Setup, Installation, and Basic Configuration

This chapter contains the following sections:

- Solution Deployment Overview, on page 1
- SMA Compatibility Matrix, on page 2
- Installation Planning , on page 2
- Preparing for Setup , on page 3
- Accessing the Security Management Appliance , on page 5
- Accessing the Security Management Appliance API Interface Using Swagger UI, on page 9
- Running the System Setup Wizard, on page 9
- About Adding Managed Appliances, on page 13
- Configuring Services on the Security Management Appliance, on page 14
- Committing and Abandoning Configuration Changes , on page 15

Solution Deployment Overview

To configure your Cisco Content Security Management appliance to provide service to your Cisco Content Security solution:

	On These Appliances	Do This	More Information
Step 1	All appliances	Ensure that your appliances meet the system requirements for the features you will use. If necessary, upgrade your appliances.	See the SMA Compatibility Matrix, on page 2.
Step 2	Email Security appliances	Before you introduce centralized services to your environment, configure all Email Security appliances to provide the security features you want, and verify that all features are working as expected on each appliance.	See the documentation for your Cisco Email Security release.
Step 3	Web Security appliances	Before you introduce centralized services to your environment, configure at least one Web Security appliance to provide the security features you want, and verify that all features are working as expected.	See the AsyncOS for Cisco Web Security Appliances User Guide.

	On These Appliances	Do This	More Information
Step 4	Security Management appliance	Set up the appliance and run the System Setup Wizard.	See the Installation Planning , on page 2, Preparing for Setup , on page 3 and the Running the System Setup Wizard, on page 9.
Step 5	All appliances	Configure each centralized service that you want to deploy.	Start with the Configuring Services on the Security Management Appliance, on page 14.

SMA Compatibility Matrix

For compatibility of your Security Management appliance with Email Security appliances and Web Security appliances, and for compatibility of configuration files when importing and publishing Web Security appliance configurations, see the Compatibility Matrix at http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html.

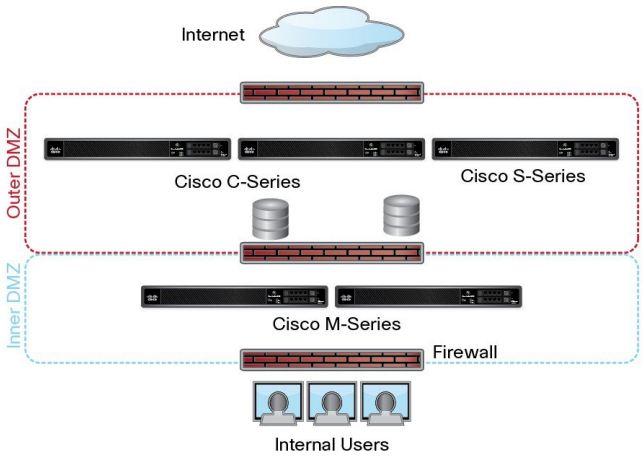
Installation Planning

- Network Planning , on page 2
- About Integrating a Security Management Appliance with Email Security Appliances , on page 3
- Deployments with Clustered Email Security Appliances , on page 3

Network Planning

The Security Management appliance lets you separate end user applications from the more secure gateway systems residing in your demilitarized zones (DMZs). Using a two-layer firewall can provide flexibility in network planning so that end users do not connect directly to the outer DMZ .

Figure 1: Typical Network Configuration Incorporating the Security Management appliance



The following figure shows a typical network configuration incorporating the Security Management appliance and multiple DMZs. You deploy the Security Management appliance outside your DMZ, in your internal

networks. All connections are initiated by the Security Management appliances (M-Series) to the managed Email Security appliances (C-Series) and managed Web Security appliances (S-Series).

Corporate data centers can share a Security Management appliance to perform centralized reporting and message tracking for multiple Web and Email Security appliances, and centralized policy configuration for multiple Web Security appliances. The Security Management appliance can also be used as an external spam quarantine.

After you connect the Email Security appliance and the Web Security appliances to a Security Management appliance and properly configure all appliances, AsyncOS gathers and aggregates data from the managed appliances. From the aggregated data, reports can be generated and an overall view of email and web usage can be determined.

About Integrating a Security Management Appliance with Email Security Appliances

Additional information about integrating the Security Management appliance with your Email Security appliances, see the "Centralizing Services on a Cisco Content Security Management Appliance" chapter in the user documentation or online help for your Email Security appliance.

Deployments with Clustered Email Security Appliances

The Security Management appliance cannot be placed in a cluster of Email Security appliances that are using the email appliances' centralized management feature. However, clustered Email Security appliances can deliver messages to the Security Management appliance for centralized reporting and tracking and to quarantine messages.

Preparing for Setup

Before you run the System Setup Wizard:

Step 1 Review the latest release notes for your product. See Network Planning , on page 2.

Step 2 Verify that the components of your security solution are compatible. See the SMA Compatibility Matrix, on page 2.

Step 3 Ensure that your network and physical space are ready to support this deployment. See Installation Planning , on page 2.

Step 4 Physically set up and connect the Security Management appliance. See Physically Setting Up and Connecting the Appliance , on page 3.

Step 5 Determine network and IP address assignments. See Determining Network and IP Address Assignments, on page 4.

Step 6 Gather information about your system setup. See Gathering the Setup Information, on page 4.

Physically Setting Up and Connecting the Appliance

Before you follow the procedures in this chapter, complete the steps described in the quick start guide that came with your appliance. In this guide, it is assumed that you have unpacked the appliance, physically installed it in a rack, and turned it on.

Before you can log in to the GUI, you need to set up a private connection between a PC and the Security Management appliance. For example, you can use the included crossover cable to connect directly from the Management port on the appliance to a laptop. Optionally, you can connect through an Ethernet connection between a PC and the network (for example, an Ethernet hub) and between the network and the Management port on the Security Management appliance.

Determining Network and IP Address Assignments

Note If you have already cabled your appliance to your network, ensure that the default IP address for the content security appliance does not conflict with other IP addresses on your network. The IP address that is pre-configured on the Management port of each appliance is 192.168.42.42.

After setup, go to the **Management Appliance > Network > IP Interfaces** page on the main Security Management appliance to change the interface that the Security Management appliance uses.

You need the following network information about each Ethernet port that you choose to use:

- IP address
- Netmask

In addition, you need the following information about your overall network:

- IP address of the default router (gateway) on your network
- IP address and hostname of your DNS servers (not required if you want to use Internet root servers)
- Hostname or IP address of your NTP servers (not required if you want to manually set system time)

For more information, see Assigning Network and IP Addresses.

Note If you are running a firewall on your network between the Internet and the content security appliance, it may be necessary to open specific ports for the appliance to work properly. For more information on firewalls, see Firewall Information

Always use the same IP address on the Security Management appliance for receiving and sending email messages to the Email Security appliances. For an explanation, see information about Mail Flow in the documentation for your Email Security appliance.

Note that IPv6 is not supported for communication between the Cisco Content Security Management appliance and the appliances it manages.

Gathering the Setup Information

Use the following table to gather information about system setup. You will need this information at hand while running the System Setup Wizard.

Note See the Assigning Network and IP Addresses for detailed information about network and IP addresses.

The following table shows the system setup worksheet

1	Notifications		Email address where system alerts are sent:
2	System Time		NTP Server (IP address or hostname):
3	Admin Passphrase		Choose a new passphrase for the “admin” account:
4	AutoSupport		Enable AutoSupport? ___ Yes ___ No
5	Hostname		Fully qualified hostname of the Security Management appliance:
6	Interface / IP Address		IP address:
			Netmask:
7	Network	Gateway	Default Gateway (router) IP address:
		DNS	___ Use the Internet’s root DNS servers
			___ Use these DNS servers:

Accessing the Security Management Appliance

The Security Management appliance has a standard web-based graphical user interface, a separate web-based interface for managing the spam quarantine, a command-line interface, and special or limited web interfaces for administrative users granted access to specific features and functionality.

- Browser Requirements, on page 5
- About Accessing the Web Interfaces , on page 6
- Accessing the Legacy Web Interface, on page 8
- Accessing the Web Interface , on page 7
- Accessing the Command Line Interface, on page 8
- Supported Languages, on page 8
- Accessing the New Web Interface on Dark Mode, on page 9

Browser Requirements

To access the GUI, your browser must support and be enabled to accept JavaScript and cookies, and it must be able to render HTML pages containing Cascading Style Sheets (CSS).

Table 1: Supported Browsers and Releases

Browser	Windows 7	MacOS 10.6
Safari	—	7.0 and later
Google Chrome	Latest Stable Version	Latest Stable Version

Browser	Windows 7	MacOS 10.6
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	Latest Stable Version	Latest Stable Version

- Internet Explorer 11.0 (Windows 7 only)
- Safari (7 and later)
- Firefox (Latest Stable Version)
- Google Chrome (Latest Stable Version)

Browsers are supported only for operating systems officially supported by the browser.

You may need to configure your browser's pop-up blocking settings in order to use the GUI, because some buttons or links in the interface will cause additional windows to open.

For a seamless navigation and rendering of HTML pages, Cisco recommends using the following browsers to access the new web interface of the appliance (AsyncOS 12.0 and later):

- Google Chrome (Latest Stable Version)
- Mozilla Firefox (Latest Stable Version)

You can access the legacy web interface of the appliance on any of the supported browsers.

The supported resolution for the new web interface of the appliance (AsyncOS 12.0 and later) is between 1280x800 and 1680x1050. The best viewed resolution is 1440x900, for all the browsers.

Note Cisco does not recommend viewing the new web interface of the appliance on higher resolutions.

About Accessing the Web Interfaces

The Security Management appliance has two web interfaces: the standard administrator interface, available by default on port 80, and the spam quarantine end user interface, available by default on port 82. The spam quarantine HTTPS interface defaults to port 83 when enabled.

Because you can specify HTTP or HTTPS when configuring each of the web interfaces (go to **Management Appliance > Network > IP Interfaces** on the Security Management appliance), you may be asked to reauthenticate if you switch between the two during your session. For example, if you access the admin web interface through HTTP on port 80 and then, in the same browser, access the spam quarantine end user web interface through HTTPS on port 83, you are asked to reauthenticate if you return to the admin web interface.

Note - When accessing the GUI, do not use multiple browser windows or tabs simultaneously to make changes to the Security Management appliance. Do not use concurrent GUI and CLI sessions either. Doing so will cause unexpected behavior and is not supported.

- By default, your session times out if you are idle for more than 30 minutes or if you close the browser without logging out. If this happens, you must reenter your user name and passphrase. To change the timeout limit, see Configuring the Web UI Session Timeout.

Accessing the Web Interface

Step 1 Open your web browser and enter the IP address or host name of your appliance.

Step 2 [New Web Interface Only] You can access the new web interface in any one of the following ways:

Note The new web interface of your appliance uses AsyncOS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the `trailblazerconfig` command in the CLI to configure the trailblazer HTTPS ports. Make sure that the trailblazer HTTPS port is opened on the firewall.

- When `trailblazerconfig` CLI command is enabled, use the following URL - `https://example.com:<trailblazer-https-port>/ng-login`

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

  For more information on the trailblazerconfig CLI command, seeThe trailblazerconfig Command.

- When `trailblazerconfig` CLI command is disabled, use the following URL - `https://example.com:<https-port>/ng-login`

  where example.com is the appliance host name and `<https-port>` is the HTTPS port configured on the appliance.

- Log in to the legacy web interface and click **Security Management appliance is getting a new look. Try it!!** link to access the new web interface.

Important
- Make sure that AsyncOS API is enabled on the appliance.
- You must login to the legacy web interface of the appliance.
- If `trailblazerconfig` is enabled, the configured HTTPS port must be opened on the firewall. The default HTTPS port is 4431.

  Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.
- If `trailblazerconfig` is disabled, the AsycnOS API ports configured in **Management Appliance > Network > IP Interfaces**, are opened on the firewall. The default AsyncOS API HTTP/HTTPS port is 6080/6443.

Step 3 Enter the following default values:

- User name: **`admin`**
- Passphrase: **`ironport`**

Note This passphrase is NOT valid after you complete the System Setup Wizard, either using the web interface or the command-line interface.

Accessing the Legacy Web Interface

Note You must login to the Security Management Appliance to access the legacy web interface. For more information, see Accessing the Web Interface , on page 7

To enable and configure reporting, message tracking, quarantines, network access, and monitor system status, you must access the legacy web interface.

To access the legacy web interface from the new web interface, click on the gear icon as shown in the following figure:

Figure 2: Accessing the Legacy Web Interface from the

The legacy web interface opens in a new browser window. You must log in again to access it.

If you want to log out of the appliance completely, you need to log out of both the new and legacy web interfaces of your appliance.

Accessing the Command Line Interface

The command line interface, or CLI, is accessed on the Security Management appliance in the same way that the CLI is accessed on all Cisco Content Security appliances. There are, however, some differences:

- System setup must be performed through the GUI.
- Some CLI commands are not available on the Security Management appliance. For a list of which commands are not supported, see the IronPort AsyncOS CLI Reference Guide for Cisco Content Security Appliances.

For production deployments, you should use SSH to access the CLI. Use a standard SSH client to access the appliance on port 22. For lab deployments, you can also use telnet; however, this protocol is not encrypted.

Supported Languages

With the appropriate license key, AsyncOS can display the GUI and CLI in any of the following languages:

- English
- French
- Spanish
- German
- Italian
- Korean

- Japanese
- Portuguese (Brazil)
- Chinese (traditional and simplified)
- Russian

To choose the GUI and default reporting language, do one of the following:

- Set the language preference. See Setting Preferences.
- Use the Options menu at the top right side of the GUI window to select the language for the session.

(The method that works depends on the method used to authenticate your login credentials.)

Accessing the New Web Interface on Dark Mode

Dark Mode is a reversed color scheme that utilizes light-colored typography, UI elements, and iconography on dark backgrounds. You can now use dark mode on the new web interface of your appliance.

To switch to the dark mode web interface on your appliance, click on the user information section on the top right corner of the new web interface and select **Dark Mode**.

Accessing the Security Management Appliance API Interface Using Swagger UI

Swagger UI allows you to visualize and interact with the API resources of your appliance. This is automatically generated from your API specifications. For more information, see https://swagger.io/tools/swagger-ui/.

You can log in to the Swagger UI on the new web interface of your Security Management appliance in any one of the following ways:

- Use the following URL - `https://example.com:<trailblazer-https-port>/swagger`

  where `example.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

  Note You must enable the trailblazer HTTPS port on the appliance to access the Swagger UI. For more information on the `trailblazerconfig` CLI command, see The trailblazerconfig Command.

- Log in to the new web interface of your appliance. Click the **?** button on the upper-right corner and select **API Help: Swagger** from the drop-down. The Swagger UI opens in a new browser window.

Running the System Setup Wizard

AsyncOS provides a browser-based System Setup Wizard to guide you through the process of system configuration. Later, you may want to take advantage of custom configuration options not available in the wizard. However, you must use the wizard for the initial setup to ensure a complete configuration.

The Security Management appliance supports this wizard via the GUI only. It does not support system setup through the command line interface (CLI).

- Before You Begin , on page 10
- Overview of the System Setup Wizard , on page 10

Before You Begin

Complete all tasks in the Preparing for Setup , on page 3.

Caution The System Setup Wizard completely reconfigures the appliance. Only use the wizard when you initially install the appliance, or if you want to completely overwrite the existing configuration.

Be sure to connect the Security Management appliance to your network through the Management port.

Caution The Security Management appliance ships with a default IP address of 192.168.42.42 on the Management port. Before connecting the Security Management appliance to your network, ensure that no other device's IP address conflicts with the factory default setting.

Note By default, your session times out if you are idle for more than 30 minutes or if you close the browser without logging out. If this happens, you must reenter your user name and passphrase. If the session times out while you are running the System Setup Wizard, you need to start over from the beginning. To change the timeout limit, see Configuring the Web UI Session Timeout.

Overview of the System Setup Wizard

Step 1 Launch the System Setup Wizard , on page 11

Step 2 Review the End User License Agreement, on page 11

Step 3 Configure the System Settings, on page 11

- Notification settings and AutoSupport
- System time settings
- Admin passphrase

Step 4 Configure the Network Settings, on page 12

- Hostname of the appliance
- IP address, network mask, and gateway of the appliance
- Default router and DNS settings

Step 5 Review Your Configuration, on page 12

Proceed through the wizard pages, and carefully review your configuration at Step 4. You can return to a step by clicking **Previous**. At the end of the process, the wizard prompts you to commit the changes that you have made. Most changes do not take effect until you commit them.

Step 6 Proceeding to the Next Steps, on page 13

Launch the System Setup Wizard

To launch the wizard, log in to the GUI as described in the Accessing the Web Interface , on page 7. The first time you log in to the GUI, the initial page of the System Setup Wizard appears by default. You can also access the System Setup Wizard from the System Administration menu (Management Appliance > System Administration > System Setup Wizard).

Review the End User License Agreement

Begin by reading the license agreement. After you have read and agreed to the license agreement, select the check box indicating that you agree, and then click Begin Setup to proceed.

Configure the System Settings

Entering an Email Address for System alertsAlerts

AsyncOS sends alert messages through email if there is a system error that requires your intervention. Enter the email address (or addresses) where the alerts are sent.

You need to add at least one email address for the system alerts. Separate multiple addresses with commas. The email addresses that you enter initially receive all types of alerts at all levels. You can customize the alert configuration later. For more information, see the Managing Alerts.

Setting the Time

Set the time zone on the Security Management appliance so that timestamps in reports, message headers and log files are correct. Use the drop-down menus to locate your time zone or to define the time zone by GMT offset.

You can set the system clock time manually, but Cisco recommends using an Network Time Protocol (NTP) server to synchronize time with other servers on your network or the Internet. By default, the Cisco NTP server (time.sco.cisco.com) is added as an entry to synchronize the time on your content security appliance. Enter the hostname of the NTP server, and click Add Entry to configure an additional NTP server. For more information, see the Configuring the System Time.

Setting the Passphrase

You must change the passphrase: adminpassphrase for the AsyncOS admin account. Keep the passphrase in a secure location. Changes to the passphrase take effect immediately.

Note If you cancel the system setup after resetting the passphrase, your passphrase changes are not undone.

Enabling AutoSupport

The AutoSupport feature (enabled by default) notifies Customer Support about issues with the Security Management appliance so that they can provide optimal support. For more information, see the Cisco AutoSupport.

Configure the Network Settings

Define the hostname of the machine and then configure the gateway and DNS settings.

Note Verify that you have connected the Security Management appliance to your network through the Management port.

Network Settings

Enter the fully qualified hostname for the Security Management appliance. This name should be assigned by the network administrator.

Enter the IP address of the Security Management appliance.

Enter the network mask and IP address of the default deerrouter (gateway) on your network.

Next, configure the Domain Name Service (DNS) settings. AsyncOS contains a high-performance internal DNS resolver/cache that can query the Internet's root servers directly, or the system can use DNS servers that you specify. If you use your own servers, you need to supply the IP address of each DNS server. You can enter up to four DNS servers when you are using the System Setup Wizard.

Note The DNS servers you specify have an initial priority of 0. For more information, see the Configuring Domain Name System Settings.

Note The appliance requires access to a working DNS server to perform DNS lookups for incoming connections. If you cannot specify a working DNS server that is reachable by the appliance while you are setting up the appliance, you can select Use Internet Root DNS Servers, or else temporarily specify the IP address of the Management interface so that you can complete the System Setup Wizard.

Review Your Configuration

Now, the System Setup Wizard displays a summary of the setup information that you have entered. If you need to make any changes, click **Previous** at the bottom of the page and edit the information.

After you have reviewed the information, click **Install This Configuration**. Then click **Install** in the confirmation dialog box that appears.

If the page appears not to respond when you click **Install This Configuration**, this is because the appliance is now using the the new IP address that you specified in the wizard. To continue using the appliance, use the new IP address. If you followed the instructions in the Quick Start Guide to temporarily change the IP address of the computer you used to access your new hardware appliance, revert your computer's IP address to its original settings first.

Proceeding to the Next Steps

After you install the Security Management appliance and run the System Setup Wizard, you can modify other settings on the appliance and configure the monitoring services.

Depending on the process you used to access the appliance in order to run the system setup wizard, the **System Setup Next Steps** page appears. If this page dos not appear automatically, you can access it by choosing **Management Appliance > System Administration > Next Steps**.

Click on any of the links on the System Setup Next Steps page to proceed with the configuration of your Cisco Content Security appliances.

About Adding Managed Appliances

You will add managed Email and Web Security appliances to the Security Management appliance when you configure the first centralized service for each appliance.

Supported Email and Web Security appliances are shown in the SMA Compatibility Matrix, on page 2.

When you add a remote appliance, the Security Management appliance compares the product name of the remote appliance with the type of appliance you are adding. For example, you add an appliance using the Add Web Security appliance page, the Security Management appliance checks the product name of the remote appliance to make sure that it is a Web Security appliance and not an Email Security appliance. The Security Management appliance will also check the monitoring services on the remote appliances to make sure that they are correctly configured and compatible.

The Security Appliances page shows the managed appliances that you have added. The Connection Established? column shows whether or not the connection for monitoring services is properly configured.

Instructions for adding managed appliances are included in the following procedures:

- Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance
- Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance
- Adding the Centralized Spam Quarantine Service to Each Managed Email Security Appliance
- Adding the Centralized Policy, Virus, and Outbreak Quarantine Service to Each Managed Email Security Appliance
- Adding the Centralized Web Reporting Service to Each Managed Web Security Appliance
- Adding Web Security Appliances and Associating Them with Configuration Master Versions

Editing Managed Appliance Configurations

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3 In the Security Appliance section, click on the name of the appliance you want to edit.

Step 4 Make the necessary changes to the appliance configuration.

For example, select or clear check boxes for monitoring services, reconfigure file transfer access, or change the IP address.

Note Changing the IP address of a managed appliance can cause several issues to occur. If you change the IP address of a Web Security appliance, the publish history for the appliance will be lost, and publishing errors will occur if the Web Security appliance is currently selected for a scheduled publish job. (This does not affect scheduled publish jobs that are set to use all assigned appliances.) If you change the IP address of an Email Security appliance, the tracking availability data for the appliance will be lost.

Step 5 Click **Submit** to submit your changes on the page, then click Commit Changes to commit your changes.

Removing an Appliance from the List of Managed Appliances

Before you begin

You may need to disable any enabled centralized services on the remote appliance before you can remove that appliance from the Security Management appliance. For example, if the Centralized Policy, Virus, and Outbreak Quarantine service is enabled, you must disable that service first on the Email Security appliance. See the documentation for your email or web security appliance.

Step 1 [New Web Interface Only] On the Security Management appliance, click to load the legacy web interface.

Step 2 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3 In the Security Appliances section, and click the trash can icon in the row for the managed appliance that you want to delete.

Step 4 In the confirmation dialog box, click **Delete.**

Step 5 Submit and commit your changes.

Configuring Services on the Security Management Appliance

Email security services:

- Using Centralized Email Security Reporting
- Tracking Messages
- Spam Quarantine
- Centralized Policy, Virus, and Outbreak Quarantines

Web security services:

- Centralized Policy, Virus, and Outbreak Quarantines
- Managing Web Security Appliances

Committing and Abandoning Configuration Changes

After you make most configuration changes in the Cisco Content Security appliance GUI, you must explicitly commit the changes.

Figure 3: The Commit Changes Button

To	Do This
Commit all pending changes	Click the orange Commit Changes button at the top right side of the window. Add a description of the changes and then click commit. If you have not made any changes that require a commit, then a gray No Changes Pending button appears instead of Commit Changes.
Abandon all pending changes	Click the orange Commit Changes button at the top right side of the window, then click Abandon Changes.

Note The configuration changes made on the old web interface is updated on the new web interface, after you logout and login to the new Cisco Content Security Management web interface.

Related Topic

- Rolling Back to a Previously Committed Configuration