Cisco Content Security Management Appliance M195, M395, M695 and M695F Getting Started Guide

Published: June 7, 2019

Contents

Cisco Systems, Inc.
www.cisco.com

Welcome

The Cisco Content Security Management Appliance M195, M395, M695 and M695F centralizes reporting and tracking, management of quarantined email messages, and web security appliance configuration settings. It also allows automated data backups. This guide describes the basic steps for setting up your appliance.

Document Network Settings

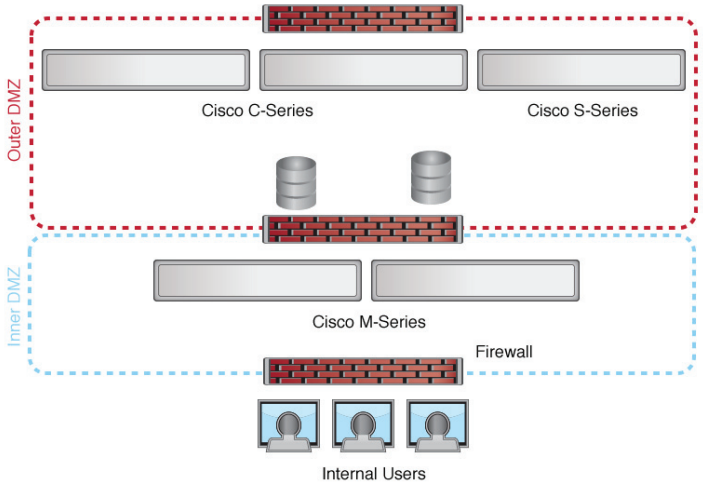
Before you begin, write down the following information about your system, network, and administrator settings.You will need this information when running the System Setup Wizard.

System Settings	
Email system alerts to:	
Time Zone Information:	
Default System Hostname:	
Deliver Scheduled Reports To:	
NTP Server:	
Admin Password: The default password will not work after you enter this new password. Your password must contain at least 8 characters, one number, one upper-case letter, one lower-case letter, and one special character.)	
AutoSupport:	Enable/Disable
Interfaces	
Data Port 1	
IP Address:	
Network Mask:	
Fully Qualified Hostname:	
Data Port 2	
IP Address:	
Network Settings	
Fully Qualified Appliance Hostname	
IP Address	
Network Mask:	
Default Gateway (Router) IP Address:	
DNS (Use the Internet's root DNS servers or specify your own):	
Locking Faceplate	
4-digit code (for the M695-LKFP appliance)	

Plan the Installation

The Cisco M195, M395, M695 and M695F appliances are designed to sit within your inner DMZ and communicate with Cisco C-Series and S-Series appliances in your outer DMZ.

Plan for your network configuration to look something like this:



Temporarily Change Your IP Address for Remote Access

To remotely configure the Cisco M195, M395, M695 and M695F appliance using the network connection, you must temporarily change the IP address of your computer. For instructions, see:

- Temporarily Change Your IP Address on Windows, page 3
- Temporarily Change Your IP Address on Mac, page 4

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

Alternatively, you can use the serial console to configure the appliance, without changing the IP address. If you use the serial console, see Connect to the Appliance, page 4.

Temporarily Change Your IP Address on Windows

The exact steps depend on your operating system version.

Procedure

Step 1 Go to the **Start** menu and choose **Control Panel**.

Step 2 Click **Network and Internet**, then **Network and Sharing Center**.

Step 3 Click the **Change adapter settings** link.

Step 4 Right-click **Local Area Connection** and choose **Properties**.

Step 5 Click **Internet Protocol Version 4**, then choose **Properties**.

Step 6 Note your current settings.

Step 7 Select **Use the Following IP Address**.

Step 8 Enter the following changes:

Step 9 IP Address: **192.168.42.43**

Step 10 Subnet Mask: **255.255.255.0**

Step 11 Default Gateway: **192.168.42.1**

Step 12 Click **OK** and **OK** again to exit the dialog box.

Temporarily Change Your IP Address on Mac

The exact steps depend on your operating system version.

Procedure

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

Step 2 Click **Network.**

Step 3 Click the lock icon to allow changes.

Step 4 Select the 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:

Step 7 IP Address: **192.168.42.43**

Step 8 Subnet Mask: **255.255.255.0**

Step 9 Router: **192.168.42.1**

Step 10 Click **OK**.

Connect to the Appliance

After rack-mounting the appliance, follow these steps to plug in, connect cables, turn on power, and verify connectivity.

- Cisco M195 Appliance, page 5
- Cisco M395 Appliance, page 6
- Cisco M695 Appliance, page 7
- Cisco M695F Appliance, page 8

Note The connection diagram in each topic shows the default configuration using a management computer connected to your private network. Your deployment may vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Cisco M195 Appliance

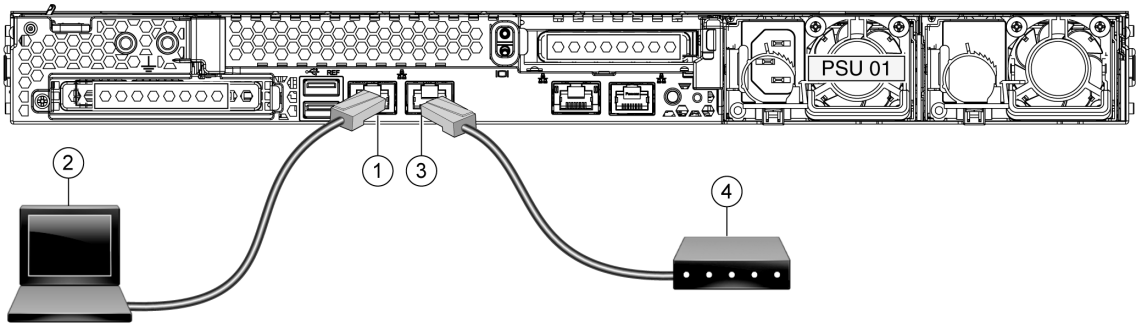
Step 1 Plug one end of the straight power cable into the power supply on the back panel of the appliance.

Note It is optional to order a separate power cable and connect to the second power supply at the back panel of the appliance for redundancy.

Step 2 Plug the other end into an electrical outlet.

Step 3 Plug the Ethernet cables into the appropriate ports on the back panel of the appliance.

- The Cisco M195 appliance has two Gigabit Ethernet ports: Data 1 and Data 2.
- For the purposes of setup, connect to Data 1 as your management interface and configure incoming web traffic or email on the Data 2 interface. These settings can be changed after the initial installation.



1	Data port 1 (P1) - (192.168.42.42)	2	Management computer (192.68.42.43)
3	Data port 2 (P2)	4	Incoming/Outgoing email (or web traffic)

Step 4 Power up the appliance by pressing the On/Off switch on the front panel of the appliance. You must wait 10 minutes for the system to initialize each time you power up the system. After the appliance powers up, a solid green light on the front panel indicates that the appliance is operational.

Caution 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.

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.

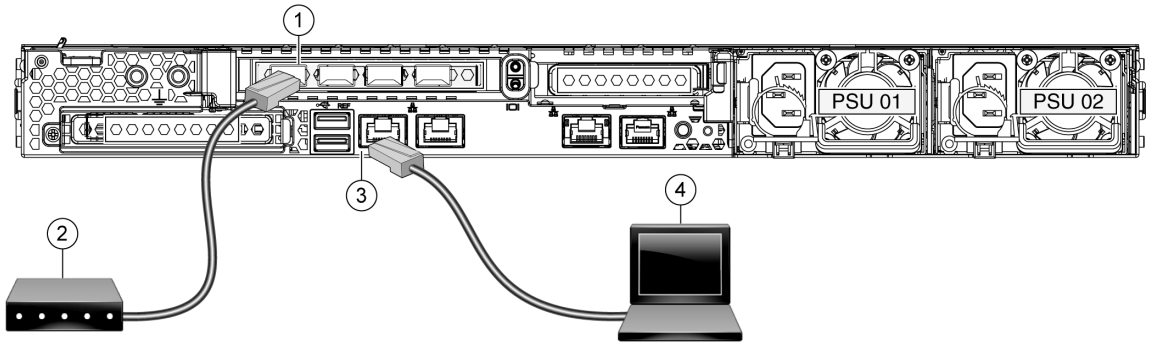
Step 5 See the *AsyncOS for Cisco Content Security Management Appliances User Guide* for further configuration.

Cisco M395 Appliance

Step 1 Plug one end of each straight power cable into the redundant power supplies on the back panel of the appliance.

Step 2 Plug the other end into an electrical outlet.

Step 3 Plug the Ethernet cables into the appropriate ports on the back panel of the appliance.



1	Data port 1 (P1)	2	Incoming/Outgoing email (or web traffic)
3	Management port (M1) - (192.168.42.42)	4	Management computer (192.168.42.43)

Step 4 Power up the appliance by pressing the On/Off switch on the front panel of the Cisco M395 Content Security Management Appliance. You must wait 10 minutes for the system to initialize each time you power up the system. After the appliance powers up, a solid green light on the front panel indicates that the appliance is operational.

Caution 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.

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.

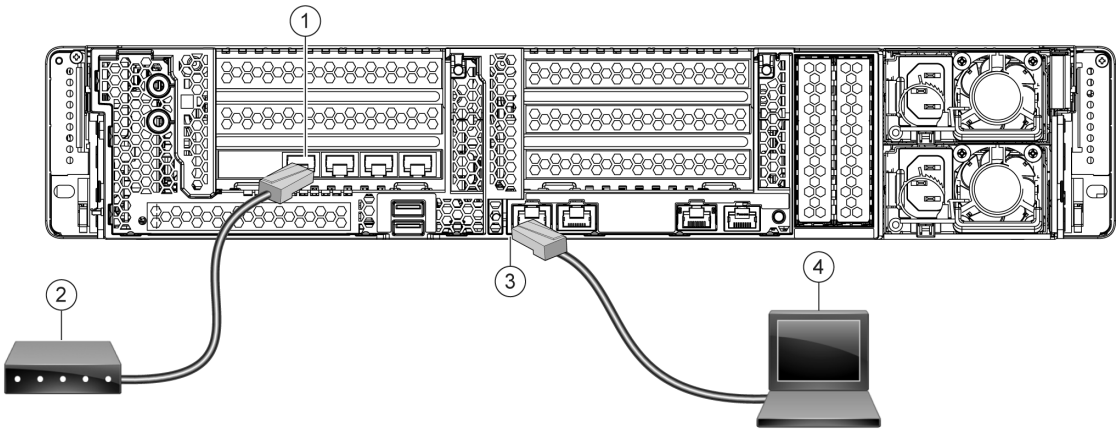
Step 5 See the *AsyncOS for Cisco Content Security Management Appliances User Guide* for further configuration.

Cisco M695 Appliance

Step 1 Plug one end of each straight power cable into the redundant power supplies on the back panel of the appliance.

Step 2 Plug the other end into an electrical outlet.

Step 3 Plug the Ethernet cables into the appropriate ports on the back panel of the appliance.



1	Data port 1 (P1)	2	Incoming/Outgoing email (or web traffic)
3	Management port (M1) - (192.168.42.42)	4	Management computer (192.168.42.43)

Step 4 Power up the appliance by pressing the On/Off switch on the front panel of the appliance. You must wait 10 minutes for the system to initialize each time you power up the system. After the appliance powers up, a solid green light on the front panel indicates that the appliance is operational.

Caution 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.

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.

Step 5 See the *AsyncOS for Cisco Content Security Management Appliances User Guide* for further configuration.

Cisco M695F Appliance

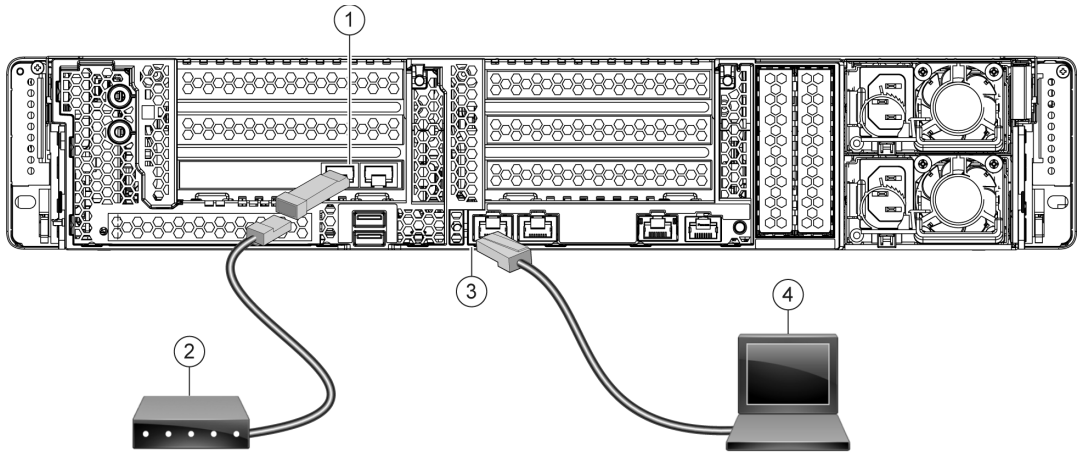
Step 1 Plug one end of each straight power cable into the redundant power supplies on the back panel of the appliance.

Step 2 Plug the other end into an electrical outlet.

Step 3 Connect the Fiber Optic cable and Ethernet cable into the appropriate ports on the back panel of the Cisco M695F appliance.

Note Fiber Optic ports are available with the M695F model of the Cisco Content Security Management Appliance. This model has two Fiber Optic ports. These ports are located above the Ethernet ports show in the following illustration. For details, see the *Cisco x95 Series Content Security Appliances Hardware Installation Guide*.

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.



1	Fiber optic port 1	2	Incoming/Outgoing email (or web traffic)
3	Management port (M1) - (192.168.42.42)	4	Management computer (192.168.42.43)

Step 4 Power up the appliance by pressing the On/Off switch on the front panel of the appliance. You must wait 10 minutes for the system to initialize each time you power up the system. After the appliance powers up, a solid green light on the front panel indicates that the appliance is operational.

Caution 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.

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.

Step 5 See the *AsyncOS for Cisco Content Security Management Appliances User Guide* for further configuration.

Log In to the Appliance

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

- Log in to the Appliance Using Web Interface, page 9
- Log in to the Appliance Using the CLI, page 10

Log in to the Appliance Using Web Interface

Procedure

Step 1 For web browser access via the Ethernet port (see the "Connect to the Appliance" section on page 4), go to the appliance's management interface by entering the following URL in a web browser:

http://192.168.42.42

Step 2 Enter the following login information:

- Username: `admin`
- Passphrase: `ironport`

Step 3 The hostname parameter is assigned during system setup. Before you can connect to the management interface using a hostname (http://hostname), you must add the appliance *hostname* and IP address to your DNS server database.

Step 4 Click **Login**.

Log in to the Appliance Using the CLI

Procedure

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 4).
- 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 passphrase **ironport**.

Step 3 At the prompt, enter the **systemsetup** command.

Run the System Setup Wizard

Run the System Setup Wizard to configure basic settings and enable a set of system defaults. The System Setup Wizard starts automatically when you access the appliance via the web-based interface (or when you run the **systemsetup** command from the command-line interface.)

Step 1 Accept the end user license agreement.

Step 2 Enter system and network information from the "Plan the Installation" section on page 3.

Step 3 If you need additional information about the settings, choose **Help and Support > Online Help**.

Step 4 Review the configuration summary page.

Step 5 Click **Install this Configuration**.

Step 6 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 7 If you temporarily changed the IP address of your computer as described above, change the IP address settings back to the original values.

Step 8 Ensure that your laptop and the appliance are connected to the network.

Step 9 Log in to the appliance again, at the hostname or IP address that you noted in the "Plan the Installation" section on page 3. Use the username **admin** and the new password that you entered in the wizard.

Step 10 The appliance uses a self-signed certificate that may trigger a warning from your web browser. Accept the certificate and ignore this warning.

Step 11 Be sure to keep your new administrator password in a safe place.

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.

For example, make sure that the new version is compatible with the AsyncOS versions of managed email and web appliances in your environment.

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

Configure Network Settings

Verify that your firewall allows your appliance to communicate via the internet using the following ports:

- DNS: port 53
- SMTP: port 25
- HTTP: port 80
- HTTPS: port 443
- SSH (for the command-line interface): port 22
- NTP: port 123
- FTP: port 21, data port TCP 1024 and higher

Note If you do not open 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.

Additional Configurations

You can now configure the following unique features of your Cisco Content Security Management Appliance, as well as other useful functionality:

- Centralized Email Reporting
- Centralized Message Tracking
- Centralized Quarantine Management
- Centralized Web Reporting and Tracking
- Centralized Configuration Management for Web Security Appliances
- Content Security Management Appliance Data Backups

For details, see the online help on your appliance or the User Guide for your AsyncOS version.

Caution If you need to shut down your appliance for any reason, use the **System Administration > Shutdown/Reboot** page to prevent corruption of your queue and configuration files.

Related Documentation

Product Documentation	
Cisco Content Security Management Appliance Documentation	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Links from this page hold release notes, user guides, and information about hardware and its installation, including: *Cisco M195, M395, M695 and M695F Content Security Management Appliance Getting Start Guide* (This document) *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide* (Includes technical specifications and information about LEDs) Safety and compliance information	
Support	
Cisco support communities for email and web security (Includes Content Security Management Appliance support)	https://supportforums.cisco.com/community/5756/email-security https://supportforums.cisco.com/community/5786/web-security
Cisco Support	http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui.