Safe Print for Email Security Appliance

Contents

Introduction

This document describes the feature "Safe Print" on the Cisco Email Security Appliance (ESA).

Prerequisites

Safe Print feature is available in ESA AsyncOS 13.0 and newer versions.

The configuration of Safe Print will involve the basic understanding of content filter behavior.

Background Information

The Email Security Appliance can be configured to provide a safe view (safe-printed PDF version) of a message attachment detected as malicious or suspicious. The safe view of the message attachment is delivered to the end-user and the original attachment is stripped from the message. The 'Safe Print' content filter action provides a variety of options based on the content filter condition.

The ability to safe print message attachments in the email gateway helps an organization to:

- Prevent message attachments with malicious or suspicious content from entering an organization network.
- View malicious or suspicious message attachments without being affected by malware.
- Deliver the original message attachment based on the end-user request.

What Safe Print does.

- Scan messages up to the size of the Scan Config "Maximum attachment size to scan field," with a max of 6M.
- Print the attachment (approved file types), to an image pdf.
- Print up to 10 pages of the original file.
- Add an optional watermark and Cover Page to the rewritten attachment.

The current [User Guide](#) provides more in-depth detail of the Safe Print Feature within the Chapter, "Configuring Email Gateway to Safe Print Message attachments."

Configure Safe Print

- Safe Print Parameters
- Create and apply a Content Filter to a Mail Policy

Safe Print Parameters

- WebUI > Navigate to > Security Services > Scan Behavior > Edit Global Settings.
- Make note of the value in the blue box.
- Safe Print "Maximum File Size," will take action on files up to 6M, but must be less than the value in the blue box.
- Maximum Page Count: 1 - 10
- Document Quality: 10 - 10

Scan Behavior > Safe Print Settings

- File Type Selection:

File Types supported in 13.0.0-285:

   Document

AcroExch.Document(.pdf)
Hancom Office File(.hwp)
Xhtmlfile(.xhtml)
Xmlfile(.xml)

Microsoft Documents
PowerPoint.Show.12(.pptx)
PowerPoint.Show.8(.ppt)
PowerPoint.ShowMacroEnabled.12(.pptm)
PowerPoint.SlideShow.12(.ppsx)
PowerPoint.SlideShowMacroEnabled.12(.ppsm)
PowerPoint.Template.12(.potx)
PowerPoint.Template.8(.pot)
PowerPoint.TemplateMacroEnabled.12(.potm)
Powerpointxmlfile(.pptxml)
Word.Document.12(.docx)
Word.Document.8(.doc)
Word.Template.12(.dotx)
Word.Template.8(.dot)
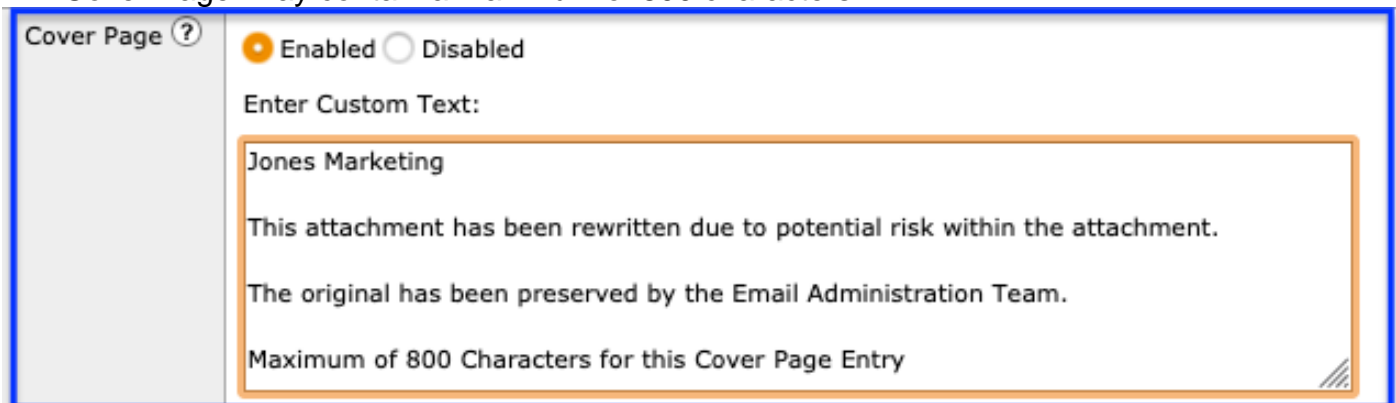Word.TemplateMacroEnabled.12(.dotm)
Wordhtmlfile(.dochtml)

Wordhtmlfile(.docm)

Wordhtmltemplate(.dothtml)

Wordxml(.docxml)

Note: Supported file types may increase with future AsyncOS releases.

- Cover Page: May contain a maximum of 800 characters.

Cover Page ?	● Enabled ◯ Disabled
	Enter Custom Text:
	Jones Marketing
	This attachment has been rewritten due to potential risk within the attachment.
	The original has been preserved by the Email Administration Team.
	Maximum of 800 Characters for this Cover Page Entry

Scan Behavior > Edit Global Settings > Cover Page

- Watermark: May contain a maximum of 20 characters.
- Submit > Commit Changes.

This is a safe-printed document.
The original attachment had 2 page(s).
Safeprint maximum page count configuration is 10 page(s).
Number of pages truncated are 0 page(s).

Jones Marketing

This attachment has been rewritten due to potential risk within the attachment.

The original has been preserved by the Email Administration Team.

Maximum of 800 Characters for this Cover Page Entry

| Cover Page | ● Enabled ○ Disabled |
| Enter Custom Text: |
| Jones Marketing |
| This attachment has been rewritten due to potential risk within the attachment. |
| The original has been preserved by the Email Administration Team. |
| Maximum of 800 Characters for this Cover Page Entry |

Sample Cover Page

Create a certificate

1. create a self signed certificate on the ESA | export in pfx format | then use sslshopper to convert or a known unix string to convert.
   a. Webui > certificate > create > create new self signed certificate > complete the template > submit > commit changes.
   b. Return to the certificate page and choose the export option.

Convert the Exported Certificate

The certificate created and exported from the ESA will be in .pfx format. The SMA only supports .pem format for importing, so this certificate will need to be converted. To convert certificate from .pfx format to .pem format, use one of the two options:
- Convert *.pfx certificate to a *.pem certificate: https://www.sslshopper.com/ssl-converter.html
- openssl command: openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes

A final clean up step is required to prepare the files.
- Create a second text file.
- Open the original certificate file and note the presence of 2 portions, certificate and private key.
- Each portion of the certificate is defined by the boundries ----- BEGIN ...... ----- AND ----- END ... ----
   o Copy the private key into the newly created text file.
   o ------BEGIN PRIVATE KEY----- to ------END PRIVATE KEY------
   o Save the file as your_name.key

   o Next, working with the original file, only save the portion -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----
   o Delete everything else above and below the certificate.
   o Save the file as your_name.cert

The final product will be the two portions to load into the Service Provider certificate options.

2. Generate a self-signed certificate using this set of commands from unix cli
===========================
Do you have a unix server which you can execute the openssl commands?

This command creates a 2048-bit private key (domain.key) and a self-signed certificate (domain.crt) from scratch:
sample:
openssl req -newkey rsa:2048 -nodes -keyout domain.key -x509 -days 365 -out domain.crt

Answer the CSR information prompt to complete the process.
The -x509 option tells req to create a self-signed certificate. The -days 365 option specifies that the certificate will be valid for 365 days. A temporary CSR is generated to gather information to associate with the certificate.

My command:
openssl req -newkey rsa:2048 -nodes -keyout esa1.home.iphmx.com.key -x509 -days 365 -out esa1.home.iphmx.com.crt

Sample:
CHARELLA-M-D2LM:~ charella$ openssl req -newkey rsa:2048 -nodes -keyout esa1.home.iphmx.com.key -x509 -days 365 -out esa1.home.iphmx.com.crt
Generating a 2048 bit RSA private key
...........+++
..+++
writing new private key to 'esa1.home.iphmx.com.key'

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Watermark Sample

Watermark Sample

Create a Content Filter

Safe Print actions will be achieved through the use of Content Filter and the Action, "Safe Print."

Note: The Content Filters will only scan the file types configured in section 1f above, Scan Behavior.

There are **three** choices within the Action, "Safe Print."

- **Safeprint all attachments**: If a Condition matches triggering the Safe Print Action, all attachments get rewritten.   Commonly applied to content filter conditions matching on the "Message Body," and/or "Attachments."This option is very flexible and will function with any condition within a Content Filter.Example: Condition - Remote IP/Hostname, If matched will rewrite all attachments.

- **Safeprint matching attachments:** Only take action on the specific attachment(s) matching the condition.
  This Action has restricted "Choices," for Conditions.Commonly used for content filters with conditions focused on the attachment content.This option can only be used with the following **Conditions**. URL Reputation (Check within: **Attachment**) only this option.URL Category (Check within: **Attachment**) only this option.Macro DetectionAttachment File Info

- **Strip unscannable attachments.**
   As stated, if an attachment is unscannable, this action will strip the attachment.Customer Replacement Message field offers an optional space adding words, phrases to notify.

Safe Print

Do you want to safe print the message attachments when a message matches a configured condition or not?

To configure Safe Print settings globally on your appliance, go to
Security Services > Scan Behavior

Action for attachment(s)
- ● Safeprint all attachments. ⑦
- ○ Safeprint matching attachments. ⑦

Strip unscannable attachment(s)
- ● Yes

    Custom Replacement Message (Optional)

- ○ No

Content Filter Action > Safe Print

Using the above Content Filter Introduction, begin creating a CF.

Tip: Consider the 3 Safe Print choices and associated condition restrictions, mentioned above, as you create the filter.

- WebUI > Navigate to > Mail Policies > Incoming Content Filters > Add Filter.
- Add Condition: The condition depends on the 3 choices for the Safe Print Action.

(Optional Action, very much recommended) Add Action > Quarantine > Duplicate message > Choose the custom quarantine you created for

Safe Print. Choose OK to add.

Action > Quarantine > Duplicate message

> **Tip**: DUPLICATE to Quarantine. As a fail-safe action, consider copying the message to quarantine with the original attachment. If an attachment performs a Safe Print rewrite, this action will act as insurance for any documents you determine to be of value even if they match the conditions. Create a custom Quarantine specifically for Safe Print for easy identification.

- Add Action > Safe Print Choose the Safe Print Choice that corresponds with the Conditions.
- (Optional) Add Action - Add Log entry and include text which will reflect in the Message Tracking to confirm a match. Examples: use special characters to highlight for visibility, Add a description or filter name to identify - # Safe Print # or > Safe Print <
- Submit to create the content filter. Commit Changes to save to the ESA.

Sample Safe Print Content Filter

Log entries specific to Safe Print Message Processing.

```
MID 95 The attachment(s) are successfully safe-printed, Filename(s):
Create_Certificate_for=20Amp.docx
MID 95 rewritten to MID 96 by safeprint-matching-attachments-strip-unscan filter 'SP_type'
```

Reporting View from the Next Generation Reporting (ng)

Allows the user to click numbers and redirect to Message Tracking using a new browser tab.
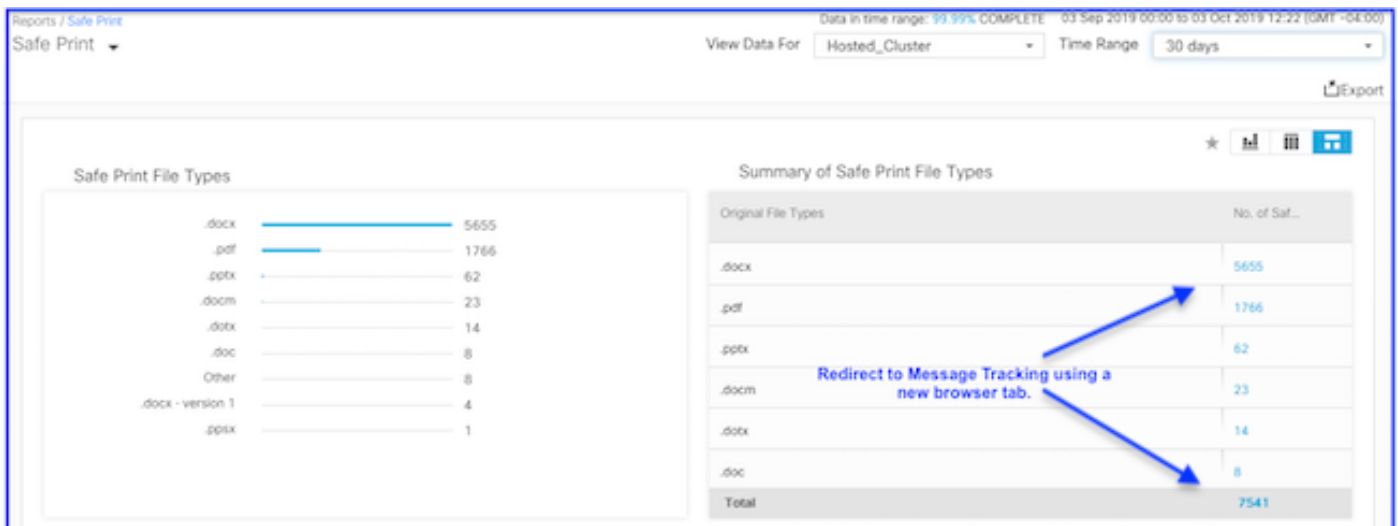
NG Report Safe Print

Tracking criteria from Report Redirect Action

Search Results from Report redirect action

 Advanced Search Option - Safe Print

Troubleshoot

Mail Logs at Trace Level: Display alerts.

Sample Logging

Related Information

- Cisco Email Security Appliance - Product Support
- Cisco Email Security Appliance - Release Notes
- Cisco Email Security Appliance - End-User Guides
- Cisco Content Security Management Appliance - Product Support
- Cisco Content Security Management Appliance - Release Notes
- Cisco Content Security Management Appliance - End-User Guides

- [Cisco Web Security - Product Support](#)
- [Cisco Web Security - Release Notes](#)
- [Cisco Web Security - End-User Guides](#)