



Free Questions for FCP_FCT_AD-7.2 by ebraindumps

Shared by Evans on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement about FortiClient comprehensive endpoint protection is true?

Options:

- A- It helps to safeguard systems from email spam
- B- It helps to safeguard systems from data loss.
- C- It helps to safeguard systems from DDoS.
- D- It helps to safeguard systems from advanced security threats, such as malware.

Answer:

D

Explanation:

FortiClient provides comprehensive endpoint protection for your Windows-based, Mac-based, and Linuxbased desktops, laptops, file servers, and mobile devices such as iOS and Android. It helps you to safeguard your systems with advanced security technologies, all of which you can manage from a single management console.

Question 2

Question Type: MultipleChoice

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  port3 
+

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  0% 144.55 MiB / 50.00 GiB

Analytics usage  0% 91.02 MiB / 35.00 GiB

(Number of days stored: 55/60)

Archive usage  0% 53.53 MiB / 15.00 GiB

(Number of days stored: 54/365)

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

Hostname	<input type="text" value="EMSServer"/>
Listen on IP	<input type="text" value="10.0.1.100"/> <input type="button" value="↻"/> <small>FQDN is required when listening to all IPs.</small>
Use FQDN	<input checked="" type="checkbox"/>
FQDN	<input type="text" value="myemsserver"/>
Remote HTTPS access	<input type="checkbox"/> <small>Only enforced when Windows Firewall is running.</small>
SSL certificate	No certificate imported <input type="button" value="↓"/>

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)?

Options:

- 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

Explanation:

Based on the FortiGate Security Fabric settings shown in the exhibits, to successfully quarantine an endpoint when it is detected as a compromised host (IOC), the following step is required:

Enable Remote HTTPS Access to EMS: This setting allows FortiGate to communicate securely with FortiClient EMS over HTTPS. Remote HTTPS access is essential for the quarantine functionality to operate correctly, enabling the EMS server to receive and act upon the quarantine commands from FortiGate.

Therefore, the administrator must enable remote HTTPS access to EMS to allow the quarantine process to function properly.

Reference

FortiGate Infrastructure 7.2 Study Guide, Security Fabric and Integration with EMS Sections

Fortinet Documentation on Enabling Remote HTTPS Access to FortiClient EMS

Question 3

Question Type: MultipleChoice

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?

Options:

- 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.

Reference

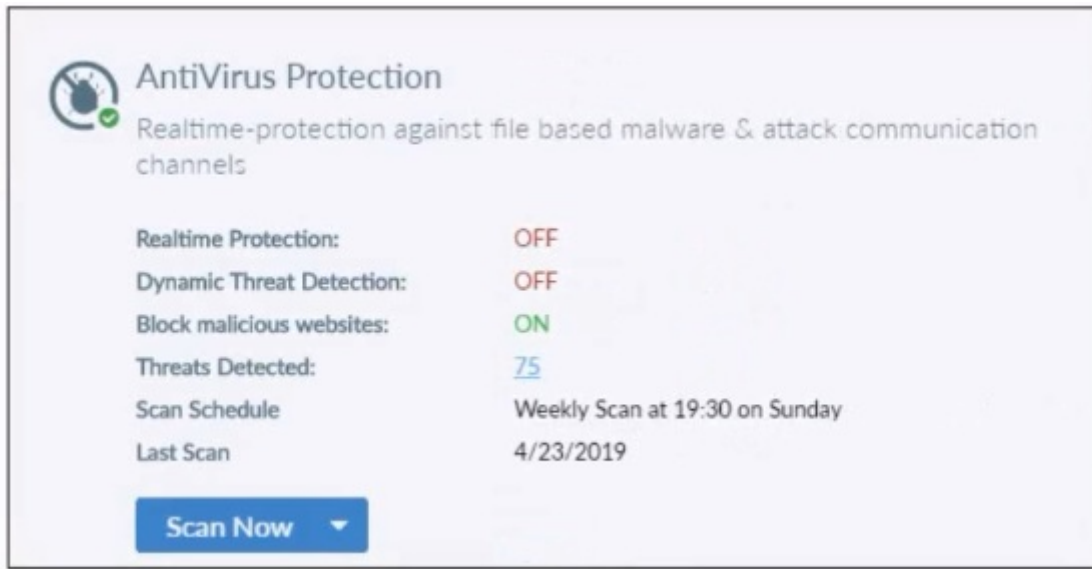
FortiClient EMS 7.2 Study Guide, Deployment and Installation Section

Fortinet Documentation on FortiClient Deployment using Microsoft AD Group Policy

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



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?

Options:

- 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

Explanation:

Block Malicious Website has nothing to do with infected files. Since Realtime Protection is OFF, it will be allowed without being scanned.

Based on the settings shown in the exhibit:

Realtime Protection: OFF

Dynamic Threat Detection: OFF

Block malicious websites: ON

Threats Detected: 75

The 'Realtime Protection' setting is crucial for preventing infected files from being downloaded and executed. Since 'Realtime Protection' is OFF, FortiClient will not actively scan files being downloaded. The setting 'Block malicious websites' is intended to prevent access to known malicious websites but does not scan files for infections.

Therefore, when a user tries to download an infected file, FortiClient will allow the file to download without scanning it due to the Realtime Protection being OFF.

Reference

FortiClient EMS 7.2 Study Guide, Antivirus Protection Section

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

```
config user fsso
  edit "Server"
    set type fortiems
    set server "10.0.1.200"
    set password ENC ebT9fHIMXIBykhWCSnG;P+Tpi/EjEdQu4hAa24LiKxHolWI7JyX
    set ssl enable
  next
end
```

Based on the CLI output from FortiGate, which statement is true?

Options:

- A- FortiGate is configured to pull user groups from FortiClient EMS
- B- FortiGate is configured with local user group

C- FortiGate is configured to pull user groups from FortiAuthenticator

D- FortiGate is configured to pull user groups from AD Server.

Answer:

A

Explanation:

Based on the CLI output from FortiGate:

The configuration shows the use of 'type fortiems,' indicating that FortiGate is set up to interact with FortiClient EMS.

The 'server' field points to an IP address (10.0.1.200), which is typically the address of the FortiClient EMS server.

The configuration includes an SSL-enabled connection, which is a common setup for secure communication between FortiGate and FortiClient EMS.

Thus, the configuration indicates that FortiGate is set up to pull user groups from FortiClient EMS.

Reference

FortiGate Security 7.2 Study Guide, FSSO Configuration Section

Fortinet Documentation on FortiGate and FortiClient EMS Integration

Question 6

Question Type: MultipleChoice

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

Options:

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

Answer:

D

Question 7

Question Type: MultipleChoice

Which two third-party tools can an administrator use to deploy FortiClient? (Choose two.)

Options:

- A- Microsoft Windows Installer
- B- Microsoft SCCM
- C- Microsoft Active Directory GPO
- D- QR code generator

Answer:

B, C

Explanation:

Administrators can use several third-party tools to deploy FortiClient:

Microsoft SCCM (System Center Configuration Manager): SCCM is a robust tool used for deploying software across large numbers of Windows-based systems. It supports deployment of FortiClient through its software distribution capabilities.

Microsoft Active Directory GPO (Group Policy Object): GPOs are used to manage user and computer settings in an Active Directory environment. Administrators can deploy FortiClient to multiple machines using GPO software installation settings.

These tools provide centralized and scalable methods for deploying FortiClient across numerous endpoints in an enterprise environment.

Reference

FortiClient EMS 7.2 Study Guide, FortiClient Deployment Section

Fortinet Documentation on FortiClient Deployment using SCCM and GPO

Question 8

Question Type: MultipleChoice

Refer to the exhibits.


FortiClient Endpoint Management Server

Invitations

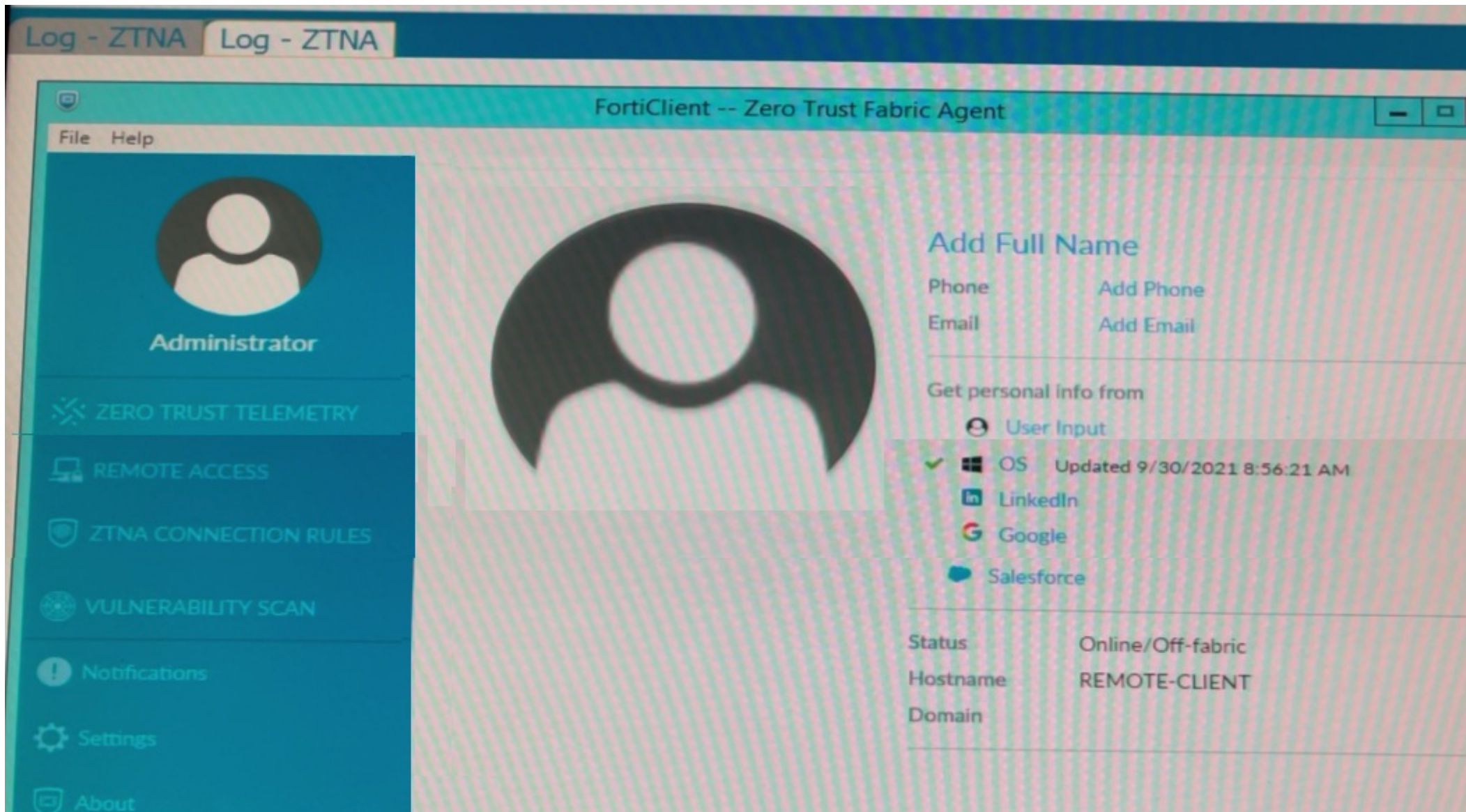
- Dashboard >
- Endpoints >
- Deployment & Installers >
- Endpoint Policy & Components >
- Endpoint Profiles >
- Zero Trust Tags** ✓
- Zero Trust Tagging Rules

Endpoint with Tag

Remote-Users (1)

Endpoint	User	IP	Tagged on
Remote-Client	 Administrator	10.0.2.20	2021-09-30 09:12:53

Zero Trust Tag Monitor



Which show the Zero Trust Tag Monitor and the FortiClient GUI status.

Remote-Client is tagged as Remote-Users on the FortiClient EMS Zero Trust Tag Monitor.

What must an administrator do to show the tag on the FortiClient GUI?

Options:

- A- Update tagging rule logic to enable tag visibility
- B- Change the FortiClient system settings to enable tag visibility
- C- Change the endpoint control setting to enable tag visibility
- D- Change the user identity settings to enable tag visibility

Answer:

B

Explanation:

Based on the exhibits provided:

The 'Remote-Client' is tagged as 'Remote-Users' in the FortiClient EMS Zero Trust Tag Monitor.

To ensure that the tag 'Remote-Users' is visible in the FortiClient GUI, the system settings within FortiClient need to be updated to enable tag visibility.

The tag visibility feature is controlled by FortiClient system settings which manage how tags are displayed in the GUI.

Therefore, the administrator needs to change the FortiClient system settings to enable tag visibility.

Reference

FortiClient EMS 7.2 Study Guide, Zero Trust Tagging Section

FortiClient Documentation on Tag Management and Visibility Settings

To Get Premium Files for FCP_FCT_AD-7.2 Visit

https://www.p2pexams.com/products/fcp_fct_ad-7.2

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/fcp-fct-ad-7.2>

