



**Document ID:** 117922

**Updated:** Nov 04, 2015

Contributed by Carl Rogers and Robert Sherwin, Cisco TAC Engineers.



[Download PDF](#)



[Print](#)

[Feedback](#)

### Related Products

- [Cisco Email Security Appliance](#)

## Contents

[Introduction](#)  
[Prerequisites](#)  
[Requirements](#)  
[Components Used](#)  
[Generate SLBL Backup Files](#)  
[Related Cisco Support Community Discussions](#)

## Introduction

This document describes how to back up Safelists/Blocklists (SLBL) on the Cisco Email Security Appliance (ESA).

## Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on the Cisco Email Security Appliance (ESA) and all versions of 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.

# Generate SLBL Backup Files

From the ESA web interface, navigate to **System Administration > Configuration File > End-User Safelist/Blocklist Database (Spam Quarantine)**. You can generate backup files from this location.

**Note:** If you have several ESAs in cluster, you must upload the backup files to each opposing unit.

Enter the **sblconfig** command into the CLI in order to import and export the SLBL configuration:

```
> sblconfig
```

```
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  
sbl-782BCB64XXYY-1234567-20140717T020032.csv (200B).
```

You must then access the ESA via File Transfer Protocol (FTP) in order to retrieve and retain the newly-created, exported SLBL configuration:

```
$ 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  
sbl-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.
```

Your backup file is now transferred locally. You can open and view the SLBL entries as needed.

Was this document helpful? [Yes](#) [No](#)

Thank you for your feedback.

[Open a Support Case](#) 📄(Requires a [Cisco Service Contract](#).)

## Related Cisco Support Community Discussions

The [Cisco Support Community](#) is a forum for you to ask and answer questions, share suggestions, and collaborate with your peers.

Refer to [Cisco Technical Tips Conventions](#) for information on conventions used in this document.