



# CISCO EMAIL SECURITY APPLIANCE

## INITIAL SETUP

**October 2015**  
**Version 1.0**

Tim Bostrom  
Cisco Sales Engineer

The most current version of this document can be found here:  
<https://cisco.com/go/emailsecurity-customer>

# ESA Initial Setup - Best Practices

<b>PURPOSE OF THIS DOCUMENT</b>	<b>3</b>
<b>OVERVIEW OF STEPS</b>	<b>3</b>
<b>STEP 1: ESA - INITIAL INSTALLATION</b>	<b>3</b>
<b>STEP 2: ESA - LICENSING</b>	<b>9</b>
<b>STEP 3: ESA - UPGRADING</b>	<b>12</b>
<b>NEXT STEPS AND SUMMARY</b>	<b>15</b>

## PURPOSE OF THIS DOCUMENT

There are a few steps that are needed to be followed in order to bootstrap and prepare a Cisco Email Security Appliance (ESA) and Secure Management Appliance (SMA) for installation. This document will cover the steps needed to prepare an ESA and SMA to run the Initial Setup Wizard. The Initial Setup Wizard is a wizard questionnaire helps customers build a base configuration for email security in their environment. Initial Setup Wizard will be covered in a separate document.

This document will cover gathering and configuring the required network settings (IP, DNS, etc.) so that the ESA and SMA can be put on the network and configured.

## OVERVIEW OF STEPS

### **Step 1: Configure network settings – initial setup**

You will need to configure network settings for your environment in order to access the ESA and SMA for deployment. These network settings include interface IP addresses, DNS, routes, etc.

### **Step 2: License the device**

You will need a valid license, either evaluation or full subscription, in order to use the ESA and SMA in your organization. This step will cover applying a license to your device.

### **Step 3: Upgrade the device**

It is best to upgrade your ESA and SMA to the latest General Deployment release to take advantage of new features and bug fixes. This section will cover upgrading the device to the latest GD version of code.

## STEP 1: ESA - INITIAL INSTALLATION

The primary audience of this document will be deploying hardware appliances. When deploying HW appliances, you should connect your laptop to the ESA's MGMT Ethernet Port and power on the ESA. This requires a crossover ethernet cable unless your laptop automatically senses the need for crossover and flips the pin logically — most modern laptops do this automatically. The ESA will have an IP address of 192.168.42.42/24 on MGMT. Configure your laptop for 192.168.42.41/24. You do not need a Default router nor do you need DNS settings.

Though most deployments will be with a HW appliance, I will discuss “virtual” appliances also in this document. I will be using a C100v and C300v ESAv appliance and an M300v SMAv appliance for the purposes of this document.

## ESA Incoming and Outgoing Content Filters - Best Practices

- We will be using Management (MGMT) Ethernet Port for both the ESAv and SMAv in my lab.
- For the ESAv, I will have a single IP Interface named “BiDirectional” and an IP address of 10.0.1.37/24. The Interface hostname will be “esa1.unc-hamiltons.com”. Note that each IP Interface requires an “Interface hostname” and it is that hostname that is used in the EHLO conversation when sending email using that Interface. You’ll see me setting this value in the “interfaceconfig” command below.
- Default Route: 10.0.1.1
- Local DNS: 10.0.1.7

The section will detail the following:

1. Setting up the IP interface
2. Setting the system hostname
3. Setting the default route
4. Setting the DNS server
5. Testing
6. Licensing
7. Upgrade the Appliance to the latest General Deployment (GD) version code
8. Ready to the Initial Setup Wizard

(To be able to easily copy the text output while running the “interfaceconfig” command and paste in to this document, I wanted to ssh into the appliance instead of using the VMWare Console feature — the VMWare Console feature has a very low resolution and does not allow an easy way to copy all text. Therefore, I used the VMWare console to run the “interfaceconfig” command and only quickly set the IP address and subnet mask (10.0.1.37/24). I then did a “commit” and hit return — or the Enter key — twice to commit changes. Now you can see below I can ssh directly to the 10.0.1.37 address and login. As explained earlier in this document “Virtual” appliances use DHCP to obtain an IP address and you can easily see what address is assigned by issuing the “interfaceconfig” command and then control-C to end the command. For HW appliances, the IP address will always be 192.168.42.42 as discussed above)

### 1. Setting up the IP interface

Connect to the Appliance over SSH (putty.exe for Windows users)

The default username/password is admin/ironport.

```
Daltons-Mac-Pro:~ dalton$ ssh admin@10.0.1.37
admin@10.0.1.37's password:
Last login: Sun May 10 13:00:39 2015 from 10.0.1.7
AsyncOS 9.1.0 for Cisco C300V build 032
```

## ESA Incoming and Outgoing Content Filters - Best Practices

Welcome to the Cisco C300V Email Security Virtual Appliance

```
ironport.example.com> interfaceconfig
```

Currently configured interfaces:

1. Management (10.0.1.37/24 on Management: ironport.example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

```
[>] edit
```

Enter the number of the interface you wish to edit.

```
[>] 1
```

IP interface name (Ex: "InternalNet"):

```
[Management]>
```

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 192.168.1.2 ):

```
[10.0.1.37]> 10.0.1.37
```

Netmask (Ex: "24", "255.255.255.0" or "0xffffffff"):

```
[0xffffffff]> <return key entered>
```

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:

1. Data 1
2. Data 2
3. Management

```
[3]> <return key entered>
```

Hostname:

```
[ironport.example.com]> esal.unc-hamiltons.com
```

Do you want to enable SSH on this interface? [Y]> <return key entered>

Which port do you want to use for SSH?

```
[22]> <return key entered>
```

Do you want to enable FTP on this interface? [N]> Y

Which port do you want to use for FTP?

```
[21]> <return key entered>
```

Do you want to enable Cluster Communication Service on this interface? [N]>

```
<return key entered>
```

Do you want to enable HTTP on this interface? [Y]> <return key entered>

Which port do you want to use for HTTP?[80]> <return key entered>

Do you want to enable HTTPS on this interface? [Y]> <return key entered>

Which port do you want to use for HTTPS?[443]> <return key entered>

Do you want to enable Spam Quarantine HTTP on this interface? [N]> <return key entered>

## ESA Incoming and Outgoing Content Filters - Best Practices

```
Do you want to enable Spam Quarantine HTTPS on this interface? [N]> <return key entered>
```

```
Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [N]> Y  
Which port do you want to use for AsyncOS API (Monitoring) HTTP? [6080]>
```

```
Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [N]> Y  
Which port do you want to use for AsyncOS API (Monitoring) HTTPS? [6443]>  
The "Demo" certificate is currently configured. You may use "Demo", but this will not be secure. To assure privacy, run "certconfig" first.
```

```
Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the secureservice? [Y]> N
```

```
Updating SNMP agent interface referencing the old interface name "Management" to the new interface name "BiDirectional".
```

```
Currently configured interfaces:
```

1. BiDirectional (10.0.1.37/24 on Management: esa1.unc-hamiltons.com)

```
Choose the operation you want to perform:
```

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

```
[ ]> <return key entered>
```

```
Please run "systemsetup" or "sethostname" then "commit" before sending mail.  
ironport.example.com>
```

### 2. Set the System Hostname

This is the “System Hostname” — which may be different than the “interface hostname” you configured in previous step. Since I have only one Interface (going with Deployment Option 1), the Interface hostname is the same as the System Hostname.

```
ironport.example.com> sethostname
```

```
[ironport.example.com]> esa1.unc-hamiltons.com
```

### 3. Set the default route

```
ironport.example.com> setgateway
```

Warning: setting an incorrect default gateway may cause the current connection to be interrupted when the changes are committed.

```
Set gateway for:
```

1. IPv4
2. IPv6

```
[1]> <return key entered>
```

```
Enter new default gateway:
```

```
[10.0.1.1]> <return key entered>
```

```
ironport.example.com>
```

# ESA Incoming and Outgoing Content Filters - Best Practices

## 4. Setup DNS resolution

```
ironport.example.com> dnsconfig
```

```
[NOTE: This is a virtual appliance and as you can see below, it obtained a DNS server from DHCP. I'll remove it and step you through how to configure your ESA to point to your local DNS server]
```

```
Currently using the local DNS cache servers:
```

1. Priority: 0 10.0.1.7

```
Choose the operation you want to perform:
```

- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.

```
[>] delete (I'm doing this for demonstration purposes - so I can create the record again to demonstrate. This record was created via DHCP since I'm on a "ESAv" appliance.)
```

```
Do you want to delete a local DNS cache server or an alternate domain server?
```

1. Delete a local DNS cache server.
2. Delete an alternate domain server.

```
[>] 1
```

```
Currently using the local DNS cache servers:
```

1. Priority: 0 10.0.1.7

```
Enter the number of the server you wish to remove.
```

```
[>] 1
```

```
Note: You have removed the last local nameserver entry. DNS will now use the Internet root servers.
```

```
Currently using the Internet root DNS servers.
```

```
No alternate authoritative servers configured.
```

```
Choose the operation you want to perform:
```

- NEW - Add a new server.
- SETUP - Configure general settings.

```
[>] setup
```

```
Do you want the Gateway to use the Internet's root DNS servers or would you like it to use your own DNS servers?
```

1. Use Internet root DNS servers
2. Use own DNS cache servers

```
[1]> 2
```

```
Please enter the IP address of your DNS server.
```

```
Separate multiple IPs with commas.
```

```
[>] 10.0.1.7 (Note, you can add more than one DNS Server. Just separate them by a comma)
```

```
Please enter the priority for 10.0.1.7.
```

```
A value of 0 has the highest priority.
```

```
The IP will be chosen at random if they have the same priority.
```

```
[0]>
```

```
Choose the IP interface for DNS traffic.
```

1. Auto
2. BiDirectional (10.0.1.37/24: esa1.unc-hamiltons.com)

```
[1]>
```

## ESA Incoming and Outgoing Content Filters - Best Practices

```
Enter the number of seconds to wait before timing out reverse DNS lookups.  
[20]>
```

```
Enter the minimum TTL in seconds for DNS cache.  
[1800]>
```

```
Currently using the local DNS cache servers:  
1. Priority: 0 10.0.1.7
```

```
Choose the operation you want to perform:
```

- NEW - Add a new server.
  - EDIT - Edit a server.
  - DELETE - Remove a server.
  - SETUP - Configure general settings.
- ```
[ ]>
```

```
ironport.example.com
```

### Commit the changes

```
ironport.example.com> commit
```

```
Please enter some comments describing your changes:  
[ ]>
```

```
Do you want to save the current configuration for rollback? [Y]>  
Changes committed: Sun May 10 13:05:31 2015 GMT
```

```
esal.unc-hamiltons.com>
```

## 5. Testing

Let's use "dig" to ensure the ESA is getting name-resolution (DNS resolution). To find out the legal parameters of any command, type help and the name of the command. Here is the help for dig (for example)

```
esal.unc-hamiltons.com> help dig
```

```
dig [options] [ @<dns_ip> ] [qtype] <hostname>
```

```
Look up a record on a DNS server.
```

```
Options:
```

- s <source\_ip> Specify the source IP address.
- t Make query over TCP.
- u Make query over UDP (default).

```
dns_ip - Query the DNS server at this IP address.
```

```
qtype - Query type: A, PTR, CNAME, MX, SOA, NS, TXT.
```

```
hostname - Record that user want to look up.
```

```
dig -x <reverse_ip> [options] [ @<dns_ip> ]
```

```
Do a reverse lookup for given IP address on a DNS server.
```

```
Options:
```

- s <source\_ip> Specify the source IP address.
- t Make query over TCP.



## ESA Incoming and Outgoing Content Filters - Best Practices

```
-u Make query over UDP (default).  
  
reverse_ip - Reverse lookup IP address.  
dns_ip - Query the DNS server at this IP address.  
esal.unc-hamiltons.com>
```

You can get the MX record for a domain by placing MX in the “qtype” field. Let’s get the MX records for “cisco.com” to test DNS resolution

```
esal.unc-hamiltons.com> dig MX cisco.com  
  
; <<>> DiG 9.8.4-P2 <<>> cisco.com MX  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16692  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;cisco.com. IN MX  
  
;; ANSWER SECTION:  
cisco.com. 21600 IN MX 10 alln-mx-01.cisco.com.  
cisco.com. 21600 IN MX 30 aer-mx-01.cisco.com.  
cisco.com. 21600 IN MX 20 rcdn-mx-01.cisco.com.  
  
;; Query time: 26 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Sun May 10 13:49:15 2015  
;; MSG SIZE rcvd: 107  
  
esal.unc-hamiltons.com>
```

Now test your outbound firewall settings by seeing if you can get a layer-4 socket connection to one of the MTAs specified in the Cisco MX records. Note that once I get connected, I enter the “Control+]” key combination to get to the “telnet” prompt where I can type “quit”.

```
Trying 72.163.7.166...  
Connected to rcdn-mx-01.cisco.com.  
Escape character is '^]'.  
220 rcdn-inbound-1.cisco.com ESMTP  
^]  
telnet> quit  
Connection closed.  
esal.sectest.net>
```

The above test proves we have good Outbound connectivity.

Now do the same test to your Exchange Server’s IP address to test Inbound connectivity.

## STEP 2: ESA - LICENSING

The hardware appliances ship with 30-day evaluation feature keys already installed on the appliance. You simply need to Accept the End-User-License for them to become active. This is covered in the Initial Setup Wizard documentation – next in the series.

## ESA Incoming and Outgoing Content Filters - Best Practices

For the ESAv virtual appliances, they do not ship with any licenses. You will need to work with your Partner or your Cisco Content Security Account Manager (Content SAM) to get an XML license file. Once you have a license file, you will install/load the license file into the virtual appliance as instructed below. We must have a license file to even receiving email and to upgrade the operating system of the appliance. So this is one of the first things we need to do.

An easy way to check the licenses of an appliance is to issue the “showlicense” command:

```
esal.unc-hamiltons.com> showlicense
No License Installed
esal.unc-hamiltons.com>
```

Once you have the XML license file, open in a text editor such as Notepad++ or Wordpad on Windows or Text Wrangler on Mac. **DO NOT USE WINDOWS NOTEPAD** as the formatting from the XML file will be destroyed and will not copy/paste correctly.

Now that the license file is open on your machine, ssh into the appliance and issue the “loadlicense” command:

```
esal.unc-hamiltons.com> loadlicense

1. Paste via CLI
2. Load from file
How would you like to load a license file?
[1]> 1

Paste the license file now.
Press CTRL-D on a blank line when done.
```

Now copy and then paste the entire text contents of the XML file into the screen. Press enter to move to blank line and then press CTRL-D to finish. The EULA will be displayed for your acceptance.

```
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS
VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR
EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU
```

```
<this message is truncated>
```

```
Do you accept the above license agreement? []> Y
The license agreement was accepted.
Virtual License
=====
```

```
Feature keys added
-----
Bounce Verification
Cloudmark Service Provider Edition
File Analysis
```

## ESA Incoming and Outgoing Content Filters - Best Practices

File Reputation  
Incoming Mail Handling  
Intelligent Multi-Scan  
IronPort Anti-Spam  
IronPort Email Encryption  
IronPort Image Analysis  
McAfee  
Outbreak Filters  
RSA Email Data Loss Prevention  
Sophos Anti-Virus

### License data

```
-----  
vln                               VLNESA000130  
begin_date                        Mon Oct 20 16:45:42 2014 GMT  
end_date                          Sat Oct 17 16:45:41 2015 GMT  
company                           Dalton Hamilton  
seats                             25  
serial                            18D9  
email                             dalthami@cisco.com  
issue                             a8d171c232f94a5da725bade5f5837dc4  
license_version                   1.1  
esal.unc-hamiltons.com>
```

Issue the “ipcheck” command and you will see the number of days for each feature key.

```
esal.unc-hamiltons.com> ipcheck
```

```
Ipcheck Rev                       1  
Date                             Sun May 10 14:38:19 2015  
Model                             C300V  
Platform                         vmware (VMware Virtual Platform)  
MGA Version                       Version: 9.1.0-032  
Build Date                       2015-03-17  
Install Date                     2015-05-10 12:56:09  
Burn-in Date                     Unknown  
Serial No.                       564DF56D18E45A4F00DE-xxxxxxxxxx  
BIOS Version                     6.00  
RAID Version                     NA  
RAID Status                      Unknown  
RAID Type                        NA  
RAID Chunk                      Unknown  
BMC Version                      NA  
  
Disk 0                           500GB VMware, VMware Virtual S 1.0 at mpt0 bus 0 scbus2  
Disk Total                       500GB  
  
Root                             400MB 72%  
Nextroot                         400MB 1%  
Var                              400MB 1%  
Log                              407GB 1%  
DB                              12GB 0%  
Swap                             8GB  
Mail Queue                      70GB  
  
RAM Total                       8192M  
  
NIC Management                   00:0c:29:38:ba:b6  
NIC Data 1                      00:0c:29:38:ba:c0  
NIC Data 2                      00:0c:29:38:ba:ca
```

## ESA Incoming and Outgoing Content Filters - Best Practices

```
PS1                Unknown
PS2                Unknown

Key                159day, Bounce Verification
Key                159day, Cloudmark SP
Key                159day, File Analysis
Key                159day, File Reputation
Key                159day, Intelligent Multi-Scan
Key                159day, IronPort Anti-Spam
Key                159day, IronPort Email Encryption
Key                159day, IronPort Image Analysis
Key                159day, McAfee
Key                159day, Outbreak Filters
Key                159day, RSA Email Data Loss Prevention
Key                159day, Sophos
Key                160day, Incoming Mail Handling
esal.unc-hamiltons.com>
```

Note: The "showlicense" will show you the VLN number and the "ipcheck" command will show you the Serial Number.

### STEP 3: ESA - UPGRADING

#### Upgrading the Appliance to the Latest General Deployment (GD) Version

In order to upgrade the ESAv (Virtual Appliances) you must have a valid "License" file loaded into the appliance. The topic immediately before this one discussed how to license the appliance.

Issue the "version" command to see the current version of code the appliance is running.

```
esal.unc-hamiltons.com> version

Current Version
=====
Product: Cisco C300V Email Security Virtual Appliance
Model: C300V
Version: 9.1.0-032
Build Date: 2015-03-17
Install Date: 2015-05-10 12:56:09
Serial #: 564DF56D18E45A4F00DE-BFB8C738BAB6
BIOS: 6.00
CPUs: 4 expected, 4 allocated
Memory: 8192 MB expected, 8192 MB allocated
RAID: NA
RAID Status: Unknown
RAID Type: NA BMC: NA
esal.unc-hamiltons.com>
```

My C300v is currently running AsyncOS version 9.1.0-032.

To see what the current GD version of code is, go to this URL:

<https://supportforums.cisco.com/community/5756/email-security>

## ESA Incoming and Outgoing Content Filters - Best Practices

As of this writing, 13 October 2015, the Current GD version of code is 9.6.0-047

NOTE: My ESAv virtual appliance is part of the ESA "Friendlies" program and can see "Early Release" versions of code. Therefore, I will show you how to do an upgrade but I will be upgrading to "Early Release" code.

Below I will issue the "upgrade" command and note that there are two options:

```
DOWNLOADINSTALL
DOWNLOAD
```

I suggest highly that you do a DOWNLOAD instead of DOWNLOADINSTALL because the DOWNLOAD will download the new AsyncOS operating system without the need for the Admin to reply to a system prompt to reboot as with the DOWNLOADINSTALL. If you issue DOWNLOADINSTALL, it will download the image and prompt you to reboot the appliance. If you do not reply before the "timeout" (because you're off doing other things), then ssh will timeout and you will have to issue the "upgrade" again and it downloads the new AsyncOS image all over again. Best to do a DOWNLOAD.

When doing the CLI 'upgrade' command, remember that you may need to do multiple upgrades to get to the latest version of code. Do the DOWNLOAD, once the new version is available, the INSTALL command will appear. Do the INSTALL and it will prompt you to reboot. Once the appliance is back online, login to the appliance again and try another 'upgrade' to see if there is another upgrade available.

```
esal.unc-hamiltons.com> upgrade
```

```
Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
[1]> DOWNLOAD
```

```
Upgrades available.
1. AsyncOS 9.5.0 build 035 upgrade For Email, 2015-04-04
2. AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22
[2]> 2
```

```
Download of AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22 has started in
background.
```

```
Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
- DOWNLOADSTATUS - Shows the download status
- CANCELDOWNLOAD - Cancel ongoing download(AsyncOS 9.5.0 build 067 upgrade For
Email, 2015-04-22).
[1]> <I typed return key here>
```

```
which took me to the prompt again
```

## ESA Incoming and Outgoing Content Filters - Best Practices

```
esal.unc-hamiltons.com> upgrade
```

```
Choose the operation you want to perform:
```

- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
  - DOWNLOAD - Downloads the upgrade image.
  - DOWNLOADSTATUS - Shows the download status
  - CANCELDOWNLOAD - Cancel ongoing download(AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22).
- ```
[ ]> DOWNLOADSTATUS
```

```
Download of upgrade image (AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22) is in progress (71% complete).
```

```
Choose the operation you want to perform:
```

- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
  - DOWNLOAD - Downloads the upgrade image.
  - DOWNLOADSTATUS - Shows the download status
  - CANCELDOWNLOAD - Cancel ongoing download(AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22).
- ```
[ ]>
```

```
esal.unc-hamiltons.com> upgrade
```

```
Choose the operation you want to perform:
```

- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
  - DOWNLOAD - Downloads the upgrade image.
  - INSTALL - AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22 (needs reboot).
  - DELETE - Delete downloaded image(AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22).
- ```
[ ]> install
```

```
Current downloaded version is AsyncOS 9.5.0 build 067 upgrade For Email, 2015-04-22.
```

```
Do you want to install it ? [Y]>
```

```
Would you like to save the current configuration to the configuration directory before upgrading? [Y]>
```

```
Would you like to email the current configuration before upgrading? [N]>
```

```
Choose the password option:
```

1. Mask passwords (Files with masked passwords cannot be loaded using loadconfig command)
  2. Encrypt passwords
  3. Plain passwords
- ```
[1]>
```

```
Performing an upgrade may require a reboot of the system after the upgrade is applied. You may log in again after this is done.
```

```
Do you wish to proceed with the upgrade? [Y]>
```

```
Preserving configuration ...
```

```
Finished preserving configuration
```

```
Cisco IronPort Email Security Appliance(tm) Upgrade
```

```
Finding partitions... done.
```

```
Setting next boot partition to current partition as a precaution... done.
```

```
Erasing new boot partition... done.
```

```
Extracting repengroot done.
```

```
Extracting eapp done.
```

```
Extracting scannerroot done.
```

```
Extracting splunkroot done.
```

## ESA Incoming and Outgoing Content Filters - Best Practices

```
Extracting bmroot done.
Extracting savroot done.
Extracting ipasroot done.
Extracting ecroot done.
Extracting distroot done.
Configuring AsyncOS disk partitions... done.
Configuring AsyncOS user passwords... done.
Configuring AsyncOS network interfaces... done.
Configuring AsyncOS timezone... done.
Moving new directories across partitions... done.
Syncing... done.
Reinstalling boot blocks... done.
Will now boot off new boot partition... done.

Upgrade complete. It will be in effect after this mandatory reboot.

Reboot takes about 20 minutes to complete. Do not interrupt power to the
appliance during this time.
Enter the number of seconds to wait before forcibly closing connections.
[30]> 2

System rebooting. Please wait while the queue is being closed..

Closing CLI connection.
Rebooting the system...
```

### **NEXT STEPS AND SUMMARY**

At this point you have setup your ESA appliance with the correct IP address, Subnet Mask, DNS Settings, Default Route, and we've discussed Firewall settings. You have also insured your Virtual Appliance has a license file — Hardware Appliances ship with 30 day Eval keys — which is required to do an upgrade. You have then upgraded the appliance to the current General Deployment (GD) version as discussed in the previous section.

You are now ready to run the Initial Setup Wizard which is covered in the next document in the series.