

Fortinet

NSE6_EDR_AD-7.0

Fortinet NSE 6 - FortiEDR 7.0 Administrator

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/nse6-edr-ad-7-0>

Latest Version: 6.0

Question: 1

An employee leaves the company and no longer has access to the FortiEDR system. You must ensure GDPR compliance regarding the employee's personal data stored in FortiEDR. Which two data types must be removed to meet GDPR requirements? (Choose two answers)

- A. Device and user name
- B. Installed applications
- C. Installed OS name
- D. IP address and MAC address

Answer: A, D

Explanation:

The correct answers are A. Device and user name and D. IP address and MAC address.

The FortiEDR 7.0.0 Administration Guide states that the GDPR feature is implemented in Administration > Settings > Personal Data Handling. It is used to remove relevant data for an employee or FortiEDR user who no longer has access to or uses the FortiEDR system. The guide explicitly identifies the personal data as device name, IP address, MAC address, and user name. It further states: "You must remove all device name, IP address, MAC address, and user name data from FortiEDR in order to fully comply with the GDPR standard."

Therefore, installed applications and installed OS name are not the required GDPR personal data types in this FortiEDR procedure. The required removal is performed iteratively for the employee's/user's device name, IP address, MAC address, and user name. The guide also instructs administrators to continue removing the other required data: IP address, MAC address, and user name, and to delete any reports that may contain the user's data.

Question: 2

Which two statements correctly describe the IoT probing process on FortiEDR? (Choose two answers)

- A. Collectors running on servers are always used for IoT probing.
- B. It identifies nearby devices by retrieving details such as hostname and IP address.
- C. Only healthy collectors participate in IoT probing.
- D. It captures all traffic from neighboring devices for deep packet inspection.

Answer: B, C

Explanation:

The correct answers are B and C.

The FortiEDR 7.0.0 Administration Guide explains that IoT device discovery continuously identifies newly connected non-workstation devices, such as printers, cameras, and media devices. During discovery, each relevant Collector periodically probes nearby neighboring devices. The guide states that nearby devices usually respond by providing information about themselves, including the device/host name and IP address. This directly supports option B. Option C is also correct because the guide states that Collectors in degraded, disabled, or isolated states do not take part in the IoT probing process. It also says FortiEDR uses the most powerful Collectors in each subnet and excludes weaker Collectors, including disabled and degraded Collectors.

Option A is wrong because the guide explicitly says Collectors running on servers do not take part in IoT probing. Option D is wrong because IoT probing is not described as deep packet inspection of all neighboring traffic; it is a discovery/probing process used to identify nearby devices and collect basic device information.

=====

Question: 3

You added three new applications to FortiEDR using only the Path attribute. What are two expected outcomes of this configuration? (Choose two answers)

- A. These applications will be disabled until explicitly enabled.
- B. Only applications in the specified directory paths will be blocked.
- C. These applications will be blocked only if the file name also matches.
- D. All instances of these applications will be blocked, regardless of location.

Answer: A, B

Explanation:

The correct answers are A and B.

The FortiEDR 7.0.0 Administration Guide states that newly added applications are disabled by default, which means they are not blocked unless enabled. The guide further explains that the default state can be changed by enabling the Enable Default application state option in the Application Control Manager settings. Therefore, option A is correct.

Option B is also correct because Application Control allows an application to be defined by Hash or by any combination of File Name / Path / Signer. The guide says that the Path field specifies the path to the executable file of the application to be blocked. When using path-based matching, the enforcement is tied to the specified path criteria, not to every possible location of the same file.

Option C is wrong because the file name does not also need to match when only the Path attribute is used. Option D is wrong because blocking all instances regardless of location applies when only the File Name field is used, not when the match is path-specific. The guide explicitly states that if only the File Name field is filled, the application is blocked no matter where the executable appears.

Question: 4

You find third-party software on a user's computer that does not appear in the application list on the communication control console. Which two statements are true about this situation? (Choose two answers)

- A. The application has not made any connection attempts.
- B. The application is blocked by the security policies.
- C. The application is ignored because its reputation score is acceptable to the security policy.
- D. The application is allowed in all communication control policies.

Answer: A, D

Explanation:

The best answers are A and D, but be careful: A is directly verified by the guide; D is the only remaining statement that can be true in policy context, but it is weaker than A.

The FortiEDR 7.0.0 Administration Guide states that the Communication Control tab identifies communicating applications detected in the organization. More specifically, the Applications page lists "all communicating applications detected in your organization that have ever attempted to communicate." Therefore, if software exists on a user's computer but does not appear in the Communication Control application list, the most direct explanation is that it has not attempted external communication.

The guide also explains that FortiEDR Communication Control reduces the scope of administration because Security/IT only needs to handle applications that communicate externally. It also states that non-authorized applications can still execute, and only their outgoing communication is prevented. This confirms that the Communication Control application list is not a full software inventory; it is a list of applications that have communicated or attempted communication.

Option B is not correct. If an application were blocked due to FortiEDR security-policy enforcement after a connection attempt, FortiEDR would generate security-event visibility in the Incidents workflow, not simply hide the application from Communication Control. FortiEDR Collectors send communication-related data for Communication Control, and security events are sent for enforcement/monitoring purposes.

Option C is also wrong. Reputation score affects policy decisions and application risk evaluation, but it does not cause an application to be ignored or excluded from the application list. The guide says each application in the Applications page shows a reputation indicator, which proves reputation is displayed for listed applications rather than used to hide them.

For option D, if the application has never attempted communication, Communication Control has no observed communication event to list. In exam logic, this can be interpreted as the application is not currently being denied by Communication Control policies. However, the stronger technical truth is this: Communication Control does not list installed software; it lists applications that have attempted to communicate.

=====

Question: 5

Within the FortiEDR architecture, which component needs JumpBox capabilities to enable authenticated and controlled communication with FortiAnalyzer? (Choose one answer)

- A. Core
- B. Central manager
- C. Aggregator
- D. Reputation Server

Answer: A

Explanation:

The correct answer is A. Core.

For FortiAnalyzer / FortiAnalyzer Cloud integration, the FortiEDR 7.0.0 Administration Guide states that one prerequisite is "A Jumpbox with connectivity to FortiAnalyzer." The same section says to refer to Setting up the FortiEDR Core for details about installing a FortiEDR Core and configuring it as a Jumpbox. In the connector configuration, the guide also states that the Jumpbox field is used to select the FortiEDR Jumpbox that will communicate with FortiAnalyzer or FortiAnalyzer Cloud.

So, the FortiEDR component associated with JumpBox capability is the Core. The Central Manager must have connectivity to Fortinet Cloud Services, but it is not the component configured as the JumpBox. The Aggregator handles registration, configuration, and monitoring between Collectors/Cores and Central Manager, and the Reputation Server is unrelated to FortiAnalyzer JumpBox communication in this context.

=====

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>