Deploying Cisco Web Security and Security Management Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services

Published: December 5, 2018

Contents

About Cisco Content Security Virtual Appliances

Cisco Content Security virtual appliances function the same as physical web security, or Content Security management hardware appliances, 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.

Note Cisco Web Security and Security Management virtual Appliances are supported on AWS EC2.

Cisco Systems, Inc.
www.cisco.com

About Amazon Machine Image

You can use an Amazon Machine Image (AMI) to create a virtual machine instance inside EC2. AMIs for Web Security appliance and Security Management appliance are available in the AWS marketplace. Choose the AMI you require and proceed with deployment.

Cisco Web Security and Security Management Virtual Appliance AMIs

The AMI details for Cisco Web Security and Security Management virtual appliances are as shown below:

Cisco Web Security Virtual Appliance (AsyncOS 11.7.0-333)
You can upgrade to AsyncOS 11.7.0-333 from your existing AsyncOS 11.5.1-115 and 11.5.0-614 deployments.

AsyncOS for Cisco Web Security Appliance Release	Virtual Appliance	AMI ID
AsyncOS 11.5.1-115	**S100V**	coeus-11-5-91-001-S100V-AMI-300818
	S300V	coeus-11-5-91-001-S300V-AMI-310818
	S600V	coeus-11-5-91-001-S600V-AMI-310818
AsyncOS 11.5.0-614	**S100V**	coeus-11-5-0-614-S100V-AMI-110518
	S300V	coeus-11-5-0-614-S300V-AMI-120518
	S600V	coeus-11-5-0-614-S600V-AMI-120518

Cisco Security Management Virtual Appliance (AsyncOS 11-5-1-114) 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-11-5-1-114-M100V, or zeus-11-5-1-114-M300V, or zeus-11-5-1-114-M600V, according to the virtual appliance model you require.

Cisco Security Management Virtual Appliance (AsyncOS 11.5.0-108)	AMI ID
M100V	zeus-11-5-0-108-M100V-AMI-040518
M300V	zeus-11-5-0-108-M300V-AMI-050518
M600V	zeus-11-5-0-108-M600V-AMI-050518

Licensing

You can use your existing Web Security or Security Management 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.

Deploying on AWS

Note

- The L4 Traffic Monitor functionality is not supported in Web Security virtual appliance releases AsyncOS 11.5 and 11.5.1.
- Web Traffic Tap is not supported in Web Security virtual appliance release AsyncOS 11.5.1.
- Cisco Email Security on-premise appliances are not supported on Cisco Security Management appliance deployments on AWS

To deploy a Web Security or Security Management virtual appliance, perform the following steps:.

	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, page 4.
Step 2	Select the AMI from the Amazon Marketplace, and choose the appropriate instance type.	Select the Virtual Appliance AMI and Choose the Instance Type, page 5.
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, page 5.
Step 4	Retain the default storage settings or configure the tags as required.	Configure Storage and Add Tags, page 6.
Step 5	Configure the security group. Review all the configuration settings and launch the instance.	Configure Security Group, Review, and Launch Instance, page 6.
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, page 7.

	Do This	More Info
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, page 7.
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.	Configure the Appliance to Send Alerts When License Expiration Nears, page 8.

Prepare Your Environment

Make sure you have the required resources and files to deploy the Web Security or Security Management virtual appliance on AWS EC2. These include:

- A valid license for Web Security or Security Management 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 Web Security or Security Management 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.

1. Navigate to your EC2 Management Console.
2. Click **Launch Instance**, select **Launch Instance** in the drop-down list.
3. Click **AWS Marketplace**.
4. Select the instance type based on the Cisco Web Security or Security Management virtual appliance model. For example, if you need the Web Security 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 Web Security Virtual Appliance	AsyncOS 11.5 and later (Web)	**S100V**	m4.large	2	6 GB	2	250 GB
		S300V	c4.xlarge	4	7.5 GB	4	1024 GB
		S600V	c4.4xlarge	16	30 GB	8	1024 GB

Product	AsyncOS Version	Model	EC2 Instance Type	vCPU	vRAM	Minimum Disk Size
Cisco Content Security Management Virtual Appliance	AsyncOS 11.5	**M100V**	m4.large	2	6 GB	250 GB
		M300v	c4.xlarge	4	7.5 GB	1024 GB
		M600v	c4.2xlarge	8	8 GB	2032 GB

Note

- When you configure an S300V appliance with 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.
- If you use split routing, you will need to assign a public IP address (Elastic IP) to the proxy listening port.

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

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

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 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 Select the Virtual Appliance AMI and Choose the Instance Type, page 5.
   - See Creating Elastic IP Addresses, page 8 to create static IP addresses.

Configure Storage and Add Tags

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.

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

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. 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.
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

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 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.
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 Web Security 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 default ports are 8443 for https, and 8080 for http.

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, page 11.
- 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. In the EC2 navigation pane, click **Elastic IPs**.
2. Click **Allocate new address**.
3. Click **Allocate**. a new public IP address will be 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 in the drop-down list.
8. Choose the private IP address to associate the Elastic IP address.
9. Click **Associate**.
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, page 11.

Managing Your Virtual Appliance

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 Web Security 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 a web proxy (Cisco Web Security appliance), or automatically handle quarantined messages (Security Management appliance) 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 Email Security 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 Cisco Web Security or Security Management virtual appliance.

CLI Commands on the Virtual Appliance

The following are the CLI command changes for virtual appliances:

Command	Supported on Virtual WSA?	Supported on Virtual SMA?	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.

Command	Supported on Virtual WSA?	Supported on Virtual SMA?	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.
reload	Yes	—	Running this command removes the virtual appliance license and all the feature keys on the appliance. This command is available only for the Cisco Web Security appliance.

diagnostic	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 the Web Security appliance.

showlicense	Yes	Yes	View license details. For virtual Cisco Web security 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 Virtual Web Security Appliances, page 11
- Product Identifier Codes (PIDs) for Virtual Content Security Management Appliances, page 11

Product Identifier Codes (PIDs) for Cisco Virtual Web Security Appliances

Functionality	PID	Description
Web Security Essentials	WSA-WSE-LIC=	Includes: • Web Usage Controls • Web Reputation
Web Security Premium	WSA-WSP-LIC=	Includes: • Web Usage Controls • Web Reputation • Sophos and Webroot Anti-Malware signatures
Web Security Anti-Malware	WSA-WSM-LIC=	Includes Sophos and Webroot Anti-Malware signatures
McAfee Anti-Malware	WSA-AMM-LIC=	—
Advanced Malware Protection	WSA-AMP-LIC=	—

Product Identifier Codes (PIDs) for Virtual Content Security Management Appliances

Functionality	PID	Description
All centralized web security functionality	SMA-WMGT-LIC=	—
All centralized email security functionality	SMA-EMGT-LIC=	

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:
Content Security Management appliances	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web Security appliances	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html