# Fortinet

## Exam Questions NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

**NEW QUESTION 1**
A system administrator wants to integrate FortiAuthenticator with an existing identity management system with the goal of authenticating and deauthenticating users into FSSO.
What feature does FortiAuthenticator offer for this type of integration?

A. The ability to import and export users from CSV files
B. RADIUS learning mode for migrating users
C. REST API
D. SNMP monitoring and traps

**Answer:** C

**Explanation:**
REST API is a feature that allows FortiAuthenticator to integrate with an existing identity management system with the goal of authenticating and deauthenticating users into FSSO. REST API stands for Representational State Transfer Application Programming Interface, which is a method of exchanging data between different systems using HTTP requests and responses. FortiAuthenticator provides a REST API that can be used by external systems to perform various actions, such as creating, updating, deleting, or querying users and groups, or sending FSSO logon or logoff events.
References: https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/rest-api

**NEW QUESTION 2**
When you are setting up two FortiAuthenticator devices in active-passive HA, which HA role must you select on the master FortiAuthenticator?

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

**Answer:** A

**Explanation:**
When you are setting up two FortiAuthenticator devices in active-passive HA, you need to select the
active-passive master role on the master FortiAuthenticator device. This role means that the device will handle all requests and synchronize data with the slave device until a failover occurs. The slave device must be configured as an active-passive slave role. The other roles are used for different HA modes, such as standalone (no HA), cluster (active-active), or load balancing (active-active with load balancing). References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372411/high-availability

**NEW QUESTION 3**
Which two capabilities does FortiAuthenticator offer when acting as a self-signed or local CA? (Choose two)

A. Validating other CA CRLs using OSCP
B. Importing other CA certificates and CRLs
C. Merging local and remote CRLs using SCEP
D. Creating, signing, and revoking of X.509 certificates

**Answer:** BD

**Explanation:**
FortiAuthenticator can act as a self-signed or local CA that can issue certificates to users, devices, or other CAs. It can also import other CA certificates and CRLs to trust them and validate their certificates. It can also create, sign, and revoke X.509 certificates for various purposes, such as VPN authentication, web server encryption, or wireless security. It cannot validate other CA CRLs using OCSP or merge local and remote CRLs using SCEP because these are protocols that require communication with external CAs. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management

**NEW QUESTION 4**
Which two statement about the RADIUS service on FortiAuthenticator are true? (Choose two)

A. Two-factor authentication cannot be enforced when using RADIUS authentication
B. RADIUS users can migrated to LDAP users
C. Only local users can be authenticated through RADIUS
D. FortiAuthenticator answers only to RADIUS client that are registered with FortiAuthenticator

**Answer:** BD

**Explanation:**
Two statements about the RADIUS service on FortiAuthenticator are true:
➢ RADIUS users can be migrated to LDAP users using the RADIUS learning mode feature. This feature allows FortiAuthenticator to learn user credentials from an existing RADIUS server and store them locally as LDAP users for future authentication requests.
➢ FortiAuthenticator answers only to RADIUS clients that are registered with FortiAuthenticator. A RADIUS client is a device that sends RADIUS authentication or accounting requests to FortiAuthenticator. A RADIUS client must be added and configured on FortiAuthenticator before it can communicate with it.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/radius-service

**NEW QUESTION 5**
A digital certificate, also known as an X.509 certificate, contains which two pieces of information? (Choose two.)

A. Issuer

B. Shared secret
C. Public key
D. Private key

**Answer:** AC

**Explanation:**
A digital certificate, also known as an X.509 certificate, contains two pieces of information:
➢ Issuer, which is the identity of the certificate authority (CA) that issued the certificate
➢ Public key, which is the public part of the asymmetric key pair that is associated with the certificate subject
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management

**NEW QUESTION 6**
Which statement about the guest portal policies is true?

A. Guest portal policies apply only to authentication requests coming from unknown RADIUS clients
B. Guest portal policies can be used only for BYODs
C. Conditions in the policy apply only to guest wireless users
D. All conditions in the policy must match before a user is presented with the guest portal

**Answer:** D

**Explanation:**
Guest portal policies are rules that determine when and how to present the guest portal to users who want to access the network. Each policy has a set of conditions that can be based on various factors, such as the source IP address, MAC address, RADIUS client, user agent, or SSID. All conditions in the policy must match before a user is presented with the guest portal. Guest portal policies can apply to any authentication request coming from any RADIUS client, not just unknown ones. They can also be used for any type of device, not just BYODs. They can also apply to wired or VPN users, not just wireless users. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management/37240

**NEW QUESTION 7**
You are the administrator of a global enterprise with three FortiAuthenticator devices. You would like to deploy them to provide active-passive HA at headquarters, with geographically distributed load balancing.
What would the role settings be?

A. One standalone and two load balancersB One standalone primary, one cluster member, and one load balancer
B. Two cluster members and one backup
C. Two cluster members and one load balancer

**Answer:** B

**Explanation:**
To deploy three FortiAuthenticator devices to provide active-passive HA at headquarters, with geographically distributed load balancing, the role settings would be:
➢ One standalone primary, which acts as the master device for HA and load balancing
➢ One cluster member, which acts as the backup device for HA and load balancing
➢ One load balancer, which acts as a remote device that forwards authentication requests to the primary or cluster member device
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/high-availability#ha-an

**NEW QUESTION 8**
Which interface services must be enabled for the SCEP client to connect to Authenticator?

A. OCSP
B. REST API
C. SSH
D. HTTP/HTTPS

**Answer:** D

**Explanation:**
HTTP/HTTPS are the interface services that must be enabled for the SCEP client to connect to FortiAuthenticator. SCEP stands for Simple Certificate Enrollment Protocol, which is a method of requesting and issuing digital certificates over HTTP or HTTPS. FortiAuthenticator supports SCEP as a certificate authority (CA) and can process SCEP requests from SCEP clients. To enable SCEP on FortiAuthenticator, the HTTP or HTTPS service must be enabled on the interface that receives the SCEP requests.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/certificate-management

**NEW QUESTION 9**
Which option correctly describes an SP-initiated SSO SAML packet flow for a host without a SAML assertion?

A. Service provider contacts idendity provider, idendity provider validates principal for service provider, service provider establishes communication with principal
B. Principal contacts idendity provider and is redirected to service provider, principal establishes connection with service provider, service provider validates authentication with identify provider
C. Principal contacts service provider, service provider redirects principal to idendity provider, after succesfull authentication identify provider redirects principal to service provider
D. Principal contacts idendity provider and authenticates, identity provider relays principal to service provider after valid authentication

**Answer:** C

**Explanation:**
SP-initiated SSO SAML packet flow for a host without a SAML assertion is as follows:

- Principal contacts service provider, requesting access to a protected resource.
- Service provider redirects principal to identity provider, sending a SAML authentication request.
- Principal authenticates with identity provider using their credentials.
- After successful authentication, identity provider redirects principal back to service provider, sending a SAML response with a SAML assertion containing the principal’s attributes.
- Service provider validates the SAML response and assertion, and grants access to the principal.

References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/saml-service-provider#

**NEW QUESTION 10**
Which behaviors exist for certificate revocation lists (CRLs) on FortiAuthenticator? (Choose two)

A. CRLs contain the serial number of the certificate that has been revoked
B. Revoked certificates are automaticlly placed on the CRL
C. CRLs can be exported only through the SCEP server
D. All local CAs share the same CRLs

**Answer:** AB

**Explanation:**
CRLs are lists of certificates that have been revoked by the issuing CA and should not be trusted by any entity. CRLs contain the serial number of the certificate that has been revoked, the date and time of revocation, and the reason for revocation. Revoked certificates are automatically placed on the CRL by the CA and the CRL is updated periodically. CRLs can be exported through various methods, such as HTTP, LDAP, or SCEP. Each local CA has its own CRL that is specific to its issued certificates. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management/3

**NEW QUESTION 10**
......