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, page 1
• About Amazon Machine Image, page 2
• Cisco Web Security and Security Management Virtual Appliance AMIs, page 2
• Deploying on AWS, page 3
• Managing Your Virtual Appliance, page 9
• Getting Support for Virtual Appliances, page 10
• Additional Information, page 11

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.
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.

<table>
<thead>
<tr>
<th>AsyncOS for Cisco Web Security Appliance Release</th>
<th>Virtual Appliance</th>
<th>AMI ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AsyncOS 11.5.1-115</td>
<td>S100V</td>
<td>coeus-11-5-91-001-S100V-AMI-300818</td>
</tr>
<tr>
<td></td>
<td>S300V</td>
<td>coeus-11-5-91-001-S300V-AMI-310818</td>
</tr>
<tr>
<td></td>
<td>S600V</td>
<td>coeus-11-5-91-001-S600V-AMI-310818</td>
</tr>
<tr>
<td>AsyncOS 11.5.0-614</td>
<td>S100V</td>
<td>coeus-11-5-0-614-S100V-AMI-110518</td>
</tr>
<tr>
<td></td>
<td>S300V</td>
<td>coeus-11-5-0-614-S300V-AMI-120518</td>
</tr>
<tr>
<td></td>
<td>S600V</td>
<td>coeus-11-5-0-614-S600V-AMI-120518</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Cisco Security Management Virtual Appliance (AsyncOS 11.5-1-114)</th>
<th>AMI ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>M100V</td>
<td>zeus-11-5-0-108-M100V-AMI-040518</td>
</tr>
<tr>
<td>M300V</td>
<td>zeus-11-5-0-108-M300V-AMI-050518</td>
</tr>
<tr>
<td>M600V</td>
<td>zeus-11-5-0-108-M600V-AMI-050518</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Do This</th>
<th>More Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Prepare your environment by completing prerequisite tasks and acquiring information that you will need before setting up an instance in EC2.</td>
<td>Prepare Your Environment, page 4.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the AMI from the Amazon Marketplace, and choose the appropriate instance type.</td>
<td>Select the Virtual Appliance AMI and Choose the Instance Type, page 5.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the network, subnet, IP address assignment, and other details necessary for your instance to be available and function as required.</td>
<td>Configure Instance Details, page 5.</td>
</tr>
<tr>
<td>Note</td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Retain the default storage settings or configure the tags as required.</td>
<td>Configure Storage and Add Tags, page 6.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Install the license in the appliance, and disable the web interface from responding with the appliance-specific hostname. Use the <code>hostheader</code> command, and commit the change.</td>
<td>Configure Your Launched Instance, page 7.</td>
</tr>
</tbody>
</table>
Deploying on AWS

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 Specifications

<table>
<thead>
<tr>
<th>Product</th>
<th>AsyncOS Version</th>
<th>Model</th>
<th>EC2 Instance Type</th>
<th>vCPU</th>
<th>vRAM</th>
<th>vNIC</th>
<th>Minimum Disk Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Web Security Virtual Appliance</td>
<td>AsyncOS 11.5</td>
<td>S100V</td>
<td>m4.large</td>
<td>2</td>
<td>6 GB</td>
<td>2</td>
<td>250 GB</td>
</tr>
<tr>
<td></td>
<td>and later (Web)</td>
<td>S300V</td>
<td>c4.xlarge</td>
<td>4</td>
<td>7.5 GB</td>
<td>4</td>
<td>1024 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S600V</td>
<td>c4.4xlarge</td>
<td>16</td>
<td>30 GB</td>
<td>8</td>
<td>1024 GB</td>
</tr>
<tr>
<td>Cisco Content Security Management Virtual Appliance</td>
<td>AsyncOS 11.5</td>
<td>M100V</td>
<td>m4.large</td>
<td>2</td>
<td>6 GB</td>
<td></td>
<td>250 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M300v</td>
<td>c4.xlarge</td>
<td>4</td>
<td>7.5 GB</td>
<td></td>
<td>1024 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M600v</td>
<td>c4.2xlarge</td>
<td>8</td>
<td>8 GB</td>
<td></td>
<td>2032 GB</td>
</tr>
</tbody>
</table>

**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

\[\text{Note}\] 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

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.

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Supported on Virtual WSA?</th>
<th>Supported on Virtual SMA?</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>loadlicense</td>
<td>Yes</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>etherconfig</td>
<td>Yes</td>
<td>—</td>
<td>The Pairing option is not included on virtual appliances.</td>
</tr>
<tr>
<td>version</td>
<td>Yes</td>
<td>—</td>
<td>This command will return all the information about the virtual appliance except for the UDI, RAID, and BMC information.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Functionality</th>
<th>PID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Security Essentials</td>
<td>WSA-WSE-LIC=</td>
<td>Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Web Usage Controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Web Reputation</td>
</tr>
<tr>
<td>Web Security Premium</td>
<td>WSA-WSP-LIC=</td>
<td>Includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Web Usage Controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Web Reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Sophos and Webroot Anti-Malware signatures</td>
</tr>
<tr>
<td>Web Security Anti-Malware</td>
<td>WSA-WSM-LIC=</td>
<td>Includes Sophos and Webroot Anti-Malware signatures</td>
</tr>
<tr>
<td>McAfee Anti-Malware</td>
<td>WSA-AMM-LIC=</td>
<td>—</td>
</tr>
<tr>
<td>Advanced Malware Protection</td>
<td>WSA-AMP-LIC=</td>
<td>—</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Functionality</th>
<th>PID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All centralized web security functionality</td>
<td>SMA-WMGT-LIC=</td>
<td>—</td>
</tr>
<tr>
<td>All centralized email security functionality</td>
<td>SMA-EMGT-LIC=</td>
<td>—</td>
</tr>
</tbody>
</table>

Cisco TAC

Contact information for Cisco TAC, including phone numbers:

Additional Information

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

<table>
<thead>
<tr>
<th>Documentation For Cisco Content Security Products:</th>
<th>Is Located At:</th>
</tr>
</thead>
</table>