



Installing a Memory Upgrade for the Cisco S370, C370, C670, or X1070 Content Security Appliances

September 14, 2015

78-100615-02

Contents

This document includes the following sections:

- [Overview](#)
- [How to Contact Cisco Support](#)
- [Regulatory Compliance and Safety Information](#)
- [Working in an ESD Environment](#)
- [Upgrading the Memory](#)
- [Related Documentation](#)

Overview

Cisco S370 Web Security Appliance (WSA) and C370, C670, or X1070 Email Security Appliances (ESAs) with 4 GB of memory may experience issues running either Cisco AsyncOS for Web Security 8.0.x or higher, or AsyncOS for Email Security 8.5.x or higher.

If you have one or more Cisco S370 WSAs or C370, C670, or X1070 Email Security Appliances (ESAs) with 4 GB, Cisco will contact you and provide you with a memory upgrade kit for each of your affected appliances and the serial numbers of the appliances that need to be upgraded. The kit enables you to upgrade the memory to 8 GB.



How to Contact Cisco Support

If you have any questions about the following upgrade instructions, contact Cisco at x70_mem_upgrade@cisco.com.

Regulatory Compliance and Safety Information

Before installing or replacing this hardware equipment in your content security appliance, read the Regulatory Compliance and Safety Information for the Cisco S370 WSA or C370, C670, or X1070 ESAs on Cisco.com or on the product CD that ships with the chassis.



Warning

Before working on the chassis, unplug the AC power cord.

Working in an ESD Environment

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures. Always follow ESD-prevention procedures when you remove and replace components. Ensure that the chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground unwanted ESD voltages. To guard against ESD damage and shocks, the wrist strap and cord must operate properly. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

Upgrading the Memory



Note

This procedure does not affect your Cisco warranty. Upgrading the memory of Cisco S370 WSAs or C370, C670, or X1070 ESAs to 8 GB does not require any special tools and does not create any radio frequency leaks.

-
- Step 1** Use the command-line interface (CLI) and the serial numbers provided by Cisco to locate the appliances that need to be upgraded. If your appliances are dispersed in various geographical locations, the CLI will enable you to remotely determine where the affected appliances are physically located.
- a.** To verify that you have located the correct appliances, use the **version** command to display the serial numbers of the affected appliances. This can be done locally or remotely.
 - b.** To further verify that you have located the appliances with only 4 GB of memory, enter the **ipcheck** command and look for the value of “RAM Total” in the output. This can be done locally or remotely.
- Step 2** Go to where each of the affected appliances are physically located and log into them using either the CLI or the web GUI.

- Step 3** Use the web GUI or the CLI to shut down the appliance.
- Using the CLI, enter the **shutdown** command. Then enter the number of seconds to wait before the connections are forcibly closed.
 - Using the GUI, select the **Shutdown/Suspend** option under the **System Administration** menu, and select **Shutdown** from the **Operation** drop-down menu in the **System Operations** section. Then enter the number of seconds to wait before the connections are forcibly closed, and click Commit.

For more information, see either the User Guide or the CLI Reference Guide for the appropriate version of the Cisco AsyncOS, located on the following listing pages:

- For ESAs (running Cisco AsyncOS for Email Security 8.5.x or higher):
 - [User Guides](#)
 - [Command Reference Guides](#)
- For WSAs (running Cisco AsyncOS for Web Security 8.0.x or higher):
 - [User Guides](#)
 - There no Command Reference Guides for the WSA. For information about the CLI commands, see the User Guides

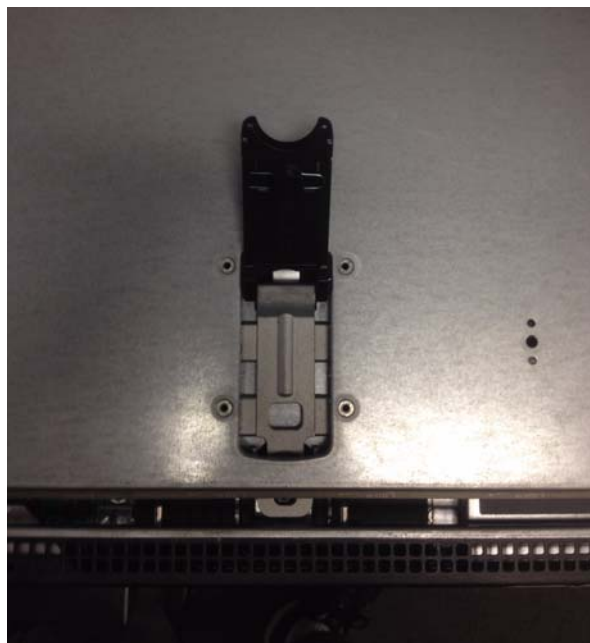
- Step 4** Once the appliance has completely shut down, disconnect all of the cables, including the network, power, and serial interface cables.



Warning

Before working on the chassis, unplug the AC power cord.

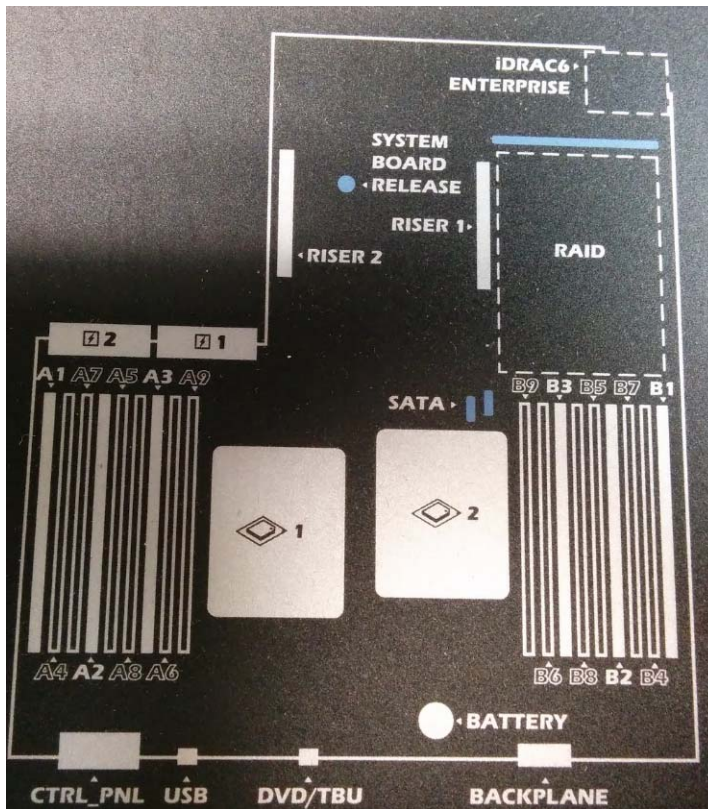
- Step 5** Remove the appliance from the rack.
- Step 6** Locate a wrist grounding strap and connect one end to the appliance, and securely attach the other to your wrist so it contacts your bare skin. For more information, see the “[Working in an ESD Environment](#)” section on page 2.
- Step 7** Open the top cover of the chassis by lifting the latch on the front center of the cover, as shown below.



- Step 8** Use the handles on the inner cover for the DIMMs to lift and remove it. A decal on the center of the inner cover shows how to safely remove it. One of the handles of the inner covers is shown below.



- Step 9** Locate the DIMMs in the memory slots as shown below.



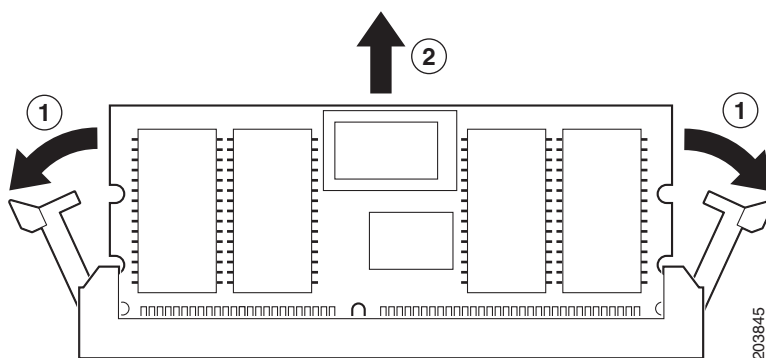
- Step 10** Remove the four 1GB DIMMs and replace them with the 2GB DIMMs, one at a time. Repeat the following procedure for each DIMM.

**Caution**

You must insert the new DIMMs into the same slots used by the old DIMMs. To ensure the same slots are used, replace the DIMMs one at a time.

If you do not insert the new DIMMs into correct slots, the appliance will not boot when the power is turned on.

- a. Pull the latches away from the DIMM at both ends, as shown below. Note that the following figure shows a DIMM that may be different from the DIMM you will be installing.



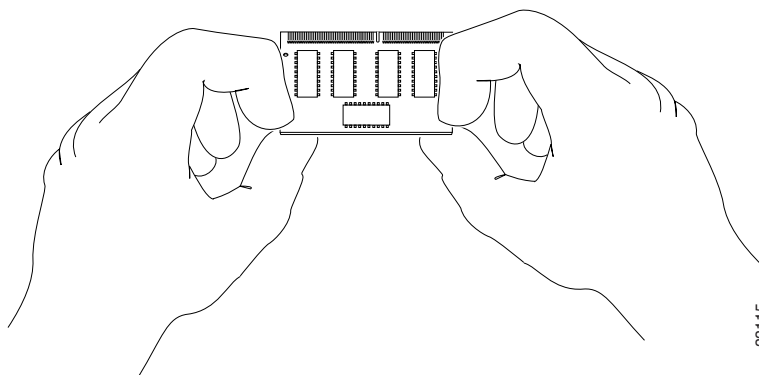
- b. Remove the 1GB DIMM and dispose of it.

When both ends of the DIMM are released from the socket, grasp the ends of the DIMM with your thumb and forefinger and pull the DIMM completely out of the socket.

- c. Remove a new 2GB DIMM from the antistatic container.

**Caution**

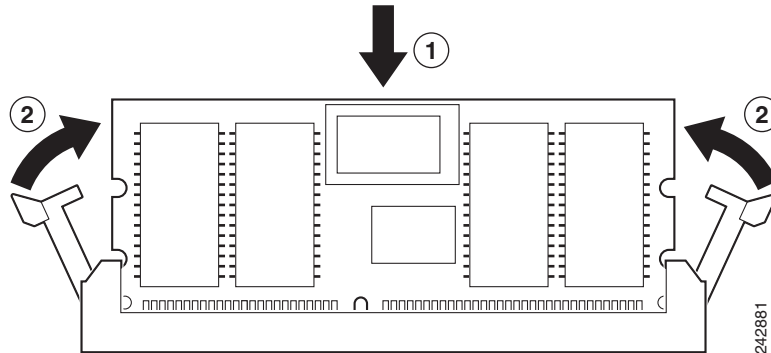
To prevent ESD damage, handle the edges of the DIMM only; avoid touching the memory modules, pins, or traces (the metal fingers along the connector edge of the DIMM), along the connector edge, as shown below. Note that the DIMM shown below may be different from the DIMM you will be installing.



- d. Hold the DIMM component side up, with the connector edge away from you. Line up the notch in the connector traces with the notch in the socket on the board.

The DIMM is designed in such a way that the connector will fit only one way.

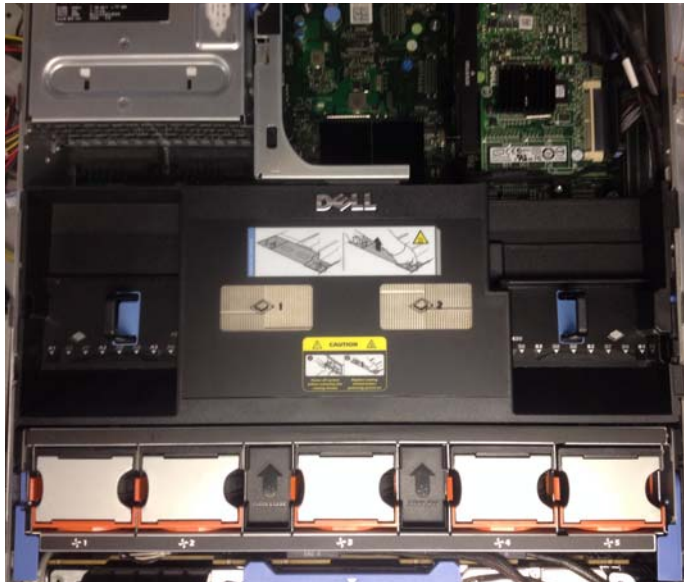
- e. Carefully insert the connector edge into the socket and firmly press the DIMM into the socket until both latches rotate to the closed position against the DIMM, as shown below. Note that the DIMM shown below may be different from the DIMM you will be installing.



Caution

When inserting DIMMs, use firm but not excessive pressure. You can cause damage to the socket.

- Step 11** After installing the four new DIMMs, replace the inner cover to its original position as shown below.



- Step 12** Replace and latch the chassis cover.
- Step 13** Replace the appliance in the rack and reconnect all of the cables, including the network, power, and serial interface cables.
- Step 14** Turn on the power switch to boot the appliance.
- Step 15** Wait at least five minutes for the system to initialize. Then verify that the appliance is operational.



Note

When the power is turned on, the fans spin and the LEDs light up. Within 30-60 seconds, the fans stop and all LEDs turn off. The appliance powers on 31 seconds later. When the power-up sequence is complete, a solid green light indicates that the appliance is operational.

**Caution**

The power-up behavior is by design to allow the system firmware and controller to synchronize.

If you do not wait for the power-up sequence to complete, and turn the appliance off, you might cause permanent damage and prevent the system from being able to ever complete the power up sequence.

Related Documentation

Documentation for Cisco Email Security Appliances

The Email Security User Guides for the affected versions of Cisco AsyncOS are located on this page:
<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html>

The Email Security CLI References Guides for the affected versions of Cisco AsyncOS are located on this page:

<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html>

The Email Security Release Notes for the affected versions of Cisco AsyncOS are located on this page:
<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html>

The Hardware Installation Guides and QuickStart Guides for the affected appliances are located on this page:

<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html>

Documentation for Cisco Web Security Appliances

The Web Security User Guides for the affected versions of Cisco AsyncOS are located on this page:
<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html>

The Web Security Release Notes for the affected versions of Cisco AsyncOS are located on this page:
<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html>

The Hardware Installation Guides and QuickStart Guides for the affected appliances are located on this page:

<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html>

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2015 Cisco Systems, Inc. All rights reserved.

