

# Certification FCP\_FML\_AD-7.4 Sample Questions | FCP\_FML\_AD-7.4 Knowledge Points



P.S. Free 2026 Fortinet FCP\_FML\_AD-7.4 dumps are available on Google Drive shared by PDFBraindumps: <https://drive.google.com/open?id=1kO3nrPflU1MnwAjjf9rtuShq2Vtvy9Yk>

All these three Fortinet FCP\_FML\_AD-7.4 exam questions formats contain the real Fortinet FCP\_FML\_AD-7.4 exam questions and are very easy to install and use. Just choose the best Fortinet FCP\_FML\_AD-7.4 Exam Questions format that suits your budget and FCP\_FML\_AD-7.4 exam preparation requirement and starts preparing today.

We truly treat our customers with the best quality service and the most comprehensive FCP\_FML\_AD-7.4 exam pdf, that's why we enjoy great popularity among most IT workers. When you want to learn something about the FCP\_FML\_AD-7.4 Online Training, our customer assisting will be available for you. We will offer you the best preparation materials regarding FCP\_FML\_AD-7.4 practice exam. You can totally trust our dumps and service.

>> Certification FCP\_FML\_AD-7.4 Sample Questions <<

## FCP\_FML\_AD-7.4 Knowledge Points, Valid Dumps FCP\_FML\_AD-7.4 Free

Not every company can make such a promise of "no help, full refund" as our PDFBraindumps. However, the FCP\_FML\_AD-7.4 exam is not easy to pass, but our PDFBraindumps have confidence with their team. Our PDFBraindumps's study of FCP\_FML\_AD-7.4 exam make our FCP\_FML\_AD-7.4 Exam software effectively guaranteed. You can download our free demo first to try out, no matter which stage you are now in your exam review, our products can help you better prepare for FCP\_FML\_AD-7.4 exam.

### Fortinet FCP\_FML\_AD-7.4 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> <li><b>Email Flow and Authentication:</b> This section of the exam measures skills of a Messaging Security Engineer and focuses on configuring FortiMail to handle email flow securely. It includes enabling and matching authentication protocols, setting up secure MTA features, and implementing access control, IP policies, and recipient-based policies to control mail delivery and security.</li> </ul>
Topic 2	<ul style="list-style-type: none"> <li><b>Encryption:</b> This section of the exam measures skills of a Messaging Security Engineer and addresses the implementation of encryption methods in FortiMail. It covers traditional SMTP encryption and identity-based encryption (IBE). Candidates are expected to configure these technologies and manage IBE users for secure email communication.</li> </ul>

Topic 3	<ul style="list-style-type: none"> <li>• <b>Server Mode and Transparent Mode:</b> This section of the exam measures skills of a Network Security Administrator and explains how to deploy and manage FortiMail in different operation modes. It includes configuring server mode to handle mail directly and deploying FortiMail in transparent mode where it acts as a gateway to filter email traffic without altering the existing mail infrastructure.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• <b>Initial Deployment and Basic Configuration:</b> This section of the exam measures skills of a Network Security Administrator and covers the foundational setup of FortiMail. It includes understanding SMTP and email flow, performing initial configurations such as selecting operation mode, system settings, and defining protected domains. It also involves deploying FortiMail in high-availability clusters to ensure service continuity.</li> </ul>
Topic 5	<ul style="list-style-type: none"> <li>• <b>Email Security:</b> This section of the exam measures skills of a Network Security Administrator and deals with implementing security controls to filter and manage email threats. Candidates must configure session-based filtering, spam detection methods, malware protection, APT mitigation, and content filtering. The section also includes email archiving configurations for compliance and storage.</li> </ul>

## Fortinet FCP - FortiMail 7.4 Administrator Sample Questions (Q52-Q57):

### NEW QUESTION # 52

Refer to the exhibits, showing SMTP limits (Session Profile -- SMTP Limits), and domain settings (Domain Settings, and Domain Settings -- Other) of a FortiMail device.

### Session Profile—SMTP Limits

**Session Profile**

Profile name

Comment

**SMTP Limits**

Restrict number of EHLO/HELOs per session to	<input type="text" value="3"/>
Restrict number of email per session to	<input type="text" value="10"/>
Restrict number of recipients per email to	<input type="text" value="500"/>
Cap message size (KB) at	<input type="text" value="51200"/>
Cap header size (KB) at	<input type="text" value="10240"/>
Maximum number of NOOPs allowed for each connection	<input type="text" value="10"/>
Maximum number of RSETs allowed for each connection	<input type="text" value="20"/>

## Domain Settings

### FortiMail

Domain name

Relay type

SMTP server  Port  [\[Test...\]](#)

Use SMTPS

Fallback SMTP server  Port  [\[Test...\]](#)

Use SMTPS

Relay Authentication

### Domain Settings—Other

Other

Webmail theme

Webmail language

Maximum message size (KB)

SMTP greeting (EHLO/HELO) name (as client)

IP pool  Direction

Remove received header of outgoing email

Use global bayesian database

Bypass bounce verification

Email continuity

Which message size limit in KB will the FortiMail apply to outbound email?

- A. 0
- **B. 1**
- C. 2
- D. There is no message size limit for outbound email from a protected domain.

Answer: B

### NEW QUESTION # 53

Which two features are available when you enable HA centralized monitoring on FortiMail?  
(Choose two.)

- **A. Cross-device log searches across all cluster members from the primary device.**
- **B. Policy configuration changes of all cluster members from the primary device.**

- C. Firmware update of all cluster members from the primary device
- D. Mail statistics of all cluster members on the primary device.

Answer: A,D

#### NEW QUESTION # 54

Refer to the exhibit. What does the Scan timeout value configure?

The screenshot shows the 'FortiSandbox Inspection' configuration page. The 'FortiSandbox type' is set to 'Cloud'. The 'Region' is 'Global'. The 'Notification email' is 'user1@example.com'. The 'Statistics interval' is 5 minutes. The 'Scan timeout' is 30 minutes. The 'Scan result expires in' is 60 minutes.

- A. How often FortiMail will query FortiSandbox for a scan result
- B. How often the local scan results cache will expire on FortiMail
- C. How long FortiMail will wait to send a file or URI to FortiSandbox
- D. How long FortiMail will wait for a scan result from FortiSandbox

Answer: D

Explanation:

The Scan timeout setting specifies how long FortiMail will wait for FortiSandbox to return a verdict before treating the analysis as timed-out.

#### NEW QUESTION # 55

What are two benefits of having authentication reputation tracking enabled on FortiMail? (Choose two.)

- A. Enforces SMTP authentication
- B. Temporarily locks out an attacker
- C. Detects spoofed SMTP header addresses
- D. Tracks offending IP addresses attempting brute force attacks

Answer: B,D

Explanation:

Authentication reputation tracking monitors repeated authentication failures and can track malicious IPs and temporarily block attackers.

#### NEW QUESTION # 56

In which two places can the maximum email size be overridden on FortiMail? (Choose two.)

- A. Protected Domain configuration
- B. IP Policy configuration
- C. Resource Profile configuration
- D. Session Profile configuration

Answer: A,C

#### NEW QUESTION # 57

