

# **ESA and SMA Installation and Best Practices Guide**

**September 2015**  
**Version 1.1**



Dalton Hamilton  
Cisco Sales Engineer

THE MOST RECENT VERSION OF THIS DOCUMENT CAN BE FOUND HERE:

<https://cisco.com/go/emailsecurity-customer>

# ESA/SMA INSTALLATION AND BEST PRACTICES

<b>THE MOST RECENT VERSION OF THIS DOCUMENT CAN BE FOUND HERE:</b>	<b>1</b>
<b>A. PRE-INSTALL DEPLOYMENT ARCHITECTURE</b>	<b>5</b>
<b>1. Initial Data Collection</b> .....	<b>5</b>
<b>2. Deployment Options - Network Architecture</b> .....	<b>6</b>
Deployment Option 1: .....	7
Deployment Option 2: .....	9
Deployment Option 3: .....	10
Deployment Option 4: .....	11
<b>3. Firewall Ports and Protocols Flow</b> .....	<b>12</b>
<b>B. PRE-INSTALL SIZING THE ESA</b>	<b>14</b>
<b>C. ESA: INITIAL INSTALLATION, LICENSING, AND UPGRADING</b>	<b>15</b>
<b>1. Setting up the IP Interface</b> .....	<b>16</b>
<b>2. Set the System Hostname</b> .....	<b>17</b>
<b>3. Set the Default Route</b> .....	<b>18</b>
<b>4. Setup DNS Resolution</b> .....	<b>18</b>
<b>5. Testing</b> .....	<b>20</b>
<b>6. Licensing</b> .....	<b>21</b>
<b>7. Upgrading the Appliance to the Latest General Deployment (GD) Version</b> .....	<b>23</b>
<b>8. Running the Initial Setup Wizard</b> .....	<b>26</b>
<b>D. SMA: INITIAL INSTALLATION, LICENSING, AND UPGRADING</b>	<b>31</b>
<b>E. SMA: BEST PRACTICES</b>	<b>32</b>
<b>1. Changing the webUI Default Login Timeout</b> .....	<b>33</b>
<b>2. LDAP</b> .....	<b>33</b>
<b>3. Disk Management</b> .....	<b>35</b>
<b>4. Enable Centralized Spam Quarantine</b> .....	<b>36</b>
<b>5. Enable Centralized Policy, Virus, and Outbreak Quarantines</b> .....	<b>39</b>
<b>6. Enable Centralized Reporting</b> .....	<b>41</b>
<b>7. Enable Centralized Message Tracking</b> .....	<b>41</b>
<b>F. ESA: BEST PRACTICES</b>	<b>42</b>
<b>1. System Administration and Network</b> .....	<b>42</b>
a) LDAP .....	42

# ESA/SMA INSTALLATION AND BEST PRACTICES

b)	System Administration > Alerts	43
c)	System Administration > Log Subscription	43
d)	System Administration > Return Address	44
e)	Set the timeout for GUI and CLI	44
f)	Network > IP Interfaces	44
g)	Network > Listeners	45
h)	Network > DNS	46
i)	Network > Incoming Relays	46
<b>2.</b>	<b>Security Services</b>	<b>47</b>
a)	Enable Anti-Spam	47
b)	Enable Graymail and Safe Unsubscribing	48
c)	Enable both AV Signature Engines: Sophos and McAfee	51
d)	Enable Advanced Malware Protection File Reputation and Analysis	51
e)	Enable DLP for outbound DLP Scanning	52
f)	Enable URL Intelligence/Filtering and Web Interaction Tracking (Click-Tracking)	53
g)	Customize the Block Page Data	53
h)	Enable Cisco IronPort Email Encryption	53
i)	Enable Cisco Outbreak Filters and Web Interaction Tracking for Outbreak Rewrites	55
j)	Ensure SenderBase is Enabled	56
k)	Enable Centralized Reporting	56
l)	Enable Centralized Message Tracking	56
m)	Enable Policy Virus and Outbreak Quarantines	56
n)	Enable External Spam Quarantine	57
<b>3.</b>	<b>Connecting the ESA and SMA</b>	<b>57</b>
<b>4.</b>	<b>Message Filters</b>	<b>58</b>
	Best Practices Message Filters:	58
	Optional Message Filters:	59
<b>5.</b>	<b>Connection-Level Settings</b>	<b>62</b>
	Modifications to the Mail Flow Policy table:	63
	HAT Table Changes: Go back to HAT Overview	69
<b>6.</b>	<b>Bounce Verification and Destination Controls</b>	<b>72</b>
<b>7.</b>	<b>Incoming Mail Policies</b>	<b>75</b>
	Anti-Spam	76
	Anti-Virus	77
	Advanced Malware Protection	78
	Graymail and Safe Unsubscribe	78
	Incoming Content Filters	82
	DKIM Protection for Hardfail	90
	Domain Spoof Protection	91
	DMARC Verification and Protection	93
	Outbreak Filters	94
	Mail Policies based on AD/LDAP Group	95
<b>8.</b>	<b>Outgoing Mail Policies</b>	<b>98</b>
	Anti-Spam	98
	Anti-Virus	98
	Outgoing Content Filters	101
	Graymail	104
	Outbreak Filters	104

# ESA/SMA INSTALLATION AND BEST PRACTICES

DLP .....	104
<b>G. MULTIPLE ESA APPLIANCES</b>	<b>110</b>
<b>Configuring additional ESA appliances</b> .....	<b>110</b>
<b>Creating and Joining a Cluster</b> .....	<b>111</b>
Step 1: Create the cluster .....	112
Step 2: Joining a new ESA to the already created cluster. ....	113
<b>Remove the Mode — Machine: PVO Settings</b> .....	<b>117</b>
<b>Different Cluster Groups to Differentiate DNS Config for two Data Centers</b> .....	<b>119</b>
<b>H. CENTRALIZED EMAIL REPORTING REPORTING GROUPS</b>	<b>123</b>
<b>What is Centralized Reporting Groups</b> .....	<b>123</b>
<b>Creating Centralized Reporting Groups</b> .....	<b>123</b>
<b>CONCLUSION</b>	<b>125</b>

## A. PRE-INSTALL DEPLOYMENT ARCHITECTURE

### 1. Initial Data Collection

Initial steps for any deployment will involve a meeting to discuss these questions:

- A. What features do you want for Inbound and Outbound Mail Flow?
- B. What is the Peak mail flow volume in “Messages Per Hour” if possible. This is needed to properly size the appliances.
- C. How many locations does the customer want to deploy Email Appliances? Some customers have a single Data Center and some have a Primary and a Backup Data Center. Some customers want both the Primary and Backup locations to be able to handle 100% of the Peak mail flow volume. Some customers only want the backup Data Center to be able to handle 50% load. Some customers want the Primary Data Center to receive all email in a normal “UP” and the have the Backup Data Center ESAs configured with their “Listeners” suspended (not accepting email) and if there is a problem with the Primary, then they enable the backup. There are many different scenarios that work and customers have their reasons for choosing one over the other. In an ideal world, we would have a Primary and Backup Data Center. Each Data Center being able to handle the full load of peak email flow and being Active/Active all the time.
- D. Once you’ve chosen a Deployment Option, you will need to start documenting:
  - i. Static IP addresses for each appliance
  - ii. Subnet Mask for each IP Address
  - iii. Default route
  - iv. Understand the DNS method to use. The ESAs heavily uses DNS queries and this should be considered when designing the deployment. You can point the ESAs to the Internal DNS servers or you can configure the ESAs to use “Split DNS” where they send queries to designated local Internal DNS for local Domain names and use the Root DNS servers for all external Domains. This puts less burden on the local DNS servers.
  - v. Add hostnames to the DNS servers - Create an A Record and a PTR Record for each IP address. Determine a hostname for each ESA and SMA appliance. Typically a hostname of “[esa1.example.com](#)”, “[esa2.example.com](#)”, etc are used for ESA and

## ESA/SMA INSTALLATION AND BEST PRACTICES

“[sma1.example.com](http://sma1.example.com)” is used for the SMA. Once you have the hostnames, add A Records and PTR Records to your DNS servers.

The below deployment scenarios gives four examples of “Cisco Recommended” designs for just a single Data Center yet it works just for scenarios where multiple Data Centers are in play.

### 2. Deployment Options - Network Architecture

A few “NOTES” before we start discussing each Deployment option.

Note 1:

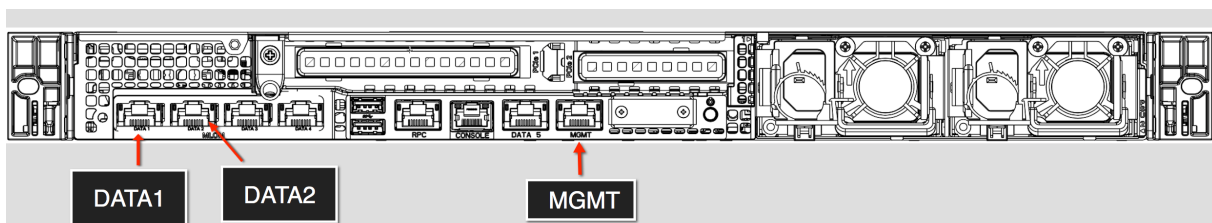
For the purposes of this document, I will refer to “Ethernet Port” when referring to the physical RJ45 jack on the appliance. I will use the term “Interface” to mean the software interface configured to run on a physical Ethernet Port. Example Ethernet Port “Data1” can have multiple “Interfaces” configured on it.

Note 2:

ESA Hardware Appliances:

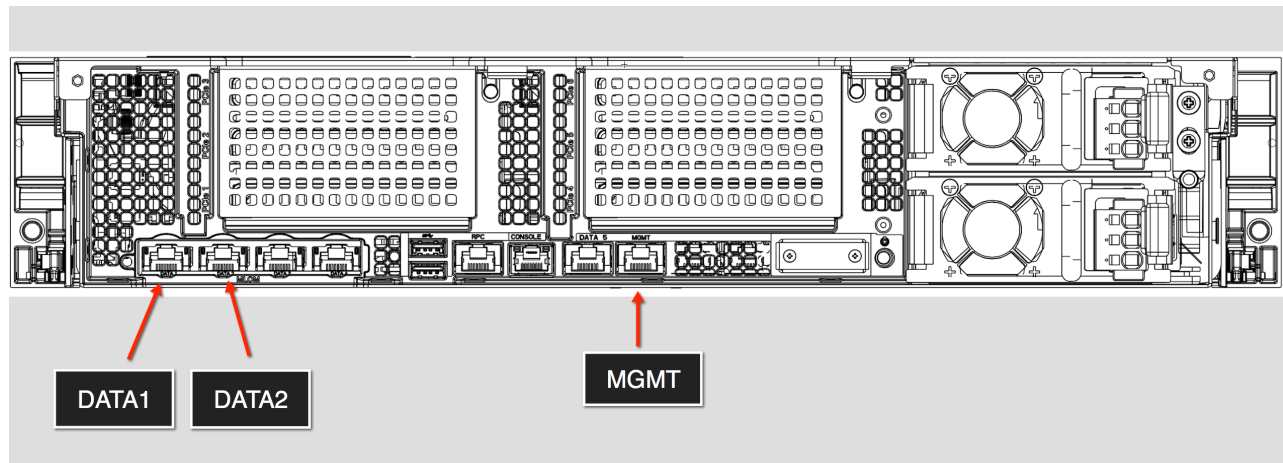
The ESA C380, C680 and C690 are 2U appliances. The C390 is a 1U appliance. There are three relevant GigE Ethernet ports — MGMT (Management), Data1, and Data2.

Here is a drawing of a C390



Here is a drawing of a C690 and M690

## ESA/SMA INSTALLATION AND BEST PRACTICES



Ignore the other physical Ethernet Ports as they cannot be used on the ESA or SMA.

All three interfaces can be used to send and receive email but we have seen that most deployments are setup with a “single-arm” configuration— i.e. only the Management (MGMT) physical Ethernet port connected. With that configuration, all email and management packets traverse the MGMT GigE port. This is more than enough bandwidth — so you don’t need to implement Data1 and/or Data2 in order to provide more bandwidth to the appliance.

Multiple Ethernet Ports can be joined using our “NIC Pairing” feature through the CLI ‘etherconfig’ > ‘pairing’ command but very few customers do this.

The Hardware ESA appliance ships with a default IP address of 192.168.42.42/24 on the Management (MGMT) Ethernet Port.

### ESA Virtual Appliances:

The ESAv Virtual appliances will use DHCP and obtain an IP address, Subnet Mask, Default Route, and DNS server. To figure out what the IP address is, you can easily get on the Console of the Virtual Appliance and login “admin/ironport” and issue the “interfaceconfig” command. Control-C gets you out of the command and back to the prompt.

Ports and Protocols: Firewall Ports and Protocols flow table can be found immediately following Deployment Option 4.

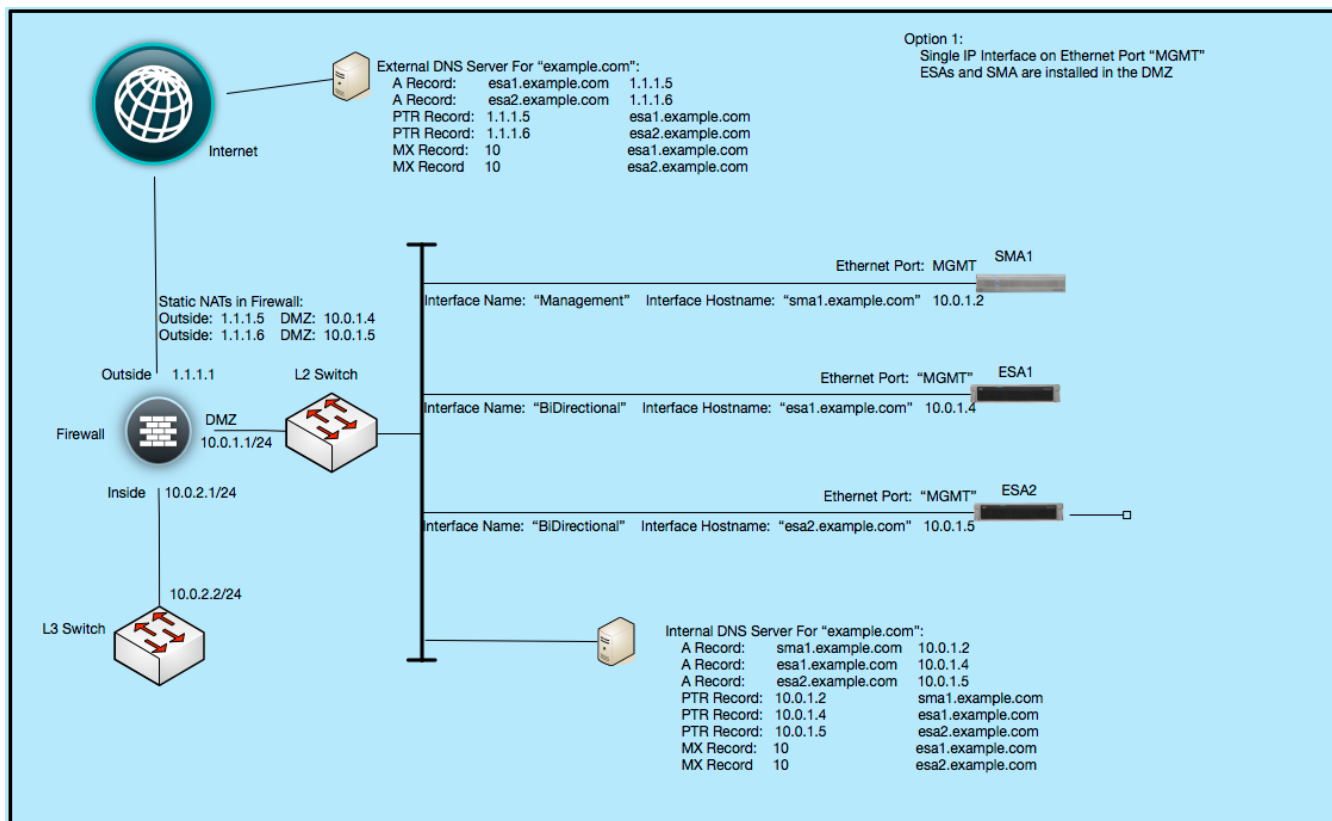
### Deployment Option 1:

## ESA/SMA INSTALLATION AND BEST PRACTICES

All ESAs and the SMA are placed on the DMZ. If the SMA were placed “Inside” the stateful firewall then we would need to open various ports to allow the ESA and SMAs to communicate with each other.

For this option the ESAs are deployed with the “MGMT” Ethernet Ports connected to DMZ and a single IP Interface (named “BiDirectional”) configured on that MGMT Ethernet Port.

In this example, the “BiDirectional” interface will both receive email off the Internet and Send outbound email. It is also used for Management traffic (SSH/HTTP/HTTPS).





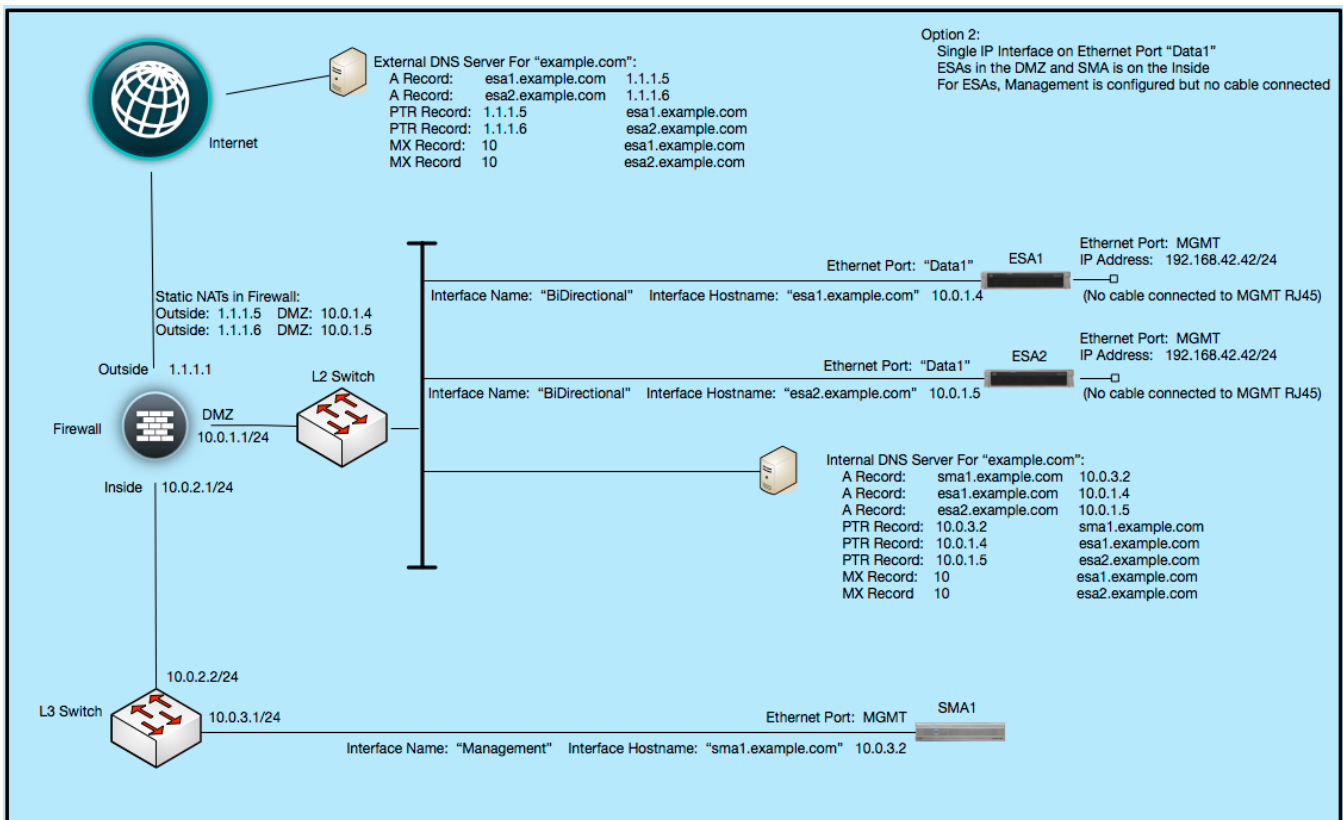
# ESA/SMA INSTALLATION AND BEST PRACTICES

## Deployment Option 2:

The example shows that we are using Data1 Ethernet Port for processing Email and Managing the appliance as it connects to the DMZ network. Note the ESAs have no Ethernet cable connected to the MGMT Ethernet Port. The MGMT Ethernet Port is still configured with an IP Interface named "Management" configured for 192.168.42.42/24. This way, if you are in the DataCenter and need to connect to any ESA directly, you know the MGMT port is configured for 192.168.42.42 and you can set your laptop to 192.168.42.41/24 (for example) and connect to the ESA directly.

The SMA is also placed on the "Inside" of the firewall in this example.

Because the ESA and SMA are separated by a Firewall, you will need to ensure all the needed ACLs are in place to allow proper communication between the SMA and ESAs for all functionality. Refer to the Firewall Ports and Protocols Flow table immediately following Option 4.

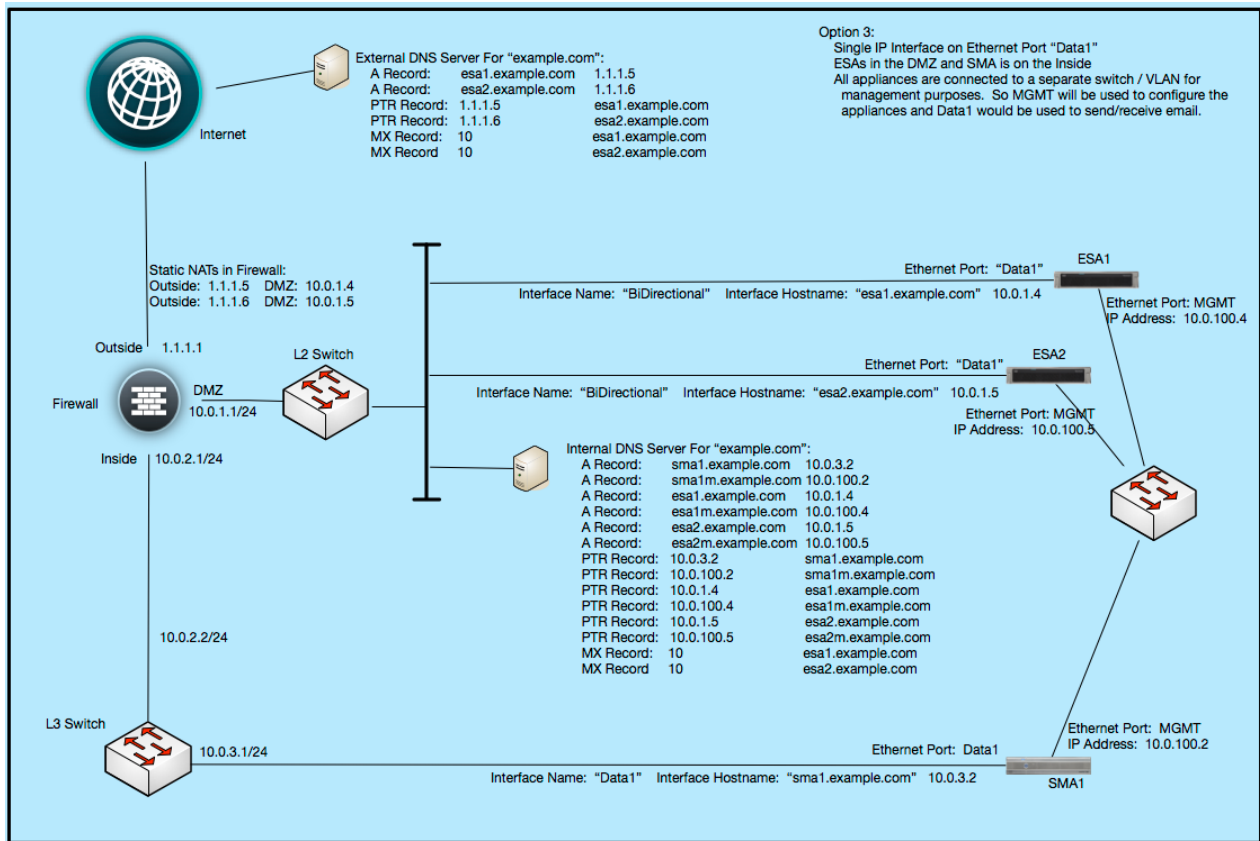


# ESA/SMA INSTALLATION AND BEST PRACTICES

## Deployment Option 3:

Some customers will have a separate “Management VLAN” and they prefer the MGMT (Management) Ethernet Port on the appliance handles only Management (Configuration and Reporting) traffic and Data1 handle the mail flow. In this example it shows that MGMT is now connected to a switch that handles the Management VLAN for the customer and MGMT will only be used for configuration and reporting purposes.

As with Deployment Option 2, because the ESA and SMA are separated by a Firewall, you will need to ensure all the needed ACLs are in place to allow proper communication between the SMA and ESAs for all functionality. Refer to the Firewall Ports and Protocols Flow table immediately following Option 4.

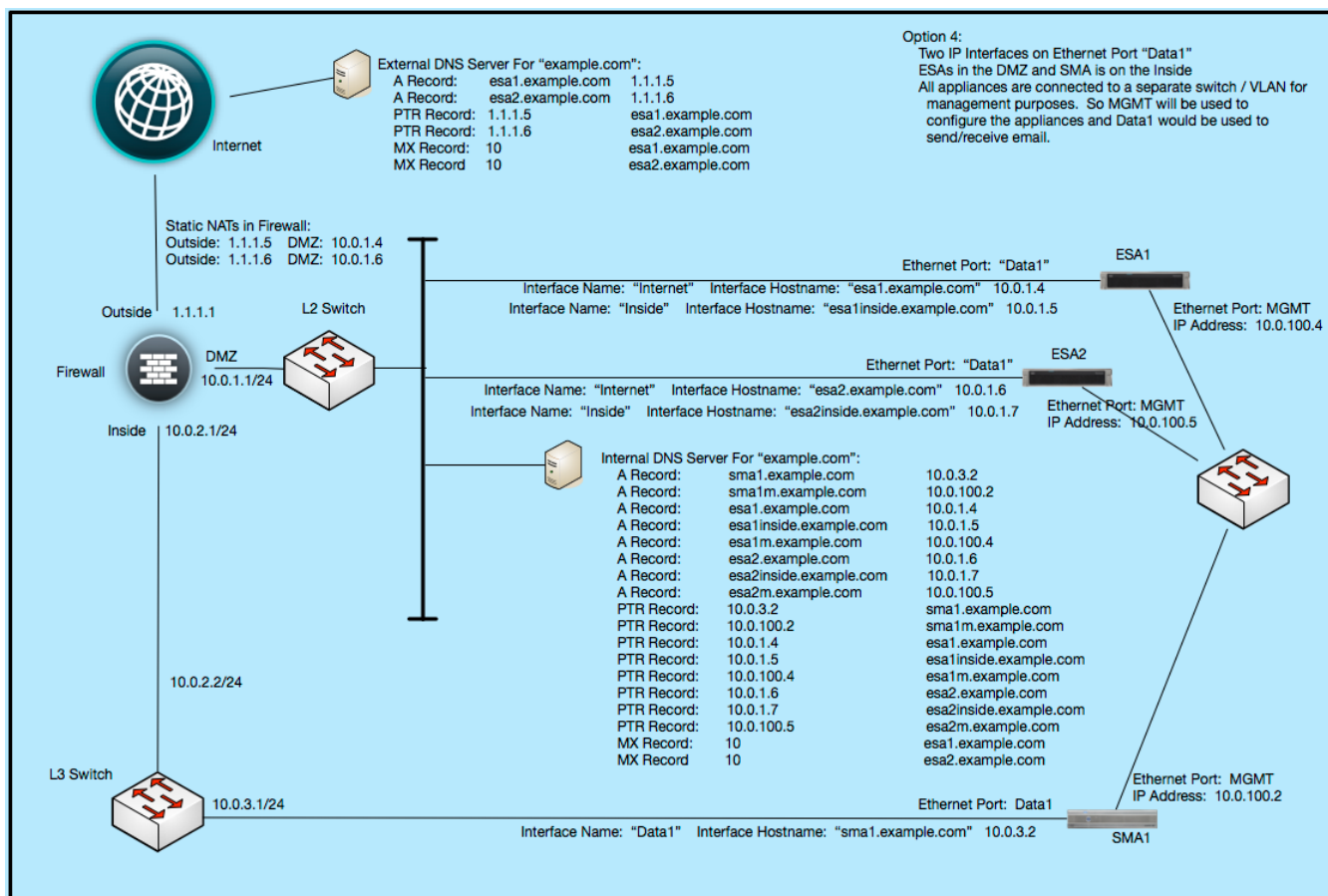


## ESA/SMA INSTALLATION AND BEST PRACTICES

### Deployment Option 4:

This option is similar to Option 3 with the addition of a second IP Interface on the ESAs. Some customers like to have two different IP addresses and two different “Listeners”. This is not a very typical deployment method but it is requested sometimes. There is nothing wrong with this method and it is a “Recommended” deployment design when the customer wants one IP Interface to handle “Incoming” mail and a separate IP Interface to handle Outbound mail. By doing this, it also creates a separate “HAT” (Host Access Table) to further segment the two types of mail flow. The HAT tables are per “Listener”. A Listener is the “process” that binds to port TCP/25 and handles mail flow. So it is the process that handles the EHLO conversion.

As with Deployment Option 2 and 3, because the ESA and SMA are separated by a Firewall, you will need to ensure all the needed ACLs are in place to allow proper communication between the SMA and ESAs for all functionality. Refer to the Firewall Ports and Protocols Flow table immediately after this option.



## ESA/SMA INSTALLATION AND BEST PRACTICES

### 3. Firewall Ports and Protocols Flow

Flow Direction	(Application) Protocol/ Port	Comments
From ANY To ESA	(SMTP) TCP/25	So that Inbound email can be delivered
From ESA To ANY	(SMTP) TCP/25	So that Outbound email can be delivered
From ESA To Exchange Servers	(SMTP) TCP/25  (LDAP) TCP/389, or TCP/3268 (for Active Directory)  (LDAPS) TCP/636 or TCP/3269 (for Active Directory)	<ul style="list-style-type: none"> <li>● To deliver Inbound email to the Exchange servers</li> <li>● If you are creating policy based on LDAP Group or using Recipient Validation using LDAP, then the ESAs will need to connect back to your LDAP servers</li> </ul>
From SMA To Exchange Servers	(LDAP) TCP/389, or TCP/3268 (for Active Directory)  (LDAPS) TCP/636 or TCP/3269 (for Active Directory)	In this document we centralize the Spam quarantine to the SMA (instead of having a Spam quarantine on every ESA). This document also recommends NOT enabling Authentication and explains why. However, if you choose to use LDAP Auth for end-user access to the Spam Quarantine, you'll need this port open.
From Exchange Servers To ESA	(SMTP) TCP/25	Exchange servers sending Outbound email through the ESA appliances
From ESA To SMA	(SPAM) TCP/6025  (Policy Quarantines) TCP/7025	<ul style="list-style-type: none"> <li>● The SPAM Quarantine is centralized on the SMA appliance and the ESA delivers this SPAM using TCP/6025.</li> <li>● All other quarantines are also centralized on the SMA and the ESA delivers to those quarantines on a single port (TCP/7025).</li> </ul>

## ESA/SMA INSTALLATION AND BEST PRACTICES

Flow Direction	(Application) Protocol/ Port	Comments
From SMA To ESA	(Reporting/Tracking)TCP/22  (SMTP) TCP/25	The SMA connects to the ESA appliances to pull down Reporting and Message tracking When the SMA needs to send an outbound email, it should always send it through the ESA. When an email is “Released” from the Spam Quarantine, it should go back through the ESA to be scanned again with the latest Virus rules.
From ESA and SMA To Internal DNS Servers	(DNS) UDP and TCP / 53	Used when the ESAs and/or SMA are pointing to the Internal DNS server or setup for Split DNS.
From ESA and SMA To ANY (Internet DNS Servers)	(DNS) UDP and TCP / 53	Used when the ESAs and/or SMA are pointing to an external DNS server or are configured for Split DNS,
From ESA and SMA To NTP Time Server	(NTP) UDP/123	Allow NTP time SYNC to whatever time server you are using.
From ESA and SMA To ANY	(HTTP and HTTPS) TCP/80 and TCP/443	The ESA and SMA need to be able to pull down signature updates from our cloud.
From ESA To ANY (For AMP File Reputation)	(AMP File Reputation) TCP/32137 You can optionally configure the ESAs to use TCP/443	This allows the ESA appliances to query the SourceFire AMP File Reputation cloud to obtain the File Reputation of an Attachment. Only needed if you have an AMP Feature License and have it configured.
From (Your Company Email Admins — or your Internal Subnet)  To: ESA and SMA	TCP/80 TCP/443 TCP/22 TCP/21	<ul style="list-style-type: none"> <li>● The Admin will be managing the ESA and SMA appliances on port 80 and/or 443. H</li> <li>● e may also want to ssh into the appliance for CLI related commands or real-time log monitoring.</li> <li>● FTP (21) is useful when getting log files or getting or putting other configuration related files. The ESA can even archive malware and allow the Admin to FTP the files off the appliance if desired.</li> </ul>

## ESA/SMA INSTALLATION AND BEST PRACTICES

Flow Direction	(Application) Protocol/ Port	Comments
From ESA To ESA	TCP/22	“Clustering” is a built-in technology on the ESA appliances that allows all the ESA to talk to each other and form a “Cluster” and keep their Configuration in SYNC. The SMA does not use Clustering and plays no role in the ESA “Configuration”. The Clustering technology uses TCP/ 22.
From Internal LAN To ESA	TCP/6080 or TCP/6443 (SSL)	The new ESA RESTAPI uses TCP/6080 or securely TCP/6443. If you plan to write applications/ scripts to Poll reporting metrics using this RESTAPI, then you will need to allow these ports to reach the ESA from the desktop/ workstation you use to run the scripts.

### **B. PRE-INSTALL SIZING THE ESA**

Sizing is an important exercise to ensure your ESA and SMA appliances perform perfectly in your environment. We size the ESA appliance to handle the peak message flow. It is best to get the peak messages-per-hour (MPH) for the customer traffic and from there we can determine what type of appliance is needed and how many of them.

As you step through this guide you will realize the many different features available on the Cisco ESA appliance. The number of messages-per-hour an ESA can handle will depend on which features are running on your appliance and which type of appliance you have. It is therefore best to work with a pre-sales Cisco Content Security CSE or your Cisco Partner to properly size the appliance.

### C. ESA: INITIAL INSTALLATION, LICENSING, AND UPGRADING

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 — MacBook Pro 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 a M300v SMAv appliance for the purposes of this document.

- We will be using Deployment Option 1 (as explained in Section A) — 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](http://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.
- For the SMAv, I will have a single IP Interface named “Management” and an IP address of 10.0.1.36/24. The Interface hostname will be [sma1.unc-hamiltons.com](http://sma1.unc-hamiltons.com).
- 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. Discuss licensing
7. Upgrade the Appliance to the latest General Deployment (GD) version code
8. Running 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

## ESA/SMA INSTALLATION AND BEST PRACTICES

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.

```
Dalton's-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

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]> esa1.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
```



## ESA/SMA INSTALLATION AND BEST PRACTICES

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>

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 secure service? [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
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

### 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>
```

### 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
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

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.

[1]> 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]>

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.

[1]>

ironport.example.com>

Commit the changes.

ironport.example.com> commit

Please enter some comments describing your changes:

[1]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Sun May 10 13:05:31 2015 GMT

esa1.unc-hamiltons.com>

## ESA/SMA INSTALLATION AND BEST PRACTICES

### 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):

```
esa1.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.

-u Make query over UDP (default).

reverse\_ip - Reverse lookup IP address.

dns\_ip - Query the DNS server at this IP address.

```
esa1.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](http://cisco.com)" to test DNS resolution.

```
esa1.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

esa1.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".

## ESA/SMA INSTALLATION AND BEST PRACTICES

```
esa1.sectest.net> telnet rcdn-mx-01.cisco.com 25
```

```
Trying 72.163.7.166...
Connected to rcdn-mx-01.cisco.com.
Escape character is '^]'.
220 rcdn-inbound-l.cisco.com ESMTP
^]
telnet> quit
Connection closed.
esa1.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.

### 6. 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. We will do that later — right before we run the Startup Wizard.

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:

```
esa1.unc-hamiltons.com> showlicense
```

```
No License Installed
```

```
esa1.unc-hamiltons.com>
```

Once you have the XML license file, you FTP it to the appliance and put it into the configuration directory.

```
Daltons-Mac-Pro:~ dalton$ ftp esa1.unc-hamiltons.com
Connected to esa1.unc-hamiltons.com.
220 esa1.unc-hamiltons.com Cisco FTP server (V9.1.0) ready
Name (esa1.unc-hamiltons.com:dalton): admin
331 Password required.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd configuration
250 CWD command successful.
ftp> bin
200 Type set to Binary.
ftp> put /Users/dalton/Desktop/license0ct2015.xml license0ct2015.xml
local: /Users/dalton/Desktop/license0ct2015.xml remote: license0ct2015.xml
227 Entering Passive Mode (10,0,1,32,22,99)
150 Opening Binary connection for license0ct2015.xml
100% |*****| 7643 18.45 MiB/s 00:00 ETA
226 Transfer Complete
7643 bytes sent in 00:00 (4.70 MiB/s)
ftp> quit
221 Goodbye.
Daltons-Mac-Pro:~ dalton$
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

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

```
esa1.unc-hamiltons.com> loadlicense

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

Enter the name of the file in /configuration to import:
[license.xml]> license0ct2015.xml

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
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
esa1.unc-hamiltons.com>
```

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

```
esa1.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
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

```
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

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
esa1.unc-hamiltons.com>
```

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

### 7. 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.

```
esa1.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
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

```
RAID Status: Unknown
RAID Type: NA
BMC: NA
esa1.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>

As of this writing, 24 Oct 2015, the Current GD version of code is 9.6.0-051

**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.

```
esa1.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).
```



## ESA/SMA INSTALLATION AND BEST PRACTICES

```
- 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).
[ ]> <I typed return key here>
```

which took me to the prompt again

```
esa1.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).
[ ]>
```

```
esa1.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 scanerroot done.
Extracting splunkroot done.
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.
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

```
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...
```

```
Connection to 10.0.1.37 closed.  
Daltons-Mac-Pro:~ dalton$
```

### 8. Running the Initial Setup Wizard

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.

We will discuss the Licenses for Hardware appliances in this section.

Login to the ESA webUI via <https://<your-esa-IP>>  
The default username/password is admin/ironport

Check the Feature Keys:

*System Administration > Feature Keys*

Click the “Check for New Keys” button. If you see any keys in the “Pending Activation” section, activate them now. All keys should be in top table — above the “Pending Activation” section.

Once all the Feature Keys are Activated, Go to:

*System Administration > System Setup Wizard*

The wizard will step you through three config panels and a review. Below are examples of how these should be setup.

**NOTE:** When you run the Wizard the first time it creates the initial configuration. If you run the Wizard a second time, it factory defaults the appliance's configuration “except” the network settings. So you can run the Wizard a second time without losing network connectivity.

System Settings:

|          |                  |            |             |           |
|----------|------------------|------------|-------------|-----------|
| 1. Start | <b>2. System</b> | 3. Network | 4. Security | 5. Review |
|----------|------------------|------------|-------------|-----------|

**System Configuration**

Before you enter your System and Network settings:

- Choose a configuration that best matches your network infrastructure
- Determine network and IP address assignments
- Gather information about your system setup

| System Settings                   |                                                                                                                                                                                                                                                                                       |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default System Hostname: ?        | esa1.unc-hamiltons.com<br><small>example: ironport-C300V.example.com</small>                                                                                                                                                                                                          |
| Email System Alerts To:           | dalton@unc-hamiltons.com<br><small>example: admin@company.com</small>                                                                                                                                                                                                                 |
| Deliver Scheduled Reports To:     | dalton@unc-hamiltons.com<br><small>example: admin@company.com. Leave blank to only archive reports on-box.</small>                                                                                                                                                                    |
| Time Zone:                        | Region: <input type="text" value="America"/><br>Country: <input type="text" value="United States"/><br>Time Zone / GMT Offset: <input type="text" value="Central Time (Chicago)"/>                                                                                                    |
| NTP Server:                       | time.unc-hamiltons.com                                                                                                                                                                                                                                                                |
| Administrator Password:           | <input type="radio"/> Generate a password:<br><input type="text"/> <input type="button" value="Generate"/><br><input checked="" type="radio"/> Enter a password of your choice<br>Password: <input type="text" value="*****"/><br>Retype Password: <input type="text" value="*****"/> |
| SenderBase Network Participation: | <input checked="" type="checkbox"/> Allow Cisco IronPort to gather and report limited data on email to SenderBase in order to identify and stop email-based threats. Learn what information is shared...                                                                              |
| AutoSupport: ?                    | <input checked="" type="checkbox"/> Send system alerts and weekly status reports to Cisco IronPort Customer Support                                                                                                                                                                   |

Cancel Next »

Network Settings:

I have checked the “Accept Incoming Mail” and also checked the “Relay Outgoing Mail” switches. If your ESA is going to process both inbound email from the Internet coming in to your company, then the “Accept Incoming Mail” switch should be checked. If your ESA is going to process outbound email to the Internet, then the second switch must be checked.

Incoming Mail:

The Incoming Mail section gives you a chance to add as many of your domains as you would like. If you have multiple Exchange servers then you can add multiple entries for a single domain and the ESA will load-balance the incoming email across those servers. Likewise, if you have multiple domains, then add as many domains as you would like. It is *\*not\** required that you add all your domains from the wizard since you can add domains and servers from the regular webUI once you’re finished with the wizard. The domains that you enter here are considered “Local” domains to the ESA and this lets the ESA know what emails can be

## ESA/SMA INSTALLATION AND BEST PRACTICES

Accepted from Internet Senders/MTAs. These domains will be added the RAT (Recipient Address Table) and to the SMTP Routes table. If the ESA receives an email from a Sending MTA that has a recipient to that is not one of these domains, then the email will be Rejected — unless the Sender/MTA is listed in the “Relay Outgoing Mail” section discussed next.

### Relay Outgoing Mail:

This section gives you the ability to add Senders/MTAs that you allow to send email to ANY domain — i.e. RELAY email. This is normally your Exchange Server(s) IP addresses or subnet.

**Note:** if you see a little circle with a ? (question mark), click that button to see all the available input options/formats that are acceptable input for that specific feature/section.

### Security Settings:

SenderBase Reputation Score (SBRS) is one of the Cisco ESA’s primary features for stopping SPAM and Threat email. Other engines within the appliance also reference the SBRS score. you should always check the “Enable SenderBase Reputation Filtering”.

If you are licensed for multiple SPAM engines, choose the engine you want to use. In the example below, my appliances is licensed for:

- IPAS (IronPort Anti-SPAM)
- IMS (Intelligent Multi-Scan)
- Cloudmark ISP Service Provider

IMS is a bundle engine that runs two SPAM engines internally — it runs both the IPAS engine and the Cloudmark engine. If you have a feature key for IMS and enable it, you will only see the term Intelligent Multi-Scan (or IMS) and not IPAS or Cloudmark but you will know that behind the scenes, IMS is running both engines. The email is first processed by IMS and the bundle of data and a score is passed to IPAS and IPAS consumes Cloudmark’s data and score and uses it’s own SPAM logic and computes the final verdict.

For signature-based AV scanning, you can use both Sophos and McAfee. The Wizard only lets you choose a single AV engine and then we can enable the second engine after we have completed the Wizard. For now, choose Sophos.

The wizard will also show you the option for enabling Advanced Malware Protection. This provides File Reputation checking, File Analysis (Sandboxing with Cisco ThreatGrid), and even provides retrospective Alerts and Reporting which, in the case that at time zero the attachment was not known and ThreatGrid Sandbox did not return a verdict in time and the file

# ESA/SMA INSTALLATION AND BEST PRACTICES

was delivered yet later found to be malicious, this retrospective “Verdict Updates” alerts provides critical details on the emails that were delivered.

|          |           |            |                    |           |
|----------|-----------|------------|--------------------|-----------|
| 1. Start | 2. System | 3. Network | <b>4. Security</b> | 5. Review |
|----------|-----------|------------|--------------------|-----------|

### Message Security

Your Cisco IronPort appliance uses message security to protect your email infrastructure from security threats. The security solutions are applied in the order depicted below. Each module reduces the overall volume of email sent to your infrastructure.

| Anti-Spam                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SenderBase Reputation Filtering</b> | <p><i>SenderBase Reputation Filtering provides a "first line of defense" against incoming spam by restricting access to your email infrastructure based on senders' trustworthiness as determined by their SenderBase Reputation Score (SBR5). More about SBR5...</i></p> <p><input checked="" type="checkbox"/> Enable SenderBase Reputation Filtering</p>                                                                                                                                                                                                                      |
| <b>Anti-Spam Scanning</b>              | <p>Select the anti-spam engine to use for the default incoming mail policy:</p> <p> <input type="radio"/> None<br/> <input checked="" type="radio"/> IronPort Anti-Spam<br/> <input type="radio"/> IronPort Intelligent Multi-Scan<br/> <input type="radio"/> Cloudmark Service Provider Edition                 </p> <p><input checked="" type="checkbox"/> Enable IronPort Spam Quarantine. This setting will quarantine positive and suspect spam.<br/> <input type="checkbox"/> Enable IronPort Spam Quarantine. This setting will quarantine positive and suspect spam.</p> |

| Anti-Virus and Malware              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Anti-Virus Scanning:</b>         | <p>Select the anti-virus engine to use for the default incoming and outgoing mail policy:</p> <p> <input type="radio"/> None<br/> <input type="radio"/> McAfee<br/> <input checked="" type="radio"/> Sophos                 </p>                                                                                                                                                                                                                                      |
| <b>Advanced Malware Protection:</b> | <p><i>Advanced Malware Protection provides additional protection against malware attachments through the File Reputation and File Analysis services.</i></p> <p><i>Advanced Malware Protection services require network communication to the cloud servers on ports 32137 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.</i></p> <p><input checked="" type="checkbox"/> Enable Advanced Malware Protection</p> |
| <b>Outbreak Filters</b>             | <p><i>Outbreak Filter quarantine suspicious messages even before traditional anti-virus security services have provided a signature file. More about Outbreak Filters...</i></p> <p><input checked="" type="checkbox"/> Enable Outbreak Filters</p>                                                                                                                                                                                                                   |

[< Previous](#) [Cancel](#)
[Next >](#)

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Review:

The final page is a review and allows you install the configuration.

|          |           |            |             |                  |
|----------|-----------|------------|-------------|------------------|
| 1. Start | 2. System | 3. Network | 4. Security | <b>5. Review</b> |
|----------|-----------|------------|-------------|------------------|

### Review Your Configuration

[Printable Page](#)

Please review your configuration. If you need to make changes, click the edit link to return to the page you'd like to edit.

| System Settings                   |                          | <a href="#">Edit</a> |
|-----------------------------------|--------------------------|----------------------|
| Default System Hostname:          | esa1.unc-hamiltons.com   |                      |
| Email System Alerts To:           | dalton@unc-hamiltons.com |                      |
| Deliver Scheduled Reports To:     | dalton@unc-hamiltons.com |                      |
| Time Zone:                        | America/Chicago          |                      |
| NTP Server:                       | time.unc-hamiltons.com   |                      |
| Admin Password:                   | <i>(hidden)</i>          |                      |
| SenderBase Network Participation: | Enabled                  |                      |
| AutoSupport:                      | Enabled                  |                      |

| Network Integration       |                                    | <a href="#">Edit</a>           |
|---------------------------|------------------------------------|--------------------------------|
| IPv4 Gateway:             | 10.0.1.1                           |                                |
| IPv6 Gateway:             |                                    |                                |
| DNS:                      | 10.0.1.7                           |                                |
| Interfaces                |                                    |                                |
| Management Port           |                                    |                                |
| IPv4 Address / Netmask:   | 10.0.1.32/24                       |                                |
| Fully Qualified Hostname: | esa1.unc-hamiltons.com             |                                |
| Accept Incoming Mail:     | <b>Domain</b><br>unc-hamiltons.com | <b>Destination</b><br>10.0.1.7 |
| Relay Outgoing Mail:      | <b>Mail Server</b><br>10.0.1.7     |                                |

| Message Security                                         |                                         | <a href="#">Edit</a> |
|----------------------------------------------------------|-----------------------------------------|----------------------|
| SenderBase Reputation Filtering:                         | Enabled                                 |                      |
| Default Incoming Mail Anti-Spam Engine:                  | IronPort Anti-Spam (Quarantine Enabled) |                      |
| Default Incoming and Outgoing Mail Anti-Virus Engine(s): | Sophos Anti-Virus                       |                      |
| Advanced Malware Protection:                             | Enabled                                 |                      |
| Outbreak Filters:                                        | Enabled                                 |                      |

[← Previous](#) [Cancel](#)

[Install This Configuration](#)

After you click the “Install This Configuration” button it installs the config and then asks if you want to run the LDAP Wizard. Cancel out of this as we will do this later.

At this point your ESA appliance has been configured with a very basic setup and can Send and Receive email.

## D. SMA: INITIAL INSTALLATION, LICENSING, AND UPGRADING

In Section C we covered initial setup of the ESA and you'll need to follow the same logic for the SMA. The 'interfaceconfig' command is a little different as it enables the interface to support the end-user Spam Quarantine on the SMA so I'm including it here. You'll still need to follow the other (additional) steps that you performed for the ESA — setgateway, sethostname, dnsconfig, ftp license file if virtual appliance, upgrade.

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 upgrade and it will prompt you to reboot. Once the appliance is back online, try another 'upgrade' to see if there is another upgrade available.

```
ironport.example.com> interfaceconfig

Currently configured interfaces:
1. Management (10.0.1.36/24 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 Address (Ex: 192.168.1.2):
[10.0.1.36]>

Ethernet interface:
1. Data 1
2. Data 2
3. Management
[3]>

Netmask (Ex: "255.255.255.0" or "0xfffff00"):
[0xfffff00]>

Hostname:
[ironport.example.com]> sma1.unc-hamiltons.com

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

Which port do you want to use for FTP?
[21]>

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

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

Which port do you want to use for SSH?
[22]>

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

Which port do you want to use for HTTP?
[80]>

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

Which port do you want to use for HTTPS?
[443]>
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

Do you want to enable Spam Quarantine HTTP on this interface? [Y]>

Which port do you want to use for Spam Quarantine HTTP?  
[82]>

Do you want to enable Spam Quarantine HTTPS on this interface? [Y]>

Which port do you want to use for Spam Quarantine HTTPS?  
[83]>

You have not entered an HTTPS certificate. To assure privacy, run "certconfig" first. You may use the demo, but this will not be secure.

Do you really wish to use a demo certificate? [Y]>

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

Both Spam Quarantine HTTP and Spam Quarantine HTTPS are enabled for this interface, should Spam Quarantine HTTP requests redirect to the secure service? [N]> Y

Do you want Management as the default interface for your Spam Quarantine? [N]> Y

Do you want to use a custom base URL in your Spam Quarantine email notifications? [N]>

You have edited the interface you are currently logged into. Are you sure you want to change it? [Y]>

Currently configured interfaces:

1. Management (10.0.1.36/24 on Management: sma1.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.
- [ ]>

Please run System Setup Wizard at <http://10.0.1.36>  
ironport.example.com>

- As with the ESA, ensure you have valid licenses (see section C).
- Upgrade to the latest version.
- Now http to the the SMA.
- If you're on a Hardware SMA Appliance ensure there are no licenses that are showing in the "Pending Activation" section.

*Management Appliance > System Administration > Feature Keys*

- We now need to run the SMA Setup Wizard.

*Management Appliance > System Administration > System Setup Wizard*

### E. SMA: BEST PRACTICES

**\*\* Note, this section does not cover all the "SMA Best Practices" as we have decided to use this section as a way to do the "initial" Best Practices changes and then describe the other "Best Practices" changes as we need them in the "Best Practices for ESA" section that follows this section.**



## ESA/SMA INSTALLATION AND BEST PRACTICES

This section covers Best Practices configuration steps for the SMA (Security Management Appliance). This section will cover the following topics:

1. Changing the webUI default login timeout
2. LDAP (useful if enabling the Spam Quarantine on the SMA)
3. Disk Management
4. Enable Centralized Spam Quarantine
5. Enable Centralized 'Policy, Virus, and Outbreak' Quarantines
6. Enable Centralized Reporting
7. Enable Centralized Message Tracking

The SMA is capable of providing centralized services for both the ESA and the WSA (Cisco's Web Security Appliance — web proxy). Customers normally purchase a separate SMA for the ESA services and one for the WSA services. This document provides instructions for letting the SMA work with the ESA and assuming the SMA is not being used for centralizing services for the Web Security Appliance (WSA).

Below are the best practices steps for the SMA.

1. Changing the webUI Default Login Timeout

Change the timeout for Admin access:

*Management Appliance > System Administration > Network Access*

I like to set this value to the max - 1440 minutes.

2. LDAP

We are going to allow End-User Spam Notifications (Spam Digests) to be emailed to the End-User (this is covered later in this section) and therefore we need to enable "Spam Quarantine Alias Consolidation Query" in the LDAP Server Profile. This requires that we check the switch (checkbox) for "Designate as the active query" — as you see in the example below. This checkbox (switch) is there because you could have multiple LDAP Server Profiles and we need to designate which one the Spam Quarantine features should use.

Add an LDAP Server Profile: *Management Appliance > System Administration > LDAP*

Here is an example of Best Practices settings:

### Edit LDAP Server Profile

**LDAP Server Settings**

**Server Attributes**

|                                                                             |                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LDAP Server Profile Name:                                                   | <input type="text" value="UNC-HAMILTONS"/>                                                                                                                                                          |
| Host Name(s):                                                               | <input type="text" value="10.0.1.16"/><br><small>Fully qualified hostname or IP, separate multiple entries with a comma</small>                                                                     |
| Authentication Method:                                                      | <input type="radio"/> Anonymous<br><input checked="" type="radio"/> Use Password<br>Username: <input type="text" value="UNC-HAMILTONS\Admini"/><br>Password: <input type="password" value="*****"/> |
| Server Type: ?                                                              | Active Directory <span style="float: right;">v</span>                                                                                                                                               |
| Port: ?                                                                     | <input type="text" value="3268"/>                                                                                                                                                                   |
| Base DN: ?                                                                  | <input type="text" value="dc=unc-hamiltons,dc=cc"/>                                                                                                                                                 |
| ▶ Advanced: System defaults for these settings are suitable for most users. |                                                                                                                                                                                                     |
| Server Attribute Testing:                                                   | <input type="button" value="Test Server(s)"/>                                                                                                                                                       |

**External Authentication Queries**

*Not configured*

**Spam Quarantine End-User Authentication Query**

*Not configured*

**Group Query**

*Not configured*

**Spam Quarantine Alias Consolidation Query**

|                  |                                                                               |                                           |
|------------------|-------------------------------------------------------------------------------|-------------------------------------------|
| Name:            | <input type="text" value="UNC-HAMILTONS.isq_alias"/>                          |                                           |
|                  | <input checked="" type="checkbox"/> Designate as the active query             |                                           |
| Query String:    | <input type="text" value="((proxyAddresses={a})(proxyAddresses=smtpp:{a}))"/> | <input type="button" value="Test Query"/> |
| Email Attribute: | <input type="text" value="mail"/>                                             |                                           |

After submitting this panel you will see the “LDAP Server Profiles” table. There must be an “asterisk” at the end of the Query — indicating this will be the one used by the Spam Quarantine functions.

### LDAP

Success — Updated LDAP server

**LDAP Server Profiles**

| Server Profile | Host Name | Port | Queries                  | Delete |
|----------------|-----------|------|--------------------------|--------|
| UNC-HAMILTONS  | 10.0.1.16 | 3268 | UNC-HAMILTONS.isq_alias* |        |

▶ Advanced

\* Active Spam Quarantine Query

**LDAP Global Settings**

Interface for LDAP Traffic: Auto

## ESA/SMA INSTALLATION AND BEST PRACTICES

### 3. Disk Management

Our assumptions above is that the SMA is only providing centralized services for ESAs and not for WSAs. With that in mind, we should recover the pre-allocated disk space on the SMA for centralizing services for the WSA.

Change Data Disk Management:

*Management Appliance > System Administration > Disk Management*

On my M300v, the default disk quotas are as follows:

**Data Disk Management**

| Centralized Service Quotas and Usage                           |                    |                                            |                                     |
|----------------------------------------------------------------|--------------------|--------------------------------------------|-------------------------------------|
| Service                                                        | Current Disk Usage | Current Disk Quota                         |                                     |
| Spam Quarantine (EUQ) <i>(service disabled)</i>                | 1 G                | 149 G                                      |                                     |
| Policy, Virus & Outbreak Quarantines <i>(service disabled)</i> | 1 G                | 149 G                                      |                                     |
| Reporting <i>(services disabled)</i>                           | 5 G                | 86 G                                       |                                     |
| Centralized Web Tracking <i>(service disabled)</i>             | 1 G                | 174 G                                      |                                     |
| Centralized Email Tracking <i>(service disabled)</i>           | 1 G                | 174 G                                      |                                     |
| Miscellaneous Files                                            | 7 G                |                                            | 99 G                                |
| System Files                                                   | 7 G                |                                            |                                     |
| User Files                                                     | 0 G                |                                            |                                     |
| <b>Total Space Used: 16 G</b>                                  |                    | <b>Total Space Allocated: 831G of 862G</b> | <a href="#">Edit Disk Quotas...</a> |

\*Some data is used for web detail reports

I changed the settings to remove the disk space allocation for Centralized Web Tracking and gave that space to additional Email Tracking and Reporting. For your environment, you may want to allocate more space for Quarantines for example.

**Edit Data Disk Management**

| Centralized Service Quotas and Usage                           |                    |                                            |                                                                     |
|----------------------------------------------------------------|--------------------|--------------------------------------------|---------------------------------------------------------------------|
| Service                                                        | Current Disk Usage | Current Disk Quota                         | Reallocate Disk Quota ?                                             |
| Spam Quarantine (EUQ) <i>(service disabled)</i>                | 1 G                | 149 G                                      | <input type="text" value="149"/> G                                  |
| Policy, Virus & Outbreak Quarantines <i>(service disabled)</i> | 1 G                | 149 G                                      | <input type="text" value="149"/> G                                  |
| Reporting <i>(services disabled)</i>                           | 5 G                | 86 G                                       | <input type="text" value="170"/> G                                  |
| Centralized Web Tracking <i>(service disabled)</i>             | 1 G                | 174 G                                      | <input type="text" value="0"/> G                                    |
| Centralized Email Tracking <i>(service disabled)</i>           | 1 G                | 174 G                                      | <input type="text" value="295"/> G                                  |
| Miscellaneous Files                                            | 7 G                |                                            | <input type="text" value="99"/> G                                   |
| System Files                                                   | 7 G                |                                            |                                                                     |
| User Files                                                     | 0 G                |                                            |                                                                     |
| <b>Total Space Used: 16 G</b>                                  |                    | <b>Total Space Allocated: 831G of 862G</b> | <b>Reallocated Total: <input checked="" type="checkbox"/> 862 G</b> |

\*Some data is used for web detail reports

[Cancel](#) [Submit](#)

## ESA/SMA INSTALLATION AND BEST PRACTICES

Once you submit this page you will get a warning about AsyncOS deleting data out of Centralized Web Tracking space — that is fine — just click “Set New Quotas” button.

### 4. Enable Centralized Spam Quarantine

We will want our ESA appliances to store Suspect SPAM in a central location — i.e. on this SMA appliance. Therefore, we must enable the Spam Quarantine on the SMA before we configure the ESA.

Enable the Spam Quarantine:

*Management Appliance > Centralized Services > Email: Spam Quarantine*

Click the Enable button. Accept the License Agreement.  
You are now taken into the Spam Quarantine configuration panel.

There are two sections:

- a) Spam Quarantine Settings
- b) End-User Quarantine Access and Spam Notifications

- a) Spam Quarantine Settings

The Spam Quarantine has two functions that could cause it to send an out-bound email.

Reason One: If you enable Spam Notifications to be sent to the End Users. This function is also known as “End-User Spam Digest Notification”.

Reason Two: If an End-User or Admin releases an Email from the Spam Quarantine.

In both cases, it is best practice to have these emails relay through the ESAs. To do this you need to change the Primary Server field to be the IP address of your ESA. If you do not have a second MTA then leave the Alternative Server field set to 127.0.0.1 so that the SMA can act as an MTA and deliver.


**IMPORTANT STEP: \*\*\*\*\***

Login to your ESA and navigate to: *Mail Policies > HAT Overview*

Click on the name RELAYLIST SenderGroup.

Click the Add Sender button and add the IP address of your SMA to the RELAYLIST.

Here is a screenshot of how to Enable the Spam Quarantine on the SMA:

| Spam Quarantine Settings                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |              |                   |                                 |                                                                                                                                                          |                    |                        |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| <input checked="" type="checkbox"/> Enable Spam Quarantine |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Quarantine IP Interface:                                   | Management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Quarantine Port:                                           | 6025                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Deliver Messages Via:                                      | <p>Notifications and released messages will be delivered by the server(s) specified below.</p> <p>Primary Server: <input type="text" value="10.0.1.37"/> Port: <input type="text" value="25"/></p> <p><small>Cisco IronPort Appliance or SMTP Server IP Address</small></p> <p>Alternative Server: <input type="text" value="127.0.0.1"/> Port: <input type="text" value="25"/></p> <p><small>Note: You must configure your destination server(s) to accept mail from this host. If you are delivering to a Cisco IronPort Appliance, it must be configured to direct spam to this appliance. See the Cisco IronPort documentation for more information.</small></p> |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Schedule Delete After:                                     | <input checked="" type="radio"/> 14 days<br><input type="radio"/> Do not schedule delete                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Notify Cisco Upon Message Release:                         | <input checked="" type="checkbox"/> Send a copy of released messages to Cisco for analysis(recommended)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Spam Quarantine Appearance:                                | <p>Current Logo:  IronPort Spam Quarantine</p> <p><input checked="" type="radio"/> Use Current Logo</p> <p><input type="radio"/> Use Cisco Spam Quarantine Logo</p> <p><input type="radio"/> Upload Custom Logo: <input type="button" value="Choose File"/> no file selected<br/><small>Maximum size 500w x 50h pixels</small></p> <p>Login Page Message: <input type="text"/></p>                                                                                                                                                                                                  |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Administrative Users: ?                                    | <table border="1"> <tr> <td>Local Users:</td> <td>No users defined.</td> </tr> <tr> <td>Externally Authenticated Users:</td> <td><a href="#">External authentication is disabled. Go to Management Appliance &gt; System Administration &gt; Users to enable external authentication.</a></td> </tr> <tr> <td>Custom User Roles:</td> <td>No user roles defined.</td> </tr> </table>                                                                                                                                                                                                                                                                                 | Local Users: | No users defined. | Externally Authenticated Users: | <a href="#">External authentication is disabled. Go to Management Appliance &gt; System Administration &gt; Users to enable external authentication.</a> | Custom User Roles: | No user roles defined. |
| Local Users:                                               | No users defined.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Externally Authenticated Users:                            | <a href="#">External authentication is disabled. Go to Management Appliance &gt; System Administration &gt; Users to enable external authentication.</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |              |                   |                                 |                                                                                                                                                          |                    |                        |
| Custom User Roles:                                         | No user roles defined.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |              |                   |                                 |                                                                                                                                                          |                    |                        |

b) End-User Quarantine Access and Spam Notifications:

Some customers desire to have the End-User receive Spam Digest Notifications and Access their Spam Digest. Let’s cover the Spam Notifications before we cover the End-User Quarantine Access.

Spam Notifications:

When customers enable Spam Notifications, a “Spam Digests” will be emailed to End-Users that have Spam in their quarantine. The “Spam Notifications” configuration panel defines how these digests will look and when these notifications will be sent.

You can selectively configure which end-users will receive Spam Notifications.

The Message Body is editable and the “Message Variables” table to the right of the Message Body allows you to insert variables that are substituted at run-time with actual values. Below the Message Body is a “Preview Message” hypertext link to preview how your Spam Notification will look to the End-User.

Because we have configured LDAP for this SMA (earlier), we gain the benefit of allowing the SMA to consolidate Spam received for the main mailbox of a user and

## ESA/SMA INSTALLATION AND BEST PRACTICES

Spam received for email ‘aliases’ into a single Spam quarantine for that user. Without this feature, the End-User would receive separate Notifications for each recipient email address they have — if that recipient address has Spam in the quarantine.

Work with the customer to decide when Notifications should be sent — Notification Schedule.

Best Practices configuration for Spam Notification:

The screenshot shows the 'Spam Notifications' configuration page. At the top, there is a checkbox for 'Enable Spam Notification' which is checked. The 'From Address' field is configured with a friendly name 'Hamilton Spam Quarantine' and an email address 'jaldon@unc-hamiltons.com'. The 'Notify To' section has 'All Users' selected. Below this, there is a section for 'All Except Users From LDAP Query' which is currently unchecked. The 'Subject' and 'Title' fields are both set to 'Hamilton Spam Quarantine Notification'. The 'Default Language' is set to 'English/United States [en-us]'. The 'Message Body' field contains a template message with variables like %new\_message\_count% and %quarantine\_url%. To the right of the message body is a 'Message Variables' box listing variables such as 'New Message Count', 'Total Message Count', 'Days Until Message Expires', 'Quarantine URL', 'Username', and 'New Message Table'. The 'Message Format' is set to 'HTML (recommended)'. The 'Deliver Bounce Message To' field is set to 'jaldon@unc-hamiltons.com'. The 'Consolidate Notifications' checkbox is checked. The 'Notification Schedule' is set to 'Monthly' with a dropdown for 'Monday' and a time of '(Sent at 12am)'. Below the schedule, there are checkboxes for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) and a grid for selecting specific days and times (12 AM, 1 PM, 2 PM, 3 PM, 4 PM, 5 PM, 6 PM, 7 PM, 8 PM, 9 PM, 10 PM, 11 PM).

### End-User Quarantine Access


End-User Authentication: None

When you enable Spam Notifications, the email received by the End-User will have a hyper-text link that takes the end-user to their specific quarantine. This URL is user specific and you can choose “End-User Authentication” to None knowing that when a End-User clicks on their digest link it is specific to their quarantine.

End-User Authentication: LDAP

On the other hand, you may wish to require the End-User to type in their credentials. In this case you could set the value to LDAP. If you do choose LDAP, be sure to go back to System Administration > LDAP and in the “Spam Quarantine Alias Consolidation Query section, check the switch-box to Enable “Designate as the active query”.

In our configuration, we choose to use None as a Best Practice since each Digest link is user specific.

| End-User Quarantine Access                                                                                                                               |                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Enable End-User Quarantine Access                                                                                    |                                                                                               |
| End-User Authentication: ?                                                                                                                               | None         |
| <small>If "None" is selected messages will be accessible via links in the Notification Message digest without additional End-User Authentication</small> |                                                                                               |
| Hide Message Bodies:                                                                                                                                     | <input type="checkbox"/> Do not display message bodies to end-users until message is released |

End-User Safelist/Blocklist: We recommend not enabling Spam Quarantine End-User Safelist/Blocklist. There is nothing wrong with using this feature but Best Practices are not to let the end-users create lists that bypass the spam engine.

**Spam Quarantine**

| Spam Quarantine Settings         |                                                       |
|----------------------------------|-------------------------------------------------------|
| Spam Quarantine:                 | Enabled<br>Default Action: Retain 14 days then Delete |
| End-User Quarantine Access:      | Authentication Method: None (use notification links)  |
| Spam Notifications:              | Enabled                                               |
| <a href="#">Edit Settings...</a> |                                                       |

| End-User Safelist/Blocklist                |  |
|--------------------------------------------|--|
| <i>This feature is currently disabled.</i> |  |
| <a href="#">Enable...</a>                  |  |

5. Enable Centralized Policy, Virus, and Outbreak Quarantines

Messages processed by certain filters, policies, and scanning operations on an ESA can be placed into quarantines to temporarily hold them for further action. You can centralize quarantines from multiple ESAs on a SMA providing Centralized services.

Enable Policy Virus and Outbreak Quarantines (PVO):

*Management Appliance > Centralized Services > Email:Policy, Virus and Outbreak Quarantines*  
 Because we are Enabling PVO and will configure the ESAs to use PVO during initial setup, we will not need to “migrate” any email or quarantines from the ESA.

### Policy, Virus and Outbreak Quarantines

| Configure Centralized Quarantines Service                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| <input checked="" type="checkbox"/> Enable Centralized Quarantines service (for Policy, Virus and Outbreak Quarantines)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                 |
| Quarantine IP Interface:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 10.0.1.36 (Management) <span>⌵</span>           |
| Quarantine Port:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 7025 <small>Specify any available port.</small> |
| <p>Configuring Centralized Policy, Virus, and Outbreak Quarantines requires the following additional steps:</p> <ol style="list-style-type: none"> <li>1. Enable Centralized Policy, Virus, and Outbreak Quarantines for each ESA by selecting Centralized Services &gt; Security Appliances.</li> <li>2. Configure migration of local quarantines to centralized quarantines by selecting Centralized Services &gt; Policy, Virus, and Outbreak Quarantines.</li> <li>3. Initiate migration to centralized quarantines by going to each ESA and selecting Security Services &gt; Policy, Virus, and Outbreak Quarantines.</li> </ol> |                                                 |
| <input type="button" value="Cancel"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <input type="button" value="Submit"/>           |

Configure the PVO Quarantines:

There are five PVO quarantines pre-created on the SMA once PVO is Enabled. Let's review these quarantines:

*Email > Message Quarantine > Policy, Virus and Outbreak Quarantines*

- a) File Analysis
- b) Outbreak
- c) Policy
- d) Unclassified
- e) Virus

- a) File Analysis

This quarantine is used by the File Analysis feature of the Advanced Malware Protection (AMP) engine on the ESA appliance. We will discuss this quarantine further in the Advanced Malware Protection discussion of the ESA customization section.

Best Practices:

Retention Period = 1 Hour  
Default Action = Release

- b) Outbreak

This quarantine is used by Outbreak Filters engine on the ESA appliance. We will discuss this quarantine further in the Outbreak Filters discussion of the ESA customization section.

Best Practices:



## ESA/SMA INSTALLATION AND BEST PRACTICES

Default Action = Release

### c) Policy

This quarantine is created as a “catch all” quarantine for Admins to use when creating Message Filters, Content Filters, or DLP Policies. It is not Best Practices to use this quarantine but instead, create new PVO quarantines specially to meet the particular policy the Admin is trying to create. We will be creating these new policy quarantines in the next section.

Best Practices:

Do not use this quarantine — it is just generic and it is a better practice to create “specific” quarantines for “specific” ESA policies and filters rather than using this generic “Policy” quarantine.

### d) Unclassified

Holds messages only if a quarantine that is specified in a message filter, content filter, or DLP message action has been deleted?

### e) Virus

The ESA appliances can run both Sophos and McAfee signature-based malware engines in parallel. If an attachment is determined to be malware, one of the “Actions” available is to Quarantine the email to the “Virus” quarantine — which is this quarantine.

We will be creating many more PVO Quarantines once we start customizing the ESA appliances.

## 6. Enable Centralized Reporting

*Management Appliance > Centralized Services > Email: Centralized Reporting*

## 7. Enable Centralized Message Tracking

*Management Appliance > Centralized Services > Email: Centralized Message Tracking*

\*\*\* **NOTE:** You’ve made a lot of changes – be sure that you are committing changes along the way.

### F. ESA: BEST PRACTICES

This section will step you through the “Best Practices” settings for the ESA. You are more than likely deploying multiple ESA appliances. The best way to do this is to fully configure the first appliance and then use the Cisco ESA Cluster technology to configure all remaining ESA appliances. Setting up and configuring the 2nd and all subsequent ESAs will be covered in Section G of this document. Clustering ESA appliances together also keeps their configuration synchronized. When you make a change on one appliance it automatically changes all appliances in the cluster. Some customer initially assume the SMA manages (or synchronizes) the configuration of multiple ESAs. The SMA plays absolutely no role in the configuration of the ESA appliances. The SMA provides “centralized services” around centralized reporting, centralized message tracking, centralized quarantines.

This section is assuming you are using Deployment Option 1 as discussed in Section A. At this point you should have already completed the steps described in Section D - “ESA: Initial Installation, Licensing, and Upgrading”.

As mentioned earlier, we are running AsyncOS 9.5 and we have all feature keys and will be covering the settings for each feature of the ESA.

#### 1. System Administration and Network

##### a) LDAP

The LDAP profile is very important in many ways. It will be used to provide “Recipient Validation” and therefore needed to configure Directory Harvest Attack Prevention (DHAP). Both will be configured later in this section.

Navigate to: *System Administration > LDAP*

Click the Add LDAP Server Profile button. Here is an example of an LDAP server profile. Be sure to enable Accept and Group queries.

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Add LDAP Server Profile

| LDAP Server Settings                                                      |                                                                                                                                      |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Server Attributes                                                         |                                                                                                                                      |
| LDAP Server Profile Name:                                                 | UNC-HAMILTONS                                                                                                                        |
| Host Name(s):                                                             | 10.0.1.16<br><small>Fully qualified hostname or IP, separate multiple entries with a comma</small>                                   |
| Base DN: ?                                                                | dc=unc-hamiltons,dc=cc                                                                                                               |
| Authentication Method:                                                    | <input type="radio"/> Anonymous<br><input checked="" type="radio"/> Use Password<br>Username: UNC-HAMILTONS\Admin<br>Password: ***** |
| Server Type: ?                                                            | Active Directory                                                                                                                     |
| Port: ?                                                                   | 3268                                                                                                                                 |
| Connection Protocol:                                                      | <input type="checkbox"/> Use SSL                                                                                                     |
| Advanced: System defaults for these settings are suitable for most users. |                                                                                                                                      |
| Server Attribute Testing:                                                 | Test Server(s)                                                                                                                       |
| ✓ Accept Query                                                            |                                                                                                                                      |
| Name:                                                                     | UNC-HAMILTONS.accept                                                                                                                 |
| Query String:                                                             | [(proxyAddresses=smtp:{a})] Test Query                                                                                               |
| ■ Routing Query<br>Not configured                                         |                                                                                                                                      |
| ■ Certificate Authentication Query<br>Not configured                      |                                                                                                                                      |
| ■ Masquerade Query<br>Not configured                                      |                                                                                                                                      |
| ✓ Group Query                                                             |                                                                                                                                      |
| Name:                                                                     | UNC-HAMILTONS.group                                                                                                                  |
| Query String:                                                             | [(&(memberOf={g}))(proxyAddresses=smtp:{a})] Test Query                                                                              |
| ■ SMTP Authentication Query<br>Not configured                             |                                                                                                                                      |
| ■ External Authentication Queries<br>Not configured                       |                                                                                                                                      |
| ■ Spam Quarantine End-User Authentication Query<br>Not configured         |                                                                                                                                      |
| ■ Spam Quarantine Alias Consolidation Query<br>Not configured             |                                                                                                                                      |

Cancel Submit

### b) System Administration > Alerts

When you ran the initial setup wizard it created one entry in the Alerts panel. However, it did not enable alerts for DHAP (Directory Harvest Attack Prevention). DHAP will be configured later. I recommend you enable DHAP alerts and the Admin will receive these types of Alerts:

*Error message:*

*Warning <Directory>: Potential Directory Harvest Attack detected. See the system ...*

*Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack. Last message occurred 43 times....*

### c) System Administration > Log Subscription

Click on the mail log name “mail\_logs” and it opens the log settings. I like to set my mail\_logs for max size of 10MBytes and rollover daily.

## ESA/SMA INSTALLATION AND BEST PRACTICES

### d) System Administration > Return Address

At some point in time one of the email addresses you have specified in the Alerts panel may no longer be valid — maybe an email Admin leaves the company. When Alerts are sent, the return email address is specified in this panel. You can leave the text in the double-quotes but set the return address to something that can bounce to a legitimate internal Admin user.

### e) Set the timeout for GUI and CLI

I set both the Web UI Inactivity Timeout and the CLI timeout to 1440 minutes.

*System Administration > Network Access*

### f) Network > IP Interfaces

Recommended Best Practices settings are below. We have enabled FTP and SSH but DO NOT enable Cluster Communication Service. As of AsyncOS 9.0 and above, the ESA's support REST API and you can write apps/scripts to query for reporting data and settings metrics from the ESA. Version 2 of the ESA's implementation of the REST API will support both READ and WRITE. Therefore, I enable the API HTTP and HTTPS.

#### Edit IP Interface

| IP Interface Settings                                                                                                                                                                                                                                                                                                 |                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Name:                                                                                                                                                                                                                                                                                                                 | Management                                            |
| Ethernet Port:                                                                                                                                                                                                                                                                                                        | Management                                            |
| IPv4 Address / Netmask:                                                                                                                                                                                                                                                                                               | 10.0.1.37/24<br><small>(example: 10.1.1.0/24)</small> |
| IPv6 Address / Netmask:                                                                                                                                                                                                                                                                                               | <br><small>(example: 2001:db8::/32)</small>           |
| Hostname:                                                                                                                                                                                                                                                                                                             | esa1.unc-hamiltons.com                                |
| HTTPS Certificate:                                                                                                                                                                                                                                                                                                    | System Default                                        |
| Services:                                                                                                                                                                                                                                                                                                             |                                                       |
| <input checked="" type="checkbox"/> FTP<br><small>Applicable only for IPv4 addresses.</small>                                                                                                                                                                                                                         | Port: 21                                              |
| <input checked="" type="checkbox"/> SSH                                                                                                                                                                                                                                                                               | 22 *                                                  |
| <input type="checkbox"/> Cluster Communication Service                                                                                                                                                                                                                                                                | 2222 *                                                |
| <input type="checkbox"/> RSA Enterprise Manager Integration                                                                                                                                                                                                                                                           | 20002                                                 |
| Appliance Management                                                                                                                                                                                                                                                                                                  |                                                       |
| <input checked="" type="checkbox"/> HTTP                                                                                                                                                                                                                                                                              | 80 *                                                  |
| <input checked="" type="checkbox"/> HTTPS                                                                                                                                                                                                                                                                             | 443 *                                                 |
| <input type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)                                                                                                                                                                                                                  |                                                       |
| AsyncOS API (Monitoring)                                                                                                                                                                                                                                                                                              |                                                       |
| <input checked="" type="checkbox"/> AsyncOS API HTTP                                                                                                                                                                                                                                                                  | 6080                                                  |
| <input checked="" type="checkbox"/> AsyncOS API HTTPS                                                                                                                                                                                                                                                                 | 6443                                                  |
| Spam Quarantine                                                                                                                                                                                                                                                                                                       |                                                       |
| <input type="checkbox"/> Spam Quarantine HTTP                                                                                                                                                                                                                                                                         | 82                                                    |
| <input type="checkbox"/> Spam Quarantine HTTPS                                                                                                                                                                                                                                                                        | 83                                                    |
| <input type="checkbox"/> Redirect HTTP requests to HTTPS (HTTP and HTTPS Services will be turned on)                                                                                                                                                                                                                  |                                                       |
| <input type="checkbox"/> This is the default interface for Spam Quarantine<br>Quarantine login and notifications will originate on this interface.<br>URL Displayed in Notifications:<br><input type="radio"/> Hostname<br><input type="radio"/><br><small>(examples: http://spamQ.url/, http://10.1.1.1:82/)</small> |                                                       |
| <small>Warnings - * Please exercise care when disabling or changing these items, as this could disrupt active connections to this appliance when changes to these items are committed.<br/>** Hyperlinks and URLs affected by these changes will not be usable until the changes are committed.</small>               |                                                       |
| <a href="#">Cancel</a>                                                                                                                                                                                                                                                                                                | <a href="#">Submit</a>                                |

## ESA/SMA INSTALLATION AND BEST PRACTICES

### g) Network > Listeners

Since we are using Deployment Option #1 as described in Section A, we have a single “Listener” named “IncomingMail”. Click on the name “IncomingMail” and modify the Listener as follows.

Change the name to something that indicates it handles both “Incoming” and “Outgoing” mail. I use “BidirectionalMail”

Open the “LDAP Queries” disclosure triangle and set the Accept Query and the Group Query.

Since we are using Deployment Option #1 as described in Section A, we have a single “Listener” named “IncomingMail”. Click on the name “IncomingMail” and modify the Listener as show in this screenshot.

#### Edit Listener

| Listener Settings             |                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Name:                         | <input type="text" value="BidirectionalMail"/>                                                                                               |
| Type of Listener:             | Public                                                                                                                                       |
| Interface:                    | Management <input type="button" value="v"/> TCP Port: <input type="text" value="25"/>                                                        |
| Bounce Profile:               | Default <input type="button" value="v"/>                                                                                                     |
| Disclaimer Above:             | None <input type="button" value="v"/><br><i>Disclaimer text will be applied above the message body.</i>                                      |
| Disclaimer Below:             | None <input type="button" value="v"/><br><i>Disclaimer text will be applied below the message body.</i>                                      |
| SMTP Authentication Profile:  | None <input type="button" value="v"/> Note: To use Certificate type Auth profile, please enable TLS on mail flow policies for this listener. |
| Certificate:                  | System Default <input type="button" value="v"/>                                                                                              |
| SMTP Address Parsing Options: | Optional settings for controlling parsing in SMTP "MAIL FROM" and "RCPT TO"                                                                  |
| Advanced:                     | Optional settings for customizing the behavior of the Listener                                                                               |
| LDAP Queries:                 | <input type="button" value="v"/> Accept                                                                                                      |
|                               | Accept Query: <input type="text" value="UNC-HAMILTONS.accept"/> <input type="button" value="v"/>                                             |
|                               | <input type="radio"/> Work Queue                                                                                                             |
|                               | Non-Matching Recipients: <input type="text" value="Bounce"/> <input type="button" value="v"/>                                                |
|                               | <input checked="" type="radio"/> SMTP Conversation                                                                                           |
|                               | If the LDAP server is unreachable:                                                                                                           |
|                               | <input type="radio"/> Allow Mail in                                                                                                          |
|                               | <input checked="" type="radio"/> Return error code:                                                                                          |
|                               | Code: <input type="text" value="451"/>                                                                                                       |
|                               | Text: <input type="text" value="Temporary recipient validation error"/>                                                                      |
|                               | <input type="button" value="v"/> Routing                                                                                                     |
|                               | <input type="button" value="v"/> Masquerade                                                                                                  |
|                               | <input type="button" value="v"/> Group                                                                                                       |
|                               | Group Query: <input type="text" value="UNC-HAMILTONS.group"/> <input type="button" value="v"/>                                               |

## ESA/SMA INSTALLATION AND BEST PRACTICES

### h) Network > DNS

The Cisco ESA appliances can place a very heavy load on DNS servers because every Incoming connection results in many DNS lookups - A Record, PTR Record, SBRS Score, DKIM record, SPF record, DMARC record, etc. If you do not have enough DNS capacity the ESAs can overload your DNS server accidentally — essentially causing a denial of service attack on your own DNS server.

Best Practice is to configure DNS for “Use the Internet’s Root DNS Servers” and define specific DNS servers for “local” domains that your internal DNS servers are “Start of Authority” (SOA) for.

If you must use internal DNS servers then ensure you have enough DNS capacity or dedicate DNS servers to the ESA.

Here is an example of Best Practices DNS settings with Split-DNS enabled.

#### Edit DNS

**DNS Server Settings**

DNS Servers:  Use these DNS Servers

| Priority (?) | Server IP |         |
|--------------|-----------|---------|
|              |           | Add Row |

Alternate DNS servers Overrides (Optional):

| Domain(s)                                      | DNS Server IP Address         |         |
|------------------------------------------------|-------------------------------|---------|
|                                                |                               | Add Row |
| <small>i.e., example.com, example2.com</small> | <small>i.e., 10.0.0.3</small> |         |

Use the Internet's Root DNS Servers

Alternate DNS servers Overrides (Optional):

| Domain                           | DNS Server FQDN                      | DNS Server IP Address         |         |
|----------------------------------|--------------------------------------|-------------------------------|---------|
| unc-hamiltons.com                | macpro.unc-hamiltons.c...            | 10.0.1.7                      | Add Row |
| <small>i.e., example.com</small> | <small>i.e., dns.example.com</small> | <small>i.e., 10.0.0.3</small> |         |

Interface for DNS Traffic: Auto

Wait Before Timing out Reverse DNS Lookups: 20

Cancel Submit

### i) Network > Incoming Relays

It is very important that the Cisco ESA is the MTA that receives the email from the Sending MTA so that the ESA’s SBRS (Senderbase Reputation Score) is accurate. Our “Reputation” engine stops about 90% of all attempted email. Once the ESA has the Reputation, that same Reputation is used in the other “Engines” in filtering — the Spam engine and Outbreak Filters.

If the ESA is not the device that receives the email off the Internet and some other MTA receives the email and then that MTA forwards the email to the ESA, it is imperative that you set the *Network > Incoming Relay* to get the real Reputation

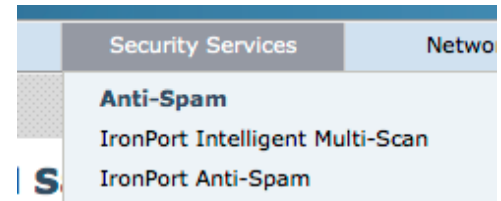
## ESA/SMA INSTALLATION AND BEST PRACTICES

for the Sender and you would need to alter the configuration in multiple other ways — which is outside of the scope of this document.

### 2. Security Services

#### a) Enable Anti-Spam

*Security Services > Ironport Anti-Spam*  
*Security Services > Ironport Intelligent Multi-Scan*



Most customers will run either the Cisco IronPort Anti-Spam (IPAS) engine or the Intelligent Multi-Scan (IMS) engine. Therefore, you should never really see both menu items under Security Services. You will probably see either IPAS or IMS.

IPAS is a great engine and most customers purchase IPAS; however if you have an IMS feature key you get both Cloudmark and IPAS — i.e. dual-layer Spam engines. There is sometimes confusion that to get dual-layer Spam protection you need to purchase both IMS and IPAS. This is not the case. IMS internally runs both Cloudmark and IPAS. At no time do you need to purchase an IMS key/license and also purchase an IPAS key/license. If you wish to have dual-layer Spam, then just purchase the IMS feature.

Also, if for some reason your ESA has a feature key for both IMS and for IPAS then you will see both of them under the Security Services menu. It is best practice to only enable IMS or only Enable IPAS — not both. If both are enabled, then when you go to Mail Policies > Incoming Mail Policies and edit a policy, you will see the checkbox for both IMS and for IPAS. You should never have an Incoming Mail Policy that has both IMS and IPAS enabled on the same Incoming Mail Policy as it will lead to a higher level of false positives. IPAS is already built in to IMS so you would be sending it through IPAS twice.

Therefore, if your ESA does have keys for both IMS and for IPAS, then from Security Services menu Enable only IMS or IPAS. We will discuss Incoming Mail Policies later in this section.

Once you enable either IPAS or IMS, then Edit Global Settings. Set “Always scan ...” to 2M. Set “Never scan...” to 3M. Set Timeout for Scanning to 60 seconds.

## ESA/SMA INSTALLATION AND BEST PRACTICES

Ensure the Rule Updates show “CASE Core Files” of at least 3.5. and there is a row showing “Bayes DB”.

| IronPort Anti-Spam Overview             |                                                   |  |  |
|-----------------------------------------|---------------------------------------------------|--|--|
| IronPort Anti-Spam Scanning:            | Enabled                                           |  |  |
| Message Scanning Thresholds:            | Always scan 2M or less.<br>Never scan 3M or more. |  |  |
| Timeout for Scanning Single Message:    | 60 seconds                                        |  |  |
| Regional Scanning:                      | Off                                               |  |  |
| <a href="#">Edit Global Settings...</a> |                                                   |  |  |

| Rule Updates                                       |                         |                                 |               |
|----------------------------------------------------|-------------------------|---------------------------------|---------------|
| Rule Type                                          | Last Update             | Current Version                 | New Update    |
| CASE Core Files                                    | Tue Sep 1 14:06:40 2015 | 3.5.0-008                       | Not Available |
| CASE Utilities                                     | Tue Sep 1 14:06:40 2015 | 3.5.0-008                       | Not Available |
| Structural Rules                                   | Wed Sep 2 03:10:50 2015 | 3.5.0-20150901_173401           | Not Available |
| Web Reputation DB                                  | Tue Sep 1 14:06:40 2015 | 20150831_073559                 | Not Available |
| Web Reputation DB Update                           | Wed Sep 2 06:37:39 2015 | 20150831_073559-20150902_113240 | Not Available |
| Content Rules                                      | Wed Sep 2 08:10:50 2015 | 20150902_130850                 | Available     |
| Content Rules Update                               | Wed Sep 2 08:10:50 2015 | 20150902_130901                 | Available     |
| Bayes DB                                           | Tue Sep 1 14:06:40 2015 | 20150901_152753-20150901_162834 | Not Available |
| No updates in progress. <a href="#">Update Now</a> |                         |                                 |               |

### b) Enable Graymail and Safe Unsubscribing

Graymail is bulk messages that do not fit the definition of spam, for example, newsletters, mailing list subscriptions, social media notifications, and so on. The difference between Graymail and Spam is that, for Graymail, you intentionally provided an email address at some point.

The Graymail management solution in the ESA consists of two components: an integrated Graymail scanning engine, and a cloud-based Safe Unsubscribe Service offered by Cisco.

Since Graymail and the Safe Unsubscribe Service are new features to our Cisco ESA product, let's take a few paragraphs to describe how the feature works.

The Graymail management solution allows organizations to:

- Identify Graymail using the integrated graymail engine and apply appropriate policy controls
- Provide an easy mechanism for end-users to safely unsubscribe from unwanted Graymail using the Unsubscribe Service. The “Unsubscribe” feature is a popular phishing technique and for this reason, the end-users should be wary of clicking the unknown unsubscribe links. For this reason, the cloud-based Unsubscribe Service extracts the original unsubscribe URI, checks the reputation of the URL,



## ESA/SMA INSTALLATION AND BEST PRACTICES

and then performs the unsubscribe process on behalf of the end-user. This protects the end-users from malicious threats masquerading as “Unsubscribe” links.

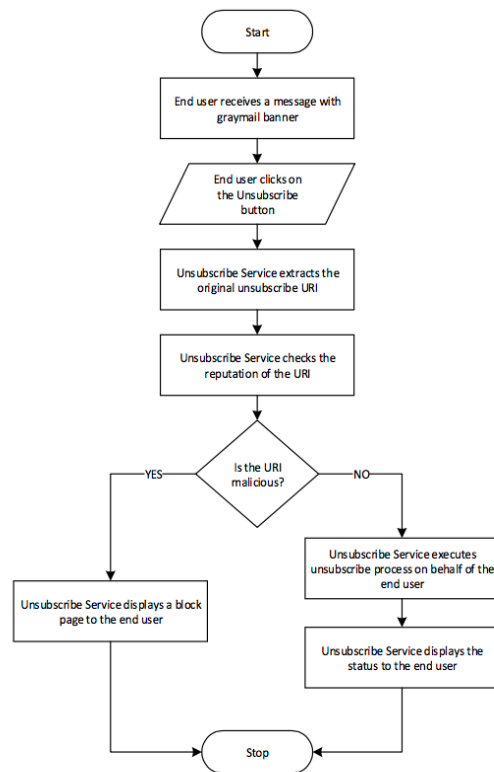
Here is a flowchart diagram of how the Safe Unsubscribe feature works:

Step 1: The end-user receives an Email and the Graymail banner has been added.

Step 2: The end-user clicks on the Unsubscribe link.

Step 3: Unsubscribe Service extracts the original unsubscribe URI and checks the URI Reputation.

Step 4: Depending on the Reputation of the URI:



- If the URI is malicious the Unsubscribe Service will not perform the unsubscribe process and displays a block page to the end-user.
- If the URI is not malicious, depending on the URI type (http or mailto), the Unsubscribe Service sends an unsubscribe request to the graymail sender.
  - If the request is successful, the Unsubscribe Service displays the “Successfully unsubscribed” status to the end-user.
  - If the first unsubscribe request fails, the Unsubscribe Service displays the “Unsubscribe process in progress” status and provides a hypertext link (URL) that can be used to track the status of the unsubscribing. End-users can use this URL to track the status over time. After the first failed attempt, the Unsubscribe Service sends periodic unsubscribe requests for a duration of four hours.

If an end-user checks the status of the unsubscribe process at a later point:

## ESA/SMA INSTALLATION AND BEST PRACTICES

- If one of the requests within the four hour duration (from the first failed attempt) is successful, the Unsubscribe Service displays the “Successfully unsubscribed” status.
- If none of the requests within the four hour duration are successful, the message will be “Unable to unsubscribe” and provides a URL that can be used to unsubscribe from the graymail manually.

Configuring Graymail and Safe Unsubscribe:

*Security Services > Graymail Detection and Safe Unsubscribing*

| Edit Global Settings                                                                                                              |                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| To detect graymail and safely unsubscribe, enable this feature on Incoming Mail Policies after you configure the global settings. |                                                                                                                                               |
| <input checked="" type="checkbox"/> <b>Enable Graymail Detection</b>                                                              |                                                                                                                                               |
| Maximum Message Size to Scan:                                                                                                     | <input type="text" value="3M"/> Maximum<br><small>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</small> |
| Timeout for Scanning Single Message:                                                                                              | <input type="text" value="60"/> Seconds                                                                                                       |

Click Enable Graymail Detection.

*Submit and Commit*

You will now see the following for Graymail. Note the “Safe Unsubscribe” still needs to be Enabled. Click Enable and accept the Acceptable Use Agreement.

You should now see the following - note that Safe Unsubscribe is now Enabled:

### Graymail Detection and Safe Unsubscribing

| Global Settings                      |                                                                                          |
|--------------------------------------|------------------------------------------------------------------------------------------|
| Graymail Detection:                  | Enabled                                                                                  |
| Maximum Message Size to Scan:        | 1M                                                                                       |
| Timeout for Scanning Single Message: | 60 seconds                                                                               |
| Safe Unsubscribe:                    | Graymail Safe Unsubscribing is currently disabled. <input type="button" value="Enable"/> |

This process just enables Graymail from a Global perspective and we will need to configure the Incoming Mail Policy for Graymail Detection and Safe Unsubscribing later in this document when we get to Incoming Mail Policies.

## ESA/SMA INSTALLATION AND BEST PRACTICES

| Global Settings                         |            |
|-----------------------------------------|------------|
| Graymail Detection:                     | Enabled    |
| Maximum Message Size to Scan:           | 3M         |
| Timeout for Scanning Single Message:    | 60 seconds |
| Safe Unsubscribe:                       | Enabled    |
| <a href="#">Edit Global Settings...</a> |            |

**c) Enable both AV Signature Engines: Sophos and McAfee**

If you have feature keys for both Sophos and McAfee then ensure they are both Enabled.

*Security Services > Sophos (Enable)*

*Security Services > McAfee (Enable)*

**d) Enable Advanced Malware Protection File Reputation and Analysis**

*Security Services > File Reputation and Analysis*

Edit the settings to ensure all File Types are enabled and check the “Use SSL” checkbox.

### Edit File Reputation and Analysis Settings

**Advanced Malware Protection**

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File Reputation Filtering: <input checked="" type="checkbox"/> Enable File Reputation<br><br>File Analysis: <input checked="" type="checkbox"/> Enable File Analysis<br><br>File Types: <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Adobe Portable Document Format (PDF)</li> <li><input checked="" type="checkbox"/> Microsoft Office 2007+ (Open XML)</li> <li><input checked="" type="checkbox"/> Microsoft Office 97-2004 (OLE)</li> <li><input checked="" type="checkbox"/> Microsoft Windows / DOS Executable</li> </ul> | Cloud Domain: <input type="text" value="a.immunet.com"/><br>Cloud Server Pool: <input type="text" value="cloud-sa.amp.sourcefire.com"/><br>SSL Communication for File Reputation: <input checked="" type="checkbox"/> Use SSL (Port 443)<br>Tunnel Proxy (Optional):<br>Server: <input type="text"/> Port: <input type="text"/><br>Username: <input type="text"/><br>Password: <input type="password"/><br>Retype Password: <input type="password"/><br><input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy <span style="font-size: small;">?</span><br>Heartbeat Interval: <input type="text" value="15"/> minutes<br>Reputation Threshold: <input checked="" type="radio"/> Use Value from Cloud Service (60)<br><input type="radio"/> Enter Custom Value: <input type="text" value="60"/><br><small>(Valid range 1 through 100)</small><br>Query Timeout: <input type="text" value="15"/> seconds<br>Processing Timeout: <input type="text" value="120"/> seconds<br>File Reputation Client ID: 6bf76f4d-4749-4095-9cf7-1af9ffb2365a<br>File Analysis Server URL: <a href="https://panacea.threatgrid.com">AMERICAS (https://panacea.threatgrid.com)</a> <span style="font-size: small;">?</span><br>File Analysis Client ID: 01_VLNESA000130_564DF56D18E45A4F00DE-BFB8C738BA66_C300V_00000000 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[Cancel](#) [Submit](#)

## ESA/SMA INSTALLATION AND BEST PRACTICES

- e) **Enable DLP for outbound DLP Scanning**  
*Security Services > RSA Email DLP*

### Data Loss Prevention Settings

| RSA Email Data Loss Prevention Settings |         |
|-----------------------------------------|---------|
| Data Loss Prevention:                   | Enabled |
| Matched Content Logging:                | Enabled |
| Automatic Updates:                      | Enabled |
| <a href="#">Edit Settings...</a>        |         |

Enable Matched Content Logging and Automatic Updates.

Updates for the RSA DLP engine and predefined content matching classifiers on your appliance are independent of updates for other security services. The 3-5 minute regular Talos/SIO signature updates is different and does not include updating RSA DLP policies and dictionaries. RSA updates which must be enabled here.

When “Matched Content Logging” is Enabled, it allows Message Tracking to show the content of the email that caused the violation. Here is an example of Message Tracking showing the email content that caused the DLP violation.

| Message Details                    |                            |
|------------------------------------|----------------------------|
| <b>Envelope and Header Summary</b> |                            |
| Received Time:                     | 20 Aug 2009 00:53:37 (GMT) |
| MID:                               | 153                        |
| Message Size:                      | 4.88 (KB)                  |
| Subject:                           | example message            |
| Envelope Sender:                   | user@example.com           |
| Envelope Recipients:               | example@recipient.com      |
| Message ID Header:                 | <40ee33\$4p@example.com>   |
| SMTP Auth User ID:                 | N/A                        |
| <b>Sending Host Summary</b>        |                            |
| Reverse DNS Hostname:              | example.com (verified)     |
| IP Address:                        | 127.0.0.1                  |
| SBR Score:                         | not enabled                |

| Message Details     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Summary             | <b>DLP Matched Content</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                     | MESSAGE ID "153" MATCHED DLP POLICY: custom_policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Violation Severity: | MEDIUM (Risk Factor: 50)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| attachment.xls:     | Credit Cards <ul style="list-style-type: none"> <li>• Carolyn Anderson 4886, Lynn Avenue Eau Claire WI 54701 US 715-491-2806 MasterCard 5337767638591724 938 4/2008</li> <li>• Albert Beamer 1141, Johnny Lane Milwaukee WI 53202 US 414-283-3835 MasterCard 5350705902658342 849 4/2010</li> <li>• Jordan Lape 2551, Browning Lane Madison WI 53703 US 608-227-8939 MasterCard 5386923042900742 513 12/2009</li> <li>• Barbara Scott 1678, Abner Road Edgar WI 54426 US 715-352-9535 MasterCard 540410R95R654RR3 110 8/2009</li> </ul> |

## ESA/SMA INSTALLATION AND BEST PRACTICES

When you click Submit it will start the DLP Assessment Wizard. Click Cancel on this Wizard and we will have DLP section later in this document.

### f) Enable URL Intelligence/Filtering and Web Interaction Tracking (Click-Tracking)

*Security Services > URL Filtering*

| URL Filtering Overview                                                         |                                                                     |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Enable URL Category and Reputation Filters |                                                                     |
| Use a URL whitelist: ?                                                         | None                                                                |
| Web Interaction Tracking: ?                                                    | <input checked="" type="checkbox"/> Enable Web Interaction Tracking |

### g) Customize the Block Page Data

Setup Block page customization. Navigate to:

*Security Services > Block Page Customization*

Set the Logo to a URL for your company icon.  
Enter your company name and contact information.  
Here is what my system looks like.

### Block Page Customization

| Block Page Customization |                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------|
| Logo URL:                | http://upload.wikimedia.org/wikipedia/commons/thumb/6/64/Cisco_logo.svg/200px-Cisco_logo.svg.png |
| Company Name:            | Cisco Systems                                                                                    |
| Contact Information:     | dalthami@cisco.com                                                                               |
| Default Language:        | English/United States [en-us]                                                                    |

### h) Enable Cisco IronPort Email Encryption

*Security Services > Cisco IronPort Email Encryption*

The Cisco IronPort Email Encryption is also referred to as CRES Encryption. CRES (Cisco Registered Envelope Service) is the name that we use for the “Key Servers” in the Cisco Cloud. The CRES encryption solution uses symmetric key encryption — which means the key used to encrypt the message is the same key used to decrypt the message. CRES is the name used to represent the Cisco Key Servers that stores / holds the keys. The ESA can decide to encrypt a message in many ways — via “flag” (like Subject content), via Content Filter matching, or via DLP Policy, for example. Once the ESA decides to encrypt a message, it needs to do so with a “Encryption Profile” created in “Security Services > Cisco IronPort Encryption” — the table named “Email Encryption Profiles. By default, there are no Profiles.

## ESA/SMA INSTALLATION AND BEST PRACTICES

When you Enable CRES Encryption, you will need to specify the Email Address for whomever is going to be the CRES Admin for the customer's account. That person must already have a CRES account. If they do not, send them an encrypted email forcing them to create a CRES account. At this point you should see the "Email Encryption Global Settings" set to something like this:

### Cisco IronPort Email Encryption Settings

| Email Encryption Global Settings                       |                    |
|--------------------------------------------------------|--------------------|
| Cisco IronPort Email Encryption:                       | Enabled            |
| Maximum message size to Encrypt:                       | 10M                |
| Email address of the encryption account administrator: | dalthami@cisco.com |
| Proxy Server (optional):                               | Not Configured     |

[Edit Settings...](#)

Now create three Encryption Profiles and name them "EncryptHigh", "EncryptMedium", and "EncryptLow". Below is a screenshot providing an example encryption profile — in this case it is for "Encrypt High". Use this same example to create all three profiles — just change the radio button for each profile.

- For Encrypt High, choose the "High Security" radio button.
- For Encrypt Medium, choose the "Medium Security" radio button.
- For Encrypt Low, choose the "No Password Required" radio button

### Edit Encryption Envelope Profile

| Encryption Profile Settings                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile Name:                                                      | EncryptHigh                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Used by (Roles):                                                   | No roles selected                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Key Server Settings</b>                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Key Service Type:                                                  | Cisco Registered Envelope Service                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Proxy:                                                             | A proxy server is not currently configured.                                                                                                                                                                                                                                                                                                                                                                                                                |
| Cisco Registered Envelope Service URL:                             | https://res.cisco.com                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Advanced <i>Advanced key server settings</i>                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Envelope Settings</b>                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Example Envelope                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Envelope Message Security:                                         | <input checked="" type="radio"/> High Security<br><i>Recipient must enter a password to open the encrypted message, even if credentials are cached ("Remember Me" selected).</i><br><input type="radio"/> Medium Security<br><i>No password entry required if recipient credentials are cached ("Remember Me" selected).</i><br><input type="radio"/> No Password Required<br><i>The recipient does not need a password to open the encrypted message.</i> |
| Logo Link:                                                         | <input checked="" type="radio"/> No link<br><input type="radio"/> Custom link URL:<br><input type="text"/><br><i>By defining a URL, the logo in the upper left corner of the recipient envelope will become a link (example: http://www.mycompany.com/).</i>                                                                                                                                                                                               |
| Read Receipts:                                                     | <input checked="" type="checkbox"/> Enable Read Receipts<br>Advanced <i>Advanced envelope settings</i>                                                                                                                                                                                                                                                                                                                                                     |
| <b>Message Settings</b>                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Example Message                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| End-User Controls:                                                 | <input checked="" type="checkbox"/> Enable Secure Reply All<br><input checked="" type="checkbox"/> Enable Secure Message Forwarding                                                                                                                                                                                                                                                                                                                        |
| <b>Notification Settings</b>                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Localized Envelopes:                                               | <input type="checkbox"/> Use Localized Envelope                                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted Message HTML Notification:                               | System Generated<br>Preview Message<br><i>(see Mail Policies &gt; Text Resources &gt; Encryption Notification Template - HTML)</i>                                                                                                                                                                                                                                                                                                                         |
| Encrypted Message Text Notification:                               | System Generated<br>Preview Message<br><i>(see Mail Policies &gt; Text Resources &gt; Encryption Notification Template - Text)</i>                                                                                                                                                                                                                                                                                                                         |
| Encryption Failure Notification:                                   | Message Subject: [ENCRYPTION FAILURE]<br>Message Body: System Generated<br>Preview Message<br><i>(see Mail Policies &gt; Text Resources &gt; DSN Bounce and Encryption Failure Notification Template)</i>                                                                                                                                                                                                                                                  |
| File name of the envelope attached to the encryption notification: | securedoc_\$(date)T\$(time).html                                                                                                                                                                                                                                                                                                                                                                                                                           |

Cancel Submit

## ESA/SMA INSTALLATION AND BEST PRACTICES

You will notice there are options to Enable Read Receipts, Enable Secure Reply All, and Enable Secure Message Forwarding.

To the right of Envelope Settings, you will see “Example Message” hypertext link which, if clicked, will show you an example of the Secure Message Envelope — what the recipient will see in their Inbox.

Read Receipts means that the Sender of the encrypted message will receive an email from CRES when the Recipient opens the Secure Message (meaning the recipient pulled down the symmetric key and decrypted the message).

To the right of the Message Settings you will see Example Message hypertext link that will show you what the opened message will look like with and without Enable Secure Reply All and Enable Secure Message Forwarding checked.

**NOTE:** Before you can create Encryption Profiles, each ESA S/N must be registered with CRES Provisioning team.

To do this, email your Cisco Content Security sales team with the following:

- Company Name
- CRES Admin Name and Email
- List of S/Ns for each ESA.
- Indicate whether an existing CRES Company account exists for this customer.

**Note:** After you have emailed this detail, it may take a day for your Company CRES account to be created (if it was not already created) and the S/Ns to be added. The “Provision” step below will not work until this is completed.

**Note:** After you submit the Encryption Profile configuration panel, you must Commit Changes.

The row in the table will then show a “Provision” button. The Provision button will not appear until after you Commit changes.

Click the Provision button (Again, this will only work after your company CRES account has been created and the appliance S/Ns have been added to your account).

- i) **Enable Cisco Outbreak Filters and Web Interaction Tracking for Outbreak Rewrites**  
*Security Services > Outbreak Filters*

## ESA/SMA INSTALLATION AND BEST PRACTICES

Enable Outbreak Filters and set the “Maximum Message Size to Scan” to 3MBytes

| Outbreak Filters Overview               |                                                                                                                                                      |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Global Status:                          | Enabled                                                                                                                                              |
| Adaptive Rules:                         | Enabled                                                                                                                                              |
| Maximum Message Size to Scan:           | 3M                                                                                                                                                   |
| Receive Emailed Alerts:                 | No                                                                                                                                                   |
| Web Interaction Tracking                | Enabled<br><small>To track URLs due to Policy rewrites, you have to enable Web Interaction Tracking at Security Services &gt; URL Filtering.</small> |
| <a href="#">Edit Global Settings...</a> |                                                                                                                                                      |

(“3M”). Ensure Adaptive Rules is Enabled and Web Interaction Tracking (URL Click-tracking) is Enabled. The ESA can “rewrite” URLs if they are deemed malicious, suspect, or Phishing. This URL rewrite ability is built in to Content Filters and Outbreak Filters. If you want to see who has clicked on the URLs rewritten within the Outbreak Filters engine, you must enable the Web Interaction Tracking here. Tracking for Content Filters rewrites are enabled when you enable Web Interaction Tracking within URL Filtering setup itself.

**j) Ensure SenderBase is Enabled**

*Security Services > SenderBase*

Ensure that Share Settings has been Enabled. This gathers limited data on email flow to improve efficacy. The data is anonymized and used in aggregate with data from other sources to identify and stop email threats. This does improve the ability to identify and stop threat email based on the email flow across your appliance.

**k) Enable Centralized Reporting**

*Security Services > Reporting*

Change the value from Local Reporting to Centralized Reporting.

**l) Enable Centralized Message Tracking**

*Security Services > Message Tracking*

Click Enable button and then click the Centralized Tracking radio button. Do not save tracking information for rejected connections.

**m) Enable Policy Virus and Outbreak Quarantines**

*Security Services > Policy Virus and Outbreak Quarantines*



## ESA/SMA INSTALLATION AND BEST PRACTICES

You cannot enable this until you have enabled on the SMA appliance and configured the SMA to communicate with the ESA. We will be doing this during the next section.

### n) Enable External Spam Quarantine

*Security Services > Spam Quarantine*

Click the Configure button. Enable and then provide any text string for a name. Put in the IP address of the SMA appliance. Be sure to leave the Port to 6025. Do not enable Safelist/Blocklist.

Name: ExternalSpamQuarantine

IP Address: 10.0.1.36

Port: 6025

## 3. Connecting the ESA and SMA

### Step A: Configure the SMA to provide services for the ESA.

*Management Appliance > Centralized Services > Security Appliances*

Click the Add Email Appliance button. Put in a Appliance Name: like “esa1”, and the IP address for the ESA1 appliance, then check all checkboxes for Spam Quarantine, PVO, Centralized Reporting, and Centralized Message Tracking. Then click the Establish Connection button. Provide the “admin” username and password. This allows the two appliances to share SSH fingerprints. This allows you to change passwords on the ESA, for example, in the future, without having to worry about this setting — so it doesn’t save the admin/pwd.

Submit and Commit.

### Step B: Run the Migration Wizard

*On the SMA, Management Appliance > Centralized Services > Policy Virus and Outbreak Quarantines*

You should notice the “Launch Migration Wizard” button can now be clicked.

Click that button and select “Automatic” radio button on the Configuration Migration panel that follows.

Then you’ll be presented with a list of Quarantines that will be migrated. In this case, no data since this is a new install. Click Next and then Submit and Commit.

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Step C: Enable PVO on the ESA

On the ESA, *Security Services > Policy Virus and Outbreak Quarantines*

Click the Enable button and accept the values that are pre-populated. Click Submit and Commit.

#### 4. Message Filters

Message filters are very similar to the more familiar “Content Filters” that are commonly used in the GUI. Message filters can only be implemented from the console (command line). You should read about “message splintering” in the ESA User Guide and you’ll get a better understanding of why we have Message Filters and also have Content Filters.

Here are some Message Filters that are considered Best Practices that you should consider implementing.

Below the list of message filters you will then see a sample of how to create a message filter (which can only be done on the CLI). Note the Y for Active and Y for Valid.

#### Best Practices Message Filters:

Filter 1: addHeaders (the name can be whatever you want)

This message filter will simply add headers to all “Incoming” messages. These headers are useful when trying to research how an email that is in your Inbox traversed the ESA.

```
addHeaders:
if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Filter 2: wqNotification###

These filters will alert you when the appliance work-queue is starting to build. Once the number of messages in the queue reach 400 you will receive and email alert. As the queue climbs and reaches 600, you receive another. Let’s say the queue builds to 620 messages in the queue. At that point you would have received 2 alerts. As the ESA processes the email and the queue goes down, when it reaches 600 again (going down this time), you will receive another alert. Like wise as it goes down to 400.

You can change these from 400, 600, 800 to whatever values fit your needs — or even add more work queue alerts.

## ESA/SMA INSTALLATION AND BEST PRACTICES

```
wqNotification400:   if workqueue-count == 400
{
    notify ("admin@somelocaladdress.com", "Email Security Appliance has workqueue hit 400");
}

wqNotification600:   if workqueue-count == 600
{
    notify ("admin@somelocaladdress.com", "Email Security Appliance has workqueue hit 600");
}

wqNotification800:   if workqueue-count == 800
{
    notify ("admin@somelocaladdress.com", "Email Security Appliance has workqueue hit 800");
}
```

### Optional Message Filters:

#### Optional Filter 1: no\_domain\_spoofing

This filter is designed to offer spoofing protection. This filter will quarantine incoming email that has a Mail From with your domain. If you use this filter, the “SpoofMail” quarantine would need to be created on the SMA.

```
no_domain_spoofing:
if ((sendergroup != "RELAYLIST") AND (mail-from == "@sectest\\.net"))
{
    quarantine('SpoofMail');
}
```

An alternative method which actually allows two Sending IP addresses to Spoof.

```
no_domain_spoofing:
if ((sendergroup != "RELAYLIST") AND (mail-from == "@sectest\\.net"))
{
    if ((remote-ip != "1.2.3.4") AND (remote-ip != "8.9.10.11"))
    {
        quarantine('SpoofMail');
    }
}
```

#### Optional Filter 2: spf\_helo\_fail

Notify the sender that SPF is failing for their domain.

```
spf_helo_fail:
if (spf-status("helo") == "Fail")
{
    notify ("$EnvelopeSender", "$Subject", "SpamFilter@domain.com", "SPF_Fail_HELO");
    drop();
}
```

#### Optional Filter 3: sourceRouted

This filter bounces emails messages with email addresses using %, extra @, and ! characters:

```
user%otherdomain@validdomain
user@otherdomain@validdomain:
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

```
domain!user@validdomain
```

Cisco appliances are not susceptible to these third party relay hacks that are often used to exploit traditional Sendmail/Qmail systems. As many of these symbols (for example %) can be part of a perfectly legal email address, Cisco appliances will accept these as valid addresses, verify them against the configured recipient lists, and pass them on to the next internal server. Cisco appliances do not relay these messages to the world.

These filters are put in place to protect users who may have open-source MTAs that are misconfigured to allow relay of these types of messages.

```
sourceRouted:
if (rcpt-to == "(%|@|!)(.*)@")
{ bounce(); }
```

### Optional Filter 4: blank\_CC

This message filter will replace Credit Card numbers with XXXX-XXXX-XXXX-XXXX

```
blank_CC:
if body-contains("*credit", 1)
{
    edit-body-text("(?:4[0-9]{12}(?:[0-9]{3})?)5[1-5][0-9]{14}|6(?:011|5[0-9][0-9])[0-9]{12}|3[47]
[0-9]{13}|3(?:0[0-5]|[68][0-9])[0-9]{11}|(?:2131|1800|35\d{3})\d{11})", "XXXX-XXXX-XXXX-XXXX");
}
```

### Optional Filter 5: strip\_all\_dangerous

Drop all attachments on messages that have a filename that match the given regular expression. Archive file attachments (zip, tar) will be dropped if they contain a file that matches.

```
strip_all_dangerous: if (true) {
    drop-attachments-by-name('(?!)\.(pif|exe|scr|msi|java|dll|com)$');
}
```

### Optional Filter 6: strip\_inbound\_exec

Drop all attachments on messages that have a MIME type, determined by either the given MIME type or the file extension. Archive file attachments (zip, tar) will be dropped if they contain a file that matches.

```
strip_inbound_exec: if (sendergroup != "RELAYLIST") {
    drop-attachments-by-filetype ('Executable');
}
```

### Optional Filter 7: high\_volume

## ESA/SMA INSTALLATION AND BEST PRACTICES

High Volume Mail (HVM) message filter can be used on Inbound and Outbound email. HVM is implemented by using the “header-repeats” rule in a message filter. The header-repeats rule evaluates to true if at a given point in time, a specified number of messages:

- With same subject are detected in the last one hour.
- From same envelope sender are detected in the last one hour.

You can use this rule to detect high volume emails. For example, political campaigns through certain websites may send out emails to organizations in high volumes. Anti-spam engines treat such emails as clean, and do not stop the delivery of these emails.

The syntax of this rule is:

```
header-repeats (<target>, <threshold> [, <direction>])
```

In the following example, at any given point in time, if the filter detects *x* or more incoming messages with identical subject in the last one hour, the subsequent messages with identical subject are sent to Policy quarantine.

```
high_volume:
if header-repeats('subject', X, 'incoming') { quarantine('Policy');}
```

In the following example, at any given point in time, if the filter detects *x* or more outgoing messages from same envelope sender in the last one hour, the subsequent messages from the same envelope sender are dropped and discarded.

```
high_volume:
if header-repeats('mail-from', X, 'outgoing') {drop();}
```

In the following example, at any given point in time, if the filter detects *x* or more incoming or outgoing messages with identical subject in the last one hour, the administrator is notified for every subsequent message with identical subject.

```
high_volume:
if header-repeats('subject', X) {notify('admin@xyz.com');}
```

Here is an example of implementing one of the message filters. You simply paste the message filter in and put a period on a line by itself to indicate the end of the filter.

```
esa1.sectest.net> filters
```

```
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[> new
```

```
Enter filter script. Enter '.' on its own line to end.
addHeaders: if (true)
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
.
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

```
insert-header("X-IronPort-MID", "$MID");
insert-header("X-IronPort-Reputation", "$Reputation");
insert-header("X-IronPort-Listener", "$RecvListener");
insert-header("X-IronPort-SenderGroup", "$Group");
insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

.  
1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.
  - DELETE - Remove a filter.
  - IMPORT - Import a filter script from a file.
  - EXPORT - Export filters to a file
  - MOVE - Move a filter to a different position.
  - SET - Set a filter attribute.
  - LIST - List the filters.
  - DETAIL - Get detailed information on the filters.
  - LOGCONFIG - Configure log subscriptions used by filters.
  - ROLLOVERNOW - Roll over a filter log file.
- [> list

```
Num Active Valid Name
1 Y Y addHeaders
```

Choose the operation you want to perform:

- NEW - Create a new filter.
  - DELETE - Remove a filter.
  - IMPORT - Import a filter script from a file.
  - EXPORT - Export filters to a file
  - MOVE - Move a filter to a different position.
  - SET - Set a filter attribute.
  - LIST - List the filters.
  - DETAIL - Get detailed information on the filters.
  - LOGCONFIG - Configure log subscriptions used by filters.
  - ROLLOVERNOW - Roll over a filter log file.
- [>

esa1.sectest.net> commit

Please enter some comments describing your changes:

[>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue May 26 16:33:25 2015 CDT  
esa1.sectest.net>

### 5. Connection-Level Settings

When any device makes a port 25 SMTP connection to the Cisco ESA (for Inbound email delivery or Outbound relaying) the ESA will look at various aspects of the layer-4 TCP/25 connection request and associate that connection to a row in the HAT table. These “rows” are called SenderGroups.

#### *Mail Policies > HAT Overview*

The default HAT table looks like this — note the “Listener” is called “BidirectionalMail” since we customized the name earlier in this section under *Network > Listeners*

### HAT Overview

**Find Senders**

Find Senders that Contain this Text:  **Find**

---

**Sender Groups (Listener: BidirectionalMail 10.0.1.37:25 )**

**Add Sender Group...** **Import HAT...**

| Order | Sender Group | SenderBase™ Reputation Score (?) |    |    |    |       |   |   |   |   |   |     | Mail Flow Policy | Delete |           |  |
|-------|--------------|----------------------------------|----|----|----|-------|---|---|---|---|---|-----|------------------|--------|-----------|--|
|       |              | -10                              | -8 | -6 | -4 | -2    | 0 | 2 | 4 | 6 | 8 | +10 |                  |        |           |  |
| 1     | RELAYLIST    |                                  |    |    |    |       |   |   |   |   |   |     |                  |        | RELAYED   |  |
| 2     | WHITELIST    |                                  |    |    |    |       |   |   |   |   |   |     |                  |        | TRUSTED   |  |
| 3     | BLACKLIST    | =====                            |    |    |    |       |   |   |   |   |   |     |                  |        | BLOCKED   |  |
| 4     | SUSPECTLIST  |                                  |    |    |    | ===== |   |   |   |   |   |     |                  |        | THROTTLED |  |
| 5     | UNKNOWNLIST  |                                  |    |    |    |       |   |   |   |   |   |     | =====            |        | ACCEPTED  |  |
|       | ALL          |                                  |    |    |    |       |   |   |   |   |   |     |                  |        | ACCEPTED  |  |

**Edit Order...** **Export HAT...**

Key:

You can see the rows of SenderGroups and to the right, you see the “Mail Flow Policy” column. Before we modify the SenderGroup table, let’s first modify the Mail Flow Policy actions.

*Mail Policies > Mail Flow Policies*

The default Mail Flow Policies table looks like this:

### Mail Flow Policies

**Policies (Listener: BidirectionalMail 10.0.1.37:25 )**

**Add Policy...**

| Policy Name               | Behavior | Delete |
|---------------------------|----------|--------|
| ACCEPTED                  | Accept   |        |
| BLOCKED                   | Reject   |        |
| RELAYED                   | Relay    |        |
| THROTTLED                 | Accept   |        |
| TRUSTED                   | Accept   |        |
| Default Policy Parameters |          |        |

#### Modifications to the Mail Flow Policy table:

This section will cover the following Best Practices changes to the Mail Flow Policies table:

- a) Modifications to the “Default Policy Parameters”.
- b) Reviewing the ACCEPTED — which should be just like the default.
- c) Modifications to RELAYED.

## ESA/SMA INSTALLATION AND BEST PRACTICES

- d) Modifications to THROTTLED
- e) Modifications to TRUSTED
- f) Create TRUSTED\_NOSBRS\_SPAMCHECK

### a) Modifications to the “Default Policy Parameters” Mail Flow Policy

It is best to set the “Default Policy Parameters” and then inherit as much as possible into the other Mail Flow Policies.

Click on the hypertext “Default Policy Parameters”.

Best Practices settings are:

Section: Default Settings (the top portion)

Max Concurrent Connections From a Single IP: 10

Max Messages Per Connection: 10

Max Recipients Per Message: 50 (some organizations use a much higher value)

Max Message Size: 20M (set this to the max size your email allows Inbound)

| Default Settings |                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Connections:     | Max. Messages Per Connection: <input type="text" value="10"/>                                                                             |
|                  | Max. Recipients Per Message: <input type="text" value="50"/>                                                                              |
|                  | Max. Message Size: <input type="text" value="20M"/><br><small>(add a trailing K for kilobytes; M for megabytes)</small>                   |
|                  | Max. Concurrent Connections From a Single IP: <input type="text" value="10"/>                                                             |
| SMTP:            | Custom SMTP Banner Code: <input type="text" value="220"/>                                                                                 |
|                  | Custom SMTP Banner Text: <input type="text"/>                                                                                             |
|                  | Custom SMTP Reject Banner Code: <input type="text" value="554"/>                                                                          |
|                  | Custom SMTP Reject Banner Text: <input type="text"/>                                                                                      |
|                  | Override SMTP Banner Hostname: <input checked="" type="radio"/> Use Hostname from Interface<br><input type="radio"/> <input type="text"/> |



# ESA/SMA INSTALLATION AND BEST PRACTICES

## Section: Mail Flow Limits

| Mail Flow Limits                            |                                                                           |                                                                                                                                                                                                                                                                      |
|---------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rate Limit for Hosts:                       | Max. Recipients Per Hour:                                                 | <input checked="" type="radio"/> Unlimited<br><input type="radio"/> <input type="text"/>                                                                                                                                                                             |
|                                             | Max. Recipients Per Hour Code:                                            | <input type="text" value="452"/>                                                                                                                                                                                                                                     |
|                                             | Max. Recipients Per Hour Text:                                            | <input type="text" value="Too many recipients received this hour"/>                                                                                                                                                                                                  |
| ▼ Rate Limit for Envelope Senders:          | Max. Recipients Per Time Interval:                                        | <input checked="" type="radio"/> Unlimited<br><input type="radio"/> <input type="text" value="100"/> Recipients per <input type="text" value="60"/> Minutes.<br><small>Number of recipients between 1 and 1,000,000 per number of minutes between 5 and 1440</small> |
|                                             | Sender Rate Limit Error Code:                                             | <input type="text" value="452"/>                                                                                                                                                                                                                                     |
|                                             | Sender Rate Limit Error Text:                                             | <input type="text" value="Too many recipients received from the sender"/>                                                                                                                                                                                            |
|                                             | Exceptions:                                                               | Ignore Rate Limit for Address List: <input type="text" value="None"/>                                                                                                                                                                                                |
| Flow Control:                               | Use SenderBase for Flow Control:                                          | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                                                                                        |
|                                             | Group by Similarity of IP Addresses:                                      | <small>This Feature can only be used if Senderbase Flow Control is off.</small><br><input type="radio"/> Off<br><input type="radio"/> <input type="text"/> (significant bits 0-32)                                                                                   |
| Directory Harvest Attack Prevention (DHAP): | Max. Invalid Recipients Per Hour:                                         | <input type="radio"/> Unlimited<br><input checked="" type="radio"/> <input type="text" value="8"/>                                                                                                                                                                   |
|                                             | Drop Connection if DHAP threshold is Reached within an SMTP Conversation: | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                                                                                        |
|                                             | Max. Invalid Recipients Per Hour Code:                                    | <input type="text" value="550"/>                                                                                                                                                                                                                                     |
|                                             | Max. Invalid Recipients Per Hour Text:                                    | <input type="text" value="Too many invalid recipient"/>                                                                                                                                                                                                              |

## ESA/SMA INSTALLATION AND BEST PRACTICES

Further down, enable DKIM Verification, SPF Verification, DMARC Verification. DMARC aggregate feedback. Bounce Verification: Consider Untagged Bounces to be Valid: No

| Security Features               |                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Spam Detection:                 | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                                                                                                                                            |
| Virus Protection:               | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                                                                                                                                            |
| Encryption and Authentication:  | TLS: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required<br><small>A security certificate/key has not been configured and assigned to a listener. (See Network &gt; Certificates.) Enabling TLS will automatically use the "Demo" certificate/key for listeners.</small> |
|                                 | SMTP Authentication: <input checked="" type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required<br><input type="checkbox"/> Verify Client Certificate                                                                                                                                           |
|                                 | If Both TLS and SMTP Authentication are enabled: <input type="checkbox"/> Require TLS To Offer SMTP Authentication                                                                                                                                                                                                       |
|                                 |                                                                                                                                                                                                                                                                                                                          |
| Domain Key/DKIM Signing:        | <input type="radio"/> On <input checked="" type="radio"/> Off                                                                                                                                                                                                                                                            |
| DKIM Verification:              | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                                                                                                                                            |
|                                 | Use DKIM Verification Profile: <input type="text" value="DEFAULT"/>                                                                                                                                                                                                                                                      |
| S/MIME Decryption/Verification: | <input type="radio"/> On <input checked="" type="radio"/> Off                                                                                                                                                                                                                                                            |
|                                 | Signature After Processing: <input checked="" type="radio"/> Preserve <input type="radio"/> Remove                                                                                                                                                                                                                       |
| S/MIME Public Key Harvesting:   | S/MIME Public Key Harvesting: <input checked="" type="radio"/> Disable <input type="radio"/> Enable                                                                                                                                                                                                                      |
|                                 | Harvest Certificates on Verification Failure: <input checked="" type="radio"/> Disable <input type="radio"/> Enable                                                                                                                                                                                                      |
|                                 | Store Updated Certificate: <input type="radio"/> Disable <input checked="" type="radio"/> Enable                                                                                                                                                                                                                         |
| SPF/SIDF Verification:          | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                                                                                                                                            |
|                                 | Conformance Level: <input type="text" value="SIDF Compatible"/>                                                                                                                                                                                                                                                          |
|                                 | Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used: <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                                                                         |
|                                 | HELO Test: <input type="radio"/> Off <input checked="" type="radio"/> On                                                                                                                                                                                                                                                 |
| DMARC Verification              | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                                                                                                                                                                                                            |
|                                 | Use DMARC Verification Profile: <input type="text" value="DEFAULT"/>                                                                                                                                                                                                                                                     |
|                                 | DMARC Feedback Reports: <input checked="" type="checkbox"/> Send aggregate feedback reports<br><small>* DMARC reporting message must be DMARC compliant.<br/>                     * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies &gt; Destination Controls.</small>     |
| Bounce Verification:            | Consider Untagged Bounces to be Valid: <input type="radio"/> Yes <input checked="" type="radio"/> No                                                                                                                                                                                                                     |
|                                 | <small>(Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.)</small>                                                                                                                                                                                              |

Bounce Verification: We made a change to Bounce Verification above. We will need to make two additional configuration changes to finish Bounce Verification setup. We will do those two changes after we finish with Mail Flow and HAT SenderGroup changes.

Enable Sender Verification

Click Submit.

| Sender Verification                             |                                                                                                                                       |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Envelope Sender DNS Verification:               | <input checked="" type="radio"/> On <input type="radio"/> Off                                                                         |
| Malformed Envelope Senders:                     | SMTP Code: <input type="text" value="553"/><br>SMTP Text: <input type="text" value="#5.5.4 Domain required for sender address"/>      |
| Envelope Senders whose domain does not resolve: | SMTP Code: <input type="text" value="451"/><br>SMTP Text: <input type="text" value="#4.1.8 Domain of sender address &lt;\$Envelope"/> |
| Envelope Senders whose domain does not exist:   | SMTP Code: <input type="text" value="553"/><br>SMTP Text: <input type="text" value="#5.1.8 Domain of sender address &lt;\$Envelope"/> |
| Use Sender Verification Exception Table:        | <input type="radio"/> On <input checked="" type="radio"/> Off                                                                         |

**b) Reviewing ACCEPTED Mail Flow Policy**

Click on the ACCEPTED policy name.

You should review it to ensure that all settings in ACCEPTED “Use Default”. No changes should be required because we want the ACCEPTED mail flow policy to act just like the Default. Click on Cancel (or Submit if you did make changes for some reason).

Click on the BLOCKED policy name. Note that the “Connection Behavior” is “Reject”. This means that the ESA will engage with the 3-way TCP handshake and form the Layer-4 connection and enter into the layer-7 (Application Layer) EHLO conversation but as soon as the ESA receives a RCPT TO address it sends the “Custom SMTP Banner Code and Text specified in this Mail Flow Policy. If you click the Connection Behavior pulldown button at the top you see there is a TCP Refuse option which configures the ESA to not even send the SYN/ACK response back to the SYN packet received from the remote MTA. Years ago this was the default value but we have migrated to the “Reject” to provide formal feedback to the bad sender that we are not going to accept your connection due to bad reputation. This way they know why they are being blocked. This normally leads to their Email Admin calling you and trying to talk you in to adding them to your WHITELIST to bypass reputation score blocking — please try to prevent from doing this. Tell them to stop sending spam and their email reputation will start improving in a day or two.

**c) Modifications to RELAYED**

Click on RELAYED

This is used for devices that send Outbound. When we look further into the HAT in the next few paragraphs, you’ll note that RELAYLIST SenderGroup implements this

## ESA/SMA INSTALLATION AND BEST PRACTICES

RELAYED Mail Flow Policy. Your Exchange Hubs (or Exchange Servers) and other internal systems that are allowed to send Outbound email will be using this.

Make the following changes from the default:

- Max Messages Per Connection: 1000
- Max Recipients Per Message: 500
- Max Message Size: <set to customer limit for max Outbound message sizes allowed>
- Flow Control: Use SenderBase for Flow Control: Off
- Directory Harvest Attack Prevention: set this to Unlimited radio button
- DKIM Verification: Off
- SPF Verification: Off
- DMARC Verification: Off
- Bounce Verification: Consider Untagged Bounces to be Valid: Yes (This is not really required since “Smart exceptions to Bounce Verification” is enabled by default. However, I like to clearly configure this policy to reflect the behavior.
- Sender Envelope Verification: Off

Submit changes

### d) Modifications to THROTTLED

Click on THROTTLED

Make the following changes from the default:

- Max Messages Per Connection: 1
- Max Recipients Per Message: 25
- Max Message Size: Use Default (this should be the size the customer allows Inbound)
- Max Concurrent Connections From a Single IP: 1

Submit changes

### e) Modifications to TRUSTED

The objective for “Trusting” someone is to “bypass” SBRS or SPAM engine. It is not to give the sending MTA superpowers to create a huge number of layer-4 socket connections and not to allow that MTA to send 5000 messages per connection and not to allow them to send to 5000 recipients per connection. Though this “TRUSTED” Mail Flow Policy has those settings, you should change these settings to normal settings. Your objective is to bypass SBRS and SPAM and not to give them super powers.

Click on TRUSTED

Rename this Mail Flow Policy and set everything to Use Default:

## ESA/SMA INSTALLATION AND BEST PRACTICES

- Rename/Name: TRUSTED\_SPAMCHECK
- Max Messages Per Connection: Use Default (10)
- Max Recipients Per Message: Use Default (50)
- Max Concurrent Connections From a Single IP: Use Default (1)
- Flow Control: Use SenderBase for Flow Control: Use Default (On)
- Directory Harvest Attack Prevention: Max Invalid Recipients Per Hour: Use Default (8)
- Spam Detection: Use Default (On)
- DKIM Verification: Use Default (On)
- SPF Verification: Use Default (On)
- DMARC Verification: Use Default (On)
- Bounce Verification: Use Default (On)
- Sender Envelope Verification: Use Default (On)

After all the changes have been made, all settings should be set to Use Default

### f) Create TRUSTED\_NOSPAM

Click the Add Policy button.

Name, then turn OFF Spam Detection and then all other settings should be “Use Default” — already set.

- Name: TRUSTED\_NOSBRS\_NOSPAM
- Spam Detection: Off

All other settings should be “Use Default”  
Submit changes. Commit changes.

The Mail Flow Policies table should look like this:

| Policy Name               | Behavior | Delete |
|---------------------------|----------|--------|
| ACCEPTED                  | Accept   | ?      |
| BLOCKED                   | Reject   | 🗑️     |
| RELAYED                   | Relay    | 🗑️     |
| THROTTLED                 | Accept   | 🗑️     |
| TRUSTED_NOSPAM            | Accept   | 🗑️     |
| TRUSTED_SPAMCHECK         | Accept   | 🗑️     |
| Default Policy Parameters |          |        |

**HAT Table Changes: [Go back to HAT Overview](#)**

*Mail Policies > HAT Overview*

The default HAT table should now look like this:

| Order | Sender Group | SenderBase™ Reputation Score ? |    |    |       |    |   |   |   |   |   |       | Mail Flow Policy | Delete            |  |
|-------|--------------|--------------------------------|----|----|-------|----|---|---|---|---|---|-------|------------------|-------------------|--|
|       |              | -10                            | -8 | -6 | -4    | -2 | 0 | 2 | 4 | 6 | 8 | +10   |                  |                   |  |
| 1     | RELAYLIST    |                                |    |    |       |    |   |   |   |   |   |       |                  | RELAYED           |  |
| 2     | WHITELIST    |                                |    |    |       |    |   |   |   |   |   |       |                  | TRUSTED_SPAMCHECK |  |
| 3     | BLACKLIST    | =====                          |    |    |       |    |   |   |   |   |   |       |                  | BLOCKED           |  |
| 4     | SUSPECTLIST  |                                |    |    | ===== |    |   |   |   |   |   |       |                  | THROTTLED         |  |
| 5     | UNKNOWNLIST  |                                |    |    |       |    |   |   |   |   |   | ===== |                  | ACCEPTED          |  |
|       | ALL          |                                |    |    |       |    |   |   |   |   |   |       |                  | ACCEPTED          |  |

Key:  Custom  Default

We are going to do the following:

- Rename WHITELIST to WHITELIST\_NOSBRS\_SPAMCHECK
- Create WHITELIST\_NOSBRS\_NOSPAM
- Create WHITELIST\_SBRS\_NOSPAM
- Throttle MTAs which have no SBRS (Reputation Score)
- Rename UNKNOWNLIST to GOODSENDERS

**a) Rename WHITELIST to WHITELIST\_NOSBRS\_SPAMCHECK**

Click on WHITELIST and then click on Edit Settings.

- Name: WHITELIST\_NOSBRS\_SPAMCHECK
- Order: 2
- Comment: Bypass SBRS but SPAM Check - Keep above BLACKLIST SenderGroup
- Policy: TRUSTED\_SPAMCHECK

Submit and then “Back to HAT Overview” button

**b) Create WHITELIST\_NOSBRS\_NOSPAM**

Click the “Add Sender Group..” button.

- Name: WHITELIST\_NOSBRS\_NOSPAM
- Order: 3
- Comment: Bypasses SBRS and SPAM - keep this above BLACKLIST SenderGroup
- Policy: TRUSTED\_NOSPAM

Click the “Submit” button and then “Back to HAT Overview” button.

## ESA/SMA INSTALLATION AND BEST PRACTICES

**c) Create WHITELIST\_SBRS\_NOSPAM**

Click the “Add Sender Group..” button.

- Name: WHITELIST\_SBRS\_NOSPAM
- Order: 5
- Comment: Bypasses SPAM - keep this below BLACKLIST SenderGroup
- Policy: TRUSTED\_SBRS\_NOSPAM

Click the “Submit” button and then “Back to HAT Overview” button.

**d) Throttle MTAs which have no SBRS (Reputation Score)**

Click the SUSPECTLIST. Edit Settings.

Click (Enable) the check-box for “Include SBRS Scores of None”.

Click the “Submit” button and then click “Back to HAT Overview” button.

**e) Rename UNKNOWNLIST to GOODSENDERS**

Click the UNKNOWNLIST. Edit Settings.

- Name/Rename: GOODSENDERS
- Uncheck (Disable) the “Include SBRS Scores of None” checkbox.

Click the “Submit” button and then “Back to HAT Overview” button.

Commit changes.

The HAT Table should now look like this:

| Sender Groups (Listener: BidirectionalMail 10.0.1.37:25) |                            |                                |    |    |       |       |                  |                   |    |   |
|----------------------------------------------------------|----------------------------|--------------------------------|----|----|-------|-------|------------------|-------------------|----|---|
| Add Sender Group... Import HAT...                        |                            |                                |    |    |       |       |                  |                   |    |   |
| Order                                                    | Sender Group               | SenderBase™ Reputation Score ? |    |    |       |       | Mail Flow Policy | Delete            |    |   |
|                                                          |                            | -10                            | -8 | -6 | -4    | -2    |                  |                   | 0  | 2 |
| 1                                                        | RELAYLIST                  |                                |    |    |       |       |                  | RELAYED           | 🗑️ |   |
| 2                                                        | WHITELIST_NOSBRS_SPAMCHECK |                                |    |    |       |       |                  | TRUSTED_SPAMCHECK | 🗑️ |   |
| 3                                                        | WHITELIST_NOSBRS_NOSPAM    |                                |    |    |       |       |                  | TRUSTED_NOSPAM    | 🗑️ |   |
| 4                                                        | BLACKLIST                  | =====                          |    |    |       |       |                  | BLOCKED           | 🗑️ |   |
| 5                                                        | WHITELIST_SBRS_NOSPAM      |                                |    |    |       |       |                  | TRUSTED_SPAMCHECK | 🗑️ |   |
| 6                                                        | SUSPECTLIST                |                                |    |    | ===== |       |                  | THROTTLED         | 🗑️ |   |
| 7                                                        | GOODSENDERS                |                                |    |    |       | ===== |                  | ACCEPTED          | 🗑️ |   |
|                                                          | ALL                        |                                |    |    |       |       |                  | ACCEPTED          |    |   |

Edit Order... Export HAT...

### 6. Bounce Verification and Destination Controls

This section will step you through setup of Bounce Verification and other Destination Controls.

When an email is sent through an ESA with bounce verification enabled, your ESA rewrites the Envelope Sender address in the message. For example, MAIL FROM: [joe@example.com](mailto:joe@example.com) becomes MAIL FROM: [prvs=joe=123ABCDEFGH@example.com](mailto:prvs=joe=123ABCDEFGH@example.com). The 123... string in the example is the bounce verification tag that is added to the Envelope Sender as it is sent by your ESA appliance. If the message bounces, the Envelope Recipient address in the bounced message will include the bounce verification tag which lets the ESA know that it is a legitimate bounced message.

You can enable or disable bounce verification tagging system-wide as a default. You can also enable or disable bounce verification tagging for specific domains. In most deployments it is enabled by default for all domains.

#### Bounce Verification Setup

Step 1: Navigate to *Mail Policies > Bounce Verification* and click “New Key” button. Enter any arbitrary text to be used as as the key in encoding and decoding address tags. For example: “uncTarheel”.

Step 2: Navigate to *Mail Policies > Destination Controls* and click on the “Default”. Configure Bounce Verification: Perform address tagging: Yes

Submit and Commit changes

#### Destination Control Good Sender Rate Limiting

If a large amount of email was sent to a particular email domain in a short time, the receiving servers may temporarily defer the email traffic by denying the email with a SMTP 450 response code and a message saying you are sending too quickly.

Google and Yahoo are two such companies. They have published guides on how fast “Senders” should send email to them.

Google:

<https://support.google.com/a/answer/1366776?hl=en>

Yahoo:

<https://help.yahoo.com/kb/mail/SLN3433.html>

Let’s setup these Destination controls for Yahoo and Gmail.



## ESA/SMA INSTALLATION AND BEST PRACTICES

### Mail Policies > Destination Controls

Yahoo: Click the Add Destination button

- Destination: yahoo.com
- IP Address Preference: IPv4 Preferred
- Concurrent Connections: Max of 20
- Max Messages Per Connection: 5
- Recipients: Max of 20 per 1 minute
- Bounce Verification: Perform address tagging: Default (Yes)

| Destination Controls   |                                                                                                                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination:           | yahoo.com                                                                                                                                                                                                                                                                                 |
| IP Address Preference: | IPv4 Preferred                                                                                                                                                                                                                                                                            |
| Limits:                | Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> (between 1 and 1,000)                                                                                                                         |
|                        | Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="5"/> (between 1 and 1,000)                                                                                                                  |
|                        | Recipients: <input type="radio"/> Use Default (No Limit) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> per <input type="text" value="1"/> minutes<br><small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small> |
|                        | Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway<br><small>(recommended if Virtual Gateways are in use)</small>                                                                                                    |
| TLS Support:           | Default (None)<br><small>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the certconfig command.)</small>                                     |
| Bounce Verification:   | Perform address tagging: <input checked="" type="radio"/> Default (Yes) <input type="radio"/> No <input type="radio"/> Yes<br><small>Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</small>                                   |
| Bounce Profile:        | Default<br><small>Bounce Profile can be configured at Network &gt; Bounce Profiles.</small>                                                                                                                                                                                               |

## ESA/SMA INSTALLATION AND BEST PRACTICES

*Gmail:* Click the Add Destination button

- Destination: gmail.com
- IP Address Preference: IPv4 Preferred
- Concurrent Connections: Max of 20
- Max Messages Per Connection: 5
- Recipients: Max of 180 per 1 minute
- Bounce Verification: Perform address tagging: Default (Yes)

| Edit Destination Controls |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination:              | <input type="text" value="gmail.com"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| IP Address Preference:    | <input type="button" value="IPv4 Preferred"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Limits:                   | <div style="margin-bottom: 5px;">                     Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> (between 1 and 1,000)                 </div> <div style="margin-bottom: 5px;">                     Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="5"/> (between 1 and 1,000)                 </div> <div style="margin-bottom: 5px;">                     Recipients: <input type="radio"/> Use Default (No Limit) <input checked="" type="radio"/> Maximum of <input type="text" value="180"/> per <input type="text" value="1"/> minutes<br/> <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small> </div> <div>                     Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway<br/> <small>(recommended if Virtual Gateways are in use)</small> </div> |
| TLS Support:              | <input type="button" value="Default (None)"/><br><small>A security certificate/key has not yet been configured. Enabling TLS will automatically enable the "Demo" certificate/key. (To configure a different certificate/key, start the CLI and use the <code>certconfig</code> command.)</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Bounce Verification:      | Perform address tagging: <input checked="" type="radio"/> Default (Yes) <input type="radio"/> No <input type="radio"/> Yes<br><small>Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Bounce Profile:           | <input type="button" value="Default"/><br><small>Bounce Profile can be configured at Network &gt; Bounce Profiles.</small>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Make the following change to the Default destination Control:

IP Address Preference: IPv4 Preferred

This is the final Destination Controls table.

| Destination Control Table                                                                                                                              |                       |                                                                                   |             |                       |                | Items per page <input type="button" value="20"/> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------|-------------|-----------------------|----------------|--------------------------------------------------|
| <input type="button" value="Add Destination..."/>                                                                                                      |                       | <input type="button" value="Import Table"/>                                       |             |                       |                |                                                  |
| Domain ▲                                                                                                                                               | IP Address Preference | Destination Limits                                                                | TLS Support | Bounce Verification * | Bounce Profile | All <input type="checkbox"/> Delete              |
| gmail.com                                                                                                                                              | IPv4 Preferred        | 20 concurrent connections, 5 messages per connection, 180 recipients in 1 minutes | Default     | Default               | Default        | <input type="checkbox"/>                         |
| yahoo.com                                                                                                                                              | IPv4 Preferred        | 20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes  | Default     | Default               | Default        | <input type="checkbox"/>                         |
| Default                                                                                                                                                | IPv4 Preferred        | 500 concurrent connections, 50 messages per connection, No recipient limit        | None        | On                    | Default        |                                                  |
| <input type="button" value="Export Table"/>                                                                                                            |                       | <input type="button" value="Delete"/>                                             |             |                       |                |                                                  |
| <small>* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</small> |                       |                                                                                   |             |                       |                |                                                  |

## ESA/SMA INSTALLATION AND BEST PRACTICES

### 7. Incoming Mail Policies

When a MTA sender is sending email to your Cisco ESA, that MTA will make a TCP port 25 SMTP connection to your ESA. That “MTA Sender” can be your Exchange server that is connecting to your Cisco ESA to send Outbound email (relay) through your Cisco ESA or that “MTA Sender” could be some remote MTA out on the Internet that is sending Inbound email to your company. The Cisco ESA matches the TCP “connection” to a SenderGroup row in the HAT table (we discussed the HAT table in the previous section).

When the TCP connection is matched to a SenderGroup the Connection behavior is defined by the settings found in the Mail Flow Policy specified for that SendGroup row. Inside the Mail Flow Policy (at the top) is a Connection Behavior pulldown button.

If the Connection Behavior is “Relay”, then any email received on that flow will be considered Outgoing email to the Cisco ESA and it will go through the Mail Policies > Outgoing Mail Policies work queue. Typically only the RELAYLIST HAT SenderGroup uses the RELAYED Mail Flow Policy implements the “Relay” Connection Behavior.

If the Connection Behavior is Accept, then any email received on that flow will be considered Incoming email to the Cisco ESA and those emails will go through the Mail Policies > Incoming Mail Policies work queue.

#### Setup the Best Practices for the Incoming Mail Policies

*Mail Policies > Incoming Mail Policies*

Here is the default Incoming Mail Policies table.

| Policies |                |           |                                                                              |                                                                                            |          |                 |                                 |        |
|----------|----------------|-----------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------|-----------------|---------------------------------|--------|
| Order    | Policy Name    | Anti-Spam | Anti-Virus                                                                   | Advanced Malware Protection                                                                | Graymail | Content Filters | Outbreak Filters                | Delete |
|          | Default Policy | Disabled  | Sophos<br>Encrypted: Deliver<br>Unscannable: Deliver<br>Virus Positive: Drop | File Reputation<br>Unscannable: Deliver<br>Malware File: Drop<br>Pending Analysis: Deliver | Disabled | Disabled        | Retention Time:<br>Virus: 1 day |        |

Most customers have multiple rows in this table to differentiate mail controls for certain Envelope Senders or Envelope Recipients. You should setup the “Default Policy” first and create additional Incoming Mail Policies (rows) if any exceptions to the Default policy are needed — meaning if you have certain Senders or Recipients that you want a different set of mail controls.

The first step is to configure the Default Policy.

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Anti-Spam

Click on “Disabled” under the Anti-Spam column. Make the following changes as shown in this screenshot. Note that I have enabled “Intelligent Multi-Scan” (IMS) under “Security Services” menu. You may have IronPort Anti-Spam enabled instead of IMS and in that case you would see IronPort Anti-Spam instead of IMS in your configuration panel.

| Anti-Spam Settings                                                                                 |                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy:</b>                                                                                     | Default                                                                                                                                                                                                                                      |
| Enable Anti-Spam Scanning for This Policy:                                                         | <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan<br><i>Spam scanning built on IronPort Anti-Spam.</i><br><input type="radio"/> Disabled                                                                                  |
| <b>Positively-Identified Spam Settings</b>                                                         |                                                                                                                                                                                                                                              |
| Apply This Action to Message:                                                                      | Drop                                                                                                                                                                                                                                         |
| Add Text to Subject:                                                                               | Prepend [SPAM]                                                                                                                                                                                                                               |
| Advanced                                                                                           | Optional settings for custom header and message delivery.                                                                                                                                                                                    |
| <b>Suspected Spam Settings</b>                                                                     |                                                                                                                                                                                                                                              |
| Enable Suspected Spam Scanning:                                                                    | <input type="radio"/> No <input checked="" type="radio"/> Yes                                                                                                                                                                                |
| Apply This Action to Message:                                                                      | Spam Quarantine<br><i>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</i>                                                                                                                        |
| Add Text to Subject:                                                                               | Prepend [SUSPECTED SPAM]                                                                                                                                                                                                                     |
| Advanced                                                                                           | Optional settings for custom header and message delivery.                                                                                                                                                                                    |
| <b>Spam Thresholds</b>                                                                             |                                                                                                                                                                                                                                              |
| <i>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</i> |                                                                                                                                                                                                                                              |
| IronPort Intelligent Multi-Scan:                                                                   | <input type="radio"/> Use the Default Thresholds<br><input checked="" type="radio"/> Use Custom Settings:<br>Positively Identified Spam: Score > 90 (50 - 100)<br>Suspected Spam: Score > 39 (minimum 25, cannot exceed positive spam score) |

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Anti-Virus

Click on the hypertext in the Anti-Virus control cell. Make the following changes as shown in this screenshot.

There are setting under the “Advanced” disclosure triangles but for Incoming Anti-Virus, there are no Advanced settings configured.

| Anti-Virus Settings                                |                                                                                                                                                                                                                                                            |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy:</b>                                     | DEFAULT                                                                                                                                                                                                                                                    |
| <b>Enable Anti-Virus Scanning for This Policy:</b> | <input checked="" type="radio"/> Yes<br><input type="radio"/> No<br><input checked="" type="checkbox"/> Use McAfee Anti-Virus<br><input checked="" type="checkbox"/> Use Sophos Anti-Virus                                                                 |
| <b>Message Scanning</b>                            |                                                                                                                                                                                                                                                            |
|                                                    | Scan for Viruses only <input type="button" value="v"/><br><input type="checkbox"/> Drop infected attachments if a virus is found<br><input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages |
| <b>Repaired Messages:</b>                          |                                                                                                                                                                                                                                                            |
| Action Applied to Message:                         | Deliver As Is <input type="button" value="v"/>                                                                                                                                                                                                             |
| Archive Original Message:                          | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                                                                                              |
| Modify Message Subject:                            | <input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append<br>[WARNING: VIRUS REMOVED]                                                                                                                                 |
|                                                    | <input type="button" value="Advanced"/> Optional settings for custom header and message delivery.                                                                                                                                                          |
| <b>Encrypted Messages:</b>                         |                                                                                                                                                                                                                                                            |
| Action Applied to Message:                         | Deliver As Is <input type="button" value="v"/>                                                                                                                                                                                                             |
| Archive Original Message:                          | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                                                                                              |
| Modify Message Subject:                            | <input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append<br>[WARNING : MESSAGE ENCRYPTED]                                                                                                                            |
|                                                    | <input type="button" value="Advanced"/> Optional settings for custom header and message delivery.                                                                                                                                                          |
| <b>Unscannable Messages:</b>                       |                                                                                                                                                                                                                                                            |
| Action Applied to Message:                         | Deliver As Is <input type="button" value="v"/>                                                                                                                                                                                                             |
| Archive Original Message:                          | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                                                                                              |
| Modify Message Subject:                            | <input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append<br>[WARNING : A/V UNSCANNABLE]                                                                                                                              |
|                                                    | <input type="button" value="Advanced"/> Optional settings for custom header and message delivery.                                                                                                                                                          |
| <b>Virus Infected Messages:</b>                    |                                                                                                                                                                                                                                                            |
| Action Applied to Message:                         | Drop Message <input type="button" value="v"/>                                                                                                                                                                                                              |
| Archive Original Message:                          | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                                                                                              |
| Modify Message Subject:                            | <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append<br>[WARNING: VIRUS DETECTED]                                                                                                                                |
|                                                    | <input type="button" value="Advanced"/> Optional settings for custom header and message delivery.                                                                                                                                                          |

**Advanced Malware Protection**

Click on the hypertext under the Advanced Malware Protection control cell. Make the following changes as show in this screenshot.

| Advanced Malware Protection Settings                |                                                                                                                                                 |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy:                                             | DEFAULT                                                                                                                                         |
| Enable Advanced Malware Protection for This Policy: | <input checked="" type="radio"/> Enable File Reputation<br><input checked="" type="checkbox"/> Enable File Analysis<br><input type="radio"/> No |
| <b>Message Scanning</b>                             |                                                                                                                                                 |
|                                                     | <input checked="" type="checkbox"/> (recommended) Include an X-header with the AMP results in messages                                          |
| <b>Unscannable Attachments:</b>                     |                                                                                                                                                 |
| Action Applied to Message:                          | Deliver As Is                                                                                                                                   |
| Archive Original Message:                           | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                   |
| Modify Message Subject:                             | <input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append                                                  |
|                                                     | [WARNING: ATTACHMENT UNSCANNED]                                                                                                                 |
| Advanced                                            | Optional settings for custom header.                                                                                                            |
| <b>Messages with Malware Attachments:</b>           |                                                                                                                                                 |
| Action Applied to Message:                          | Drop Message                                                                                                                                    |
| Archive Original Message:                           | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                   |
| Drop Malware Attachments:                           | <input type="radio"/> No <input checked="" type="radio"/> Yes                                                                                   |
| Modify Message Subject:                             | <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append                                                  |
|                                                     | [WARNING: MALWARE DETECTED]                                                                                                                     |
| Advanced                                            | Optional settings for custom header.                                                                                                            |
| <b>Messages with File Analysis Pending:</b>         |                                                                                                                                                 |
| Action Applied to Message:                          | Quarantine                                                                                                                                      |
| Archive Original Message:                           | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                   |
| Modify Message Subject:                             | <input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append                                                  |
|                                                     | [WARNING: ATTACHMENT(S) MAY CONT/                                                                                                               |
| Advanced                                            | Optional settings for custom header.                                                                                                            |

**Graymail and Safe Unsubscribe**

In the *Security Services > Graymail Detection* configuration portion of this document we gave a comprehensive description of the Graymail feature and how it works. Here we configure Graymail on the Incoming Mail Policy.

*Mail Policies > Incoming Mail Policies*

Click on the “Disabled” hypertext under the Graymail column.

- Enable Graymail Detection for This Policy: Yes
- Enable Graymail Unsubscribing for this Policy: Yes
- Perform this action for: “All Messages”

Enable Marketing, Social Network, and Bulk Email.

## ESA/SMA INSTALLATION AND BEST PRACTICES

Some organizations elect to set the Apply Action to “Spam Quarantine” for some or all of these categories. In our example, we will Prepend the Subject with the appropriate [MARKETING] / [SOCIAL NETWORK] / [BULK] subject tag and set the Action to “Deliver”.

Here is what the Graymail configuration panel should look like:

| Graymail Settings                                     |                                                                                                                                                 |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy:</b>                                        | DEFAULT                                                                                                                                         |
| <b>Enable Graymail Detection for This Policy:</b>     | <input checked="" type="radio"/> Yes <input type="radio"/> No                                                                                   |
| <b>Enable Graymail Unsubscribing for This Policy:</b> | <input checked="" type="radio"/> Yes <input type="radio"/> No                                                                                   |
|                                                       | Perform this action for: <input checked="" type="radio"/> All Messages <input type="radio"/> Unsigned Messages                                  |
| <b>✓ Action on Marketing Email</b>                    |                                                                                                                                                 |
| Apply this action to Message:                         | Deliver <input type="button" value="v"/><br>Send to Alternate Host (optional): <input type="text"/>                                             |
| Add Text to Subject:                                  | <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append<br><input type="text" value="[MARKETING]"/>      |
| <a href="#">Advanced</a>                              | <i>Optional settings for custom header and message delivery.</i>                                                                                |
| <b>✓ Action on Social Network Email</b>               |                                                                                                                                                 |
| Apply this action to Message:                         | Deliver <input type="button" value="v"/><br>Send to Alternate Host (optional): <input type="text"/>                                             |
| Add Text to Subject:                                  | <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append<br><input type="text" value="[SOCIAL NETWORK]"/> |
| <a href="#">Advanced</a>                              | <i>Optional settings for custom header and message delivery.</i>                                                                                |
| <b>✓ Action on Bulk Email</b>                         |                                                                                                                                                 |
| Apply this action to Message:                         | Deliver <input type="button" value="v"/><br>Send to Alternate Host (optional): <input type="text"/>                                             |
| Add Text to Subject:                                  | <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append<br><input type="text" value="[BULK]"/>           |
| <a href="#">Advanced</a>                              | <i>Optional settings for custom header and message delivery.</i>                                                                                |

Graymail and Safe Unsubscribe has been enabled on the Default Policy for Incoming Mail.

## ESA/SMA INSTALLATION AND BEST PRACTICES


Here is a quick view of what an email will look like that has been marked with an “Safe Unsubscribe” banner at the top:


Reply Reply All Forward  
Sun 5/31/2015 6:34 AM  
Pyramyd Air <sales@pyramydair.com>  
[MARKETING] Welcome to Pyramyd Air!

To Sarah Vale  
If there are problems with how this message is displayed, click here to view it in a web browser.

**Unsubscribe**  
It appears that you have subscribed to commercial messages from this sender. To stop receiving such messages from this sender, please [unsubscribe](#)

Don't forget your coupon code!  
[PyramydAir.Com](#) | [View in browser](#)

Airguns | Specials | New Products | Airsoft Guns | Ammo | Accessories



**SUBSCRIPTION STATUS:  
CONFIRMED**

Now that you're on board you will receive updates on exclusive sales, special promotions, new products and the latest trends.

**10% OFF\*** Take 10% off\* your next purchase by entering code **WELCOME-2015** at checkout

**SHOP NOW**

**GET MESSAGES** *TAILORED TO YOUR INTERESTS*  
Tell us what you want to hear about in the [email preference center](#).

Airguns | Specials | New Products | Airsoft Guns | Ammo | Accessories

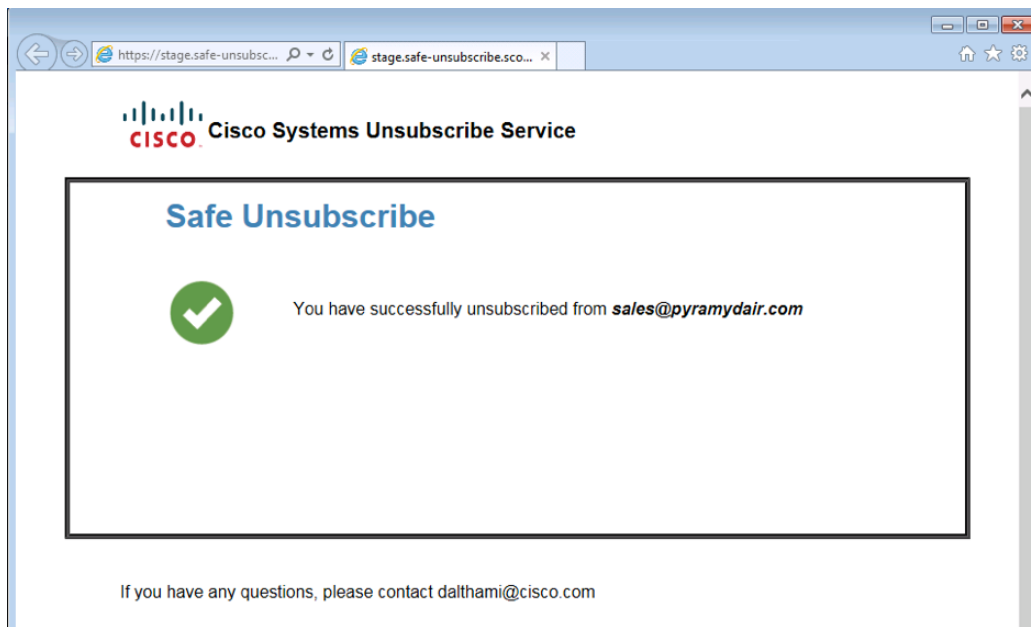


## ESA/SMA INSTALLATION AND BEST PRACTICES

If you hover your mouse over the “unsubscribe” link within the banner, here is an example of the unsubscribe link:



When you click the “unsubscribe” hypertext link in the unsubscribe banner at the top of the email, a browser starts and here is what you see:



## ESA/SMA INSTALLATION AND BEST PRACTICES

### Incoming Content Filters

Content Filters allow you to inspect the many characteristics of the Email and take Actions (or no Action) on the Email. All the things we discuss here about Incoming Content Filters will be directly applicable to Outgoing Content Filters when we cover Outgoing Mail Policies. Once the Incoming Content Filter is created, you apply it to a Incoming Mail Policy. When any Email matches the Content Filter the Monitor>ContentFilters Report on the ESA and SMA will be able to show you all Email that matched any Content Filter. Therefore, even if no Action is taken, it is an excellent way to “Pattern” your email flow — to find out what types of Emails are coming in and going out.

The next steps show you how to implement some Best Practices Incoming Content Filters. The Content Filters we are going to create will have reference a couple of Dictionaries that we have not Imported yet — so we will need to Import those Dictionaries first.

The Actions on some of these Content Filters will be to Quarantine the Email (or a copy of the Email) into designated custom (new) Quarantines that we need to first create on the SMA — since we have enabled Centralized Policy, Virus, and Outbreak Quarantines between the ESA and SMA earlier in this document.

Importing the Dictionaries:

On the ESA appliance, navigate to *Mail Policies > Dictionaries*

Click the “*Import Dictionary*” button on the right side of the page.

Profanity:

- Select “Import from the configuration directory on your IronPort appliance. Select the “profanity.txt” and click “Next”.
- Name: Profanity
- Click the “Match whole words” (VERY IMPORTANT)
- Modify the terms (add new terms or remove unwanted terms)

Sexual Content:

- Select “Import from the configuration directory on your IronPort appliance. Select the “sexual\_content.txt” and click “Next”.
- Name: Sexual\_Content
- Click the “Match whole words” (VERY IMPORTANT)
- Modify the terms (add new terms or remove unwanted terms)

Quarantines: Next we need to create the needed quarantines on the SMA.

On the SMA, navigate to: Email Tab > Message Quarantine > PVO Quarantines

## ESA/SMA INSTALLATION AND BEST PRACTICES

This is what the table should look like before we start. All quarantines are default except the “SpooMail” quarantine. SpooMail was created to support a Message Filter that protects against Spoofed Email that we added earlier in this document.

| Quarantines                          |                             |                           |                                     |                             |      |        |
|--------------------------------------|-----------------------------|---------------------------|-------------------------------------|-----------------------------|------|--------|
| Add Policy Quarantine...             |                             | Search Across Quarantines |                                     |                             |      |        |
| Quarantine Name                      | Type                        | Messages                  | Default Action                      | Last Message Quarantined On | Size | Delete |
| File Analysis                        | Advanced Malware Protection | 0                         | Retain 1 hour then Release          | --                          | 0    |        |
| Outbreak<br>[Manage by Rule Summary] | Outbreak                    | 0                         | Retention Varies<br>Action: Release | --                          | 0    |        |
| Policy                               | Centralized Policy          | 0                         | Retain 10 days then Delete          | --                          | 0    |        |
| SpooMail                             | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| Unclassified                         | Unclassified                | 0                         | Retain 30 days then Release         | --                          | 0    |        |
| Virus                                | Antivirus                   | 0                         | Retain 30 days then Delete          | --                          | 0    |        |

Available space for Policy, Virus & Outbreak quarantines is 149G.

Click the “Add Policy Quarantine” button and Create the below Quarantines to be used by both Inbound Content Filters and Outbound Content Filters.

Here is how your PVO table should look after creating all of the PVO Quarantines.

| Quarantines                          |                             |                           |                                     |                             |      |        |
|--------------------------------------|-----------------------------|---------------------------|-------------------------------------|-----------------------------|------|--------|
| Add Policy Quarantine...             |                             | Search Across Quarantines |                                     |                             |      |        |
| Quarantine Name                      | Type                        | Messages                  | Default Action                      | Last Message Quarantined On | Size | Delete |
| Bank Data Inbound                    | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| Bank Data Outbound                   | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| DKIM Hard Fail                       | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| DLP HIPAA                            | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| DLP PCI                              | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| DLP SOX                              | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| DLP SSN                              | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| DLP US Drivers License               | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| File Analysis                        | Advanced Malware Protection | 0                         | Retain 1 hour then Release          | --                          | 0    |        |
| Inappropriate Inbound                | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| Inappropriate Outbound               | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| Outbreak<br>[Manage by Rule Summary] | Outbreak                    | 0                         | Retention Varies<br>Action: Release | --                          | 0    |        |
| Policy                               | Centralized Policy          | 0                         | Retain 10 days then Delete          | --                          | 0    |        |
| Pwd Protected Inbound                | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| Pwd Protected Outbound               | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| SPF Hard Fail                        | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| SPF Soft Fail                        | Centralized Policy          | 0                         | Retain 1 day 16 hours then Delete   | --                          | 0    |        |
| SpooMail                             | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| SSN Inbound                          | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| SSN Outbound                         | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| Unclassified                         | Unclassified                | 0                         | Retain 30 days then Release         | --                          | 0    |        |
| URL Category Inbound                 | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| URL Category Outbound                | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| URL Malicious Inbound                | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| URL Malicious Outbound               | Centralized Policy          | 0                         | Retain 14 days then Delete          | --                          | 0    |        |
| Virus                                | Antivirus                   | 0                         | Retain 30 days then Delete          | --                          | 0    |        |

Available space for Policy, Virus & Outbreak quarantines is 149G.

## ESA/SMA INSTALLATION AND BEST PRACTICES

| PVO Quarantines - used by Incoming Mail Policies                                                                                             |                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>URL Malicious Inbound:</b><br>Name: URL Malicious Inbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable | <b>SPF Hard Fail:</b><br>Name: SPF Hard Fail<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                      |
| <b>URL Category Inbound:</b><br>Name: URL Category Inbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable   | <b>SPF Soft Fail:</b><br>Name: SPF Soft Fail<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                      |
| <b>Bank Data Inbound:</b><br>Name: Bank Data Inbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable         | <b>SpoofMail:</b><br>Name: SpoofMail<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                              |
| <b>SSN Inbound:</b><br>Name: SSN Inbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                     | <b>DKIM Hard Fail:</b><br>Name: DKIM Hard Fail<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                    |
| <b>Inappropriate Inbound:</b><br>Name: Inappropriate Inbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable | <b>Password Protected Inbound:</b><br>Name: Pwd Protected Inbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable |

| PVO Quarantines - used by Outgoing Mail Policies                                                                                               |                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bank Data Outbound:</b><br>Name: Bank Data Outbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable         | <b>URL Malicious Outbound:</b><br>Name: URL Malicious Outbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable      |
| <b>SSN Outbound:</b><br>Name: SSN Outbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                     | <b>URL Category Outbound:</b><br>Name: URL Category Outbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable        |
| <b>Inappropriate Outbound:</b><br>Name: Inappropriate Outbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable | <b>Password Protected Outbound:</b><br>Name: Pwd Protected Outbound<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable |

## ESA/SMA INSTALLATION AND BEST PRACTICES

If you do not have a DLP feature key then you do not need to create the below Quarantines that are to be used by DLP Policies. If you do plan to use the integrated DLP engine, create the below listed quarantines to be used by DLP:

| Will be used by DLP Policies                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------|
| HIPAA (Used by DLP):<br>Name: DLP HIPAA<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                           |
| PCI (Used by DLP):<br>Name: DLP PCI<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                               |
| Sarbanes-Oxley (Used by DLP):<br>Name: DLP SOX<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                    |
| SSN (Used by DLP):<br>Name: DLP SSN<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable                               |
| US Drivers License (Used by DLP):<br>Name: DLP US Drivers License<br>Retention Period: 14 Days<br>Default Action: Delete<br>Free up space: Enable |

### Create the Incoming Content Filters

Once the Dictionaries have been imported and the PVO Quarantines have been created, you can now start creating the Incoming Content Filters:

Navigate to: *Mail Policies > Incoming Content Filters*

Here is a table of Incoming Content Filters you should create. For example purposes, below the table is a screenshot exemplifying how to create the first one.

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Create these Incoming Content Filters

Name: Bank\_Data

Add Two Conditions:

Message Body or Attachment:

Contains Smart Identifier: ABA Routing Number

Contains Smart Identifier: Credit Card Number

Add One Action:

Quarantine:

Send message to quarantine: "Bank Data Inbound (centralized)"

Duplicate message: Enabled

(Note the Apply Rule should be "If one or more conditions match")

Name: SSN

Add One Condition:

Message Body or Attachment:

Contains Smart Identifier: Social Security Number (SSN)

Add One Action:

Quarantine:

Send message to quarantine: "SSN Inbound (centralized)"

Duplicate message: Enabled

Name: Inappropriate

Add Two Conditions:

Message Body or Attachment:

Contains term in dictionary: Profanity

Contains term in dictionary: Sexual\_Content

Add One Action:

Quarantine:

Send message to quarantine: "Inappropriate Inbound (centralized)"

Duplicate message: Enabled

Name: URL\_Category

Add One Condition:

URL Category:

Select Categories:

Adult, Dating, Filter Avoidance, Freeware and Shareware, Gambling,

Games, Hacking, Lingerie and Swimsuits, Non-sexual Nudity,

Parked Domains, Peer File Transfer, Pornography

Add One Action:

Quarantine:

Send message to quarantine: "URL Category Inbound (centralized)"

Duplicate message: Enabled

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Create these Incoming Content Filters

Name: URL\_Malicious  
Add One Condition:  
    URL Reputation:  
        URL Reputation is: Malicious (-10.0 to -6.0)  
Add One Action:  
    Quarantine:  
        Send message to quarantine: “URL Malicious Inbound (centralized)”  
        Duplicate message: Disabled (\*\*\*\* Quarantine the original \*\*\*\*)

Name: Password\_Protected  
Add One Condition:  
    Attachment Protection: One or more attachments are protected  
Add One Action:  
    Quarantine:  
        Send message to quarantine: “Pwd Protected Inbound (centralized)”  
        Duplicate message: Enabled

Name: Size\_10M  
Add One Condition:  
    Message Size is:  
        Greater than or equal to: 10M  
Add One Action:  
    Add Message Tag:  
        Enter a Term: NOOP

(Note: There must be some action so here we “Tag” the message to represent no operation taken. The fact that the content filter was “Matched” will allow it to show up in reporting. No ‘Action’ need be taken for it to show in Reporting.)

Name: SPF\_Hard\_Fail  
Add One Condition:  
    SPF Verification: “is” Fail  
Add One Action:  
    Quarantine:  
        Send message to quarantine: “SPF Hard Fail (centralized)”  
        Duplicate message: Enabled

(Note: “is Fail” is a Hard SPF failure and it means the owner of the domain is telling you to drop all emails received from senders that are not listed in their SPF record. Initially, it is a good idea to use “Duplicate message” and review the failures for a week or two before moving you start quarantining the original (turn off duplicate message).

(Note2: We will be using SPF a little later to implement Spoof Protection for your own domain so don’t worry about that here.)

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Create these Incoming Content Filters

Name: SPF\_Soft\_Fail

Add One Condition:

SPF Verification: "is" Softfail

Add One Action:

Quarantine:

Send message to quarantine: "SPF Soft Fail (centralized)"

Duplicate message: Enabled

Name: DKIM\_Hardfail\_Copy

Add One Condition:

DKIM Authentication: "is" Hardfail

Add One Action:

Quarantine:

Send message to quarantine: "DKIM Hard Fail (centralized)"

Duplicate message: Enabled

(Note: Quarantine a copy of the message initially.)

Name: DKIM\_Hardfail\_Original

Add One Condition:

DKIM Authentication: "is" Hardfail

Add One Action:

Quarantine:

Send message to quarantine: "DKIM Hard Fail (centralized)"

Duplicate message: Disabled

(Note: We will be creating another Incoming Mail Policy row for PayPal and Ebay domains and will use this Content Filter for domains that we know should pass DKIM Verification.)

Name: Spoof\_SPF\_Failures

Add One Condition but it has BOTH Softfail and Hardfail checked:

SPF Verification: "is" Softfail

SPF Verification: "is" Fail

Add One Action:

Quarantine:

Send message to quarantine: "SpoofMail (centralized)"

Duplicate message: Enable

(Note: We will use this Content Filter to take action for incoming email pretending to send from your own domain — spoofing. Start with the action set to quarantine a copy and after a couple of weeks of reviewing the SpoofMail quarantine, you can modify your SPF TXT DNS record to add all legitimate senders and at some point you can change this content filter to quarantine the original by disabling the duplicate message checkbox)



## ESA/SMA INSTALLATION AND BEST PRACTICES

Example: This is what the Bank\_Data Content Filter should look like before you Submit:

**Content Filter Settings**

|                      |                             |                                                           |
|----------------------|-----------------------------|-----------------------------------------------------------|
|                      | Name:                       | <input type="text" value="Bank_Data"/>                    |
| <b>URL Filtering</b> | Currently Used by Policies: | Default Policy                                            |
|                      | Description:                | <div style="border: 1px solid #ccc; height: 20px;"></div> |
|                      | Order:                      | <input type="text" value="1"/> (of 7)                     |

**Conditions**

Add Condition...
Apply rule:

| Order | Condition                  | Rule                       | Delete |
|-------|----------------------------|----------------------------|--------|
| 1     | Message Body or Attachment | body-contains("aba", 1)    |        |
| 2     | Message Body or Attachment | body-contains("credit", 1) |        |

**Actions**

Add Action...

| Order | Action     | Rule                                      | Delete |
|-------|------------|-------------------------------------------|--------|
| 1     | Quarantine | duplicate-quarantine("Bank Data Inbound") |        |

After creating all of the Incoming Content Filters, the table should now look like this:

Because the “Policies” function is selected (you’ll see the Policies hypertext at the top middle) the middle column shows the Incoming Mail Policies the Content Filter has been applied to. Because we have not applied them to any Incoming Mail Policy, the “Not in use” is displayed.

| Filters                                                                  |                        |                                |           |        |  |
|--------------------------------------------------------------------------|------------------------|--------------------------------|-----------|--------|--|
| <span style="border: 1px solid #ccc; padding: 2px;">Add Filter...</span> |                        |                                |           |        |  |
| Order                                                                    | Filter Name            | Description   Rules   Policies | Duplicate | Delete |  |
| 1                                                                        | Bank_Data              | Not in use                     |           |        |  |
| 2                                                                        | SSN                    | Not in use                     |           |        |  |
| 3                                                                        | Inappropriate          | Not in use                     |           |        |  |
| 4                                                                        | URL_Category           | Not in use                     |           |        |  |
| 5                                                                        | URL_Malicious          | Not in use                     |           |        |  |
| 6                                                                        | Password_Protected     | Not in use                     |           |        |  |
| 7                                                                        | Size_10M               | Not in use                     |           |        |  |
| 8                                                                        | SPF_Hard_Fail          | Not in use                     |           |        |  |
| 9                                                                        | SPF_Soft_Fail          | Not in use                     |           |        |  |
| 10                                                                       | DKIM_Hardfail_Copy     | Not in use                     |           |        |  |
| 11                                                                       | DKIM_Hardfail_Original | Not in use                     |           |        |  |
| 12                                                                       | Spoof_SPF_Failures     | Not in use                     |           |        |  |

Edit Filter Order...

## ESA/SMA INSTALLATION AND BEST PRACTICES

Navigate to: *Mail Policies > Incoming Mail Policies*

Click on the “Disabled” text in the Content Filters cell for the Default Policy.

The pull-down button is set to “Disable Content Filters”. Click the button and set to Enable Content Filters and you will immediately be presented with all Incoming Content Filters that have been created. Enable all filters except the DKIM\_Hardfail\_Original.

Submit and Commit

### DKIM Protection for Hardfail

Email received from Ebay and Paypal should always pass DKIM verification. We will therefore create another Incoming Mail Policy to use the DKIM\_Hardfail\_Original Incoming Content Filter for email from those domains.

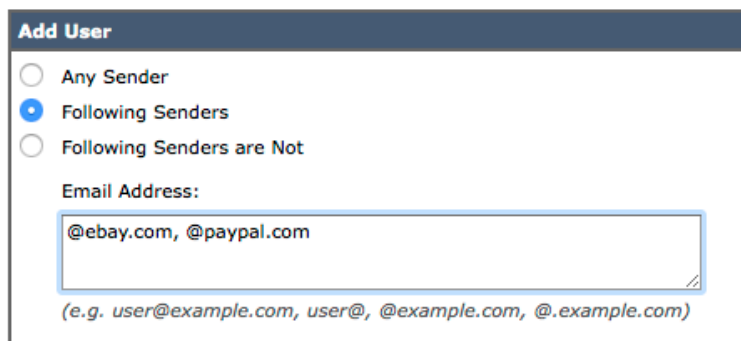
Navigate to: *Mail Policies > Incoming Mail Policies*

Click the Add Policy button.

Enter the Name: DKIM Hardfail Original

The next configuration panel lets you define what messages will match this new Incoming Mail Policy. We only want to define criteria for the Sender (the left portion of the configuration panel).

Click “Following Senders” radio button and in the Email Addresses table enter “[@ebay.com](#), [@paypal.com](#)”



**Add User**

Any Sender

Following Senders

Following Senders are Not

Email Address:

(e.g. user@example.com, user@, @example.com, @.example.com)

Click the “Ok” button at the bottom.

Click Submit.

## ESA/SMA INSTALLATION AND BEST PRACTICES

You are presented with the Incoming Mail Policies table again but now you have a new Mail Policy above the Default Policy.

Click the (use default) in the Content Filters cell for the new row.

Flip the pulldown menu to “Enable Content Filters (Customized Settings)”.

Uncheck the “DKIM\_Hardfail\_Copy” and Check the “DKIM\_Hardfail\_Original”.

Click Submit and Commit changes.

The Incoming Mail Policies table should now look like this:

| Policies      |                        |                                                                            |                                                                       |                                                                                               |                                                                                            |                                                          |                                                   |        |
|---------------|------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------|--------|
| Add Policy... |                        |                                                                            |                                                                       |                                                                                               |                                                                                            |                                                          |                                                   |        |
| Order         | Policy Name            | Anti-Spam                                                                  | Anti-Virus                                                            | Advanced Malware Protection                                                                   | Graymail                                                                                   | Content Filters                                          | Outbreak Filters                                  | Delete |
| 1             | DKIM Hardfail Original | (use default)                                                              | (use default)                                                         | (use default)                                                                                 | (use default)                                                                              | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | (use default)                                     |        |
|               | Default Policy         | IronPort Intelligent Multi-Scan<br>Positive: Drop<br>Suspected: Quarantine | Sophos<br>McAfee<br>Encrypted: Deliver<br>Unscannable: Deliver<br>... | File Reputation<br>Unscannable: Deliver<br>Malware File: Drop<br>Pending Analysis: Quarantine | Graymail Detection<br>Unsubscribe: Enabled<br>Marketing: Deliver<br>Social: Deliver<br>... | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | Retention Time:<br>Virus: 1 day<br>Other: 4 hours |        |

### Domain Spoof Protection

One of the main requests from customers is to prevent Incoming messages spoofing their own domain — i.e. using a mail-from address with their own domain. We will configure that protection by creating a new Incoming Mail Policy and using the Spoof\_SPF\_Failures Incoming Content filter that we created earlier.

Navigate to: *Mail Policies > Incoming Mail Policies*

Click the “Add Policy” button.

Enter the Name: Spoof Detection

Insert Before Policy: 1 (we want this new Spoof Detection policy to be the first row)

Click the Add User button.

As before, click the “Following Senders” radio button and enter all you local domains — example “[@example.com](#)” if you owned [example.com](#) domain.

Click Ok. Now click Submit.

You are presented with the Incoming Mail Policies table again but now you see the newly created “Spoof Detection” Incoming Mail Policy.

## ESA/SMA INSTALLATION AND BEST PRACTICES

Click the (use default) in the Content Filters cell for the new row.

Flip the pulldown menu to “Enable Content Filters (Customized Settings)”.

Disable/Uncheck the following Content Filters:

- SPF\_Hard\_Fail
- SPF\_Soft\_Fail
- DKIM\_Hardfail\_Copy
- DKIM\_Hardfail\_Original

Enable all other Content Filters. The point here is that we created a special Incoming Content Filter named “Spoof\_SPF\_Failures” which matches on both Hard and Soft SPF failures and the Action is to quarantine a “copy” of the emails to a special PVO Quarantine we also created earlier — named “SpoofMail”. This way the ESA Admin knows to go to that quarantine for a complete list of emails trying to spoof their domain.

The “Action” for the “Spoof\_SPF\_Failure” is to place a “copy” of the email in the “SpoofMail” quarantine because it is rare that a customer knows all the legitimate senders that have been authorized to send legitimate email out on their behalf using the customer’s own domain in the Mail-From.

So for the first week or two you would review the “SpoofMail” quarantine and if you find any legitimate senders that are allowed to send email with your mail-from and are failing SPF, then add them to your SPF record. Keep the ~all (Soft Fail) on the SPF record until you are sure you have a complete list. At that point you would flip the SPF record to -all (Hard Fail) and you would want to change the Action to place the Original email into the quartile instead of a copy and deliver the original.

Click Submit and Commit changes.

The Incoming Mail Policies table should now look like this:

| Policies      |                        |                                                                            |                                                                       |                                                                                               |                                                                                            |                                                          |                                                   |        |
|---------------|------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------|--------|
| Add Policy... |                        |                                                                            |                                                                       |                                                                                               |                                                                                            |                                                          |                                                   |        |
| Order         | Policy Name            | Anti-Spam                                                                  | Anti-Virus                                                            | Advanced Malware Protection                                                                   | Graymail                                                                                   | Content Filters                                          | Outbreak Filters                                  | Delete |
| 1             | Spoof Detection        | (use default)                                                              | (use default)                                                         | (use default)                                                                                 | (use default)                                                                              | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | (use default)                                     |        |
| 2             | DKIM Hardfail Original | (use default)                                                              | (use default)                                                         | (use default)                                                                                 | (use default)                                                                              | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | (use default)                                     |        |
|               | Default Policy         | IronPort Intelligent Multi-Scan<br>Positive: Drop<br>Suspected: Quarantine | Sophos<br>McAfee<br>Encrypted: Deliver<br>Unscannable: Deliver<br>... | File Reputation<br>Unscannable: Deliver<br>Malware File: Drop<br>Pending Analysis: Quarantine | Graymail Detection<br>Unsubscribe: Enabled<br>Marketing: Deliver<br>Social: Deliver<br>... | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | Retention Time:<br>Virus: 1 day<br>Other: 4 hours |        |

## ESA/SMA INSTALLATION AND BEST PRACTICES

### DMARC Verification and Protection

Domain-Based Message Authentication, Reporting, and Conformance (DMARC) was created to help resolve the shortcomings of DKIM and SPF. With DKIM and SPF an organization must write policies to define what actions to take with emails that fail DKIM and/or SPF. DMARC gives the legitimate domain owner the ability to tell the receiving organization what to do with a message that fails DKIM and SPF checks. This capability reduces the guesswork and limits the recipient's exposure to potentially malicious or fraudulent messages.

For the ESA to be able to utilize DMARC, we must enable DMARC verification within the Mail Flow Policy — which we have already done earlier in this document.

On the ESA navigate to *Mail Policies > DMARC*

Click on the Edit Global Settings: (Here is how I have my DMARC Global Settings configured)

| DMARC Global Settings                          |                                                                                                                    |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Specific senders bypass address list:          | No address lists are currently defined. To use an address list, please create one at Mail Policies > Address Lists |
| Bypass verification for messages with headers: | <input type="text"/><br><small>(e.g. List-ID, List-Subscribe)</small>                                              |
| Schedule for report generation:                | 12 <input type="button" value="↓"/> 00 <input type="button" value="↓"/> AM <input type="button" value="↓"/>        |
| Entity generating reports:                     | <input type="text" value="esa1.unc-hamiltons.com"/>                                                                |
| Additional contact information for reports:    | <input type="text" value="dalton@cisco.com"/>                                                                      |
| Send copy of all aggregate reports to:         | <input type="text" value="dalton@cisco.com"/>                                                                      |
| Error Reports:                                 | <input checked="" type="checkbox"/> Enable sending of delivery error reports                                       |

Submit

Now we need to configure the DEFAULT Verification Profile.

Click on DEFAULT

We recommend you take the action specified by the DMARC record created by the owner of the domain. If the DMARC record is Reject, then we recommend Reject. If the DMARC record is Quarantine, then we recommend you follow that direction.

For the Quarantine Action in the screenshot below, I have created another PVO quarantine on the SMA named “DMARC Fail” and that is what I’ve chosen in my DEFAULT DMARC Verification Profile.

Submit

## ESA/SMA INSTALLATION AND BEST PRACTICES

| Edit DMARC Verification Profile                               |                                                                                                                                                                                                                        |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile Name:                                                 | DEFAULT                                                                                                                                                                                                                |
| Message Action when the Policy in DMARC Record is Reject:     | <input type="radio"/> No Action<br><input type="radio"/> Quarantine to: Bank Data Inbound (centralized)<br><input checked="" type="radio"/> Reject<br>SMTP Code: 550<br>SMTP Response: #5.7.1 DMARC unauthenticated ma |
| Message Action when the Policy in DMARC Record is Quarantine: | <input type="radio"/> No Action<br><input checked="" type="radio"/> Quarantine to: DMARC Fail (centralized)                                                                                                            |
| Message Action for Temporary Failure:                         | <input checked="" type="radio"/> Accept<br><input type="radio"/> Reject<br>SMTP Code: 451<br>SMTP Response: #4.7.1 Unable to perform DMARC v                                                                           |
| Message Action for Permanent Failure:                         | <input checked="" type="radio"/> Accept<br><input type="radio"/> Reject<br>SMTP Code: 550<br>SMTP Response: #5.7.1 DMARC verification failed.                                                                          |

Cancel Submit

Commit changes.

With DMARC there is no need to create a Content Filter for messages that fail DKIM or SPF checks, the DMARC record will specify how to handle these failures.

If you would like to review DMARC records for organizations, you can do so by using the tool found at:

<https://dmarcian.com/dmarc-inspector>

### Outbreak Filters

Click on the text in the Outbreak Filters cell for the Default Policy.

Outbreak Filters is one of the most important threat defense engines on the appliance. Always purchase the Outbreak Filters license!!!! There are three reasons OF is a staple on this appliance:

1. It is the best engine for catching zero-hour malware/viruses. The Outbreak Filters report will also show you how much lead-time (protection time) you are getting out of Outbreak Filters for your production mail traffic.
2. The URL Filtering engine requires the Outbreak Filters license. URL Filtering is key for Anti-Spam, Content Filters, and even Outbreak Filters for being able to detect malicious URLs and categorize URLs within emails.
3. The “Other Threats” portion of Outbreak Filters is designed to detect and neutralize Phishing emails.

## ESA/SMA INSTALLATION AND BEST PRACTICES

Here is how Outbreak Filters should be setup:

| Outbreak Filter Settings                                                                                                         |                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Quarantine Threat Level: (?)                                                                                                     | 3                                                                                                                                                                                                                                                              |
| Maximum Quarantine Retention:                                                                                                    | Viral Attachments: 1 Days<br>Other Threats: 4 Hours<br><input type="checkbox"/> Deliver messages without adding them to quarantine                                                                                                                             |
| Bypass Attachment Scanning:                                                                                                      | None configured                                                                                                                                                                                                                                                |
| Message Modification                                                                                                             |                                                                                                                                                                                                                                                                |
| <input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments) |                                                                                                                                                                                                                                                                |
| Message Modification Threat Level: (?)                                                                                           | 3                                                                                                                                                                                                                                                              |
| Message Subject:                                                                                                                 | Prepend [SUSPICIOUS MESSAGE] <a href="#">Insert Variables</a>   <a href="#">Preview Text</a>                                                                                                                                                                   |
| Include the X-IronPort-Outbreak-Status headers:                                                                                  | <input checked="" type="radio"/> Enable for all messages<br><input type="radio"/> Enable only for threat-based outbreak<br><input type="radio"/> Disable                                                                                                       |
| Include the X-IronPort-Outbreak-Description header:                                                                              | <input type="radio"/> Enable<br><input checked="" type="radio"/> Disable                                                                                                                                                                                       |
| Alternate Destination Mail Host (Other Threats only):                                                                            | <input type="text"/><br><small>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</small>                                                                                                                                                                     |
| URL Rewriting:                                                                                                                   | Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails.<br><input type="radio"/> Enable only for unsigned messages (recommended)<br><input checked="" type="radio"/> Enable for all messages<br><input type="radio"/> Disable |
| Bypass Domain Scanning (?)                                                                                                       | <input type="text"/><br><small>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</small>                                                                                                                        |
| Threat Disclaimer:                                                                                                               | None<br><small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies &gt; Text Resources &gt; Disclaimers</small>                                           |

Submit and Commit

The Incoming Mail Policies table should now look like this:

| Policies |                |                                                                            |                                                                       |                                                                                               |                                                                                            |                                                          |                                                   |        |
|----------|----------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------|--------|
| Order    | Policy Name    | Anti-Spam                                                                  | Anti-Virus                                                            | Advanced Malware Protection                                                                   | Graymail                                                                                   | Content Filters                                          | Outbreak Filters                                  | Delete |
|          | Default Policy | IronPort Intelligent Multi-Scan<br>Positive: Drop<br>Suspected: Quarantine | Sophos<br>McAfee<br>Encrypted: Deliver<br>Unscannable: Deliver<br>... | File Reputation<br>Unscannable: Deliver<br>Malware File: Drop<br>Pending Analysis: Quarantine | Graymail Detection<br>Unsubscribe: Enabled<br>Marketing: Deliver<br>Social: Deliver<br>... | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | Retention Time:<br>Virus: 1 day<br>Other: 4 hours |        |

### Mail Policies based on AD/LDAP Group

We've already created a couple new Incoming Mail Policies but there are many times when an organization will create new Incoming Mail Policies to differentiate email policy for recipients that are part of a certain AD Group — like HR or Executives or Information Technology.

## ESA/SMA INSTALLATION AND BEST PRACTICES

The steps below demonstrate the method for an Incoming Mail Policy but the same principle applies for Outgoing Mail Policies — however, for Outgoing Mail Policy AD/LDAP group matches, you would match the LDAP Group based on the Sender instead of the Recipient.

Navigate to: *Mail Policies > Incoming Mail Policies*

Click the “Add Policy” button.

Provide a name. I used: “HR AD Group”

Change the “Insert Before Policy” pulldown menu to choose location 1.

Now click on “Add User”

The left portion of the Add User panel is to define matching criteria based on Sender. The right portion of the screen is for defining matching criteria by Recipient. We want to define a match based on the Active Directory Group named “HR”.

Click on “Following Recipients” radio button.

The Query LDAP Group should already be chosen since we added the LDAP Server Profile earlier in this document.

In the Group: text field enter your DN format for your HR group. For my lab, it is as follows:

*CN=HR,OU=groups,DC=unc-hamiltons,DC=com*

Click the Add Group button and the LDAP Group will appear in the text box.

The screenshot shows the 'Add User' configuration interface. On the left, under 'Any Sender', there are radio buttons for 'Any Sender', 'Following Senders', and 'Following Senders are Not'. Below these are fields for 'Email Address' and 'LDAP Group' with a query dropdown set to 'UNC-HAMILTONS.group'. On the right, under 'Following Recipients', there are radio buttons for 'Any Recipient' and 'Following Recipients'. Below these are a large text field for the recipient list, a 'LDAP Group' section with a query dropdown set to 'UNC-HAMILTONS.group', and a 'Group' field containing the DN 'CN=HR,OU=groups,DC=unc-hamiltons,DC=com' with 'Add Group' and 'Remove' buttons. At the bottom, a text box displays the full LDAP query: 'ldap(CN=HR,OU=groups,DC=unc-hamiltons,DC=com,UNC-HAMILTONS.group)'. A dropdown menu at the top right of the right panel is set to 'Only if all conditions match'.



## ESA/SMA INSTALLATION AND BEST PRACTICES

Click the Ok button at the bottom right of the Add User panel.  
You now see something similar to this:

**Edit Policy**

|                                                       |                                                                                                    |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Policy Name: <span style="font-size: small;">?</span> | <input style="width: 90%;" type="text" value="HR AD Group"/><br><small>(e.g. my IT policy)</small> |
| Insert Before Policy:                                 | <input style="width: 90%;" type="text" value="1 (HR AD Group)"/>                                   |

**Users**

Add User...

| Sender | Recipients                              | Edit                                | Delete                                |
|--------|-----------------------------------------|-------------------------------------|---------------------------------------|
| ANY    | ldap(CN=HR,OU=groups,DC=unc-hamilton... | <input type="button" value="Edit"/> | <input type="button" value="Delete"/> |

Click Submit and Commit  
My Incoming Mail Policies table now looks like this:

| Policies      |                        |                                                                            |                                                                       |                                                                                               |                                                                                            |                                                          |                                                   |                                       |
|---------------|------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------|---------------------------------------|
| Add Policy... |                        |                                                                            |                                                                       |                                                                                               |                                                                                            |                                                          |                                                   |                                       |
| Order         | Policy Name            | Anti-Spam                                                                  | Anti-Virus                                                            | Advanced Malware Protection                                                                   | Graymail                                                                                   | Content Filters                                          | Outbreak Filters                                  | Delete                                |
| 1             | HR AD Group            | (use default)                                                              | (use default)                                                         | (use default)                                                                                 | (use default)                                                                              | (use default)                                            | (use default)                                     | <input type="button" value="Delete"/> |
| 2             | Spoof Detection        | (use default)                                                              | (use default)                                                         | (use default)                                                                                 | (use default)                                                                              | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | (use default)                                     | <input type="button" value="Delete"/> |
| 3             | DKIM Hardfail Original | (use default)                                                              | (use default)                                                         | (use default)                                                                                 | (use default)                                                                              | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | (use default)                                     | <input type="button" value="Delete"/> |
|               | <b>Default Policy</b>  | IronPort Intelligent Multi-Scan<br>Positive: Drop<br>Suspected: Quarantine | Sophos<br>McAfee<br>Encrypted: Deliver<br>Unscannable: Deliver<br>... | File Reputation<br>Unscannable: Deliver<br>Malware File: Drop<br>Pending Analysis: Quarantine | Graymail Detection<br>Unsubscribe: Enabled<br>Marketing: Deliver<br>Social: Deliver<br>... | Bank_Data<br>SSN<br>Inappropriate<br>URL_Category<br>... | Retention Time:<br>Virus: 1 day<br>Other: 4 hours |                                       |

The entire reason for creating a new row in the Incoming Mail Policy for HR is to differentiate how the Incoming Mail is processed for recipients that are part of the HR group. When you first create the new row all the cells are set to “(use default)”, which means it acts in the same manner in which you have configured the “Default Policy”. Therefore, in a real-world scenario you would change some portion of the setup for the new row — maybe apply or do not apply a Content Filter, etc.

For the purposes of this document, the point was to show you how to create a policy based on LDAP Group membership so I will leave everything set to (use default) on my configuration.

8. Outgoing Mail Policies

Navigate to *Mail Policies > Outgoing Mail Policies*

This is what the default view is of the Outgoing Mail Policies table:

| Policies |                |           |                                                                              |          |                 |                  |          |        |
|----------|----------------|-----------|------------------------------------------------------------------------------|----------|-----------------|------------------|----------|--------|
| Order    | Policy Name    | Anti-Spam | Anti-Virus                                                                   | Graymail | Content Filters | Outbreak Filters | DLP      | Delete |
|          | Default Policy | Disabled  | Sophos<br>Encrypted: Deliver<br>Unscannable: Deliver<br>Virus Positive: Drop | Disabled | Disabled        | Disabled         | Disabled |        |

**Anti-Spam**

Anti-Spam should remain disabled for Outgoing email.

**Anti-Virus**

Click on Anti-Virus. Make the following changes:

**Dual-Layer Signature-Based AV:**

Enable both Sophos and McAfee AV engines

**Enable Anti-Virus Scanning for This Policy:**

Yes

- Use McAfee Anti-Virus
- Use Sophos Anti-Virus

No

**Message Scanning:**

Leave Scanning set to: “Scan for Viruses Only”

**Message Scanning**

Scan for Viruses only

Drop infected attachments if a virus is found

(recommended) Include an X-header with the Anti-Virus scanning results in messages

**Repaired Messages:**

This section is not enabled because we are not repairing the message.

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Encrypted Messages:

Action Applied to Message: “Deliver As Is” (This is the typical setting)

Archive Original Message: No

Modify Message Subject: No

Advanced:

Enable Notification if you wish to be notified when an internal user send an outbound email that they encrypt themselves.

### Unscannable Messages:

Action Applied to Message: Deliver As Is

Archive Original Message: No

Modify Message Subject: No

Advanced:

Enable Notification if you wish to be notified when an attachment could not be scanned.

### Virus Infected Messages:

Action Applied to Message: Drop Message

Archive Original Message: No

Modify Message Subject: (should not be selectable since we drop message)

Advanced:

Container Notification: Not configurable because Action is Drop

Other Notification:

Enable “Sender” and “Others”. Put the Email admin or help-desk email address in for Other. You want to know when a desktop is sending malware outbound.

| Virus Infected Messages:              |                                                                                                                                                                                           |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action Applied to Message:            | Drop Message                                                                                                                                                                              |
| Archive Original Message:             | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                             |
| Modify Message Subject:               | <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append                                                                                            |
|                                       | [WARNING: VIRUS DETECTED]                                                                                                                                                                 |
| Advanced                              |                                                                                                                                                                                           |
| Add Custom Header to Message:         | <input checked="" type="radio"/> No <input type="radio"/> Yes                                                                                                                             |
|                                       | Header: <input type="text"/>                                                                                                                                                              |
|                                       | Value: <input type="text"/>                                                                                                                                                               |
| Container Notification:               | System Generated<br>Preview Message Body <input type="checkbox"/><br>(see Mail Policies > Text Resources > Anti-Virus Container Template)                                                 |
| Other Notification:                   | Recipients: <input checked="" type="checkbox"/> Sender<br><input type="checkbox"/> Recipient<br><input checked="" type="checkbox"/> Others: <input type="text" value="dalton@cisco.com"/> |
|                                       | Notification: System Generated<br>Preview Notification <input type="checkbox"/><br>(see Mail Policies > Text Resources > Anti-Virus Notification)                                         |
|                                       | Subject: <input type="text" value="Outbound Malware: \$Subject"/>                                                                                                                         |
| Modify Message Recipient:             | <input type="radio"/> No <input type="radio"/> Yes                                                                                                                                        |
|                                       | Address: <input type="text"/>                                                                                                                                                             |
| Send Message to Alternate Destination | <input type="radio"/> No <input type="radio"/> Yes                                                                                                                                        |
| Host:                                 | Host: <input type="text"/>                                                                                                                                                                |

## Submit and Commit

### **Optional: Get detailed AV Details by using the Anti-Virus Container Notifications:**

Some customers use the Anti-Virus Advanced Container Notification to receive very granular detail about the email and the virus attachments found in the email. By enabling the Container Notification, a “Notification Alert” will sent to the Alert Recipients found in the *System Administration > Alerts* page. When setting up an Alert Recipient there is a column for “Anti-Virus and AMP”. Those are the Alert Recipients that would receive the Container Notification.

To use a Container Notification you would need to change the “Action Applied to Message” to be “Deliver as Attachment (text/plain) to New Message” or as (RFC 822) — either is fine. You will then note the Container Notification section is active. There is a “System-Generated” Container Notification that you can choose but it has limited data compared to the many variables of data available by creating a custom Anti-Virus Container Template. You can create your own Container Template in *Mail Policies > Text Resources > Anti-Virus Container Template* and define as much detail in the container as you would like to see.

Here is an example format. You do not need to know all the dollar-sign variables, just open the Insert Variables window by clicking the “Insert Variables” hypertext. By clicking on one of the variables, it places the dollar-sign variable name wherever you mouse is within the text window:

```
Date: $Date          Time: $Time
From: $From
Envelope Sender: $EnvelopeFrom

To: $To
Envelope Recipients: $enveloperecipients

Subject: $Subject

Remote IP: $remotehost
SBRS: $Reputation
SenderGroup: $Group
Mail Flow Policy: $Policy
MID: $MID

All-Headers:
$AllHeaders

Virus List:
$AV_VIRUSES

File Names:
$filenames

Virus Verdict:
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

\$AV\_VERDICT

Infected Parts List:  
\$AV\_INFECTED\_PARTS

### Outgoing Content Filters

Navigate to: *Mail Policies > Outgoing Content Filters*

Add the following Outgoing Content Filters

| Create these Outgoing Content Filters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Name: Bank_Data</p> <p>Add Two Conditions:</p> <ul style="list-style-type: none"><li>Message Body or Attachment:<ul style="list-style-type: none"><li>Contains Smart Identifier: ABA Routing Number</li><li>Contains Smart Identifier: Credit Card Number</li></ul></li></ul> <p>Add One Action:</p> <ul style="list-style-type: none"><li>Quarantine:<ul style="list-style-type: none"><li>Send message to quarantine: “Bank Data Outbound (centralized)”</li><li>Duplicate message: Enabled</li></ul></li></ul> <p>(Note the Apply Rule should be “If one or more conditions match”)</p> |
| <p>Name: SSN</p> <p>Add One Condition:</p> <ul style="list-style-type: none"><li>Message Body or Attachment:<ul style="list-style-type: none"><li>Contains Smart Identifier: Social Security Number (SSN)</li></ul></li></ul> <p>Add One Action:</p> <ul style="list-style-type: none"><li>Quarantine:<ul style="list-style-type: none"><li>Send message to quarantine: “SSN Outbound (centralized)”</li><li>Duplicate message: Enabled</li></ul></li></ul>                                                                                                                                   |

Create these Outgoing Content Filters

Name: Inappropriate

Add Two Conditions:

Message Body or Attachment:

Contains term in dictionary: Profanity

Contains term in dictionary: Sexual\_Content

Add One Action:

Quarantine:

Send message to quarantine: "Inappropriate Outbound (centralized)"

Duplicate message: Enabled

Name: URL\_Category

Add One Condition:

URL Category:

Select Categories:

Adult, Dating, Filter Avoidance, Freeware and Shareware, Gambling,

Games, Hacking, Lingerie and Swimsuits, Non-sexual Nudity,

Parked Domains, Peer File Transfer, Pornography

Add One Action:

Quarantine:

Send message to quarantine: "URL Category Outbound (centralized)"

Duplicate message: Enabled

Name: URL\_Malicious

Add One Condition:

URL Reputation:

URL Reputation is: Malicious (-10.0 to -6.0)

Add One Action:

Quarantine:

Send message to quarantine: "URL Malicious Outbound (centralized)"

Duplicate message: Disabled (\*\*\*\* Quarantine the Original \*\*\*\*)

Name: Password\_Protected

Add One Condition:

Attachment Protection: One or more attachments are protected

Add One Action:

Quarantine:

Send message to quarantine: "Pwd Protected Outbound (centralized)"

Duplicate message: Enabled

Create these Outgoing Content Filters

Name: Size\_10M  
 Add One Condition:  
     Message Size is:  
         Greater than or equal to: 10M  
 Add One Action:  
     Add Message Tag:  
         Enter a Term: NOOP

(Note: There must be some action so here we “Tag” the message to represent no operation taken. The fact that the content filter was “Matched” will allow it to show up in reporting. No ‘Action’ need be taken for it to show in Reporting.)

The Outgoing Content Filters table should now look like this — in the example below, I have already applied the Content Filters to the Default Outgoing Mail Policy — ‘Default Policy’.

| Filters       |                    |                                |           |        |
|---------------|--------------------|--------------------------------|-----------|--------|
| Add Filter... |                    |                                |           |        |
| Order         | Filter Name        | Description   Rules   Policies | Duplicate | Delete |
| 1             | Bank_Data          | Default Policy                 |           |        |
| 2             | SSN                | Default Policy                 |           |        |
| 3             | Inappropriate      | Default Policy                 |           |        |
| 4             | URL_Category       | Default Policy                 |           |        |
| 5             | URL_Malicious      | Default Policy                 |           |        |
| 6             | Password_Protected | Default Policy                 |           |        |
| 7             | Size_10M           | Default Policy                 |           |        |

Edit Filter Order...

Navigate to *Mail Policies > Outgoing Mail Policies* and click on the “Disabled” text in the Content Filters cell for the Default Policy.

The pull-down button is set to “Disable Content Filters”. Click the button and set to Enable Content Filters and you will immediately be presented with all Outgoing Content Filters that have been created. We want all of these applied to the Default Policy, so check them all (Enable them all).

Submit and Commit

### Graymail

Graymail detection should be disabled for Outgoing Mail Policy.

### Outbreak Filters

Outbreak Filters should be disabled for Outgoing Mail Policy.

### DLP

#### Step A: Enable DLP

Cisco ESA on-box full DLP is not enabled by default. Click on the “Disabled” link for DLP. Change the Disable DLP setting to Enable DLP.

You will note the DLP Policies section shows no DLP Policies. We must first create them in order to choose them here.

#### Submit and Commit

#### Step B: Create DLP Message Actions

You specify primary and secondary DLP Actions that the ESA will take when it detects a DLP violation in an outgoing email. Different actions can be assigned for different violation types and severities.

Primary actions include:

- Deliver
- Drop
- Quarantine

Secondary actions include:

- Sending a copy to any custom quarantine or the ‘Policy’ quarantine.
- Encrypt the message. The appliance only encrypts the message body. It does not encrypt the message headers.
- Altering the Subject header.
- Adding disclaimer text/html to the message.
- Sending the message to an alternate destination mailhost.
- Sending bcc copies of the message.
- Sending DLP violation notification to sender and/or other contacts.

These actions are not mutually exclusive — you can combine some of them within different DLP policies for various processing needs for different user groups.

We are going to implement the following DLP Action:



## ESA/SMA INSTALLATION AND BEST PRACTICES

### Quarantine:

When we configured the SMA we created the following custom policy quarantines with the intention of them being used by the DLP Actions:

- DLP HIPAA
- DLP PCI
- DLP SOX
- DLP SSN

### Encrypt:

Earlier in this document we created three Encryption Profiles:

- EncryptHigh
- EncryptMedium
- EncryptLow

Create the DLP Actions. Navigate to:

*Mail Policies > DLP Message Customizations*

Click the “Add Message Action” button and add the following DLP Actions.

#### Create these DLP Message Actions

Name: EncryptHigh Deliver and Copy to DLP HIPAA  
Message Action: Deliver  
    Enable Encryption: Enabled (Checked)  
        Encryption Rule: Always use message encryption  
        Encryption Profile: EncryptHigh  
Send a copy of message to: DLP HIPAA  
Advanced: No setting in Advanced for this Action

Name: EncryptMedium Deliver and Copy to DLP HIPAA  
Message Action: Deliver  
    Enable Encryption: Enabled (Checked)  
        Encryption Rule: Always use message encryption  
        Encryption Profile: EncryptMedium  
Send a copy of message to: DLP HIPAA  
Advanced: No setting in Advanced for this Action

Create these DLP Message Actions

Name: EncryptLow Deliver and Copy to DLP HIPAA  
 Message Action: Deliver  
     Enable Encryption: Enabled (Checked)  
         Encryption Rule: Always use message encryption  
         Encryption Profile: EncryptLow  
     Send a copy of message to: DLP HIPAA  
 Advanced: No setting in Advanced for this Action

Name: EncryptMedium Deliver and Copy to DLP PCI  
 Message Action: Deliver  
     Enable Encryption: Enabled (Checked)  
         Encryption Rule: Always use message encryption  
         Encryption Profile: EncryptMedium  
     Send a copy of message to: DLP PCI  
 Advanced: No setting in Advanced for this Action

Name: EncryptMedium Deliver and Copy to DLP SOX  
 Message Action: Deliver  
     Enable Encryption: Enabled (Checked)  
         Encryption Rule: Always use message encryption  
         Encryption Profile: EncryptMedium  
     Send a copy of message to: DLP SOX  
 Advanced: No setting in Advanced for this Action

Name: Copy to DLP HIPAA  
 Message Action: Deliver  
     Enable Encryption: Disabled (Not Checked)  
     Send a copy of message to: DLP HIPAA  
 Advanced: No setting in Advanced for this Action

Name: Copy to DLP PCI  
 Message Action: Deliver  
     Enable Encryption: Disabled (Not Checked)  
     Send a copy of message to: DLP PCI  
 Advanced: No setting in Advanced for this Action

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Create these DLP Message Actions

Name: Copy to DLP SOX  
 Message Action: Deliver  
     Enable Encryption: Disabled (Not Checked)  
     Send a copy of message to: DLP SOX  
 Advanced: No setting in Advanced for this Action

Name: Copy to DLP SSN  
 Message Action: Deliver  
     Enable Encryption: Disabled (Not Checked)  
     Send a copy of message to: DLP SSN  
 Advanced: No setting in Advanced for this Action

Commit changes

### Step C: Create the DLP Policies

Navigate to:

*Mail Policies > DLP Message Customizations*

Open the “Regulatory Compliance” disclosure triangle.

| Add DLP Policy from Templates                                                                         |                                                                                            |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Display Settings: <a href="#">Expand All Categories</a>   <a href="#">Display Policy Descriptions</a> |                                                                                            |
| ▼ Regulatory Compliance                                                                               |                                                                                            |
| Add                                                                                                   | <b>FERPA (Family Educational Rights and Privacy Act)</b> <i>Customization recommended.</i> |
| Add                                                                                                   | <b>GLBA (Gramm-Leach Bliley Act)</b> <i>Customization recommended.</i>                     |
| Add                                                                                                   | <b>HIPAA and HITECH</b> <i>Customization recommended.</i>                                  |
| Add                                                                                                   | <b>HIPAA and HITECH Low Threshold</b> <i>Customization recommended.</i>                    |
| Add                                                                                                   | <b>PCI-DSS (Payment Card Industry Data Security Standard)</b>                              |
| Add                                                                                                   | <b>PIPEDA (Personal Information Protection and Electronic Documents Act)</b>               |
| Add                                                                                                   | <b>Puerto Rico DACO 7207, 7336 and 7376</b> <i>Customization recommended.</i>              |
| Add                                                                                                   | <b>SOX (Sarbanes-Oxley)</b>                                                                |
| ▸ US State Regulatory Compliance                                                                      |                                                                                            |
| ▸ Acceptable Use                                                                                      |                                                                                            |
| ▸ Privacy Protection                                                                                  |                                                                                            |
| ▸ Intellectual Property Protection                                                                    |                                                                                            |
| ▸ Company Confidential                                                                                |                                                                                            |
| ▸ Custom Policy                                                                                       |                                                                                            |

## ESA/SMA INSTALLATION AND BEST PRACTICES

For the “Low Severity Incidents” try using the “Copy to <quarantine name>” instead of Encrypt Deliver and Copy to Quarantine. This allows you to monitor the Quarantine for a week to check for false-positives on those messages that barely breached the Severity scale.

### HIPAA Policy:

Click the “Add” button to the left of “HIPAA and HIGHTECH”

Name: HIPAA and HITECH

Severity Settings:

Critical Severity Incident: EncryptHigh Deliver and Copy to DLP HIPAA

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: EncryptMedium Deliver and Copy to DLP HIPAA

Low Severity Incident: Copy to DLP HIPAA

### PCI Policy:

Click the “Add” button to the left of “PCI-DSS”

Name: PCI-DSS (Payment Card Industry Data Security Standard)

Severity Settings:

Critical Severity Incident: EncryptMedium Deliver and Copy to DLP PCI

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Copy to DLP PCI

### SOX Policy:

Click the “Add” button to the left of “SOX”

Name: SOX (Sarbanes–Oxley)

Severity Settings:

Critical Severity Incident: EncryptMedium Deliver and Copy to DLP SOX

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Copy to DLP SOX

### SSN Policy:

Close the Regulatory disclosure triangle and open the “Privacy Protection” disclosure triangle. Click the “Add” button to the left of “US Social Security Numbers” — the very last row.

Name: US Social Security Numbers

Severity Settings:

Critical Severity Incident: Copy to DLP SSN

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Inherit Action from Medium Severity Incident

## ESA/SMA INSTALLATION AND BEST PRACTICES

### US Drivers License Policy:

Open the “Privacy Protection” disclosure triangle. Click the “Add” button to the left of “US Drivers License Numbers” — the 5th row from the bottom.

Name: US Drivers License Numbers

Severity Settings:

Critical Severity Incident: Copy to DLP US Drivers License

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Inherit Action from Medium Severity Incident

**NOTE:** Go to Mail Policies > DLP Policy Manager and within the Advanced Settings section there is a hypertext button to the right of “US Drivers Licenses” named “All Classifiers Enabled”. Click the hypertext. These Global settings are used in policies that refer to US Drivers Licenses. For example, general policies like GLBA and state-specific policies like California AB-1298 and Montana HB-732 use them. If you experience a high number of false positives on any Policy that matches US Drivers License (not just the one we created above), or if you are concerned about ESA CPU Performance, deselect states in which you do not conduct business.

### Step D: Apply the DLP Policies to the Default Outgoing Mail Policy

Navigate to:

*Mail Policies > Outgoing Mail Policies*

Click on the control cell for DLP for the Default Policy. It will read “Disabled” if you have not enabled it yet.

Change the pulldown button from Disable DLP to Enable DLP and you will immediately be presented with all the DLP Policies you just created.

Click the “Enable All” checkbox.

Submit and then Commit the changes.

### Step E: Learn to create Custom DLP Policies and Custom Classifiers

Navigate to:

*Mail Policies > DLP Policy Customizations*

## ESA/SMA INSTALLATION AND BEST PRACTICES

The “Custom Classifiers” table is empty. Play around with creating your own Custom Classifier. These custom classifiers can be very powerful when building your own Custom DLP Policy.

You can build custom classifiers with one or many “rules”. Each rule can be of either:

To create a Custom DLP Policy, navigate to: Word or Phrase, Regular Expression, Dictionary, or Entity. Entities are objects that RSA provides and uses in pre-defined DLP policies. This allows you to combine entities in a way that no pre-defined DLP Policy has done. You’ll see next how to use the “NOT” operator to tune out false positives.

If you set the Rule type to Dictionary you are allowed to actually see and use the integrated RSA Dictionaries for matching.

*Mail Policies > DLP Policy Manager*

Click the Add DLP Policy button. Open the Custom Policy disclosure triangle and click Add.

When you click the “Content Matching Classifier” button, a list of classifiers are shown with the Custom Classifiers (the ones you created) are at the top.

Choose any classifier and click the Add button on the right. This adds the classifier to the “Match Classifiers” table. Within that table you can choose the NOT checkbox to set the Policy to only consider it a Match if that particular classifier does NOT match the message content. Nice way to tune out false positives.

### **G. MULTIPLE ESA APPLIANCES**

In a production environment you will have multiple ESA appliances. This section will discuss and demonstrate:

1. Configuring additional ESA appliances
2. Adding additional ESA appliances to the SMA
3. Creating Centralized Reporting Groups on the SMA

Configuring additional ESA appliances

At this point you have upgraded your first ESA and completely configured it. We will use the Cisco ESA “cluster” technology to quickly add additional ESA appliances and keep their configuration in sync for all future changes.

## ESA/SMA INSTALLATION AND BEST PRACTICES

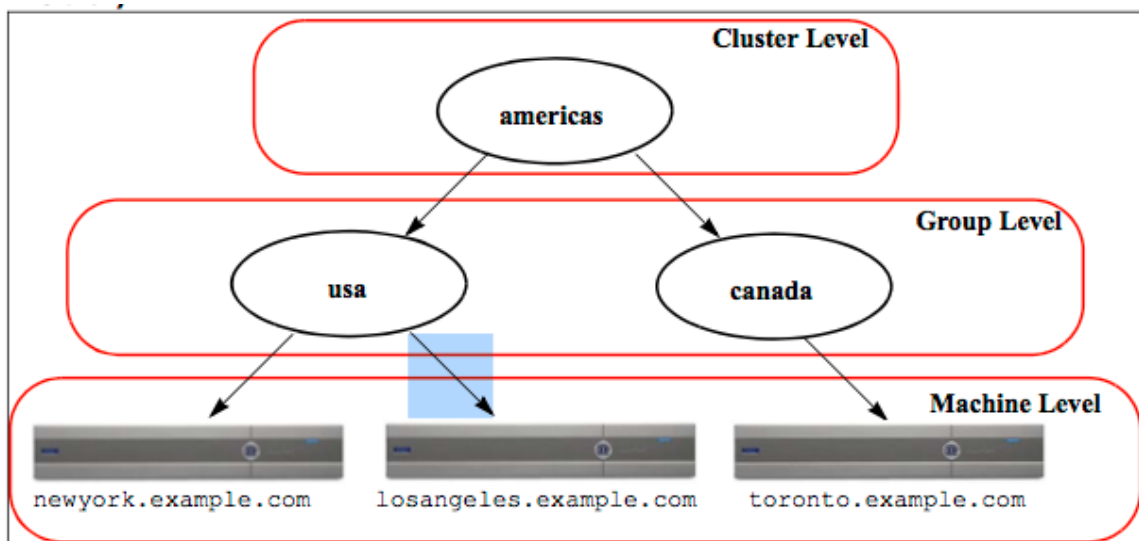
The clustering technology on the ESA allows you to manage multiple appliances at the same time. A cluster is defined as a set of machines that share configuration information. Within the cluster, ESAs are divided into *groups*. Every cluster contains at least one group. When making configuration changes on an ESA, you can configure certain portions of the configuration to be at the cluster level, the group level, or even at machine level.

All ESAs in the cluster are at the same “level” — they are peers — there is not Master/Slave relationship within a cluster. Once your ESAs are in the cluster, you can login to any ESA in the cluster and make a cluster-level change and that change is immediately applied to all ESAs in the cluster. If you make a group-level config change, then all ESAs that you have placed in that group are updated with the config change.

There is only one Cluster but you can have many Groups within the Cluster. All ESA appliances must be on the same version of code. The ESA models do not need to be the same — you can cluster a C380 with a C100v (a small virtual appliance) — for example.

There are three levels to the cluster: Cluster Level, Group Level, and Machine Level.

Here is a depiction:



### Creating and Joining a Cluster

You cannot create or join a cluster from the webUI (GUI). You must use the CLI. Once you have created the cluster you can make changes from either the CLI or the webUI.

## ESA/SMA INSTALLATION AND BEST PRACTICES

In my deployment, I've already configured my first ESAv ([esa1.unc-hamiltons.com](http://esa1.unc-hamiltons.com)) running at 10.0.1.37/24. Below I will add a second ESAv appliance and give it a hostname of [esa2.unc-hamiltons.com](http://esa2.unc-hamiltons.com) and assign it 10.0.1.38/24.

The C300v is running 9.5.0-201. My C000v has not been upgraded at all and is running 9.1.0-032. In order to cluster them, they must be on the exact same version and build.

Before we configure the new C000v appliance, I will first create the cluster using the already configured C300v.

### Step 1: Create the cluster

Even though I may have 10 or 15 or 20 ESAs to deploy, I always only work with the first appliance initially and configure it completely and then I use that ESA (fully configured) to create the cluster. That does not make that particular ESA the "Master" because there is no Master/Slave in the ESA clustering technology — all ESA appliances are at the same level once they are in the cluster.

Here is how I created the cluster from [esa1.unc-hamiltons.com](http://esa1.unc-hamiltons.com).

I logged in to esa1 from an ssh session.

```
esa1.unc-hamiltons.com> clusterconfig

Do you want to join or create a cluster?
1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.
[1]> 2

Enter the name of the new cluster.
[1]> UNC-HAMILTONS

Should all machines in the cluster communicate with each other by hostname or by IP address?
1. Communicate by IP address.
2. Communicate by hostname.
[2]> 1

What IP address should other machines use to communicate with Machine esa1.unc-hamiltons.com?
1. 10.0.1.37 port 22 (SSH on interface Management)
2. Enter an IP address manually
[1]> 1

Other machines will communicate with Machine esa1.unc-hamiltons.com using IP address 10.0.1.37 port
22. You can change this by using the COMMUNICATION subcommand of the clusterconfig command.

New cluster committed: Sat Jun 13 11:48:23 2015 CDT

Creating a cluster takes effect immediately, there is no need to commit.

Cluster UNC-HAMILTONS

Choose the operation you want to perform:
- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETGROUP - Remove a cluster group.
- REMOVEACHINE - Remove a machine from the cluster.
```



## ESA/SMA INSTALLATION AND BEST PRACTICES

- SETNAME - Set the cluster name.
  - LIST - List the machines in the cluster.
  - CONNSTATUS - Show the status of connections between machines in the cluster.
  - COMMUNICATION - Configure how machines communicate within the cluster.
  - DISCONNECT - Temporarily detach machines from the cluster.
  - RECONNECT - Restore connections with machines that were previously detached.
  - PREPJOIN - Prepare the addition of a new machine over CCS.
- ```
[]>
```

(Cluster UNC-HAMILTONS)>

### Step 2: Joining a new ESA to the already created cluster.

Whether the second ESA is a Hardware appliance or a Virtual appliance, it is probably not on the same version of code as the first ESA that created the cluster. All appliances must be on the same version of code. In my case, I had to upgrade my new C000v to 9.5.0-201.

**NOTE:** Never upgrade a HW appliance from a console connection on the serial port of the appliance. Always use the console connection only to get the IP address configured and then ssh (or Putty) into the ESA and do the upgrade. There is a known issue whereby if you issue the upgrade command from the console connection it will take a very long time.

The steps to get the new ESA appliance ready to join the cluster are:

- Understand the Licenses/Features that you have on the first appliance by going to System Administration > Feature Keys. The licenses should be the same for all appliances in the cluster. We will verify the keys on the second/new appliance in the steps to follow.

Connect to the console of the new ESA appliance:

- Issue the following commands:

```
interfaceconfig
```

*Note: Be sure to use the same "IP interface name" that you used on the first ESA. Below is an example this from my first [esa1.unc-hamiltons.com](http://esa1.unc-hamiltons.com) ESA appliance. I run the "interfaceconfig" command and type in edit and provide the interface number (1 in this case). It then asks me for the Interface name. I did not change it from the default name of "Management".*

*The Interface settings are Machine specific settings but the Listener (the port 25 smtp process) is a cluster setting. The Listener runs on IP interfaces specified by text string IP Interface names. So if the "cluster" is configured for the Listener to*

## ESA/SMA INSTALLATION AND BEST PRACTICES

run on “Management” then each Interface name Machine setting needs to have the same IP Interface name.

Here is the setting I’m talking about. Below is from my esa1 and I’m only pasting the top portion of the out put from the interfaceconfig command that is relevant:

```
(Machine esa1.unc-hamiltons.com)> interfaceconfig
Currently configured interfaces:
1. Management (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.
[ ]> edit

Enter the number of the interface you wish to edit.
[ ]> 1

IP interface name (Ex: "InternalNet"):
[Management]> ***** This is the setting. *****

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

---

Now run the following remaining commands:

```
setgateway
dnsconfig
sethostname
commit (be sure to commit changes before you continue)
```

The details for the above commands were covered in Section C of this document when we configured the first ESA appliance.

- c) Virtual Appliance Only: If your new appliance is an ESAv virtual appliance you need to install a license file into the appliance. You can use the same license file for all your virtual appliances so if your ‘first’ ESA was a virtual appliance, use the same license file.

To install the license file, ftp to the new ESAv and login as admin/ironport. “cd configuration” and put the license file into that configuration directory.

Now ssh (or Putty) into the new ESAv and issue the “loadlicense” command. Choose the option to load the license from a file and provide the name of the license file that you just placed on the ESAv when you did the FTP above.

- d) Now upgrade your appliance to the same version of code the first appliance is running. I use the “upgrade” command from the CLI and issue the DOWNLOAD

## ESA/SMA INSTALLATION AND BEST PRACTICES

sub-command and then the INSTALL sub-command once the new image has been downloaded. Again, the upgrade process is detailed earlier in this document. Upgrading from the webUI (GUI) is also possible under *System Administration > Upgrade*.

- e) Now we want to add the new ESA to the SMA. On the webUI of the SMA, go to *Management Appliance > Centralized Services > Security Appliances* and click the Add Email Appliance button. My settings were as follows:

Name: esa2

IP Address: 10.0.1.38

ESA Centralized Services: Check all checkboxes

Now click the Establish Connection button and type in the admin/ironport password.

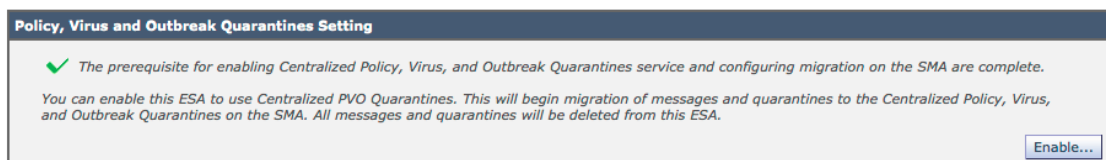
Submit.

On the SMA, now go to *Centralized Services > Policy Virus and Outbreak Quarantines*.

Click the “Launch Migration Wizard” button.

Commit changes

- f) Now on the new ESA on the webUI navigate to *Security Services > Policy, Virus, and Outbreak Quarantines*. You should now be able to click the Enable button.



Commit changes

- g) The next step will be to join the new ESA to the cluster. You can only join the cluster from the CLI. SSH or Putty into the new ESA appliance. Here is how I joined my second ESA to the already existing cluster:

```
esa2.unc-hamiltons.com> clusterconfig
```

```
Do you want to join or create a cluster?
```

1. No, configure as standalone.
  2. Create a new cluster.
  3. Join an existing cluster over SSH.
  4. Join an existing cluster over CCS.
- ```
[1]> 3
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

While joining a cluster, you will need to validate the SSH host key of the remote machine to which you are joining. To get the public host key fingerprint of the remote host, connect to the cluster and run: `logconfig -> hostkeyconfig -> fingerprint`.

**WARNING:** All non-network settings will be lost. System will inherit the values set at the group or cluster mode for the non-network settings. Ensure that the cluster settings are compatible with your network settings (e.g. `dnsconfig` settings)

Exception: Centralized Policy, Virus, and Outbreak Quarantine settings are not inherited from the cluster. These settings on this machine will remain intact.

Do you want to enable the Cluster Communication Service on `esa2.unc-hamiltons.com`? [N]>

Enter the IP address of a machine in the cluster.

[ ]> 10.0.1.37

Enter the remote port to connect to. This must be the normal admin ssh port, not the CCS port.

[22]>

Enter the name of an administrator present on the remote machine

[admin]>

Enter password:

Joining cluster group `Main_Group`.

The machine added to the cluster runs DLP engine (version 3.0.2.31)

**WARNING:** Please run the `'dlpstatus'` command on a machine in the cluster and ensure the new machine has the same DLP engine version. Otherwise, DLP scanning may not work properly.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster `UNC-HAMILTONS`

Choose the operation you want to perform:

- `ADDGROUP` - Add a cluster group.
- `SETGROUP` - Set the group that machines are a member of.
- `RENAMEGROUP` - Rename a cluster group.
- `DELETEDGROUP` - Remove a cluster group.
- `REMOVEMACHINE` - Remove a machine from the cluster.
- `SETNAME` - Set the cluster name.
- `LIST` - List the machines in the cluster.
- `CONNSTATUS` - Show the status of connections between machines in the cluster.
- `COMMUNICATION` - Configure how machines communicate within the cluster.
- `DISCONNECT` - Temporarily detach machines from the cluster.
- `RECONNECT` - Restore connections with machines that were previously detached.
- `PREPJOIN` - Prepare the addition of a new machine over CCS.

[ ]>

(Cluster `UNC-HAMILTONS`)>

Now issue the “list” `clusterconfig` command:

Choose the operation you want to perform:

- `ADDGROUP` - Add a cluster group.
- `SETGROUP` - Set the group that machines are a member of.
- `RENAMEGROUP` - Rename a cluster group.
- `DELETEDGROUP` - Remove a cluster group.
- `REMOVEMACHINE` - Remove a machine from the cluster.
- `SETNAME` - Set the cluster name.
- `LIST` - List the machines in the cluster.
- `CONNSTATUS` - Show the status of connections between machines in the cluster.
- `COMMUNICATION` - Configure how machines communicate within the cluster.
- `DISCONNECT` - Temporarily detach machines from the cluster.
- `RECONNECT` - Restore connections with machines that were previously detached.
- `PREPJOIN` - Prepare the addition of a new machine over CCS.

[ ]> list

Cluster `UNC-HAMILTONS`

=====

Group `Main_Group`:

Machine `esa1.unc-hamiltons.com` (Serial #: 564DF56D18Exxxxxxxx-xxxxxxxxxxxx)

Machine `esa2.unc-hamiltons.com` (Serial #: 564D7C71EDExxxxxxxx-xxxxxxxxxxxx)

# ESA/SMA INSTALLATION AND BEST PRACTICES

Cluster UNC-HAMILTONS

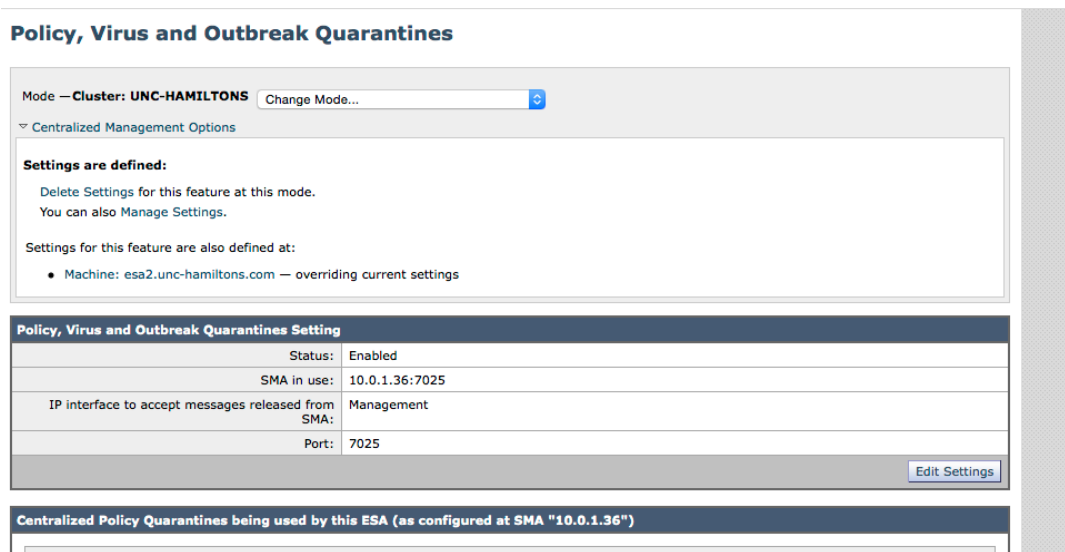
Once you see the “Cluster UNC-HAMILTONS” prompt, this means the new ESA is in the cluster.

Remove the Mode – Machine: PVO Settings

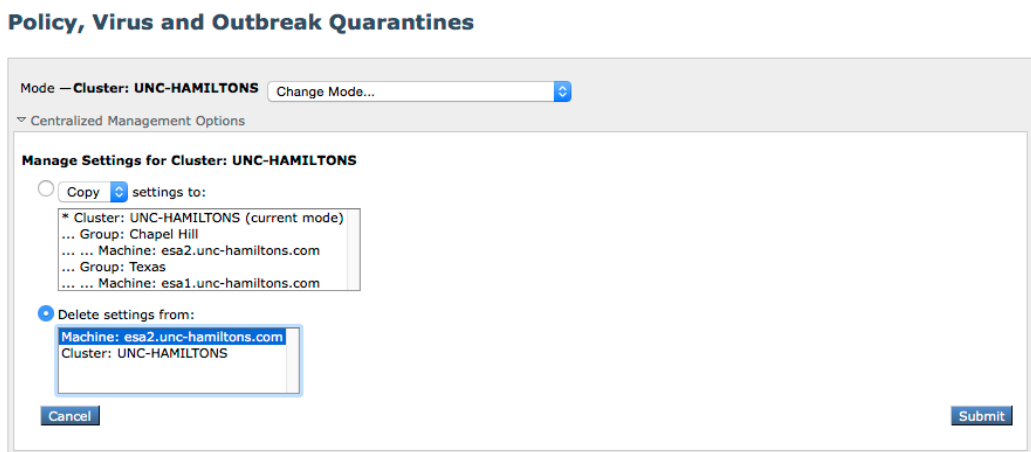
Login to the webUI of the new ESA appliance. The webUI has slightly changed and you can see that your appliance is now in the cluster.

Navigate to *Centralized Services > Policy, Virus, and Outbreak Quarantines*

Here is what I see — note I have opened the disclosure triangle for “Centralized Management Options”



Click the “Manage Settings” hypertext link. You’ll see something like this:



We want to remove all Machine settings for PVO. We only want to keep the Cluster: UNC-HAMILTONS settings. In my case, I do not see Machine settings for esa1 but I do see them for “Machine: [esa2.unc-hamiltons.com](http://esa2.unc-hamiltons.com)” settings.

I clicked on the “Delete settings from:” radio button and selected “Machine: [esa2.unc-hamiltons.com](http://esa2.unc-hamiltons.com)”

Click the Submit button.

By clicking Submit it removes the Machine settings but doesn’t make the window close — it just performs the action defined.

Therefore to close the window, click the Cancel button.

Commit changes.

At this point there is now only a single PVO configuration in the Cluster and that is a Cluster-Level setting. Both [esa1.unc-hamiltons.com](http://esa1.unc-hamiltons.com) and [esa2.unc-hamiltons.com](http://esa2.unc-hamiltons.com) are using the Cluster-Level PVO Settings.

At this point esa2 is completely setup and ESA1 and ESA2 are clustered. Most all settings are at a “Cluster” level.

From this point forward, to make any changes to your ESA configuration, you simply login to either esa1 or esa2 and make the change and commit the changes. The change will be applied to all systems in the cluster.

Only a few things are not a Cluster-Level: (example)

- Monitor > (all the reports and Message Tracking)*
- Network > Interfaces*
- System Administration > Trace*
- System Administration > Disk Management (which you should not need to modify)*
- System Administration > Feature Keys*

Those are very few items and are very seldom changed. Therefore, as you can see, nearly all of the configuration is at the Cluster-Level.

Some customers have upwards to 20 or 25 appliances in a single cluster.

## ESA/SMA INSTALLATION AND BEST PRACTICES

### Different Cluster Groups to Differentiate DNS Config for two Data Centers

In my example I have a C300v and a C000v in my cluster at this point. For example purposes let's assume I have two Data Centers — one in Texas and one in Chapel Hill. The C300v is in the Texas data center and the C000v is in the Chapel Hill data center. Let's create two different Cluster Groups and place the appliances in the appropriate group.

When we created the cluster, we named the cluster “UNC-HAMILTONS”. Creating the cluster automatically created the default Cluster Group named “Main\_Group”. Since “Main\_Group” is the only group, all ESA appliances are in the Main\_Group by default.

Below I rename the “Main\_Group” to “Texas” and at that point, all of my appliances are in the “Texas” cluster group.

<once you're in the clusterconfig command, issue the renamegroup command>

```
[> renamegroup
Choose which group you wish to rename.
1. Main_Group
[1]>
Enter the new name of the group.
[Main_Group]> Texas
Group Main_Group renamed to Texas.
Cluster UNC-HAMILTONS
```

**NOTE:** You must 'commit' changes

Now create the “Chapel Hill” cluster group and then put the C000v (esa2) in that group.

<once you're in the clusterconfig command, issue the addgroup command>

```
[> addgroup
Enter the name of the new cluster group to create.
[> Chapel Hill
Cluster group Chapel Hill created.
Cluster UNC-HAMILTONS
Choose the operation you want to perform:
- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
```

## ESA/SMA INSTALLATION AND BEST PRACTICES

- PREPJOIN - Prepare the addition of a new machine over CCS.  
[> setgroup

Choose the machine to move to a different group. Separate multiple machines with commas.

1. esa1.unc-hamiltons.com (group Texas)  
2. esa2.unc-hamiltons.com (group Texas)  
[1]> 2

Choose the group that esa2.unc-hamiltons.com should be a member of.

1. Chapel Hill  
2. Texas  
[1]> 1

esa2.unc-hamiltons.com set to group Chapel Hill.  
Cluster UNC-HAMILTONS

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEDGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.

[>

Now list the group assignments:

[> list

Cluster UNC-HAMILTONS

=====

Group Chapel Hill:

Machine esa2.unc-hamiltons.com (Serial #: 564D7C71EDE7CC74A911-3F15CEE67AE8)

Group Texas:

Machine esa1.unc-hamiltons.com (Serial #: 564DF56D18E45A4F00DE-BFB8C738BAB6)

Cluster UNC-HAMILTONS

**NOTE: You must 'commit' changes before they take affect**

Now let's give an example of how multiple Groups can be beneficial. In this next step we will change the DNS configuration for all appliances in the Chapel Hill group to be Group settings instead Cluster config. This allows you to change the DNS config for those ESA appliances in the Chapel Hill group to be different than the Cluster settings.

Time Zone settings and SMTP Routes are also two additional configuration panels that are sometimes moved from Cluster-Level to Group-Level to accommodate for the need to have different settings due to different locations of the Data Centers.

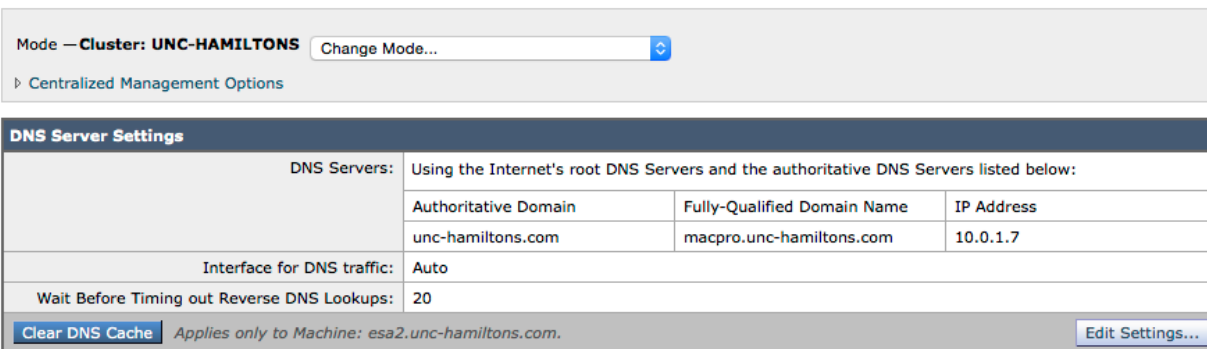
For this example, let's change the DNS settings to demonstrate how this works.

Step 1: Navigate to Network > DNS

Note the mode is "Mode — Cluster: UNC-HAMILTONS".



## ESA/SMA INSTALLATION AND BEST PRACTICES



Mode — **Cluster: UNC-HAMILTONS**

▸ Centralized Management Options

**DNS Server Settings**

DNS Servers: Using the Internet's root DNS Servers and the authoritative DNS Servers listed below:

| Authoritative Domain | Fully-Qualified Domain Name | IP Address |
|----------------------|-----------------------------|------------|
| unc-hamiltons.com    | macpro.unc-hamiltons.com    | 10.0.1.7   |

Interface for DNS traffic: Auto

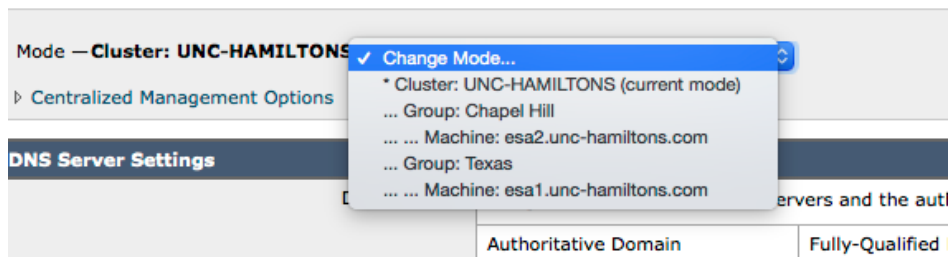
Wait Before Timing out Reverse DNS Lookups: 20

[Clear DNS Cache](#) *Applies only to Machine: esa2.unc-hamiltons.com.* [Edit Settings...](#)

This means that there is DNS Configuration settings at the Cluster level. Of course there should be because all appliance (both Cluster Groups) are using the Cluster DNS settings.

Now let's change the DNS settings to be at a Group level for both the Texas group and the Chapel Hill group.

Below, I clicked on the “Change Mode” and selected “Group: Chapel Hill”



Mode — **Cluster: UNC-HAMILTONS**

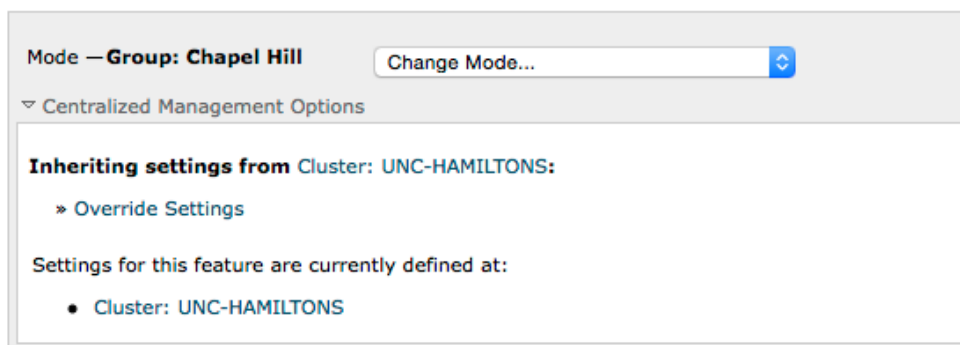
- ✓ Change Mode...
- \* Cluster: UNC-HAMILTONS (current mode)
- ... Group: Chapel Hill
- ... .. Machine: esa2.unc-hamiltons.com
- ... Group: Texas
- ... .. Machine: esa1.unc-hamiltons.com

▸ Centralized Management Options

**DNS Server Settings**

| Authoritative Domain | Fully-Qualified |
|----------------------|-----------------|
|----------------------|-----------------|

Next, below I clicked on the “Override Settings” hypertext:



Mode — **Group: Chapel Hill**

▾ Centralized Management Options

**Inheriting settings from Cluster: UNC-HAMILTONS:**

- » [Override Settings](#)

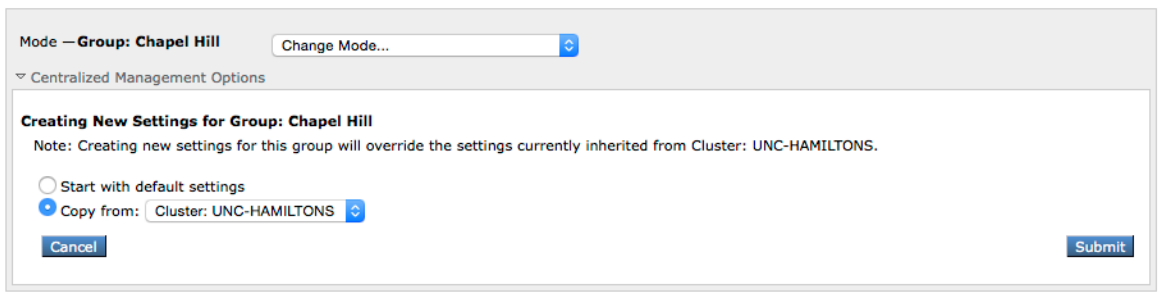
Settings for this feature are currently defined at:

- [Cluster: UNC-HAMILTONS](#)

I then clicked on the Copy from: [Cluster: UNC-HAMILTONS]

I then clicked the “Submit” button.

Commit changes.



You will now see the Group: Chapel Hill now has DNS Settings defined. This means that all ESAs in Group “Chapel Hill” will use those settings instead of the Cluster settings.

The order of precedence is Machine settings always take the highest priority, then Group, and finally Cluster.

I could leave the Group: Texas DNS settings empty and then the C300v that is in that Group will use the Cluster settings, but I’d rather keep things consistent and if I am going to create Group Settings for Chapel Hill, then I like to set the for all Groups.

I used the steps above to do the same thing for the Texas group. At this point I can easily go to Network > DNS and select “Mode — Group: Chapel Hill” and set the DNS config for Group: Chapel Hill to point to DNS servers that are in the Chapel Hill data center.

Then commit changes. The “Mode — Group: Texas” is already setup correctly to point to the DNS servers in the Texas data center so no changes would need to be applied.

At this point I would then delete the Cluster mode DNS settings so that I never have to “remember” that I should be in Group mode for DNS settings.

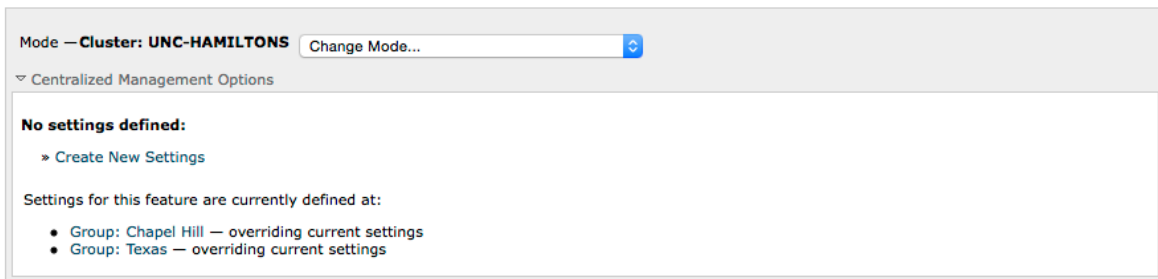
I go to Network > DNS and change the mode to “Cluster: UNC-HAMILTONS”. Note that you can be on this config panel and in this mode and be presented full DNS settings which can be misleading — if you’re not thinking, you would think you were looking at DNS config settings for the ESA appliances — which actually, neither of my ESA appliances are using the DNS Config stored at the Cluster level. Therefore, let’s eliminate the confusion.

I clicked opened the disclosure triangle for “Centralized Management Options”

I then clicked on “Delete Settings” for this feature at this mode.

I then clicked “Delete” to confirm.

I then see this when at Cluster mode for Network > DNS settings:



This is exactly what I’d like to see. Realize that nearly all of the remaining portion of the config is at the Cluster level. Your webUI will be at the Cluster level nearly all the time and if you then Navigate to Network > DNS (while in cluster mode), you will realize that there are no DNS settings at the mode and you will go to each Group mode to make the DNS changes — which is what we want to do because the ESA appliances are installed in different Data Centers.

## H. CENTRALIZED EMAIL REPORTING REPORTING GROUPS

What is Centralized Reporting Groups

There can be many reasons why you may want to have the option to view reporting data by “groups” of ESA appliances. Here I mean “Reporting Groups” so don’t confuse this with Cluster Groups that was discussed in the previous section. Reporting Groups can be configured on the SMA to allow you to see reporting data by groups of ESA appliances.

A typical use-case to see reports based on email flow through ESA appliances deployed in two different data centers. This would allow you to see how much traffic and the nature of the email traffic for one data center alone — instead of statistics from a company wide perspective.

In my example, I have ESA1 deployed in my Texas data center and ESA2 in my Chapel Hill data center.

Creating Centralized Reporting Groups

On the SMA, navigate to: *Management Appliance > Centralized Services > Centralized Reporting*

Click the Add Group button. Here is the “Texas Data Center” reporting group.

**Add Email Reporting Group**

The screenshot shows a web interface for adding an email reporting group. At the top, there's a header 'Add Email Reporting Group'. Below it, a 'Group' section contains a 'Group Name' field with the value 'Texas Data Center'. Underneath, there are two columns: 'Email Appliances' and 'Group Members'. The 'Email Appliances' column contains a list with one item: 'esa2 (10.0.1.38)'. The 'Group Members' column contains a list with one item: 'esa1 (10.0.1.37)'. Between these two columns are two buttons: 'Add »' and « Remove'. At the bottom left is a 'Cancel' button and at the bottom right is a 'Submit' button.

I

then

create

the “Chapel Hill Data Center” reporting group:

**Add Email Reporting Group**

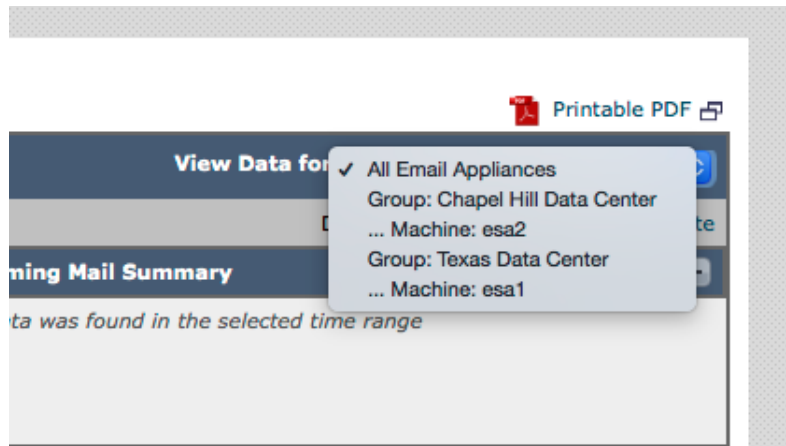
The screenshot shows the same web interface as above, but with different data. The 'Group Name' field now contains 'Chapel Hill Data Center'. The 'Email Appliances' column contains a list with one item: 'esa1 (10.0.1.37)'. The 'Group Members' column contains a list with one item: 'esa2 (10.0.1.38)'. The 'Add »' and « Remove' buttons are still present between the lists. The 'Cancel' and 'Submit' buttons are at the bottom.

Commit changes.

On the SMA, navigate to Email tab > Reporting > Overview

Click the “View Data for” pull-down button located at the top-right portion of the page. Here you can select what data the SMA uses for the reports that are displayed. Running reports with “All Email Appliances” selected will show you a holistic view of all messages. When Group: Texas is selected, the SMA will only include data from ESA appliances that have been placed in that Reporting Group when it generates the reporting metrics/statistics. You can even choose a specific Machine.

## ESA/SMA INSTALLATION AND BEST PRACTICES



### CONCLUSION

Hopefully this document has given you the understanding and steps to completely configure your new ESA and SMA appliances. With a document of this size, I'm sure there are some mistakes. If you do find some, please email them to "[dalton@cisco.com](mailto:dalton@cisco.com)" so that I may correct the document.

## ESA/SMA INSTALLATION AND BEST PRACTICES



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

---

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)