Mejores prácticas para la directiva centralizada, cuarentenas del virus y del brote puestas y migración del ESA al S A

Contenido

Introducción

Las cuarentenas siguientes se pueden ahora centralizar colectivamente en un dispositivo de la Administración del Cisco Security (S A):

- Contra virus
- Brote
- Cuarentenas de la directiva usadas para los mensajes por los cuales son cogidos: Filtros del mensajeFiltros contentosDirectivas de prevención de la pérdida de datos

La centralización de estas cuarentenas ofrece las siguientes ventajas:

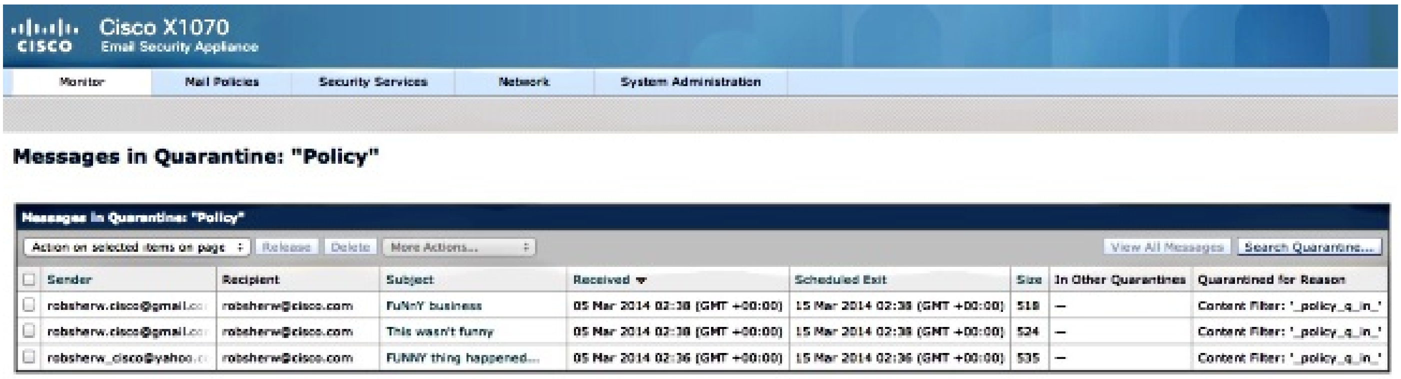
- Los administradores pueden manejar los mensajes quarantined de los dispositivos de seguridad múltiples del correo electrónico (ESA) en una ubicación.
- Los mensajes Quarantined se salvan detrás del Firewall en vez en del DMZ, reduciendo el riesgo de seguridad.
- Las cuarentenas centralizadas se pueden sostener como parte de la funcionalidad de backup estándar en el S A.

Prerequisites

- S A que ejecuta 8.1 (guía del usuario S A, capítulo 8, directiva centralizada, virus, y cuarentenas del brote)
- ESA que ejecuta 8.0.1 (guía del usuario ESA, capítulo 27, cuarentenas)
- Puerto de firewall 7025 /TCP (en y hacia fuera)/uso del nombre de host: AsyncOS IP/descripción: Pase la directiva, el virus, y los datos de la cuarentena del brote entre los dispositivos de seguridad del correo electrónico y el dispositivo de la Administración de seguridad cuando se centraliza esta característica

Configurar

Están comenzando con el ESA, en una cuarentena de la política existente, mensajes activos en la cuarentena de la directiva:



Cisco X1070
Email Security Appliance

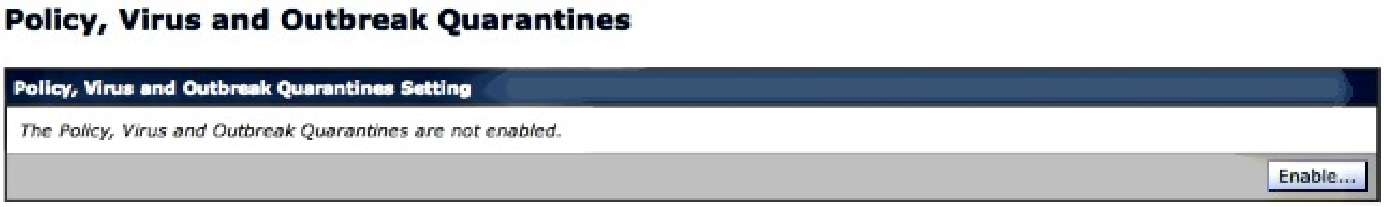
Messages in Quarantine: "Policy"

Messages in Quarantine: "Policy"

□	Sender	Recipient	Subject	Received ▼	Scheduled Exit	Size	In Other Quarantines	Quarantined for Reason
□	robsherw.cisco@gmail.co	robsherw@cisco.com	FuNnY business	05 Mar 2014 02:38 (GMT +00:00)	15 Mar 2014 02:38 (GMT +00:00)	518	—	Content Filter: '_policy_q_in_'
□	robsherw.cisco@gmail.co	robsherw@cisco.com	This wasn't funny	05 Mar 2014 02:38 (GMT +00:00)	15 Mar 2014 02:38 (GMT +00:00)	524	—	Content Filter: '_policy_q_in_'
□	robsherw_cisco@yahoo.c	robsherw@cisco.com	FUNNY thing happened...	05 Mar 2014 02:36 (GMT +00:00)	15 Mar 2014 02:36 (GMT +00:00)	535	—	Content Filter: '_policy_q_in_'

Para emigrar estos mensajes y después confiar en el S A para ser el dispositivo activo que posee la cuarentena de la directiva, complete las direcciones siguientes.

En el S A, navegue al **dispositivo de la Administración > los servicios > las cuarentenas centralizados de la directiva, del virus y del brote**. Si no habilitado ya, **permiso del** tecleo**:**



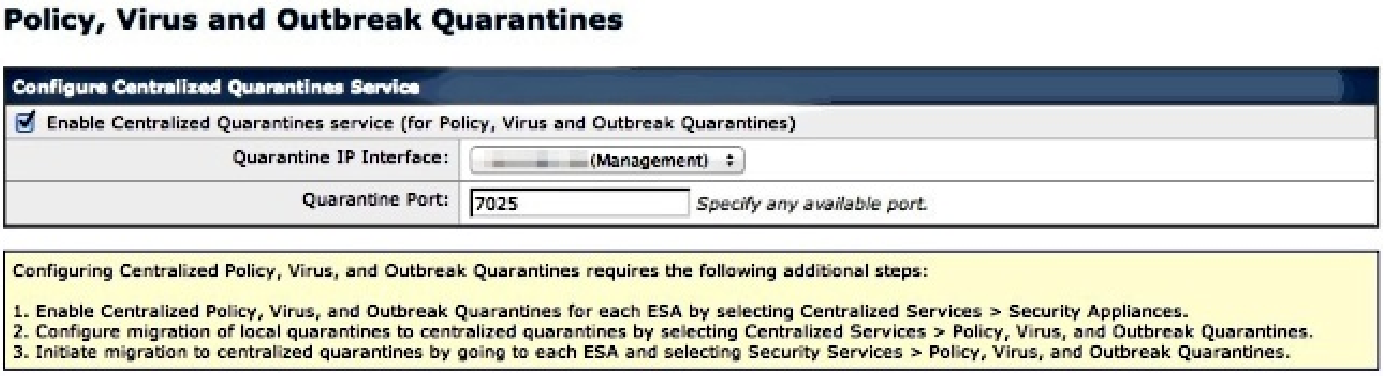
Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines Setting

The Policy, Virus and Outbreak Quarantines are not enabled.

Seleccione la interfaz, si procede, que se piensa para manejar el tráfico del ESA al S A.

> **Note**: El puerto de la cuarentena puede ser cambiado, pero éste necesitará ser abierto si hay un Firewall/una red ACL en el lugar.



Policy, Virus and Outbreak Quarantines

Configure Centralized Quarantines Service

☑ Enable Centralized Quarantines service (for Policy, Virus and Outbreak Quarantines)

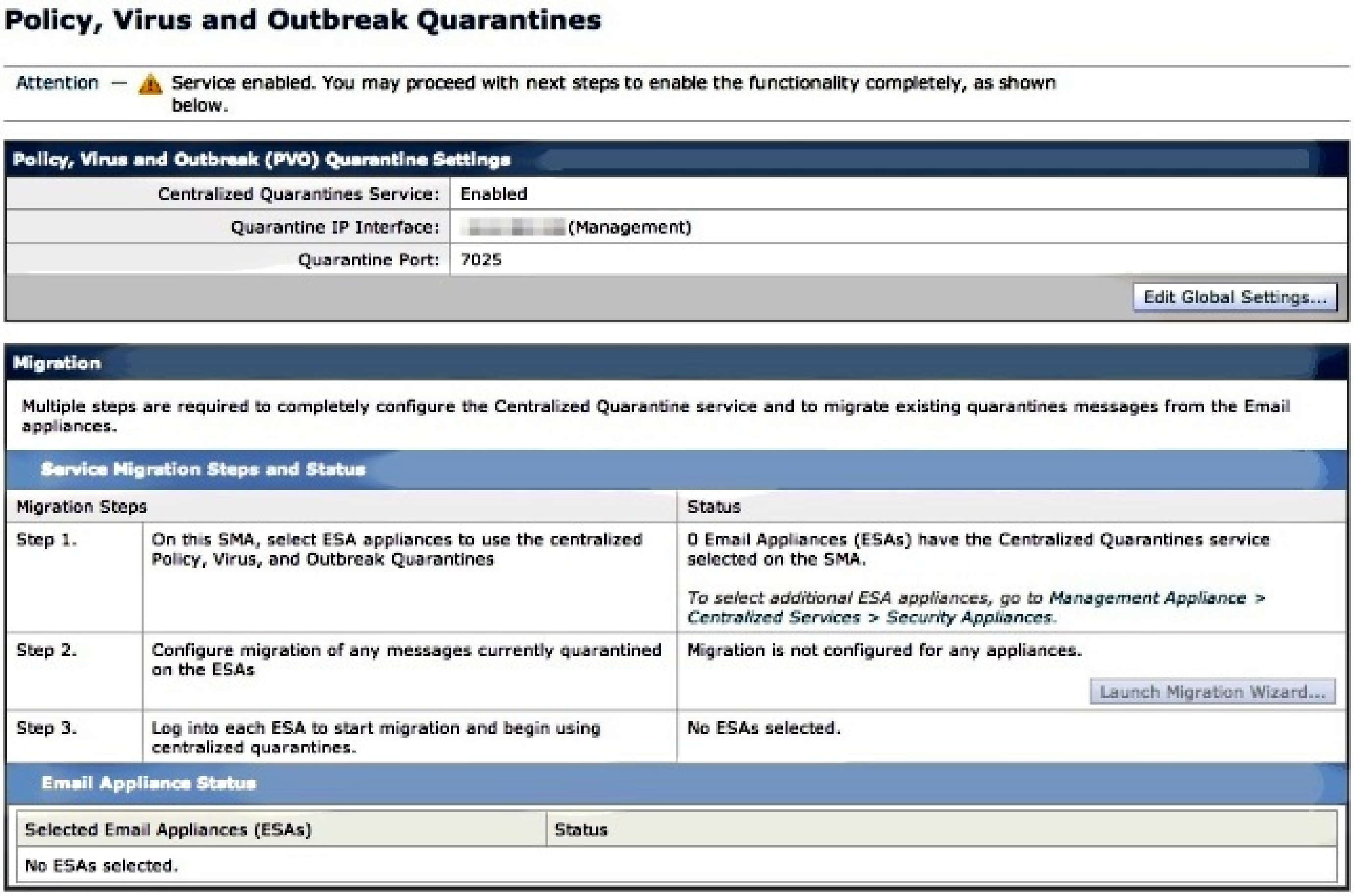
Quarantine IP Interface: (Management)

Quarantine Port: 7025 *Specify any available port.*

Configuring Centralized Policy, Virus, and Outbreak Quarantines requires the following additional steps:

1. Enable Centralized Policy, Virus, and Outbreak Quarantines for each ESA by selecting Centralized Services > Security Appliances.
2. Configure migration of local quarantines to centralized quarantines by selecting Centralized Services > Policy, Virus, and Outbreak Quarantines.
3. Initiate migration to centralized quarantines by going to each ESA and selecting Security Services > Policy, Virus, and Outbreak Quarantines.

Haga clic en Submit (Enviar). ¿La pantalla restaurará para mostrar? ¿Servicio habilitado? mensaje, visto abajo:



Policy, Virus and Outbreak Quarantines

Attention — ⚠ Service enabled. You may proceed with next steps to enable the functionality completely, as shown below.

Policy, Virus and Outbreak (PVO) Quarantine Settings

Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	[redacted] (Management)
Quarantine Port:	7025

Edit Global Settings...

Migration

Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.

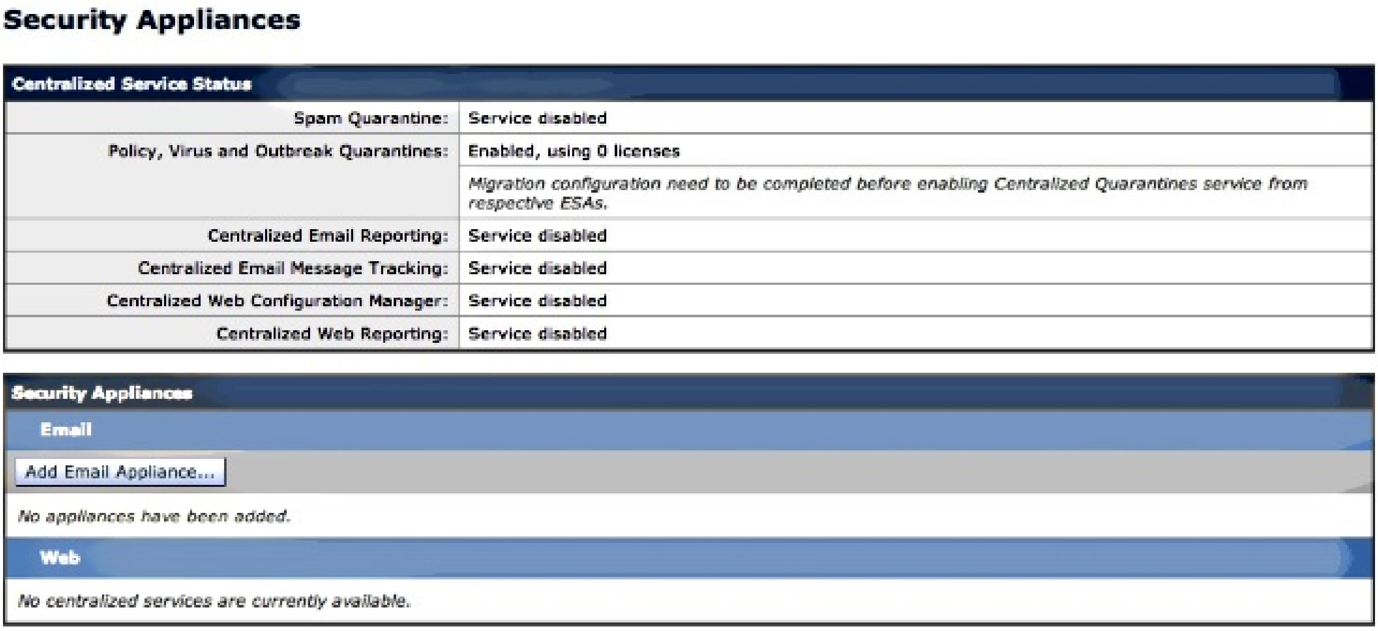
Service Migration Steps and Status

Migration Steps		Status
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	0 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. *To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.*
Step 2.	Configure migration of any messages currently quarantined on the ESAs	Migration is not configured for any appliances. Launch Migration Wizard...
Step 3.	Log into each ESA to start migration and begin using centralized quarantines.	No ESAs selected.

Email Appliance Status

Selected Email Appliances (ESAs)	Status
No ESAs selected.	

Navegue al **dispositivo de la Administración > los dispositivos centralizados del > Security (Seguridad) de los servicios** y agregue la comunicación ESA al S A:



Security Appliances

Centralized Service Status

Spam Quarantine:	Service disabled
Policy, Virus and Outbreak Quarantines:	Enabled, using 0 licenses *Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.*
Centralized Email Reporting:	Service disabled
Centralized Email Message Tracking:	Service disabled
Centralized Web Configuration Manager:	Service disabled
Centralized Web Reporting:	Service disabled

Security Appliances

Email

Add Email Appliance...

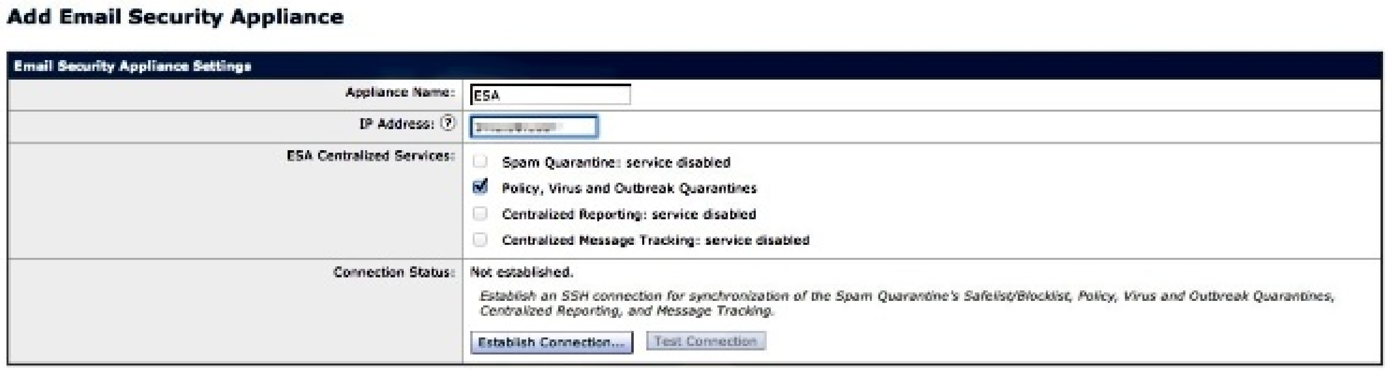
No appliances have been added.

Web

No centralized services are currently available.

El tecleo **agrega el dispositivo del correo electrónico**.

> **Note**: Usted necesita solamente agregar la dirección IP que el S A utilizará para comunicar con el ESA. El nombre del dispositivo se utiliza solamente como referencia administrativa.

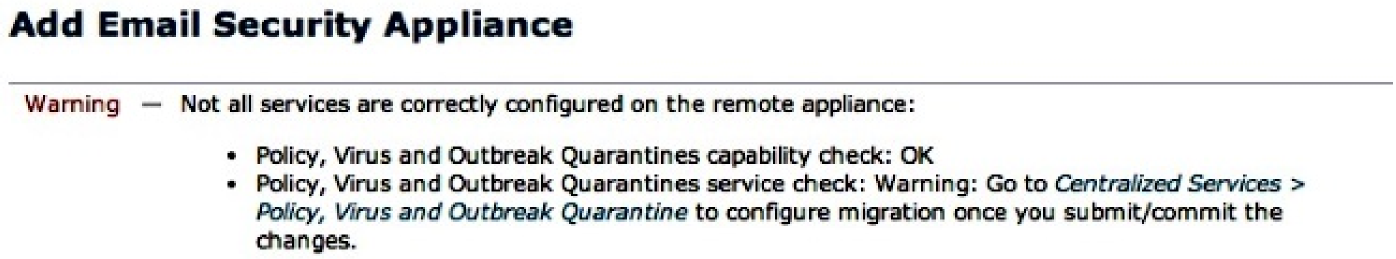


Add Email Security Appliance

Email Security Appliance Settings

Appliance Name:	ESA
IP Address:	[redacted]
ESA Centralized Services:	□ Spam Quarantine: service disabled ☑ Policy, Virus and Outbreak Quarantines □ Centralized Reporting: service disabled □ Centralized Message Tracking: service disabled
Connection Status:	Not established. *Establish an SSH connection for synchronization of the Spam Quarantine's Safelist/Blocklist, Policy, Virus and Outbreak Quarantines, Centralized Reporting, and Message Tracking.*

Esté seguro **de establecer la conexión** y la **conexión de prueba**. Sobre el establecimiento de la conexión del S A al ESA, el nombre y la contraseña de usuario administrador serán pedidos. Ésta es el usuario administrador y la contraseña del ESA se está agregando que. De acuerdo con cuál es ya activo contra lo que se está agregando, los resultados de la prueba pueden variar, pero deben ser similares a:



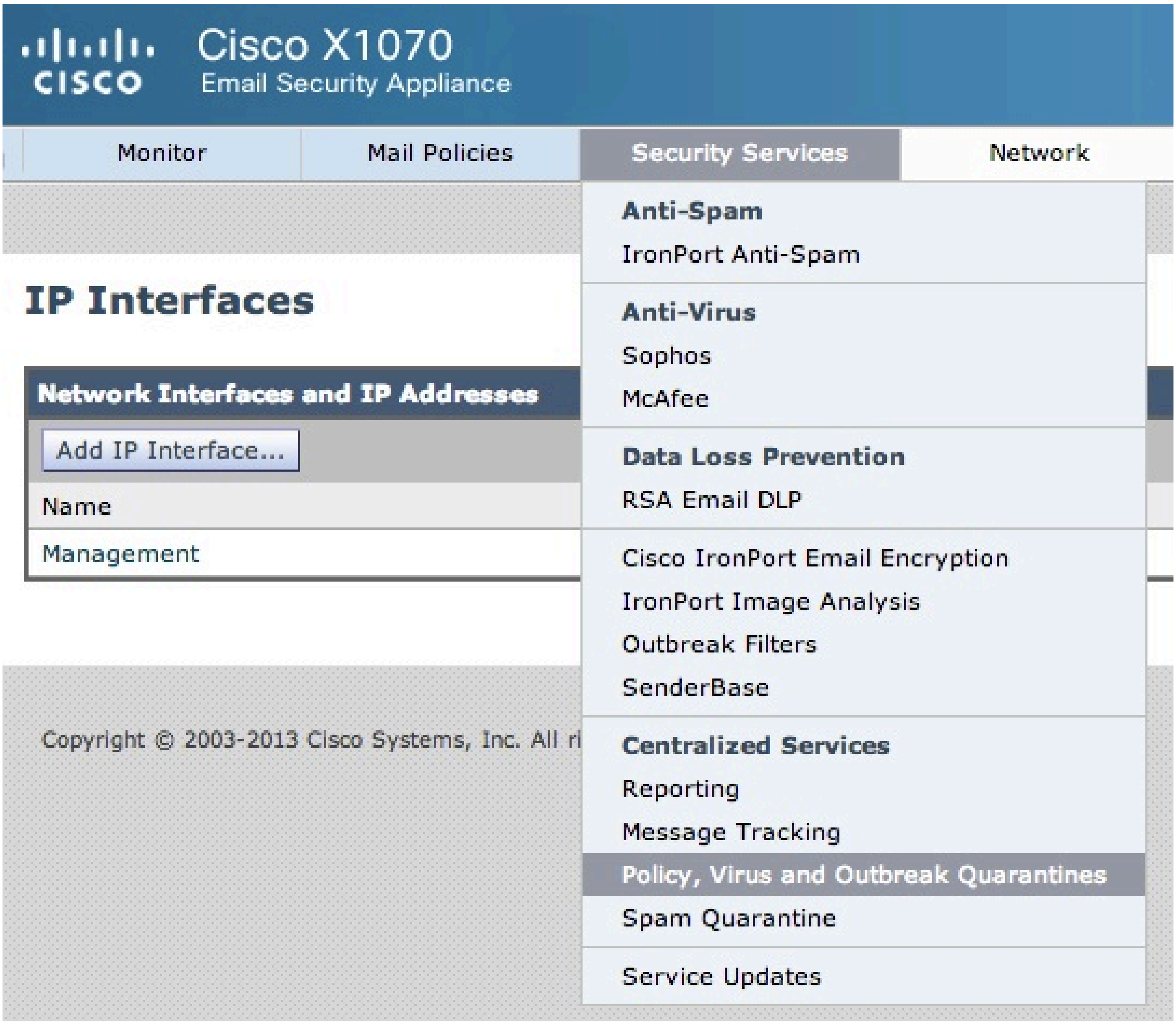
Add Email Security Appliance

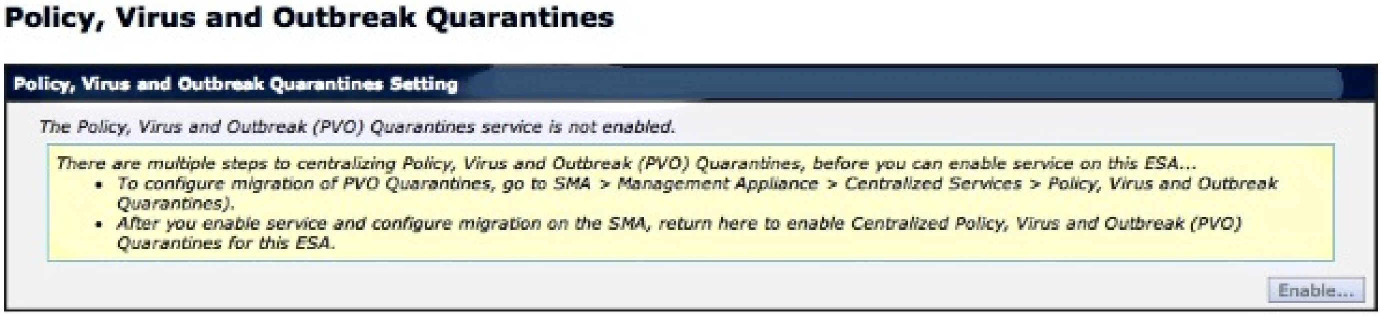
Warning — Not all services are correctly configured on the remote appliance:

- Policy, Virus and Outbreak Quarantines capability check: OK
- Policy, Virus and Outbreak Quarantines service check: Warning: Go to *Centralized Services > Policy, Virus and Outbreak Quarantine* to configure migration once you submit/commit the changes.

Esté seguro **de someter** y **de confiar los cambios** en este momento en el S A.

Ahora, si usted revisitara el ESA e intentara configurar la sección centralizada de los servicios de la cuarentena de la directiva, sería similar al siguiente:



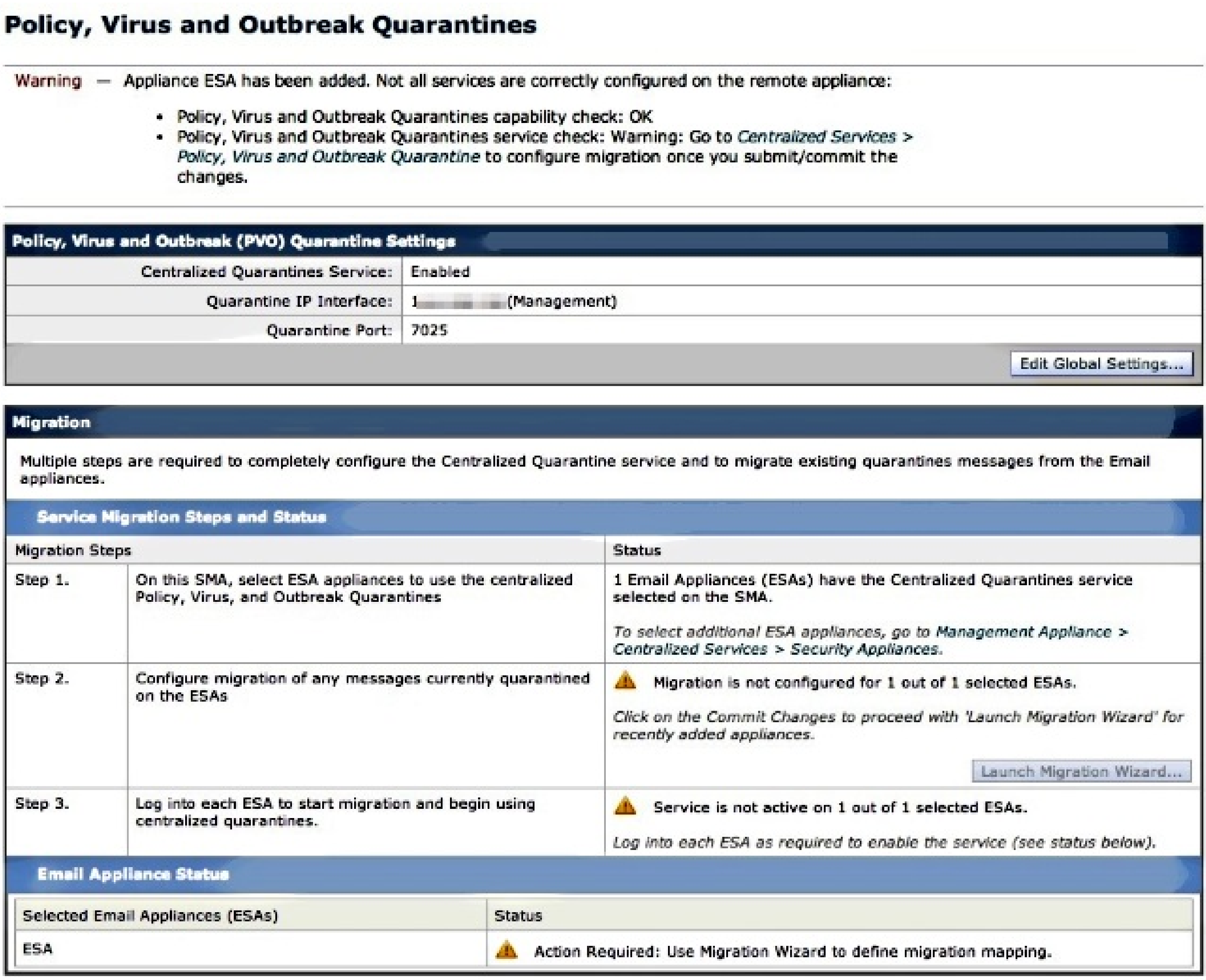

Policy, Virus and Outbreak Quarantines
Policy, Virus and Outbreak Quarantines Setting
Enable...

The Policy, Virus and Outbreak (PVO) Quarantines service is not enabled.

There are multiple steps to centralizing Policy, Virus and Outbreak (PVO) Quarantines, before you can enable service on this ESA...

- *To configure migration of PVO Quarantines, go to SMA > Management Appliance > Centralized Services > Policy, Virus and Outbreak Quarantines).*
- *After you enable service and configure migration on the SMA, return here to enable Centralized Policy, Virus and Outbreak (PVO) Quarantines for this ESA.*

Los pasos de la migración se deben todavía completar en el S A. Vuelva al S A y continúe con la sección siguiente.



Policy, Virus and Outbreak Quarantines

Warning — Appliance ESA has been added. Not all services are correctly configured on the remote appliance:

- Policy, Virus and Outbreak Quarantines capability check: OK
- Policy, Virus and Outbreak Quarantines service check: Warning: Go to *Centralized Services > Policy, Virus and Outbreak Quarantine* to configure migration once you submit/commit the changes.

Policy, Virus and Outbreak (PVO) Quarantine Settings

Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	1[redacted](Management)
Quarantine Port:	7025

Migration

Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.

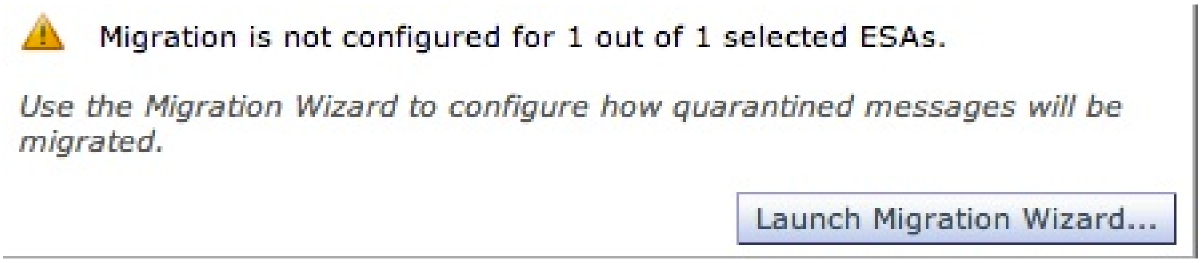
Service Migration Steps and Status

Migration Steps		Status
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. *To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.*
Step 2.	Configure migration of any messages currently quarantined on the ESAs	⚠ Migration is not configured for 1 out of 1 selected ESAs. *Click on the Commit Changes to proceed with 'Launch Migration Wizard' for recently added appliances.* Launch Migration Wizard...
Step 3.	Log into each ESA to start migration and begin using centralized quarantines.	⚠ Service is not active on 1 out of 1 selected ESAs. *Log into each ESA as required to enable the service (see status below).*

Email Appliance Status

Selected Email Appliances (ESAs)	Status
ESA	⚠ Action Required: Use Migration Wizard to define migration mapping.

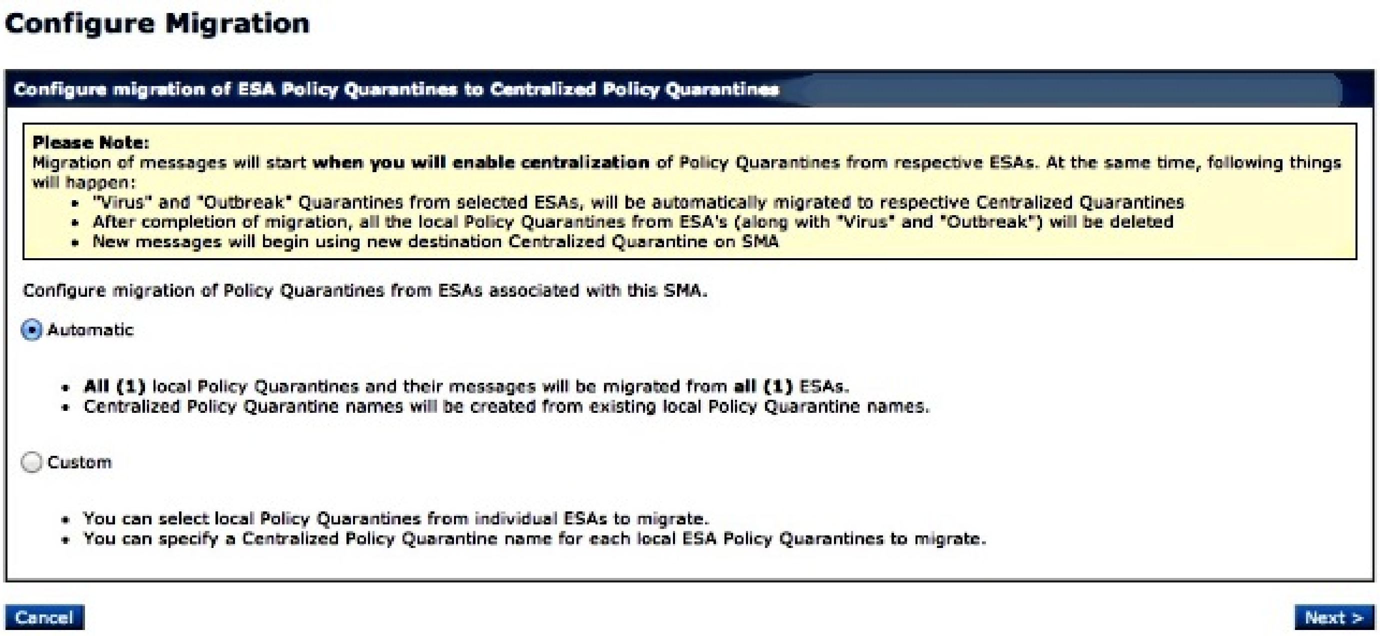
¿Los cambios del cometer se completan una vez, el Asisitente de la migración del lanzamiento? del paso 2 llegarán a ser activos:



⚠ Migration is not configured for 1 out of 1 selected ESAs.

Use the Migration Wizard to configure how quarantined messages will be migrated.

Seleccione al **Asisitente de la migración del lanzamiento** y continúe como sigue:



Configure Migration

Configure migration of ESA Policy Quarantines to Centralized Policy Quarantines

Please Note:
Migration of messages will start **when you will enable centralization** of Policy Quarantines from respective ESAs. At the same time, following things will happen:
- "Virus" and "Outbreak" Quarantines from selected ESAs, will be automatically migrated to respective Centralized Quarantines
- After completion of migration, all the local Policy Quarantines from ESA's (along with "Virus" and "Outbreak") will be deleted
- New messages will begin using new destination Centralized Quarantine on SMA

Configure migration of Policy Quarantines from ESAs associated with this SMA.

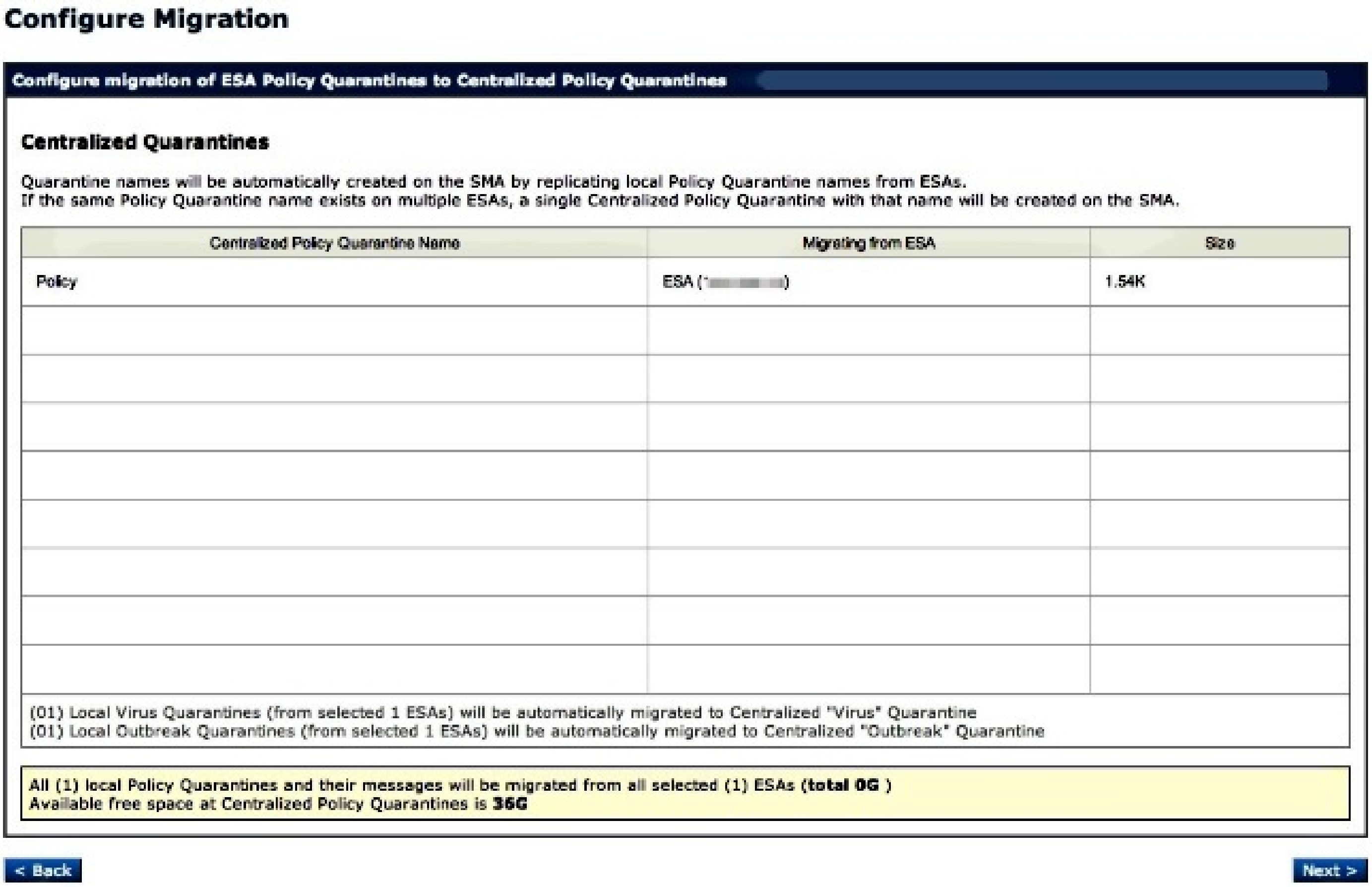
● Automatic

- **All (1)** local Policy Quarantines and their messages will be migrated from **all (1)** ESAs.
- Centralized Policy Quarantine names will be created from existing local Policy Quarantine names.

○ Custom

- You can select local Policy Quarantines from individual ESAs to migrate.
- You can specify a Centralized Policy Quarantine name for each local ESA Policy Quarantines to migrate.

Si solamente se va una cuarentena determinada a ser emigrada, elija la **aduana**. En este ejemplo, continuaremos con **automático**, que emigrará las cuarentenas de la directiva ANY/ALL del ESA al S A. Observe por favor que usted verá el nombre especificado elegido durante el ESA para agregar mencionado anterior, seguido por la dirección IP usada en la comunicación:



Configure Migration

Configure migration of ESA Policy Quarantines to Centralized Policy Quarantines

Centralized Quarantines

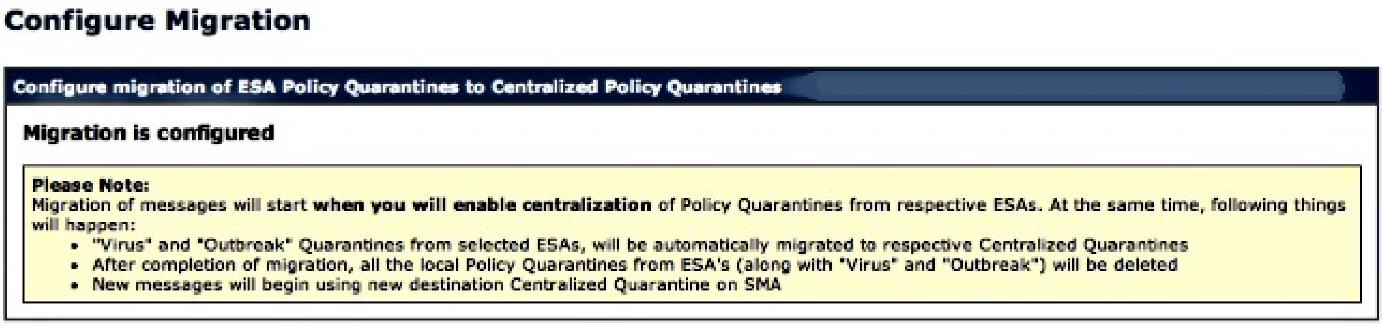
Quarantine names will be automatically created on the SMA by replicating local Policy Quarantine names from ESAs.
If the same Policy Quarantine name exists on multiple ESAs, a single Centralized Policy Quarantine with that name will be created on the SMA.

Centralized Policy Quarantine Name	Migrating from ESA	Size
Policy	ESA ([redacted])	1.54K

(01) Local Virus Quarantines (from selected 1 ESAs) will be automatically migrated to Centralized "Virus" Quarantine
(01) Local Outbreak Quarantines (from selected 1 ESAs) will be automatically migrated to Centralized "Outbreak" Quarantine

All (1) local Policy Quarantines and their messages will be migrated from all selected (1) ESAs (**total 0G**)
Available free space at Centralized Policy Quarantines is **36G**

Haga clic **después**, y continúe:



Configure Migration

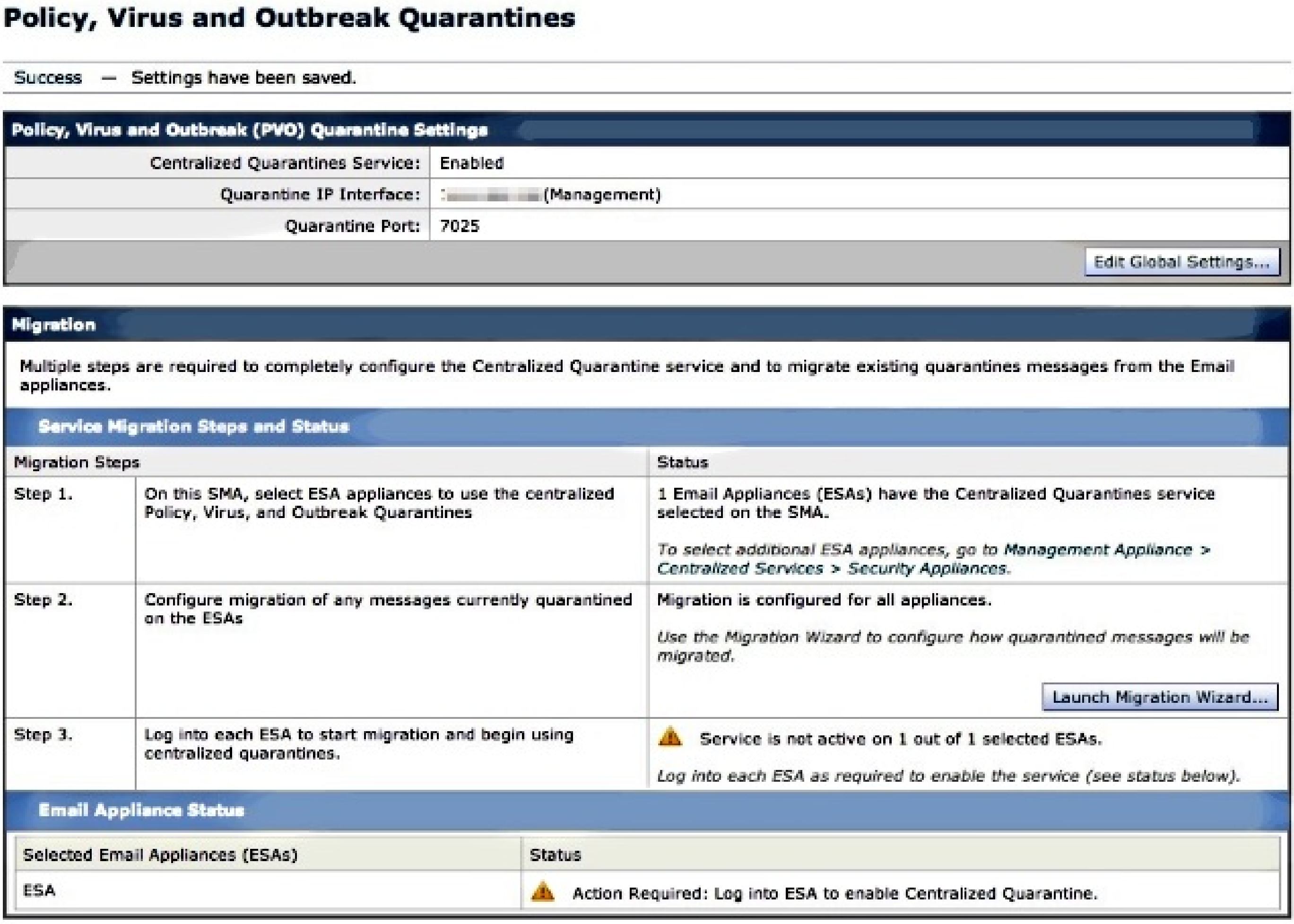
Configure migration of ESA Policy Quarantines to Centralized Policy Quarantines

Migration is configured

Please Note:
Migration of messages will start **when you will enable centralization** of Policy Quarantines from respective ESAs. At the same time, following things will happen:

- "Virus" and "Outbreak" Quarantines from selected ESAs, will be automatically migrated to respective Centralized Quarantines
- After completion of migration, all the local Policy Quarantines from ESA's (along with "Virus" and "Outbreak") will be deleted
- New messages will begin using new destination Centralized Quarantine on SMA

Finalmente, el tecleo **somete**, y se presenta la notificación del "éxito":



Policy, Virus and Outbreak Quarantines

Success — Settings have been saved.

Policy, Virus and Outbreak (PVO) Quarantine Settings

Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	[redacted] (Management)
Quarantine Port:	7025

Migration

Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.

Service Migration Steps and Status

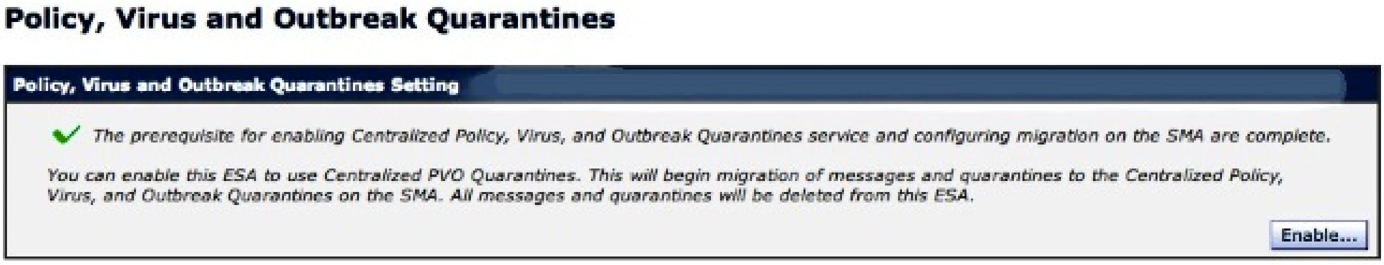
Migration Steps		Status
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. *To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.*
Step 2.	Configure migration of any messages currently quarantined on the ESAs	Migration is configured for all appliances. *Use the Migration Wizard to configure how quarantined messages will be migrated.* Launch Migration Wizard...
Step 3.	Log into each ESA to start migration and begin using centralized quarantines.	⚠ Service is not active on 1 out of 1 selected ESAs. *Log into each ESA as required to enable the service (see status below).*

Email Appliance Status

Selected Email Appliances (ESAs)	Status
ESA	⚠ Action Required: Log into ESA to enable Centralized Quarantine.

Confíe sus cambios en el S A.

Volviendo al ESA, navegue a los **Servicios de seguridad > a las cuarentenas de la directiva, del virus y del brote**. Los pasos necesarios de antemano en el S A ahora se reconocen:



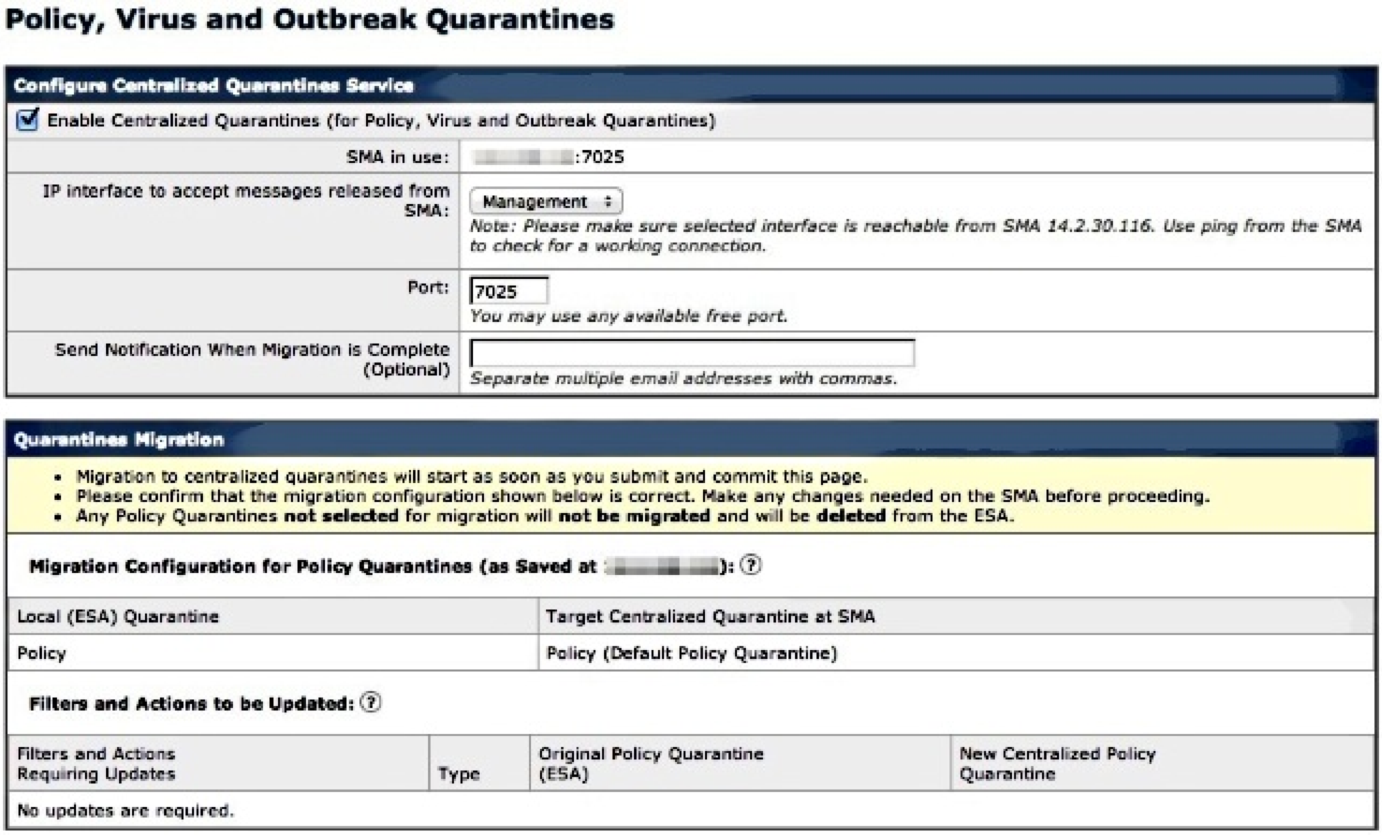
Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines Setting

✓ *The prerequisite for enabling Centralized Policy, Virus, and Outbreak Quarantines service and configuring migration on the SMA are complete.*

You can enable this ESA to use Centralized PVO Quarantines. This will begin migration of messages and quarantines to the Centralized Policy, Virus, and Outbreak Quarantines on the SMA. All messages and quarantines will be deleted from this ESA.

¿Permiso del tecleo? , y continúe:



Policy, Virus and Outbreak Quarantines

Configure Centralized Quarantines Service

☑ Enable Centralized Quarantines (for Policy, Virus and Outbreak Quarantines)

SMA in use:	[redacted]:7025
IP interface to accept messages released from SMA:	Management ÷ *Note: Please make sure selected interface is reachable from SMA 14.2.30.116. Use ping from the SMA to check for a working connection.*
Port:	7025 *You may use any available free port.*
Send Notification When Migration is Complete (Optional)	 *Separate multiple email addresses with commas.*

Quarantines Migration

- Migration to centralized quarantines will start as soon as you submit and commit this page.
- Please confirm that the migration configuration shown below is correct. Make any changes needed on the SMA before proceeding.
- Any Policy Quarantines **not selected** for migration will **not be migrated** and will be **deleted** from the ESA.

Migration Configuration for Policy Quarantines (as Saved at [redacted]): ?

Local (ESA) Quarantine	Target Centralized Quarantine at SMA
Policy	Policy (Default Policy Quarantine)

Filters and Actions to be Updated: ?

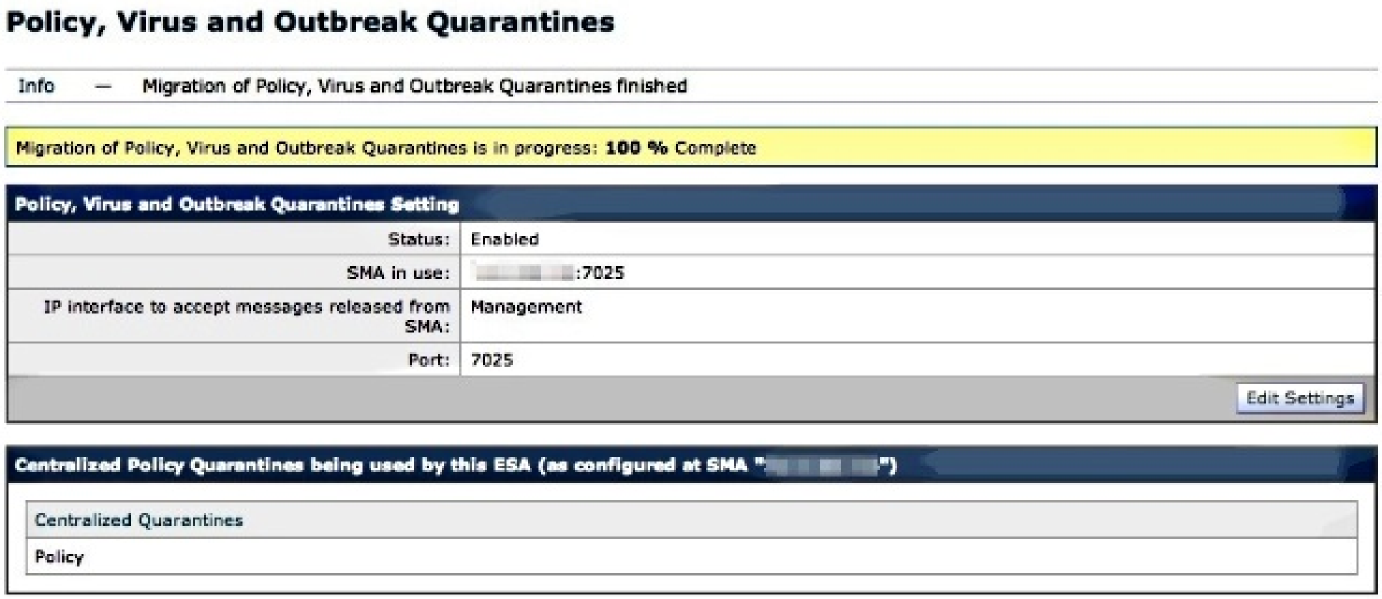
Filters and Actions Requiring Updates	Type	Original Policy Quarantine (ESA)	New Centralized Policy Quarantine
No updates are required.			

El aviso, eso aquí el puerto apropiado usado para la comunicación se observa otra vez. Éstos **deben** hacer juego, y si el Firewall/la red ACL es funcionando, se deben abrir para permitir la migración apropiada entre el ESA y el S A.

> **Note**: Si usted tiene la directiva, el virus, y cuarentenas del brote configuradas en un ESA, la migración de las cuarentenas y de todos sus mensajes comienza tan pronto como usted confíe este cambio.

> **Note**: Solamente un proceso de migración puede estar en curso en cualquier momento. No habilite la directiva centralizada, el virus, y las cuarentenas del brote en otras dispositivo de seguridad del correo electrónico hasta que la migración anterior sea completa.

El tecleo **somete**, y finalmente hace clic el **cometer**. La notificación de información debe ser similar. Si hay un gran número de mensajes ya en la cuarentena local, éstos pueden tomar tiempo para procesar del ESA al S A:



Policy, Virus and Outbreak Quarantines

Info — Migration of Policy, Virus and Outbreak Quarantines finished

Migration of Policy, Virus and Outbreak Quarantines is in progress: **100 %** Complete

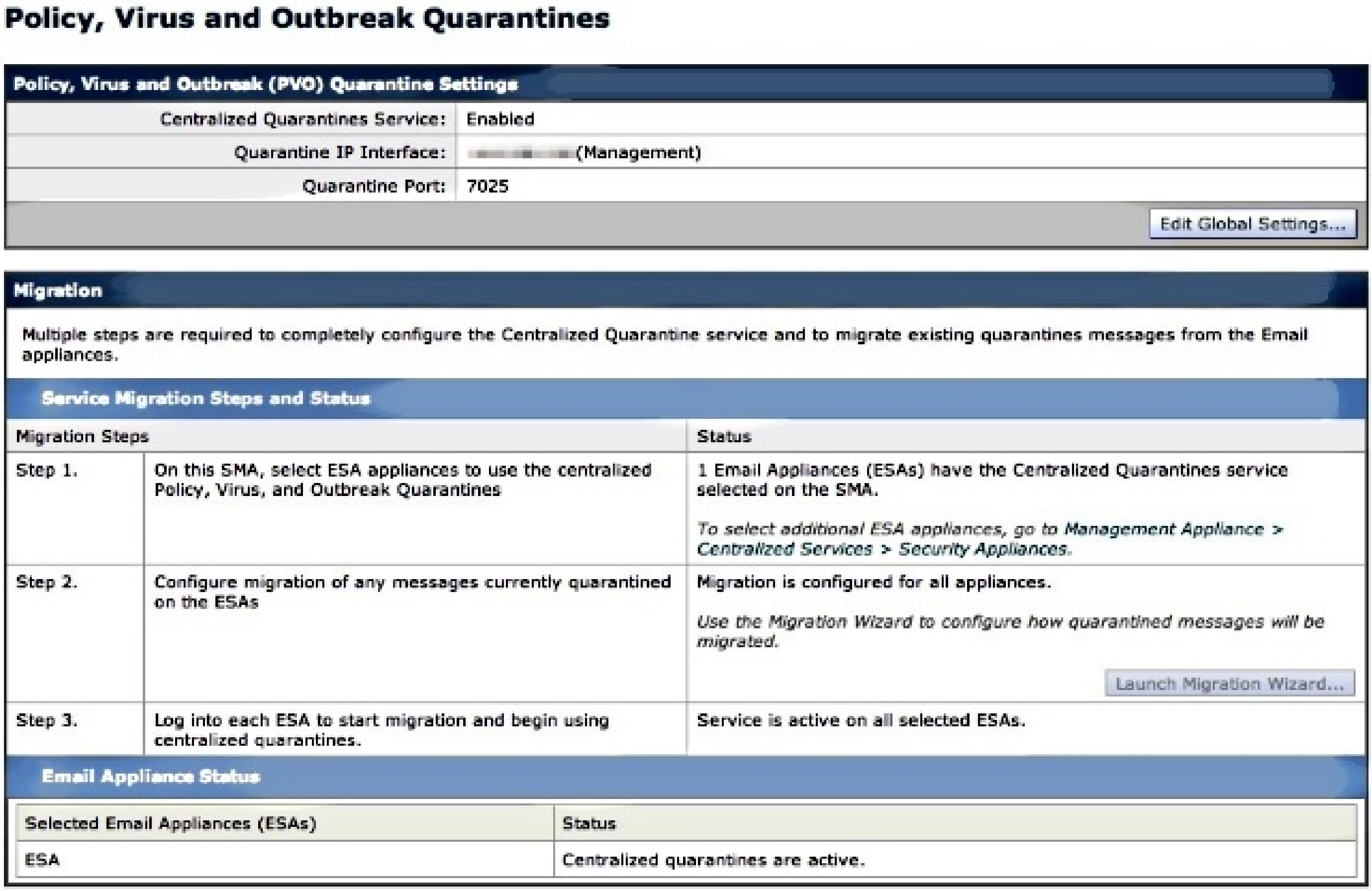
Policy, Virus and Outbreak Quarantines Setting

Status:	Enabled
SMA in use:	[redacted]:7025
IP interface to accept messages released from SMA:	Management
Port:	7025

Centralized Policy Quarantines being used by this ESA (as configured at SMA "[redacted]")

Centralized Quarantines
Policy

Revisite el S A, y navegue al **dispositivo de la Administración > los servicios > las cuarentenas centralizados de la directiva, del virus y del brote**. Los pasos de la migración ahora serán completados:



Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak (PVO) Quarantine Settings

Centralized Quarantines Service:	Enabled
Quarantine IP Interface:	[redacted](Management)
Quarantine Port:	7025

Migration

Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.

Service Migration Steps and Status

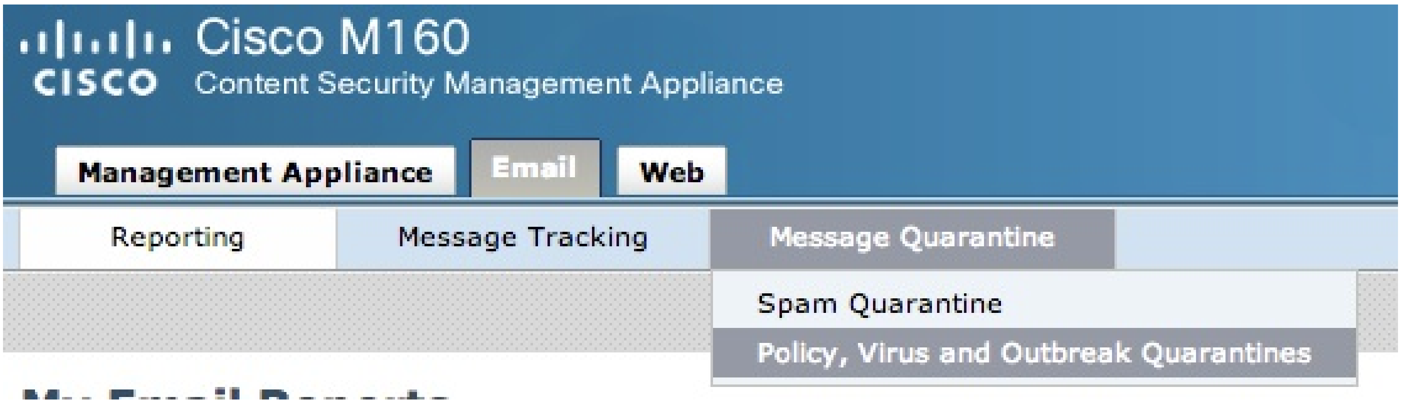
Migration Steps		Status
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. *To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.*
Step 2.	Configure migration of any messages currently quarantined on the ESAs	Migration is configured for all appliances. *Use the Migration Wizard to configure how quarantined messages will be migrated.* Launch Migration Wizard...
Step 3.	Log into each ESA to start migration and begin using centralized quarantines.	Service is active on all selected ESAs.

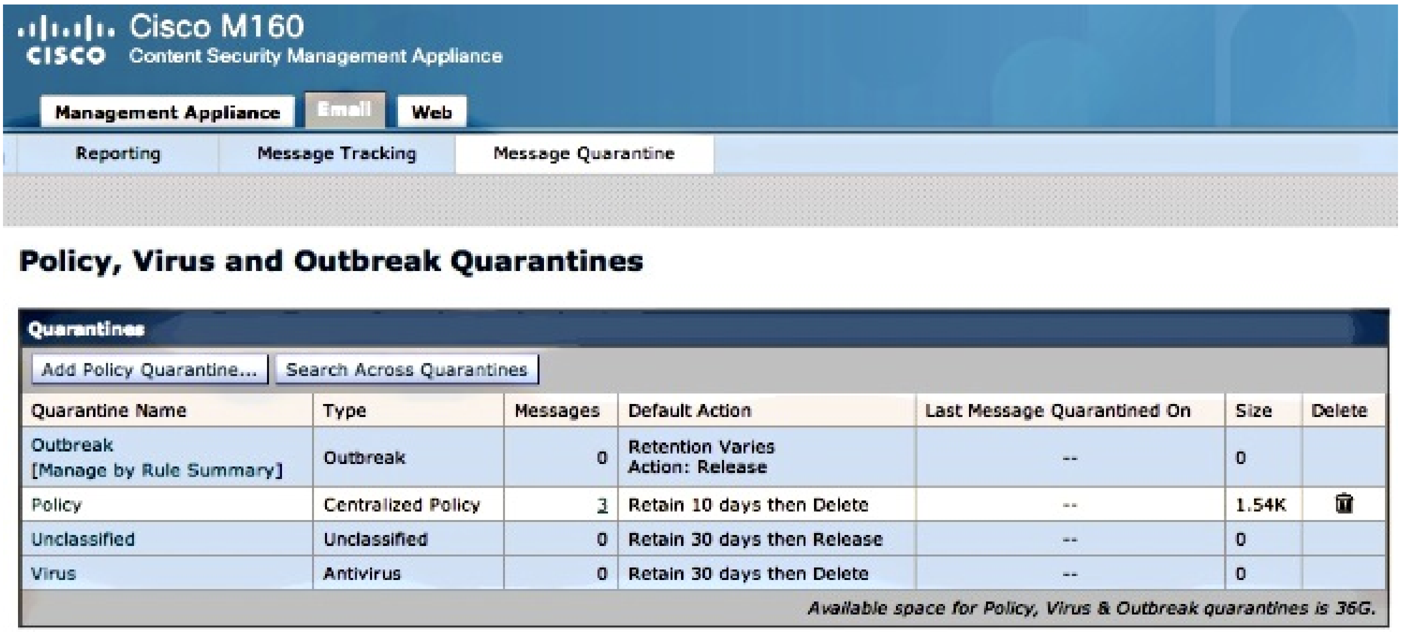
Email Appliance Status

Selected Email Appliances (ESAs)	Status
ESA	Centralized quarantines are active.

Verificación

Ahora, la migración de la cuarentena de la directiva del ESA al S A es completa. Para la verificación final, marque la cuarentena de la directiva en el S A:





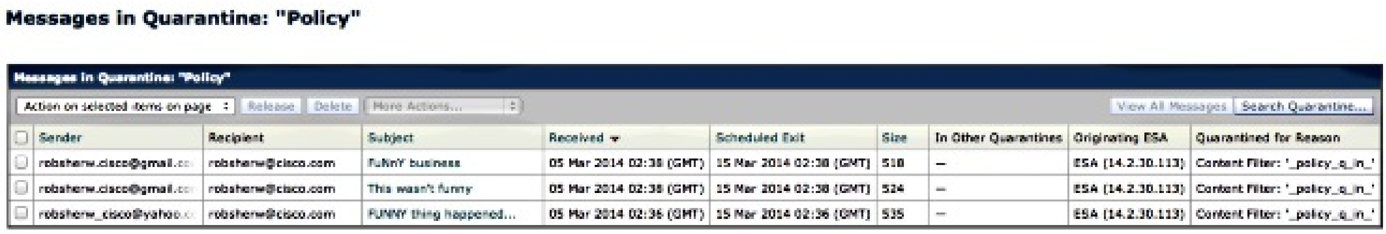
Policy, Virus and Outbreak Quarantines

Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	3	Retain 10 days then Delete	--	1.54K	🗑
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 36G.

Usted debe ver los mismos mensajes que fueron enumerados originalmente en el ESA. Seleccione # enlace hipertexto en la columna de los mensajes, y verifiquelo:


Messages in Quarantine: "Policy"

Messages in Quarantine: "Policy"

□	Sender	Recipient	Subject	Received ▾	Scheduled Exit	Size	In Other Quarantines	Originating ESA	Quarantined for Reason
□	robsherw.cisco@gmail.c	robsherw@cisco.com	FuNnY business	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	518	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
□	robsherw.cisco@gmail.c	robsherw@cisco.com	This wasn't funny	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	524	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
□	robsherw_cisco@yahoo.c	robsherw@cisco.com	FUNNY thing happened...	05 Mar 2014 02:36 (GMT)	15 Mar 2014 02:36 (GMT)	535	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'

Si usted mira los mail_logs en el ESA, la migración de los mensajes actuales será presentada:

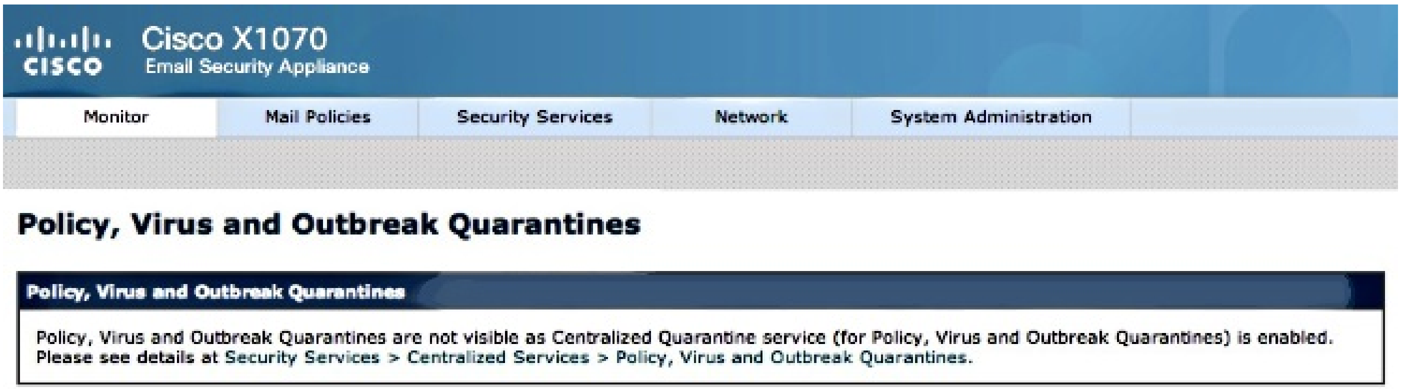
> **Note**: Observe el uso de la comunicación entre el ESA (XX.X.XX.XX X) y S A (YY.Y.YY.YY Y) vía el puerto 7025.

```
Wed Mar  5 02:48:40 2014 Info: New SMTP DCID 2 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:48:40 2014 Info: DCID 2 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:49:52 2014 Info: New SMTP DCID 3 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:49:52 2014 Info: DCID 3 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:22 2014 Info: New SMTP DCID 4 interface XX.X.XX.XXX address
```

```
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:22 2014 Info: DCID 4 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:23 2014 Info: New SMTP DCID 5 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:23 2014 Info: DCID 5 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:40 2014 Info: New SMTP DCID 6 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:40 2014 Info: DCID 6 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:41 2014 Info: New SMTP DCID 7 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:41 2014 Info: DCID 7 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:42 2014 Info: New SMTP DCID 8 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:42 2014 Info: DCID 8 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 9 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 9 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: CPQ listener cpq_listener starting
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 10 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 10 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 11 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 11 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: MID 1 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 1 queued for delivery
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 12 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 12 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 1 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: MID 2 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 2 queued for delivery
Wed Mar  5 02:51:02 2014 Info: MID 3 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 3 queued for delivery
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 1 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 1 RID [0] Response 'ok:  Message 1 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 1 done
Wed Mar  5 02:51:02 2014 Info: MID 1 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 2 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 13 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 13 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 14 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 14 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 2 to RID [0] (centralized
policy quarantine)
```

```
Wed Mar  5 02:51:02 2014 Info: MID 2 RID [0] Response 'ok:  Message 2 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 2 done
Wed Mar  5 02:51:02 2014 Info: MID 2 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 3 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 3 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 3 RID [0] Response 'ok:  Message 3 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 3 done
Wed Mar  5 02:51:02 2014 Info: MID 3 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 15 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 15 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:07 2014 Info: DCID 12 close
```

Revisite el ESA, y lo que sigue ahora se presenta al ver la directiva, el virus, brote Quarantines:



Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines

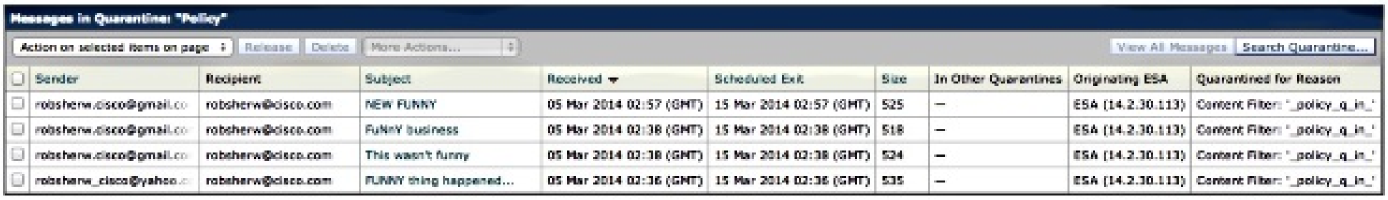
Policy, Virus and Outbreak Quarantines are not visible as Centralized Quarantine service (for Policy, Virus and Outbreak Quarantines) is enabled. Please see details at Security Services > Centralized Services > Policy, Virus and Outbreak Quarantines.

El siguiente paso de la verificación está enviando un nuevo mensaje de prueba con el ESA que será cogido para la cuarentena de la directiva. Mirando los mail_logs en el ESA, note la línea resaltada el indicar de la transferencia del ESA al S A vía 7025, indicando la cuarentena de la directiva:

```
Wed Mar  5 02:57:47 2014 Info: Start MID 4 ICID 6
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 From: <robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 RID 0 To: <robsherw@cisco.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 Message-ID
'<7642E61C-4BA2-432E-A524-E163EA0B9753@gmail.com>'
Wed Mar  5 02:57:47 2014 Info: MID 4 Subject 'NEW FUNNY'
Wed Mar  5 02:57:47 2014 Info: MID 4 ready 525 bytes from
<robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Mar  5 02:57:47 2014 Info: MID 4 enqueued for transfer to centralized
quarantine "Policy" (content filter _policy_q_in_)
Wed Mar  5 02:57:47 2014 Info: MID 4 queued for delivery
Wed Mar  5 02:57:47 2014 Info: New SMTP DCID 16 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:57:47 2014 Info: DCID 16 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:57:47 2014 Info: Delivery start DCID 16 MID 4 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:57:47 2014 Info: Message done DCID 16 MID 4 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:57:47 2014 Info: MID 4 RID [0] Response 'ok:  Message 4 accepted'
Wed Mar  5 02:57:47 2014 Info: Message finished MID 4 done
Wed Mar  5 02:57:52 2014 Info: DCID 16 close
```

Revisite la cuarentena previamente mencionada de la directiva en el S A, el nuevo mensaje de prueba ahora está en la cuarentena también:

Messages in Quarantine: "Policy"



Messages in Quarantine: "Policy"

□	Sender	Recipient	Subject	Received ▼	Scheduled Exit	Size	In Other Quarantines	Originating ESA	Quarantined for Reason
□	robsherw.cisco@gmail.co	robsherw@cisco.com	NEW FUNNY	05 Mar 2014 02:57 (GMT)	15 Mar 2014 02:57 (GMT)	525	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
□	robsherw.cisco@gmail.co	robsherw@cisco.com	FuNnY business	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	518	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
□	robsherw.cisco@gmail.co	robsherw@cisco.com	This wasn't funny	05 Mar 2014 02:38 (GMT)	15 Mar 2014 02:38 (GMT)	524	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'
□	robsherw_cisco@yahoo.c	robsherw@cisco.com	FUNNY thing happened...	05 Mar 2014 02:36 (GMT)	15 Mar 2014 02:36 (GMT)	535	—	ESA (14.2.30.113)	Content Filter: '_policy_q_in_'

Información Relacionada

- La directiva de centralización ESA, el virus, y la cuarentena del brote (PVO) no pueden ser habilitados
- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems