# Procedimiento de copia de seguridad de listas de seguridad/listas de bloqueo ESA

## Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Generar archivos de respaldo SLBL](#)

## Introducción

Este documento describe cómo realizar una copia de seguridad de las listas de seguridad/listas de bloqueo (SLBL) en Cisco Email Security Appliance (ESA).

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información de este documento se basa en Cisco Email Security Appliance (ESA) y en todas las versiones de AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Generar archivos de respaldo SLBL

Desde la interfaz web ESA, navegue hasta **Administración del sistema > Archivo de configuración > Base de datos de lista de seguridad/lista de bloqueo de usuario final (Spam Quarantine).** Puede generar archivos de copia de seguridad desde esta ubicación.

**Nota:** Si tiene varios ESA en clúster, debe cargar los archivos de copia de seguridad en

cada unidad opuesta.

Ingrese el comando **slblconfig** en la CLI para importar y exportar la configuración SLBL:

```
> slblconfig

End-User Safelist/Blocklist: Enabled

Choose the operation you want to perform:
- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.
[]> export

End-User Safelist/Blocklist export has been initiated...
Please wait while this operation executes.

End-User Safelist/Blocklist successfully exported to
slbl-782BCB64XXYY-1234567-20140717T020032.csv (200B).
```

A continuación, debe acceder al ESA mediante el protocolo de transferencia de archivos (FTP) para recuperar y conservar la configuración SLBL recién creada y exportada:

```
$ ftp user@myesa.local
Connected to myesa.local.
220 myesa.local.rtp Cisco IronPort FTP server (V8.5.6) ready
331 Password required.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> hash
Hash mark printing on (1024 bytes/hash mark).
ftp> bin
200 Type set to Binary.
ftp> cd configuration
250 CWD command successful.
ftp> ls
227 Entering Passive Mode (172,16,1,1,XX,YYY)
150 Opening ASCII mode data connection for file list
drwxrwx--- 2 root config 512 Oct 14 2013 iccm
-rw-rw---- 1 admin config 1117 Oct 14 2013 profanity.txt
-rw-rw---- 1 admin config 90 Oct 14 2013 proprietary_content.txt
-rw-rw---- 1 admin config 2119 Oct 14 2013 sexual_content.txt
-rw-rw---- 1 admin config 28025 Oct 14 2013 ASYNCOS-MAIL-MIB.txt
-rw-rw---- 1 admin config 1292 Oct 14 2013 IRONPORT-SMI.txt
-r--r--r-- 1 root wheel 436237 Jul 9 16:51 config.dtd
drwxrwx--- 2 root config 512 May 28 20:23 logos
-rw-rw---- 1 root config 1538 May 30 17:25 HAT_TEST
-rw-r----- 1 admin config 18098688 Jul 9 16:59 warning.msg
-r--r--r-- 1 root wheel 436710 Jul 9 16:51 cluster_config.dtd
-rw-rw---- 1 nobody config 200 Jul 16 22:00
slbl-782BCB64XXYY-1234567-20140717T020032.csv
#
226 Transfer Complete
ftp> get slbl-782BCB64XXYY-1234567-20140717T020032.csv
local: slbl-782BCB64XXYY-1234567-20140717T020032.csv remote:
slbl-782BCB64XXYY-1234567-20140717T020032.csv
227 Entering Passive Mode (172,16,1,1,XX,YYY)
150 Opening Binary mode data connection for file
'slbl-782BCB64XXYY-1234567-20140717T020032.csv'
```

```
#
226 Transfer Complete
200 bytes received in 00:00 (8.63 KiB/s)
ftp> exit
221 Goodbye.
```

El archivo de copia de seguridad se transfiere ahora localmente. Puede abrir y ver las entradas SLBL según sea necesario.