Actual exam question from Fortinet's NSE6_FAC-6.1
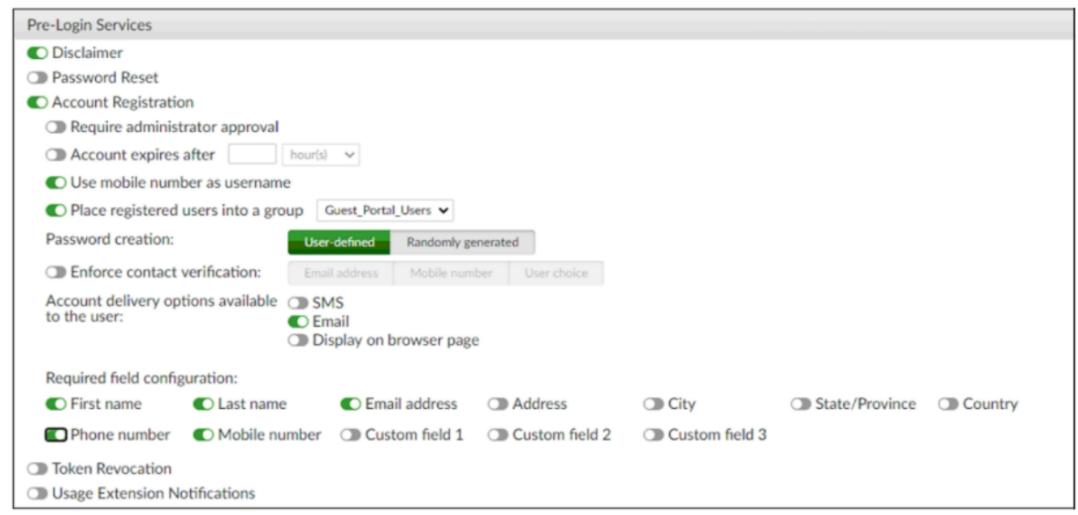
Question #: 1

Topic #: 1

[All NSE6_FAC-6.1 Questions]

A device or user identity cannot be established transparently, such as with non-domain BYOD devices, and allow users to create their own credentials.

In this case, which user identity discovery method can FortiAuthenticator use?

A. RADIUS accounting

B. Kerberos-based authentication

C. Portal authentication

D. Syslog messaging or SAMI IdP

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 2

Topic #: 1

[All NSE6_FAC-6.1 Questions]

What are three key features of FortiAuthenticator? (Choose three.)

    A. RSSO server

    B. Log server

    C. Portal services

    D. Certificate authority

    E. Identity management device

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

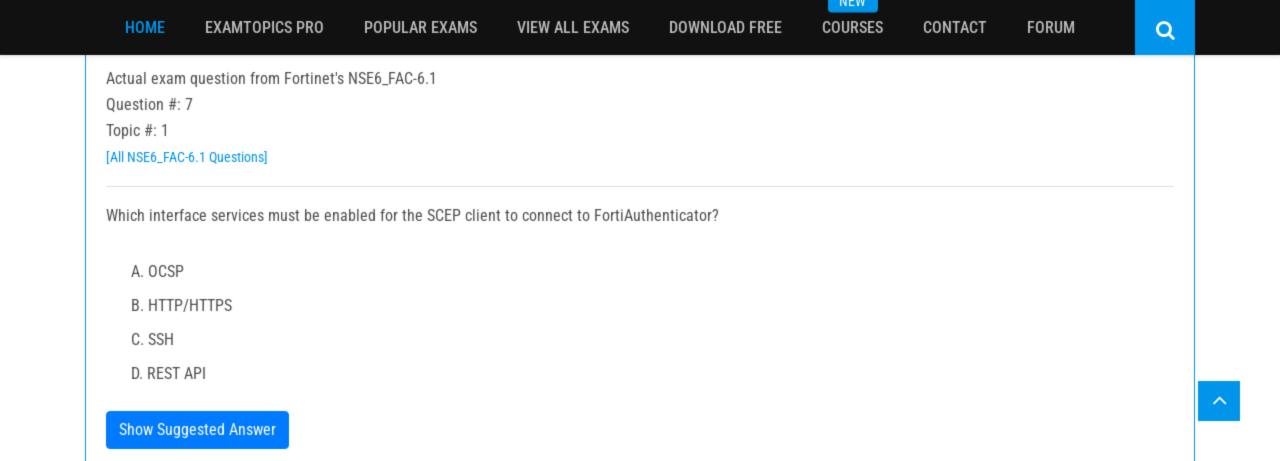Question #: 3

Topic #: 1

[All NSE6_FAC-6.1 Questions]

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

A. Merging local and remote CRLs using SCEP

B. Creating, signing, and revoking of X.509 certificates

C. Validating other CA CRLs using OCSP

D. Importing other CA certificates and CRLs

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 4

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which two are supported captive or guest portal authentication methods? (Choose two.)

A. LinkedIn

B. Email

C. Apple ID

D. Instagram

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 5

Topic #: 1

[All NSE6_FAC-6.1 Questions]

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

A. External CAs will periodically query FortiAuthenticator and automatically download revoked certificates

B. Revoked certificates are automatically added to the CRL

C. All certificates signed by a revoked CA certificate are automatically revoked

D. Revoked certificates cannot be reinstated for any reason

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 6

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Refer to the exhibit.

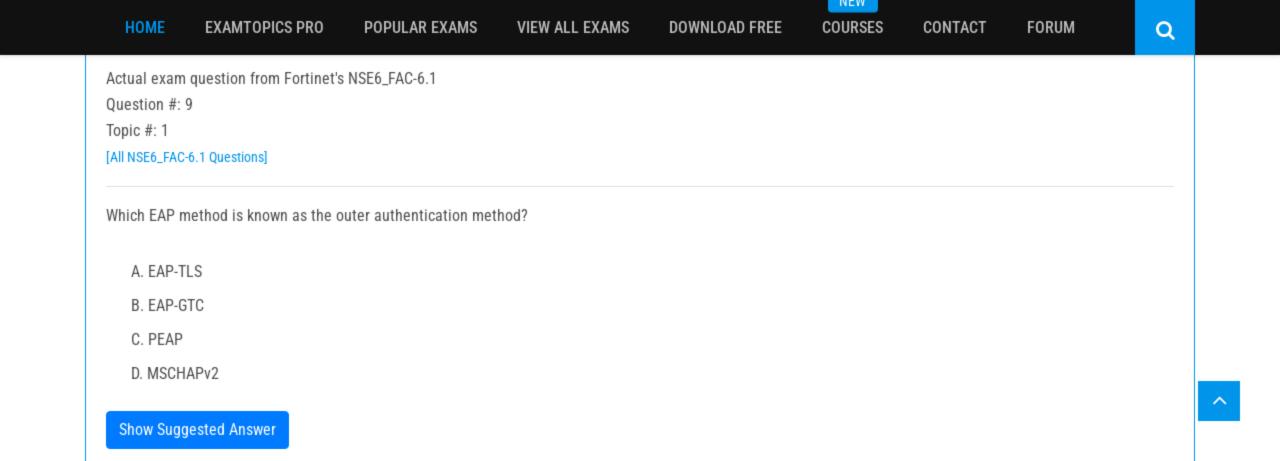Examine the screenshot shown in the exhibit.

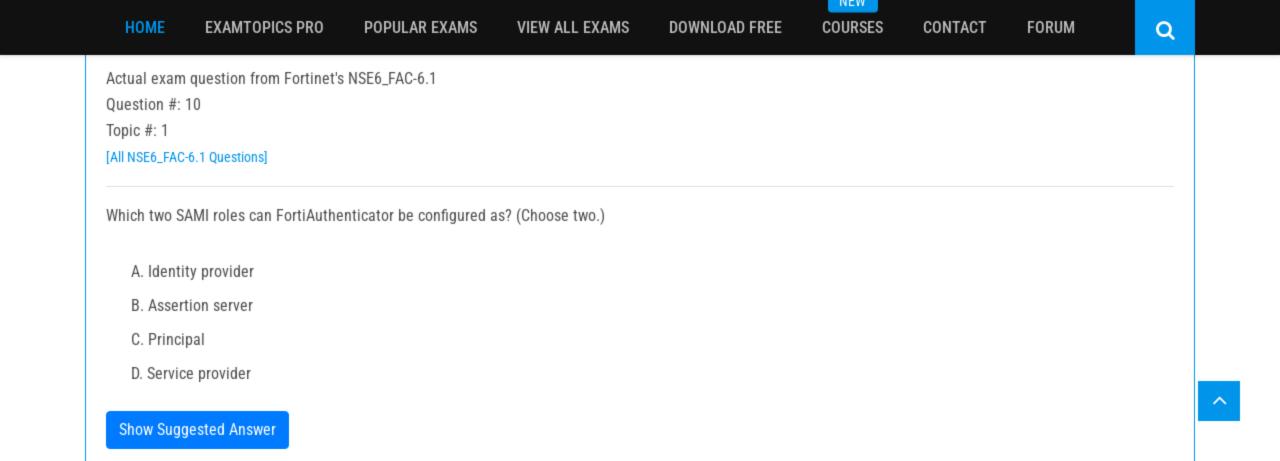Which two statements regarding the configuration are true? (Choose two.)

A. Guest user account will expire after eight hours.

B. All guest accounts created using the account registration feature will be placed under the Guest_Portal_Users group.

C. Guest users must fill in all the fields on the registration form.

D. All accounts registered through the guest portal must be validated through email.

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 7

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which interface services must be enabled for the SCEP client to connect to FortiAuthenticator?

A. OCSP

B. HTTP/HTTPS

C. SSH

D. REST API

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 8

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which two statements about the EAP-TTLS authentication method are true? (Choose two.)

A. Supports a port access control (wired) solution only

B. Uses digital certificates only on the server side

C. Uses mutual authentication

D. Requires an EAP server certificate

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 9

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which EAP method is known as the outer authentication method?

A. EAP-TLS

B. EAP-GTC

C. PEAP

D. MSCHAPv2

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 10

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which two SAMI roles can FortiAuthenticator be configured as? (Choose two.)

A. Identity provider

B. Assertion server

C. Principal

D. Service provider

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 11

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which two types of digital certificates can you create in FortiAuthenticator? (Choose two.)

    A. Organization validation certificate

    B. User certificate

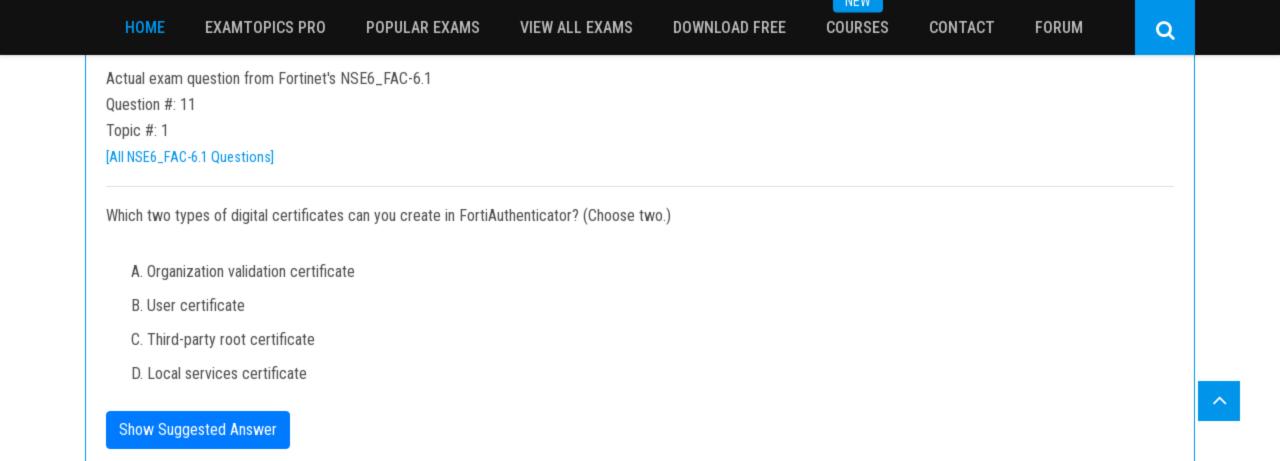   C. Third-party root certificate

    D. Local services certificate

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 12

Topic #: 1

[All NSE6_FAC-6.1 Questions]

You are a FortiAuthenticator administrator for a large organization. Users who are configured to use FortiToken 200 for two-factor authentication can no longer authenticate. You have verified that only the users with two-factor authentication are experiencing the issue.
What can cause this issue?

    A. FortiAuthenticator has lost contact with the FortiToken Cloud servers

    B. Time drift between FortiAuthenticator and hardware tokens

    C. One of the FortiAuthenticator devices in the active-active cluster has failed
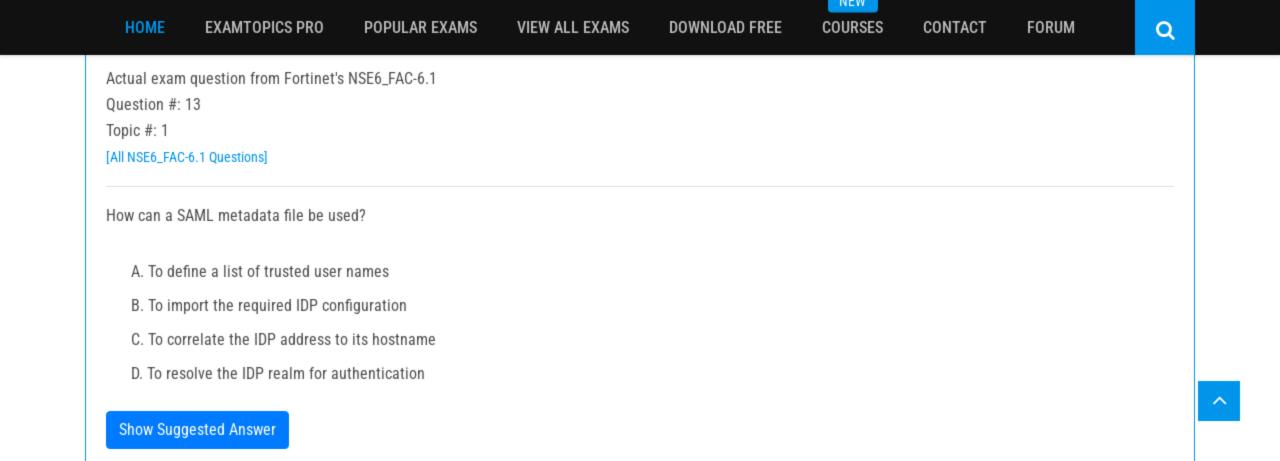
    D. FortiToken 200 license has expired

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 13

Topic #: 1

[All NSE6_FAC-6.1 Questions]

How can a SAML metadata file be used?

    A. To define a list of trusted user names

    B. To import the required IDP configuration

    C. To correlate the IDP address to its hostname

    D. To resolve the IDP realm for authentication

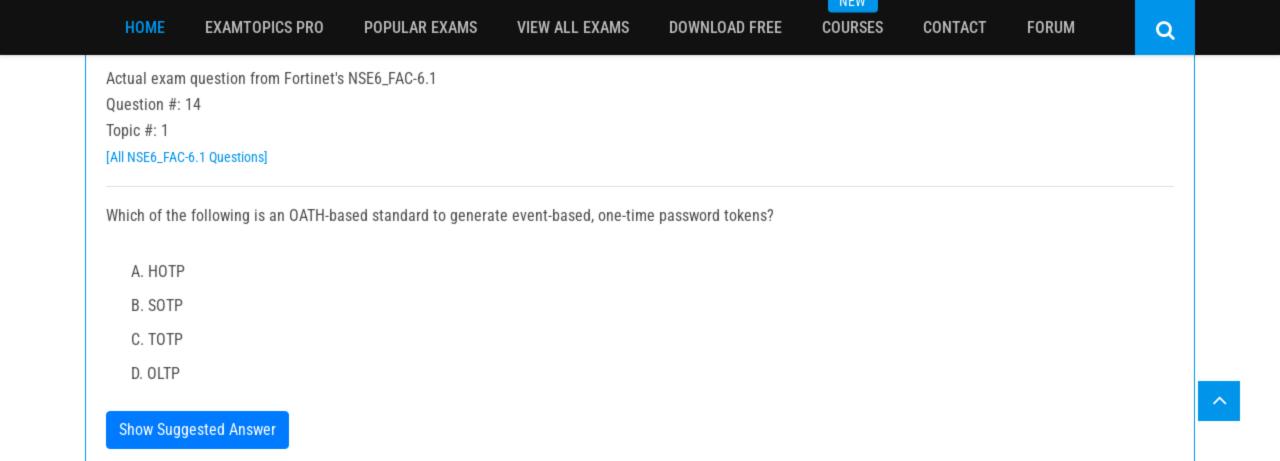**Show Suggested Answer**

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 14

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which of the following is an OATH-based standard to generate event-based, one-time password tokens?

A. HOTP

B. SOTP

C. TOTP

D. OLTP

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 15

Topic #: 1

[All NSE6_FAC-6.1 Questions]

You are a Wi-Fi provider and host multiple domains. How do you delegate user accounts, user groups and permissions per domain when they are authenticating on a single FortiAuthenticator device?

A. Create realms

B. Create multiple directory trees on FortiAuthenticator

C. Automatically import hosts from each domain as they authenticate

D. Create user groups

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 16

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which option correctly describes an SP-Initiated SSO SAMI packet flow for a host without a SAML assertion?

A. Service provider contacts identity provider, identity provider validates principal for service provider, service provider establishes communication with principal

B. Principal contacts service provider, service provider redirects principal to identity provider, after successful authentication identity provider redirects principal to service provider

C. Principal contacts identity provider and authenticates, identity provider relays principal to service provider after valid authentication

D. Principal contacts identity provider and is redirected to service provider, principal establishes connection with service provider, service provider validates authentication with Identity provider

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 17

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which two statements about the RADIUS service on FortiAuthenticator are true? (Choose two.)

A. FortiAuthenticator answers only to RADIUS clients that are registered with FortiAuthenticator

B. RADIUS users can be migrated to LDAP users

C. Only Local users can be authenticated through RADIUS

D. Two-factor authentication cannot be enforced when using RADIUS authentication

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 18

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which FSSO discovery method transparently detects logged off users without having to rely on external features such as WMI polling?

A. RADIUS accounting

B. DC polling

C. FortiClient SSO mobility agent

D. Windows AD polling

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 19

Topic #: 1

[All NSE6_FAC-6.1 Questions]

Which three of the following can be used as SSO sources? (Choose three.)

    A. FortiClient SSO Mobility Agent

    B. RADIUS accounting

    C. FortiGate

    D. FortiAuthenticator in SAML SP role

    E. SSH sessions

Show Suggested Answer

Actual exam question from Fortinet's NSE6_FAC-6.1

Question #: 20

Topic #: 1

[All NSE6_FAC-6.1 Questions]

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. Load balancing master

    C. Standalone master

    D. Cluster member

Show Suggested Answer