from the Management port (http://192.168.42.42:8080), so ensure you have a connection to the Management port.
	Also, verify that you open firewall ports 80 and 443 on your management interface.

Item	Description
Data	After running the System Setup Wizard, at least one port on the appliance is configured to receive web traffic from the clients on the network: M1 only; M1 and P1; M1, P1 and P2; P1 only; or P1 and P2.
	✎
	Note If you configured the web proxy in explicit forward mode, the applications on the client machines must be configured to explicitly forward web traffic to the web security appliance's web proxy using the IP address configured for data, either M1 or P1.
Traffic Monitor	After running the System Setup Wizard, one or both L4 traffic monitor ports (T1 only or both T1 and T2) are configured to listen to traffic on all TCP ports. The default setting for the L4 traffic monitor is monitor only. During or after setup, you can configure the L4 traffic monitor to both monitor and block suspicious traffic.
Computer Address	Remember to change your computer IP address back to the original settings that you noted in the "Temporarily Change Your IP Address for Remote Access" section on page 9.
	✎
	Note You can review a summary of your system settings from the **System Administration > Configuration Summary** page.

15 Additional Configuration

Congratulations. Now that you have completed the installation and basic configuration, you can start using your Cisco S690 Web Security Appliance. You may wish to consider taking some of the following steps to get more out of the appliance:

User Policies

Use the web interface to create policies that define which users can access which web resources as necessary.

- Identify Users—Choose **Web Security Manager > Identity Profiles** to define groups of users that can access the Internet.

- Define Access Policies—Choose **Web Security Manager > Access Policies** to control user access to the Internet by configuring which objects and applications to allow or block, which URL categories to monitor or block, and web reputation and anti-malware settings.

You can also define several other policy types to enforce your organization's acceptable use policies by controlling access to the Internet. For example, you can define policies for decrypting HTTPS transactions and other polices that control upload requests.

For information about configuring policies on the Cisco S690 appliance, see the *AsyncOS for Cisco Web Security Applicance User Guide*.

Reporting

You can view statistics about blocked and monitored web traffic on your network by viewing reports available in the web interface. You can view reports about the top URL categories blocked, client activity, system status, and more.

More Information

There are other features that you may want to configure for your Cisco S690 appliance. For more information about configuring feature keys, end user notifications, logging, and for details about other available web security appliance features, see the Cisco S690 Web Security Appliance documentation.

16   Where to Go from Here

Support	
Cisco Support	http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
U.S. and Canada Toll-Free Number	800-553-2447
International Contacts	Worldwide Phone Numbers
Email:	tac@cisco.com
Online Technical Support and Documentation (login may be required)	www.cisco.com/support
Cisco Web Security Appliance Support Community	https://supportforums.cisco.com/community/5786/web-security
Product Documentation	
Cisco S690 Web Security Appliance Quick Start Guide (Most current version of this document)	http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Cisco x90 Series Content Security Appliances Installation and Maintenance Guide Includes information about LEDs, technical specifications, and rack-mounting options.	http://www.cisco.com/c/en/us/support/ security/web-security-appliance/produ cts-installation-guides-list.html
Cisco Web Security Appliance Documentation All hardware and software documentation for your Cisco Web Security Appliance	http://www.cisco.com/c/en/us/support/ security/web-security-appliance/tsd-pr oducts-support-series-home.html
Safety and Compliance Guide	http://www.cisco.com/c/en/us/support/ security/web-security-appliance/tsd-pr oducts-support-series-home.html
MIBs	
AsyncOS MIBs for Cisco Web Security Appliance (Related Tools section)	http://www.cisco.com/c/en/us/support/ security/web-security-appliance/tsd-pr oducts-support-series-home.html

17 Cisco Notification Service

Sign up to receive notifications relevant to your Cisco Content Security Appliances, such as Security Advisories, Field Notices, End of Sale and End of Support statements, and information about software updates and known issues.

You can specify options such as notification frequency and types of information to receive. You should sign up separately for notifications for each product that you use.

To sign up, visit
http://www.cisco.com/cisco/support/notifications.html

A Cisco.com account is required. If you do not have one, register at https://tools.cisco.com/RPF/register/register.do.