Cisco C390 Email Security Appliance Quick Start Guide

- Welcome
- Before You Begin
- Document Network Settings
- Plan the Installation
- Install the Appliance in a Rack
- Plug In the Appliance
- Temporarily Change Your IP Address for Remotes Access
- Connect to the Appliance
- Power Up the Appliance
- Log In to the Appliance
- Run the System Setup Wizard
- Run the Active Directory Wizard (Optional)
- Check for Available Upgrades
- Configure Network Settings
- Configuration Summary

Cisco Systems, Inc.
www.cisco.com

- Additional Configurations
- Where to Go from Here
- Cisco Notification Service

Welcome

Thank you for choosing the Cisco C390 Email Security Appliance (Cisco C390).

The Cisco C390 appliance is designed to serve as your SMTP email gateway at your network perimeter—that is, the first appliance with an IP address that is directly accessible to the Internet for sending and receiving email. Many of the features (including reputation filtering, data loss prevention, content scanning, spam detection, and virus protection) require you to install the Cisco appliance into your existing network infrastructure.

This guide describes how to physically install your Cisco C390 appliance and use the System Setup Wizard to configure basic settings.

Before You Begin

Before you begin the installation, make sure that you have the items needed.The following items are included with the
Cisco C390 Email Security Appliance:

- Rail kit
- Power cables (2)
- 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 "Document Network Settings" section on page 3 and "go live" configuration

Document Network Settings

Before you begin, write down the following information about your network and administrator settings.

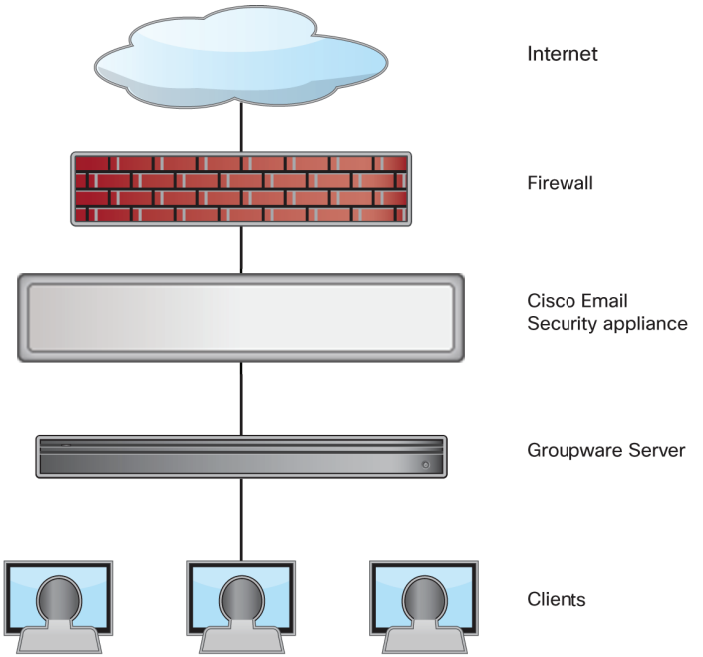
System Settings	
Default System Hostname:	
Email System Alerts To:	
Deliver Scheduled Reports To:	
Time Zone Information:	
NTP Server:	
Admin Password:	
SenderBase Network Participation:	Enable/Disable
AutoSupport:	Enable/Disable
Network Integration	
Default Gateway (Router) IP Address:	
DNS (Internet or Specify Own):	
Interfaces	
Data Port 1	
IP Address:	
Network Mask:	
Fully Qualified Hostname:	
Accept Incoming Mail Domain:	
Accept Incoming Mail Destination:	
Relay Outgoing Mail:	
Data Port 2	
IP Address:	
Network Mask:	
Fully Qualified Hostname:	
Accept Incoming Mail Domain:	
Accept Incoming Mail Destination:	
Relay Outgoing Mail:	
Message Security	

SenderBase Reputation Filtering:	Enable/Disable
Cisco Anti-Spam Scanning Engine:	Enable/Disable
McAfee Anti-Virus Scanning Engine:	Enable/Disable
Sophos Anti-Virus Scanning Engine:	Enable/Disable
Virus Outbreak Filters:	Enable/Disable
Advanced Malware Protection Scanning Engine	Enable/Disable

Plan the Installation

To defend your email system against spam, malware, phishing, and other threats, the Cisco C390 appliance must be installed at the perimeter of your network. It needs to be the first appliance with an IP address that can access the Internet.

Plan for your network configuration to look something like this:



Install the Appliance in a Rack

Install the Cisco C390 Email Security Appliance using the rails supplied. For information about installing the appliance in a rack, see the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*.

Appliance Placement in a Rack

- 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.

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.

Temporarily Change Your IP Address for Remotes Access

To remotely configure the Cisco C390 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 C390, without changing the IP address. If you use the serial console, proceed to section 8 below.

Note Make a note of your current IP configuration settings because 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 **Close** 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

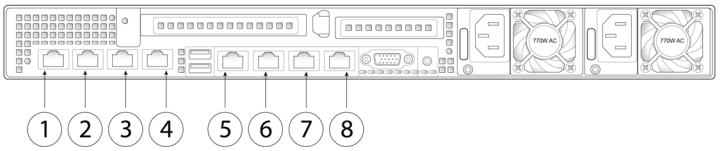
The Cisco C390 appliances have five gigabit network ports and a Management port, as shown in the figure on the following page . At least one static IP address is required to send and receive email.

You can receive and deliver email from a single connection to either network port if your network topology dictates it. Two IP addresses can be configured on one network interface.

Or, you can connect the Data 1 network port to your public network and connect the Data 2 network port to your private network.

To access and manage the appliance by Ethernet, use the Management network port. The IPv4 address that has been assigned to the Management port by the factory is 192.168.42.42.

For serial access to the appliance's console port, use the RJ-45 to DB-9 Rollover cable provided in the accessory kit to connect the computer to the console port on the appliance.



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.

Item	Port	Description
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	A Gigabit Ethernet interface that is restricted to management use only.

Power Up the Appliance

Power up the appliance by pressing the On/Off switch on the front panel of the Cisco C390. 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.

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.

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 in to the Cisco C390 appliance 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 7), go to the appliance's management interface by entering the following URL in a web browser:

http://192.168.42.42

Step 2 Log in with the following credentials:

- Username: **admin**
- Password: **ironport**

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

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 Start the System Setup Wizard.

Step 2 Accept the end user license agreement.

Step 3 Enter information from the "Document Network Settings" section on page 3.

Step 4 Set anti-spam and anti-virus security settings.

Step 5 Review the configuration summary page.

Step 6 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 7 If you temporarily changed the IP address of your computer as described in the "Temporarily Change Your IP Address for Remotes Access" section on page 5, 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 back in to the appliance with the username **admin** and the new password that you set in the System Setup Wizard.

The Cisco C390 Email Security 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 10 Write down your new administrator password and keep it in a safe place.

Run the Active Directory Wizard (Optional)

After running the System Setup Wizard in the web interface, the Active Directory Wizard appears. If you are running an Active Directory server on your network, use the Active Directory Wizard to configure an LDAP server profile for the Active Directory server.

If you are not using Active Directory or want to configure it later, click **Skip this Step**. You can run the Active Directory Wizard later by going to **System Administration > LDAP**. Select the "using Active Directory Wizard" check box, and then click **Add LDAP Server Profile**.

Note You will need the hostname and login information for your Active Directory account to run the Active Directory Wizard.

Note Commit any changes you make in the GUI by clicking **Commit Changes**. This button appears if you have any uncommitted changes that need to be saved.

303359

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.

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

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 25

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

- 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
- SSH: port 22
- Telnet: port 23

Note If you do not open port 80 and port 443, you cannot download feature keys.

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

Configuration Summary

Item	Description
Management	You can manage your email security appliance from the management port (Data Port 1) by entering http://192.168.42.42 or by using the hostname assigned to your appliance during system setup. Also, verify that you open firewall ports 80 and 443 on your management interface.
Incoming Email	After running the System Setup Wizard, your Data Port 2 port is configured to accept inbound email.
Outbound Email	To configure the appliance to relay outbound email if you did not do so in the System Setup Wizard, see the user guide for your version of AsyncOS for Cisco Email Security Appliances.

Additional Configurations

Congratulations! You have completed installation and basic configuration. You can now configure additional features of your appliance. See the online help or user guide for your AsyncOS release for complete details.

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, choose **Monitor > Message Tracking**.

Reporting

You can view statistics about spam and virus blocking on your network by viewing reports available in the Email Security Monitor (in the GUI). To access the reporting overview page, choose **Monitor > Overview**.

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

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

Where to Go from Here

Product Documentation	
Cisco Email Security Appliance Documentation	http://www.cisco.com/c/en/us/support/security/email-security-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 C390 Email Security 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	http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html
Cisco Email Security Support Community	https://supportforums.cisco.com/community/5756/email-security

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.