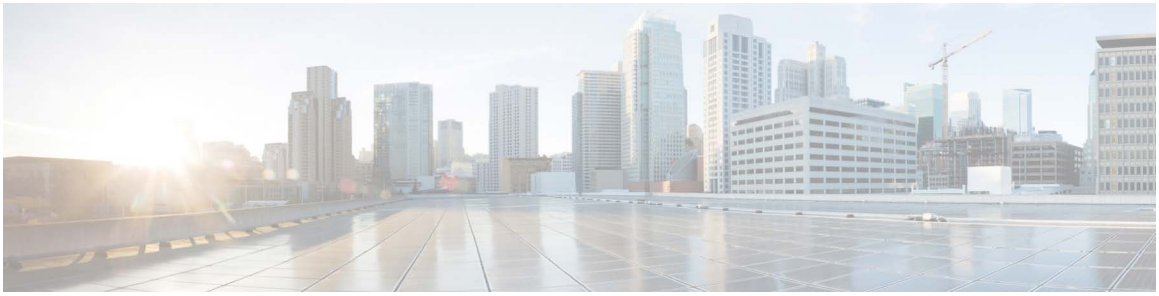

Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide

Published: July 27,2023

Contents

About Cisco Secure Virtual Appliances

Cisco Secure virtual appliances function the same as physical Cisco Secure Email Gateway or Cisco Secure Email and Web Manager hardware appliances, with only a few minor differences, which are documented in Manage Your Cisco Secure Virtual Appliance, page 19.

Cisco Systems, Inc.
www.cisco.com

Supported Virtual Appliance Models and AsyncOS Releases for Hyper-V Deployments

Product	AsyncOS Release	Model	Recommended Disk Size	Memory	Processor Cores
Cisco Secure Email Virtual Gateway	AsyncOS 15.0 and later	**C600V**	500 GB	16GB	8

Product	AsyncOS Release	Model	Recommended Disk Size	Memory	Processor Cores
Cisco Secure Email and Web Manager Virtual	AsyncOS 15.0 and later	**M600V**	2032 GB	16 GB	8

Supported Virtual Appliance Models and AsyncOS Releases for KVM Deployments

Product	AsyncOS Release	Model	Recommended Disk Size	Memory	Processor Cores
Cisco Secure Email Virtual Gateway	AsyncOS 15.0 and later	**C600V**	500 GB	16 GB	8
	AsyncOS 14.0 and later	**C100V**	200 GB	6 GB	2
		C300V	500 GB	8 GB	4
	AsyncOS 13.0 and later	**C600V**	500 GB	8 GB	8
	AsyncOS 12.0 and later				
	AsyncOS 11.0 and later				
	AsyncOS 10.0.1 and later				

Product	AsyncOS Release	Model	Disk Size	Memory	Max Memory	Processor Cores
Cisco Secure Email and Web Manager Virtual	AsyncOS 15.0 and later	**M600V**	2032 GB	16 GB	16 GB	8
	AsyncOS 14.1.0 and later	**M600V**	2032 GB	8 GB	16 GB	8

For information on increasing RAM in the virtual machine, see Increase RAM in Virtual Machine, page 21.

Virtual Appliance Models for VMWare ESXi Deployments

Note **Except as explicitly stated in the AsyncOS documentation, modifications to the ESXi configurations defined in the OVF are not supported.**

[**AsyncOS 15.0 and later**]

[Upgrade Scenario]: Cisco Content Security virtual appliance OVF images allow you to switch from the pre-configured memory values of a previous AsyncOS version to the new values on the upgrade as follows:

- C100v model: 8 GB
- C300v and C600v model: 16 GB
- M600v model: 16 GB

For information on increasing RAM in the virtual machine, see Increase RAM in Virtual Machine, page 21.

[**New Install Scenario**]: Cisco Content Security virtual appliance OVF images allows you to use the following pre-configured memory values:

- C100v model: 8 GB
- C300v and C600v model: 16 GB
- M600v model: 16 GB

Product	Model	Disk Space	Memory	Processor Cores
Cisco Secure Email Virtual Gateway	**C100V**	200 GB	8 GB	2
	C300V	500 GB	16 GB	4
	C600V	500 GB	16 GB	8

Product	Model	Disk Space	Memory	Max Memory	Processor Cores
Cisco Secure Email and Web Manager Virtual	**M100V**	250 GB	6 GB	8 GB	2
	M300V	1024 GB	8 GB	16 GB	4
	M600V	2032 GB	16 GB	16 GB	8

[**Before AsyncOS 15.0**] Cisco Content Security virtual appliance OVF images allows you to switch from the pre-configured memory values to the new maximum values as follows:

- M100v /C100v models: 6 GB to 8 GB
- M300v / M600v / C300v / C600v models: 8 GB to 16 GB

Product	Model	Disk Space	Memory	Max Memory*	Processor Cores
Cisco Secure Email Virtual Gateway	**C100V**	200 GB	6 GB	8 GB	2
	C300V	500 GB	8 GB	16 GB	4
	C600V	500 GB	8 GB	16 GB	8

Product	Model	Disk Space	Memory	Max Memory*	Processor Cores
Cisco Secure Email and Web Manager Virtual	**M100V**	250 GB	6 GB	8 GB	2
	M300V	1024 GB	8 GB	16 GB	4
	M600V	2032 GB	8 GB	16 GB	8

* The Maximum Memory column indicates the maximum memory configuration that is tested and qualified.

AsyncOS version requirements are described in Supported VMWare ESXi Hypervisors, page 6.

System Requirements

Microsoft Hyper-V Deployments

Supported Microsoft Hyper-V and host operating systems

AsyncOS Version	Hyper-V Version
AsyncOS 15.0 (Email) and later	Microsoft Hyper-V Server 2019
AsyncOS 15.0 (Management) and later	Microsoft Hyper-V Server 2019

Hardware Requirements for Microsoft Hyper-V Deployments

[**Secure Email Virtual Gateway**]

Hardware:

- Supported on Cisco UCS C Series 220/240 M5
- Cisco Secure Email Virtual performance test labs use as minimum the following: Cisco Unified Computing System™ (Cisco UCS®) C series M5 server with the Intel® Xeon® Gold 6126 CPU @ 2.60GHz processor running at 2.6GHz

Note From AsyncOS 15.0 and later, Secure Email Virtual Gateway supports Generation 2 deployments.

[**Secure Email and Web Manager Virtual**]

Hardware:

- Supported on Cisco UCS C Series 220/240 M5
- Cisco Secure Email and Web Manager Virtual performance test labs use as minimum the following: Cisco Unified Computing System™ (Cisco UCS®) C series M5 server with the Intel® Xeon® Gold 6140 CPU @ 2.30GHz

Note From AsyncOS 15.0 and later, Secure Email and Web Manager Virtual supports only Generation 2 deployments.

KVM Deployments

The following are the qualified environments for KVM deployments. All deployments use thin provisioning for disk storage.

Red Hat Enterprise Linux Server

Host OS:

- Red Hat Enterprise Linux Server 8.6 (Redhat does not support code name for the release.)

Version Information:

- Linux : 4.18.0-372.9.1.el8.x86_64
- libvirt/QEMU:

  Compiled against library: libvirt 8.0.0

  Using library: libvirt 8.0.0

  Using API: QEMU 8.0.0

  Running hypervisor: QEMU 6.2.0

Hardware:

- Supported on Cisco UCS C Series 220/240 M4 or M5
- Cisco Secure Email Virtual performance test labs use as minimum the following: Cisco Unified Computing System™ (Cisco UCS®) C series M5 server with the Intel® Xeon® Gold 6126 CPU @ 2.60GHz processor running at 2.6GHz

KVM Drivers

Supported KVM drivers:

- Network: E1000, Virtio
- Disk: VirtIO

VMWare ESXi Deployments

Supported VMWare ESXi Hypervisors

AsyncOS Version	VMWare ESXi Version
AsyncOS (Email)	
AsyncOS 15.0.x	6.7 and 7.0
AsyncOS 14.x	6.7 and 7.0
AsyncOS 13.x	6.5 and 6.7
AsyncOS 12.0	6.5 and 6.7
AsyncOS (Management)	
AsyncOS 15.0.x	6.7 and 7.0
AsyncOS 14.2.x	6.7 and 7.0
AsyncOS 14.1.x	6.7 and 7.0
AsyncOS 14.0.x	6.7
AsyncOS 13.8.x	6.7
AsyncOS 13.6.2	6.7
AsyncOS 13.5.x	6.5
AsyncOS 13.x	6.5
AsyncOS 12.x	6.5

Other VMware hypervisors are supported on a “Best Effort” basis: Cisco will try to help you, but it may not be possible to reproduce all problems, and Cisco cannot guarantee a solution.

Hardware Requirements for VMWare ESXi Deployments

Cisco UCS servers are the supported hardware platform.

Minimum requirements for the server hosting your virtual appliances:

Hypervisor Details:

VMware ESXi 6.7/7.0 (for more information, refer to Supported VMWare ESXi Hypervisors, page 6)

Hardware:

Supported on Cisco UCS C Series 220/240 M4 or M5

Note Except as explicitly stated in the documentation, Cisco does not support the alteration of the Cisco Content Security virtual appliance’s hardware configuration, such as removing IP interfaces or changing the appliance’s CPU cores or RAM size. The appliance may send alerts if such changes are made.

ESXi Drivers

Supported ESXi drivers:

Network Adapter Type: E1000

(Hosted Email Security Only) Deployment in FlexPod Solutions

For AsyncOS for Email release 8.5 and later:

For more information about deploying a Cisco Secure Email Virtual Gateway as part of a FlexPod solution, see http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/white-paper-c11-731731.pdf. Your CCO login determines whether you have access to this document.

For general information about FlexPod, see http://www.cisco.com/en/US/netsol/ns1137/index.html.

FlexPod does not apply to Cisco Secure Email and Web Manager Virtual deployments.

Prepare the Content Secure Image and Files

Determine the Best-Sized Virtual Appliance Image for Your Deployment

Determine the best-sized virtual appliance image for your needs. See the data sheet for your products, available from the following locations:

Appliance	Link to Data Sheet
Cisco Secure Email Gateway	Look for the “Cisco Secure Email Gateway Appliance Data Sheet” link on this page: https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet-c78-742868.html In the data sheet, look for the table titled “Cisco Secure Email Virtual Gateway Specifications.”
Cisco Secure Email and Web Manager	Look for the "Cisco Secure Email and Web Manager Appliance Data Sheet" link on this page: https://www.cisco.com/c/dam/en/us/products/se/2019/4/Collateral/security-management-app-ds.pdf In the data sheet, look for the table titled "Cisco Secure Email and Web Manager Virtual."

Download the Cisco Content Security Virtual Appliance Image

Before You Begin

- Obtain a license from Cisco for your virtual appliance.
- See Determine the Best-Sized Virtual Appliance Image for Your Deployment, page 8.

Step 1 Go to the Cisco Download Software page for your virtual appliance:

- For Cisco Secure Email Virtual Gateway:

  https://software.cisco.com/download/home/284900944/type/282975113/release
- For Cisco Secure Email and Web Manager Virtual:

  https://software.cisco.com/download/home/286283259/type/286283388/release

Step 2 In the left navigation pane, select an AsyncOS version.

Step 3 Click **Download** for the virtual appliance model image you want to download.

Step 4 Save the image to your local machine.

Related Topics

- Deploy on Microsoft Hyper-V, page 9
- Deploy on KVM, page 10
- Deploy on VMWare ESXi, page 13

Deploy on Microsoft Hyper-V

	Action	More Information
1.	Review the Release Notes for your AsyncOS release.	Release Notes are available from the locations in Additional Information, page 25.
2.	Download the virtual appliance image and MD5 hash from Cisco.	You will need the MD5 hash to check the data integrity of the appliance image. Prepare the Content Secure Image and Files, page 8.
3.	Deploy the virtual appliance on Hyper-V.	a. Set up the Windows Server Operating System. Ensure that you have installed the required Hyper-V roles. See System Requirements, page 4 for more information. b. Download the image as described in Prepare the Content Secure Image and Files, page 8. c. Using the Hyper-V Manager, install the virtual appliance image using the New Virtual Machine Wizard. d. Complete the wizard. e. Edit the processor settings in the Hyper-V Manager. See Determine the Best-Sized Virtual Appliance Image for Your Deployment, page 8 to check for the number of processors and NICs required.
4.	If DHCP is disabled, set up the appliance on your network.	If DHCP Is Disabled, Set Up the Appliance on the Network (Microsoft Hyper-V), page 10
5.	Install the license file	Install the Virtual Appliance License File, page 17.
6.	Log in to the web UI of your appliance and configure the appliance software as you would do for a physical appliance. For example, you can: • Run the System Setup Wizard. • 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 25. • 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.

Note From AsyncOS 15.0 and later, Secure Email Gateway supports Generation 2 deployments.

From AsyncOS 15.0 and later, Secure Email and Web Manager supports only Generation 2 deployments.

Currently, there is no support for “Secure Boot” and “Trusted Platform Module (TPM)” technologies in Generation 2 deployment.

If DHCP Is Disabled, Set Up the Appliance on the Network (Microsoft Hyper-V)

Note If you cloned the virtual security appliance image, perform the following steps for each image.

Step 1 From the Hyper-V manager console, run `interfaceconfig`.

Step 2 Write down the IP address of the virtual appliance's Management port.

Note The Management port obtains its IP address from your DHCP server. If the appliance cannot reach a DHCP server, it will use `192.168.42.42` by default.

Note Configure the default gateway using the `setgateway` command.

Step 3 Commit the changes.

Note The hostname does not update until after you have completed the setup wizard.

Deploy on KVM

	Action	More Information
1.	Ensure that your equipment and software meet all system requirements.	See System Requirements, page 4 and the documentation for the products and tools that you will use.
2.	Review the Release Notes for your AsyncOS release.	Release Notes are available from the locations in Additional Information, page 25.
3.	Set up the UCS server, host OS, and KVM.	See the documentation for the products and tools you will use.
4.	Download the virtual content security appliance image.	See Download the Cisco Content Security Virtual Appliance Image, page 8.
5.	Ensure that the Cisco image is compatible with your deployment.	See Ensure Virtual Appliance Image Compatibility With Your KVM Deployment, page 11
6.	Determine the amount of RAM and the number of CPU cores to allocate to your virtual appliance model.	See, page 2.
7.	Deploy the virtual content security appliance image.	Use one of the following methods: • Deploy the Virtual Appliance Using Virtual Machine Manager, page 11 • Deploy the Virtual Appliance Using virt-install: Example, page 12

	Action	More Information
8.	Install the virtual appliance license file. Install feature licenses and configure your Cisco content security virtual appliance.	To install feature licenses and configure the appliance, see the User Guide or online help for your AsyncOS release.
9.	Configure the appliance to send alerts when the license is about to expire.	See the online help or user guide for your AsyncOS release.

Ensure Virtual Appliance Image Compatibility With Your KVM Deployment

The qcow version of our image is not compatible with QEMU versions lower than 1.1. If your QEMU version is lower than 1.1, you must convert the image to make it compatible with your deployment.

Deploy the Virtual Appliance Using Virtual Machine Manager

Step 1 Launch the virt-manager application.

Step 2 Select **New**.

Step 3 Enter a unique name for your virtual appliance.

Step 4 Select **Import existing image**.

Step 5 Select **Forward**.

Step 6 Enter options:

- OS Type: **UNIX**.
- Version: **FreeBSD 13**

Step 7 Browse and select the virtual appliance image that you downloaded.

Step 8 Select **Forward**.

Step 9 Enter RAM and CPU values for the virtual appliance model that you want to deploy.

See , page 2.

Step 10 Select **Forward**.

Step 11 Select the **Customize** check box.

Step 12 Select **Finish**.

Step 13 Configure the disk drive:

a. In the left pane, select the drive.

b. Under Advanced options, select options:

- Disk bus:**Virtio**.
- Storage format: qcow2

c. Select **Apply.**

Step 14 Configure the network device for the management interface:

a. In the left pane, select a NIC.

b. Select options:

- Source Device: Your management vlan
- Device model: virtIO
- Source mode: VEPA.

c. Select **Apply.**

Step 15 Configure network devices for four additional interfaces:

Repeat the previous set of substeps for each interface you will use.

Step 16 Select **Begin Installation**.

Related Topics

- Deploy on KVM, page 10

Deploy the Virtual Appliance Using virt-install: Example

Before You Begin

Determine the amount of RAM and number of CPU cores needed for your appliance. See, page 2.

Procedure

Step 1 Create the storage pool where your virtual appliance will reside.

```
virsh pool-define-as --name vm-pool --type dir --target /home/username/vm-pool
virsh pool-start vm-pool
```

Step 2 Copy the virtual appliance image to your storage pool.

```
cd /home/yusername/vm-pool
tar xvf ~/asyncos-15-0-0-068-C600V.qcow2.tar.gz
```

Step 3 Install the virtual appliance.

```
virt-install \
--virt-type kvm \
--os-type=unix \
--os-variant=freebsd13 \
--name test-dut \ (This name should be unique)
--ram 16384 \ (Use the value appropriate to your virtual appliance model)
--vcpus 8 \ (Use the value appropriate to your virtual appliance model)
--noreboot \
--import \
--disk
path=/home/username/vm-pool/asyncos-15-0-0-068-C600V.qcow2,format=qcow2,bus=virtio \
--network type=direct,source=enp6s0.483,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.484,source_mode=vepa,model=virtio \
```

```
--network type=direct,source=enp6s0.485,source_mode=vepa,model=virtio \
```

Step 4 Restart the virtual appliance.

```
virsh start test-dut
virsh --connect qemu:///system start test-dut
```

Step 5 To Start or Stop the virtual appliance:

```
--virsh shutdown test-dut
--virsh start test-dut
```

Related Topics

- Deploy on KVM, page 10

Deploy on VMWare ESXi

	Action	More Information
1.	Review the Release Notes for your AsyncOS release.	Release Notes are available from the locations in Additional Information, page 25.
2.	Download the virtual appliance image and MD5 hash from Cisco.	You will need the MD5 hash to check the data integrity of the appliance image. Prepare the Content Secure Image and Files, page 8.
3.	Deploy the virtual appliance on your ESXi host or cluster.	Deploy the Virtual Appliance, page 14.
4.	Prevent intermittent connectivity issues.	Disable unused network interface cards (NICs) on the virtual machine.
5.	Configure synchronization on the virtual machine to avoid random failures on your Cisco Content Security virtual appliance.	Important! Prevent Random Failures, page 15
6.	If DHCP is disabled, set up the appliance on your network.	If DHCP Is Disabled, Set Up the Appliance on the Network (VMware vSphere), page 16
7.	Install the license file.	Install the Virtual Appliance License File, page 17.

	Action	More Information
8.	Log in to the web UI of your appliance and configure the appliance software as you would do for a physical appliance. For example, you can: • Run the System Setup Wizard • 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 25. • 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.
9.	Configure the appliance to send alerts when 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 25.

(Optional) Clone the Virtual Appliance

If you will run multiple virtual security appliances in your environment:

- Cisco recommends that you clone the virtual security appliance before you run it the first time.
- Cloning a virtual security appliance after the license for the virtual appliance has been installed forcefully expires the license. You will have to install the license again.
- You must shut down the virtual appliance before cloning it.
- If you want to clone a virtual appliance that is already in use, see Clone a Virtual Appliance Already in Use, page 18 for more information.

For instructions on cloning a virtual machine, see VMWare's technical documentation at http://www.vmware.com/support/ws55/doc/ws_clone.html.

Related Topics

- Deploy on Microsoft Hyper-V, page 9
- Deploy on KVM, page 10
- Deploy on VMWare ESXi, page 13

Deploy the Virtual Appliance

Before You Begin

- Set up the ESXi host or cluster on which you will deploy the virtual appliance. See System Requirements, page 4 for more information.
- Install the VMware vSphere Client on your local machine.
- Download the image as described in Prepare the Content Secure Image and Files, page 8.

Step 1 Unzip the .zip file for the virtual appliance in its own directory; for example, `C:\vESA\C100V`.

Step 2 Open the VMware vSphere Client on your local machine.

Step 3 Select the ESXi host or cluster to which you want to deploy the virtual appliance.

Step 4 Choose **File > Deploy OVF template**.

Step 5 Enter the path to the OVF file in the directory you created.

Step 6 Click **Next**.

Step 7 Complete the wizard.

Thin provisioning for disk storage is supported at the hypervisor layer. Disk space and performance may be reduced if you select this option.

Note **Except as explicitly stated in the AsyncOS documentation, modifications to the ESXi configurations defined in the OVF are not supported.**

Note Do not take backup (snapshot) of the virtual appliance using VMware or any other third-party tools, or restore a virtual appliance from a snapshot. Alternatively, you can take backup of the configuration using the **System Administration > Configuration File** menu in the user interface or using the `saveconfig` CLI command. You can then load it on another spawned virtual appliance.

Related Topics

- Deploy on Microsoft Hyper-V, page 9
- Deploy on KVM, page 10
- Deploy on VMWare ESXi, page 13

Important! Prevent Random Failures

Caution It is important that you do not shutdown or restart the virtual appliances using vSphere client or web client unless advised to do so by Cisco Technical Support. Cisco recommends that you use the shutdown or reboot command from the CLI, or the Shutdown/Reboot option that is listed in the system administration tab of the appliance GUI. If you power cycle the appliance (or experience power outage to the virtual infrastructure), it may lead to loss of messages, database corruption, or loss of logging data. The failure to unmount the file system cleanly damages the file system, resulting the system in a broken state.

Virtual machines have inherent timing quirks that you must address in order to avoid random failures on your Cisco Content Security virtual appliance. To prevent these issues, enable exact time stamp counter synchronization on your virtual machine.

Before You Begin

- For more information on timekeeping basics, virtual time stamp counters, and exact synchronization, see VMWare's Timekeeping in Virtual Machines PDF at http://www.vmware.com/files/pdf/techpaper/Timekeeping-In-VirtualMachines.pdf.
- Instructions for your version of the vSphere client may vary from the procedure below. Use this as a general guide and see the documentation for your client as needed.

Step 1 Select a virtual appliance from the list of machines in the vSphere Client.

Step 2 Log in to the CLI, and type the command `shutdown` to power off the virtual appliance.

Step 3 Right-click the appliance and select **Edit Settings**.

Step 4 Click the **Options** tab and select **Advanced > General**.

Step 5 Click **Configuration Parameters**.

Step 6 Edit or add the following parameters:

```
monitor_control.disable_tsc_offsetting=TRUE
monitor_control.disable_rdtscopt_bt=TRUE
timeTracker.forceMonotonicTTAT=TRUE
```

Step 7 Close the settings window and run appliance.

Related Topics

- Deploy on Microsoft Hyper-V, page 9
- Deploy on KVM, page 10
- Deploy on VMWare ESXi, page 13

If DHCP Is Disabled, Set Up the Appliance on the Network (VMware vSphere)

Note If you cloned the virtual security appliance image, perform the following steps for each image.

Step 1 From the vSphere client console, run `interfaceconfig`.

Step 2 Write down the IP address of the virtual appliance's Management port.

Note The Management port obtains its IP address from your DHCP server. If the appliance cannot reach a DHCP server, it will use `192.168.42.42` by default.

Step 3 Configure the default gateway using the `setgateway` command.

Step 4 Commit the changes.

Note The hostname does not update until you have completed the setup wizard.

Related Topics

- Deploy on Microsoft Hyper-V, page 9
- Deploy on KVM, page 10
- Deploy on VMWare ESXi, page 13

Microsoft Azure Deployments

For information on Microsoft Azure deployments, see the Deploying Cisco Secure Email Virtual Gateway and Cisco Secure Email and Web Manager Virtual on Microsoft Azure Cloud Platform Guide.

Amazon Web Services (AWS) EC2 Deployments

For information on Amazon Web Services (AWS) EC2 deployments, see the Deploying Cisco Secure Email Gateway and Secure Email and Web Manager Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services guide.

Install the Virtual Appliance License File

Note If you cloned the virtual security appliance image, perform the following steps for each image.

Before You Begin

(Optional) FTP into the virtual appliance to upload the license file. If you will paste the license into the terminal, you do not need to do this.

Procedure

Step 1 Log in to the appliance's CLI as the admin or ironport user using SSH or telnet in a terminal application.

Note You cannot paste the contents of the license file into the CLI using the vSphere client console.

Step 2 Run the `loadlicense` command.

Step 3 Install the license file using one of the following options:

- Select option 1 and paste the contents of the license file into the terminal.
- Select option 2 and load the license file in the `configuration` directory, if you have already uploaded the license file to the appliance's `configuration` directory using FTP.

Step 4 Read and agree to the license agreement.

Step 5 (Optional) Run `showlicense` to review the license details.

What to Do Next

For Microsoft Hyper-V deployments:

- Return to Deploy on Microsoft Hyper-V, page 9.

For KVM deployments:

- Return to Deploy on KVM, page 10.

For ESXi deployments:

- For more information on the Management interface's IP address, see Deploy on VMWare ESXi, page 13.
- If you cloned the virtual security appliance image, repeat the procedure in this topic for each image.
- See remaining setup steps in Deploy on VMWare ESXi, page 13.

Migrate Your Virtual Appliance to Another Physical Host

You can use VMware® VMotion™ to migrate a running virtual appliance to a different physical host.

Requirements:

- Both physical hosts must have the same network configuration.
- Both physical hosts must have access to the same defined network(s) to which the interfaces on the virtual appliance are mapped.
- Both physical hosts must have access to the datastore that the virtual appliance uses. This datastore can be a storage area network (SAN) or Network-attached storage (NAS).
- The Cisco Secure Email Virtual Gateway must have no mail in its queue.

Note Migrate the virtual machine using the VMotion documentation.

Clone a Virtual Appliance Already in Use

Before You Begin

- For instructions on cloning a virtual machine, see VMWare's technical documentation at http://www.vmware.com/support/ws55/doc/ws_clone.html.
- For information on how to manage the network settings and security features of your appliance, see the user guide for your Cisco Secure product and release.

Step 1 If you are cloning a Cisco Secure Email Virtual Gateway:
Suspend the appliance using the `suspend` command in the CLI and enter a delay period long enough for the appliance to deliver all messages in the queue.

Step 2 If you are cloning a Cisco Secure Email and Web Manager:
Disable centralized services on your managed Secure Email Gateway.

Step 3 Shut down the virtual appliance using the `shutdown` command in the CLI.

Step 4 Clone the virtual appliance image.

Step 5 Start the cloned appliance using the VMware vSphere Client and perform the following:

a. If you cloned a configured image rather than the unmodified OVF image file downloaded from Cisco.com:

- Install the license file on the cloned virtual appliance.
- Modify the network settings of the cloned virtual appliance.

Network adapters do not automatically connect when powered on. Reconfigure IP address, Hostname, and Gateway IP address, then power on the network adapters.

Configurations will not be complete until you install feature keys.

b. For cloned Cisco Secure Email Virtual Gateway appliances:
   - Delete all messages in the quarantines.
   - Delete the message tracking and reporting data.

Step 6 Start the original virtual appliance using the VMware vSphere Client and resume operation. Make sure that it is running properly.

Step 7 Resume operation on the cloned appliance.

Manage Your Cisco Secure Virtual Appliance

IP Address

When the virtual appliance is first powered on, the Management port gets an IP address from your DHCP host. If the virtual appliance is unable to obtain an IP address from a DHCP server, it will use `192.168.42.42` as the Management interface's IP address. The CLI displays the Management interface's IP address when you run the System Setup Wizard on the virtual appliance.

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 Secure virtual appliance requires an additional license to run the virtual appliance on a host. You can use this license for multiple, cloned virtual appliances. Licenses are hypervisor-independent.

For AsyncOS for Secure Email Gateway 8.5.x and later, and AsyncOS for Secure Email and Web Manager 8.4 and later:

- Feature keys for individual features can have different expiration dates.
- After the virtual appliance license expires, the appliance will continue to deliver mail (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, administrators and end users cannot manage quarantines, but the management appliance continues to accept quarantined messages from managed Cisco Secure Email Gateway Appliances, and scheduled deletion of quarantined messages will occur.
- As feature keys are included in the virtual appliance license, there are no evaluation licenses for AsyncOS features.

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

Related Topics

- Install the Virtual Appliance License File, page 17

Force Reset, Power Off, and Reset Options

The following actions are the equivalent of pulling the plug on a hardware appliance and are not supported, especially during AsyncOS startup:

- In KVM, the Force Reset option.
- In VMWare, the Power Off and Reset options.

CLI Commands on the Virtual Appliance

The Cisco Secure virtual appliances include updates to existing CLI commands and includes a virtual appliance-only command, `loadlicense`. The following CLI command changes have been made:

Command	Supported on Virtual SMA?	Information
`loadlicense`	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`	—	The Pairing option is not included on virtual appliances.
`version`	—	This command will return all the information about the virtual appliance except for the UDI, RAID, and BMC information.
`resetconfig`	—	Running this command leaves the virtual appliance license and the feature keys on the appliance.
`revert`	—	Beginning with AsyncOS 8.5 for Email Security: Behavior is described in the System Administration chapter in the online help and user guide for your appliance.

`diagnostic`	Yes	The following `diagnostic` > `raid` submenu options will not return information:
		`1. Run disk verify`
		`2. Monitor tasks in progress`
		`3. Display disk verify verdict`
		`4. Check disk firmware`

`showlicense`	Yes	View license details. For Secure Email Virtual Gateway, 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`

Increase RAM in Virtual Machine

Before you upgrade to Secure Email Virtual Gateway or Secure Email and Web Manager Virtual 15.0 and later, you must upgrade RAM.

Perform the following steps to upgrade RAM:

1. Shut down Secure Email Gateway or Secure Email and Web Manager using the steps mentioned in the user guide.
2. Increase the memory of the virtual machine.
3. Turn on the virtual machine and check if Secure Email Gateway or Secure Email and Web Manager is accessible.

Troubleshoot and Support

Troubleshoot: KVM Deployments

Virtual Appliance Hangs on Reboot

Problem The virtual appliance hangs when rebooting.

Solution This is a KVM issue. Perform the following workaround each time you reboot the host:

Step 1 Check the following:

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

Step 2 If the above value is set to Y:

a. Stop your virtual appliances and reinstall the KVM kernel module:

```
rmmod kvm_intel
modprobe kvm_intel enable_apicv=N
```

b. Restart your virtual appliance.

For more information, see https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html and https://bugs.launchpad.net/qemu/+bug/1329956.

Network Connectivity Works Initially, then Fails

Problem Network connectivity is lost, which was previously connected.

Solution This is a KVM issue. See the section on "KVM: Network connectivity works initially, then fails" in the openstack documentation at http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html.

Slow Performance, Watchdog Issues, and High CPU Usage

Problem Appliance performance is slow, watchdog issues occur, and the appliance shows unusually high CPU usage when running Virtual Appliances using KVM on Red Hat™ Enterprise Linux.

Solution Install the latest Host OS updates from Red Hat™ Enterprise Linux.

Troubleshoot: VMWare ESXi Deployments

Intermittent Connectivity Issues

Problem Intermittent connectivity issues.

Solution Ensure that all unused NICs are disabled in ESXi.

Random Failures

Problem Random failures occur that have no obvious cause.

Solution See Important! Prevent Random Failures, page 15

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 Secure 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 23
- Product Identifier Codes (PIDs) for Cisco Secure Email and Web Manager Virtual, page 24

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

Cisco Secure Email Unified SKU overview

Orders for Cisco Secure Email Unified SKU involve four SKU types:

- The subscription SKU, which is used to define the subscription term and start date.
- The product SKUs, which are used to define the products and quantities that make up the subscription.
- The product add-on SKUs, which can only be added on to other product SKUs.
- The support SKUs, which define the level of support for the subscription.

Orders commence with the selection of the Email Security subscription SKU. This is followed by the configuration of the subscription by selecting the product, add-on, and support SKUs that will constitute the subscription.

Subscription SKU

There is only one subscription SKU for Email Security-CSEMAIL-SEC-SUB. The term and payment option of the subscription applies to all products included in the subscription.

Functionality	PID	Description
Cisco Secure Email Gateway Essentials	ESA-ESS-LIC	Includes: • Anti-Spam • Anti-Virus • Outbreak Filters • Cisco Secure Malware Defense(AMP) Limited Samples
Cisco Secure Email Gateway Advantage	ESA-ADV-LIC	Includes: • Anti-Spam • Anti-Virus • Outbreak Filters • Cisco Secure Malware Defense(AMP) Un-limited Samples • Gray Mail Safe unsubscribe • Data loss prevention • Encryption

Functionality	PID	Description
Cisco Secure Email Gateway Premier	ESA-PRE-LIC	Includes: • Anti-Spam • Anti-Virus • Outbreak Filters • Cisco Secure Malware Defense(AMP) Un-limited Samples • Gray Mail Safe unsubscribe • Data loss prevention • Encryption • Cisco Secure Awareness Training
Cisco Secure Email and Web Manager Appliance (SMA)	SMA-EMGT-LIC	All Centralized Email Security Functionality
Image Analyzer	ESA-IA-LIC	Available as Add-on
Intelligent Multi-Scan	ESA-IMS-LIC	Available as Add-on
McAfee Anti-Malware	ESA-MFE-LIC	Available as Add-on
Graymail Safe-Unsubscribe	ESA-GSU-LIC	Available as Add-on (Part of Advantage and Premier Bundles)
Data loss prevention	ESA-DLP-LIC	Available as Add-on (Part of Advantage and Premier Bundles)
Encryption	ESA-ENC-LIC	Available as Add-on (Part of Advantage and Premier Bundles)

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 Secure Products	Location
Cisco Secure Email and Web Manager	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Email Gateway	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Related Topics

- Deploy on Microsoft Hyper-V, page 9
- Deploy on KVM, page 10
- Deploy on VMWare ESXi, page 13