Introduce Password Protected File Analysis (PPFA)

Contents

Introduction

This document describes the new Password Protected File Analysis (PPFA) added to the Email Security Appliance (ESA) version 14.X.

Prerequisites

Requirements

Cisco recommends that you have knowledge of ESA concepts and configuration.

Components Used

The information in this document is based on AsyncOS for ESA 14.0 and later.

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, ensure that you understand the potential impact of any command.

Background Information

Previously, the contents of a password protected document or archive file attachment such as PDF, Doc, ZIP and so on, could not be analyzed because the password was unknown.

With the introduction of PPFA, emails which contain password-protected file attachments can be analyzed for malicious activity and data privacy if the password is present in the mail body.

Supported Formats and Language

Here is the list of supported formats:

- PDF
- MS Office File

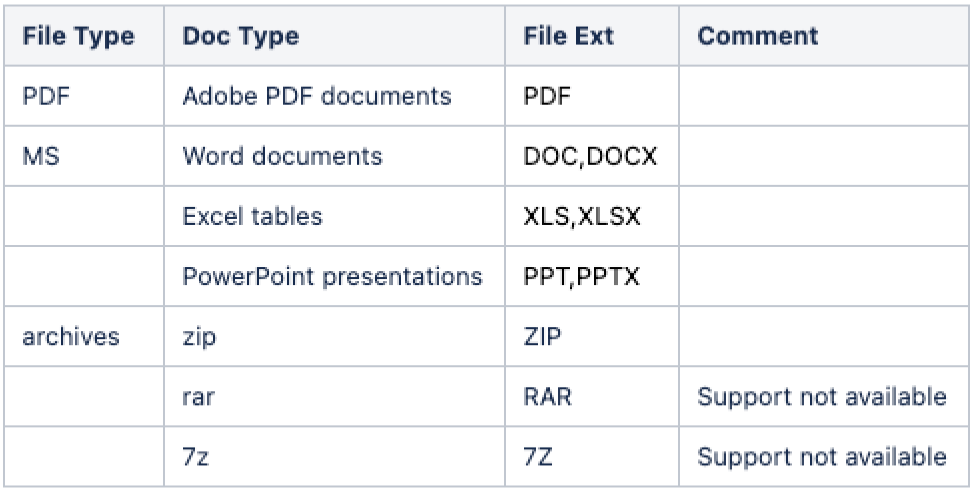
  doc/x 2007-2019 / doc 2002 to 2004

  xls/x 2007-2019

ppt/x 2007-2019

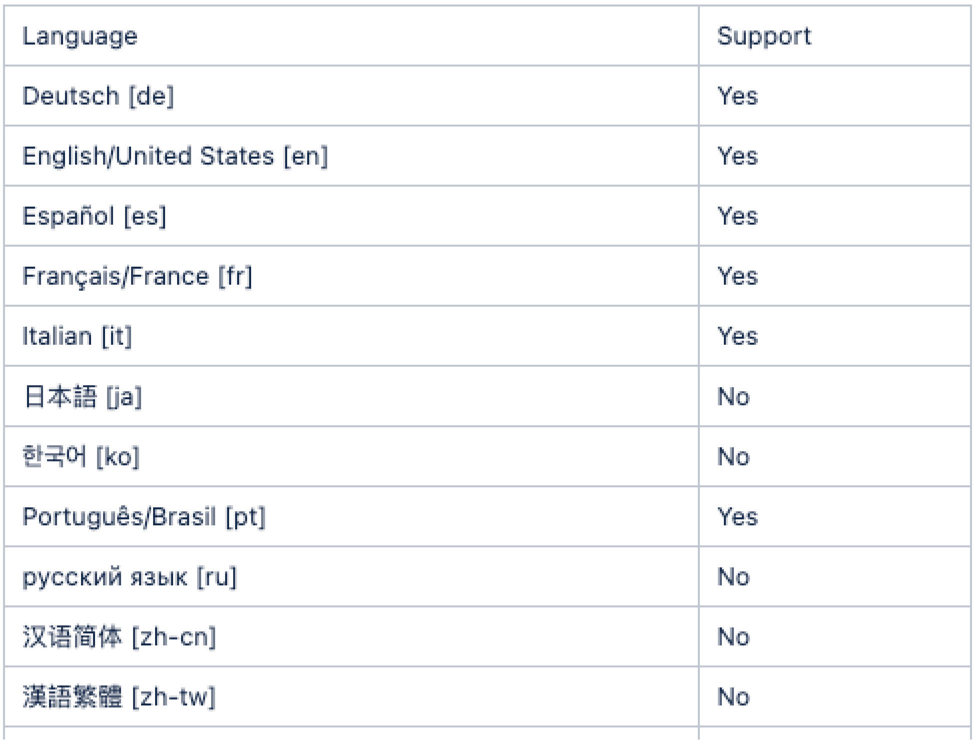
- Archive

zip, rar, 7z



File Type	Doc Type	File Ext	Comment
PDF	Adobe PDF documents	PDF	
MS	Word documents	DOC,DOCX	
	Excel tables	XLS,XLSX	
	PowerPoint presentations	PPT,PPTX	
archives	zip	ZIP	
	rar	RAR	Support not available
	7z	7Z	Support not available

Here you can find the list of supported languages:



Language	Support
Deutsch [de]	Yes
English/United States [en]	Yes
Español [es]	Yes
Français/France [fr]	Yes
Italian [it]	Yes
日本語 [ja]	No
한국어 [ko]	No
Português/Brasil [pt]	Yes
русский язык [ru]	No
汉语简体 [zh-cn]	No
漢語繁體 [zh-tw]	No

Considerations

PPFA is disabled by default.

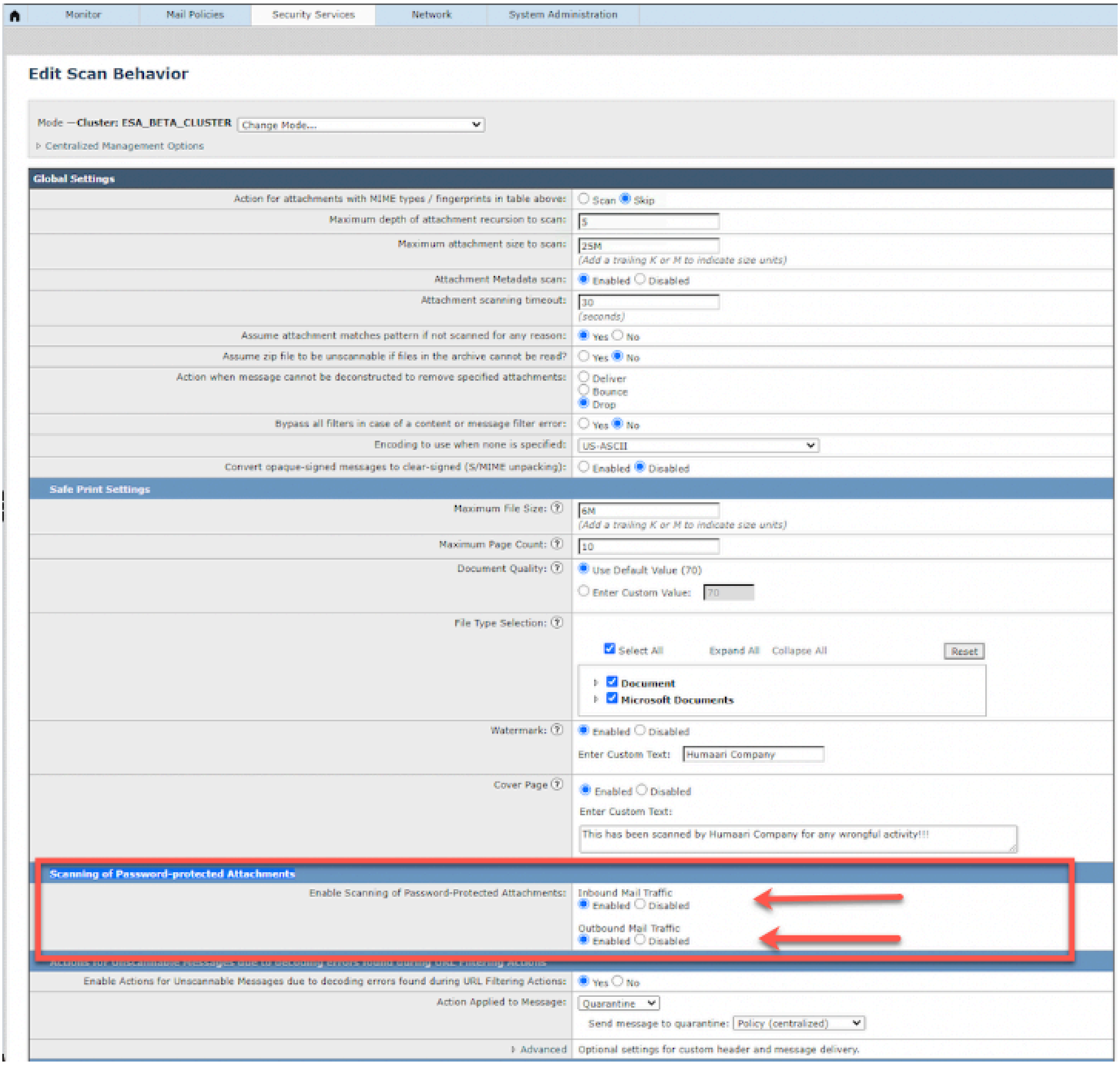
Password protected file attachments can be analyzed currently only if the password is present in the mail body. The passwords are case sensitive and do not recognize "space".

A list of up to 5 passwords provided by admin is now supported.

Configuration Steps

Graphical User Interface (GUI)

To configure PPFA from GUI, navigate to **Security Service** > **Scan Behavior** > **Edit Global Settings** > **Scanning of Password-protected Attachments** > choose to **Enable** for Inbound Mail traffic/Outbound Mail Traffic or Both >**Submit** >**Commit**



Edit Scan Behavior

Mode —**Cluster: ESA_BETA_CLUSTER** Change Mode...

Centralized Management Options

Global Settings	
Action for attachments with MIME types / fingerprints in table above:	○ Scan ● Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	25M (Add a trailing K or M to indicate size units)
Attachment Metadata scan:	● Enabled ○ Disabled
Attachment scanning timeout:	30 (seconds)
Assume attachment matches pattern if not scanned for any reason:	● Yes ○ No
Assume zip file to be unscannable if files in the archive cannot be read?	○ Yes ● No
Action when message cannot be deconstructed to remove specified attachments:	○ Deliver ○ Bounce ● Drop
Bypass all filters in case of a content or message filter error:	○ Yes ● No
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	○ Enabled ● Disabled
Safe Print Settings	
Maximum File Size: ?	6M (Add a trailing K or M to indicate size units)
Maximum Page Count: ?	10
Document Quality: ?	● Use Default Value (70) ○ Enter Custom Value: 70
File Type Selection: ?	☑ Select All Expand All Collapse All Reset ☑ **Document** ☑ **Microsoft Documents**
Watermark: ?	● Enabled ○ Disabled Enter Custom Text: Humaari Company
Cover Page ?	● Enabled ○ Disabled Enter Custom Text: This has been scanned by Humaari Company for any wrongful activity!!!
Scanning of Password-protected Attachments	
Enable Scanning of Password-Protected Attachments:	Inbound Mail Traffic ● Enabled ○ Disabled Outbound Mail Traffic ● Enabled ○ Disabled
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions	
Enable Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	● Yes ○ No
Action Applied to Message:	Quarantine Send message to quarantine: Policy (centralized)
Advanced	Optional settings for custom header and message delivery.

Command Line Interface (CLI)

To configure PPFA from CLI, run the command **scanconfig** > **PROTECTEDATTACHMENTCONFIG > Commit**

```
(ESA_CLI) (SERVICE)> scanconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode (Machine esa

What would you like to do?
1. Switch modes to edit at mode "Cluster ESA_BETA_CLUSTER".
2. Start a new, empty configuration at the current mode (Machine esa1.lab.cisco.com).
3. Copy settings from another cluster mode to the current mode (Machine esa1.lab.cisco.com).
[1]>


There are currently 5 attachment type mappings configured to be SKIPPED.

Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.
- CLUSTERSET - Set how scanconfig is configured in a cluster.
- CLUSTERSHOW - Display how scanconfig is configured in a cluster.
[]> PROTECTEDATTACHMENTCONFIG

Scanning of password-protected attachments for inbound mails: enabled.
Scanning of password-protected attachments for outbound mails: enabled.

Do you want to scan password-protected attachments for inbound mails? y/n [Y]>

Do you want to scan password-protected attachments for outbound mails? y/n [Y]>

Scan password protected attachments configuration unchanged.
```

> **Note**: By default 5 passwords in the emails body is scanned/extracted.

To increase the maximum number of passwords extracted from an email body, the hidden command "**scanconfig** > **password_list_size**" can be used in CLI. You can configure a maximum of 10 passwords.

> **Caution**: changing this settings to higher value could have performance impact.

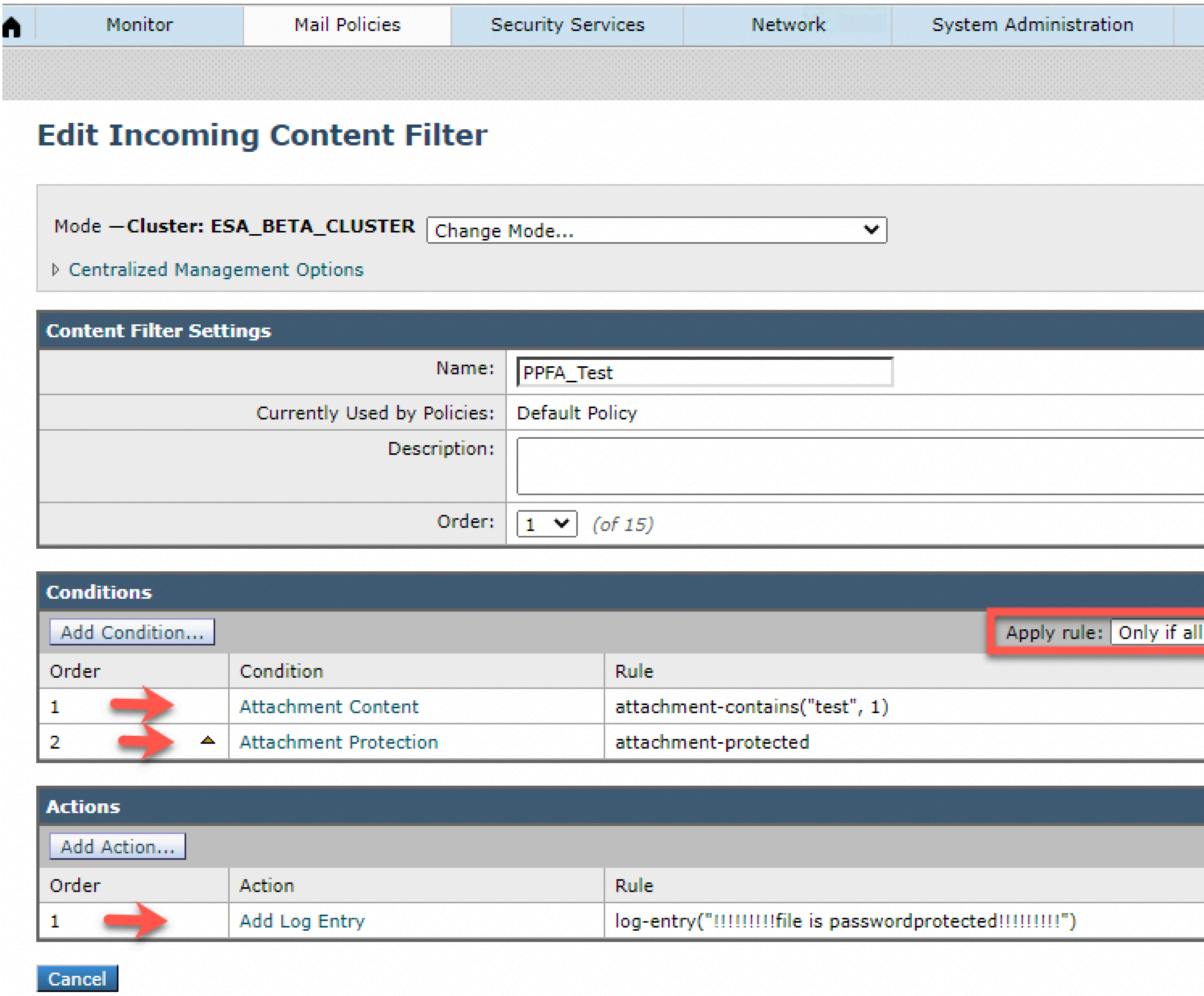
```
(ESA_CLI) (SERVICE)> scanconfig
There are currently 5 attachment type mappings configured to be SKIPPED.

Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
- SAFEPRINT - Configure safeprint settings.
- PROTECTEDATTACHMENTCONFIG - Scan password protected attachments.
- CLUSTERSET - Set how scanconfig is configured in a cluster.
- CLUSTERSHOW - Display how scanconfig is configured in a cluster.
[]> password_list_size

Enter maximum number of passwords to process:
[5]> 1000

Value must be an integer from 1 to 10.

Enter maximum number of passwords to process:
[5]> 10

Password list size is changed.
```

Troubleshoot and Verification

In this example, the content filter with conditions:

1. attachment content contains "**test**" and
2. if attachment is password protected

then action is log "**!!!!!file is passwordprotected!!!!!!!**"



Edit Incoming Content Filter

Mode —**Cluster: ESA_BETA_CLUSTER** Change Mode...

Centralized Management Options

Content Filter Settings

Name:	PPFA_Test
Currently Used by Policies:	Default Policy
Description:	
Order:	1 *(of 15)*

Conditions

Apply rule: Only if all

Order	Condition	Rule
1	Attachment Content	attachment-contains("test", 1)
2	Attachment Protection	attachment-protected

Actions

Order	Action	Rule
1	Add Log Entry	log-entry("!!!!!!!!!file is passwordprotected!!!!!!!!!")

Verification From CLI for Successful Process

a) In CLI from **mail_logs** you can see:

```
Wed Feb 24 12:11:59 2022 Info: Start MID 22178287 ICID 122555
Wed Feb 24 12:11:59 2022 Info: MID 22178287 ICID 122555 From: <test@lab.cisco.com>
Wed Feb 24 12:11:59 2022 Info: MID 22178287 ICID 122555 RID 0 To: <test@lab.cisco.com>
Wed Feb 24 12:11:59 2022 Info: MID 22178287 using engine: SPF Verdict Cache using cached verdict
Wed Feb 24 12:11:59 2022 Info: MID 22178287 SPF: helo identity postmaster@[10.0.201.16] None
Wed Feb 24 12:11:59 2022 Info: MID 22178287 using engine: SPF Verdict Cache using cached verdict
Wed Feb 24 12:11:59 2022 Info: MID 22178287 SPF: mailfrom identity test@lab.cisco.com Pass (v=spf1)
Wed Feb 24 12:11:59 2022 Info: MID 22178287 using engine: SPF Verdict Cache using cached verdict
Wed Feb 24 12:11:59 2022 Info: MID 22178287 SPF: pra identity test@lab.cisco.com None headers from
Wed Feb 24 12:11:59 2022 Info: MID 22178287 DMARC: Message from domain lab.cisco.com, DMARC pass (SPF al
Wed Feb 24 12:11:59 2022 Info: MID 22178287 DMARC: Verification passed
Wed Feb 24 12:11:59 2022 Info: MID 22178287 Message-ID '<4be194cc-4c95-9d15-6528-81a05dc56a66@lab.cisco.
Wed Feb 24 12:11:59 2022 Info: MID 22178287 Subject ppfa test with xls
Wed Feb 24 12:11:59 2022 Info: MID 22178287 SDR: Domains for which SDR is requested: reverse DNS host: N
Wed Feb 24 12:11:59 2022 Info: MID 22178287 SDR: Consolidated Sender Reputation: Tainted, Threat Catego
Wed Feb 24 12:11:59 2022 Info: MID 22178287 SDR: Tracker Header : 1+lIjVgkzfH9oTTP+SaBrzZC3Gs6TTYhJbW8D/
Wed Feb 24 12:11:59 2022 Info: MID 22178287 ready 22082 bytes from <test@lab.cisco.com>
Wed Feb 24 12:11:59 2022 Info: LDAP: Masquerade query LDAP.masquerade MID 22178287 address test@lab.cisc
Wed Feb 24 12:11:59 2022 Info: LDAP: Masquerade query LDAP.masquerade MID 22178287 address test@lab.cisc
Wed Feb 24 12:11:59 2022 Info: MID 22178287 attachment 'testfile.xlsx'
Wed Feb 24 12:12:01 2022 Info: MID 22178287 matched all recipients for per-recipient policy test1 in the
Wed Feb 24 12:12:04 2022 Info: MID 22178287 interim verdict using engine: CASE spam negative
Wed Feb 24 12:12:04 2022 Info: MID 22178287 using engine: CASE spam negative
Wed Feb 24 12:12:04 2022 Info: MID 22178287 interim AV verdict using McAfee ENCRYPTED
Wed Feb 24 12:12:04 2022 Info: MID 22178287 interim AV verdict using Sophos ENCRYPTED
Wed Feb 24 12:12:04 2022 Info: MID 22178287 antivirus encrypted
Wed Feb 24 12:12:04 2022 Info: MID 22178287 AMP file reputation verdict : UNKNOWN(File analysis pending)
Wed Feb 24 12:12:04 2022 Info: MID 22178287 SHA d1e67e9640c598162b891028d967d2e5621d0c1bc1141ef2cec21a0e
Wed Feb 24 12:12:04 2022 Info: MID 22178287 using engine: GRAYMAIL negative
Wed Feb 24 12:12:04 2022 Info: MID 22178287 Custom Log Entry: !!!!!!!!!file is passwordprotected!!!!!!!!
Wed Feb 24 12:12:04 2022 Info: MID 22178287 Unable to safe print the attachment, Filename: testfile.xlsx
Wed Feb 24 12:12:04 2022 Info: MID 22178287 rewritten to MID 22178289 by safeprint-all-attachments-strip
Wed Feb 24 12:12:04 2022 Info: Message finished MID 22178287 done
```

b) From **content_scanner** logs you can see if the file has been successfully extracted

```
Wed Feb 24 12:12:01 2022 Info: PF: MID 22178287 The password-protected file - "testfile.xlsx" is scanned
```

c) From **amp_logs**, You can see that the extracted file is now sent to Advanced Malware Protection (AMP) and File Analysis for analysis.

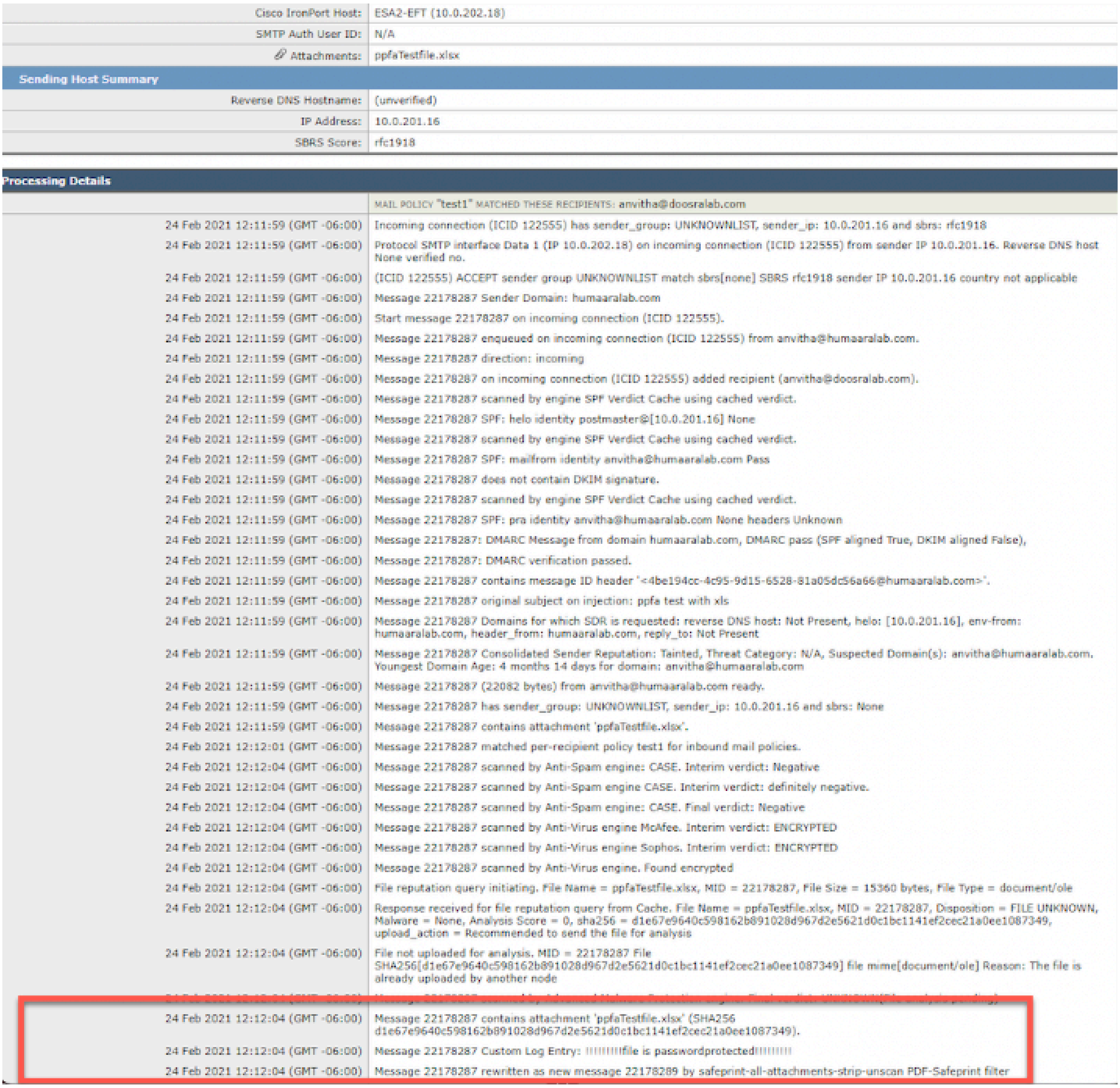
```
Tue Mar 16 11:21:03 2022 Info:   File reputation query initiating. File Name = 'testfile.zip', MID = 221
Tue Mar 16 11:21:03 2022 Info:   Response received for file reputation query from Cloud. File Name = 'te
mmended to send the file for analysis, verdict_source = None
Tue Mar 16 11:21:03 2022 Info:   Compressed/Archive File: sha256 = fb997bf3891f81edc3a4292c22d9fa7fbfc65
962427f8aa, Disposition = FILE UNKNOWN, Response received from = Cloud, Malware = None, Analysis Score =
Tue Mar 16 11:21:04 2022 Info:   File uploaded for preclassification. SHA256: f2d2638afb528c7476c9ee8e83
Tue Mar 16 11:21:31 2022 Info:   File uploaded for analysis. SHA256: f2d2638afb528c7476c9ee8e83ddb20e686
```

d) If the amp_logs are in Debug level, you can see more information related to password protected file:

```
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_supported_file_mime: Supported mime : application
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: _amp_unarchv_mem2file - in_buf=0x96682000, size=70637
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: password is Cisco
Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_context_create - ctext=0x96610ec0
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: archive size = 706376, max archive size=14127520
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: password is Cisco
Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_context_create - ctext=0x96610ec0
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: archive size = 706376, max archive size=14127520
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_make_dated_dir - path=/data/tmp/amp/2022_03_16
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: update_full_pathname entered - path=/data/tmp/amp/202
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: update_full_pathname - archive_entry_set_pathname, /d
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_queue_entry_insert - ctext=0x96610ec0, parent=0x0
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: _amp_unarchv_file2file - ctext=0x96610ec0, parent_qe=
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: Unsupported file type: application/x-dosexec
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: _amp_unarchv_mem2file - in_buf=0x97284000, size=10960
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: _amp_unarchv_mem2file - decode depth (0)
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: _amp_unarchv_file2file - archive cumulative size=1096
 Tue Mar 16 11:21:03 2022   AMPPyrex:-   AMP-INFO: set_analysis_params do_sandbox=0, do_analysis=0,file_
Tue Mar 16 11:21:03 2022   AMPPyrex:-   AMP-INFO: set_analysis_params do_sandbox=1, do_analysis=1,file_m
Tue Mar 16 11:21:03 2022 AMPCloudIF:-  AMP-DEBUG: AMP Query Request, FileType[0] SHA256[fb997bf3891f81ed

......

ue Mar 16 11:21:03 2022  CloudPool:-  AMP-DEBUG: cb in callback_thread
Tue Mar 16 11:21:03 2022 AMPCloudIF:-  AMP-DEBUG: AMP Query Response[Cloud], SHA256[fb997bf3891f81edc3a4
 Tue Mar 16 11:21:03 2022 CacheUtils:-  AMP-DEBUG: Found SHA256: - SHA256::fb997bf3891f81edc3a4292c22d9f
Tue Mar 16 11:21:03 2022  CloudPool:-  AMP-DEBUG: imcloud callback thread going to sleep
Tue Mar 16 11:21:03 2022 VRTCloudIF:-  AMP-DEBUG: Status List, Server Response HTTP code:[200]
Tue Mar 16 11:21:03 2022 CacheUtils:-  AMP-DEBUG: Found SHA256: - SHA256::f2d2638afb528c7476c9ee8e83ddb2
Tue Mar 16 11:21:03 2022 VRTCloudIF:-  AMP-DEBUG: File SHA256[f2d2638afb528c7476c9ee8e83ddb20e686b0b05f5
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_entry_preserve_file - ctext=0x96610ec0, pathname=
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_entry_preserve_file - preserved  pathname=/data/t
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_context_delete - ctext=0x96610ec0
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_queue_entry_free - entry=0x9666a2e0, pathname=/da
 Tue Mar 16 11:21:03 2022  Unarchive:-  AMP-DEBUG: amp_context_free - ctext=0x96610ec0
 Tue Mar 16 11:21:03 2022     AMPRPC:-   AMP-INFO: Adjusted verdict - {'file_type': 'application/zip', '
s': 1, 'analysis_score': 0, 'score': 0, 'sha256': 'fb997bf3891f81edc3a4292c22d9fa7fbfc652756eec5e9b7ffd4
ategory': 'amp', 'uploaded': True, 'original_verdict': 'FILE UNKNOWN', 'analysis_status': 4, 'verdict_nu
: None, 'upload_reason': None, 'sha256': 'f2d2638afb528c7476c9ee8e83ddb20e686b0b05f53f2f966fd9eb962427f8
Tue Mar 16 11:21:03 2022 VRTCloudIF:-  AMP-DEBUG: Set curl options URL[https://tg1-clean.lab.cisco.com/c
 Tue Mar 16 11:21:03 2022 VRTCloudIF:-  AMP-DEBUG: {"message":"Success","hash":"f2d2638afb528c7476c9ee8e
yzing":"unknown","sample":"d5c8d83543d92c0cc428d6377d1c665d","query":"https://tg1-clean.lab.cisco.com/cs
 Tue Mar 16 11:21:03 2022 VRTCloudIF:-  AMP-DEBUG:  File upload successful filename testfile.exe
 Tue Mar 16 11:21:03 2022 CacheUtils:-  AMP-DEBUG: Found SHA256: - SHA256::f2d2638afb528c7476c9ee8e83ddb
Tue Mar 16 11:21:03 2022 VRTCloudIF:-  AMP-DEBUG: File SHA256[f2d2638afb528c7476c9ee8e83ddb20e686b0b05f5
Tue Mar 16 11:21:03 2022   AMPPyrex:-   AMP-INFO: Upload SHA[f2d2638afb528c7476c9ee8e83ddb20e686b0b05f53
Tue Mar 16 11:21:17 2022   AMPPyrex:-  AMP-DEBUG: AMP Extraction monitoring thread entering into sleep.
```

Verification From GUI for Successful Process

Navigate to **Message Tracking** and filter the message ID.



Cisco IronPort Host:	ESA2-EFT (10.0.202.18)
SMTP Auth User ID:	N/A
Attachments:	ppfaTestfile.xlsx
Sending Host Summary	
Reverse DNS Hostname:	(unverified)
IP Address:	10.0.201.16
SBRS Score:	rfc1918

Processing Details

	MAIL POLICY "test1" MATCHED THESE RECIPIENTS: anvitha@doosralab.com
24 Feb 2021 12:11:59 (GMT -06:00)	Incoming connection (ICID 122555) has sender_group: UNKNOWNLIST, sender_ip: 10.0.201.16 and sbrs: rfc1918
24 Feb 2021 12:11:59 (GMT -06:00)	Protocol SMTP interface Data 1 (IP 10.0.202.18) on incoming connection (ICID 122555) from sender IP 10.0.201.16. Reverse DNS host None verified no.
24 Feb 2021 12:11:59 (GMT -06:00)	(ICID 122555) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS rfc1918 sender IP 10.0.201.16 country not applicable
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 Sender Domain: humaaralab.com
24 Feb 2021 12:11:59 (GMT -06:00)	Start message 22178287 on incoming connection (ICID 122555).
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 enqueued on incoming connection (ICID 122555) from anvitha@humaaralab.com.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 direction: incoming
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 on incoming connection (ICID 122555) added recipient (anvitha@doosralab.com).
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 scanned by engine SPF Verdict Cache using cached verdict.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 SPF: helo identity postmaster@[10.0.201.16] None
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 scanned by engine SPF Verdict Cache using cached verdict.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 SPF: mailfrom identity anvitha@humaaralab.com Pass
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 does not contain DKIM signature.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 scanned by engine SPF Verdict Cache using cached verdict.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 SPF: pra identity anvitha@humaaralab.com None headers Unknown
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287: DMARC Message from domain humaaralab.com, DMARC pass (SPF aligned True, DKIM aligned False),
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287: DMARC verification passed.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 contains message ID header '<4be194cc-4c95-9d15-6528-81a05dc56a66@humaaralab.com>'.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 original subject on injection: ppfa test with xls
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 Domains for which SDR is requested: reverse DNS host: Not Present, helo: [10.0.201.16], env-from: humaaralab.com, header_from: humaaralab.com, reply_to: Not Present
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 Consolidated Sender Reputation: Tainted, Threat Category: N/A, Suspected Domain(s): anvitha@humaaralab.com, Youngest Domain Age: 4 months 14 days for domain: anvitha@humaaralab.com
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 (22082 bytes) from anvitha@humaaralab.com ready.
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 has sender_group: UNKNOWNLIST, sender_ip: 10.0.201.16 and sbrs: None
24 Feb 2021 12:11:59 (GMT -06:00)	Message 22178287 contains attachment 'ppfaTestfile.xlsx'.
24 Feb 2021 12:12:01 (GMT -06:00)	Message 22178287 matched per-recipient policy test1 for inbound mail policies.
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 scanned by Anti-Spam engine: CASE. Final verdict: Negative
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 scanned by Anti-Virus engine McAfee. Interim verdict: ENCRYPTED
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 scanned by Anti-Virus engine Sophos. Interim verdict: ENCRYPTED
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 scanned by Anti-Virus engine. Found encrypted
24 Feb 2021 12:12:04 (GMT -06:00)	File reputation query initiating. File Name = ppfaTestfile.xlsx, MID = 22178287, File Size = 15360 bytes, File Type = document/ole
24 Feb 2021 12:12:04 (GMT -06:00)	Response received for file reputation query from Cache. File Name = ppfaTestfile.xlsx, MID = 22178287, Disposition = FILE UNKNOWN, Malware = None, Analysis Score = 0, sha256 = d1e67e9640c598162b891028d967d2e5621d0c1bc1141ef2cec21a0ee1087349, upload_action = Recommended to send the file for analysis
24 Feb 2021 12:12:04 (GMT -06:00)	File not uploaded for analysis. MID = 22178287 File SHA256[d1e67e9640c598162b891028d967d2e5621d0c1bc1141ef2cec21a0ee1087349] file mime[document/ole] Reason: The file is already uploaded by another node
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 scanned by Advanced Malware Protection engine. Final verdict: UNKNOWN(file analysis pending)
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 contains attachment 'ppfaTestfile.xlsx' (SHA256 d1e67e9640c598162b891028d967d2e5621d0c1bc1141ef2cec21a0ee1087349).
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 Custom Log Entry: !!!!!!!!!file is passwordprotected!!!!!!!!!
24 Feb 2021 12:12:04 (GMT -06:00)	Message 22178287 rewritten as new message 22178289 by safeprint-all-attachments-strip-unscan PDF-Safeprint filter

Verification From CLI for Failed Process

Condition: incorrect password or password not found.

a) From **mail_logs** in CLI

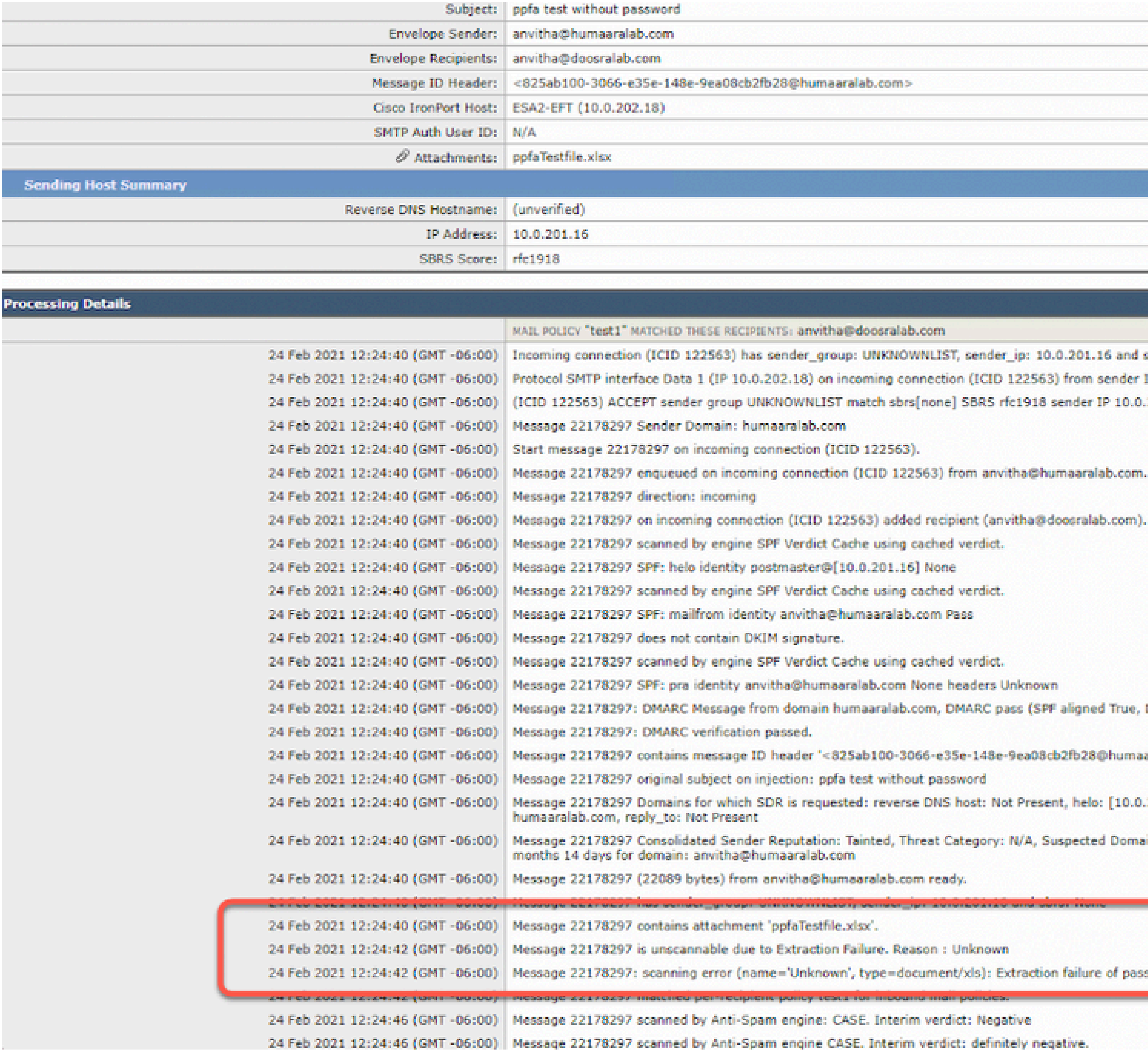
```
Wed Feb 24 12:24:40 2022 Info: MID 22178297 ICID 122563 From: <test@lab.cisco.com>
Wed Feb 24 12:24:40 2022 Info: MID 22178297 ICID 122563 RID 0 To: <test2@lab.cisco.com>
Wed Feb 24 12:24:40 2022 Info: MID 22178297 using engine: SPF Verdict Cache using cached verdict
Wed Feb 24 12:24:40 2022 Info: SPF Verdict Cache cache status: hits = 10, misses = 531, expires = 318, a
Wed Feb 24 12:24:40 2022 Info: MID 22178297 SPF: helo identity postmaster@[10.0.201.16] None
Wed Feb 24 12:24:40 2022 Info: MID 22178297 using engine: SPF Verdict Cache using cached verdict
Wed Feb 24 12:24:40 2022 Info: MID 22178297 SPF: mailfrom identity test@lab.cisco.com Pass (v=spf1)
Wed Feb 24 12:24:40 2022 Info: MID 22178297 using engine: SPF Verdict Cache using cached verdict
Wed Feb 24 12:24:40 2022 Info: MID 22178297 SPF: pra identity test@lab.cisco.com None headers from
Wed Feb 24 12:24:40 2022 Info: MID 22178297 DMARC: Message from domain lab.cisco.com, DMARC pass (SPF al
Wed Feb 24 12:24:40 2022 Info: MID 22178297 DMARC: Verification passed
Wed Feb 24 12:24:40 2022 Info: MID 22178297 Message-ID '<825ab100-3066-e35e-148e-9ea08cb2fb28@lab.cisco.
Wed Feb 24 12:24:40 2022 Info: MID 22178297 Subject ppfa test without password
Wed Feb 24 12:24:40 2022 Info: MID 22178297 SDR: Domains for which SDR is requested: reverse DNS host: N
Wed Feb 24 12:24:40 2022 Info: MID 22178297 SDR: Consolidated Sender Reputation: Tainted, Threat Categor
Wed Feb 24 12:24:40 2022 Info: MID 22178297 SDR: Tracker Header : jiOYjEFgtyhTbL9t0GE5obyJYv3d6lj/sYLgch
Wed Feb 24 12:24:40 2022 Info: MID 22178297 ready 22089 bytes from <test@lab.cisco.com>
Wed Feb 24 12:24:40 2022 Info: LDAP: Masquerade query LDAP.masquerade MID 22178297 address test@lab.cisc
Wed Feb 24 12:24:40 2022 Info: ICID 122563 close
Wed Feb 24 12:24:40 2022 Info: LDAP: Masquerade query LDAP.masquerade MID 22178297 address test@lab.cisc
Wed Feb 24 12:24:40 2022 Info: MID 22178297 attachment 'testfile.xlsx'
Wed Feb 24 12:24:42 2022 Info: MID 22178297 was marked unscannable due to extraction failures. Reason: T
Wed Feb 24 12:24:42 2022 Warning: MID 22178297: scanning error (name='testfile.xlsx', type=document/xls)
Wed Feb 24 12:24:42 2022 Info: MID 22178297 matched all recipients for per-recipient policy test1 in the
Wed Feb 24 12:24:46 2022 Info: MID 22178297 interim verdict using engine: CASE spam negative
Wed Feb 24 12:24:46 2022 Info: MID 22178297 using engine: CASE spam negative
Wed Feb 24 12:24:46 2022 Info: MID 22178297 interim AV verdict using McAfee ENCRYPTED
Wed Feb 24 12:24:46 2022 Info: MID 22178297 interim AV verdict using Sophos ENCRYPTED
Wed Feb 24 12:24:46 2022 Info: MID 22178297 antivirus encrypted
Wed Feb 24 12:24:46 2022 Info: MID 22178297 AMP file reputation verdict : UNKNOWN
Wed Feb 24 12:24:46 2022 Info: MID 22178297 using engine: GRAYMAIL negative
Wed Feb 24 12:24:46 2022 Info: MID 22178297 Unable to safe print the attachment, Filename: testfile.xlsx
Wed Feb 24 12:24:46 2022 Info: MID 22178297 rewritten to MID 22178298 by safeprint-all-attachments-strip
Wed Feb 24 12:24:46 2022 Info: Message finished MID 22178297 done
```

b) In **content_scanner** you can see:

```
Wed Feb 24 12:24:42 2022 Info: PF: MID 22178297 Failed to open document - 'testfile.xlsx' because it is
```

Verification From GUI for Failed Process

a) From GUI in **Message Tracking**, filter for Message ID



Subject:	ppfa test without password
Envelope Sender:	anvitha@humaaralab.com
Envelope Recipients:	anvitha@doosralab.com
Message ID Header:	<825ab100-3066-e35e-148e-9ea08cb2fb28@humaaralab.com>
Cisco IronPort Host:	ESA2-EFT (10.0.202.18)
SMTP Auth User ID:	N/A
Attachments:	ppfaTestfile.xlsx
Sending Host Summary	
Reverse DNS Hostname:	(unverified)
IP Address:	10.0.201.16
SBRS Score:	rfc1918

Processing Details

	MAIL POLICY "test1" MATCHED THESE RECIPIENTS: anvitha@doosralab.com
24 Feb 2021 12:24:40 (GMT -06:00)	Incoming connection (ICID 122563) has sender_group: UNKNOWNLIST, sender_ip: 10.0.201.16 and s
24 Feb 2021 12:24:40 (GMT -06:00)	Protocol SMTP interface Data 1 (IP 10.0.202.18) on incoming connection (ICID 122563) from sender I
24 Feb 2021 12:24:40 (GMT -06:00)	(ICID 122563) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS rfc1918 sender IP 10.0.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 Sender Domain: humaaralab.com
24 Feb 2021 12:24:40 (GMT -06:00)	Start message 22178297 on incoming connection (ICID 122563).
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 enqueued on incoming connection (ICID 122563) from anvitha@humaaralab.com.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 direction: incoming
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 on incoming connection (ICID 122563) added recipient (anvitha@doosralab.com).
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 scanned by engine SPF Verdict Cache using cached verdict.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 SPF: helo identity postmaster@[10.0.201.16] None
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 scanned by engine SPF Verdict Cache using cached verdict.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 SPF: mailfrom identity anvitha@humaaralab.com Pass
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 does not contain DKIM signature.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 scanned by engine SPF Verdict Cache using cached verdict.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 SPF: pra identity anvitha@humaaralab.com None headers Unknown
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297: DMARC Message from domain humaaralab.com, DMARC pass (SPF aligned True, I
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297: DMARC verification passed.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 contains message ID header '<825ab100-3066-e35e-148e-9ea08cb2fb28@humaa
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 original subject on injection: ppfa test without password
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 Domains for which SDR is requested: reverse DNS host: Not Present, helo: [10.0. humaaralab.com, reply_to: Not Present
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 Consolidated Sender Reputation: Tainted, Threat Category: N/A, Suspected Domai months 14 days for domain: anvitha@humaaralab.com
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 (22089 bytes) from anvitha@humaaralab.com ready.
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 has sender_group: UNKNOWNLIST, sender_ip: 10.0.201.16 and sbrs: None
24 Feb 2021 12:24:40 (GMT -06:00)	Message 22178297 contains attachment 'ppfaTestfile.xlsx'.
24 Feb 2021 12:24:42 (GMT -06:00)	Message 22178297 is unscannable due to Extraction Failure. Reason : Unknown
24 Feb 2021 12:24:42 (GMT -06:00)	Message 22178297: scanning error (name='Unknown', type=document/xls): Extraction failure of pass
24 Feb 2021 12:24:42 (GMT -06:00)	Message 22178297 matched per-recipient policy test1 for inbound mail policies.
24 Feb 2021 12:24:46 (GMT -06:00)	Message 22178297 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
24 Feb 2021 12:24:46 (GMT -06:00)	Message 22178297 scanned by Anti-Spam engine CASE. Interim verdict: definitely negative.

Nested password protected files

Nested password protected files cannot be extracted. Currently this is not supported.

You can see this error in mail_logs

```
Sun Nov 22 21:09:31 2022 Info: MID 19597596 attachment 'testfile.zip'
Sun Nov 22 21:09:31 2022 Info: ICID 465893 close
Sun Nov 22 21:09:41 2022 Info: MID 19597596 was marked unscannable due to extraction failures. Reason: T
```

View Status

Use "**ppfastats**" command in CLI to view the summary of the messages that had password protected attachments and were scanned by ESA.

> **Note**: **ppfastats** is a hidden command.

```
(Machine esa1.lab.cisco.com)> ppfastats

Incoming PPFA Statistics:
Total number of Password Protected Attachments : 425
Total number of Sucessfully scanned Password Protected Attachments : 386
Total number of Protected PDF Attachments : 136
Total number of Sucessfully scanned PDF Attachments : 136
Total number of Protected Office Attachments (XLS, PPT, DOC) : 36
Total number of Sucessfully scanned Office Attachments : 36
Total number of Protected Archive Attachments : 253
Total number of Sucessfully scanned Archive Attachments (ZIP) : 214

Outgoing PPFA Statistics:
PPFA Statistics data not available for Outgoing Mails.
```

Related Information

- User Guide for AsyncOS 14.3 for Cisco Secure Email Cloud Gateway - Cisco