

## FCP\_FCT\_AD-7.2 Dumps

### FCP-FortiClient EMS 7.2 Administrator

[https://www.certleader.com/FCP\\_FCT\\_AD-7.2-dumps.html](https://www.certleader.com/FCP_FCT_AD-7.2-dumps.html)



### NEW QUESTION 1

What is the function of the quick scan option on FortiClient?

- A. It scans programs and drivers that are currently running, for threats
- B. It performs a full system scan including all files, executable file
- C. DLLs, and drivers for threats.
- D. It allows users to select a specific file folder on their local hard disk drive (HDD), to scan for threats.
- E. It scans executable file
- F. DLLs, and drivers that are currently running, for threats.

**Answer:** B

**Explanation:**

? Understanding Quick Scan Function:

? Evaluating Scan Scope:

? Conclusion:

References:

? FortiClient scanning options documentation from the study guides.

### NEW QUESTION 2

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

**Explanation:**

? Understanding the Need for Root CA Certificate:

? Evaluating Use Cases:

? Conclusion:

References:

? FortiClient EMS and FortiGate certificate management documentation from the study guides.

### NEW QUESTION 3

Refer to the exhibit.

## AV Protection Settings

**AntiVirus Protection** ☒

**Settings**

- ☒ Scan files as they are downloaded or copied to my system
- ☐ Antimalware Scan Interface (AMSI)
- ☐ Dynamic threat detection using threat intelligence data

**Scheduled Scan**

Schedule Type: Monthly

Scan On: 1

Start (HH:MM): 19:30

Scan Type: Full Scan

☐ Disable Scheduled Scan

**Exclusions**

Add/remove files or folders to exclude from scanning

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

**Explanation:**

Based on the settings shown in the exhibit, FortiClient is configured to scan files as they are downloaded or copied to the system. This means that if a user copies files to the ??Resources?? folder, which is not listed under exclusions, FortiClient will scan these files for infections. The exclusion path mentioned in the settings, "C:\Users\Administrator\Desktop\Resources", indicates that any files copied to this specific folder will not be scanned, but since the question implies that the ??Resources?? folder is not the same as the excluded path, FortiClient will indeed scan the files for infections.

**NEW QUESTION 4**

Which two statements are true about ZTNA? {Choose two.)

- A. ZTNA manages access for remote users only.
- B. ZTNA provides role-based access.
- C. ZTNA provides a security posture check.
- D. ZTNA manages access through the client only.

**Answer:** BC

**Explanation:**

ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.

Two functions of ZTNA are:

ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the

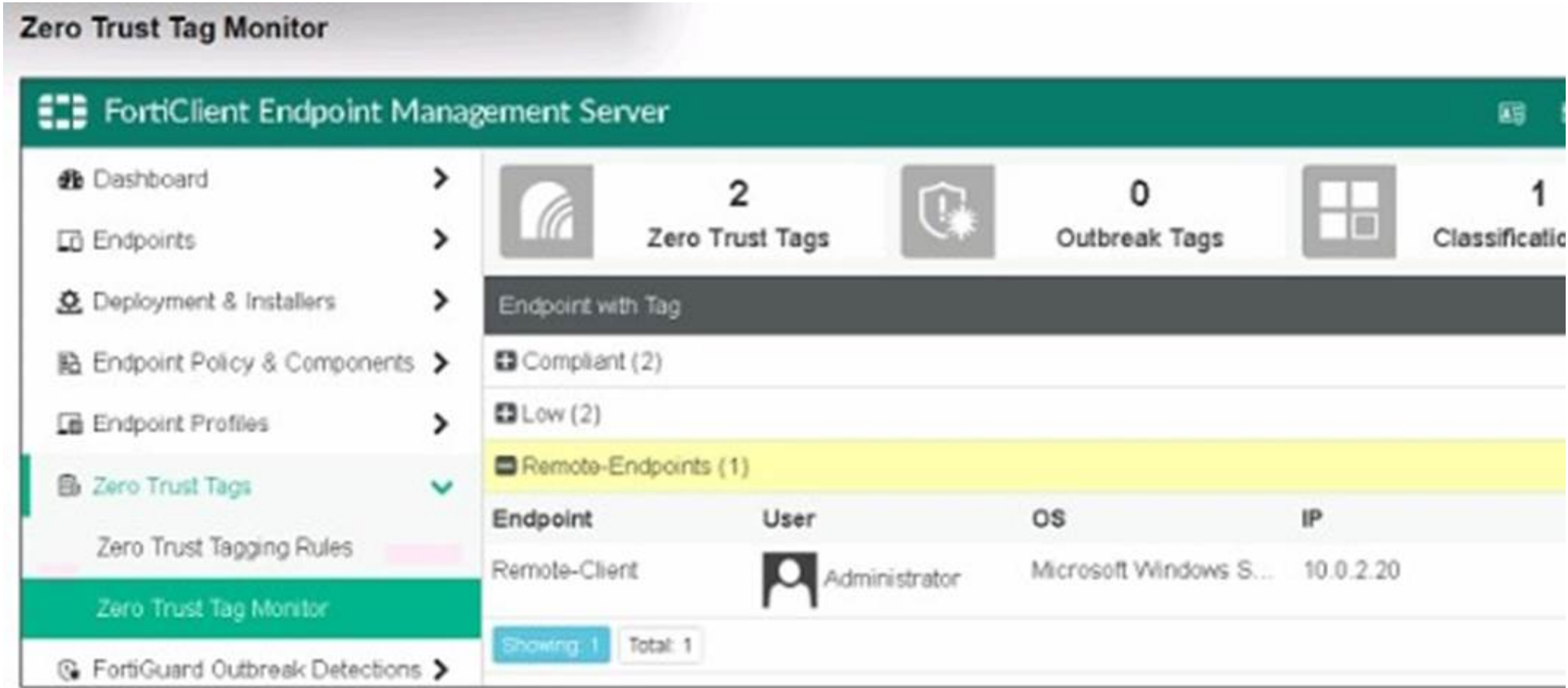
device's software and hardware configurations, security settings, and the presence of malware.

ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data

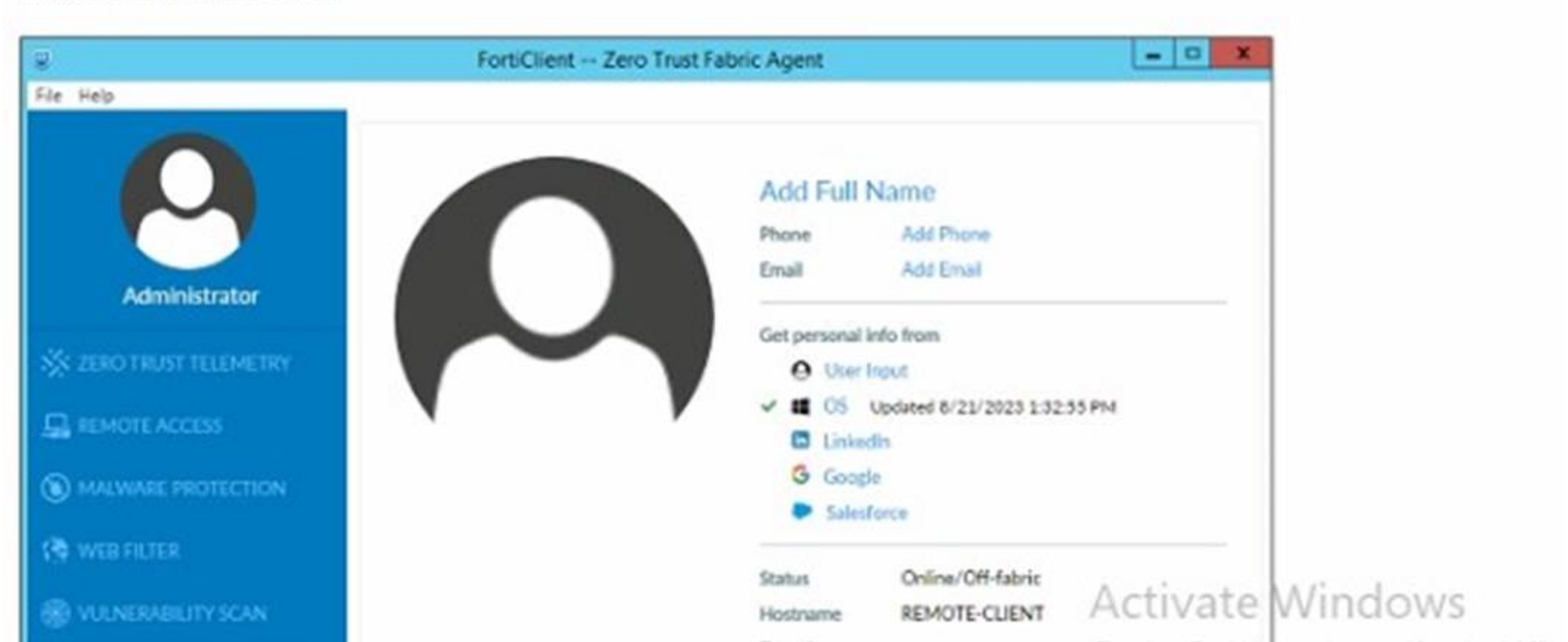
breaches.

**NEW QUESTION 5**

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

**Explanation:**

- ? Observation of Exhibits:
- ? Enabling Tag Visibility:
- ? Verification:
- References:
- ? FortiClient EMS and FortiClient configuration documentation from the study guides.

**NEW QUESTION 6**

Which statement about FortiClient enterprise management server is true?

- A. It provides centralized management of FortiGate devices.
- B. It provides centralized management of multiple endpoints running FortiClient software.
- C. It provides centralized management of FortiClient Android endpoints only.
- D. It provides centralized management of Chromebooks running real-time protection



**Answer:** B

**Explanation:**

FortiClient EMS is designed to provide centralized management and control of multiple endpoints running FortiClient software. It serves as a central management server that allows administrators to efficiently manage and configure a large number of FortiClient installations across the network.

**NEW QUESTION 7**

Which component or device shares device status information through ZTNA telemetry?

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

**Answer:** A

**Explanation:**

FortiClient communicates directly with FortiClient EMS to continuously share device status information through ZTNA telemetry.

**NEW QUESTION 8**

An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing. What could have caused this problem?

- A. The FortiClient exe file is included in the distribution package
- B. The FortiClient MST file is missing from the distribution package
- C. FortiClient does not have permission to access the distribution package.
- D. The FortiClient package is not assigned to the group

**Answer:** D

**Explanation:**

When deploying FortiClient via Microsoft AD Group Policy, it is essential to ensure that the deployment package is correctly assigned to the target group. The absence of custom configuration after installation can be due to several reasons, but the most likely cause is:

? Deployment Package Assignment: The FortiClient package must be assigned to the appropriate group in Group Policy Management. If this step is missed, the installation may proceed, but the custom configurations will not be applied. Thus, the administrator must ensure that the FortiClient package is correctly assigned to the group to include all custom configurations.

References

? FortiClient EMS 7.2 Study Guide, Deployment and Installation Section

? Fortinet Documentation on FortiClient Deployment using Microsoft AD Group Policy

**NEW QUESTION 9**

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-EHVK8EA3S71 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 cb828898d1ae56916f84cc7909a1eb1a
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

**Explanation:**

? Observation of Logs:

? Evaluating Policies:

? Conclusion:

References:

? FortiClient EMS policy configuration and log analysis documentation from the study guides.

**NEW QUESTION 10**

Which security fabric component sends a notification to quarantine an endpoint after IOC detection in the automation process?

- A. FortiAnalyzer  
B. FortiClient  
C. ForbClient EMS  
D. Forti Gate

Answer: D

NEW QUESTION 10

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 trainingAD.training.lab	VPN Training	ZTNA Training	ON-FABRIC On-Fabric	On-Fabric	1	1	<input type="checkbox"/>	
		WEB Training	VULN Training						
		MW Training	SB Training						
		FW Training	SYS Training						
Training	trainingAD.training.lab	VPN Training	ZTNA Training	ON-FABRIC On-Fabric	On-Fabric	1	2	<input checked="" type="checkbox"/>	
		WEB Training	VULN Training						
		MW Training	SB Training						
		FW Training	SYS Training						
Default		VPN Default	ZTNA Default			1	3	<input type="checkbox"/>	
		WEB Default	VULN Default						
		MW Default	SB Default						
		FW Default	SYS Default						

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

Explanation:

? Observation of Endpoint Policies:

? Evaluating Policy Assignment:

? Conclusion:

References:

? FortiClient EMS policy configuration and priority management documentation from the study guides.

NEW QUESTION 13

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

## 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

**Explanation:**

Based on the Zero Trust Tagging Rule Set configuration shown in the exhibit:

? The rule set includes two conditions:

? The Rule Logic is specified as "(1 and 3) or 2," meaning: Therefore, the endpoint must satisfy either:

? Antivirus is installed and running and Windows 10 is running.

? Windows Server 2012 R2 is running.

References

? FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Rule Set Configuration Section

? Fortinet Documentation on Configuring Zero Trust Tagging Rules and Logic

**NEW QUESTION 17**

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:

? Prerequisites for Connection:

? Conclusion:

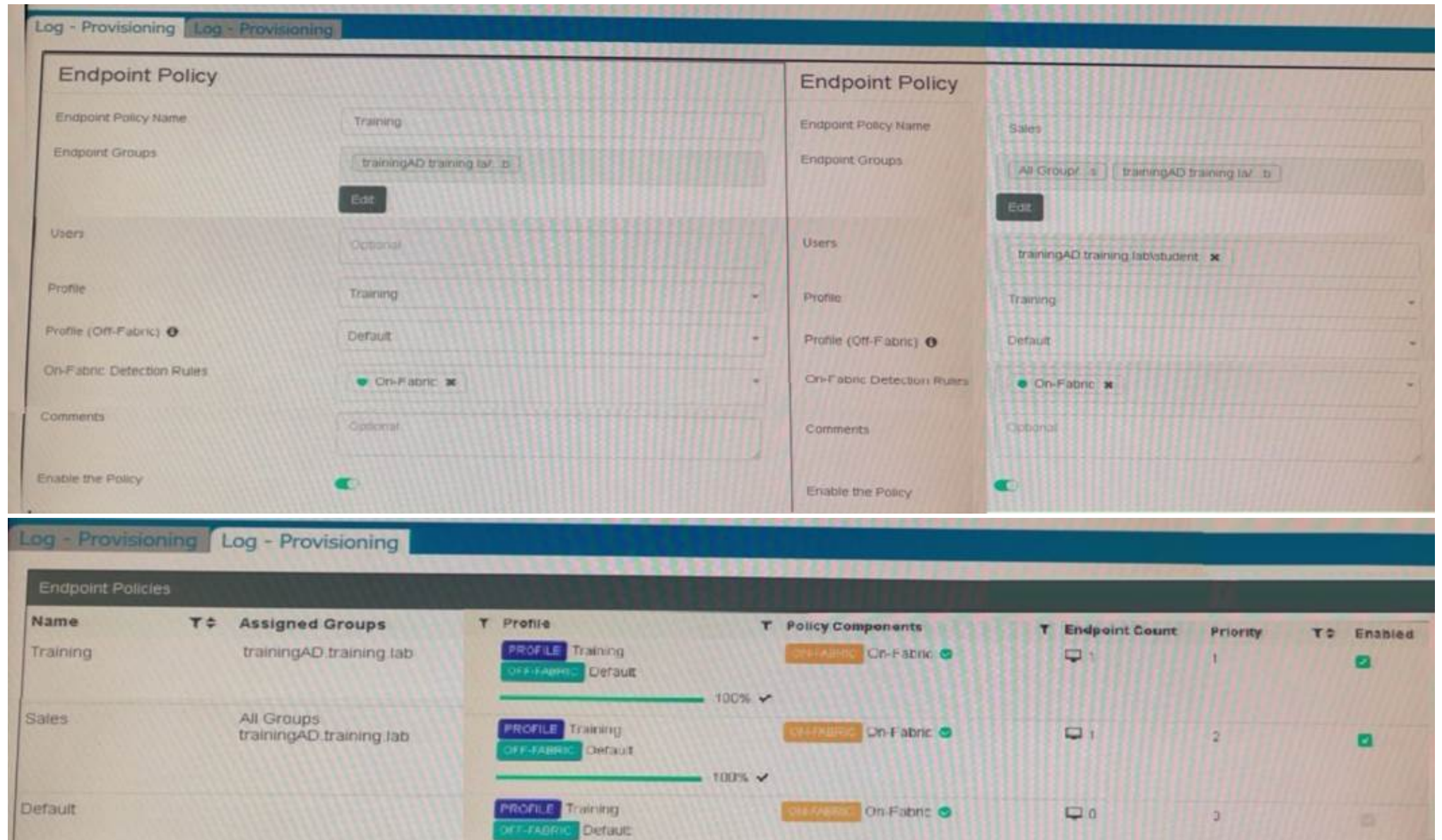
References:

? FortiClient EMS and FortiGate connection and certificate management documentation from the study guides.

**NEW QUESTION 19**



Refer to the exhibits.



Which shows the configuration of endpoint policies.

Based on the configuration, what will happen when someone logs in with the user account student on an endpoint in the trainingAD domain?

- A. FortiClient EMS will assign the Sales policy
- B. FortiClient EMS will assign the Training policy
- C. FortiClient EMS will assign the Default policy
- D. FortiClient EMS will assign the Training policy for on-fabric endpoints and the Sales policy for the off-fabric endpoint

**Answer: B**

**Explanation:**

Based on the configuration shown in the exhibits:

- ? There are three endpoint policies configured: Training, Sales, and Default.
- ? The "Training" policy is assigned to the "trainingAD.training.lab" group.
- ? The "Sales" policy is assigned to "All Groups" and "trainingAD.training.lab/student."
- ? The "Default" policy has no specific groups assigned.

When someone logs in with the user account "student" on an endpoint in the "trainingAD" domain:

- ? The "Training" policy is specifically assigned to the "trainingAD.training.lab" group.
- ? The "Sales" policy includes "trainingAD.training.lab/student" but not the general "trainingAD.training.lab" group.
- ? The system will prioritize the most specific match for the group.

Therefore, FortiClient EMS will assign the "Training" policy to the "student" account logging into the "trainingAD" domain as it matches the group "trainingAD.training.lab" directly. References

- ? FortiClient EMS 7.2 Study Guide, Endpoint Policy Configuration Section
- ? FortiClient EMS Documentation on Group Policy Assignment and Matching

**NEW QUESTION 24**

Which two VPNtypes can a FortiClientendpoint user inmate from the Windows command prompt? (Choose two)

- A. L2TP
- B. PPTP
- C. IPSec
- D. SSL VPN

**Answer: CD**

**Explanation:**

FortiClient supports initiating the following VPN types from the Windows command prompt:

- ? IPSec VPN:FortiClient can establish IPSec VPN connections using command line instructions.
  - ? SSL VPN:FortiClient also supports initiating SSL VPN connections from the Windows command prompt.
- These two VPN types can be configured and initiated using specific command line parameters provided by FortiClient.

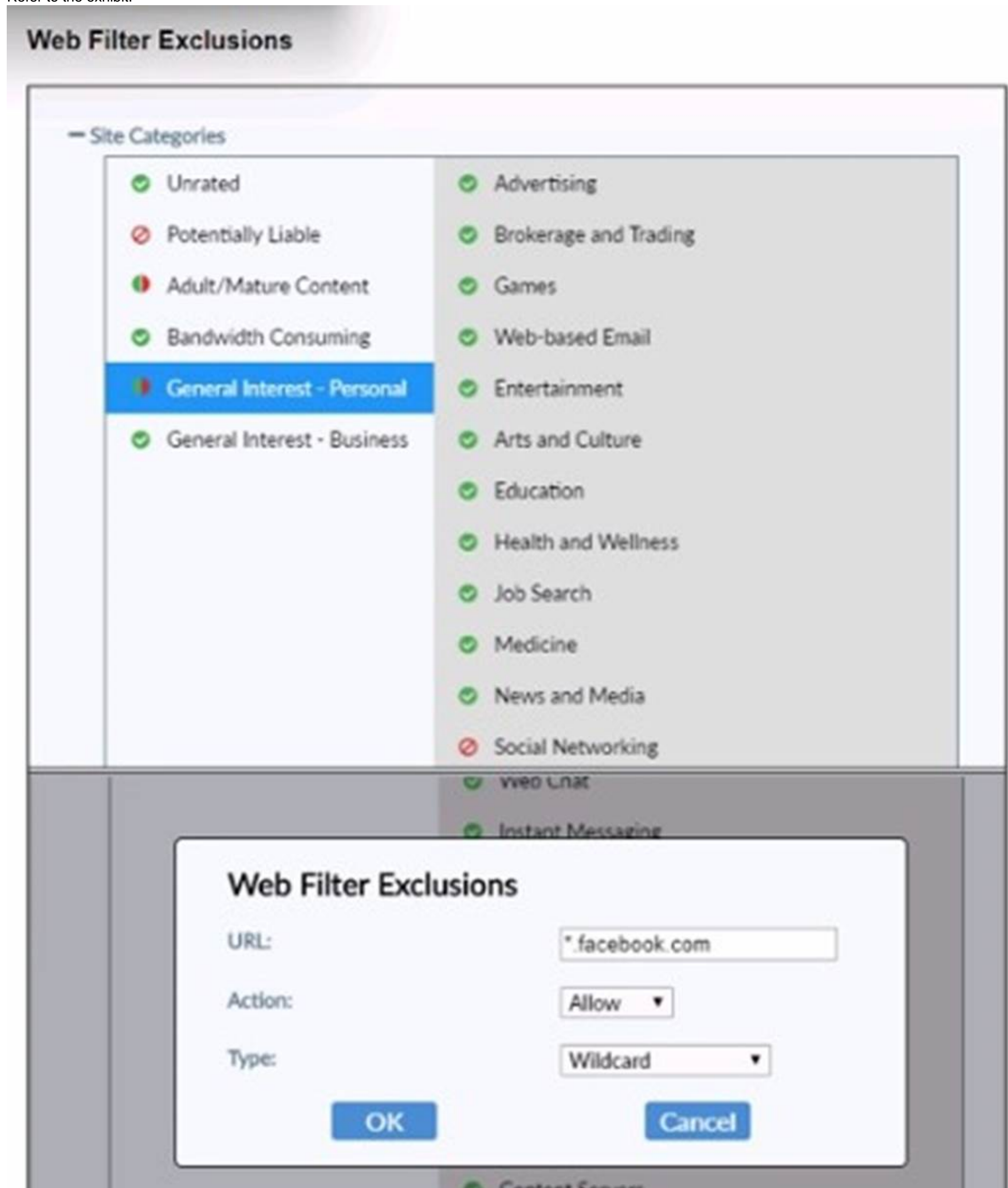
References

- ? FortiClient EMS 7.2 Study Guide, VPN Configuration Section
- ? Fortinet Documentation on Command Line Options for FortiClient VPN



**NEW QUESTION 28**

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: B**

**Explanation:**

? Observation of Web Filter Exclusions:

? Evaluating Actions:

? Conclusion:

References:

? FortiClient web filter configuration and exclusion documentation from the study guides.

**NEW QUESTION 32**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your FCP\_FCT\_AD-7.2 Exam with Our Prep Materials Via below:**

[https://www.certleader.com/FCP\\_FCT\\_AD-7.2-dumps.html](https://www.certleader.com/FCP_FCT_AD-7.2-dumps.html)