



Configure Network Settings

- [Configure Network Settings, on page 1](#)
- [Configuration Summary, on page 2](#)

Configure Network Settings

Depending on your network configuration, you may need to configure your firewall 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 443, you cannot download feature keys.

For more information, see firewall information in the user guide for your version of AsyncOS for Cisco Web Security Appliances.

Configuration Summary

Item	Description
Management	<p>You can manage the web security appliance from the management port (Management port) by entering <code>https://192.168.42.42:8443</code> or using the IP address assigned to the management interface after you have completed the System Setup Wizard.</p> <p>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 (<code>https://192.168.42.42:8443</code>), so ensure you have a connection to the Management port.</p> <p>Also, verify that you open firewall ports 80 and 443 on your management interface.</p>
Data	<p>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.</p> <p>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.</p>
Traffic Monitor	<p>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.</p>
Computer Address	<p>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".</p> <p>Note You can review a summary of your system settings from the System Administration > Configuration Summary page.</p>