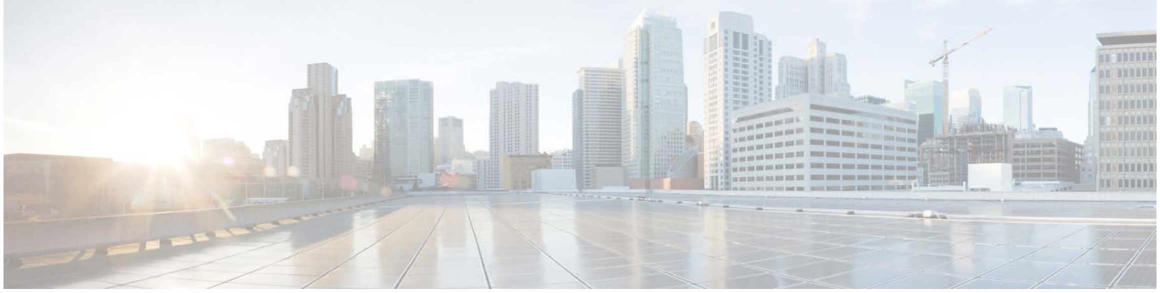

Deploying Cisco Secure Email Gateway and Secure Email and Web Manager Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services

Published: May 4, 2023

Revised: June 20, 2023

Contents

About Cisco Content Security Virtual Appliances

Cisco Content Security virtual appliances function the same as physical Secure Email Gateway (formerly known as Email Security Appliance or ESA) and Secure Email and Web Manager (formerly known as Security Management Appliance or SMA), with only a few minor differences, which are documented in Managing Your Virtual Appliance, page 9.

For implementations on the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) deployments, use the Amazon Machine Images (AMI) available in the Amazon Marketplace.

Cisco Systems, Inc.
www.cisco.com

Note Cisco Secure Email Gateway and Secure Email and Web Manager virtual appliances are supported on AWS EC2.

About Amazon Machine Image

You can use an Amazon Machine Image (AMI) to create a virtual machine instance inside EC2. AMIs for Secure Email and Web Manager are available in the AWS marketplace. Secure Email Gateway is not available in the AWS marketplace, contact Cisco TAC with your AWS account details (username and region) to provision an AMI image.

Choose the AMI you require and proceed with deployment.

Cisco Secure Email Gateway and Secure Email and Web Manager Virtual Appliance AMIs

Cisco Secure Email Virtual Gateway

AsyncOS for Cisco Secure Email Virtual Gateway Release	Virtual Appliance	AMI ID
AsyncOS 15.0	C600V	Contact Cisco TAC to obtain the AMI ID.

Cisco Secure Email and Web Manager Virtual

AsyncOS for Cisco Secure Email and Web Manager Virtual Release	Virtual Appliance	AMI ID
AsyncOS 15.0	M600V	Contact Cisco TAC to obtain the AMI ID.

Cisco Secure Email and Web Manager Virtual public AMIs

Perform the following steps to find the shared public AMIs using the console:

1. Contact Cisco TAC to obtain the AMI ID.
2. Open the Amazon EC2 console.
3. Choose **AMIs** in the navigation pane.
4. Choose **Public images** in the first filter.
5. In the search bar, enter the “build number” and “model” according to the virtual appliance model you require.

Licensing

You can use your existing Secure Email Gateway or Secure Email and Web Manager appliance license for deployments in Amazon AWS. After you deploy and launch the instance, you can install the license. You will have to pay only the AWS infrastructure charges.

If you are an existing customer, see the Obtain a Virtual License (VLN) topic in the Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses tech notes. If you are a new customer, contact your nearest Cisco partner to obtain a license.

Deploying on AWS

Note Cisco Secure Email Gateway on-premise appliances are not supported on Cisco Secure Email and Web Manager appliance deployments on AWS.

Perform the following steps to deploy a Secure Email Gateway or Secure Email and Web Manager virtual appliance:

	Do This	More Info
Step 1	Prepare your environment by completing prerequisite tasks and acquiring information that you need before setting up an instance in EC2.	Preparing Your Environment, page 4.
Step 2	Select the AMI from the Amazon Marketplace, and choose the appropriate instance type. **Note** Secure Email Gateway is not available in the AWS marketplace, contact Cisco TAC with your AWS account details (username and region) to provision an AMI image.	Selecting Virtual Appliance AMI and Choosing Instance Type, page 4.
Step 3	Configure the network, subnet, IP address assignment, and other details necessary for your instance to be available and function as required. **Note** One primary network interface (management), is automatically assigned to an instance. If required, you can create data interfaces (D1, D2 for C600V).	Configuring Instance Details, page 6.
Step 4	Retain the default storage settings or configure the tags as required.	Configuring Storage, page 7.
Step 5	Configure the security group. Review all the configuration settings and launch the instance.	Configuring Security Group, Review, and Launch Instance, page 7.
Step 6	Install the license in the appliance.	Configuring Your Launched Instance, page 7.
Step 7	Connect to the appliance’s web interface. You can run the System Setup Wizard, upload a configuration file, or configure features.	Connecting to the Appliance’s Web Interface, page 8.

	Do This	More Info
Step 8	(Optional) If required, configure Elastic IP addresses in the AWS EC2 Management Console.	Creating Elastic IP Addresses, page 8.
Step 9	Configure the appliance for license expiration alerts.	Configuring Appliance to Send Alerts, page 9.

Preparing Your Environment

Make sure you have the required resources and files to deploy the Secure Email Gateway or Secure Email and Web Manager virtual appliance on AWS EC2. These include:

- A valid license for Secure Email Gateway or Secure Email and Web Manager virtual appliance.
- The default username and password for your Secure Email Gateway or Secure Email and Web Manager virtual appliance:
  - `admin` and `ironport`
- Resources in your EC2 Management Console:
  - If you require a persistent public IP address that can be associated to instances, decide which Elastic IP address to use, or create a new one. The public IP address which is automatically assigned during the process of launching a new instance is dynamic.
  - Ensure you know which VPC to use, or configure a VPC to use with the deployment. You can also use the default VPC.
  - Based on how administrators and other users will access the appliance, you must determine the type of IP address to be assigned to the appliance (public or private).
  - Be aware of which IAM role to use, or configure a IAM role to use with the deployment.
  - Configure the subnet, and ensure that the routing table has the default route pointing to the Internet gateway.
  - Configure the Security Group, or create a new one.
  - The most common ports to open for the virtual appliance to communicate properly are:
    - SSH TCP 22
    - TCP 443
    - (Optional) ICMP, where required, for debugging.
- Confirm that you are able to access the private key (PEM or CER file) you want AWS to register with the EC2 instance. You can also create a new private key during the process of launching the virtual appliance instance.

Note For Windows clients, you need an SSH client to access the PEM file.

Selecting Virtual Appliance AMI and Choosing Instance Type

Ensure you have the correct region selected in your AWS account.

1. Navigate to your EC2 Management Console.
2. Click **Launch Instance**, select **Launch Instance** from the drop-down list.

3. Click **AWS Marketplace**.

Note Secure Email Gateway is not available in the AWS marketplace, contact Cisco TAC with your AWS account details (username and region) to provision an AMI image.

4. Select the instance type based on the virtual appliance model. For example, if you need the Secure Email Gateway virtual appliance C600V model, select c4.4xlarge, and the corresponding vCPU, vRAM, and so on.

Product	AsyncOS Version	Model	EC2 Instance Type	vCPU	vRAM	vNIC	Minimum Disk Size
Cisco Secure Email Gateway Virtual Appliance	AsyncOS 15.0 and later (Email)	**C600V**	c4.4xlarge	16	30 GB	1 (*)	500 GB
	AsyncOS 14.0 and later (Email)	**C100V**	c4.xlarge	4	7.5 GB	1 (*)	200 GB
		C300V	c4.2xlarge	8	15 GB	1 (*)	500 GB
		C600V	c4.4xlarge	16	30 GB	1 (*)	500 GB

(*) Single NIC is presented by default, but the user can create an additional interface when initiating the instance.

Note You must add additional interfaces before your email gateway boots up for the first time. If you add an additional interface after your email gateway boots up, the interface is not detected by your email gateway.

Product	AsyncOS Version	Model	EC2 Instance Type	vCPU	vRAM	Minimum Disk Size
Cisco Secure Email and Web Manager Virtual Appliance	AsyncOS 15.0 and later	**M600V**	c4.2xlarge	8	15 GB	2032 GB
	AsyncOS 14.0 and later	**M100V**	Currently, image is not available.	-	-	-
		M300V	c4.xlarge	4	7.5 GB	1024 GB
		M600V	c4.2xlarge	8	15 GB	2032 GB

Note You must add additional interfaces before Secure Email and Web Manager boots up for the first time. If you add an additional interface after your Secure Email and Web Manager boots up, the interface is not detected by your Secure Email and Web Manager.

5. Click **Next: Configure Instance Details**.

Configuring Instance Details

1. Enter the number of instances.

Note The spot instances purchasing option allows you to buy spare compute capacity in the AWS cloud. Refer to Amazon EC2 documentation for more information.

2. Choose the correct VPC from the **Network** drop-down list.
3. Choose the subnet required for this deployment, from the **Subnet** drop-down list.
4. Choose the required option from the **Auto-assign Public IP** drop-down list:
   - Choose **Use subnet setting (Enable)** to assign a public IP address according to the settings specified in the subnet settings.
   - Choose **Enable** to request a public IP address for this instance. This option overrides the subnet settings for public IP addresses.
   - Choose **Disable** if you do not require an auto assigned public IP. This option overrides the subnet settings for public IP addresses.
5. Choose the IAM role.
6. Choose the **Shutdown behavior**. Cisco recommends choosing **Stop**.

Caution Choosing **Terminate** will delete the instance and all its data.

7. (Optional) Check the **Protect against accidental termination** check box.
8. (Optional) Review and select other options like **Monitoring**, **EBS-optimized instance**, and **Tenancy**, according to your requirements.
9. Choose the **Network Interface**.
   - You can add more interfaces if required, from previously created network interfaces.
   - To add another network interface, choose **Add Device**. You can specify up to two network interfaces when you launch an instance. After you launch the instance, choose **Network Interfaces** in the navigation pane to add additional network interfaces.
   - You cannot auto-assign a public IP address if you specify more than one network interface.
   - There is a maximum number of network interfaces you can create for an instance type. See Step 4.of Selecting Virtual Appliance AMI and Choosing Instance Type, page 4.
   - See Creating Elastic IP Addresses, page 8 to create static IP addresses.

Configuring Storage

Retain the default storage options. You may edit them as required.

Note Cisco recommends using Provisioned IOPS SSD for all deployments. You may use General Purpose SSD, but Provisioned IOPS SSD provides optimal performance. It may take up to 45 minutes for your instance to be available to log in for the first time.

Configuring Security Group, Review, and Launch Instance

1. Select the correct **Security Group** for the deployment.
2. Click **Review and Launch**.
3. Review your configuration, and ensure that all the details match your requirements.
4. Launch the instance.
5. Select an existing Key Pair, or create a new Key Pair and download it. Creating an instance without a Key Pair is not supported.
6. Click **Launch** to launch the instance.
7. Click **Instances**.

   You will be able to view the newly configured instance in the EC2 **Instances** page. If the instance's checks are successful, under the **Status Checks** column, a green check mark is displayed, followed by **2/2 checks passed**.
8. (Optional) View the system log by performing the following steps:
   a. Select the instance in the **Instances** page.
   b. Click **Actions**.
   c. Click **Get System Log** under **Instance Settings**.
   d. If you see a login prompt, this indicates that the instance is up, and running.
9. (Optional) If you have chosen to assign a public IP to the instance, check if you access it using the public IP address.

Configuring Your Launched Instance

1. Click **Instances** on your EC2 navigation panel.
2. Select the instance, and click **Connect**.
3. Review the connectivity information in the **Connect to Your Instance** dialog box. You will need this information to connect to the virtual appliance through SSH. This includes the PEM file used with the public DNS. Ensure that your key is not publicly visible.

   Note The default username is `admin`, and not root as displayed.
4. Use an SSH client to connect to the instance.
5. Use the `loadlicense` command to paste the license via CLI, or load from a file.

Note For M600V appliances with the recommended 15 GB vRAM, you will see warning messages about a mis-configured virtual machine image, or the RAID status being suboptimal. These warning messages will display when using CLI commands like `loadlicense` and `upgrade`. You may safely ignore these messages. The vRAM configuration will not have an impact on the normal functioning of the appliance.

Connecting to the Appliance's Web Interface

Use the web interface to configure the appliance software. When you select an instance, the IP address is displayed in the **Description** tab. The default username and password are `admin` and `ironport`.

The following table lists the default ports for the virtual appliances:

Product	HTTP Port	HTTPS Port
Cisco Secure Email Gateway	80	443
Cisco Secure Email and Web Manager	80	443

For example, you can:

- Run the System Setup Wizard

  Note The IP address and the default gateway are picked from AWS. These can be retained. It is good practice to set all malware to Block.

- Upload a configuration file.
- Manually configure features and functionality.
- For instructions on accessing and configuring the appliance, including gathering required information, see the online help or user guide for your AsyncOS release, available from the relevant location in Additional Information, page 12.
- To migrate settings from a physical appliance, see the release notes for your AsyncOS release.
- Feature keys are not activated until you enable the respective features.

Creating Elastic IP Addresses

To create an Elastic IP address, perform the following steps:

1. Click **Elastic IPs** in the EC2 navigation pane.
2. Click **Allocate new address**.
3. Click **Allocate**. A new public IP address is allocated. You can either click the IP address, or click **Close**.
4. Select the IP address you created.
5. Click **Actions**, and choose **Associate Address**.
6. Select the **Resource type**.
7. Choose the instance from the drop-down list.
8. Choose the private IP address to associate the Elastic IP address.

9. Click **Associate**.
10. Click **Close**.

Configuring Appliance to Send Alerts

For information on configuring the appliance to send alerts when the license is about to expire, see the online help or user guide for your AsyncOS release, available from the relevant location in Additional Information, page 12.

Managing Your Virtual Appliance

Virtual Appliance License

Note You cannot open a Technical Support tunnel before installing the virtual appliance license. The information about Technical Support tunnels is available in the User Guide for your AsyncOS release.

The Cisco Content Security virtual appliance requires an additional license to run the virtual appliance on a host. You can use this license for multiple, cloned virtual appliances.

For Cisco Secure Email Gateway virtual appliances:

- Feature keys for individual features can have different expiration dates.
- After the virtual appliance license expires, the appliance will continue to serve as an SMTP proxy (Cisco Secure Email Gateway) or automatically handle quarantined messages (Secure Email and Web Manager) without security services for 180 days. Security services are not updated during this period. On the Content Security Management appliance, administrators and end users cannot manage quarantines, but the management appliance continues to accept quarantined messages from managed Secure Email Gateway appliances, and scheduled deletion of quarantined messages will occur.

Note For information about the impact of reverting the AsyncOS version, see the online help or user guide for your AsyncOS release.

Powering Off Virtual Appliance

Force reset, power off, and reset options are not fully supported. You can terminate or stop the instance running the Secure Email Gateway or Secure Email and Web Manager virtual appliance.

CLI Commands on Virtual Appliance

The following are the CLI command changes for virtual appliances:

Command	Supported on Virtual Secure Email Gateway	Supported on Virtual Secure Email and Web Manager?	Information
`loadlicense`	Yes	Yes	This command allows you to install a license for your virtual appliance. You cannot run System Setup Wizard on the virtual appliance without installing a license using this command first.
`etherconfig`	Yes	—	The Pairing option is not included on virtual appliances.
`version`	Yes	—	This command will return all the information about the virtual appliance except for the UDI, RAID, and BMC information.
`resetconfig`	Yes	—	Running this command leaves the virtual appliance license and the feature keys on the appliance.
`revert`	Yes	—	Behavior is described in the System Administration chapter in the online help and user guide for your appliance.

`diagnostic`	Yes	Yes	The following `diagnostic > raid` sub-menu options will not return information:
			`1. Run disk verify`
			`2. Monitor tasks in progress`
			`3. Display disk verify verdict`

`showlicense`	Yes	Yes	View license details. For virtual Cisco Secure Email Virtual Gateway, additional information is available via the `featurekey` command.

SNMP on Virtual Appliance

AsyncOS on virtual appliances will not report any hardware-related information and no hardware-related traps will be generated. The following information will be omitted from queries:

- `powerSupplyTable`
- `temperatureTable`
- `fanTable`
- `raidEvents`
- `raidTable`

Getting Support for Virtual Appliances

Note To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.

If you file a support case for a Cisco Content Security virtual appliance, you must provide your contract number and your Product Identifier code (PID).

You can identify your PID based on the software licenses running on your virtual appliance, by referencing your purchase order, or from the following lists:

- Product Identifier Codes (PIDs) for Cisco Secure Email Virtual Gateway, page 11
- Product Identifier Codes (PIDs) for Cisco Secure Email and Web Manager Virtual, page 12

Product Identifier Codes (PIDs) for Cisco Secure Email Virtual Gateway

Functionality	PID	Description
Cisco Secure Email	CSEMAIL-SEC-SUB	A Cisco Secure Email software subscription license that can be deployed on-premises, cloud or hybrid. This Stock Keeping Unit (SKU) only allows prepaid and annual billing options.
Essential		Includes: • Anti-spam filtering • Outbreak Filtering • Sophos Anti-Virus filtering • Cisco Secure Email Malware Defense - includes reputation and Cisco Threat Grid sandboxing capabilities
Advantage		Includes: • All Essential features • Cisco Secure Email Encryption Service • Cisco Data Loss Protection (DLP)
Premier		Includes: • All Advantage features • Cisco Secure Awareness Training

Functionality	PID	Description
Add-on - Intelligence Multiscan		Provides additional antispam classification capabilities by combining the results of the multiple antis-pam classifiers with the Cisco IPAS classifier in the Inbound and Premium Bundles. It increases the spam catch rate at the possible expense of a greater number of false positives.
Add-on: Graymail Safe Unsubscribe		Allows users who receive legitimate marketing emails to unsubscribe safely through a third party.
Add-on: McAfee Anti-Malware		Provides additional anti-virus protection as an add-on to the Sophos Anti-Virus engine that comes with the Inbound and Premium Bundles.
Add-on: Image Analyzer		Provides scanning for adult content in images contained in emails, often deployed along with DLP to implement acceptable user policies.
Centralized Email Management	SMA-EMGT-LIC	All centralized Secure Email functionality.

Product Identifier Codes (PIDs) for Cisco Secure Email and Web Manager Virtual

Functionality	PID	Description
Cisco Secure Email and Web Manager Appliance (SMA)	SMA-EMGT-LIC	All Centralized Email Security Functionality

Cisco TAC

Contact information for Cisco TAC, including phone numbers: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Additional Information

For more information, including information about support options, see the Release Notes and User Guide or online help for your AsyncOS release.

Documentation For Cisco Content Security Products:	Is Located At:
Cisco Secure Email and Web Manager	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
Cisco Secure Email Gateway	https://www.cisco.com/c/en/us/support/security/email-security-virtual-appliance/series.html
Cisco Secure Web Appliance	https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html

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.