

# La directiva de centralización ESA, el virus, y la cuarentena del brote (PVO) no pueden ser habilitados

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Escenario 1](#)

[Escenario 2](#)

[Escenario 3](#)

[Situación 4](#)

[Situación 5](#)

[Situación 6](#)

[Información Relacionada](#)

## Introducción

Este documento describe un problema encontrado donde la directiva, el virus, y la cuarentena de centralización del brote (PVO) no se pueden habilitar en el dispositivo de seguridad del correo electrónico de Cisco (ESA) porque el botón Enable Button es grayed hacia fuera y ofrece una solución al problema.

## Prerequisites

## Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo habilitar PVO en el dispositivo de la Administración de seguridad (S A).
- Cómo agregar el servicio PVO a cada ESA manejado.
- Cómo configurar la migración de PVO.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 8.1 y posterior S A
- Versión 8.0 y posterior ESA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

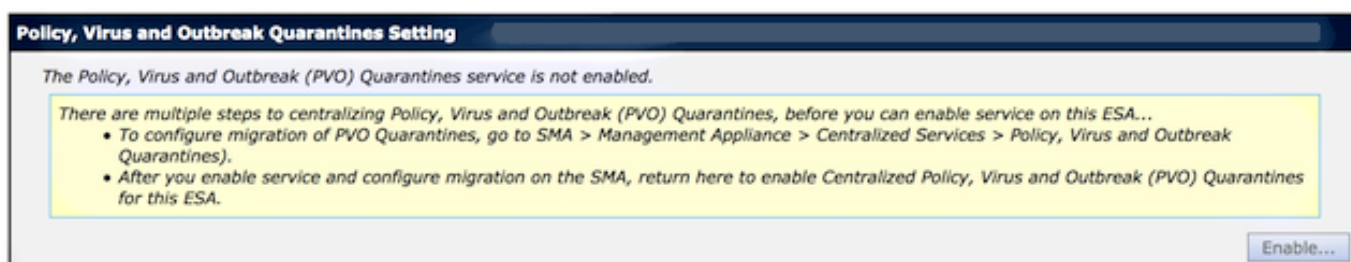
## Antecedentes

Los mensajes procesados por ciertos filtros, las directivas, y las operaciones de exploración en un ESA se pueden poner en las cuarentenas para llevarlas a cabo temporalmente para la acción adicional. En algunos casos, aparece que el PVO no se puede habilitar en el ESA aunque fuera configurado correctamente en el S A y utilizaron al Asistente de la migración. El botón para habilitar esta característica en el ESA sigue siendo generalmente grayed hacia fuera porque el ESA no puede conectar con el S A en el puerto 7025.



## Problema

En el ESA, el botón Enable Button es grayed hacia fuera.

### Policy, Virus and Outbreak Quarantines



Las demostraciones S A mantienen no activo y la acción requeridos

| 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.<br><br><i>To select additional ESA appliances, go to Management Appliance &gt; Centralized Services &gt; Security Appliances.</i>  |
| Step 2.  | Configure migration of any messages currently quarantined on the ESAs   | Migration is configured for all appliances.<br><br><i>Use the Migration Wizard to configure how quarantined messages will be migrated.</i><br><br><a href="#">Launch Migration Wizard...</a>                               |
| 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.<br><br><i>Log into each ESA as required to enable the service (see status below).</i> |
| Email Appliance Status   |   |  |
| Selected Email Appliances (ESAs)   | Status  |  |
| Sobek  |  Action Required: Log into ESA to enable Centralized Quarantine. |  |

## Solución

Hay varios escenarios, que se describen aquí.

### Escenario 1

En el S A, funcione con el **comando status** en el CLI para asegurarse que el dispositivo está en un estado en línea. Si el S A es offline, el PVO no se puede habilitar en el ESA porque la conexión falla.

```
sma.example.com> status
```

Enter "status detail" for more information.

```
Status as of:           Mon Jul 21 11:57:38 2014 GMT
Up since:              Mon Jul 21 11:07:04 2014 GMT (50m 34s)
Last counter reset:   Never
System status:        Offline
Oldest Message:      No Messages
```

Si el S A es offline, funcione con el comando del **curriculum vitae** para traerlo detrás en línea, que comienza el cpq\_listener.

```
sma.example.com> resume
```

Receiving resumed for euq\_listener, cpq\_listener.

### Escenario 2

Después de que usted utilice al Asistente de la migración en el S A, es importante confiar los cambios. El [Enable...] el botón en el ESA sigue siendo grayed hacia fuera si usted no confía los cambios.

1. El registro en el S A y el ESA con la **cuenta del administrador**, no el **operador** (u otros tipos de la cuenta) o la configuración se pueden realizar solamente el [Enable...] el botón será grayed hacia fuera en el lado ESA.
2. En el S A, elija el **dispositivo de la Administración > los servicios > directiva, virus, y las cuarentenas centralizados del brote**.
3. Haga clic al **Asistente de la migración del lanzamiento** y elija un método de la migración.
4. **Someta y confíe** sus cambios.

## Escenario 3

Si el ESA se ha configurado con una interfaz predeterminada de la salida vía el comando del **deliveryconfig** y si esa interfaz predeterminada no tiene ninguna Conectividad hacia el S A porque reside en una diversa subred o allí no es ninguna ruta, el PVO no se puede habilitar en el ESA.

Aquí está un ESA con la interfaz predeterminada de la salida configurada para interconectar **en**:

```
mx.example.com> deliveryconfig
```

```
Default interface to deliver mail: In
```

Aquí está una prueba de conectividad ESA de la interfaz **adentro al puerto 7025 S A**:

```
mx.example.com> telnet
```

```
Please select which interface you want to telnet from.
```

```
1. Auto  
2. In (192.168.1.1/24: mx.example.com)  
3. Management (10.172.12.18/24: mgmt.example.com)  
[1]> 2
```

```
Enter the remote hostname or IP address.
```

```
[> 10.172.12.17
```

```
Enter the remote port.
```

```
[25]> 7025
```

```
Trying 10.172.12.17...
```

```
telnet: connect to address 10.172.12.17: Operation timed out
```

```
telnet: Unable to connect to remote host
```

Para solucionar este problema, configure el interace predeterminado al **auto** donde el ESA utiliza la interfaz correcta automáticamente.

```
mx.example.com> deliveryconfig
```

```
Default interface to deliver mail: In
```

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

```
- SETUP - Configure mail delivery.
```

```
[> setup
```

Choose the default interface to deliver mail.

1. **Auto**
  2. In (192.168.1.1/24: mx.example.com)
  3. Management (10.172.12.18/24: mgmt.example.com)
- ```
[1]> 1
```

## Situación 4

Las conexiones a la cuarentena centralizada son Transport Layer Security (TLS) - cifrado por abandono. Si usted revisa el archivo del registro del correo en el ESA y busca para los ID de conexiones de la salida (DCIDs) al puerto 7025 en el S A, usted puede ser que vea los errores fallados TLS tales como esto:

```
Mon Apr 7 15:48:42 2014 Info: New SMTP DCID 3385734 interface 172.16.0.179
address 172.16.0.94 port 7025
Mon Apr 7 15:48:42 2014 Info: DCID 3385734 TLS failed: verify error: no certificate
from server
Mon Apr 7 15:48:42 2014 Info: DCID 3385734 TLS was required but could not be
successfully negotiated
```

Cuando usted ejecuta un `tlsverify` en el ESA CLI, usted ve lo mismo.

```
mx.example.com> tlsverify
```

```
Enter the TLS domain to verify against:
[ ]> the.cpq.host
```

```
Enter the destination host to connect to. Append the port (example.com:26) if you are not
connecting on port 25:
[the.cpq.host]> 10.172.12.18:7025
```

```
Connecting to 10.172.12.18 on port 7025.
Connected to 10.172.12.18 from interface 10.172.12.17.
Checking TLS connection.
TLS connection established: protocol TLSv1, cipher ADH-CAMELLIA256-SHA.
Verifying peer certificate.
Certificate verification failed: no certificate from server.
TLS connection to 10.172.12.18 failed: verify error.
TLS was required but could not be successfully negotiated.
```

```
Failed to connect to [10.172.12.18].
TLS verification completed.
```

De acuerdo con esto, la cifra **ADH-CAMELLIA256-SHA** usada para negociar con el S A hace el S A no poder presentar un certificado de peer. La investigación adicional revela que todas las cifras alimentador de originales utilizan la autenticación anónima, que no proporciona un certificado de peer. **El arreglo aquí es eliminar las cifras anónimas.** Para hacer esto, cambie la lista saliente de la cifra a **HIGH:MEDIUM:ALL:-aNULL:-SSLv2.**

```
mx.example.com> sslconfig
```

```
sslconfig settings:
GUI HTTPS method: sslv3tlsv1
GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
Inbound SMTP method: sslv3tlsv1
Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
Outbound SMTP method: sslv3tlsv1
Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
```

Choose the operation you want to perform:

- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.

[>] **OUTBOUND**

Enter the outbound SMTP ssl method you want to use.

1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1

[5]>

Enter the outbound SMTP ssl cipher you want to use.

[RC4-SHA:RC4-MD5:ALL]> **HIGH:MEDIUM:ALL:-aNULL:-SSLv2**

sslconfig settings:

```
GUI HTTPS method:  sslv3tlsv1
GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
Inbound SMTP method:  sslv3tlsv1
Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
Outbound SMTP method:  sslv3tlsv1
Outbound SMTP ciphers: HIGH:MEDIUM:ALL:-aNULL:-SSLv2
```

Choose the operation you want to perform:

- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.

[>]

mx.example.com> **commit**

**Tip:** También agregue **-SSLv2** porque éstas son cifras inseguras también.

## Situación 5

El PVO no se puede habilitar y muestra a este tipo de mensaje de error.

Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines configuration as host1 and host2 in Cluster have content filters / DLP actions available at a level different from the cluster Level.

El mensaje de error puede indicar que uno de los host no tiene las teclas de función DLP aplicadas y el DLP está inhabilitado. La solución es agregar las teclas de función que falta y aplicar las configuraciones DLP idénticas como en el host que tiene las teclas de función aplicadas. Esta inconsistencia de las teclas de función pudo tener el mismo efecto con los filtros del brote, el antivirus de Sophos, y las claves de la otra función.

## Situación 6

El botón Enable Button para el PVO será grayed hacia fuera si, en una configuración de clúster hay configuración de la máquina o del grupo-nivel por contenido, mensaje filtra, las

configuraciones DLP, y DMARC. Para solucionar este problema, todos los filtros del mensaje y del contenido se deben mover desde el cluster-nivel de la máquina o del grupo-nivel así como las configuraciones DLP y DMARC. Alternativamente, usted puede quitar totalmente la máquina que tiene configuración del nivel de equipo del cluster. Ingrese el **clusterconfig > el removemachine** del comando CLI y después únase a lo de nuevo al cluster para heredar la configuración de clúster.

## Información Relacionada

- [Resuelva problemas la salida y a la cuarentena PVO en el S A](#)
- [Requisitos para el Asistente de la migración PVO cuando se agrupa el ESA](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)