Fortinet
FCP_FAC_AD-6.5
Fortinet FCP - FortiAuthenticator 6.5 Administrator

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Latest Version: 6.0

Question: 1

When working with administrator profiles, which permission sets can be customized?
Response:

A. All permission sets can be customized.
B. Only the pre-existing permission sets can be customized.
C. Only non-administrator permission sets can be customized.
D. Only user-created or cloned permission sets can be customized.

Answer: D

Question: 2

Which FSSO discovery method makes use of service tickets to authenticate new users and validate the currently logged on users?
Response:

A. Kerberos-based FSSO
B. FortiClient SSO mobility agent
C. RADIUS accounting
D. DC polling

Answer: A

Question: 3

FortiAuthenticator has several roles that involve digital certificates. Which role allows FortiAuthenticator to receive the signed certificate signing requests (CSRs) and send certificate revocation lists (CRLs)?
Response:

A. Remote LDAP server
B. EAP server
C. SCEP server
D. OCSP server

Answer: C

Question: 4

A device that is 802.1X non-compliant must be connected to the network. Which authentication method can you use to authenticate the device with FortiAuthenticator?
Response:

A. EAP-TTLS
B. EAP-TLS
C. MAC-based authentication
D. Machine-based authentication

Answer: C

Question: 5

You are the administrator of a large network and you want to track your users by leveraging the FortiClient SSO Mobility Agent. As part of the deployment you want to make sure that a bad actor will not be allowed to authenticate with an unauthorized AD server and appear as a legitimate user when reported by the agent.
Which option can prevent such an attack?
Response:

A. Add only the trusted AD servers to a valid servers group.
B. Change the Secret key in the Enable authentication option for the FortiClient Mobility Agent Service.
C. Enable the Enable RADIUS accounting SSO clients method.
D. Enable the Enable NTLM option in the FortiClient Mobility Agent Service.

Answer: D

Question: 6

You are a network administrator with a large wireless environment. FortiAuthenticator acts as the RADIUS server for your wireless controllers. You want specific wireless controllers to authenticate users against specific realms. How would you satisfy this requirement?
Response:

A. Create Access point groups
B. Enable Adaptive Authentication
C. RADUIS policy
D. Define RADIUS clients

Answer: C

Question: 7

Which three factors can determine which RADIUS policy is matched during a RADIUS authentication?
(Choose three.)
Response:

A. Policy ranking
B. RADIUS client
C. Selected realm
D. RADIUS response
E. RADIUS attribute

Answer: A,B,E

Question: 8

What happens when a certificate is revoked?
(Choose two.)
Response:

A. Revoked certificates cannot be reinstated for any reason
B. External CAs will periodically query FortiAuthenticator and automatically download revoked certificates
C. All certificates signed by a revoked CA certificate are automatically revoked
D. Revoked certificates are automatically added to the CRL

Answer: C,D

Question: 9

When you are setting up two FortiAuthenticator devices in active-passive HA, which HA role must you select on the primary FortiAuthenticator?
Response:

A. Standalone primary
B. Cluster member
C. Active-passive primary
D. Load balancing primary

Answer: B

When revoking a certificate, which reason must be selected if you want the ability to reinstate it at a later time?
Response:

A. Unspecified
B. Operation ceased
C. On Hold
D. Superseded

Answer: C

PRODUCT FEATURES

- **100% Money Back Guarantee**
- **90 Days Free updates**
- **Special Discounts on Bulk Orders**
- **Guaranteed Success**
- **50,000 Satisfied Customers**
- **100% Secure Shopping**
- **Privacy Policy**
- **Refund Policy**

16 USD Discount Coupon Code: NB4XKTMZ