Deploying on AWS

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

	Do This	More Info
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.
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.

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 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:

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.

Configure Instance Details

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

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

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**.

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:

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.