EXAMTOPICS

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



CERTIFICATION TEST

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

Question #1 *Topic 1*

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

Suggested Answer: *C*

mmelo 3 years, 7 months ago
C is correct
upvoted 4 times

nm1122 Most Recent 3 years, 6 months ago
C is the answer
upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *A, D, E*

mszacilowski Highly Voted 3 years, 9 months ago

Correct answers: CDE. FortiAuthenticator_6.4_Study_Guide page 13: FortiAuthenticator is a user authentication and identity management device. Some of the key features include: two-factor authentication, wired or wireless authentication using the 802.1X standard, certificate management, portal services, and Fortinet single sign-on (FSSO).

upvoted 8 times

python_tamer Highly Voted 3 years, 8 months ago

Selected Answer: CDE

Yep - CDE

upvoted 6 times

PhoenixJames Most Recent 3 years, 4 months ago

Selected Answer: CDE

FortiAuthenticator_6.4_Study_Guide page 13

upvoted 1 times

mmelo 3 years, 7 months ago

C, D and E are correct

upvoted 4 times

Question #3 *Topic 1*

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

Suggested Answer: *B, D*

Artbrut Most Recent 2 years, 6 months ago

Selected Answer: BD

Study guide 6.5 from p. 328 on

upvoted 1 times

mai340 3 years, 2 months ago

A,B pg 344 Study_Guide

upvoted 1 times

mmelo 3 years, 7 months ago

B and D is correct

upvoted 4 times

Question #4 *Topic 1*

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

A. LinkedIn

B. Email

C. Apple ID

D. Instagram

Suggested Answer: *A, B*

PhoenixJames Most Recent 3 years, 4 months ago

Selected Answer: AB

A&B - LinkedIn: https://docs.fortinet.com/document/fortiauthenticator/5.5.0/cookbook/399729/social-wifi-captive-portal

upvoted 1 times

engel 3 years, 4 months ago

B. Email: FortiAuthenticator can send an email message to guests that contains a temporary username and password. The guest can use these credentials to authenticate to the captive or guest portal and access the network resources.

C. Apple ID: FortiAuthenticator can authenticate guests using their Apple ID credentials. This allows guests to use their existing Apple ID account to access the network resources.

Therefore, options B and C are the supported captive or guest portal authentication methods in FortiAuthenticator. Note that LinkedIn and Instagram are not supported authentication methods for captive or guest portals.

upvoted 1 times

nm1122 3 years, 6 months ago

A & B are correct

upvoted 1 times

mmelo 3 years, 7 months ago

A and B is correct

upvoted 4 times

Question #5 *Topic 1*

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

Suggested Answer: *A, B*

k3rnelpanicpj Highly Voted 3 years, 6 months ago

Selected Answer: BC

Validate with Fortinet Sample Questions: B&C

upvoted 7 times

nm1122 Most Recent 3 years, 6 months ago

B & C are correct.

upvoted 3 times

python_tamer 3 years, 8 months ago

Selected Answer: BC

Correct answer is: B & C

upvoted 3 times

mszacilowski 3 years, 9 months ago

My mistake, correst answers are: A & C. This specific question is one of the sample questions on fortinet training portal and those two are correct.

upvoted 2 times

mszacilowski 3 years, 9 months ago

B & C... definitely B & C. "A" was a typo.

upvoted 3 times

mszacilowski 3 years, 9 months ago

Answer: B & D

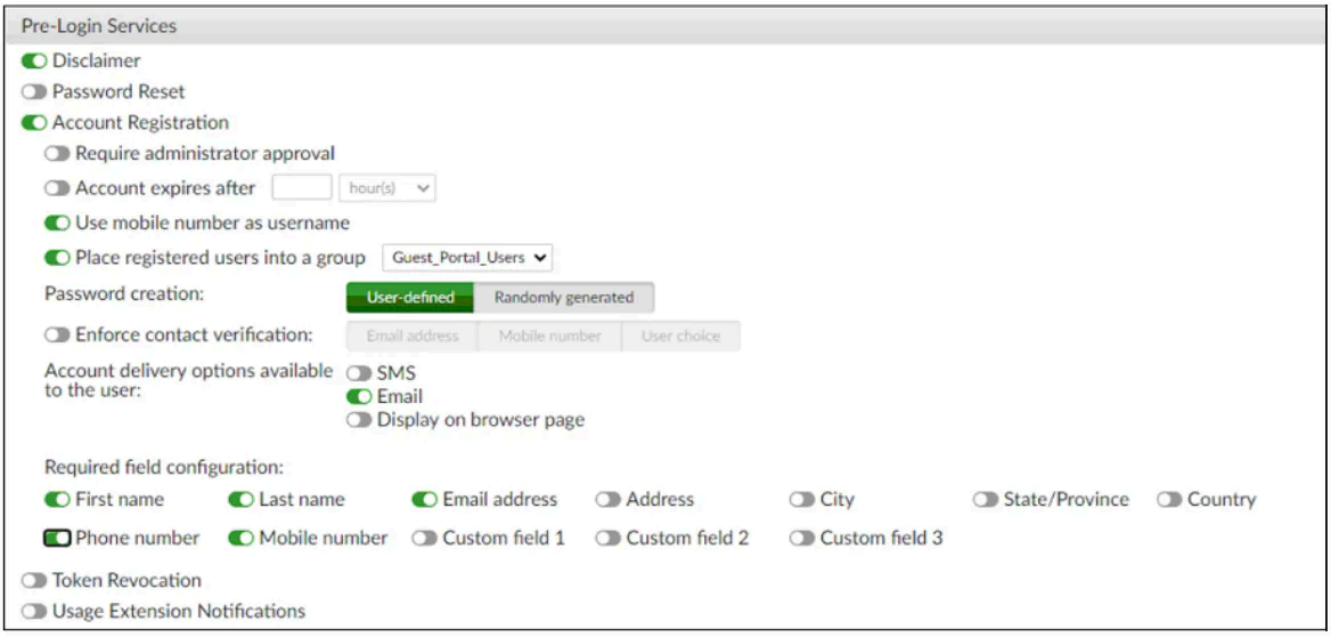
upvoted 3 times

Question #6 *Topic 1*

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.

Suggested Answer: *B, D*

mai340 Most Recent 3 years, 2 months ago

B and C is coorect. it´s no necessary any validation by email.

upvoted 1 times

paulhack 3 years, 4 months ago

B/C correct answer

upvoted 2 times

nm1122 3 years, 6 months ago

B & D. clearly stated.

upvoted 2 times

mordechayd 3 years, 6 months ago

Selected Answer: BD

according to t=study guide page 279

upvoted 1 times

Question #7 *Topic 1*

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

A. OCSP

B. HTTP/HTTPS

C. SSH

D. REST API

Suggested Answer: *B*

engel Most Recent 3 years, 4 months ago

option B is the interface service that must be enabled for the SCEP client to connect to FortiAuthenticator. Note that options A, C, and D are not required for the SCEP client to connect.

upvoted 2 times

Question #8 *Topic 1*

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

Suggested Answer: *B, D*

Artbrut Most Recent 2 years, 6 months ago

Selected Answer: BD

Hvae to correct myself, think it´s B and D. You need an EAP server certificate, and opposite to EAP-TLS, EAP-TTLS only uses server side certificates. EAP-TLS uses also client-side certificates = mutual authentication

upvoted 1 times

Artbrut 2 years, 6 months ago

Selected Answer: BC

https://docs.fortinet.com/document/fortiauthenticator/6.6.0/administration-guide/125951/extensible-authentication-protocol

upvoted 1 times

Shamrock 3 years, 5 months ago

B & C reference: rfc-editor.org/rfc/rfc5281 reference: globalreachtech.com/why-eap-ttls/

upvoted 3 times

faeem 3 years, 6 months ago

I think it is B and D.

EAP-TTLS/PAP uses Cleartext Credentials EAP-TTLS/PAP is a credential-based authentication protocol that was initially designed to make the setup more accessible by requiring only the server to be authenticated, with client authentication being optional. Here, the credentials are delivered over the air in “clear text,” which means they are not encrypted and may be deciphered easily.

upvoted 1 times

theklee 3 years, 6 months ago

B and C. It's mutual authentication but the client isn't using cert auth. EAP-TTLS (or tunneled transport layer security) extends the TLS protocol. It uses digital certificates on the server side only. After the server is securely authenticated to the client, it uses the tunnel (the secure connection) to authenticate the client. P. 381

upvoted 3 times

Question #9 *Topic 1*

Which EAP method is known as the outer authentication method?

A. EAP-TLS

B. EAP-GTC

C. PEAP

D. MSCHAPv2

Suggested Answer: *C*

ThatWhyImHere Most Recent 3 years, 7 months ago

PEAP - 6.4 Study Guide Page 381

upvoted 4 times

Question #10 *Topic 1*

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

A. Identity provider

B. Assertion server

C. Principal

D. Service provider

Suggested Answer: *A, D*

nm1122 3 years, 6 months ago

SAML.. A & D are correct.

upvoted 3 times

nm1122 Most Recent 3 years, 6 months ago

https://docs.fortinet.com/document/fortigate/6.2.0/new-features/164358/saml-sso

upvoted 1 times

ThatWhyImHere 3 years, 7 months ago

IdP and SP are correct -

upvoted 1 times

Question #11 *Topic 1*

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

Suggested Answer: *B, D*

engel Most Recent 3 years, 4 months ago

B. User certificate: A user certificate is a digital certificate that is issued to a user and used for authentication and/or encryption purposes.

D. Local services certificate: A local services certificate is a digital certificate that is used to secure services provided by FortiAuthenticator, such as the web-based manager, the REST API, and the SCEP server.

Therefore, options B and D are the two types of digital certificates that can be created in FortiAuthenticator. Options A and C are not valid certificate types that can be created in FortiAuthenticator.

upvoted 2 times