



Introduction to the Secure Web Appliance

- [About Secure Web Appliance, on page 1](#)
- [Document Network Settings, on page 1](#)

About Secure Web Appliance

Cisco Web Security Appliance S195, S395, S695, and S695F (WSA) helps organizations secure and control web traffic. This guide describes how to setup your appliances and use the System Setup Wizard to configure basic settings for the appliance. You can also refer to the “Deployment” chapter in the [AsyncOS for Cisco Web Security Appliances User Guide](#) for information about how to configure appliance settings.

Document Network Settings

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

Deployment Options	
Web Proxy: <ul style="list-style-type: none">• Transparent with L4• Switch Transparent with WCCP Router• Explicit Forward Proxy	L4 Traffic Monitor: <ul style="list-style-type: none">• 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:	<ul style="list-style-type: none"> • Layer 4 Switch or No Device • WCCP Router <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> • Limited • Standard
Security Services	
L4 Traffic Monitor:	<ul style="list-style-type: none"> • Monitor only • Block
Acceptable Use Controls:	Enable <ul style="list-style-type: none"> • Cisco IronPort Web Usage Controls
Web Reputation Filters:	Enable
Malware and Spyware Scanning:	<ul style="list-style-type: none"> • Enable Webroot • Enable McAfee • Enable Sophos

Action for Detected Malware:	<ul style="list-style-type: none">• Monitor only• Block
IronPort Data Security Filtering:	Enable
Locking Faceplate	
4-digit code (for the S695-LKFP appliance)	