

# Fortinet

## Exam Questions FCP\_FCT\_AD-7.4

FCP - FortiClient EMS 7.4 Administrator



### NEW QUESTION 1

An administrator wants to simplify remote access without asking users to provide user credentials Which access control method provides this solution?

- A. ZTNA full mode
- B. SSL VPN
- C. L2TP
- D. ZTNA IP/MAC littering mode

**Answer: A**

### NEW QUESTION 2

Refer to the exhibit.



Based on The settings shown in The exhibit, which statement about FortiClient behaviour is Hue?

- A. FortiClient scans infected files when the user copies files to the Resources folder.
- B. FortiClient quarantines infected ties and reviews later, after scanning them.
- C. FortiClient copies infected files to the Resources folder without scanning them.
- D. FortiClient blocks and deletes infected files after scanning them.

**Answer: A**

### NEW QUESTION 3

When multitenancy is enabled on FortiClient EMS, which administrator role can provide access to the global site only? (Choose one answer)

- A. Tenant administrator
- B. Settings administrator
- C. Standard administrator
- D. Global administrator

**Answer: B**

NEW QUESTION 4

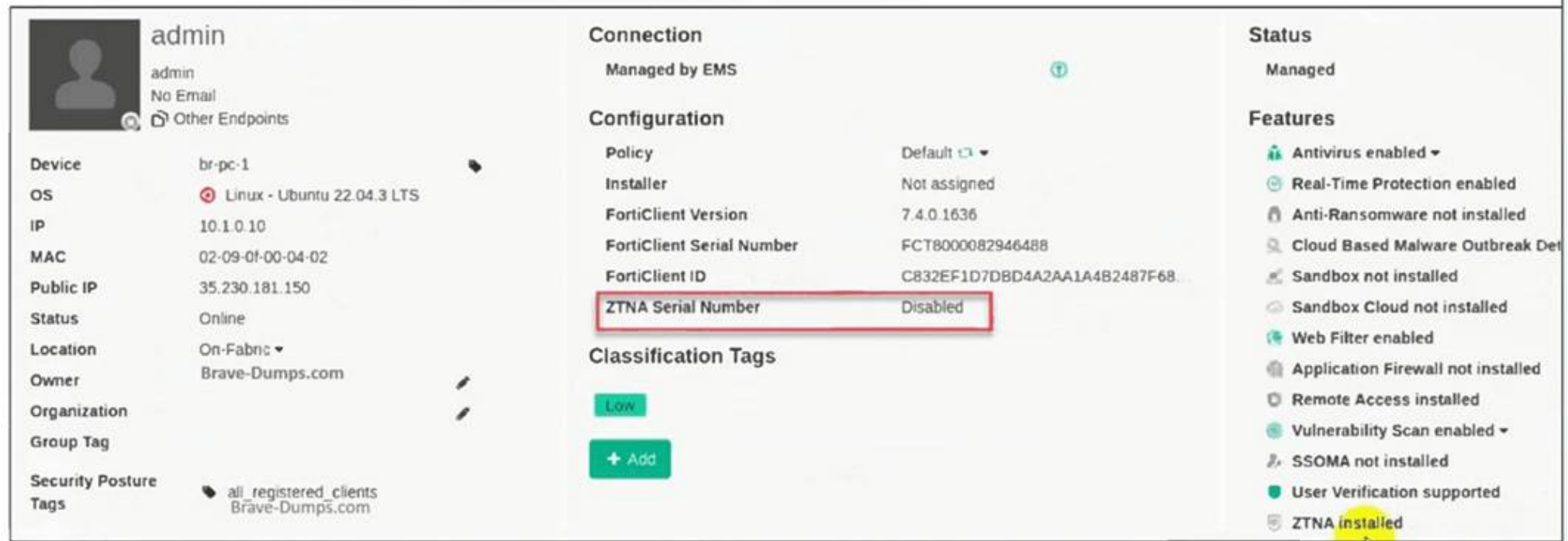
A FortiClient EMS administrator has enabled the compliance rule for the sales department Which Fortinet device will enforce compliance with dynamic access control?

A. FortiClient  
B. FortiClient EMS  
C. FortiGate  
D. FortiAnalyzer

Answer: C

NEW QUESTION 5

Refer to the exhibit.  
All Endpoints



The screenshot shows the FortiClient EMS interface for an endpoint named 'br-pc-1'. The 'Configuration' section shows 'ZTNA Serial Number' as 'Disabled'. The 'Features' section on the right shows 'ZTNA installed' as enabled (highlighted in yellow).

The zero trust network access (ZTNA) serial number on endpoint br-pc-1 is in a disabled state.  
What is causing the problem? (Choose one answer)

- A. The ZTNA feature is not installed on FortiClient.  
B. The ZTNA destinations endpoint profile is disabled.  
C. The ZTNA is disabled due to FortiClient disconnected from FortiClient EMS.  
D. The ZTNA certificate has been revoked by administrator.

Answer: B

NEW QUESTION 6

FortiClient EMS endpoint policies

| Endpoint Policies                                |                                       |                                                            |                                                               |                     |          |         |  |  |  |
|--------------------------------------------------|---------------------------------------|------------------------------------------------------------|---------------------------------------------------------------|---------------------|----------|---------|--|--|--|
| + Add Change Priority Refresh Clear Filters Edit |                                       |                                                            |                                                               |                     |          |         |  |  |  |
| Name                                             | Assigned Groups                       | Profile Components                                         | Policy Components                                             | Endpoint Count      | Priority | Enabled |  |  |  |
| Sales                                            | All Groups<br>trainingAD training.lab | VPN Training<br>WEB Training<br>MW Training<br>FW Training | ZTNA Training<br>VULN Training<br>SB Training<br>SYS Training | ON-FABRIC On-Fabric | 1        |         |  |  |  |
| Training                                         | trainingAD training.lab               | VPN Training<br>WEB Training<br>MW Training<br>FW Training | ZTNA Training<br>VULN Training<br>SB Training<br>SYS Training | ON-FABRIC On-Fabric | 1        | 2       |  |  |  |
| Default                                          |                                       | VPN Default<br>WEB Default<br>MW Default<br>FW Default     | ZTNA Default<br>VULN Default<br>SB Default<br>SYS Default     |                     | 1        | 3       |  |  |  |

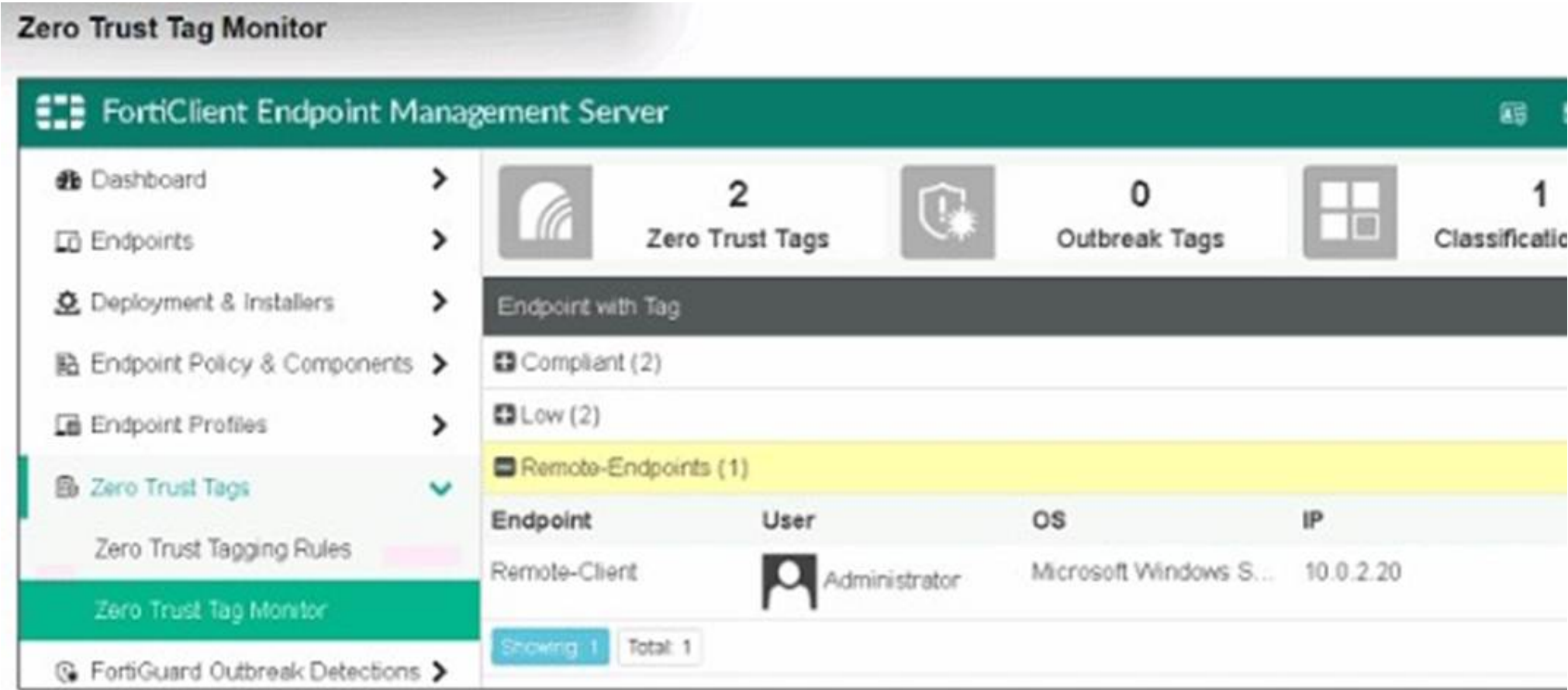
Refer to the exhibit, which shows multiple endpoint policies on FortiClient EMS. Which policy is applied to the endpoint in the AD group trainingAD

- A. The Training policy  
B. Both the Sales and Training policies because their priority is higher than the Default policy  
C. The Default policy because it has the highest priority  
D. The sales policy

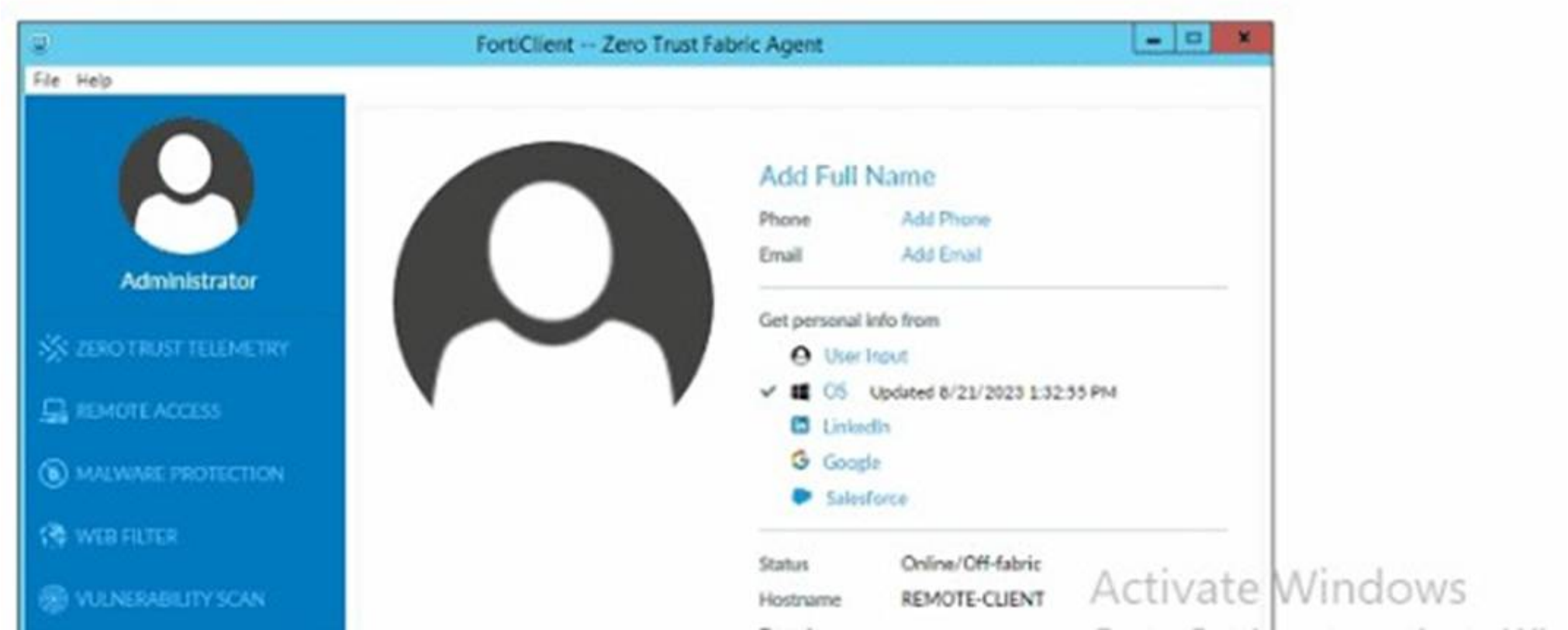
Answer: A

NEW QUESTION 7

Exhibit.



FortiClient Status - GUI



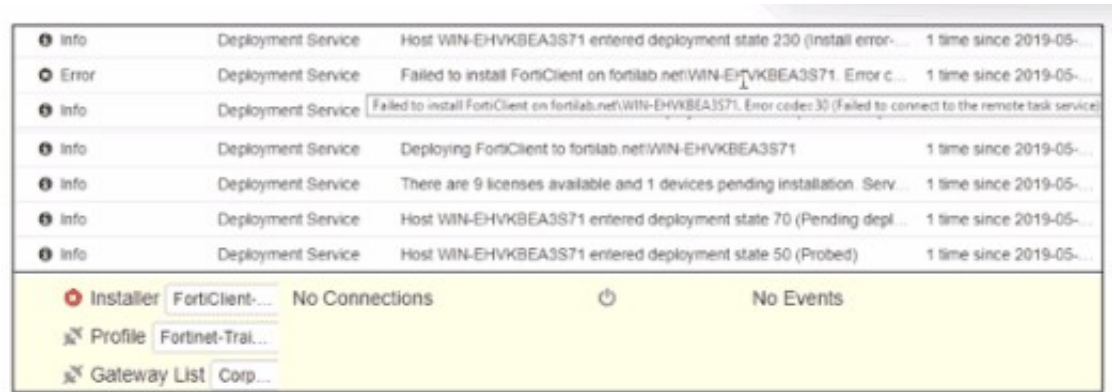
Refer to the exhibits, which show the Zero Trust Tag Monitor and the FortiClient GUI status. Remote-Client is tagged as Remote-User\* on the FortiClient EMS Zero Trust Tag Monitor. What must an administrator do to show the tag on the FortiClient GUI?

- A. Change the FortiClient EMS shared settings to enable tag visibility.
- B. Change the endpoint alerts configuration to enable tag visibility.
- C. Update tagging rule logic to enable tag visibility.
- D. Change the FortiClient system settings to enable lag visibility.

Answer: B

NEW QUESTION 8

Exhibit.



Based on the logs shown in the exhibit, why did FortiClient EMS fail to install FortiClient on the endpoint?

- A. The FortiClient antivirus service is not running.
- B. The Windows installer service is not running.
- C. The remote registry service is not running.

D. The task scheduler service is not running.

**Answer: D**

#### NEW QUESTION 9

Refer to the exhibit, which shows FortiClient EMS deployment, profiles.

| Deployments <span>+ Add</span> <span>Change Priority</span> |                                       |                         |                        |          |                                     |
|-------------------------------------------------------------|---------------------------------------|-------------------------|------------------------|----------|-------------------------------------|
| Name                                                        | Assigned Groups                       | Deployment Package      | Scheduled Upgrade Time | Priority | Enabled                             |
| Deployment-1                                                | All Groups                            | First-Time-Installation |                        | 1        | <input type="checkbox"/>            |
| Deployment-2                                                | All Groups<br>trainingAD.training.lab | To-Upgrade              |                        | 2        | <input checked="" type="checkbox"/> |

When an administrator creates a deployment profile on FortiClient EMS, which statement about the deployment profile is true?

- A. Deployment-2 will upgrade FortiClient on both the AD group and workgroup.
- B. Deployment-1 will install FortiClient on new AO group endpoints.
- C. Deployment-2 will install FortiClient on both the AD group and workgroup.
- D. Deployment-1 will upgrade FortiClient only on the workgroup.

**Answer: A**

#### NEW QUESTION 10

Exhibit.

```
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_srvc=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_srvc=os social_user=Admin
2:14:32 PM Information ESNAC id=96959 emshostname=WIN-EHVKB8EA3S71 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_srvc=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 cb828898d1ae56916f84cc7909a1ebla
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.
```

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

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

**Answer: A**

#### NEW QUESTION 10

Refer to the exhibit, which shows the endpoint summary information on FortiClient EMS.

Remote-Client

Other Endpoints

Administrator

10.0.2.20

Policy Default

EMS

VUL 99+

SYS 1

Summary

Webfilter Events

Vulnerability Events

System Events

Administrator

No User

No Email

Other Endpoints

Device

Remote-Client

OS

Microsoft Windows Server ...

IP

10.0.2.20

MAC

00-50-56-01-ea-1a

Public IP

161.156.10.132

Status

Online

Location

Off-Fabric

Owner

Organization

Zero Trust Tags

Remote-Users

Windows-Endpoints

Network Status

Ethernet0

Ethernet1 2

Connection

Managed by EMS

Configuration

Policy

Default

Profile

Training

Off-Fabric Profile

Default

Installer

Not assigned

FortiClient Version

7.0.0.0029

FortiClient Serial Number

FCT8000906335614

FortiClient ID

8B12DB30D20B4735AAA...

ZTNA Serial Number

6FC0BEB5D562E778DA8...

Classification Tags

Low

+ Add

Status

Managed

Features

Antivirus installed

Anti-Ransomware installed

Cloud Based Malware Outbre Detection installed

Sandbox installed

Sandbox Cloud installed

Web Filter enabled (hidden)

Application Firewall installed

Remote Access configured

Vulnerability Scan enabled

SSOMA installed

Third Party Features

Virus & Threat Protection

Disk Encryption

None

None

What two conclusions can you make based on the Remote-Client status shown above? (Choose two.)

- A. The endpoint is classified as at risk.
- B. The endpoint has been assigned the Default endpoint policy.
- C. The endpoint is configured to support FortiSandbox.
- D. The endpoint is currently off-net.

Answer: BD

NEW QUESTION 14

Refer to the exhibit, which shows the Zero Trust Tagging Rule Set configuration.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

### Zero Trust Tagging Rule Set

Name

Compliance

Tag Endpoint As ⓘ

Compliant

Enabled

☒

Comments

Optional

Rules

↺ Default Logic + Add Rule

| Type               | Value                                  |
|--------------------|----------------------------------------|
| Windows (2)        |                                        |
| AntiVirus Software | 1 AV Software is installed and running |
| OS Version         | 2 Windows Server 2012 R2               |
|                    | 3 Windows 10                           |

Rule Logic ⓘ

(1 and 3) or 2

↺ Reset

Which two statements about the rule set are true? (Choose two.)

- A. The endpoint must satisfy that only Windows 10 is running.
- B. The endpoint must satisfy that only AV software is installed and running.
- C. The endpoint must satisfy that antivirus is installed and running and Windows 10 is running.
- D. The endpoint must satisfy that only Windows Server 2012 R2 is running.

Answer: CD

NEW QUESTION 17

Refer to the exhibit.

 **AntiVirus Protection**  
Realtime-protection against file based malware & attack communication channels

Realtime Protection:

OFF

Dynamic Threat Detection:

OFF

Block malicious websites:

ON

Threats Detected:

75

Scan Schedule

Weekly Scan at 19:30 on Sunday

Last Scan

4/23/2019

Scan Now

Based on the settings shown in the exhibit what action will FortiClient take when it detects that a user is trying to download an infected file?

- A. Blocks the infected files as it is downloading
- B. Quarantines the infected files and logs all access attempts
- C. Sends the infected file to FortiGuard for analysis
- D. Allows the infected file to download without scan

Answer: D

**NEW QUESTION 22**

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

**NEW QUESTION 23**

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

**NEW QUESTION 25**

Refer to the exhibits.

## Security Fabric Settings

### ☒ FortiGate Telemetry

Security Fabric role **Serve as Fabric Root** Join Existing Fabric

Fabric name

Topology  FGVM010000052731 (Fabric Root)

Allow other FortiGates to join ☒  

Pre-authorized FortiGates None  Edit

SAML Single Sign-On  ☐

Management IP/FQDN  **Use WAN IP** Specify

Management Port **Use Admin Port** Specify

### ☒ FortiAnalyzer Logging

IP address

Logging to ADOM root

Storage usage  144.55 MiB / 50.00 GiB

Analytics usage  91.02 MiB / 35.00 GiB  
(Number of days stored: 55/60)

Archive usage  53.53 MiB / 15.00 GiB  
(Number of days stored: 54/365)

Upload option  **Real Time** Every Minute Every 5 Minutes

SSL encrypt log transmission

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate  FAZ-VMTM19008187

### ☒ FortiClient Endpoint Management System (EMS)

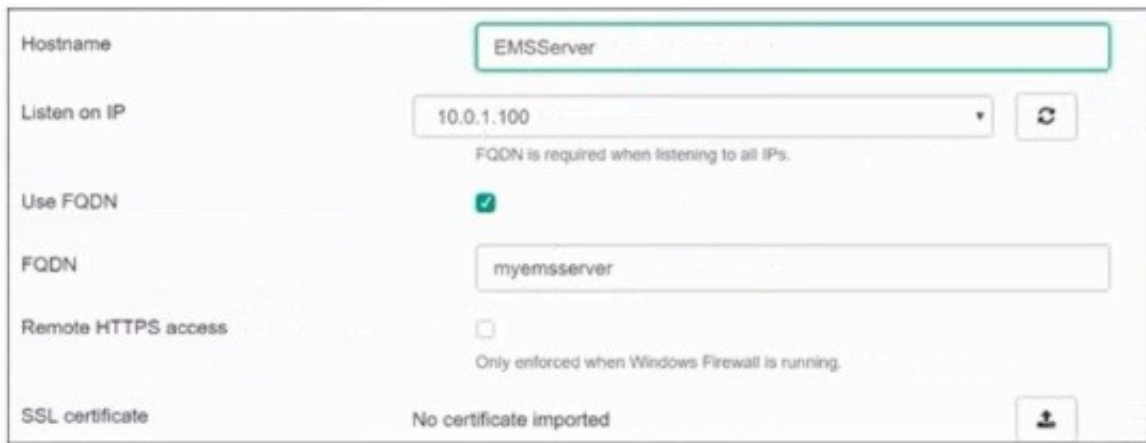
Name  

IP/Domain Name

Serial Number

Admin User

Password



Hostname: EMSServer

Listen on IP: 10.0.1.100

Use FQDN: ☒

FQDN: myemsserver

Remote HTTPS access: ☐

SSL certificate: No certificate imported

Based on the FortiGate Security Fabric settings shown in the exhibits, what must an administrator do on the EMS server to successfully quarantine an endpoint when it is detected as a compromised host (IoC)?

- A. The administrator must enable remote HTTPS access to EMS.
- B. The administrator must enable FQDN on EMS.
- C. The administrator must authorize FortiGate on FortiAnalyzer.
- D. The administrator must enable SSH access to EMS.

Answer: A

#### NEW QUESTION 29

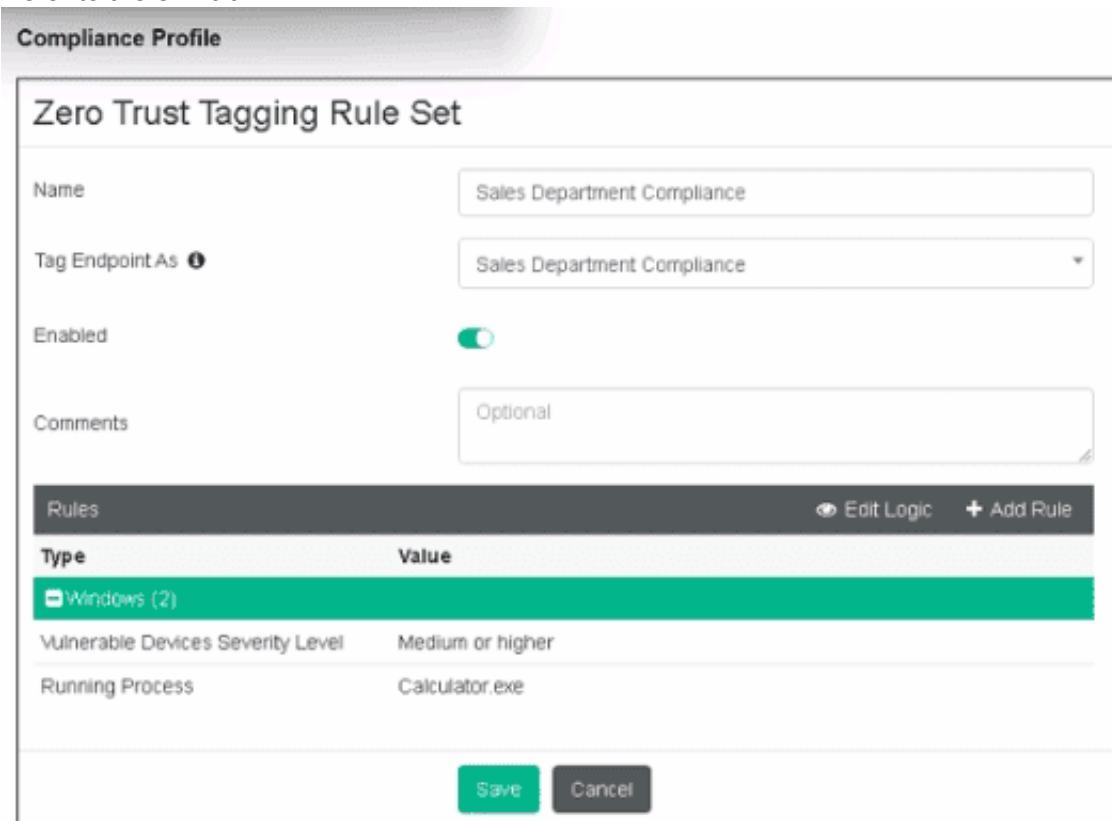
Which statement about the FortiClient enterprise management server is true?

- A. It receives the configuration information of endpoints from FortiGate.
- B. It provides centralized management of multiple endpoints running FortiClient software.
- C. It enforces compliance on the endpoints using tags
- D. It receives the CA certificate from FortiGate to validate client certificates.

Answer: C

#### NEW QUESTION 32

Refer to the exhibit.



Compliance Profile

Zero Trust Tagging Rule Set

Name: Sales Department Compliance

Tag Endpoint As: Sales Department Compliance

Enabled: ☒

Comments: Optional

| Type                              | Value            |
|-----------------------------------|------------------|
| Windows (2)                       |                  |
| Vulnerable Devices Severity Level | Medium or higher |
| Running Process                   | Calculator.exe   |

Buttons: Save, Cancel

Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two.)

- A. Enable the web filter profile.
- B. Run Calculator application on the endpoint.
- C. Integrate FortiSandbox for infected file analysis
- D. Patch applications that have vulnerability rated as high or above.

Answer: BD

#### NEW QUESTION 33

An administrator has lost web access to the FortiClient EMS console, and the web page to access to the console is timing out. How can the administrator gather information to investigate the issue? (Choose one answer)

- A. Use the CLI diagnostic tool on the EMS server.
- B. Download the webserver logs from the PostgreSQL server.
- C. Use the diagnostic logs option from the FortiClient EMS GUI.
- D. Download the log generator from the support site and run it on the EMS server.

Answer: A

**NEW QUESTION 35**

A company must integrate the FortiClient EMS with their existing identity management infrastructure for user authentication, and implement and enforce administrative access with multi-factor authentication (MFA). Which two authentication methods can they use in this scenario? (Choose two answers)

- A. LDAPS
- B. RADIUS
- C. TACACS
- D. SAML

**Answer:** BD

**NEW QUESTION 39**

Refer to the exhibit.

Edit Automation Stitch

Name

Stitch

Status

Enabled

Disabled

FortiGate

All FortiGates

Trigger

Compromised Host

Threat level threshold

Medium

High

Action

CLI Script

Email

FortiExplorer Notification

Access Layer Quarantine

Quarantine FortiClient via EMS

NSX

Assign VMware NSX Security Tag

IP Ban

AWS Lambda

Azure Function

Google Cloud Function

AliCloud Function

Webhook

Minimum interval (seconds)

0

Based on the Security Fabric automation settings, what action will be taken on compromised endpoints?

- A. Endpoints will be quarantined through EMS
- B. Endpoints will be banned on FortiGate
- C. An email notification will be sent for compromised endpoints
- D. Endpoints will be quarantined through FortiSwitch

**Answer:** A

**NEW QUESTION 41**

Refer to the exhibit.

Endpoints > All Endpoints

|                                                                                                                       |         |               |             |                                                                                     |         |        |
|-----------------------------------------------------------------------------------------------------------------------|---------|---------------|-------------|-------------------------------------------------------------------------------------|---------|--------|
| Endpoints                                                                                                             |         |               |             | Scan                                                                                | Patch   | Action |
| <input type="checkbox"/>                                                                                              | JUMPBOX | Administrator | 10.150.0.41 | Policy                                                                              | Default | EMS    |
| Other Endpoints                                                                                                       |         |               |             |                                                                                     |         |        |
| SummaryAntivirus EventsWeb Filter EventsVideo Filter EventsVulnerability EventsPUA EventsSystem EventsBrave-Dumps.com |         |               |             |                                                                                     |         |        |
| Date                                                                                                                  |         | Count         |             | Message                                                                             |         |        |
| 2025-02-12 00:40:51                                                                                                   |         | 1             |             | Malware: EICAR_TEST_FILE found in C:\Users\administrator\Desktop\Resources\testfile |         |        |

You provide a webserver hosting service. An endpoint downloads a test file, testfile.txt, that gets blocked by FortiClient. Which configuration can you use to make the file accessible on the endpoint? (Choose one answer)

- A. Restore access to file directly using FortiClient.
- B. Allow the webserver URL in the exclusion list in the web filter profile.
- C. Exclude testfile.txt from the malware protection profile.
- D. Add the file to the allowlist in quarantine management on FortiClient EMS.

Answer: D

NEW QUESTION 43

Which component or device shares ZTNA tag information through Security Fabric integration?

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

Answer: A

NEW QUESTION 44

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: A

NEW QUESTION 49

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### FCP\_FCT\_AD-7.4 Practice Exam Features:

- \* FCP\_FCT\_AD-7.4 Questions and Answers Updated Frequently
- \* FCP\_FCT\_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- \* FCP\_FCT\_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* FCP\_FCT\_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The FCP\\_FCT\\_AD-7.4 Practice Test Here](#)**