



NSE5_FCT-7.0^{Q&As}

Fortinet NSE 5 - FortiClient EMS 7.0

Pass Fortinet NSE5_FCT-7.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/nse5_fct-7-0.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Refer to the exhibit.

Log - Policy

```
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-EHVKBEA3571 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. Default
- B. Compliance rules default
- C. Fortinet- Training
- D. Default configuration policy

Correct Answer: C

QUESTION 2

Refer to the exhibit.



The screenshot shows the FortiClient application window. A blue error dialog box is overlaid on top, displaying the message "Failed to process the file." with an "OK" button. Below the dialog, the XML configuration for the SSLVPN service is visible in a text editor.

```

<sslvpn>
  <options>
    <enabled>1</enabled>
    <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
    <dnscache_service_control>0</dnscache_service_control>
    <use_legacy_ssl_adapter>0</use_legacy_ssl_adapter>
    <preferred_dtls_tunnel>0</preferred_dtls_tunnel>
    <no_dhcp_server_route>0</no_dhcp_server_route>
    <no_dns_registration>0</no_dns_registration>
    <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
  </options>
  <connections>
    <connection>
      <name>Student-SSLVPN</name>
      <description>SSL VPN to Fortigate</description>
      <server>10.0.0.254:10443</server>
      <username />
      <single_user_mode>0</single_user_mode>
      <ui>
        <show_remember_password>0</show_remember_password>
      </ui>
      <password />
      <prompt_username>1</prompt_username>
      <on_connect>
        <script>
          <os>windows</os>
          <script>
            <![CDATA[]]>
          </script>
        </script>
      </on_connect>
      <on_disconnect>
        <script>
          <os>windows</os>
          <script>
            <![CDATA[]]>
          </script>
        </script>
      </on_disconnect>
    </connection>
  </connections>
</sslvpn>
<ipsecvpn>

```



An administrator has restored the modified XML configuration file to FortiClient and sees the error shown in the exhibit.

Based on the XML settings shown in the exhibit, what must the administrator do to resolve the issue with the XML configuration file?

- A. The administrator must resolve the XML syntax error.
- B. The administrator must use a password to decrypt the file
- C. The administrator must change the file size
- D. The administrator must save the file as FortiClient-config.conf.

Correct Answer: A

QUESTION 3

A new chrome book is connected in a school's network.

Which component can the EMS administrator use to manage the FortiClient web filter extension installed on the Google Chromebook endpoint?

- A. FortiClient site categories
- B. FortiClient customer URL list
- C. FortiClient web filter extension
- D. FortiClient EMS

Correct Answer: C

QUESTION 4

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

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: | 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:

Listen on IP:

FQDN is required when listening to all IPs.

Use FQDN:

FQDN:

Remote HTTPS access:
Only enforced when Windows Firewall is running.

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.

Correct Answer: A

QUESTION 5

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

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

Correct Answer: BC

[Latest NSE5_FCT-7.0 Dumps](#)

[NSE5_FCT-7.0 VCE Dumps](#) [NSE5_FCT-7.0 Study Guide](#)