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.

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).
- The Cisco Secure Email Virtual Gateway must have no mail in its queue.

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.

Step 1 If you are cloning an 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 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 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 Cisco Secure Email Virtual Gateway 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 > 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 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.