QUICK START GUIDE

Cisco C170 Email Security Appliance

1 Welcome
2 Before You Begin
3 Document Network Settings
4 Plan the Installation
5 Install the Appliance in a Rack
6 Plug In the Appliance
7 Temporarily Change Your IP Address
8 Connect to the Appliance
9 Power Up the Appliance
10 Log In to the Appliance
11 Run the System Setup Wizard
12 Run the Active Directory Wizard (Optional)
13 Configure Network Settings
14 Configuration Summary
15 You’re Done!
16 Where to Go from Here
1 Welcome

Thank you for choosing the Cisco C170 Email Security Appliance (Cisco C170).

The Cisco C170 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 C170 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 C170 Email Security Appliance:

- Quick Start Guide (this guide)
- Rails and adaptor kit
- Power cable(s)
- Ethernet cable for connecting the appliance to your network
- Regulatory Safety and Compliance Information

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 Gigabit Base-T 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 and “go live” configuration
3 Document Network Settings

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

<table>
<thead>
<tr>
<th>System Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default System Hostname:</td>
<td></td>
</tr>
<tr>
<td>Email System Alerts To:</td>
<td></td>
</tr>
<tr>
<td>Deliver Scheduled Reports To:</td>
<td></td>
</tr>
<tr>
<td>Time Zone Information:</td>
<td></td>
</tr>
<tr>
<td>NTP Server:</td>
<td></td>
</tr>
<tr>
<td>Admin Password:</td>
<td></td>
</tr>
<tr>
<td>SenderBase Network Participation:</td>
<td>Enable/Disable</td>
</tr>
<tr>
<td>AutoSupport:</td>
<td>Enable/Disable</td>
</tr>
</tbody>
</table>

| Network Integration                         |       |
| Default Gateway (router) IP Address:        |       |
| DNS (Internet or specify own):              |       |

| Interfaces                                  |       |
| P1                                          |       |
| IP Address:                                  |       |
| Network Mask:                                |       |
| Fully Qualified Hostname:                    |       |
| Accept Incoming Mail Domain:                |       |
| Accept Incoming Mail Destination:           |       |
| Relay Outgoing Mail:                         |       |
| P2                                          |       |
| 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 |
4 Plan the Installation

To defend your email system against spam, viruses, phishing, and other threats, the Cisco C170 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 C170 Email Security Appliance using either the slide rails or fixed rack mount brackets. For information about these installation options, see the Cisco 170 Series Hardware Installation 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.
6 Plug In the Appliance

Plug the female end of the power cable into the power supply on the back panel of the appliance. Plug the male end into an electrical outlet.
7 Temporarily Change Your IP Address

To connect to the Cisco C170 appliance, you must temporarily change the IP address of your computer.

**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

- **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** Select the network configuration with the green icon. This is your active connection. Then click Advanced.

**Step 4** Click the TCP/IP tab and from Ethernet settings, choose Manually from the drop-down list.

**Step 5** Enter the following changes:
- IP Address: 192.168.42.43
- Subnet Mask: 255.255.255.0
- Router: 192.168.42.1

**Step 6** Click OK.
8 Connect to the Appliance

The Cisco C170 appliance has two gigabit network ports: P1 and P2. 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 P1 network port to your public network and connect the P2 network port to your private network.

To access the appliance by Ethernet, connect to P1 as your management interface and configure incoming email on P2.

Or, for serial access to the appliance, connect to the console port.

P1:
Management: 192.168.42.42
Connect the P1 port to your computer using an Ethernet cable.

P2:
Incoming Email
Connect the P2 port to your network using an Ethernet cable.
9 Power Up the Appliance

Power up the appliance by pressing the On/Off switch on the front panel of the Cisco C170. After the appliance powers up, a solid green light indicates that the appliance is operational.

10 Log In to the Appliance

You can log in to the Cisco C170 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 10), go to the appliance’s management interface by entering the following URL in a web browser:

http://192.168.42.42

Welcome

Step 2  Enter the following login information:
- Username: admin
- Password: ironport

Command-Line Interface

Step 1  For command-line interface access via the serial port (see the “Connect to the Appliance” section on page 10), access the command-line interface by terminal emulator using 9600 bits, 8 bits, no parity, 1 stop bit (9600, 8, N, 1) and setting flow control set to Hardware.

Step 2  Initiate a 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

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 anti-spam and anti-virus 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 C170 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 8** Write down your new administrator password and keep it in a safe place.
12 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.
13 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 the appendix “Firewall Information” in the Cisco AsyncOS for Email Security Configuration Guide.

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management</strong></td>
<td>You can manage your email security appliance from the management port (P1) by entering <a href="http://192.168.42.42">http://192.168.42.42</a> 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.</td>
</tr>
<tr>
<td><strong>Incoming Email</strong></td>
<td>After running the System Setup Wizard, your P2 port is configured for inbound email.</td>
</tr>
<tr>
<td><strong>Outbound Email</strong></td>
<td>After running the System Setup Wizard, your appliance is configured to accept inbound email. You can also configure it to relay outbound email during system setup. For instructions on configuring outbound email, see the <em>Cisco AsyncOS for Email Configuration Guide</em>.</td>
</tr>
<tr>
<td><strong>Computer Address</strong></td>
<td>Remember to change your computer IP address back to the original settings that you noted in the “Temporarily Change Your IP Address” section on page 8.</td>
</tr>
</tbody>
</table>
15  You’re Done!

Congratulations. You are now ready to start using your Cisco C170 Email Security Appliance. You may wish to consider taking some of the following steps to get more out of the appliance.

**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*. 
## Where to Go from Here

### Support

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco IronPort Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>U.S. Toll-Free Number</strong></td>
<td>1-800-553-2447</td>
</tr>
<tr>
<td></td>
<td>1-408-526-7209</td>
</tr>
<tr>
<td><strong>Online Technical Support and</strong></td>
<td><a href="http://www.cisco.com/support">Link</a></td>
</tr>
<tr>
<td><strong>Documentation (login may be</strong></td>
<td></td>
</tr>
<tr>
<td><strong>required)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Email Security</strong></td>
<td><a href="https://supportforums.cisco.com/community/netpro/security/email">Link</a></td>
</tr>
<tr>
<td><strong>Appliance Support Community</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Product Documentation

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco C170 Email Security</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Appliance Quick Start Guide</strong></td>
<td></td>
</tr>
<tr>
<td>(this document)</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco 170 Series Hardware</strong></td>
<td><a href="http://www.cisco.com/en/US/docs/security/esa/hw/170Series_HW_Install.pdf">Link</a></td>
</tr>
<tr>
<td><strong>Installation Guide</strong></td>
<td></td>
</tr>
<tr>
<td>Includes information about LEDs,</td>
<td></td>
</tr>
<tr>
<td>technical specifications, and</td>
<td></td>
</tr>
<tr>
<td>rack-mounting options.</td>
<td></td>
</tr>
</tbody>
</table>
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.