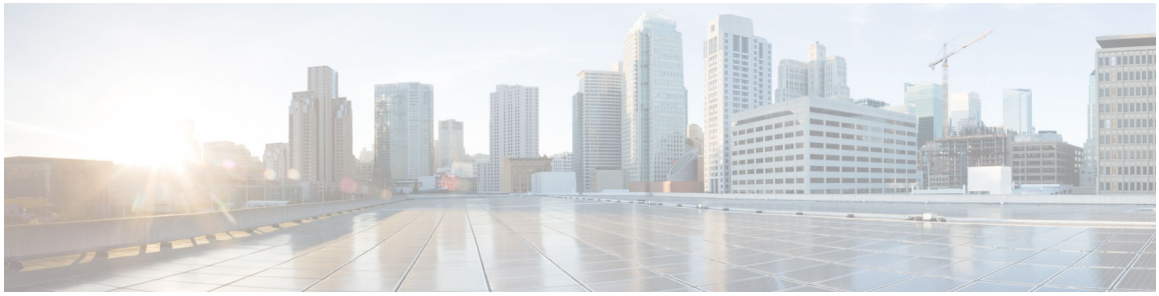

Cisco Content Security Virtual Appliance Installation Guide

Last Updated: April 24, 2019

Contents

About Cisco Content Security Virtual Appliances

Cisco content security virtual appliances function the same as physical email security, web security, or content security management hardware appliances, with only a few minor differences, which are documented in Managing Your Cisco Content Security Virtual Appliance, page 22.

Cisco Systems, Inc.
www.cisco.com

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

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
Cisco Web Security Virtual Appliance	AsyncOS 11.7 and later	**S000V**	250 GB	200 GB	4 GB	1
		S100V	250 GB	200 GB 250 GB	6 GB	2
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 11.0 and later	**S000V**	250 GB	-	4 GB	1
		S100V	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4
		S600V	1024 GB	-	24 GB	12

Supported Virtual Appliance Models and AsyncOS Releases for KVM Deployments

Product	AsyncOS Release	Model	Recommended Disk Size	RAM	Processor Cores
Cisco Email Security Virtual Appliance	AsyncOS 12.0 and later AsyncOS 11.0 and later AsyncOS 10.0.1 and later	**C000V**	200 GB	4 GB	1
		C100V	200 GB	6 GB	2
		C300V	500 GB	8 GB	4
		C600V	500 GB	8 GB	8

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
Cisco Web Security Virtual Appliance	AsyncOS 11.7 and later	**S000V**	250 GB	200 GB	4 GB	1
		S100V	250 GB	200 GB 250 GB	6 GB	2
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 10.1 and later	**S600V**	1024 GB	-	24 GB	12
	AsyncOS 8.6 and later	**S000V**	250 GB	-	4 GB	1
		S100V	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4

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.**

Cisco Content Security virtual appliance OVF images have been pre-configured with the values in the following table.

Product	Model	Disk Space	Memory	Processor Cores
Cisco Email Security Virtual Appliance	**C000V** (For evaluation and demonstration only)	200 GB	4 GB	1
	C100V	200 GB	6 GB	2
	C300V	500 GB	8 GB	4
	C600V	500 GB	8 GB	8

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
Cisco Web Security Virtual Appliance	AsyncOS 11.7 and later	**S000V**	250 GB	200 GB	4 GB	1
		S100V	250 GB	200 GB 250 GB	6 GB	2
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 10.1 and later	**S600V**	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 8.6 and later	**S000V**	250 GB	-	4 GB	1
		S100V	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4

AsyncOS version requirements are described in Supported VMWare ESXi Hypervisors, page 7.

Product	Model	Disk Space	Memory	Processor Cores
Cisco Content Security Management Virtual Appliance	**M000V**	250 GB	4 GB	1
	M100V	250 GB	6 GB	2
	M300V	1024 GB	8 GB	4
	M600V	2032 GB	8 GB	8

System Requirements

Microsoft Hyper-V Deployments

Supported Microsoft Hyper-V and host operating systems

AsyncOS Version	Hyper-V
AsyncOS 11.0 (Web) and later	Hyper-V version 5.0

Hardware Requirements for Microsoft Hyper-V Deployments

Cisco UCS servers blade M3, M4 servers and later are the only supported hardware platforms.

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 7.0

  (Red Hat Enterprise Virtualization and Red Hat OpenStack platform are NOT supported.)

Version Info:

- Linux: 3.10.0-123.13.2.el7.x86_64
- libvirt/QEMU:

  Compiled against library: libvirt 1.1.1

  Using library: libvirt 1.1.1

  Using API: QEMU 1.1.1

  Running hypervisor: QEMU 1.5.3

Hardware:

- Qualified on: UCS B200 M3
- Redhat 7.0 certified UCS Platforms: https://access.redhat.com/search/browse/certified-hardware/#?&col=portal_certified_hardware&language=All&portal_certification_version=Red+Hat+Enterprise+Linux+7&portal_vendor=Cisco

Ubuntu Server

Host OS:

- Ubuntu Server 14.04.1 LTS (latest update)

Version Info:

- Linux: 3.13.0-43-generic
- Virsh/QEMU

  Compiled against library: libvirt 1.2.2

  Using library: libvirt 1.2.2

  Using API: QEMU 1.2.2

  Running hypervisor: QEMU 2.0.0

Hardware:

- Qualified on: UCS B200 M3
- Ubuntu 14.04 Certified UCS Platform: http://www.ubuntu.com/certification/server/make/Cisco%20UCS/?query=&level=Certified&release=14.04+LTS

KVM Drivers

Supported KVM drivers:

- CDROM: IDE CDROM
- Network: E1000, Virtio
- Disk: VirtIO

KVM Packages

Required/related KVM packages to be installed on the host:

- qemu-kvm
- qemu-img
- libvirt
- libvirt-python
- libvirt-client
- virt-manager (requires X-windows)
- virt-install

VMWare ESXi Deployments

Supported VMWare ESXi Hypervisors

AsyncOS Version	VMWare ESXi Version
AsyncOS 12.0 (Email) AsyncOS 12.x (Management) AsyncOS 11.7 (Web)	6.0 and 6.5
AsyncOS 11.5.1 (Web)	6.0 and 6.5
AsyncOS 11.5.1 (Management)	6.0
AsyncOS 11.1 (Email)	6.0 and 6.5
AsyncOS 11.0 (Email) AsyncOS 11.x (Management) AsyncOS 10.1 and later (Web)	6.0
AsyncOS 11.0 (Email) AsyncOS 11.x (Management) AsyncOS 9.x and later (Web)	6.0
AsyncOS 10.x (Email) AsyncOS 10.x (Management) AsyncOS 10.1 and later (Web)	6.0
AsyncOS 10.x (Email) AsyncOS 10.x (Management) AsyncOS 9.x and later (Web)	6.0
AsyncOS 9.x (Email) AsyncOS 9.x (Management) AsyncOS 8.7 and later (Web)	6.0

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 (blade or rack-mounted) are the only supported hardware platform.

Minimum requirements for the server hosting your virtual appliances:

- Two 64-bit x86 processors of at least 1.5 GHz each
- 8 GB of physical RAM
- A 10k RPM SAS hard drive disk

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

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.

(Hosted Email Security Only) Deployment in FlexPod Solutions

For AsyncOS for Email release 8.5 and later:

For more information about deploying a virtual Email Security appliance 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 virtual Web Security appliance or virtual Content Security Management appliance deployments.

(For Deployments On VMware ESXi 4.x Only) Create a New Datastore

VMware ESXi version 4.x comes with a file system that has a default block-size of 4 MB, which supports a virtual disk image of up to 1 TB. However, the larger Cisco virtual security appliances (e.g., S300V, C600V) require more than 1 TB of disk space. In order to run these models, you will need to create a new datastore and format it with an 8 MB or larger block size.

For information on block size and instructions on how to create a new datastore, see VMware's technical documentation at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003565.

Prepare the Content Security 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
ESA	Look for the “Cisco Email Security Appliance Data Sheet” link on this page: http://www.cisco.com/c/en/us/products/security/email-security-appliance/datasheet-listing.html. In the data sheet, look for the table titled “Email Security Virtual Appliance Specifications.”
WSA	Look for the "Cisco Web Security Appliance Data Sheet" link on this page: http://www.cisco.com/c/en/us/products/security/web-security-appliance/datasheet-listing.html. In the data sheet, look for the table titled "Cisco WSAV."
SMA	Look for the "Cisco Content Security Management Appliance Data Sheet" link on this page: http://www.cisco.com/c/en/us/products/security/content-security-management-appliance/datasheet-listing.html. In the data sheet, look for the table titled "Cisco SMAV."

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 email security: https://software.cisco.com/download/release.html?mdfid=284900944&flowid=41782&softwareid=282975113&release=9.1.0&relind=AVAILABLE&rellifecycle=ED&reltype=latest
- For web security: https://software.cisco.com/download/release.html?mdfid=284806698&flowid=41610&softwareid=282975114&release=10.1.0&relind=AVAILABLE&rellifecycle=&reltype=latest
- For content security management:

  https://software.cisco.com/download/release.html?mdfid=286283259&flowid=72402&softwareid=286283388&release=9.0&relind=AVAILABLE&rellifecycle=GD&reltype=latest

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 10
- Deploy on KVM, page 12
- Deploy on VMWare ESXi, page 16

Prepare the License and Configuration Files to Load at Startup (KVM Deployments)

This feature was introduced in AsyncOS 8.6 for Cisco Web Security Appliances. It is not available for other content security appliances or in other AsyncOS releases.

You can automatically load the Cisco Content Security Virtual Appliance license and configuration files the first time the Cisco appliance starts. (These files will not load after the first startup.)

Step 1 Obtain and name your license and/or configuration files:

- Configuration file: `config.xml`
- License file: `license.xml`

Step 2 Create an ISO image that contains one or both of these files.

What To Do Next

When you deploy the AsyncOS.QCOW image, you will attach the ISO as a virtual CD-ROM drive to the virtual machine instance.

After startup, you can check the status log on your Cisco virtual appliance. Error messages related to this functionality include the keyword **zero**. You must log into the appliance, and use the `tail` command from the CLI. For more information, see the "Web Security Appliance CLI Commands" topic in the "Command Line Interface" chapter in the user guide.

Related Topics

- Deploy on KVM, page 12

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 27.
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 Security Image and Files, page 8.

	Action	More Information
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 Security 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 12
5.	Install the license file	Install the Virtual Appliance License File, page 19.
6.	Log into 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 27. • 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.

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.

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

Step 4 Commit the changes.

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

Deploy on KVM

	Action	More Information
Step 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.
Step 2	Review the Release Notes for your AsyncOS release.	Release Notes are available from the locations in Additional Information, page 27.
Step 3	Set up the UCS server, host OS, and KVM.	See the documentation for the products and tools you will use.
Step 4	Download the virtual content security appliance image.	See Download the Cisco Content Security Virtual Appliance Image, page 9.
Step 5	Ensure that the Cisco image is compatible with your deployment.	See Ensure Virtual Appliance Image Compatibility With Your KVM Deployment, page 13
Step 6	(Optional) Prepare an ISO file that includes the license and configuration files to automatically load at startup.	See Prepare the License and Configuration Files to Load at Startup (KVM Deployments), page 10.
Step 7	Determine the amount of RAM and the number of CPU cores to allocate to your virtual appliance model.	See Supported Virtual Appliance Models and AsyncOS Releases for KVM Deployments, page 2.

	Action	More Information
Step 8	Deploy the virtual content security appliance image.	Use one of the following methods: • Deploy the Virtual Appliance Using Virtual Machine Manager, page 13 • Deploy the Virtual Appliance Using virt-install: Example, page 14
Step 9	If you will deploy the High Availability feature introduced in AsyncOS 8.5 for Cisco Web Security Appliances, configure the host to support this feature.	See (Optional) Configure the Virtual Interface to Support High Availability, page 15.
Step 10	If you did not configure the system to load license and configuration files at first startup: • Install the virtual appliance license file • Install feature licenses • Configure your Cisco content security virtual appliance.	• To install the virtual appliance license file, see Amazon Web Services (AWS) EC2 Deployments, page 19 • To install feature licenses and configure the appliance, see the User Guide or online help for your AsyncOS release.
Step 11	Configure the appliance to send alerts when license expiration nears.	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 8.X**

Step 7 Browse to 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 you are deploying.

See Supported Virtual Appliance Models and AsyncOS Releases for KVM Deployments, 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 (WSA only):

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

Step 16 If you prepared an ISO image with the license and configuration files to be loaded at startup:

Attach the ISO as a virtual CD-ROM drive to the Virtual Machine instance.

Step 17 Select **Begin Installation**.

Related Topics

- Deploy on KVM, page 12

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 Supported Virtual Appliance Models and AsyncOS Releases for KVM Deployments, 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-8-6-0-007-S100V.qcow2.tar.gz
```

Step 3 Install the virtual appliance:

```
virt-install \
--virt-type kvm \
--os-type=unix \
--os-variant=freebsd8 \
--name wsa-example \ (This name should be unique)
--ram 6144 \ (Use the value appropriate to your virtual appliance model)
--vcpus 2 \ (Use the value appropriate to your virtual appliance model)
--noreboot \
--import \
--disk
path=/home/username/vm-pool/asyncos-8-6-0-007-S100V.qcow2,format=qcow2,bus=virtio \
--disk path=/home/username/vm-pool/wsa.iso,bus=ide,device=cdrom \ (If you created an ISO with the license and configuration file to load at startup)
--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 \
--network type=direct,source=enp6s0.486,source_mode=vepa,model=virtio \
--network type=direct,source=enp6s0.487,source_mode=vepa,model=virtio
```

Step 4 Start the virtual appliance:

```
virsh start wsa-example
```

Related Topics

- Deploy on KVM, page 12

(Optional) Configure the Virtual Interface to Support High Availability

The high availability feature was introduced in AsyncOS 8.5 for Cisco Web Security Appliances and is described in detail in the user guide and online help.

If your Web Security appliance will be added to a failover group for high availability, configure the virtual interface to use promiscuous mode, in order to enable the appliances in the failover group to communicate with each other using multicasting.

You can make this change at any time.

Step 1 On the host OS, find the `macvtap` interface associated with the interface with which the multicast traffic will be associated.

Step 2 Set the `macvtap` interface to use promiscuous mode:

```
Enter on the host: ifconfig macvtapX promisc
```

Related Topics

- Deploy on KVM, page 12

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 27.
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 Security Image and Files, page 8.
3.	Deploy the virtual appliance on your ESXi host or cluster.	Deploy the Virtual Appliance, page 17.
4.	(Optional) Clone the image if you want to run multiple virtual appliances on your network.	(Optional) Clone the Virtual Appliance, page 16.
5.	Prevent intermittent connectivity issues.	Disable unused network interface cards (NICs) on the virtual machine.
6.	Configure synchronization on the virtual machine to avoid random failures on your Cisco Content Security virtual appliance.	Important! Prevent Random Failures, page 18
7.	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 19
8.	Install the license file.	Install the Virtual Appliance License File, page 19.
9.	Log into 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 27. • 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.
10.	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 27.

(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 21 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 10
- Deploy on KVM, page 12
- Deploy on VMWare ESXi, page 16

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 Security Image and Files, page 8.

Step 1 Unzip the .zip file for the virtual appliance in its own directory; e.g., `C:\vESA\C100V` or `:\vWSA\S300V`.

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.**

Related Topics

- Deploy on Microsoft Hyper-V, page 10
- Deploy on KVM, page 12
- Deploy on VMWare ESXi, page 16

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 lost messages, database corruption, or lost 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 In the vSphere Client, select a virtual appliance from the list of machines.

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 10
- Deploy on KVM, page 12
- Deploy on VMWare ESXi, page 16

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 after you have completed the setup wizard.

Related Topics

- Deploy on Microsoft Hyper-V, page 10
- Deploy on KVM, page 12
- Deploy on VMWare ESXi, page 16

Amazon Web Services (AWS) EC2 Deployments

See the Deploying Cisco Web Security and Security Management Virtual Appliances on Amazon Elastic Compute Cloud (EC2) on Amazon Web Services (AWS) 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 Using SSH or telnet in a terminal application, log into the appliance's CLI as the `admin/ironport` user.

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 10.

For KVM deployments:

- Return to Deploy on KVM, page 12.

For ESXi deployments:

- For more information on the Management interface's IP address, see Deploy on VMWare ESXi, page 16.
- 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 16.

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 Email Security virtual appliance must have no mail in its queue.

Step 1 Migrate the virtual machine using the VMotion documentation.

Step 2 After migration, load the license.

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 content security product and release.

Step 1 If you are cloning an Email Security virtual appliance:
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 Security Management virtual appliance:
Disable centralized services on your managed Email and Web Security appliances.

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 powering on. Reconfigure IP address, Hostname and IP address. Then power on network adapters.

Configurations will not be complete until after you install feature keys.

b. For cloned Email Security virtual appliances:

- Delete all messages in the quarantines.
- Delete the message tracking and reporting data.

c. For cloned Web Security virtual appliances:

- Clear the proxy cache.
- Clear the proxy authentication cache using the `authcache > flushall` command in the CLI.
- Remove reporting and tracking data with the `diagnostic > reporting > deletedb` command in the CLI.
- Run the System Setup Wizard (SSW); a license must be available.
- For Authentication Realms, rejoin the domain.
- For Authentication Settings, modify the redirect hostname.
- If the original virtual appliance was managed by an Security Management appliance, add the cloned appliance to the Security Management appliance.

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.

Managing Your Cisco Content Security 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.

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. Licenses are hypervisor-independent.

For AsyncOS for Web Security 8.5 and later, AsyncOS for Email Security 8.5.x and later, and AsyncOS for Security Management 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 serve as a web proxy (Web Security appliance), deliver mail (Email 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 AsyncOS for Email Security 8.0 and AsyncOS for Web Security 7.7.5 and 8.0:

- Feature keys are included as part of the virtual appliance license. The feature keys expire at the same time as the license, even if the feature has not been activated. Purchasing new feature keys will require downloading and installing a new virtual appliance license file.
- Because 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 19

Force Reset, Power Off, and Reset Options Are Not Fully Supported

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 Content Security 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.
`reload`	—	Running this command removes the virtual appliance license and all the feature keys on the appliance. This command is available only for the Web Security appliance.

`diagnostic`	—	The following `diagnostic > raid` submenu 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 Email Security appliance.

`showlicense`	Yes	View license details. For virtual Email and 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`

Troubleshooting and Support

Troubleshooting: 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 after previously working.

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 on an Ubuntu virtual machine.

Solution Install the latest Host OS updates from Ubuntu.

General Troubleshooting on Linux Deployments

Problem Any issues with virtual appliances running on KVM deployments.

Solution See the troubleshooting section and other information in the *Virtualization Deployment and Administration Guide*, available from https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf.

Troubleshooting: 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 18

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 Virtual Email Security Appliances, page 26
- Product Identifier Codes (PIDs) for Virtual Web Security Appliances, page 26
- Product Identifier Codes (PIDs) for Virtual Content Security Management Appliances, page 27

Product Identifier Codes (PIDs) for Virtual Email Security Appliances

Functionality	PID	Description
Email Security Inbound	ESA-ESI-LIC=	Includes: • Anti-Spam • Anti-Virus • Outbreak Filters
Email Security Outbound	ESA-ESO-LIC=	Includes: • DLP • Encryption
Email Security Premium	ESA-ESP-LIC=	Includes: • Anti-Spam • Anti-Virus • Outbreak Filters • DLP • Encryption
Cloudmark Anti-Spam	ESA-CLM-LIC=	—
Image Analyzer	ESA-IA-LIC=	—
McAfee Anti-Virus	ESA-MFE-LIC=	—
Intelligent Multi-Scan	ESA-IMS-LIC=	—
Advanced Malware Protection	ESA-AMP-LIC=	—
Graymail safe-unsubscribe	ESA-GSU-LIC=	(A la carte)

Product Identifier Codes (PIDs) for 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 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
Email Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html

Related Topics

- Deploy on Microsoft Hyper-V, page 10
- Deploy on KVM, page 12
- Deploy on VMWare ESXi, page 16