

Cisco Secure Web Virtual Appliance Installation Guide

First Published: 2023-03-03

Last Modified: 2025-05-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **About Cisco Secure Web Virtual Appliance** 1

Supported Virtual Appliance Models and AsyncOS Releases for Hyper-V Deployments 2

Supported Secure Web Virtual Appliance Models and AsyncOS Releases for KVM Deployments 4

Virtual Appliance Models for VMWare ESXi Deployments 5

CHAPTER 2 **System Requirements** 9

Microsoft Hyper-V Deployments 9

Supported Microsoft Hyper-V and host operating systems 9

Hardware Requirements for Microsoft Hyper-V Deployments 9

KVM Deployments 9

Red Hat Enterprise Linux Server 9

KVM Drivers 10

VMWare ESXi Deployments 10

Supported VMWare ESXi Hypervisors 10

Hardware Requirements for VMWare ESXi Deployments 11

ESXi Drivers 11

CHAPTER 3 **Prepare the Content Secure Image and Files** 13

Determine the Best-Sized Virtual Appliance Image for Your Deployment 13

Download the Cisco Content Security Virtual Appliance Image 13

Prepare the License and Configuration Files to Load at Startup (KVM Deployments) 14

CHAPTER 4 **Deploy on Microsoft Hyper-V** 15

Deploy on Microsoft Hyper-V 15

Deploy a Virtual Appliance on Microsoft Hyper-V 16

If DHCP Is Disabled, Set Up the Appliance on the Network (Microsoft Hyper-V) 17

CHAPTER 5 **Deploy on KVM** 19

Deploy on KVM 19

Ensure Virtual Appliance Image Compatibility With Your KVM Deployment 20

Deploy the Virtual Appliance Using Virtual Machine Manager 20

Deploy the Virtual Appliance Using virt-install: Example 22

(Optional) Configure the Virtual Interface to Support High Availability 23

CHAPTER 6 **Deploy on VMWare ESXi** 25

Deploy on VMWare ESXi 25

(Optional) Configure the Virtual Interface to Support High Availability for ESXi 26

(Optional) Clone the Virtual Appliance 26

Deploy the Virtual Appliance 27

Important! Prevent Random Failures 28

If DHCP Is Disabled, Set Up the Appliance on the Network (VMware vSphere) 29

CHAPTER 7 **Amazon Web Services (AWS) EC2 and Microsoft Azure Marketplace Deployments Deployments** 31

CHAPTER 8 **Managing Your Cisco Secure Virtual Appliance** 33

IP Address 33

The Virtual Appliance License 33

Install the Virtual Appliance License File 34

Migrate Your Virtual Appliance to Another Physical Host 35

Clone a Virtual Appliance Already in Use 35

Force Reset, Power Off, and Reset Options Are Not Fully Supported 36

CLI Commands on the Virtual Appliance 36

SNMP on the Virtual Appliance 37

CHAPTER 9 **Troubleshooting and Support** 39

Troubleshooting: KVM Deployments 39

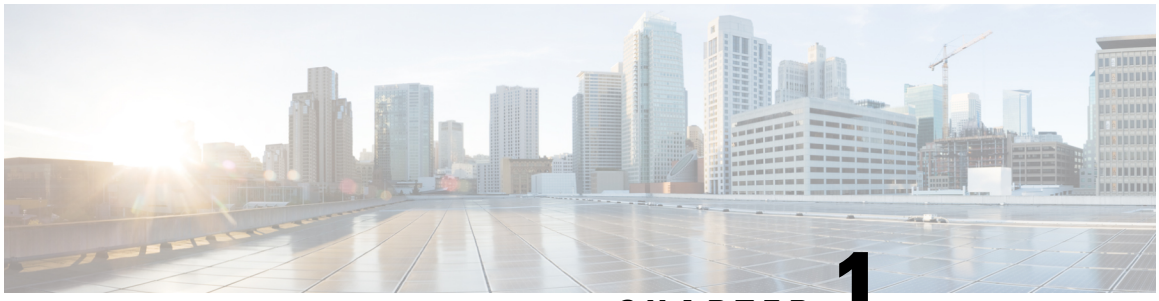
Virtual Appliance Hangs on Reboot 39

Network Connectivity Works Initially, Then Fails 40

Slow Performance, Watchdog Issues, and High CPU Usage 40

Troubleshooting: VMWare ESXi Deployments 40
Intermittent Connectivity Issues 40
Random Failures 40
Getting Support for Virtual Appliances 40
Cisco TAC 42

CHAPTER 10 **Additional Information** 43
Additional Information 43



CHAPTER 1

About Cisco Secure Web Virtual Appliance

Cisco Secure Web virtual appliance function the same as physical Cisco Secure Web Appliance, with only a few minor differences, which are documented in Managing Your Cisco Secure Virtual Appliance.

- Supported Virtual Appliance Models and AsyncOS Releases for Hyper-V Deployments, on page 2
- Supported Secure Web Virtual Appliance Models and AsyncOS Releases for KVM Deployments, on page 4
- Virtual Appliance Models for VMWare ESXi Deployments, on page 5

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 Secure Web Virtual Appliance	AsyncOS 14.5 and later	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
		S1000V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	48 GB	24
	AsyncOS 12.5 and later	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 12.0	**S100V**	250 GB	200 GB 250 GB	8 GB	3

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
		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 11.8 and later	**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
		S100V	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4
		S600V	1024 GB	-	24 GB	12

Supported Secure Web Virtual Appliance Models and AsyncOS Releases for KVM Deployments

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
Cisco Secure Web Virtual Appliance	AsyncOS 14.5 and later	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
		S1000V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	48 GB	24
	AsyncOS 12.5 and later	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 12.0	**S100V**	250 GB	200 GB 250 GB	8 GB	3

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
		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 11.8 and later	**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
		S600V	1024 GB	-	24 GB	12
		S100V	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4

Virtual Appliance Models for VMWare ESXi Deployments

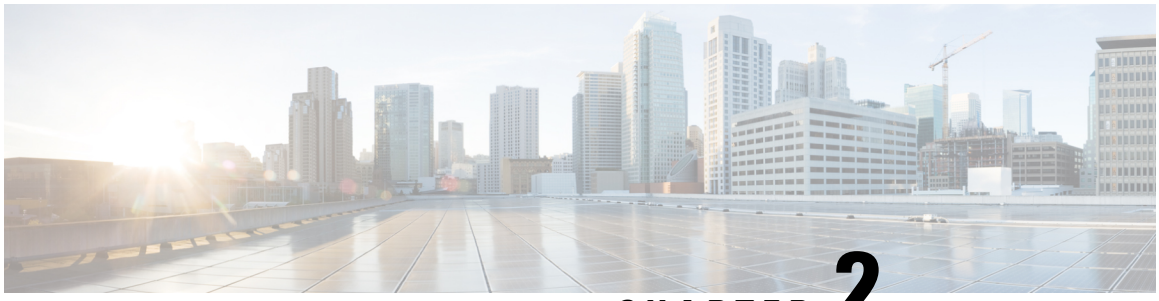


Note Except as explicitly stated in the AsyncOS documentation, modifications to the ESXi configurations defined in the OVF are not supported.

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
Cisco Secure Web Virtual Appliance	AsyncOS 14.5 and later	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
		S1000V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	48 GB	24
	AsyncOS 12.5 and later	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	12 GB	5
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
	AsyncOS 12.0	**S100V**	250 GB	200 GB 250 GB	8 GB	3
		S300V	1024 GB	500 GB 750 GB 1.0 TB	8 GB	4
		S600V	1024 GB		24 GB	12

Product	AsyncOS Release	Model	Recommended Disk Size	Supported Disk Sizes	RAM	Processor Cores
				750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB		
	AsyncOS 11.8 and later	**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
		S600V	1024 GB	750 GB 1.0 TB 1.5 TB 2.0 TB 2.4 TB	24 GB	12
		S100V	250 GB	-	6 GB	2
		S300V	1024 GB	-	8 GB	4

AsyncOS version requirements are described in Supported VMWare ESXi Hypervisors.



CHAPTER 2

System Requirements

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

Microsoft Hyper-V Deployments

Supported Microsoft Hyper-V and host operating systems

AsyncOS Version	Hyper-V
AsyncOS 11.8 (Web) and later	Microsoft Hyper-V Server 2019

Hardware Requirements for Microsoft Hyper-V Deployments

- Supported on Cisco UCS C-Series servers, with Intel Xeon based CPUs
- Cisco Secure Web Virtual performance test labs use as minimum the following: Cisco Unified Computing System™ (Cisco UCS®) C-Series M5 server with the Intel(R) Xeon(R) Gold 6246 CPU @ 3.30GHz

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 release 8.6 (Ootpa)

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

Version Info:

- Linux: 4.18.0-372.32.1.el8_6.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 servers, with Intel Xeon based CPUs
- Cisco Secure Web Virtual performance test labs use as minimum the following: Cisco Unified Computing System™ (Cisco UCS®) C-Series M5 server with the Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz

KVM Drivers

Supported KVM drivers:

- Network: E1000, Virtio
- Disk: VirtIO

VMWare ESXi Deployments

Supported VMWare ESXi Hypervisors

AsyncOS (Web)	VMWare ESXi Version
AsyncOS 15.5.x	7.0 and 8.0
AsyncOS 15.2.3 and later	7.0 and 8.0
AsyncOS 15.2.x	7.0
AsyncOS 15.0.x	7.0
AsyncOS 14.5.x	7.0
AsyncOS 14.0.x	7.0
AsyncOS 12.7.x	7.0
AsyncOS 12.5.x	7.0
AsyncOS 12.0.x	7.0

AsyncOS (Web)	VMWare ESXi Version
AsyncOS 11.8.1 and later	7.0
AsyncOS 11.8.0	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 (blade or rack-mounted) are the only supported hardware platform.

Minimum requirements for the server hosting your virtual appliances:

Hypervisor Details:

- VMware ESXi 7.x/8.x (for more information, refer to Supported VMWare ESXi Hypervisors)

Hardware:

- Supported on: Cisco UCS C Series 220/240 M5

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.

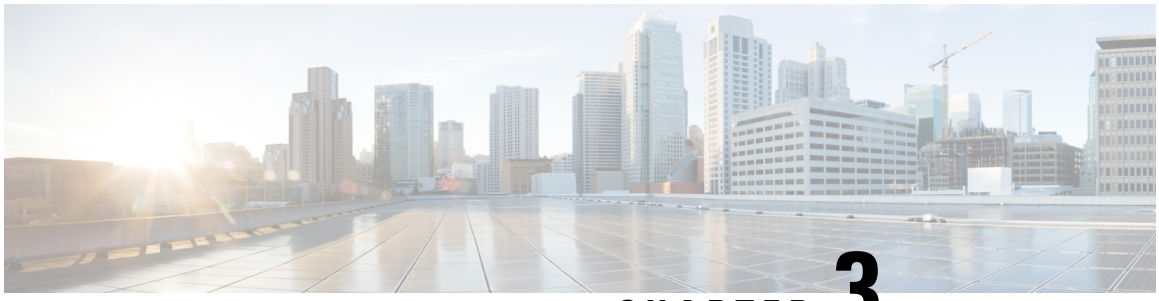
Note Except as explicitly stated in the documentation, Cisco does not support the alteration of the Cisco Content Security virtual appliance’s hardware configuration, such as removing IP interfaces or changing the appliance’s CPU cores or RAM size. The appliance may send alerts if such changes are made.

Note VMWare ESXi 7.0 deployment is supported on Cisco UCS M4 and M5 chassis servers with AsyncOS 14.0.1-053 and later (for Cisco Secure Web Appliances).

ESXi Drivers

Supported ESXi drivers:

- Network Adapter Type: E1000



CHAPTER 3

Prepare the Content Secure Image and Files

- Determine the Best-Sized Virtual Appliance Image for Your Deployment, on page 13
- Download the Cisco Content Security Virtual Appliance Image, on page 13
- Prepare the License and Configuration Files to Load at Startup (KVM Deployments), on page 14

Determine the Best-Sized Virtual Appliance Image for Your Deployment

Determine the best-sized virtual appliance image for your needs. See the Cisco Secure Web Appliance data sheet available in the following location:

- https://www.cisco.com/c/en/us/products/security/web-security-appliance/datasheet-listing.html

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.

Procedure

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

- Cisco Secure Web Appliance

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
- Deploy on KVM
- Deploy on VMWare ESXi

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

This feature was introduced in AsyncOS 8.6 for Cisco Secure Web Appliance. 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).

Procedure

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.

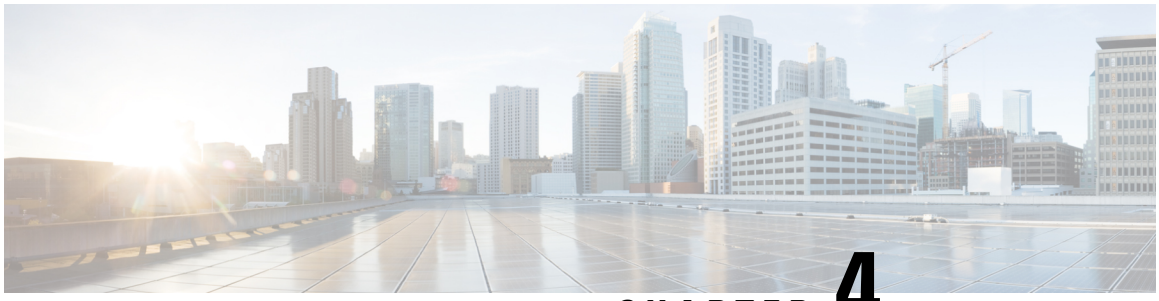
What to do next

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 “Cisco Secure Web Appliance CLI Commands” topic in the “Command Line Interface” chapter in the user guide.

Related Topics:

- Deploy on KVM



CHAPTER 4

Deploy on Microsoft Hyper-V

- Deploy on Microsoft Hyper-V, on page 15
- Deploy a Virtual Appliance on Microsoft Hyper-V, on page 16
- If DHCP Is Disabled, Set Up the Appliance on the Network (Microsoft Hyper-V), on page 17

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, on page 43.
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, on page 13.
3.	Deploy the virtual appliance on Hyper-V.	**1.** Set up the Windows Server Operating System. Ensure that you have installed the required Hyper-V roles. See System Requirements for more information. **2.** Download the image as described in Prepare the Content Secure Image and Files, on page 13. **3.** Using the Hyper-V Manager, install the virtual appliance image using the New Virtual Machine Wizard and edit the processor setting. For detailed steps, see Deploy a Virtual Appliance on Microsoft Hyper-V, on page 16
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).
5.	Install the license file	Install the Virtual Appliance License File.

	Action	More Information
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, on page 43. • 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 The following are the limitations for virtual Cisco Secure Web appliances (with FreeBSD 10.x) deployed on Microsoft Hyper-V generation 1 platform:

- It is not possible to modify the virtual appliance interfaces using the **etherconfig** CLI command.
- The **ifconfig** CLI command displays the virtual appliance interface status as Unknown or Simplex even though it runs on Duplex mode.

However, there is no impact on the performance of the appliance due to the above limitations.

Deploy a Virtual Appliance on Microsoft Hyper-V

Before you begin

Download the image as described in Prepare the Content Secure Image and Files, on page 13.

Procedure

Step 1 Open the Hyper-V Manger and select **Action** > **New** > **Virtual Machine**.

Step 2 In the **New Virtual Machine Wizard**, do the following:

a) Review the **Before You Begin** page and click **Next**.

b) Specify the name and storage location for your virtual machine and then click **Next**.

Note
The virtual machines dynamically increase their storage size, so we recommend you to select a storage location with ample space.

c) Select the generation for the virtual machine and click **Next**.

Note

Some of the older operating systems and hardwares does not support the new features in **Generation 2** virtual machines. If you are using an older hardware or operating system, we recommend you to always select **Generation 1**.

d) Assign the memory that you want to allocate for the virtual machine. Enter the value in MBs and click **Next**.
e) Choose the Cisco VIC Ethernet interface virtual switch from the **Connection** drop-down list and then click **Next**.
f) Choose the option **Use an existing virtual hard disk**. Browse and select the `vhdx.tgz` image that you have downloaded from Cisco.com and then click **Next**.
g) Review the virtual machine details and click **Finish**.

Step 3 Right-click the newly deployed virtual machine and select **Settings**.

Step 4 Select **Processor** and enter the number of processors. For more information on the number processors and NICs required, see Determine the Best-Sized Virtual Appliance Image for Your Deployment to check for the number of processors and NICs required.

Step 5 (Optional) Select **Add Hardware** and add network interfaces for P1 and P2.

Step 6 Select the interfaces and configure VLAN with appropriate values.

Step 7 Click **OK** to save the settings.

Step 8 Right-click the virtual machine and select **connect** to launch the virtual appliance.

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.

Procedure

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

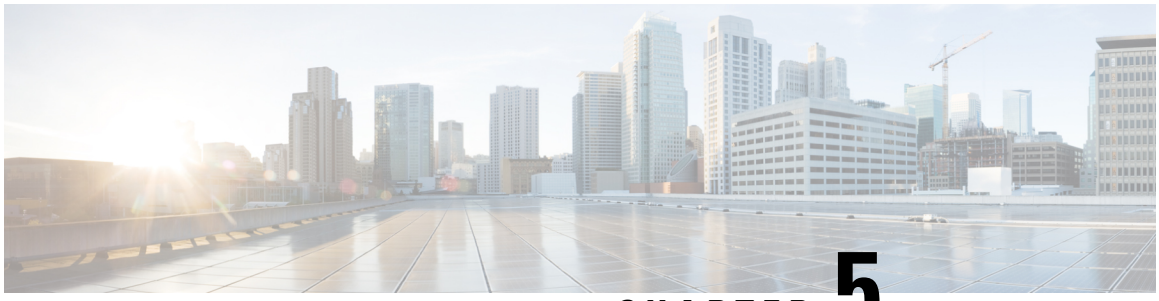
Step 2 Write down the IP address of the virtual appliance's Management port.

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.



CHAPTER 5

Deploy on KVM

- Deploy on KVM, on page 19
- Ensure Virtual Appliance Image Compatibility With Your KVM Deployment, on page 20
- Deploy the Virtual Appliance Using Virtual Machine Manager, on page 20
- Deploy the Virtual Appliance Using virt-install: Example, on page 22
- (Optional) Configure the Virtual Interface to Support High Availability, on page 23

Deploy on KVM

	Action	More Information
Step 1	Ensure that your equipment and software meet all system requirements.	See System Requirements 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, on page 43.
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.
Step 5	Ensure that the Cisco image is compatible with your deployment.	See Ensure Virtual Appliance Image Compatibility With Your KVM Deployment.
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).
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.

	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. • Deploy the Virtual Appliance Using virt-install: Example.
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.
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 Install the Virtual Appliance License File, on page 34. • 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

Procedure

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 10**

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.

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

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.

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=freebsd10 \
--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 Restart the virtual appliance:

```
virsh start wsa-example
```

```
virsh --connect qemu:///system start wsa-example
```

Step 5 To Start/Stop the virtual appliance:

```
--virsh shutdown wsa-example
```

```
--virsh start wsa-example
```

Related Topics:

- Deploy on KVM

(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 Cisco Secure Web 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.

Procedure

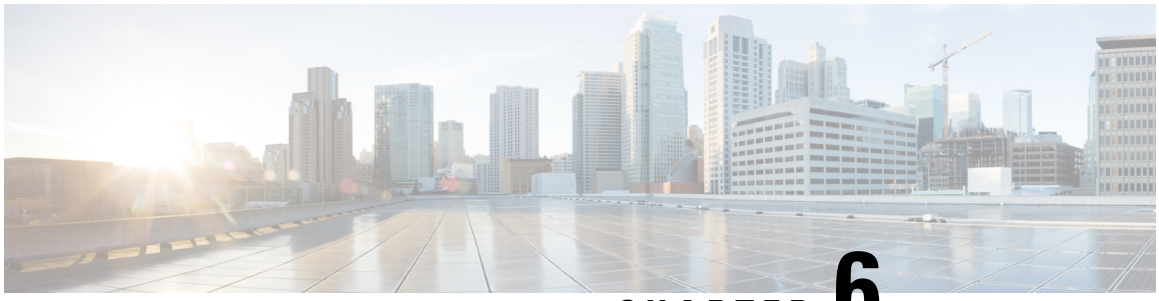
Step 1 On the host OS, find the **macvtap** interface associated with the interface with which the multicast traffic will be associated.

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

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

Related Topics:

- Deploy on KVM



CHAPTER 6

Deploy on VMWare ESXi

- Deploy on VMWare ESXi, on page 25
- (Optional) Configure the Virtual Interface to Support High Availability for ESXi, on page 26
- (Optional) Clone the Virtual Appliance, on page 26
- Deploy the Virtual Appliance, on page 27
- Important! Prevent Random Failures, on page 28
- If DHCP Is Disabled, Set Up the Appliance on the Network (VMware vSphere), on page 29

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, on page 43.
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.
3.	Deploy the virtual appliance on your ESXi host or cluster.	Deploy the Virtual Appliance.
4.	(Optional) Clone the image if you want to run multiple virtual appliances on your network.	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. For more information, see (Optional) Configure the Virtual Interface to Support High Availability for ESXi.
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

	Action	More Information
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)
8.	Install the license file.	Install the Virtual Appliance License File.
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, on page 43. • 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, on page 43.

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. For more information, see (Optional) Configure the Virtual Interface to Support High Availability for ESXi.

(Optional) Configure the Virtual Interface to Support High Availability for ESXi

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 Cisco Secure Web 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.

Configure **Promiscuous mode** to **Accept** state for the **VLAN Port Group/Distributed Port Group** associated with the virtual interface of the appliance.

(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 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
- Deploy on KVM
- Deploy on VMWare ESXi

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 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.

Procedure

Step 1 Unzip the .zip file for the virtual appliance in its own directory;

Example:

```
C:\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.

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
- Deploy on KVM
- Deploy on VMWare ESXi

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.

Procedure

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
- Deploy on KVM
- Deploy on VMWare ESXi

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.

Procedure

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

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

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.

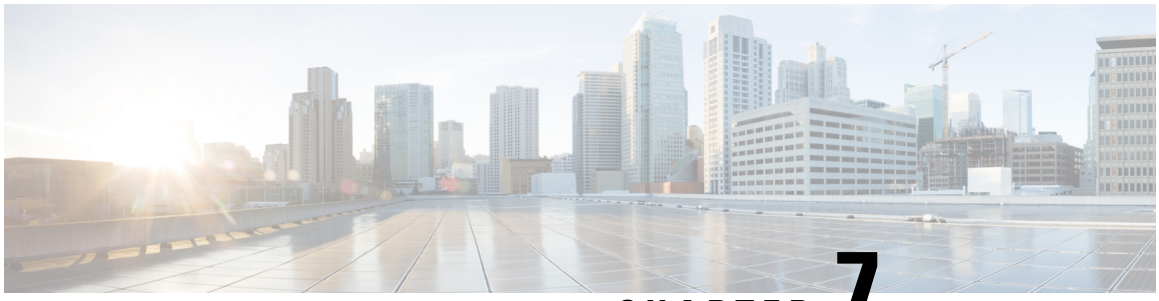
Step 3 Configure the default gateway using the **setgateway** command.

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
- Deploy on KVM
- Deploy on VMWare ESXi

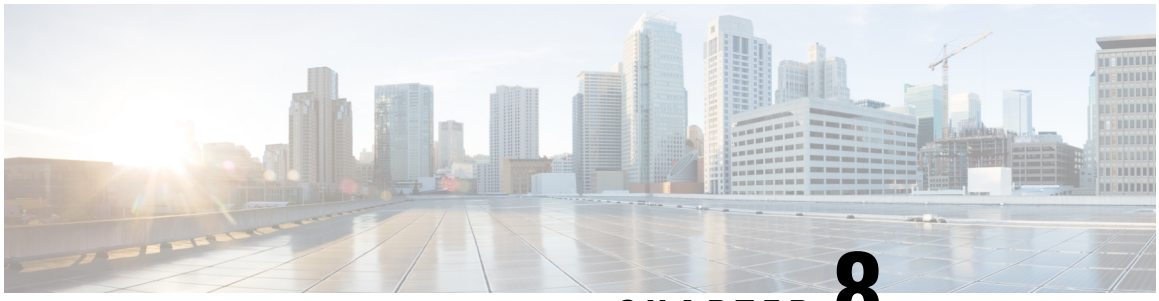


CHAPTER 7

Amazon Web Services (AWS) EC2 and Microsoft Azure Marketplace Deployments Deployments

Refer the following standalone guides for Amazon Web Services (AWS) EC2 and Microsoft Azure Marketplace deployments:

- For Amazon Web Services (AWS) EC2, see Deploying Cisco Web Security and Security Management Virtual Appliances on Amazon Elastic Compute Cloud (EC2) on Amazon Web Services (AWS)
- For Microsoft Azure Marketplace Deployments, see Deploy Cisco Secure Web Appliance on Microsoft Azure Marketplace



CHAPTER 8

Managing Your Cisco Secure Virtual Appliance

- IP Address, on page 33
- The Virtual Appliance License, on page 33
- Install the Virtual Appliance License File, on page 34
- Migrate Your Virtual Appliance to Another Physical Host, on page 35
- Clone a Virtual Appliance Already in Use, on page 35
- Force Reset, Power Off, and Reset Options Are Not Fully Supported, on page 36
- CLI Commands on the Virtual Appliance, on page 36
- SNMP on the Virtual Appliance, on page 37

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 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 Web Security 8.5 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 without security services for 180 days. Security services are not updated during this period. On the Cisco Secure Web appliance, administrators and end users cannot manage quarantines and scheduled deletion of quarantined messages will occur.

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

Related Topics:

- Install the Virtual Appliance License File

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.

For KVM deployments:

- Return to Deploy on KVM.

For ESXi deployments:

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

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).



Note Migrate the virtual machine using the VMotion documentation. Automatic VMotion is currently not supported in Secure Web Appliance.

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.

Procedure

Step 1 Disable centralized services on your Web Security appliances.

Step 2 Shut down the virtual appliance using the **shutdown** command in the CLI.

Step 3 Clone the virtual appliance image.

Step 4 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 fromCisco.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 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 > flushall > 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 5 Start the original virtual appliance using the VMware vSphere Client and resume operation. Make sure that it is running properly.

Step 6 Resume operation on the cloned appliance.

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

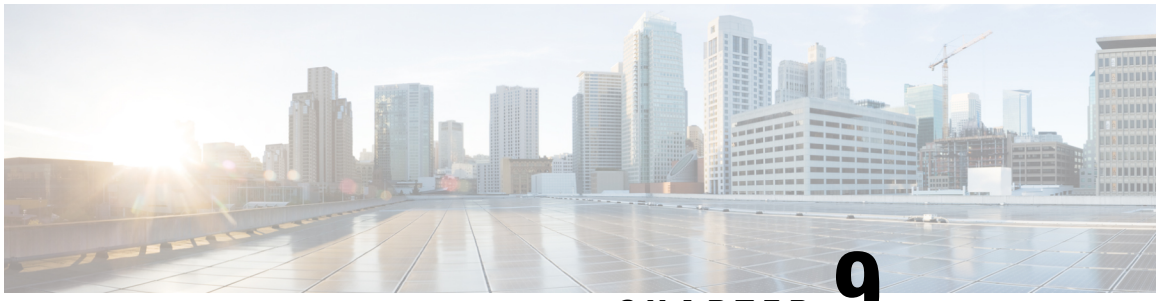
Command	Information
loadlicense	This command allows you to install a license for your virtual appliance. You cannot run System Setup Wizard on the virtual appliance without installing a license using this command first.
etherconfig	The Pairing option is not included on virtual appliances.

Command	Information
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.
reload	Running this command removes the virtual appliance license and all the feature keys on the appliance.
showlicense	View license details. For Secure Web Appliance, 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`



CHAPTER 9

Troubleshooting and Support

- Troubleshooting: KVM Deployments, on page 39
- Troubleshooting: VMWare ESXi Deployments, on page 40
- Getting Support for Virtual Appliances, on page 40
- Cisco TAC, on page 42

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:

Procedure

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.

What to do next

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 Virtual Appliances using KVM on Red Hat™ Enterprise Linux.

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

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

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 Product Identifier Codes (PIDs) for Cisco Secure Web Virtual Appliance.

Product Identifier Codes (PIDs) for Cisco Secure Web Virtual Appliance

Cisco Secure Web Appliance Unified SKU overview

Orders for Cisco Secure Web Appliance 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 Secure Web Appliance 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 Cisco Secure Web appliance – WEB-SEC-SUB. The term and payment option of the subscription applies to all products included in the subscription.

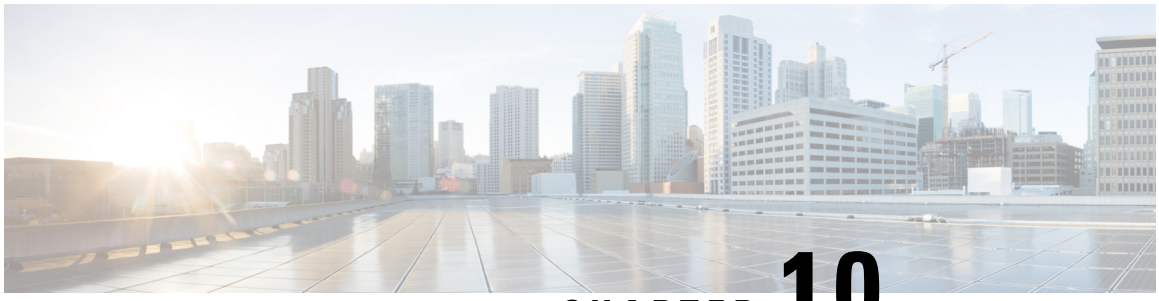
Functionality	PID	Description
Cisco Secure Web Essentials	WSA-WSE-LIC	Includes: • Web Usage Controls • Web Reputation
Cisco Secure Web Advantage	WSA-WSP-LIC	Includes: • Web Usage Controls • Web Reputation • Sophos and Webroot Anti-Malware signatures
Cisco Secure Web Premier	WSA-WSS-LIC	Includes: • Web Usage Controls • Web Reputation • Sophos and Webroot Anti-Malware signatures • Cisco Secure Malware Analytics • Cisco Cognitive Intelligence
Cisco Secure Malware Analytics	WSA-AMP-LIC	Includes: • Cisco Secure Malware Analytics
Cisco Secure Web Anti-Virus McAfee	WSA-AMM-LIC	Includes: • McAfee Anti-Malware signatures
Cisco Secure Web Sophos Anti-Malware	WSA-AMS-LIC	Includes: • Sophos Anti-Malware signatures

Functionality	PID	Description
Cisco Secure Web Webroot Anti-Malware	WSA-AMW-LIC	Includes: • Webroot Anti-Malware signatures

Cisco TAC

Contact information for Cisco TAC, including phone numbers:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html



CHAPTER 10

Additional Information

- Additional Information, on page 43

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:
Cisco Secure Web Appliances	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
- Deploy on KVM
- Deploy on VMWare ESXi

Additional Information