

Cisco Content Security Virtual Appliances on AWS EC2 Installation Guide

First Published: 2023-09-22

Last Modified: 2025-09-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **About Cisco Content Security Virtual Appliances** 1

About Amazon Machine Image 1

Cisco Secure Email Gateway, Secure Web, and Secure Email and Web Manager Virtual Appliance AMIs 1

Licensing 2

CHAPTER 2 **Deploying on AWS** 3

Deploying on AWS 3

Prepare Your Environment 4

Select the Virtual Appliance AMI and Choose the Instance Type 5

Deploying Secure Web Appliance (SWA) on AWS for Coeus 14.5 7

Deploying Secure Web Appliance (SWA) on AWS for Coeus 15.2.4 8

Configure Instance Details 8

Configure Storage and Add Tags 9

Configure Security Group, Review, and Launch Instance 10

Configure Your Launched Instance 10

Connect to the Appliance's Web Interface 11

Creating Elastic IP Addresses 12

Configure the Appliance to Send Alerts When License Expiration Nears 12

CHAPTER 3 **Managing Your Virtual Appliance** 13

The Virtual Appliance License 13

Powering Off a Virtual Appliance 14

CLI Commands on the Virtual Appliance 14

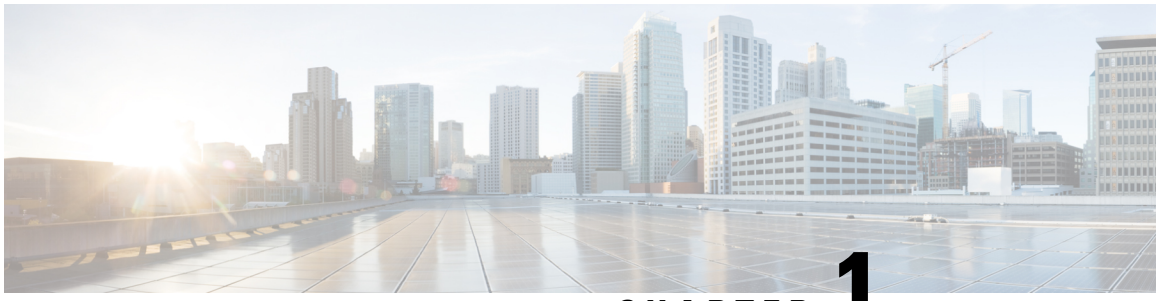
SNMP on the Virtual Appliance 15

Getting Support for Virtual Appliances 15

Cisco TAC 18

APPENDIX A **Additional Information 19**

Additional Information 19



CHAPTER 1

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), Secure Web Appliance (formerly known as Web Security Appliance or WSA) 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.

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

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

- About Amazon Machine Image, on page 1
- Licensing, on page 2

About Amazon Machine Image

You can use an Amazon Machine Image (AMI) to create a virtual machine instance inside EC2. AMIs for Secure Web Appliance and Secure Email and Web Manager are available in the AWS marketplace. Secure Email Gateway is not available in the AWS marketplace, contact your Cisco sales representative 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, Secure Web, and Secure Email and Web Manager Virtual Appliance AMIs

The following tables list the AMI details for Cisco Secure Email Gateway, Secure Web, and Secure Email and Web Manager virtual appliances:

Cisco Secure Email Gateway Virtual Appliance (AsyncOS 14.0.0-692)

AsyncOS for Cisco Secure Email Gateway Virtual Appliance Release	Virtual Appliance	AMI ID
AsyncOS 14.0.0-692	**C100V**	Cisco Secure Email Virtual Gateway-14-0-0-692-C100V-200421.ami
	C300V	Cisco Secure Email Virtual Gateway-14-0-0-692-C300V-200421.ami
	C600V	Cisco Secure Email Virtual Gateway-14-0-0-692-C600V-200421.ami

Cisco Secure Email and Web Manager Virtual Appliance (AsyncOS 14.0.0-404) public AMIs

To find the shared public AMIs using the console, perform the following steps:

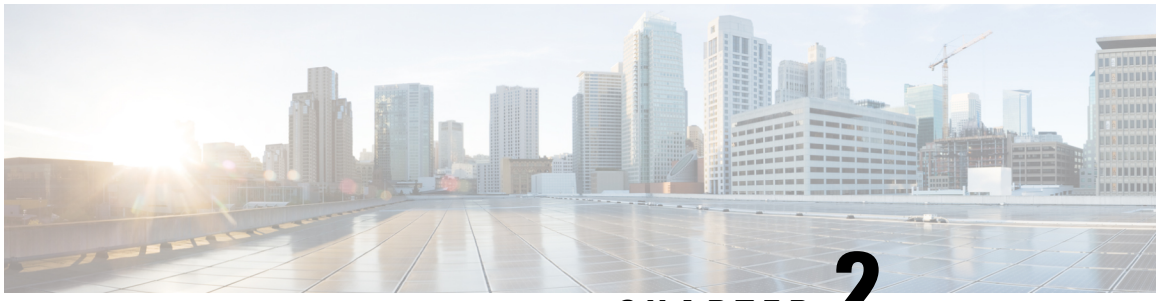
1. Open the Amazon EC2 console.
2. In the navigation pane, choose **AMIs**.
3. In the first filter, choose **Public images**.
4. Choose the search bar and enter zeus-14-0-0-404-M600V according to the virtual appliance model you require.

Cisco Secure Email and Web Manager Virtual Appliance (AsyncOS 14.0.0-404)	AMI ID
M600V	zeus-14-0-0-404-M600V-AMI-230421
M300V	zeus-14-0-0-404-M300V-AMI-230421
M100V	Currently, no image is available.

Licensing

You can use your existing Secure Email Gateway, Secure Web 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 be required 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.



CHAPTER 2

Deploying on AWS

- Deploying on AWS, on page 3
- Prepare Your Environment, on page 4
- Select the Virtual Appliance AMI and Choose the Instance Type, on page 5
- Configure Instance Details, on page 8
- Configure Storage and Add Tags, on page 9
- Configure Security Group, Review, and Launch Instance, on page 10
- Configure Your Launched Instance, on page 10
- Connect to the Appliance's Web Interface, on page 11
- Creating Elastic IP Addresses, on page 12
- Configure the Appliance to Send Alerts When License Expiration Nears, on page 12

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, Secure Web 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 will need before setting up an instance in EC2.	Prepare Your Environment
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 your Cisco sales representative with your AWS account details (username and region) to provision an AMI image.	Select the Virtual Appliance AMI and Choose the Instance Type.

	Do This	More Info
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 (P1, for S100V; P1, P2 for S300V and S600V).	Configure Instance Details
Step 4	Retain the default storage settings or configure the tags as required.	Configure Storage and Add Tags.
Step 5	Configure the security group. Review all the configuration settings and launch the instance.	Configure Security Group, Review, and Launch Instance.
Step 6	Install the license in the appliance, and disable the web interface from responding with the appliance-specific hostname. Use the **hostheader** command, and commit the change.	Configure Your Launched Instance.
Step 7	Connect to the appliance's web interface. You can run the System Setup Wizard, upload a configuration file, or configure features.	Connect to the Appliance's Web Interface.
Step 8	(Optional) If required, configure Elastic IP addresses in the AWS EC2 Management Console.	Creating Elastic IP Addresses.
Step 9	Configure the appliance for license expiration alerts.	Configure the Appliance to Send Alerts When License Expiration Nears.

Prepare Your Environment

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

- A valid license for Secure Email Gateway, Secure Web, or Secure Email and Web Manager virtual appliance.
- The default username and password for your Web Security 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
- TCP 8443
- TCP 3128
- (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 will need an SSH client to access the PEM file.

Select the Virtual Appliance AMI and Choose the Instance Type

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

Procedure

Step 1 Navigate to your EC2 Management Console.

Step 2 Click **Launch Instance**, select **Launch Instance** in the drop-down list.

Step 3 Click **AWS Marketplace**.

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

Step 4 Select the instance type based on the virtual appliance model. For example, if you need the Secure Web virtual appliance S300V model, select c4.xlarge, 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 16.0.3 and later (Email)	**C600V**	c6i.4xlarge	16	32 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.

Product	AsyncOS Version	Model	EC2 Instance Type	vCPU	vRAM	vNIC	Minimum Disk Size
Cisco Secure Web Virtual Appliance	AsyncOS 14.5 and later (Web)	**S100V**	c5.xlarge	4	8 GB	2	200 GB
		S300V	c5.2xlarge	8	16 GB	3	500 GB
		S600V	c5.4xlarge	16	32 GB	3	750 GB
	AsyncOS 14.0 and later (Web)	**S100V**	m4.large	2	8 GB	2	200 GB
		S300V	c4.xlarge	4	7.5 GB	3	500 GB
		S600V	c4.4xlarge	16	30 GB	3	750 GB

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

Note

- When you configure a C100V and S300V appliance with 7.5 GB vRAM, you will see warning messages about a misconfigured 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.
- If you use split routing on Secure Web virtual appliance, you need to assign a public IP address (Elastic IP) to the proxy listening port.

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

Deploying Secure Web Appliance (SWA) on AWS for Coeus 14.5

For a successful AWS scan for coeus 14.5, perform the below steps:

Procedure

Step 1 Deploy AMI with the respective **C4** instance type as listed in the following table:

Model	Instance Type
S100V	m4.large
S300V	c4.2xlarge
S600V	c4.4xlarge

Step 2 Once an instance is active, verify its reachability by connecting to it using **SSH** and admin credentials.

Step 3 Shut down the instance using the Secure Web Appliance CLI, and verify the instance using the AWS CLI.

Step 4 To update the instances, connect the AWS CLI with the Access Key ID and Secret Access Key.

Step 5 To check if ENA is already enabled in the EC2 instance, execute the following command with the instance ID and region.

```
aws ec2 describe-instances --instance-id <your-instance-id>
--query"Reservations[].Instances[].EnaSupport" --region <your-region>
```

- If ENA is enabled successfully, it returns status as **'True'**. Proceed to Step 7.
- If ENA is not enabled, it returns an empty string. Proceed to the next step.

Step 6 To enable ENA in a EC2 instance, execute the following command:

```
aws ec2 modify-instance-attribute --instance-id <your-instance-id> --ena-support --region <your-region>
```

Note
This command does not return any output. Go to Step 5.

Step 7 Change the instance type from **C4** to **C5** as listed in the following table:

Model	Instance Type
S100V	c5.xlarge
S300V	c5.2xlarge
S600V	c5.4xlarge

Step 8 Start the instance.

What to do next

Note Upgrade of AWS instances from coeus 14.0 to coeus 14.5 are not supported. We recommend you to deploy the new instance in coeus 14.5.

If you have an AWS instance running in coeus-14-0, and want to create a compatible configuration to load the newly deployed coeus 14.5 instance, upgrade coeus-14-0 instance to coeus 14.5. You can then download the configuration. For more information, see Saving, Loading, and Resetting the Appliance Configuration topic of the Cisco Secure Web Appliance User Guide (Recommended only to obtain compatible coeus 14.5 configuration).

For procedure to load the compatible configuration in the newly deployed coeus 14.5 instance, see the Loading the Appliance Configuration File topic of the Cisco Secure Web Appliance User Guide.

For more information on:

- AWS CLI Installation and Setup, see

  https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html.

- Setup and prerequisite configuration for using AWS CLI, see

  https://docs.aws.amazon.com/cli/latest/userguide/getting-started-prereqs.html.

Deploying Secure Web Appliance (SWA) on AWS for Coeus 15.2.4

Starting with AsyncOS 15.2.4, you can deploy virtual Secure Web Appliance (SWA) in AWS using C5 instance types. You no longer need to deploy a C4 instance and change it to C5; deploy the SWA with a C5 instance type directly.

Configure Instance Details

Procedure

Step 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.

Step 2 Choose the correct VPC in the **Network** drop-down list.

Step 3 Choose the subnet required for this deployment, in the **Subnet** drop-down list.

Step 4 Choose the required option in 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 subnetsettings 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.

Step 5 Choose the IAM role.

Step 6 Choose the **Shutdown behavior**. Cisco recommends choosing **Stop**.

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

Step 7 (Optional) Check the **Protect against accidental termination** check box.

Step 8 (Optional) Review and select other options like **Monitoring**, **EBS-optimized instance**, and **Tenancy**, according to your requirements.

Step 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 Select the Virtual Appliance AMI and Choose the Instance Type.
- See Creating Elastic IP Addresses to create static IP addresses.

Configure Storage and Add Tags

Procedure

Step 1 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.

Step 2 Enter the tags required. You can create a tag or multiple tags for an instance.

For example, *name* as the key and its value, *Cisco wsa*.

Configure Security Group, Review, and Launch Instance

Procedure

Step 1 Select the correct **Security Group** for the deployment.

Step 2 Click **Review and Launch**.

Step 3 Review your configuration, and ensure that all the details match your requirements.

Step 4 Launch the instance.

Step 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.

Step 6 Click **Launch** to launch the instance.

Step 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**.

Step 8 (Optional) View the system log by performing the following steps:

a. In the **Instances** page, select the instance.

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.

Step 9 (Optional) If you have chosen to assign a public IP to the instance, check if you access it using the public IP address.

Configure Your Launched Instance



Note On the Secure Web Appliance, SSH access for the default 'admin' user works only with key-basedauthentication. Password-based authentication will be available for users who are configured using the **userconfig** CLI command and the application GUI under **System Administration** > **Users**.

Procedure

Step 1 Click **Instances** on your EC2 navigation panel.

Step 2 Select the instance, and click **Connect**.

Step 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.

Step 4 Use an SSH client to connect to the instance.

Step 5 Use the **loadlicense** command to paste the license via CLI, or load from a file.

Note
For C100V and S300V appliances with the recommended 7.5 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.

Step 6 Disable the web interface from responding with the appliance-specific hostname. Use the **adminaccessconfig > hostheader** CLI, and commit the change.

See the Additional Security Settings for Accessing the Appliance topic in the Perform System Administration Tasks chapter in the Cisco Secure Web Appliance user guide.

Connect 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 Web Appliance	8080	8443
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 is 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.
- 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

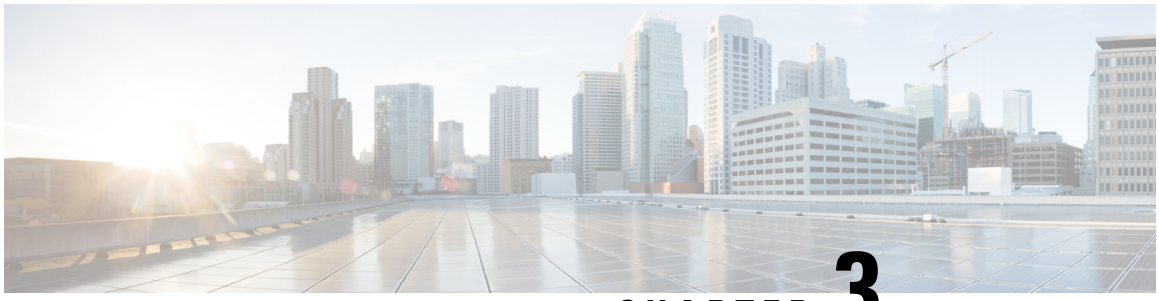
To create an Elastic IP address, perform the following steps:

Procedure

Step 1 In the EC2 navigation pane, click **Elastic IPs**.
Step 2 Click **Allocate new address**.
Step 3 Click **Allocate**. A new public IP address will be allocated. You can either click the IP address, or click **Close**.
Step 4 Select the IP address you created.
Step 5 Click **Actions**, and choose **Associate Address**.
Step 6 Select the **Resource type**.
Step 7 Choose the instance in the drop-down list.
Step 8 Choose the private IP address to associate the Elastic IP address.
Step 9 Click **Associate**.
Step 10 Click **Close**.

Configure the Appliance to Send Alerts When License Expiration Nears

See the online help or user guide for your AsyncOS release, available from the relevant location in Additional Information.



CHAPTER 3

Managing Your Virtual Appliance

- The Virtual Appliance License, on page 13
- Powering Off a Virtual Appliance, on page 14
- CLI Commands on the Virtual Appliance, on page 14
- SNMP on the Virtual Appliance, on page 15
- Getting Support for Virtual Appliances, on page 15
- Cisco TAC, on page 18

The Virtual Appliance License

Note You cannot open a Technical Support tunnel before installing the virtual appliance license. Information about Technical Support tunnels is 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 and Cisco Secure Web 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), web proxy (Cisco Secure Web Appliance), 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 a 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, Secure Web or Secure Email and Web Manager virtual appliance.

CLI Commands on the Virtual Appliance

The following are the CLI command changes for virtual appliances:

Command	Supported on Virtual Secure Email Gateway	Supported on Virtual Secure Web Appliance?	Supported on Virtual Secure Email and Web Manager?	Information
loadlicense	Yes	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	Yes	—	The Pairing option is not included on virtual appliances.
version	Yes	Yes	—	This command will return all the information about the virtual appliance except for the UDI, RAID, and BMC information.
resetconfig	Yes	Yes	—	Running this command leaves the virtual appliance license and the feature keys on the appliance.
revert	Yes	Yes	—	Behavior is described in the System Administration chapter in the online help and user guide for your appliance.
reload	Yes	Yes	—	Running this command removes the virtual appliance license and all the feature keys on the appliance. This command is available only for Secure Web Appliance.

Command	Supported on Virtual Secure Email Gateway	Supported on Virtual Secure Web Appliance?	Supported on Virtual Secure Email and Web Manager?	Information
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** This command is only available for Secure Web Appliance.
showlicense	Yes	Yes	Yes	View license details. For virtual Cisco Secure Web appliances, additional information is available via the **featurekey** command.

SNMP on the 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 Gateway Virtual Appliances
- Product Identifier Codes (PIDs) for Cisco Secure Web Virtual Appliances

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

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
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.

Functionality	PID	Description
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 Web Virtual Appliances

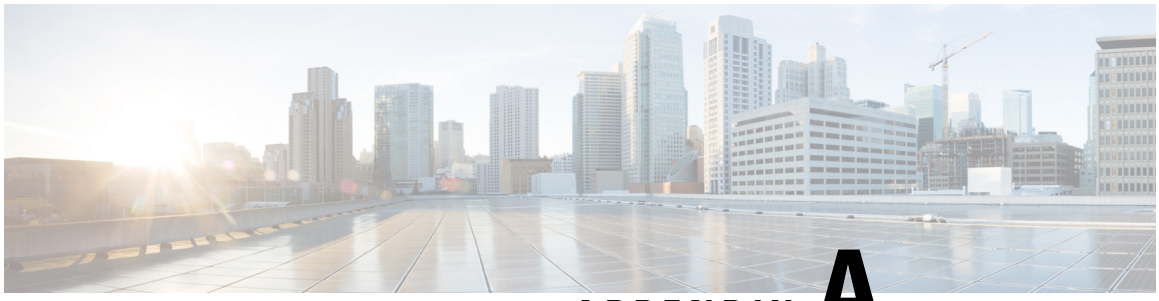
Functionality	PID	Description
Cisco Secure Web	WEB-SEC-SUB	Cisco Web Security Unified SKU
Web Security Essentials	WSA-WSE-LIC	Includes: • Web Usage Controls • Web Reputation
Web Security Advantage	WSA-WSP-LIC	Includes: • Essentials feature • Sophos and Webroot Anti-Malware signatures
Web Security Premier	WSA-WSS-LIC	Includes: • Advantage feature • Cisco Advanced Malware Protection • Cisco Cognitive Threat Analytics • Cisco Threat Grid
McAfee Anti-Malware	WSA-AMM-LIC	—
Advanced Malware Protection	WSA-AMP-LIC	—
SMA Centralized Web Management	SMA-WMGT-LIC	All centralized Secure Web functionality.
SMA Add-On: Advanced Reporting - Higher Data Tier	SMA-WSPL-HIGH-LIC	—

Functionality	PID	Description
SMA Add-On: Advanced Reporting - Lower Data Tier	SMA-WSPL-LOW-LIC	—

Cisco TAC

Contact information for Cisco TAC, including phone numbers:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html



APPENDIX A

Additional Information

- Additional Information, on page 19

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:
Secure Email and Web Manager	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
Secure Web Appliance	https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html
Secure Email Gateway	https://www.cisco.com/c/en/us/support/security/email-security-virtual-appliance/series.html

Additional Information