Cisco M390 Content Security Management Appliance Quick Start Guide

Cisco Systems, Inc.
www.cisco.com

- Cisco Notification Service

Welcome

Thank you for choosing the Cisco M390 Content Security Management Appliance (Cisco M390).

The Cisco M390 Content Security Management Appliance 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.

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 M390 Content Security Management Appliance:

- Rail kit
- Power cords
- Console cable
- A card listing the location of online documentation for your appliance.

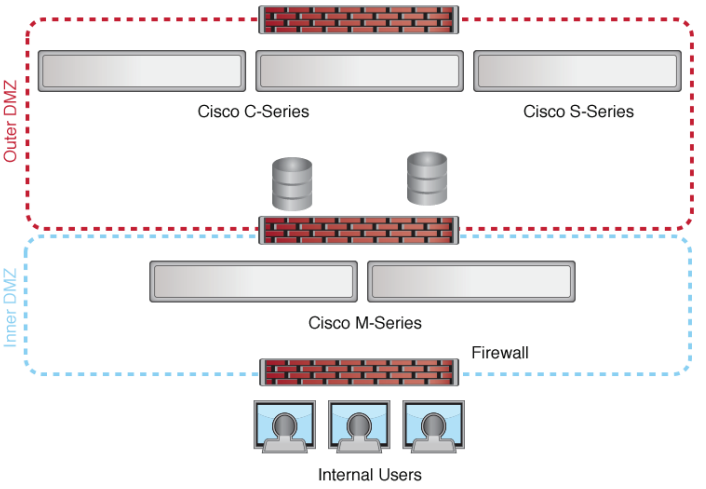
You will need to provide the following items yourself:

- Rack cabinet enclosure (if rack-mounting the appliance)
- Phillips-head screwdriver for assembling rails
- 10/100/1000 Base TX TCP/IP LAN
- Ethernet cable for connecting the appliance to your network
- Desktop or laptop computer
- Web browser (or SSH and terminal software)
- Network and administrator information for the "Plan the Installation" section on page 3

Plan the Installation

The Cisco M390 appliance is 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:



Document Required 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:	
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
Fully Qualified Appliance Hostname	
IP Address (Management port)	
Network Mask:	
Default Gateway (Router) IP Address:	
DNS (Use the Internet's root DNS servers or specify your own):	
Data Port 2	
IP Address:	
Network Mask:	

Install the Appliance in a Rack

Install the Cisco M390 Content Security Management Appliance following the instructions in 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.

Temporarily Change Your IP Address for Remote Access

To remotely configure the Cisco M390 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 M390, without changing the IP address. If you use the serial console, proceed to section 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

The exact steps depend on your operating system version.

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:

- IP Address: **192.168.42.43**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.42.1**

Step 9 Click **OK** and **OK** again to exit the dialog box.

For Mac

The exact steps depend on your operating system version.

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.

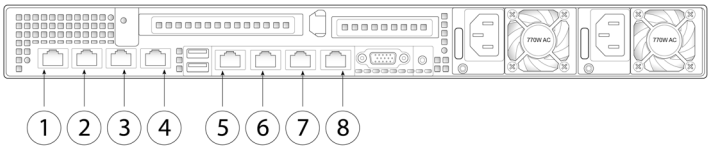
Step 6 Enter the following changes:

- IP Address: **192.168.42.43**
- Subnet Mask: **255.255.255.0**
- Router: **192.168.42.1**

Step 7 Click **OK**.

Connect to the Appliance

Connect your laptop to the Management port. The Cisco M390 appliance uses the Management port only.



Item	Port	Description
1	Data 1	A Gigabit Ethernet customer data interface.
2	Data 2	A Gigabit Ethernet customer data interface.
3	Data 3	A Gigabit Ethernet customer data interface.
4	Data 4	A Gigabit Ethernet customer data interface.
5	Remote Power Cycle	The port that is used for Remote Power Cycle (RPC).
6	Console	Console port that directly connects a computer to the appliance.
7	Data 5	A Gigabit Ethernet customer data interface.
8	Management interface	The Gigabit Ethernet interface that is restricted to management use only.

Plug In and Power Up the Appliance

Plug in the appliance, then power up the appliance by pressing the On/Off switch on the front panel of the Cisco M390. You must wait 10 minutes for the system to initialize each time you power up the system.

After the machine powers up, solid green lights on the front of the appliance indicate that the appliance is operational. The network activity light will be green but may not be solid.

Caution 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.

Log In to the Appliance

You can log into the Cisco M390 using 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 7), go to the Cisco M390 appliance 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**

- Password: **ironport**

Note 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.

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 7).
- 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**.

Step 3 At the prompt, run 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.

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**.

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

Step 6 Ensure that your laptop and the appliance are connected to the network.

Step 7 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.

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 8 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

Congratulations! 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.**

Where to Go From Here

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 M390 Content Security Management Appliance Quick 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://tools.cisco.com/RPF/register/register.do.