Procedure ottimali per la configurazione e la migrazione di quarantene centralizzate per virus ed epidemie da ESA a SMA

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Configurazione](#)
[Verifica](#)
[Informazioni correlate](#)

Introduzione

Le seguenti quarantene possono ora essere collettivamente centralizzate su una appliance Cisco Security Management Appliance (SMA):

- Antivirus
- Epidemia
- Quarantene criteri utilizzate per i messaggi intercettati da:
  Filtri messaggiFiltri dei contenutiPolitiche di prevenzione della perdita dei dati

La centralizzazione di queste quarantene offre i seguenti vantaggi:

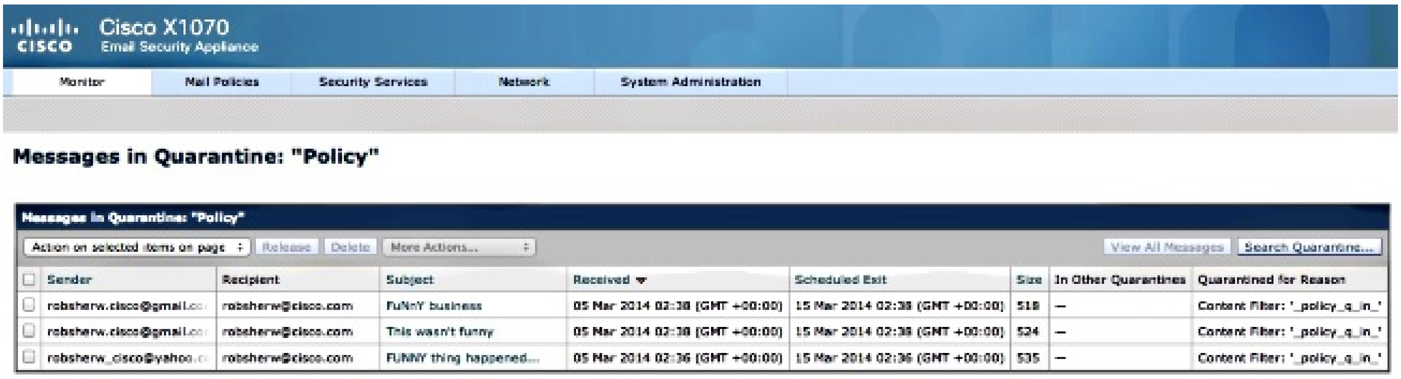
- Gli amministratori possono gestire i messaggi in quarantena da più appliance ESA (Email Security Appliance) in un'unica posizione.
- I messaggi in quarantena vengono archiviati dietro il firewall anziché nella DMZ, riducendo i rischi per la sicurezza.
- Èpossibile eseguire il backup delle quarantene centralizzate come parte della funzionalità di backup standard dell'SMA.

Prerequisiti

- SMA in esecuzione 8.1 (Guida per l'utente SMA, [Capitolo 8, Criteri centralizzati, Virus e quarantene di epidemie](#))
- ESA in esecuzione 8.0.1 (Guida dell'utente ESA, [Capitolo 27, Quarantene](#))
- Firewall - porta 7025 / TCP (entrata e uscita) / uso nome host: IP AsyncOS / Descrizione: trasferimento dei dati di quarantena relativi a criteri, virus ed epidemie tra Email Security Appliance e Security Management Appliance quando questa funzionalità è centralizzata

Configurazione

A partire dall'ESA, in una quarantena delle politiche esistente, sono presenti messaggi attivi nella quarantena delle politiche:



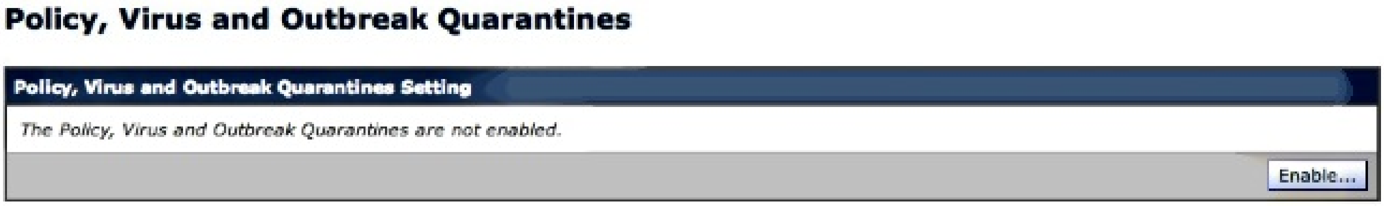
Messages in Quarantine: "Policy"

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_'

Per eseguire la migrazione di questi messaggi e quindi fare affidamento sull'SMA come appliance attiva proprietaria della quarantena delle policy, attenersi alle istruzioni riportate di seguito.

Nell'SMA, passare a **Management Appliance > Centralized Services > Policy, Virus and Outbreak Quarantines** (Appliance di gestione > Servizi centralizzati > Quarantene criteri, virus ed epidemie). Se non è già abilitato, fare clic su **Abilita:**

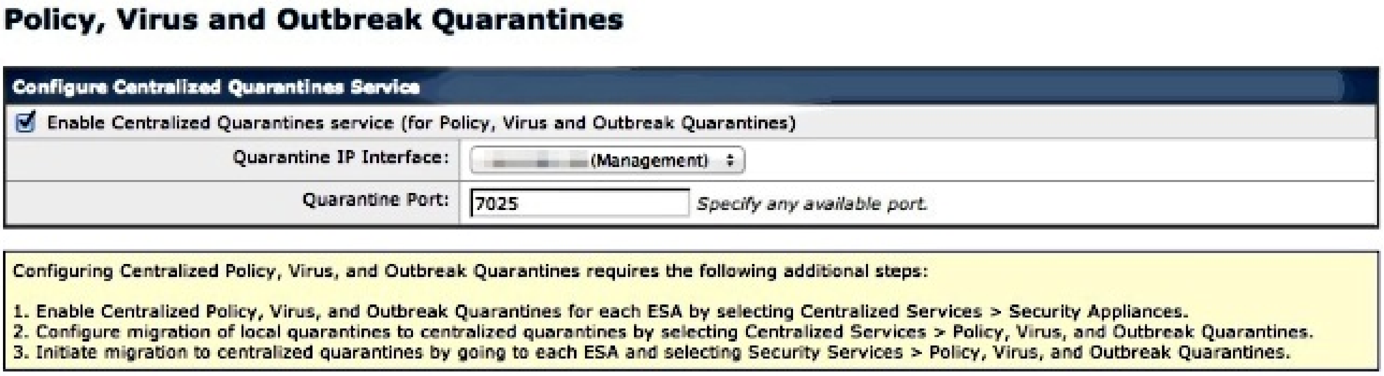

Policy, Virus and Outbreak Quarantines

Policy, Virus and Outbreak Quarantines Setting

The Policy, Virus and Outbreak Quarantines are not enabled.

Selezionare l'interfaccia, se applicabile, destinata a gestire il traffico dall'ESA allo SMA.

> **Nota:** La porta di quarantena può essere modificata, ma sarà necessario aprirla se è presente un firewall o un ACL di rete.


Policy, Virus and Outbreak Quarantines

Configure Centralized Quarantines Service

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

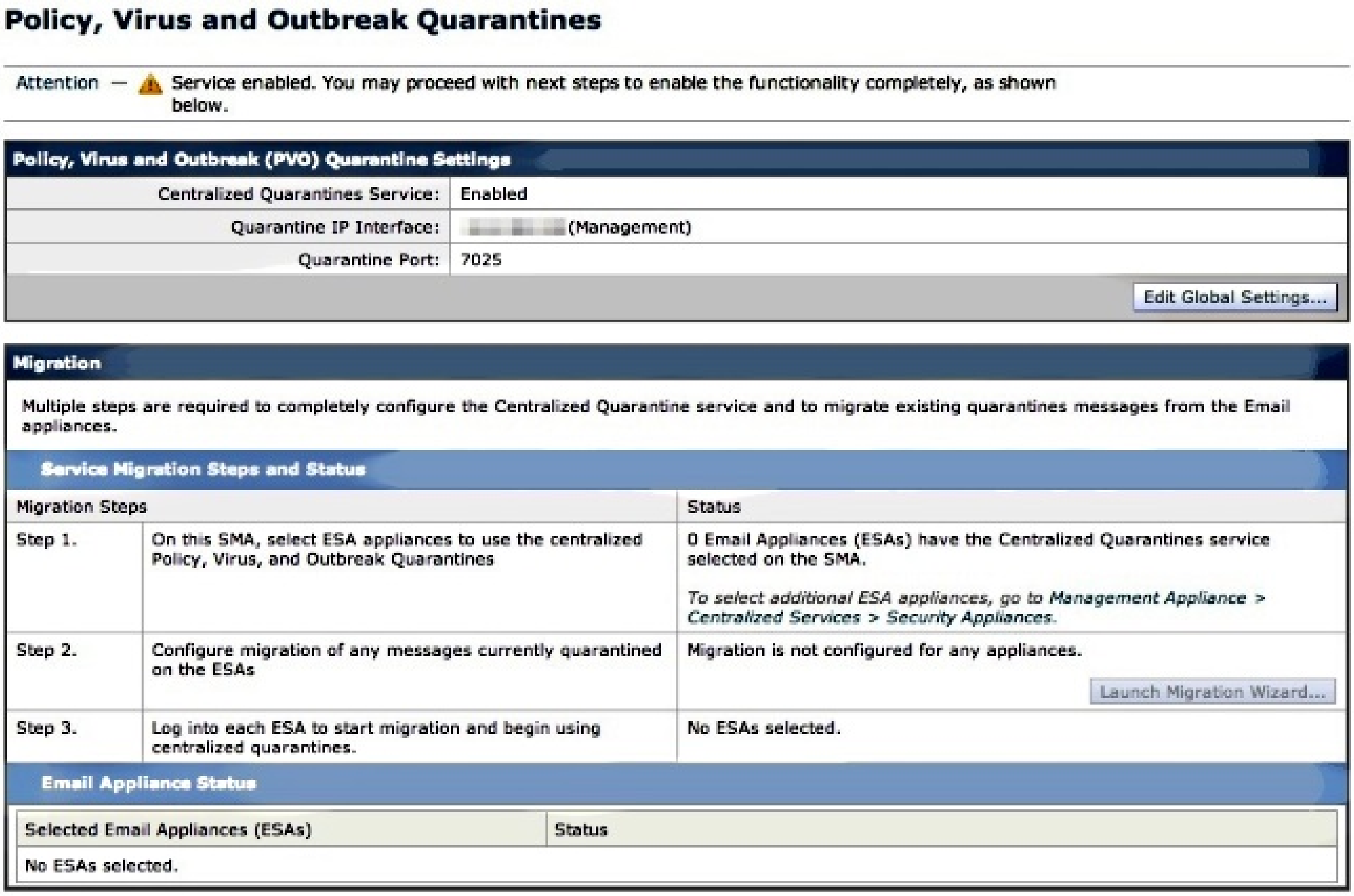
Quarantine IP Interface: [redacted] (Management)

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.

Fare clic su **Invia**. La schermata viene aggiornata per mostrare il Servizio abilitato messaggio, visto di seguito:



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

Migration

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

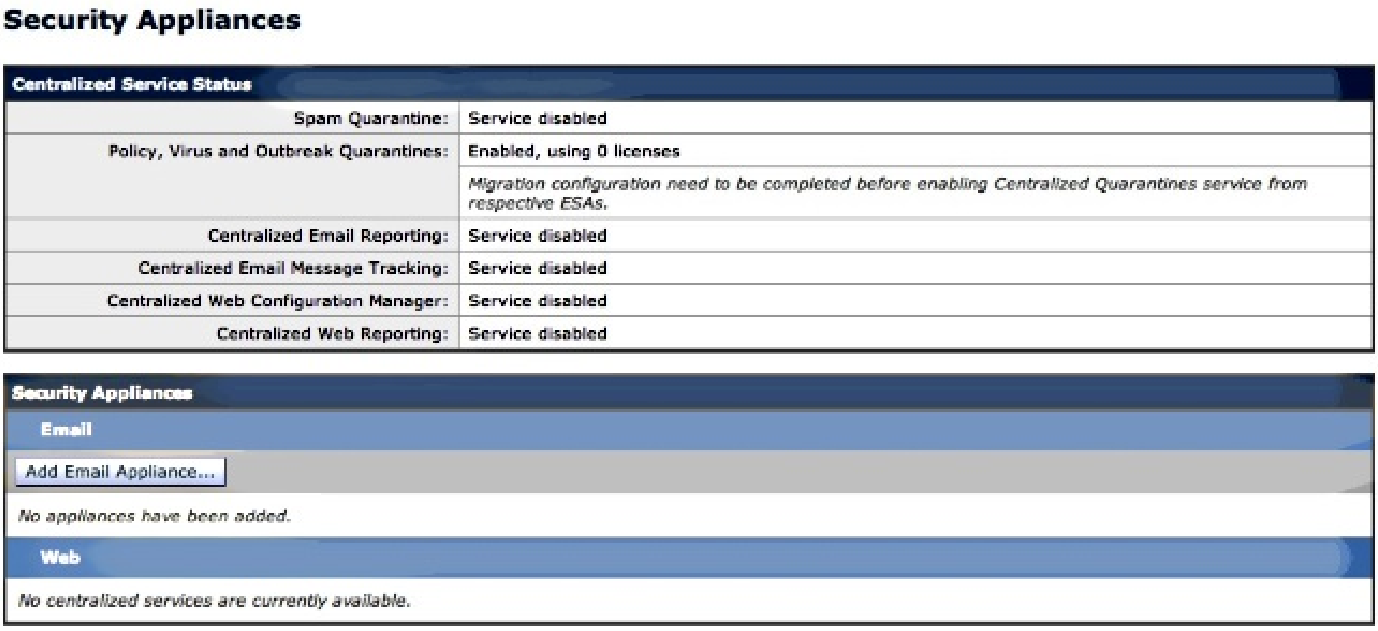
Service Migration Steps and Status

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.
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.	

Passare a **Management Appliance > Centralized Services > Security Appliance** e aggiungere la comunicazione ESA all'SMA:



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

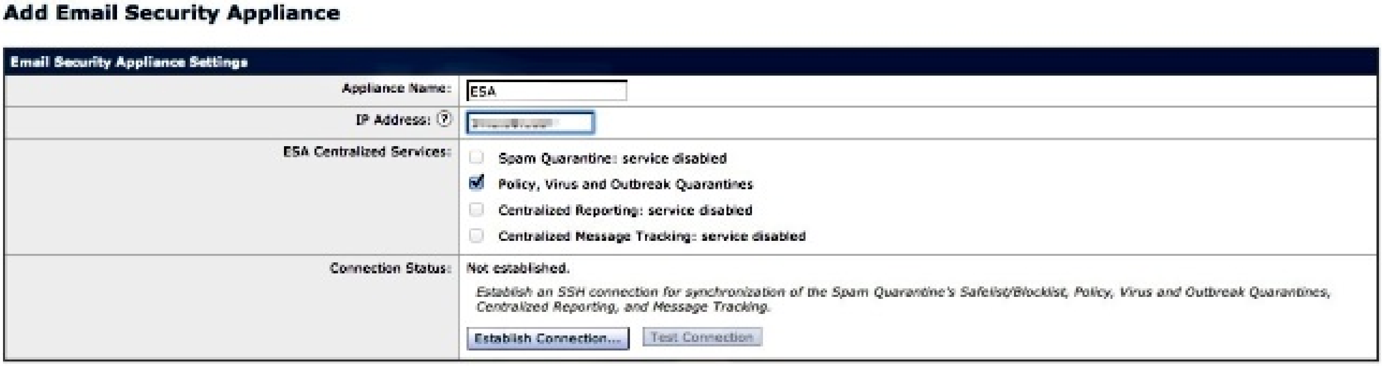
No appliances have been added.

Web

No centralized services are currently available.

Fare clic su **Add Email Appliance** (Aggiungi accessorio di posta elettronica).

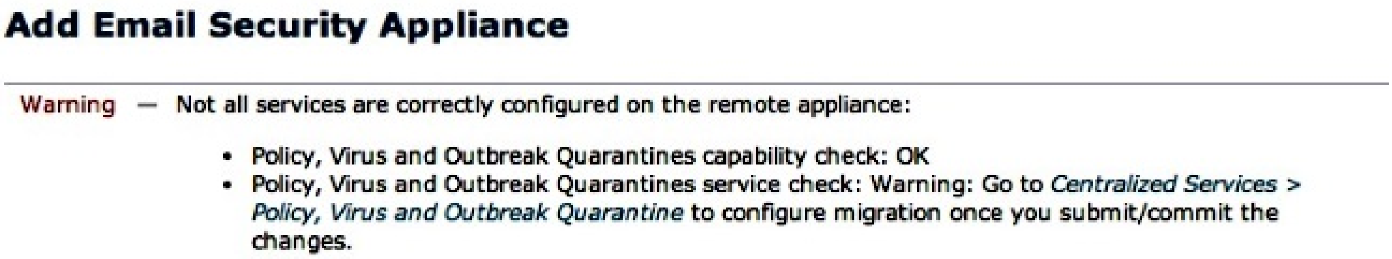
> **Nota:** È sufficiente aggiungere l'indirizzo IP che l'SMA utilizzerà per comunicare con l'ESA. Il nome dell'accessorio viene utilizzato solo come riferimento amministrativo.



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.* Establish Connection... Test Connection

Accertarsi di **stabilire** la **connessione** e di **verificarla**. Una volta stabilita la connessione tra l'SMA e l'ESA, vengono richiesti il nome utente e la password dell'amministratore. Si tratta dell'utente amministrativo e della password dell'ESA che viene aggiunta. I risultati del test possono variare in base all'elemento già attivo e all'elemento aggiunto, ma devono essere simili ai seguenti:



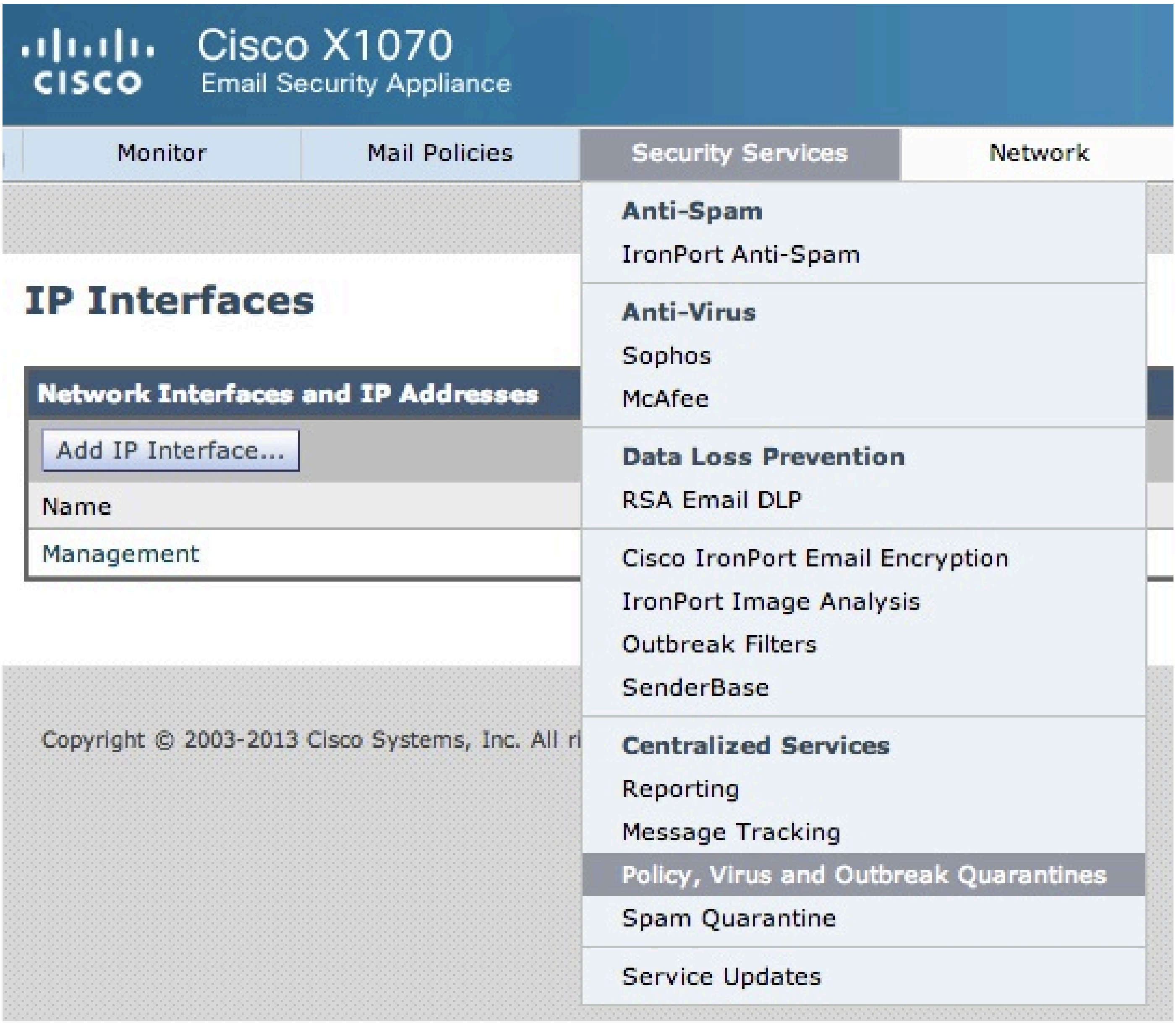
Add Email Security Appliance

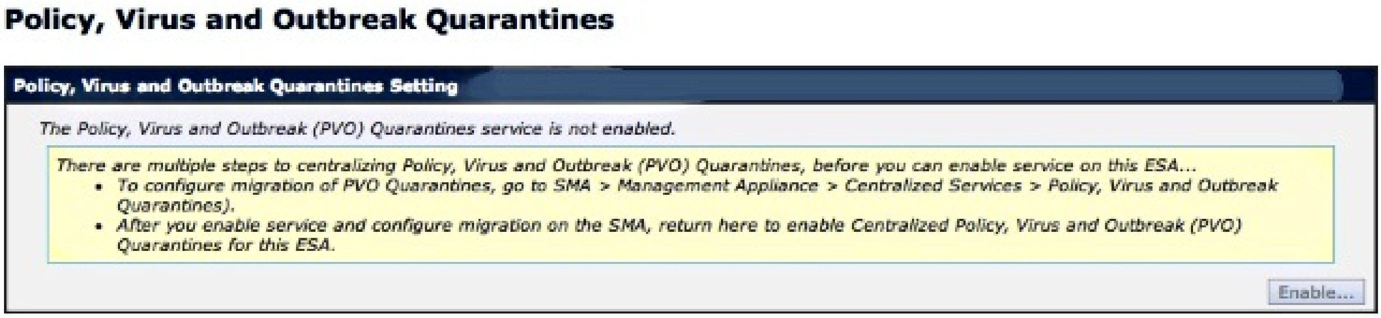
Warning — Not all services are correctly configured on the remote appliance:

- 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.

A questo punto, **inviare** e **confermare le modifiche** sullo SMA.

In questo momento, se si dovesse rivisitare l'ESA e tentare di configurare la sezione Servizi centralizzati della quarantena politica, sarebbe simile a quanto segue:



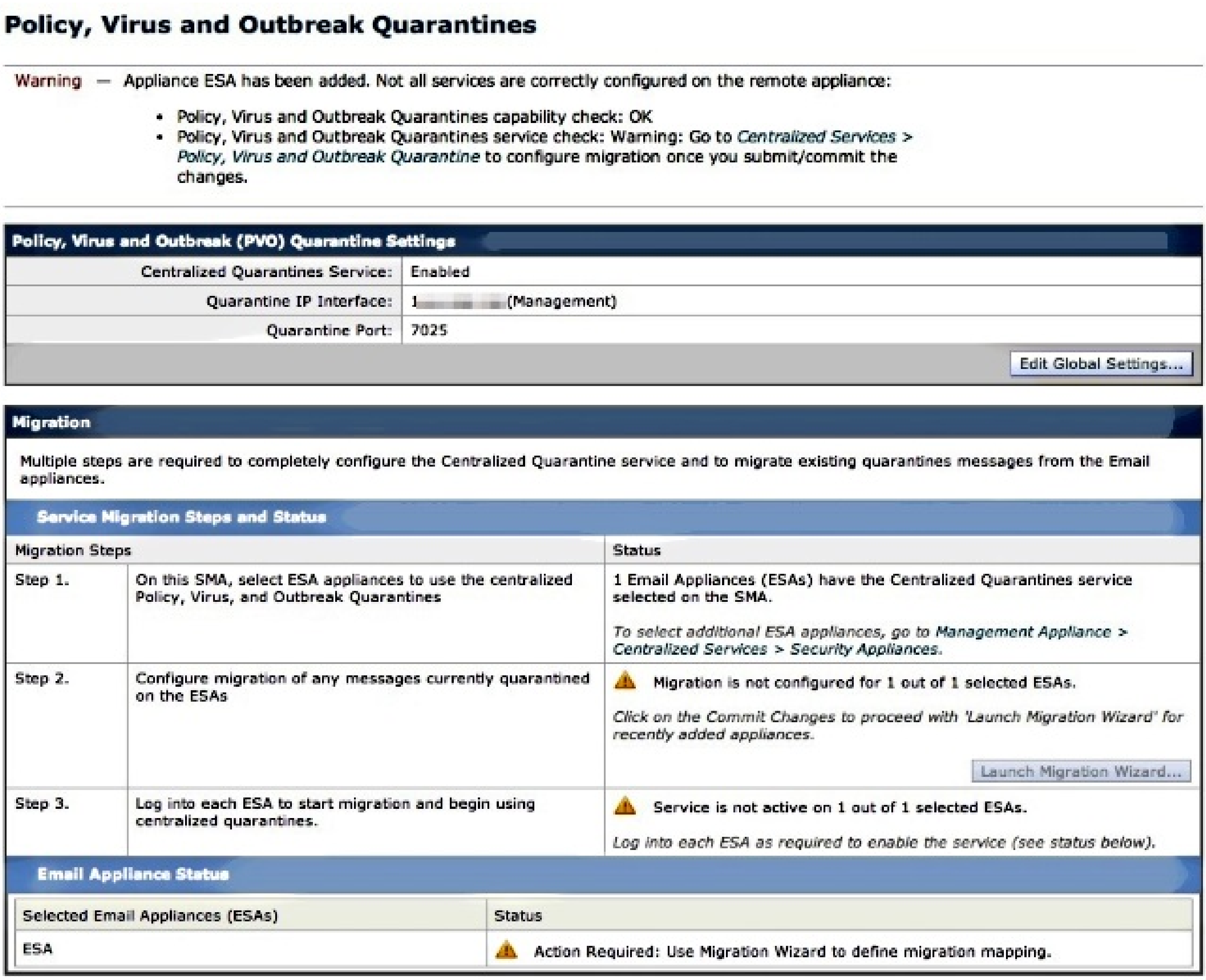

Policy, Virus and Outbreak Quarantines
Policy, Virus and Outbreak Quarantines Setting

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.*

Le fasi di migrazione devono essere ancora completate nell'SMA. Tornare all'SMA e continuare con la sezione seguente.



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.

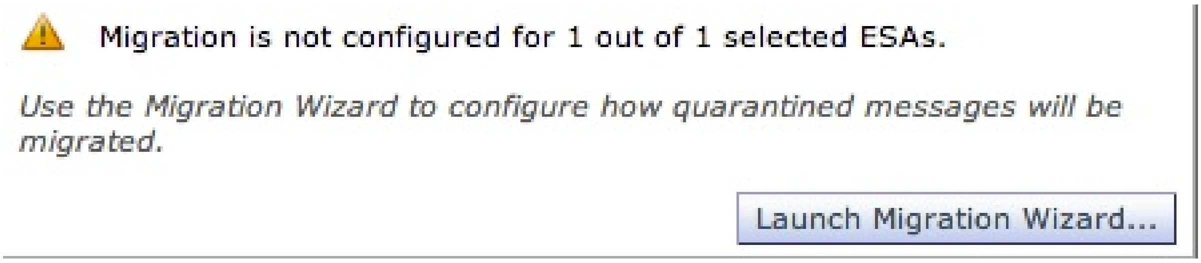
Service Migration Steps and Status

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.

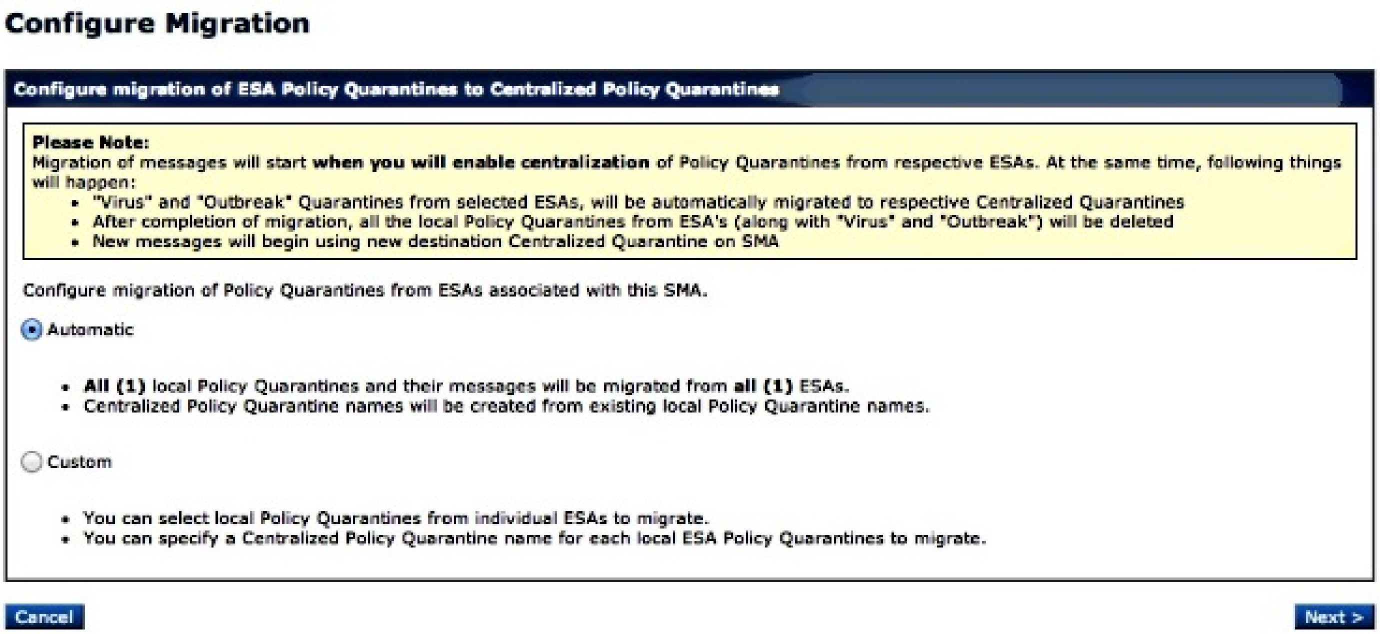
Avviare la Migrazione guidata al termine del commit delle modifiche? del passaggio 2 diventerà attivo:



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

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

Selezionare **Avvia migrazione guidata** e continuare come segue:



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.

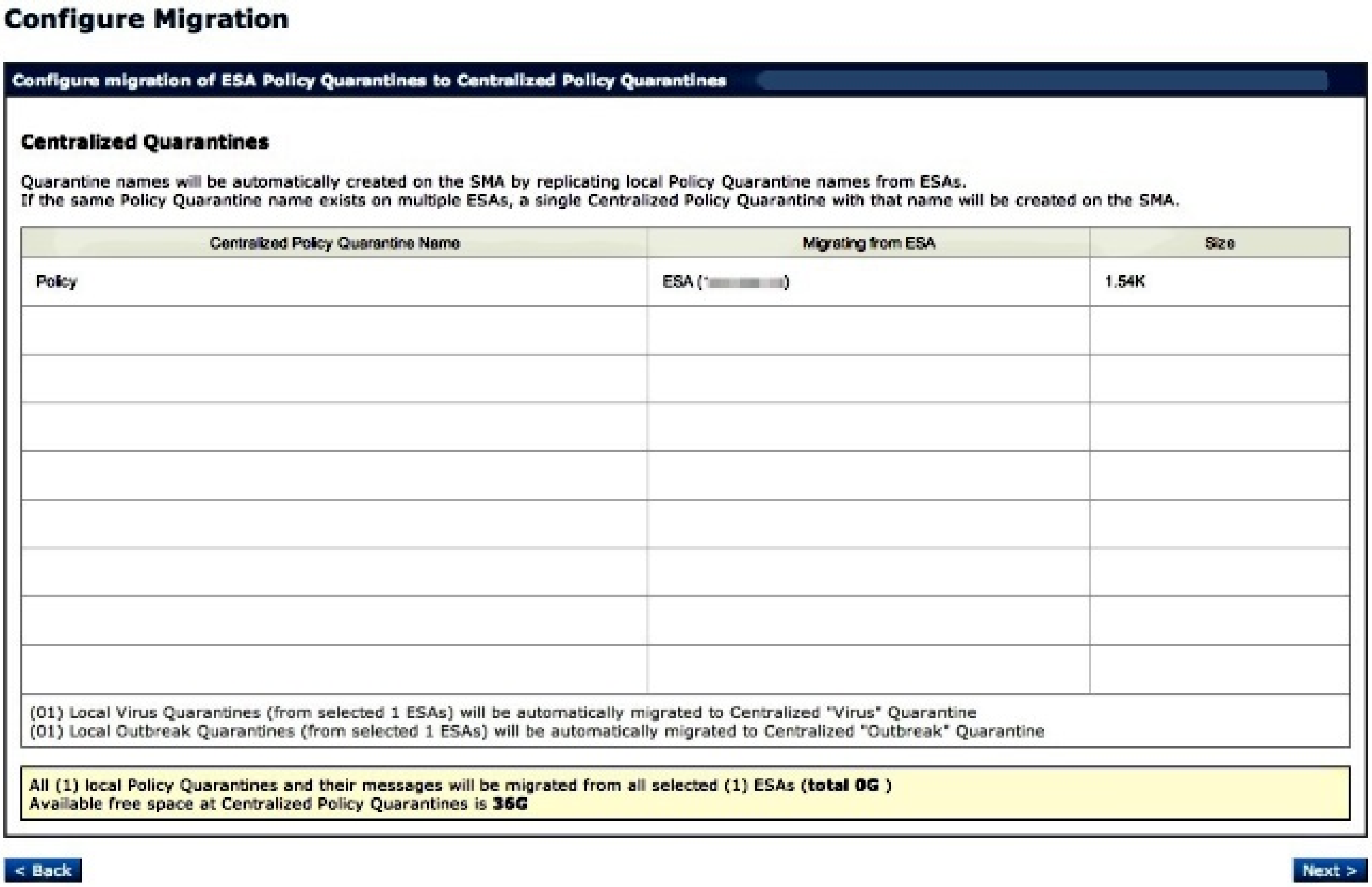
● Automatic

- **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.

Se è necessario migrare solo una particolare quarantena, scegliere **Personalizzata**. In questo esempio, proseguiremo con **Automatic**, che migrerà ANY/ALL Policy Quarantines dall'ESA all'SMA. Notare che vedrete il nome specificato scelto durante l'aggiunta dell'ESA menzionata in precedenza, seguito dall'indirizzo IP usato nella comunicazione:



Configure Migration

Configure migration of ESA Policy Quarantines to Centralized Policy Quarantines

Centralized Quarantines

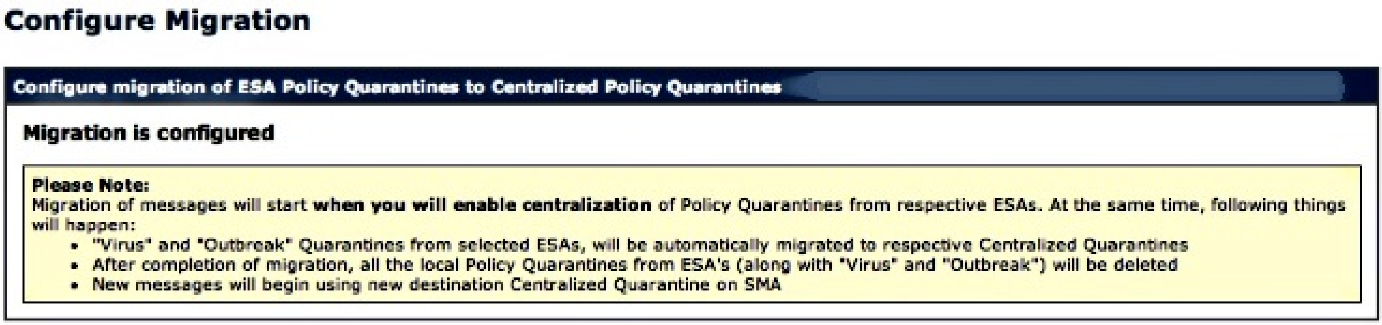
Quarantine names will be automatically created on the SMA by replicating local Policy Quarantine names from ESAs.
If the same Policy Quarantine name exists on multiple ESAs, a single Centralized Policy Quarantine with that name will be created on the SMA.

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**

Fare clic su **Avanti** e continuare:



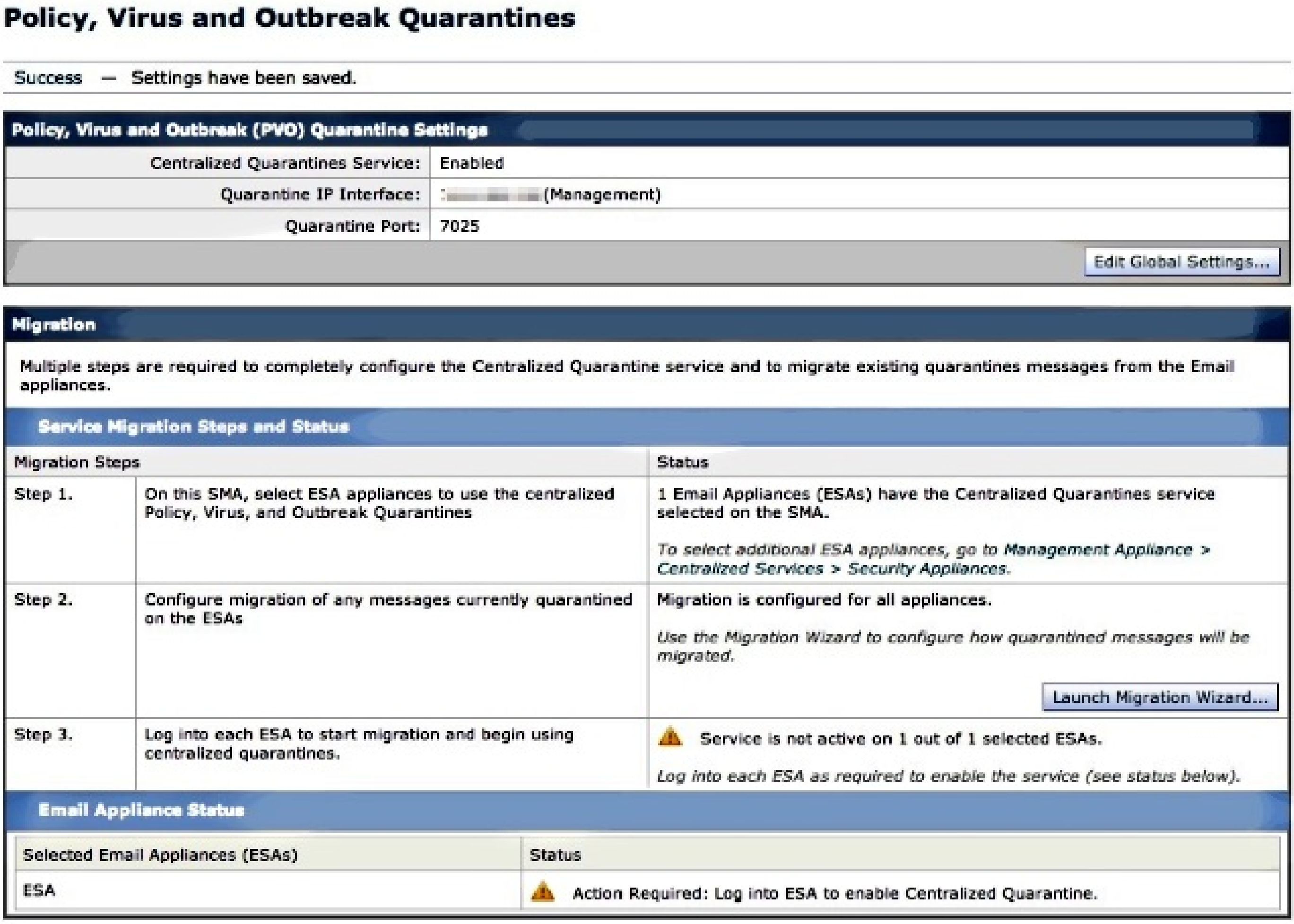
Configure Migration

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

Infine, fare clic su **Submit** (Invia) per visualizzare la notifica di esito positivo:



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

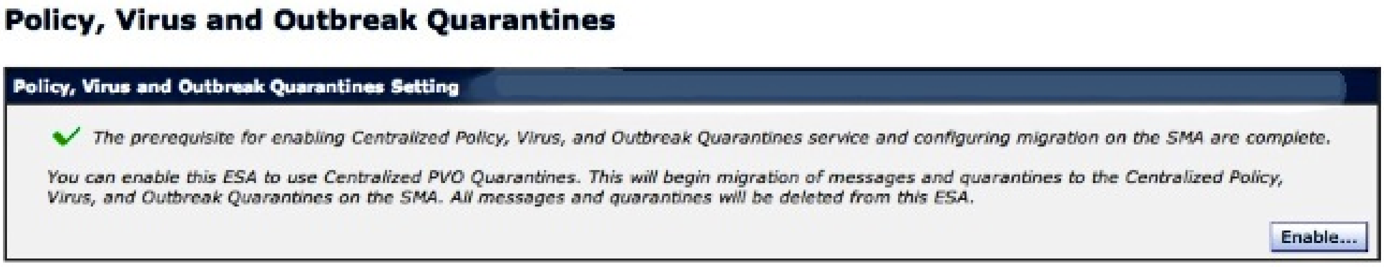
Migration Steps		Status
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. *To select additional ESA appliances, go to Management Appliance > Centralized Services > 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.

Eseguire il commit delle modifiche nell'SMA.

Per tornare all'ESA, selezionare **Security Services > Policy, Virus and Outbreak Quarantines** (Servizi di sicurezza > Quarantene di policy, virus ed epidemie). I prerequisiti dell'SMA sono ora riconosciuti:



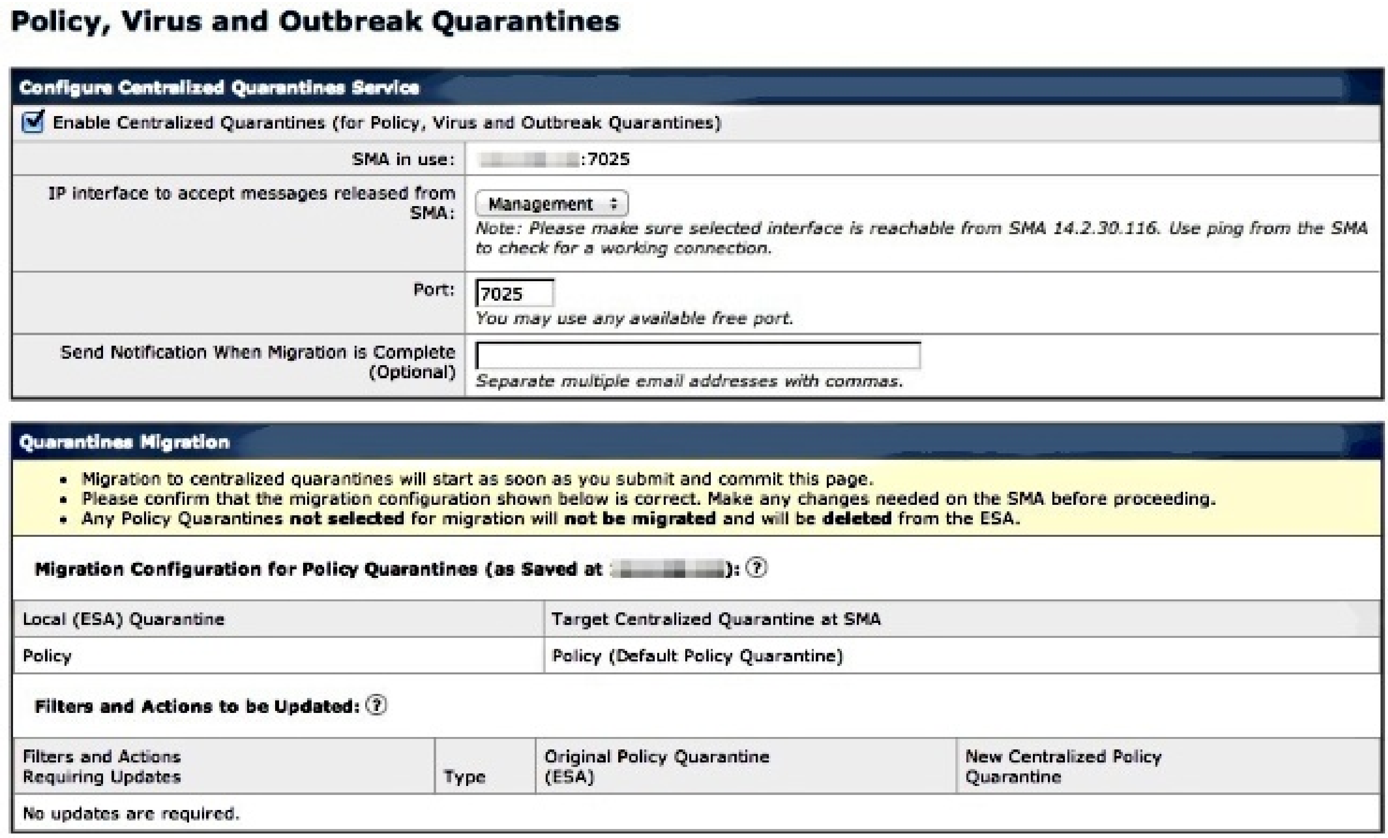
Policy, Virus and Outbreak Quarantines

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.

Fare clic su **Enable?** e continuare:



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: ?

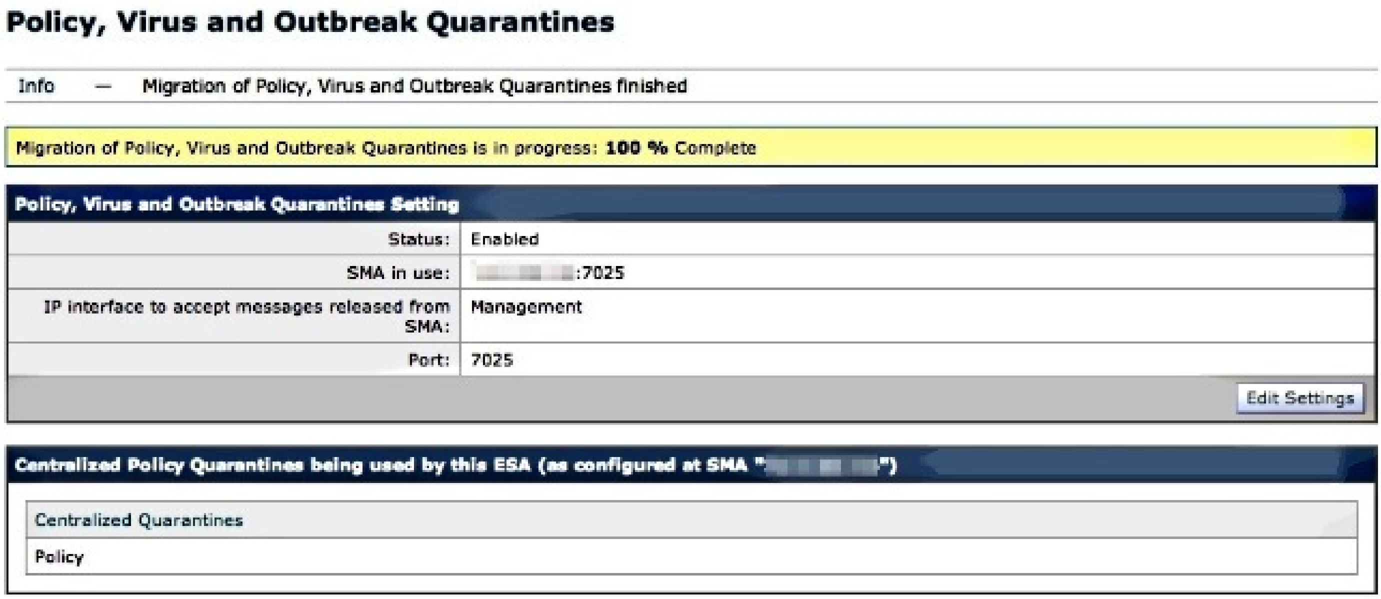
Filters and Actions Requiring Updates	Type	Original Policy Quarantine (ESA)	New Centralized Policy Quarantine
No updates are required.			

Notare che anche in questo caso viene rilevata la porta corretta utilizzata per la comunicazione. Queste **devono** corrispondere e, se si usa un ACL firewall/di rete, devono essere aperte per consentire la corretta migrazione tra l'ESA e l'SMA.

> **Nota**: se su un'ESA sono state configurate quarantene per policy, virus ed epidemie, la migrazione delle quarantene e di tutti i relativi messaggi inizia non appena si esegue il commit della modifica.

> **Nota**: è possibile eseguire un solo processo di migrazione alla volta. Non attivare la quarantena centralizzata di policy, virus ed epidemie su un altro dispositivo di sicurezza e-mail fino al completamento della migrazione precedente.

Fare clic su **Invia** e infine su **Conferma**. La notifica informativa dovrebbe essere simile. Se sono presenti numerosi messaggi già in quarantena locale, l'elaborazione dall'ESA all'SMA potrebbe richiedere del tempo:



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

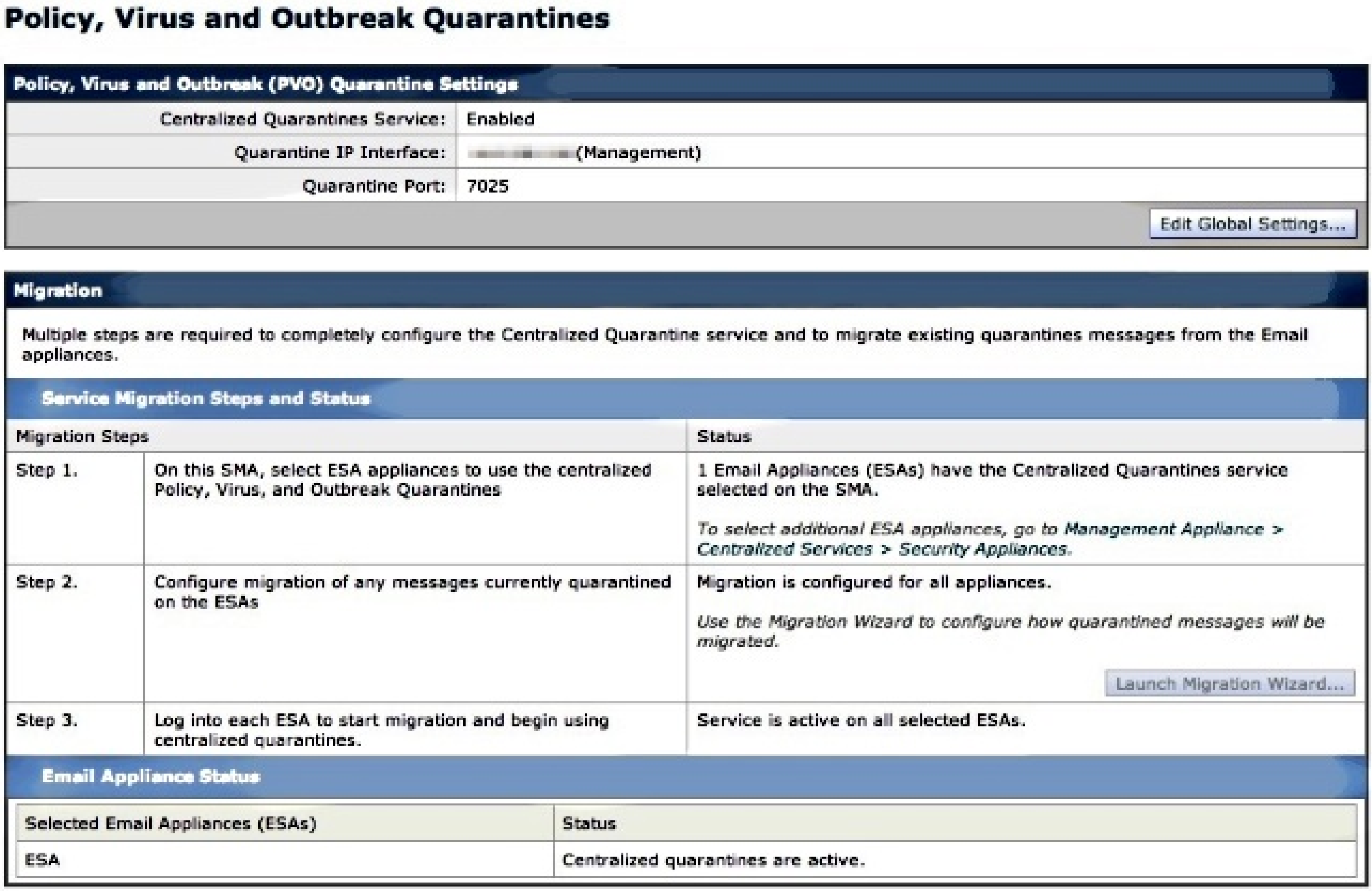
Policy, Virus and Outbreak Quarantines Setting

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

Rivedere l'SMA e selezionare **Management Appliance > Centralized Services > Policy, Virus and Outbreak Quarantines** (Appliance di gestione > Servizi centralizzati > Quarantene criteri, virus ed epidemie). A questo punto, le operazioni di migrazione saranno completate:



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

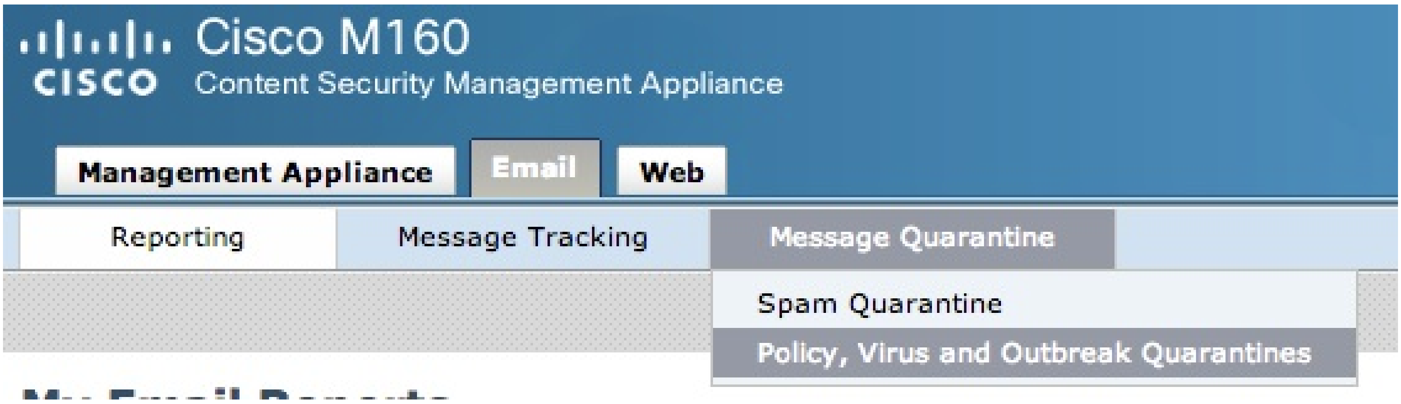
Migration Steps		Status
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. *To select additional ESA appliances, go to Management Appliance > Centralized Services > 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.

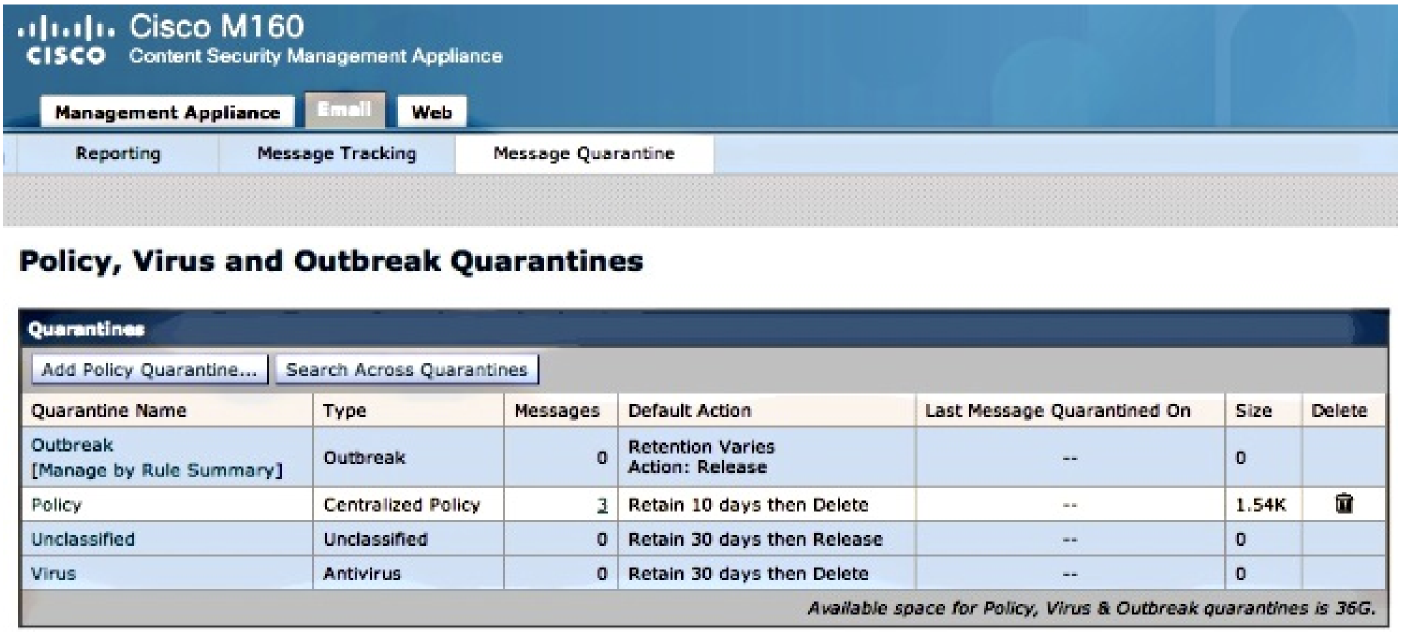
Email Appliance Status

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

Verifica

Al momento, la migrazione della quarantena politica dall'ESA all'SMA è completa. Per la verifica finale, controllare la quarantena della policy sull'SMA:





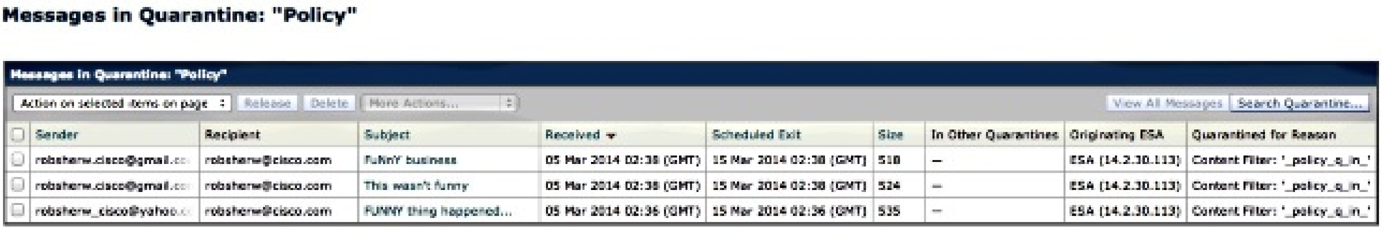
Policy, Virus and Outbreak Quarantines

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.

Dovrebbero essere visualizzati gli stessi messaggi originariamente elencati nell'ESA. Selezionare il collegamento ipertestuale # nella colonna messaggi e verificare:


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_'

Se si guardano i mail_logs sull'ESA, la migrazione dei messaggi effettivi sarà presentata:

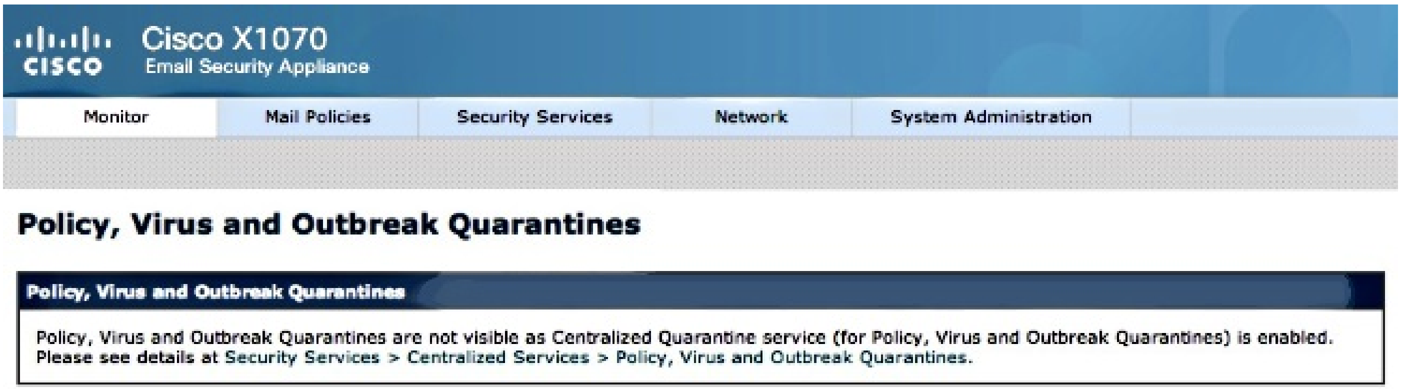
> **Nota**: notare l'uso della comunicazione tra ESA (XX.X.XX.XXX) e SMA (YY.Y.YY.YYY) tramite la porta 7025.

```
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
```

Rivedere l'ESA, e quanto segue è ora presentato quando si visualizza la politica, virus, epidemie quarantene:



Policy, Virus and Outbreak Quarantines

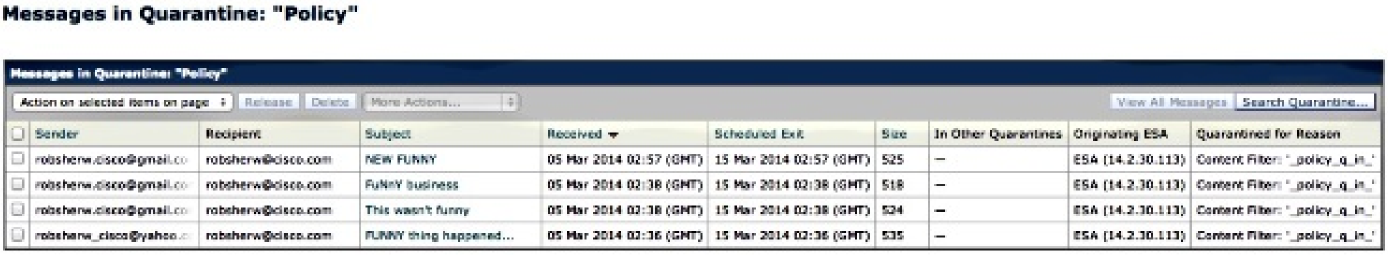
Policy, Virus and Outbreak Quarantines

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.

Il passo successivo della verifica è l'invio di un nuovo messaggio di prova attraverso l'ESA che sarà preso in quarantena. Osservando mail_logs sull'ESA, notate la riga evidenziata che indica il trasferimento dall'ESA all'SMA tramite 7025, che indica la Quarantena della Politica:

```
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
```

Rivedere la precedente messa in quarantena delle policy sull'SMA, il nuovo messaggio di prova è ora in quarantena:



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_'

Informazioni correlate

- Non è possibile abilitare la policy di centralizzazione ESA, la quarantena per virus ed epidemie (PVO)
- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems