Quick Start Guide

Cisco M380 and Cisco M680 Content Security Management Appliance

Part Number: 78-21149-01

1 Welcome

Thank you for choosing the Cisco M380 and Cisco M680 Content Security Management Appliance (Cisco M380 and Cisco M680).

The Content Security Management appliance centralizes and consolidates important policy and runtime data, providing administrators and end-users with a single interface for managing their email and web security systems. It ensures top performance from Cisco C-Series and S-Series appliances, and protects corporate network integrity by increasing deployment flexibility.

The Content Security Management appliance provides the central platform for managing all reporting and auditing information for Cisco Email and Web Security appliances. Optional management features allow you to coordinate all your security operations from a single Content Security Management appliance or to spread the load across multiple appliances.

This guide describes how to physically install the Cisco M380 and Cisco M680 appliance and use the System Setup Wizard to configure basic settings.

2 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 M380 and Cisco M680 Content Security Management Appliance:

- Quick Start Guide (this guide)
- Slide rail kit
- Power cables (2)
- Ethernet cable for connecting the appliance to your network
- RJ-45 to DB-9 cable for connecting a computer to the console port
- Cisco Content Security documentation pointer card

Note Two locking keys are included with the locking faceplate version of the Cisco M680 appliance. Keep these keys safe because you will need the 4-digit key code to replace missing keys.

You will need to provide the following items yourself:

- Rack cabinet enclosure (if rack-mounting the appliance)
- 10/100/1000 Base TX TCP/IP LAN
- Desktop or laptop computer
- Web browser (or SSH and terminal software)
- Network and administrator information for the "Document Network Settings" section on page 4

3 Document Network Settings

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

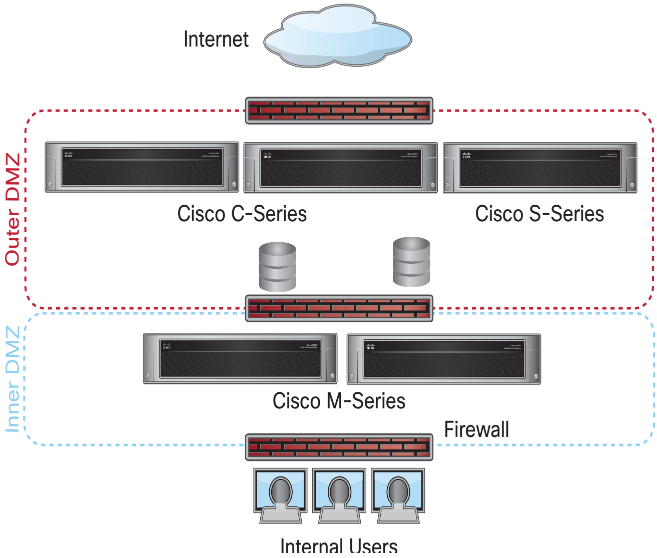
System Settings	
Default System Hostname:	
Deliver Scheduled Reports To:	
Time Zone Information:	
NTP Server:	
Admin Password:	
AutoSupport:	Enable/Disable
Network Integration	
Default Gateway (Router) IP Address:	
DNS (Internet or Specify Own):	
Interfaces	
Data Port 1	
IP Address:	
Network Mask:	
Fully Qualified Hostname:	
Data Port 2	
IP Address:	
Network Mask:	
Locking Faceplate	
4-digit code (for the M680-LKFP appliance)	

4 Plan the Installation

The Cisco M380 and Cisco M680 Content Security Management Appliance is designed to serve as an external or "off box" location to monitor corporate policy settings and audit information. It combines hardware, an operating system (AsyncOS), and supporting services to centralize and consolidate important policy and runtime data.

The Cisco M380 and Cisco M680 is designed to sit within your inner DMZ and receive quarantined spam from Cisco C-Series and S-Series appliances in your outer DMZ. Internal users access the Content Security Management appliance to view and manage messages in their quarantines.

Plan for your network configuration to look something like this:

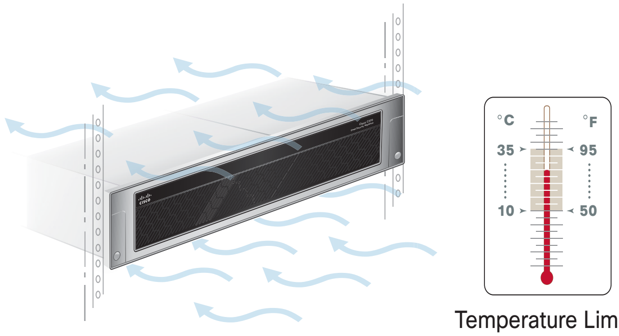


5 Install the Appliance in a Rack

Install the Cisco M380 and Cisco M680 Content Security Management Appliance using the slide rails supplied. For information about installing the appliance in a rack, see the *Cisco 380 and Cisco 680 Series Hardware Installation 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.

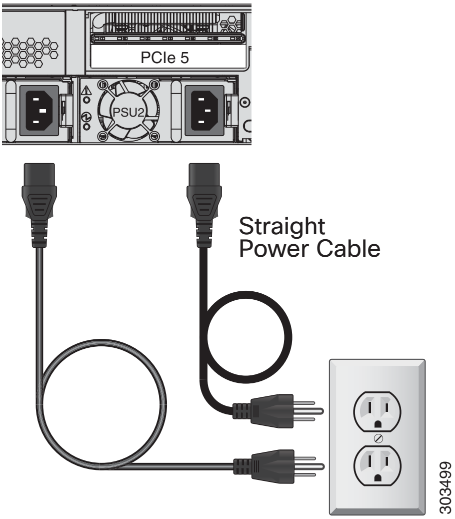


Temperature Limits

6 Plug In the Appliance

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

Plug the male end(s) into an electrical outlet.



7 Temporarily Change Your IP Address

To connect to the Cisco M380 and Cisco M680, you must temporarily change the IP address of your computer.

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

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

Step 2 Double-click **Network and Sharing Center**.

Step 3 Click **Local Area Connection** and then click **Properties**.

Step 4 Select **Internet Protocol** (**TCP/IP**) and then click **Properties**.

Step 5 Select **Use the Following IP Address**.

Step 6 Enter the following changes:

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

Step 7 Click **OK** and **Close** to exit the dialog box.

For Mac

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 Ethernet 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.

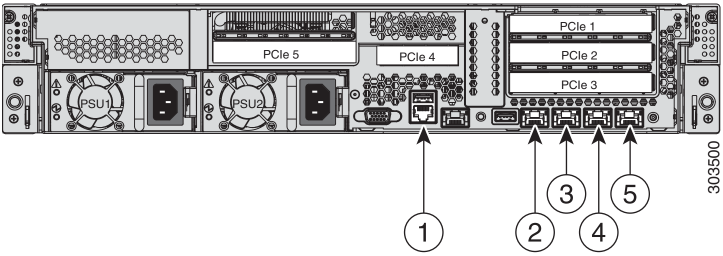
Step 6 Enter the following changes:

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

Step 7 Click **OK**.

8 Connect to the Appliance

Connect your laptop to the Management port using the Ethernet cable included in the system box. The Cisco M380 and Cisco M680 appliance uses the Management port only.



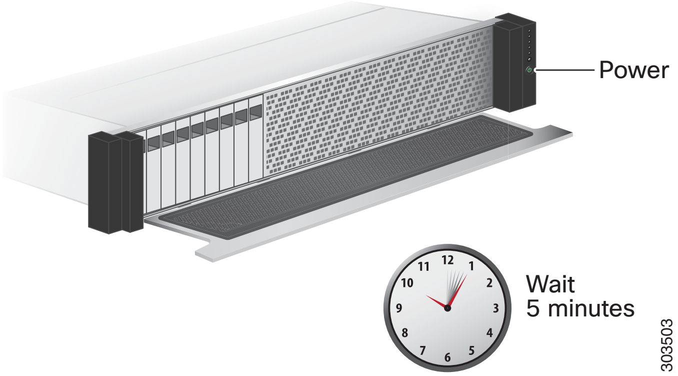
Item	Port	Description
1	Console	Indicates the console port that directly connects a computer to the appliance.
2	Management interface	Indicates the Gigabit Ethernet interface that is restricted to management use only. Connect with a RJ-45 cable.
3	Data 1	Indicates the Gigabit Ethernet customer data interface Data 1.
4	Data 2	Indicates the Gigabit Ethernet customer data interface Data 2.
5	Data 3	Indicates the Gigabit Ethernet customer data interface Data 3.

Note If you ordered a NIC card with your appliance, see the detailed information in the PCI NIC Slot Configurations section of the *Cisco 380 and Cisco 680 Series Hardware Installation Guide.*

9 Power Up the Appliance

Power up the appliance by pressing the On/Off switch on the front panel of the Cisco M380 and Cisco M680. You must wait five minutes for the system to initialize each time you power up the system. After the machine powers up, a solid green light indicates that the appliance is operational.

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.



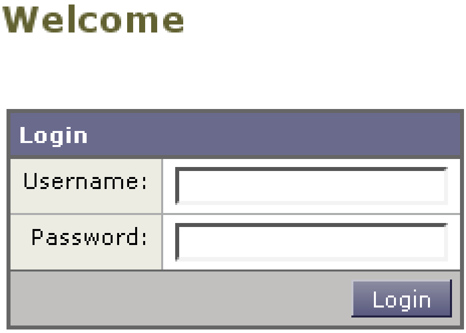
10 Log In to the Appliance

You can log into the Cisco M380 and Cisco M680 using one of two interfaces: 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 9), go to the Cisco M380 and Cisco M680 appliance management interface by entering the following URL in a web browser:

http://192.168.42.42:8080



303360

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:8080), you must add the appliance *hostname* and IP address to your DNS server database.

Step 3 Click **Login**.

Command-Line Interface

Step 1 For command-line interface access via the serial port (see the "Connect to the Appliance" section on page 9), access the command-line interface terminal emulator using 9600 bits, 8 bits, no parity, 1 stop bit (**9600, 8, N, 1**) and flow control set to Hardware.

Step 2 Initiate a telnet or SSH session to the IP address **192.168.42.42**.

Step 3 Log in as **admin** with the password **ironport**.

Step 4 At the prompt, run the **systemsetup** command.

11 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) and displays the end user license agreement (also known as the EULA).

Step 1 Start the System Setup Wizard.

Step 2 Accept the end user license agreement.

Step 3 Enter registration information.

Step 4 Enter information from the "Document Network Settings" section on page 4.

Step 5 Set web security settings.

Step 6 Review the configuration summary page.

Step 7 Log back in to the appliance with the username **admin** and the new password that you set in the System Setup Wizard.

The Cisco M380 and Cisco M680 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 Write down your new administrator password and keep it in a safe place.

12 Configure Network Settings

Depending on your network configuration, your firewall may need to be configured to allow access using the following ports. SMTP and DNS services must have access to the Internet.

- DNS: port 53
- SMTP: port 6025 and 25

For other system functions, the following services may be required:

- FTP: port 21, data port TCP 1024 and higher
- HTTP: port 80 or 82
- HTTPS: port 83 or 443
- LDAP: port 389 or 3268
- LDAP over SSL: port 636
- LDAP with SSL for global catalog queries: port 3269
- NTP: port 123
- Quarantine Authentication: 110 (POP) and/or 143 (IMAP)
- SSH: port 22
- Telnet: port 23

Note If you do not open port 443, you cannot download feature keys.

For more information, see the appendix, "Firewall Information" in the *Cisco AsyncOS for Content Security Management User Guide* for more information.

Warning **You must shut down your appliance from the System Administration > Shutdown/Reboot page to prevent corruption of your queue and configuration files.**

13 Configuration Summary

Review the following details of your configuration.

Item	Description
Management	You can manage your content security management appliance from the management port (Data 1) by entering http://192.168.42.42, or the hostname assigned to your appliance when you have completed the System Setup Wizard. If you reset your configuration to factory default settings (for example, by re-running the System Setup Wizard), you can only access the management interface from the Data 1 port (http://192.168.42.42), so ensure you have a connection to the Data 1 port. Also, verify that you open firewall ports 80 or 82 for HTTP, and 83 and 443 for HTTPS on your management interface.
Computer Address	Remember to change your computer IP address back to the original settings that you noted in the "Document Network Settings" section on page 4. You can review a summary of your system settings from the **Management Appliance > Centralized Services > Security Appliances** page.

14 You're Done!

Congratulations, you are now ready to start using your Cisco M380 and Cisco M680 Content Security Management Appliance. You may wish to consider taking some of the following steps to get more out of the appliance:

Adding Security Appliances

You can add the Cisco Email Security appliances and Cisco Web Security appliances that you want to manage. To add Cisco Security appliances to the Cisco M380 and Cisco M680, choose **Management Appliance > Centralized Services > Security Appliances.**

Enabling Centralized Email and Web Reporting

The Cisco M380 and Cisco M680 Content Security Management Appliance supports both email reporting and web reporting as well as web tracking, which allows a centralized view of email and web traffic across multiple Email and Web Security Appliances.

To enable centralized email reporting, choose **Management Appliance > Centralized Services > Email > Centralized Reporting.**

To enable centralized web reporting, choose **Management Appliance > Centralized Services > Web > Centralized Reporting.**

Once you have enabled centralized reporting, you can view statistics and information for web and email reporting from the **Management Appliance > Centralized Services > Email > Centralized Reporting or Management Appliance > Centralized Services > Web > Centralized Reporting Overview** page.

Message Tracking

You can view details about message delivery and blocking by running queries using the Message Tracking service (in the GUI).

To access message tracking for the email security appliance, choose Monitor > Message Tracking.

Scheduled Email and Web Reporting

The Cisco M380 and Cisco M680 Content Security Management Appliance allows you to generate scheduled reports from the data coming from your Email or Web Security Appliance. Reports can be scheduled to run on a daily, weekly, or monthly basis, and can be configured to include data for the previous day, previous seven days, or previous month.

More Information

There are other features that you may want to configure for your Cisco M380 and Cisco M680 appliance. For more information about other available features, see the Content Security Management appliance documentation.

15 Frequently Asked Questions

Q. How do I delete older Configuration Masters on my Cisco M380 and Cisco M680 Content Security Management Appliance?

A. Go to the **Web > Utilities > Security Services Display** page, and click **Edit Settings**. At the top of each Configuration Master you can uncheck the corresponding Configuration Master checkbox. Click **Submit** and that Configuration Master no longer shows up as a Configuration tab on the GUI.

Q. How do I add an appliance to my Cisco M380 and Cisco M680 Content Security Management Appliance?

A. After you have enabled monitoring services on the Cisco M380 and Cisco M680 appliance, you can add connection information for the appliances that it manages. You can connect any Cisco Email Security appliance using AsyncOS 6.0 or later, and any Cisco Web Security appliance running AsyncOS 5.7, 6.3, or 7.1 or later.

a. On the Cisco M380 and Cisco M680 Content Security Management Appliance, choose **Management Appliance > Centralized Services > Security Appliances**.

b. Click **Add Email Appliance** to display the Add Email Security Appliance page or click **Add Web Appliance** to display the Add Web Security Appliance page.

c. In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Cisco appliance.

d. Select the services that you want to use when managing the Cisco appliance.

e. Click **Establish Connection**.

f. Click **Test Connection** to verify that the monitoring services on the remote appliance have been correctly configured and are compatible.

g. If you are adding a Web Security appliance, choose the Configuration Master to which you want to assign the appliance.

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

Q. Do I need to forward access logs from the Web Security appliance to the Content Security Management appliance?

A. No. This is handled internally by the Web Security appliance once Centralized Reporting is enabled. To enable Centralized Reporting, go to **Management Appliance > Centralized Services > Web > Centralized Reporting**.

Q. How long is data available in the Web Reporting tool?

A. Data retention is dependent upon overall usage, that is, the number of records present. However, at a minimum, each appliance is sized to accommodate at least 45 days of reporting.

Q. How do I hide user names on my Web reports?

a. On the Cisco M380 and Cisco M680 Content Security Management Appliance, choose **Management Appliance > Centralized Services > Web > Centralized Reporting**.

b. Click **Edit Settings**.

c. Check the Anonymize User Names in Reports check box.

d. Click **Submit**.

Q. How often is reporting data updated?

A. The Cisco M380 and Cisco M680 Content Security Management Appliance pulls data for all reports from all managed appliances approximately every 15 minutes and aggregates the data from these appliances. Depending on your appliance, it may take awhile for a particular message to be included in the reporting data on the Content Security Management appliance. Check the System Status page for information on your data.

16 Where to Go From Here

Support	
Cisco Support Portal	http://www.cisco.com/support
U.S. and Canada Toll-Free Number	800-553-2447
International Contacts	Worldwide Phone Numbers
Email:	tac@cisco.com
Cisco Email Security Support Community Cisco Web Security Support Community (Includes Content Security Management Appliance Support)	https://supportforums.cisco.com/community/netpro/security/email https://supportforums.cisco.com/community/netpro/security/web
Product Documentation	
Cisco M380 and Cisco M680 Content Security Management Appliance Quick Start Guide (this document)	http://www.cisco.com/en/US/docs/security/security_management/sma/hw/quick_start/M380_M680_QSG_78_21149.pdf

Cisco 380 and Cisco 680 Series Hardware Installation Guide Includes information about LEDs, technical specifications, and mounting options.	http://www.cisco.com/en/US/docs/security/esa/hw/380_680_Series_HW_Install.pdf
Cisco Content Security Management Appliance Documentation Includes documentation about configuring the appliance features, CLI commands, and release notes.	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Safety and Compliance Guide	http://www.cisco.com/en/US/docs/security/content_security/compliance/ContentSecurity_regulatory_compliance_information.fm
MIBs	
AsyncOS MIBs for Cisco Content Security Management Appliance (Related Tools section)	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

♻ Printed in the USA on recycled paper containing 10% postconsumer waste.

Part Number: 78-21149-01