EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

An administrator must deploy FortiClient for an organization that has BYOD and remote users.
What can the administrator use to deploy FortiClient?

A. FortiClient zero-touch provisioning

B. Microsoft System Center Configuration Manager (SCCM)

C. Microsoft Intune

D. Group policy Object (GPO)

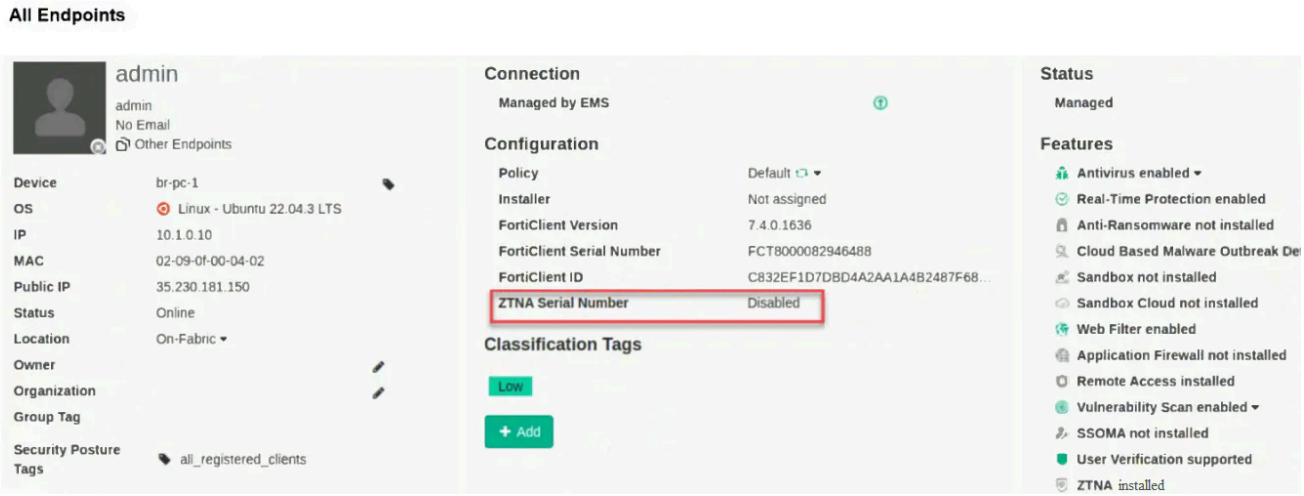
**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Refer to the exhibit.

The zero trust network access (ZTNA) serial number on endpoint br-pc-1 is in a disabled state.
What is causing the problem?




A. The ZTNAfeature is not installed on FortiClient.

B. The ZTNAdestinations endpoint profile is disabled.

C. The ZTNA is disabled due to FortiClient disconnected from FortiClient EMS.

D. The ZTNA certificate has been revoked by administrator.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Refer to the exhibit.

Why is the user not able to access bbc.com?

**FortiClient logs**

```
20250226 05:50:24.563 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /
20250226 05:50:24.563 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com
20250226 05:50:24.563 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /
20250226 05:50:24.564 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com /
20250226 05:50:24.564 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com / rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.564 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com / Unknown 2025-02-26 05:50:24.564598172
+0100 CET m=+4561.038040408 admin 368039 /opt/google/chrome/chrome}
20250226 05:50:24.601 TZ=+0100 [DEBUG] http2_handler:312 set table size to 65536
20250226 05:50:24.820 TZ=+0100 [DEBUG] proxy:381 ConnID 1557243034: now rate bbc.com /favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] accessors:127 url comparing https://www.twitter.com https://bbc.com/favicon.ico
20250226 05:50:24.820 TZ=+0100 [DEBUG] fgdahandle:346 Category request: host bbc.com path /favicon.ico
20250226 05:50:24.821 TZ=+0100 [ERROR] rating_db:97 Category query failure: failed to UrlRequestSendReceive
receiveResponse error: FortiGuard server down, task dropped, https bbc.com /favicon.ico
20250226 05:50:24.821 TZ=+0100 [INFO ] proxy:383 ConnID 1557243034: bbc.com /favicon.ico rating: -1 action: WF_ACTION_BLOCK
20250226 05:50:24.821 TZ=+0100 [INFO ] accessors:352 inserting violation: {bbc.com /favicon.ico Unknown 2025-02-26 05:50:24.8212255
+0100 CET m=+4561.294667764 admin 368039 /opt/google/chrome
```

A. The URL is blocked by the web filter endpoint profile.

B. The endpoint cannot resolve the URL FQDN.

C. FortiGuard servers are not reachable from the endpoint.

D. The application firewall is blocking Google Chrome.

**Suggested Answer:** *C*

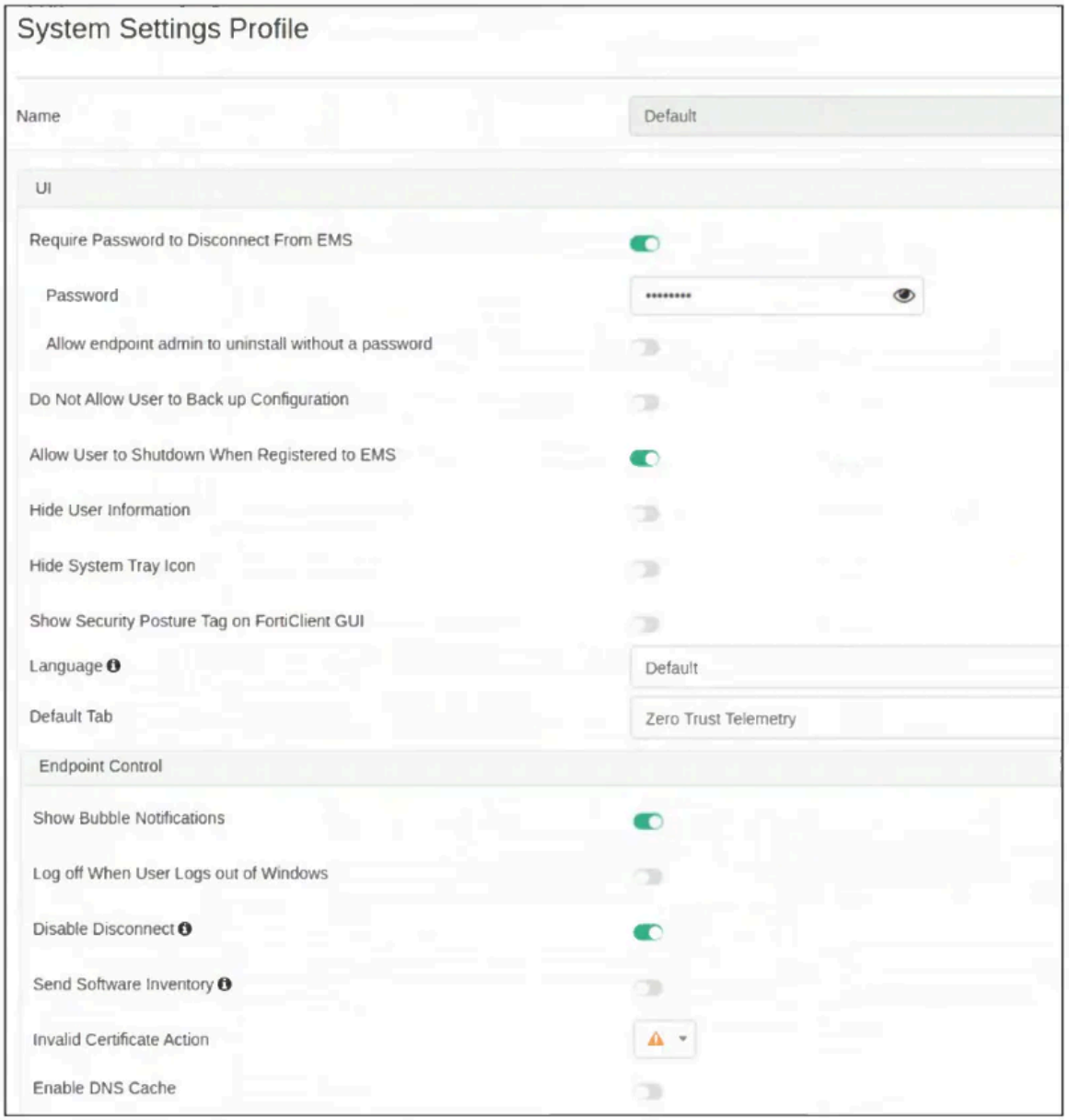
Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Refer to the exhibit.

Which behavior should you expect when FortiClient with an invalid certificate is connecting to FortiClient EMS?

**System settings profile**




A. FortiClient is blocked from connecting to FortiClient EMS.

B. FortiClient requires an additional password to connect to FortiClient EMS.

C. FortiClient displays a warning message to the end user.

D. FortiClient EMS pushes a valid certificate to FortiClient.

**Suggested Answer:** *C*

Invalid Certificate Action is set to warn, so the user sees a warning.

*Community vote distribution*

C (100%)

**AgentSmith** Most Recent 7 months, 3 weeks ago

Selected Answer: C

https://docs.fortinet.com/document/forticlient/7.4.5/ems-administration-guide/107284

Invalid Certificate Action

Select the action to take when FortiClient attempts to connect to EMS with an invalid certificate:

Allow: allows FortiClient to connect to EMS with an invalid certificate.

Warn: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate.

Deny: block FortiClient from connecting to EMS with an invalid certificate.

upvoted 1 times

Question #5 *Topic 1*

An administrator has lost web access to the FortiClient EMS console, and the web page to access to the console is timing out.

How can the administrator gather information to investigate the issue?

A. Use the CLI diagnostic tool on the EMS server.

B. Download the webserver logs from the PostgreSQL server.

C. Use the diagnostic logs option from the FortiClient EMS GUI.

D. Download the log generator from the support site and run it on the EMS server.

**Suggested Answer:** *A*

Use the EMS server's CLI diagnostic tool when the GUI is unavailable.

*Community vote distribution*

A (100%)

**AgentSmith** Most Recent 7 months, 1 week ago

Selected Answer: A

Agreed, you can use it to retrieve or set configuration settings etc

upvoted 1 times

**3xaminator** 7 months, 2 weeks ago

Selected Answer: A

page 328 in study guide = "Use the CLI diagnostic tool in CLI when the GUI is inaccessible"

upvoted 2 times

Question #6 *Topic 1*

When multitenancy is enabled on FortiClient EMS, which administrator role can provide access to the global site only?

A. Tenant administrator

B. Settings administrator

C. Standard administrator

D. Global administrator

**Suggested Answer:** *D*

Global administrators have access to the global site.

*Community vote distribution*

B (100%)

**prepengine** Most Recent 4 months, 2 weeks ago

Selected Answer: B

Settings administrator: Access to the global site only. Can access all configuration options on the global site, except for administrator configuration.

upvoted 1 times

**Ahabib80** 6 months, 1 week ago

Selected Answer: B

Settings administrator and super administrator have access to global site.

upvoted 2 times

**AgentSmith** 7 months, 1 week ago

Selected Answer: B

https://docs.fortinet.com/document/forticlient/7.4.6/ems-administration-guide/554374/adding-a-multitenancy-administrator

Settings administrator

Access to the global site only. Can access all configuration options on the global site, except for administrator configuration.

upvoted 1 times

Question #7 *Topic 1*

Which Fortinet solution can you integrate FortiClient with to use the single sign-on mobility agent (SSOMA) feature?

A. FortiAuthenticator

B. FortiSASE

C. FortiPAM

D. FortiNAC

**Suggested Answer:** *A*
FortiAuthenticator integrates with FortiClient for SSOMA.

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which two statements about FortiClient EMS integration with Active Directory (AD) are true? (Choose two.)

A. FortiClient EMS has full read-write access on the AD server.

B. FortiClient installations on domain endpoints can deployed from FortiClient EMS.

C. Endpoint profiles can be assigned to endpoints based on domain groups.

D. Imported AD endpoints cannot be directly deleted on FortiClient EMS.

**Suggested Answer:** *C, D*

EMS assigns profiles by AD group; imported AD endpoints cannot be directly deleted in EMS.

*Community vote distribution*

CD (100%)

**prepengine** Most Recent 4 months, 2 weeks ago

Selected Answer: CD

C. Endpoint profiles can be assigned through endpoint policies to AD groups or AD users.

D. AD-imported endpoints are synchronized from AD through a read-only LDAP/LDAPS connection; EMS cannot modify the AD source directly, so they are not directly deleted in EMS.

upvoted 2 times

**AgentSmith** 7 months, 1 week ago

Selected Answer: CD

Using v7.4.x and later only, the correct answers are C and D.

C. Endpoint profiles can be assigned to endpoints based on domain groups. EMS endpoint policies can target device and user groups from imported domains and workgroups.

D. Imported AD endpoints cannot be directly deleted on FortiClient EMS. Fortinet states endpoint deletion in EMS is available only for non-domain devices.

Why the others are wrong:

A is false because the AD/LDAP connection is read-only, not read-write.

B is false in 7.4.x because EMS can deploy upgrades to endpoints that already have FortiClient installed, but Fortinet says you cannot deploy initial FortiClient installations to Active Directory domain-joined devices from EMS.

upvoted 1 times

Question #9 *Topic 1*

Which two statements apply to FortiClient forensics analysis? (Choose two.)

A. FortiClient sends an alert notification when malicious activity is triggered.

B. The administrator must request analysis for the desired endpoint.

C. The endpoint is quarantined until forensics is completed.

D. Forensics analysis features must be enabled in the system settings profile.

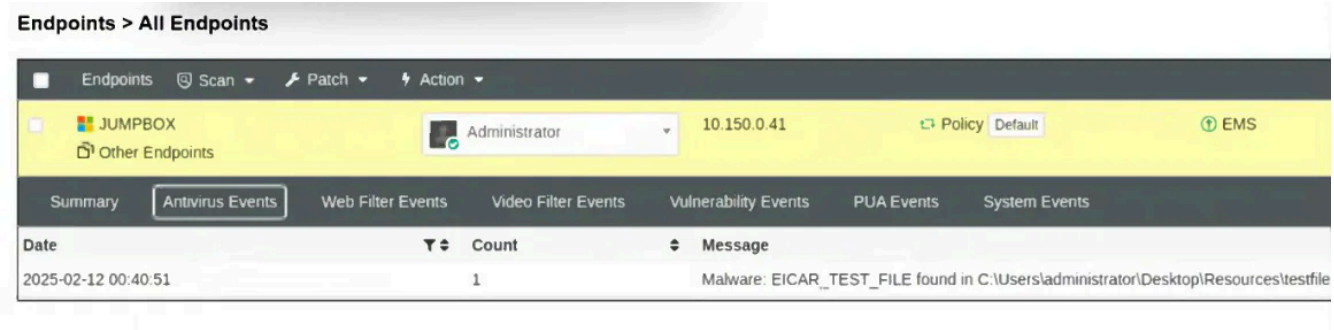
**Suggested Answer:** *A, D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Refer to the exhibit.

You provide a webserver hosting service. An endpoint downloads a test file, testfile.txt, that gets blocked by FortiClient.
Which configuration can you use to make the file accessible on the endpoint?




A. Restore access to file directly using FortiClient.

B. Allow the webserver URL in the exclusion list in the web filter profile.

C. Exclude testfile.txt from the malware protection profile.

D. Add the file to the allowlist in quarantine management on FortiClient EMS.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Which statement about deploying FortiClient EMS in an air-gapped environment is true?

A. You can generate FortiClient installers on the FortiClient EMS instance.

B. You can sync a license on the FortiClient EMS GUI using your FortiCloud account.

C. You can configure FortiClient EMS to receive updates from FortiManager.

D. You can use offline antimalware data on FortiClient EMS to operate in an air-gapped deployment.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

An administrator is configuring a zero trust network access (ZTNA) access proxy solution to share endpoint information with a FortiGate device.

Which two configuration actions will achieve this solution? (Choose two.)

A. Add the FortiGate IP address to the Fabric device configurations on FortiClient EMS.

B. Authorize FortiGate on FortiClient EMS as a Fabric connector.

C. Use the FortiClient EMS connector on FortiGate to connect to FortiClient EMS.

D. Apply the ZTNA license on FortiGate.

**Suggested Answer:** *B, C*
Authorize FortiGate as a Fabric connector and configure its EMS connector.

**AgentSmith** Most Recent 7 months, 2 weeks ago

Selected Answer: BC

FortiClient_EMS_7.4 _Administrator_Study_Guide-Online P208

You can configure the on-premises FortiClient EMS connector on FortiGate by clicking Security Fabric >

Fabric Connectors. After applying the FortiClient EMS settings, FortiGate must accept the FortiClient EMS server certificate

Next, you must authorize FortiGate on FortiClient EMS. If you log in to FortiClient EMS, a pop-up window opens, requesting you to authorize FortiGate. If you do not log in, you can click Administration > Fabric Devices, select the FortiGate device, and then authorize it

upvoted 2 times

Question #13 *Topic 1*

Refer to the exhibit.

Why is the end user denied access to twitter.com?




A. They are being blocked by the application firewall endpoint profile.

B. They are being blocked by the exclusion list in the web filter endpoint profile.

C. They are being blocked by FortiGuard categories in the web filter endpoint profile.

D. They are being blocked by the deny list in the malware protection endpoint profile.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

You are performing a proof-of-concept for a Fortinet Endpoint Protection solution.

Which endpoint should you install, in addition to FortiClient, as a part of a FortiEndpoint deployment?

A. FortiPAM

B. FortiEDR

C. FortiNAC

D. FortiMonitor

**Suggested Answer:** *B*
FortiEDR is the additional endpoint protection solution in a FortiEndpoint deployment.

**Jordancueay** Most Recent 3 months, 1 week ago

Selected Answer: B

Answer is B FortiEDR

https://docs.fortinet.com/document/fortiendpoint/latest/administration-guide/757719/introduction

upvoted 2 times