ESA/SMA Virtual Deployment FAQ

Contents

Introduction

This document provides answers to frequently asked questions regarding the deployment, migration, and configuration of virtual Email Security Appliance (ESA) and virtual Security Management Appliance (SMA) devices.

Contributed by Dennis McCabe Jr, and Vibhor Amrodia, Cisco TAC Engineers.

Recommended Resources

Cisco recommends you familiarize yourself with these resources before deployment, configuration, and migration of your virtual ESA/SMA.

- Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses
- Cisco Content Security Virtual Appliance Installation Guide
- ESA User Guides (Setup and Installation sections)
- SMA User Guides (Setup and Installation sections)
- Virtual ESA Software Download
- Virtual SMA Software Download

Frequently Asked Questions

When replacing a hardware appliance (e.g. C190, M690), how do I know which virtual model to select?

In general, you'll want to replace the hardware model with a virtual model that starts with the same number. As an example, you can replace a C**1**90 with a C**1**00V or an M**6**90 with an M**6**00V. More

information on sizing can be found here for ESA and here for SMA. If in doubt, please contact your Cisco Account Team or Reseller and they can provide additional sizing recommendations. If working with data that needs to be migrated (e.g. PVO quarantine), it is also essential to take into account needed disk space during model selection.

When should I deploy and/or migrate to a virtual ESA/SMA?

You can deploy a virtual ESA/SMA at any time and it is recommended if you need additional devices for load distribution or for backing up centralized SMA data. However, it would be extremely beneficial and important to move to a virtual ESA/SMA if your hardware appliance is going End-of-Life (EoL) or End-of-Support (EoS).

You can find the EoL/EoS notices for ESA and SMA below:

- EoL/EoS for ESA
- EoL/EoS for SMA

You can also verify supported hardware in the respective version(s) release notes in the **Supported Hardware for This Release** sections:

- ESA Release Notes
- SMA Release Notes

How do I obtain and install a license for a virtual ESA/SMA?

If you have an existing hardware license then you're entitled to a virtual license for an ESA and/or SMA respectively. You can obtain a virtual license file using the steps in the following article:

- Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses

If you encounter a "Malformed license" error when installing the virtual license(s), please review the following troubleshooting document:

- "Malformed license" Error When Trying to Install a License File on Virtual

How many devices can I deploy using my virtual ESA/SMA license?

You can spin up as many as you like. Unlike a hardware license that is tied to a specific physical appliance, the virtual license can be used and reused for any number of virtual devices that you deploy.

Does a virtual ESA/SMA support Smart Licensing?

Smart Licensing is supported. You can refer to this document for more information on how you can go about enabling Smart Licensing on a virtual ESA/SMA:

- Smart Licensing Overview and Best Practices for Cisco Email and Web Security (ESA, WSA, SMA)

  Note: After enabling Smart Licensing, you might receive "**Dynamic manifest fetch failure: Failed to authenticate with the manifest server**" errors on the virtual ESA/SMA devices. This is a known issue and is documented here: Field Notice: FN - 70490

How would I plan a migration from a legacy hardware device to a new virtual ESA?

The process and overview of the steps included in planning the migration of the configuration from the legacy ESA devices to virtual devices would be similar to the documented steps in this article:

- Migrating a Configuration from an Older HW Model (Cx70) to a New HW Model (Cx95)

While the article is primarily for migrating from an x70 EoL hardware device to a newer supported x95, the Utilizing a vESA to Bridge Configuration to New HW (Cx95) section can be used for deploying a new virtual ESA and joining it to an existing cluster. Once joined to an existing cluster and the new virtual ESA has a copy of your current configuration, you can then decide if you wish to keep everything as-is, or if you then want to proceed with decommissioning your legacy hardware. If the latter, you can then remove the legacy hardware from the cluster.

How do I verify my virtual ESA/SMA is using the correct update server?

Hardware and virtual devices utilize different *dynamichost* servers when fetching updates (e.g. Anti-Spam, Anti-Virus, Etc.).

You can use the **dynamichost** sub-command under **updateconfig** in the CLI to review the current configuration. Do note that it is a hidden command.

```
esa.lab.local> updateconfig

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> dynamichost

Enter new manifest hostname:port
[update-manifests.sco.cisco.com:443]>
```

Hardware and virtual models use the following dynamichost servers respectively:

Hardware Manifest: update-manifests.ironport.com:443
Virtual Manifest: update-manifests.sco.cisco.com:443

If your virtual ESA is not able to download updates, you can follow the steps in the articles below to confirm everything is configured properly:

- vESA Is Not Able to Download and Apply Updates
- ESA AsyncOS Upgrade and Troubleshoot Procedure

> **Note**: Virtual appliances (e.g. x100V, x300V, x600V) should ONLY use the dynamic host URL of *update-manifests.sco.cisco.com:443*. If there is a cluster configuration with both hardware and virtual appliances, **updateconfig** must be configured at the machine level and then confirm that **dynamichost** is set accordingly.

How do I export a configuration file from one ESA/SMA and import it into another?

The following articles can be referenced for exporting and importing configuration files:

- How to Load or Migrate ESA Configuration on a Replacement ESA
- Saving and Exporting Configuration Settings (ESA User Guide)
- Saving and Importing Configuration Settings (SMA User Guide)

> **Note**: Configuration files exported with masked passphrases cannot be loaded. Instead, they should be exported using the **Plain** or **Encrypt** passphrase option.

How do I load a partial configuration?

When migrating from a hardware appliance to a virtual ESA/SMA, or between different model types, it is common that you will not be able to simply export the configuration from one and import into another without modification. This is due to different disk sizing, the number of interfaces, AsyncOS version, Etc.

If this happens, you can contact Cisco TAC to assist, or you can try loading a partial portion of the configuration using the steps below:

- How to Import Partial Configurations Into the ESA?