

# *PassTest*

Bessere Qualität , bessere Dienstleistungen!



## Q&A

<http://www.passtest.de>

Einjährige kostenlose Aktualisierung

**Exam** : **NSE5\_FCT-6.2**

**Title** : Fortinet NSE 5 - FortiClient  
EMS 6.2

**Version** : DEMO

1.Refer to the exhibit.

The screenshot displays the FortiClient endpoint management interface. It is divided into two main sections. The top section is for a 'Running Process' rule, which is currently set to 'Required'. Below this, a list of processes is shown, with 'Calculator.exe' marked as 'NOT' compliant. The bottom section is for a 'Vulnerable Devices' rule, which is currently set to 'Medium' severity level. Other settings include 'Assign to' set to 'All' and 'Tag endpoint as' set to 'Sales Department Compliance'.

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

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

**Answer:** C,D

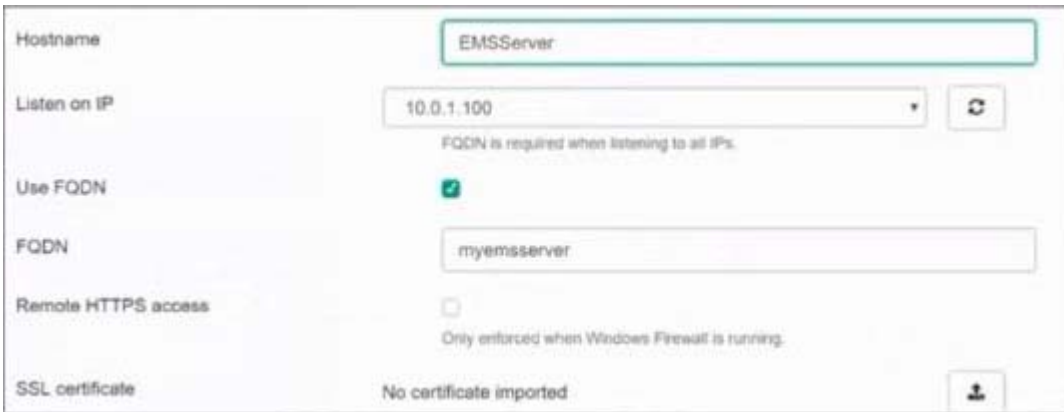
2.What action does FortiClient anti-exploit detection take when it detects exploits?

- A. Terminates the compromised application process
- B. Patches the compromised application process
- C. Blocks memory allocation to the compromised application process
- D. Deletes the compromised application process

**Answer:** A

3.Refer to the exhibits.





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**

4. 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?

- 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**

5. 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**