# Release Notes for Configuration Migration Tool 1.0 for Cisco Content Security Virtual Appliances

# Contents

# Purpose of the Configuration Migration Tool

This Configuration Migration Tool converts a configuration file from a physical Cisco Email Security appliance or Cisco Web Security appliance into a new file that can be uploaded to a virtual appliance. You can also convert a configuration file from a virtual appliance in order to upload it to a physical appliance.

**Cisco Systems, Inc.**
www.cisco.com

# Configuration Migration Requirements

## System Requirements

The Configuration Migration Tool is a command line application that requires a computer running Windows 7.

## Compatible Versions of AsyncOS

The following table displays the compatible versions of AsyncOS for Web and Email. You must have the latest build for each version in order to migrate your configuration.

The versions of AsyncOS running on a virtual appliance are referred to as "WSAV" and "ESAV".

*Table 1-1*    *Compatible Versions of AsyncOS for the Configuration Migration Tool*

| Source AsyncOS Version | Destination AsyncOS Version |
|---|---|
| WSA 7.5.0 | WSAV 7.7.5 |
| WSA 7.5.1 | WSAV 7.7.5 |
| WSA 7.5.2 | WSAV 7.7.5 |
| WSA 7.7.0 | You can upload a 7.7.0 configuration file directly to a virtual appliance running 7.7.5. Do not use the Configuration Migration Tool. |
| WSAV 7.7.5 | WSA 7.7.0 |
| ESA 7.6.0 | ESAV 8.0.0 |
| ESA 7.6.1 | ESAV 8.0.0 |
| ESA 7.6.2 | ESAV 8.0.0 |
| ESA 7.6.3 | ESAV 8.0.0 |
| ESA 8.0.0 | ESAV 8.0.0 |
| ESAV 8.0.0 | ESA 8.0.0 |

**For AsyncOS releases later than the versions listed in this table:**
The configuration migration tool is not compatible with newer AsyncOS releases.
For configuration migration instructions, see the AsyncOS release notes.

# Appliance Settings Not Transferred

The following settings cannot be transferred between physical and virtual security appliances:

- Network settings
- Hardware-specific settings
- SaaS certificate names

Before you upload the converted configuration file to the destination appliance, you will need to configure the network settings on that appliance. You can install any necessary SaaS certificates after you upload the new configuration file.

**Note** If the new network settings and interfaces you configure differ from the settings on the original physical appliance, certain features migrated to the virtual appliance may not work correctly, such as service updates, the Network Time Protocol server, packet capture, and (vESA only) content filters. You will need to update those configurations.

# Downloading and Installing the Configuration Migration Tool

Download the Configuration Migration Tool from the Software Downloads area on Cisco.com.

**Step 1** Navigate to the the relevant URL:

- For Email Security Appliances:

  http://software.cisco.com/download/release.html?mdfid=284900944&flowid=41782&softwareid=282975113&release=8.0.0&relind=AVAILABLE&rellifecycle=GD&reltype=latest

- For Web Security Appliances:

  http://software.cisco.com/download/release.html?mdfid=284806698&flowid=41610&softwareid=282975114&release=7.7.5&relind=AVAILABLE&rellifecycle=GD&reltype=latest

**Step 2** Click the link for this tool in the navigation bar on the left side of the page and download the tool.

**Step 3** Run the installation wizard on a Windows 7 computer and use the default settings.

The Configuration Migration Tool will be installed in the following directory:
`C:\Cisco\ConfigMigration`.

# Migrating Your Appliance's Configuration

**Before You Begin**

- For instructions about downloading and uploading configuration files, read the documentation on configuration files in the online help or user guide for your AsyncOS version.

- Install the Configuration Migration Tool.

- From the source appliance, download the configuration file that you want to convert. It must be saved on the local Windows 7 computer.

  **Note** Do not mask passwords.

- Configure the network settings on the destination appliance.

**Procedure**

**Step 1** Click the Start menu on the local Windows 7 computer.

**Step 2** Enter `cmd.exe` in the search field and press Enter.

Windows opens the command line prompt.

**Step 3** Run the `C:\Cisco\ConfigMigration\ConfigMigration.bat [option]` program with the following options:

| Option | Description |
|---|---|
| `-h, --help` | Shows the list of options for the Configuration Migration Tool command. |
| `-i FILE, --input=FILE` | Enter the path and filename of the existing configuration file you want to convert. |
| `-o FILE, --output=FILE` | Enter the filename for the new configuration file. |
| `-l FILE, --log-file=FILE` | Enter the filename for the log you want to create for the migration. By default, the log filename is `migration.log`. |
| `-t TEMP_DIR, --temp-dir=TEMP_DIR` | Enter the name of a new directory to store the new configuration file. |
| `-p PRODUCT, --product=PRODUCT` | (Optional) Enter whether the configuration is for the Email Security appliance or the Web Security appliance. Enter `ESA` or `WSA` as the product. The tool can determine the product based on the input configuration file. |
| `-m MODEL, --source_model=MODEL` | (Optional) Enter the model name for the source appliance. For example, `S660`. The tool can determine the model based on the input configuration file. |
| `-s VERSION, --source_version=VERSION` | (Optional) Enter the version of AsyncOS running on the source appliance. For example, `7.5.0.359`. The tool can determine the source version of AsyncOS based on the input configuration file. |
| `-d MODEL, --dest_model=MODEL` | (Optional) Enter the model name of the destination appliance. For example, `S300V`. The tool can determine the model of the destination appliance. |

**Step 4** On the destination appliance, upload the converted configuration file from the local computer:

Use the Load Configuration section of the **System Administration > Configuration File** page

-or-

Run the `loadconfig` command in the appliance's CLI and upload the configuration file from the local computer.

**Step 5** If you see a warning message stating that the configuration file is not supported by the current AsyncOS version, ignore this warning.

**Step 6** Commit your changes.

**Step 7** (Email Security appliances only) Resume the operation of the appliance:

Use the **System Administration > Shutdown/Suspend** page in the Web interface.

-or-

Run the `resume` command in the CLI.

**What To Do Next**

Configure settings not transferred by the configuration file. See Appliance Settings Not Transferred, page 2.

# Known Issues

*Table 2 Known Issues for Cisco Configuration Migration Tool*

| Old Defect ID | Bug Toolkit ID | Affects | Description |
|---|---|---|---|
| 89817 | CSCzv30028 | WSA | **Report data exceeds limits set in reportingconfig > counters settings** <br><br> These `reportingconfig > counters` settings are not preserved after upgrading or after using saveconfig, resetconfig, and loadconfig: <br><br> • Minimally Limited Reporting Data. <br><br> • Moderately Limited Reporting Data. |
| — | CSCuh03579 | ESA | **Can't load configuration which has PIPv6 range in network access page** <br><br> An error occurs when loading a configuration file that has an IPv6 in the Network Access settings. |
| 91686 | CSCzv58354 | ESA | **Configuration load: Interface name must be a name of interface** <br><br> Configuration saved on an appliance was loaded back on either the same appliance or a new appliance and it produced an error due to an old packet capture test that used an interface that has been renamed since the packet capture. <br><br> Workaround: Set up the packet capture again and set the interface to "ALL." <br><br> If the interface is not set to "ALL" and you set it as a specific interface, it stores in to the configuration. When you try to load the configuration again after the interface name change it fails due to the file referencing an interface that is no longer available. |
| 86130 | CSCzv56986 | ESA | **Can't load configuration which contains specific IPv6 format address in HAT sender group** <br><br> An error occurs when you attempt to load a configuration file that contains an IPv6 address in a HAT sender group. |
| 88881 | CSCzv63858 | ESA | **The loadconfig command does not accept 'message_tag_list' from within the DLP sections** <br><br> The "message_tag_list" element may appear in the wrong order in the configuration guide when exporting from an appliance running AsyncOS for Email 7.6.1 and 7.6.2. This causes an error when loading the configuration file on another appliance. |

***Table 2        Known Issues for Cisco Configuration Migration Tool***

| Old Defect ID | Bug Toolkit ID | Affects | Description |
|---|---|---|---|
| 81763 | CSCzv11261 | ESA | **Loading a configuration file fails when an alias domain is written as IPv6 or IPv4 addresses**<br><br>Aliases for domains can be written as IPv6 and IPv4 addresses, but loadconfig fails when an alias domain is written in one of these formats. |
| 82164 | CSCzv50701 | ESA | **Can't load configuration if DLP notification template is empty**<br><br>You cannot load a configuration file to another appliance if you've created a DLP notification template that's empty. |
| 76241 | CSCzv24706 | ESA | **Can't load configuration if "modified subject" on DLP page contains double byte symbols with a length is more than 128 bytes**<br><br>Can't load a configuration file on a new appliance if the "modified subject" for a DLP policy contains a double-byte symbol with a length of more than 128 bytes. |

# Related Documentation

The documentation set for Cisco Content Security virtual appliances includes the following documents and books:

- *Release Notes for the Configuration Migration Tool for Cisco Content Security Virtual Appliances* (This document)
- *Cisco Content Security Virtual Appliance Installation Guide*
- *Cisco IronPort AsyncOS for Web User Guide*
- *Cisco IronPort AsyncOS CLI Reference Guide*
- *Cisco AsyncOS for Email User Guide*

This and other documentation is available at the following locations:

| Documentation For Cisco Content Security Products | Location |
|---|---|
| Cisco Email Security | http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html |
| Cisco Web Security | http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html |
| Cisco Content Security Managment | http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html |
| CLI reference guide for Cisco Content Security appliances | http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html |
| Cisco IronPort Encryption | http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html |

# Service and Support

To obtain support, visit:

International: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.