



**Vendor:** Fortinet

**Exam Code:** FCP\_FCT\_AD-7.2

**Exam Name:** FCP - FortiClient EMS 7.2 Administrator

**Version:** DEMO

### QUESTION 1

An administrator needs to connect FortiClient EMS as a fabric connector to FortiGate. What is the prerequisite to get FortiClient EMS to connect to FortiGate successfully?

- A. Import and verify the FortiClient EMS tool CA certificate on FortiGate.
- B. Revoke and update the FortiClient client certificate on EMS.
- C. Import and verify the FortiClient client certificate on FortiGate.
- D. Revoke and update the FortiClient EMS root CA.

**Answer: A**

**Explanation:**

Connecting FortiClient EMS to FortiGate:

The administrator needs to establish a connection between FortiClient EMS and FortiGate as a fabric connector.

Prerequisites for Connection:

A key prerequisite is the import and verification of the FortiClient EMS tool CA certificate on FortiGate to ensure a trusted connection.

Conclusion:

The correct prerequisite for a successful connection is to import and verify the FortiClient EMS tool CA certificate on FortiGate.

### QUESTION 2

An administrator must add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection.

Which solution can provide secure access between FortiClient EMS and the Active Directory server?

- A. Configure and deploy a FortiGate device between FortiClient EMS and the Active Directory server.
- B. Configure Active Directory and install FortiClient EMS on the same VM.
- C. Configure a slave FortiClient EMS on a virtual machine.
- D. Configure an Active Directory connector between FortiClient EMS and the Active Directory server.

**Answer: A**

**Explanation:**

Requirement:

The administrator needs to add an authentication server on FortiClient EMS in a different security zone that cannot allow a direct connection.

Solution Analysis:

The goal is to securely connect FortiClient EMS and the Active Directory server despite being in different security zones.

Evaluating Options:

Installing FortiClient EMS on the same VM as Active Directory (option B) is not practical due to security zone separation.

Configuring a slave FortiClient EMS on a virtual machine (option C) does not address the need for secure communication.

Configuring an Active Directory connector (option D) may not be sufficient without secure routing.

Conclusion:

Deploying a FortiGate device between FortiClient EMS and the Active Directory server ensures secure and controlled access between the two zones.

### QUESTION 3

What does FortiClient do as a fabric agent? (Choose two.)

- A. Provides IOC verdicts
- B. Creates dynamic policies
- C. Provides application inventory
- D. Automates Responses

**Answer:** CD

### QUESTION 4

Based on the FortiClient logs shown in the exhibit, which endpoint profile policy is currently applied to the FortiClient endpoint from the EMS server?

Log - Policy

```

1:40:39 PM Information Vulnerability id=96521 msg="A vulnerability scan result has been logged" status=N/A vulncat="Operating
1:40:39 PM Information Vulnerability id=96520 msg="The vulnerability scan status has changed" status="scanning finished" vulnc
1:41:38 PM Information ESNAC id=96958 user=Admin msg="User social media information" social_srvcs=os social_user=Admin
2:12:22 PM Information Config id=96882 msg="Policy 'Default' was received and applied"
2:13:27 PM Information ESNAC id=96958 user=Admin msg="User social media information" social_srvcs=os social_user=Admin
2:14:32 PM Information ESNAC id=96959 emshostname=WIN-EHVKB3571 msg="Endpoint has AV whitelist engine version 6.00134 and si
2:14:54 PM Information Config id=96882 msg="Policy 'Default' was received and applied"
2:16:01 PM Information ESNAC id=96958 user=Admin msg="User social media information" social_srvcs=os social_user=Admin
2:20:19 PM Information Config id=96883 msg="Compliance rules 'default' were received and applied"
2:20:23 PM Debug ESNAC PIPEMSG_CMD_ESNAC_STATUS_RELOAD_CONFIG
2:20:23 PM Debug ESNAC cb828898d1ae56916f84cc7909alebla
2:20:23 PM Debug ESNAC Before Reload Config
2:20:23 PM Debug ESNAC ReloadConfig
2:20:23 PM Debug Scheduler stop_task() called
2:20:23 PM Debug Scheduler GUI change event
2:20:23 PM Debug Scheduler stop_task() called
2:20:23 PM Information Config id=96882 msg="Policy 'Fortinet-Training' was received and applied"
2:20:23 PM Debug Config 'scan on registration' is disabled - delete 'on registration' vulnerability scan.
2:20:23 PM Debug Config ImportConfig: tag <\forticlient_configuration\antiexploit\exclusion_applications> value is empty.
    
```

- A. Fortinet-Training
- B. Default configuration policy
- C. Compliance rules default
- D. Default

**Answer:** A

**Explanation:**

Observation of Logs:

The logs show a policy named "Fortinet-Training" being applied to the endpoint.

Evaluating Policies:

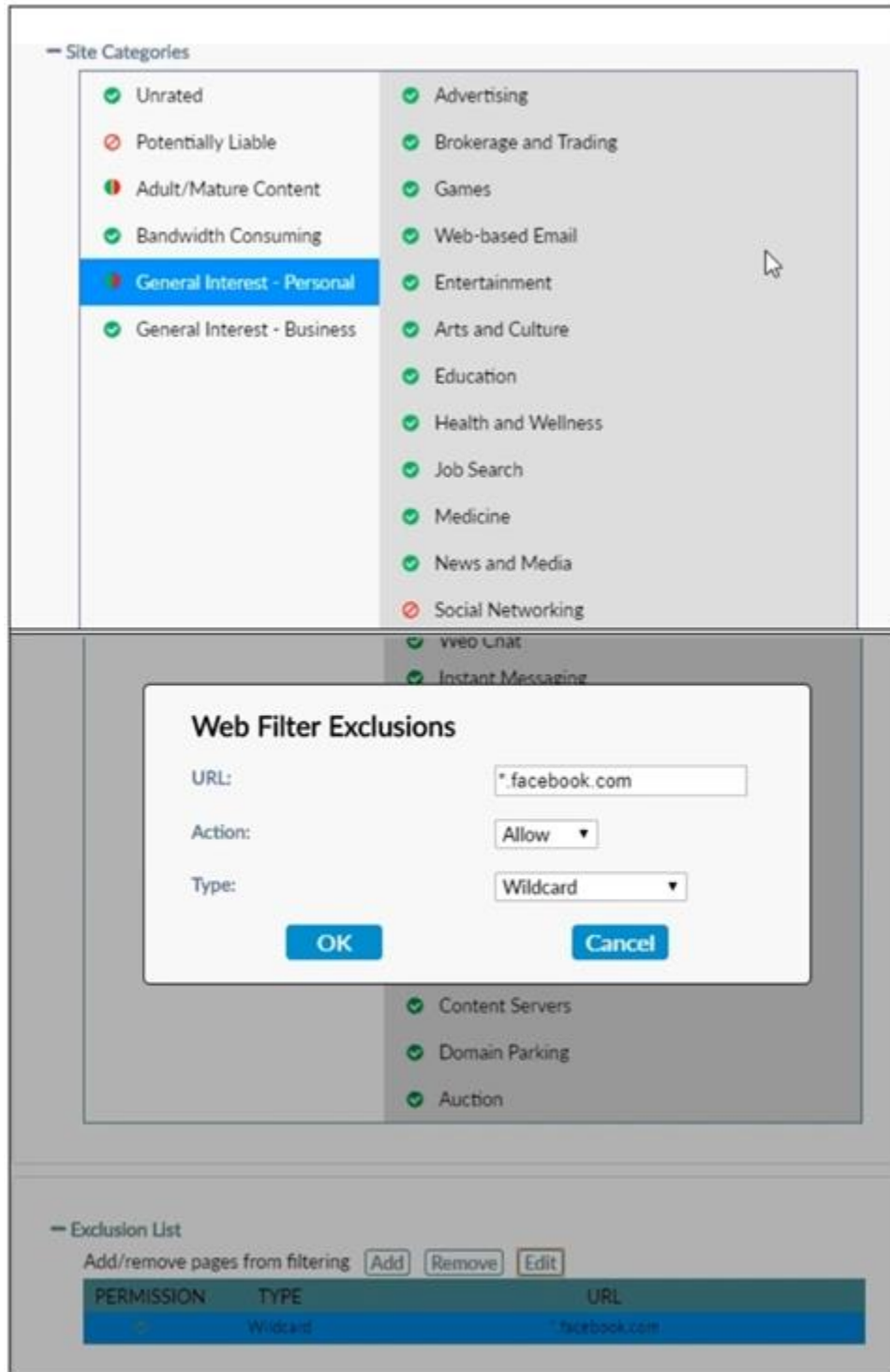
The log entries indicate that the "Fortinet-Training" policy was received and applied.

Conclusion:

Based on the logs, the currently applied policy on the FortiClient endpoint is "Fortinet-Training".

### QUESTION 5

Refer to the exhibit. Based on the settings shown in the exhibit, which action will FortiClient take when users try to access www.facebook.com?



- A. FortiClient will allow access to Facebook.
- B. FortiClient will block access to Facebook and its subdomains.
- C. FortiClient will monitor only the user's web access to the Facebook website
- D. FortiClient will prompt a warning message to want the user before they can access the Facebook website

**Answer:** A

**Explanation:**

Observation of Web Filter Exclusions:

The exhibit shows a web filter exclusion for "\*.facebook.com" with the action set to "Allow."

Evaluating Actions:

This configuration means that FortiClient will allow access to Facebook and its subdomains.

Conclusion:

When users try to access "www.facebook.com," FortiClient will allow the access based on the web filter exclusion settings.

**QUESTION 6**

Why does FortiGate need the root CA certificate of FortiClient EMS?

- A. To revoke FortiClient client certificates
- B. To sign FortiClient CSR requests
- C. To update FortiClient client certificates
- D. To trust certificates issued by FortiClient EMS

**Answer:** D

**Explanation:**

Understanding the Need for Root CA Certificate:

The root CA certificate of FortiClient EMS is necessary for FortiGate to trust certificates issued by FortiClient EMS.

Evaluating Use Cases:

FortiGate needs the root CA certificate to establish trust and validate certificates issued by FortiClient EMS.

Conclusion:

The primary reason FortiGate needs the root CA certificate of FortiClient EMS is to trust certificates issued by FortiClient EMS.

**QUESTION 7**

Which three features does FortiClient endpoint security include? (Choose three.)

- A. DLP
- B. Vulnerability management
- C. L2TP
- D. IPsec
- E. Real-time protection

**Answer:** BDE

**Explanation:**

Understanding FortiClient Features:

FortiClient endpoint security includes several features aimed at protecting and managing endpoints.

Evaluating Feature Set:

Vulnerability management is a key feature of FortiClient, helping to identify and address vulnerabilities (B).

IPsec is supported for secure VPN connections (D).

Real-time protection is crucial for detecting and preventing threats in real-time (E).

Eliminating Incorrect Options:

Data Loss Prevention (DLP) (A) is typically managed by FortiGate or FortiMail.

L2TP (C) is a protocol used for VPNs but is not specifically a feature of FortiClient endpoint security.

### QUESTION 8

Which component or device defines ZTNA tag information in the Security Fabric integration?

- A. FortiClient
- B. FortiGate
- C. FortiClient EMS
- D. FortiGate Access Proxy

**Answer: C**

**Explanation:**

Understanding ZTNA:

Zero Trust Network Access (ZTNA) requires defining tags for identifying and managing endpoint access.

Evaluating Components:

FortiClient EMS is responsible for managing and defining ZTNA tag information within the Security Fabric.

Conclusion:

The correct component that defines ZTNA tag information in the Security Fabric integration is FortiClient EMS.

## Thank You for Trying Our Product

### Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**