

Fortinet

FCP_FML_AD-7.4

FCP - FortiMail 7.4 Administrator

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/fcp-fml-ad-7-4>

Latest Version: 6.0

Question: 1

Refer to the exhibit.

DLP Scan Rule 1

Message Scan Rule

Name: DLPOut
Comment:

Scan Rule **Conditions** Exceptions

Match all conditions **Match any condition**

+ New... Edit... Delete Total 3

ID ...	Condition
1	Body contains sensitive data "Credit_Card_Number"
2	Attachment contains sensitive data "Credit_Card_Number"
3	Subject contains Credit Card

DLP Scan Rule 2

Message Scan Rule

Name: DLPOut
Comment:

Scan Rule **Conditions** **Exceptions**

+ New... Edit... Delete Total 1

ID ...	Condition
1	Sender contains sales@example.com

Refer to the exhibits, which shows a DLP scan profile configuration (DLP Scan Rule 1 and DLP Scan Rule 2)

from a FortiMail device.

Which two message types will trigger this DLP scan rule? (Choose two.)

- A. An email that contains credit card numbers in the body, attachment, and subject will trigger this scan rule.
- B. An email sent from sales@internal.lac will trigger this scan rule, even without matching any conditions.
- C. An email message that contains credit card numbers in the body will trigger this scan rule.
- D. An email message with a subject that contains the term 'credit card' will trigger this scan rule.

Answer: C, D

Question: 2

Refer to the exhibit, which displays a history log entry.



The screenshot shows a web interface for FortiMail history logs. At the top, there are tabs for 'History', 'System Event', 'Mail Event', 'AntiVirus', 'AntiSpam', 'Encryption', and 'Log Search Task'. Below the tabs are navigation controls: 'List', 'View', 'Search', and 'Export'. A date range filter is set to '2024-04-09 10:21:39 -> Current'. Below this, there are pagination controls showing '1 / 1' records and 'Records per page: 100'. The main table has the following columns: #, Date, Time, Classifier, Disposition, From, Header From, To, Subject, and Policy ID. The first row shows a record with ID 1, dated 2024-04-10 at 09:54:35.287, classified as 'Not Spam', with a disposition of 'Accept', from 'extuser@exte...', to 'user1@intern...', and a subject of 'Meeting minutes 20-Apr-24'. The Policy ID is '0:1:0:SYSTEM'.

#	Date	Time	Classifier	Disposition ...	From	Header From ...	To	Subject	Policy ID
1	2024-04-10	09:54:35.287	Not Spam	Accept	extuser@exte...	extuser@exte...	user1@intern...	Meeting minutes 20-Apr-24	0:1:0:SYSTEM

In the Policy ID column, why is the last policy ID value SYSTEM?

- A. The email was dropped by a system blacklist.
- B. The email matched a system-level authentication policy.
- C. It is an inbound email.
- D. The email did not match a recipient-based policy.

Answer: D

Question: 3

Refer to the exhibit, which shows the Authentication Reputation list on a FortiMail device running in gateway mode.

Sender Reputation		Authentication Reputation		
<input type="button" value="Delete"/> <input type="button" value="Add to Exempt List"/> <input type="button" value="View Blocked History"/>				
<input type="button" value="Refresh"/> <input type="button" value="Previous"/> <input type="text" value="1"/> / <input type="text" value="1"/> <input type="button" value="Next"/> <input type="button" value="More"/> Records per page: <input type="text" value="50"/>				
IP	Location	Violation	Access	Expiry Time
10.0.1.254	ZZ (Reserved)	Mail	CLI, Mail, Web	5 minutes

Why was the IP address blocked?

- A. The IP address had consecutive SMTPS login failures to FortiMail..
- B. The IP address had consecutive IMAP login failures to FortiMail.
- C. The IP address had consecutive administrative password failures to FortiMail.
- D. The IP address had consecutive SSH login failures to FortiMail.

Answer: A

Question: 4

Which three configuration steps must you set to enable DKIM signing for outbound messages on FortiMail? (Choose three.)

- A. Generate a public/private key pair in the protected domain configuration.
- B. Enable the DKIM checker in a matching session profile.
- C. Publish the public key as a TXT record in a public DNS server.
- D. Enable the DKIM checker in a matching antispam profile.
- E. Enable DKIM signing for outgoing messages in a matching session profile.

Answer: A, C, E

Question: 5

Exhibit.

Email Archiving Policy

Email Archiving Policy

Status

Account journal + ✕

Policy type Recipient

Pattern marketing@example.com

Comment

Create Cancel

Email Archiving Exempt Policy

Email Archiving Exempt Policy

Status

Account journal + ✕

Policy type Spam Email

Pattern

Comment

Create Cancel

Refer to the exhibits, which show an email archiving configuration (Email Archiving 1 and Email Archiving 2) from a FortiMail device.

What two archiving actions will FortiMail take when email messages match these archive policies? (Choose two.)

- A. FortiMail will save archived email in the journal account.
- B. FortiMail will archive email sent from marketingexample. com.
- C. FortiMail will exempt spam email from archiving.
- D. FortiMail will allow only the marketingexample.com account to access the archived email.

Answer: A, C

Thank You for Trying Our Product
Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>