Fortinet

Exam Questions NSE6_FAC-6.4

Fortinet NSE 6 - FortiAuthenticator 6.4

NEW QUESTION 1
At a minimum, which two configurations are required to enable guest portal services on FortiAuthenticator? (Choose two)

A. Configuring a portal policy
B. Configuring at least on post-login service
C. Configuring a RADIUS client
D. Configuring an external authentication portal

Answer: AB

Explanation:
enable guest portal services on FortiAuthenticator, you need to configure a portal policy that defines the conditions for presenting the guest portal to users and the authentication methods to use. You also need to configure at least one post-login service that defines what actions to take after a user logs in successfully, such as sending an email confirmation, assigning a VLAN, or creating a user account. Configuring a RADIUS client or an external authentication portal are optional steps that depend on your network setup and requirements. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management

NEW QUESTION 2
Which three of the following can be used as SSO sources? (Choose three)

A. FortiClient SSO Mobility Agent
B. SSH Sessions
C. FortiAuthenticator in SAML SP role
D. Fortigate
E. RADIUS accounting

Answer: ADE

Explanation:
FortiAuthenticator supports various SSO sources that can provide user identity information to other devices in the network, such as FortiGate firewalls or FortiAnalyzer log servers. Some of the supported SSO sources are:

- FortiClient SSO Mobility Agent: A software agent that runs on Windows devices and sends user login information to FortiAuthenticator.
- FortiGate: A firewall device that can send user login information from various sources, such as FSSO agents, captive portals, VPNs, or LDAP servers, to FortiAuthenticator.
- RADIUS accounting: A protocol that can send user login information from RADIUS servers or clients, such as wireless access points or VPN concentrators, to FortiAuthenticator.

SSH sessions and FortiAuthenticator in SAML SP role are not valid SSO sources because they do not provide user identity information to other devices in the network. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372410/single-sign-on

NEW QUESTION 3
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 4
You are an administrator for a large enterprise and you want to delegate the creation and management of guest users to a group of sponsors.
How would you associate the guest accounts with individual sponsors?

A. As an administrator, you can assign guest groups to individual sponsors.
B. Guest accounts are associated with the sponsor that creates the guest account.
C. You can automatically add guest accounts to groups associated with specific sponsors.
D. Select the sponsor on the guest portal, during registration.

Answer: B

Explanation:
Guest accounts are associated with the sponsor that creates the guest account. A sponsor is a user who has permission to create and manage guest accounts on behalf of other users3. A sponsor can create guest accounts using the sponsor portal or the REST API3. The sponsor’s username is recorded as a field in the guest account’s profile3.
References: 3 https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/guest

NEW QUESTION 5

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

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

Answer: BC

Explanation:
When a certificate is revoked, it means that it is no longer valid and should not be trusted by any entity. Revoked certificates are automatically added to the certificate revocation list (CRL) which is published by the issuing CA and can be checked by other parties. If a CA certificate is revoked, all certificates signed by that CA are also revoked and added to the CRL. Revoked certificates can be reinstated if the reason for revocation is resolved, such as a compromised private key being recovered or a misissued certificate being corrected. External CAs do not query FortiAuthenticator for revoked certificates, but they can use protocols such as SCEP or OCSP to exchange certificate information with FortiAuthenticator. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372408/certificate-management

NEW QUESTION 6
At a minimum, which two configurations are required to enable guest portal services on FortiAuthenticator? (Choose two)

A. Configuring a portal policy
B. Configuring at least on post-login service
C. Configuring a RADIUS client
D. Configuring an external authentication portal

Answer: AB

Explanation:
To enable guest portal services on FortiAuthenticator, you need to configure a portal policy that defines the conditions for presenting the guest portal to users and the authentication methods to use. You also need to configure at least one post-login service that defines what actions to take after a user logs in successfully, such as sending an email confirmation, assigning a VLAN, or creating a user account. Configuring a RADIUS client or an external authentication portal are optional steps that depend on your network setup and requirements. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372404/guest-management

NEW QUESTION 7
You are the administrator of a large network that includes a large local user datadabase on the current Fortiauthenticatior. You want to import all the local users into a new Fortiauthenticator device.
Which method should you use to migrate the local users?

A. Import users using RADIUS accounting updates.
B. Import the current directory structure.
C. Import users from RADUIS.
D. Import users using a CSV file.

Answer: D

Explanation:
The best method to migrate local users from one FortiAuthenticator device to another is to export the users from the current device as a CSV file and then import the CSV file into the new device. This method preserves all the user attributes and settings and allows you to modify them if needed before importing. The other methods are not suitable for migrating local users because they either require an external RADIUS server or do not transfer all the user information. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372409/user-management

NEW QUESTION 8
You have implemented two-factor authentication to enhance security to sensitive enterprise systems. How could you bypass the need for two-factor authentication for users accessing form specific secured
networks?

A. Create an admin realm in the authentication policy
B. Specify the appropriate RADIUS clients in the authentication policy
C. Enable Adaptive Authentication in the portal policy
D. Enable the Resolve user geolocation from their IP address option in the authentication policy.

Answer: C

Explanation:
Adaptive Authentication is a feature that allows administrators to bypass the need for two-factor authentication for users accessing from specific secured networks. Adaptive Authentication uses geolocation information from IP addresses to determine whether a user is accessing from a trusted network or not. If the user is accessing from a trusted network, FortiAuthenticator can skip the second factor of authentication and grant access based on the first factor only.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/authentication-policies

NEW QUESTION 9
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

Answer: A

NEW QUESTION 10
When configuring syslog SSO, which three actions must you take, in addition to enabling the syslog SSO method? (Choose three.)

A. Enable syslog on the FortiAuthenticator interface.
B. Define a syslog source.
C. Select a syslog rule for message parsing.
D. Set the same password on both the FortiAuthenticator and the syslog server.
E. Set the syslog UDP port on FortiAuthenticator.

Answer: BCE

Explanation:
To configure syslog SSO, three actions must be taken, in addition to enabling the syslog SSO method:
- Define a syslog source, which is a device that sends syslog messages to FortiAuthenticator containing user logon or logoff information.
- Select a syslog rule for message parsing, which is a predefined or custom rule that defines how to extract the user name, IP address, and logon or logoff action from the syslog message.
- Set the syslog UDP port on FortiAuthenticator, which is the port number that FortiAuthenticator listens on for incoming syslog messages.

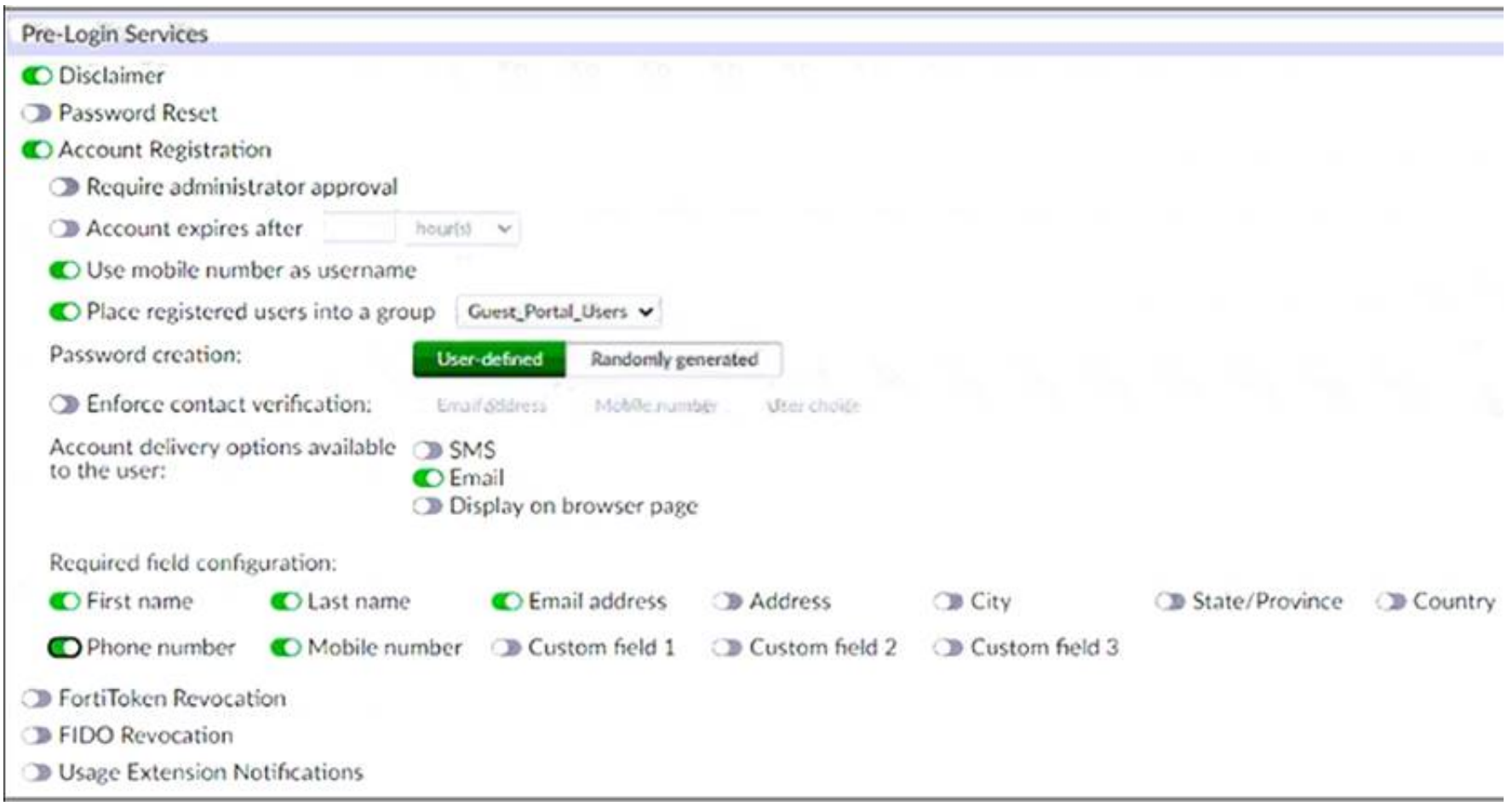
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/single-sign-on#syslog-s

NEW QUESTION 10
A device or user identity cannot be established transparently, such as with non-domain BYOD devices, and allow users to create their own credentialis.
In this case, which user idendity discovery method can Fortiauthenticator use?

A. Syslog messaging or SAML IDP
B. Kerberos-base authentication
C. Radius accounting
D. Portal authentication

Answer: D

Explanation:
Portal authentication is a user identity discovery method that can be used when a device or user identity cannot be established transparently, such as with non-domain BYOD devices, and allow users to create their own credentials. Portal authentication requires users to enter their credentials on a web page before accessing network resources. The other methods are used for transparent identification of domain devices or users. References:
https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372406/user-identity-discovery
Examine the screenshot shown in the exhibit.



NEW QUESTION 13
Which two features of FortiAuthenticator are used for EAP deployment? (Choose two)

A. Certificate authority
B. LDAP server
C. MAC authentication bypass
D. RADIUS server

Answer: AD

Explanation:

Two features of FortiAuthenticator that are used for EAP deployment are certificate authority and RADIUS server. Certificate authority allows FortiAuthenticator to issue and manage digital certificates for EAP methods that require certificate-based authentication, such as EAP-TLS or PEAP-EAP-TLS. RADIUS server allows FortiAuthenticator to act as an authentication server for EAP methods that use RADIUS as a transport protocol, such as EAP-GTC or PEAP-MSCHAPV2.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/wireless-802-1x-authen

NEW QUESTION 17
Which method is the most secure way of delivering FortiToken data once the token has been seeded?

A. Online activation of the tokens through the FortiGuard network
B. Shipment of the seed files on a CD using a tamper-evident envelope
C. Using the in-house token provisioning tool
D. Automatic token generation using FortiAuthenticator

Answer: A

Explanation:
Online activation of the tokens through the FortiGuard network is the most secure way of delivering FortiToken data once the token has been seeded because it eliminates the risk of seed files being compromised during transit or storage. The other methods involve physical or manual delivery of seed files which can be intercepted, lost, or stolen. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372403/fortitoken

NEW QUESTION 22
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. FortiToken 200 license has expired
B. One of the FortiAuthenticator devices in the active-active cluster has failed
C. Time drift between FortiAuthenticator and hardware tokens
D. FortiAuthenticator has lost contact with the FortiToken Cloud servers

Answer: C

Explanation:
One possible cause of the issue is time drift between FortiAuthenticator and hardware tokens. Time drift occurs when the internal clocks of FortiAuthenticator and hardware tokens are not synchronized. This can result in mismatched one-time passwords (OTPs) generated by the hardware tokens and expected by FortiAuthenticator. To prevent this issue, FortiAuthenticator provides a time drift tolerance option that allows a certain number of seconds of difference between the clocks.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/two-factor-authenticati

NEW QUESTION 24
Which statement about the assignment of permissions for sponsor and administrator accounts is true?

A. Only administrator accounts permissions are assigned using admin profiles.
B. Sponsor permissions are assigned using group settings.
C. Administrator capabilities are assigned by applying permission sets to admin groups.
D. Both sponsor and administrator account permissions are assigned using admin profiles.

Answer: D

Explanation:
Both sponsor and administrator account permissions are assigned using admin profiles. An admin profile is a set of permissions that defines what actions an administrator or a sponsor can perform on FortiAuthenticator. An admin profile can be assigned to an admin group or an individual admin user. A sponsor is a special type of admin user who can create and manage guest accounts on behalf of other users.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/administrators#admin-p

NEW QUESTION 28
Which two statements about the self-service portal are true? (Choose two)

A. Self-registration information can be sent to the user through email or SMS
B. Realms can be used to configure which seld-registered users or groups can authenticate on the network
C. Administrator approval is required for all self-registration
D. Authenticating users must specify domain name along with username

Answer: AB

Explanation:
Two statements about the self-service portal are true:
- Self-registration information can be sent to the user through email or SMS using the notification templates feature. This feature allows administrators to customize the messages that are sent to users when they register or perform other actions on the self-service portal.
- Realms can be used to configure which self-registered users or groups can authenticate on the network using the realm-based authentication feature. This feature allows administrators to apply different authentication policies and settings to different groups of users based on their realm membership.

References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/user-management#self-
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/user-management#real

NEW QUESTION 31
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 35
Which statement about captive portal policies is true, assuming a single policy has been defined?

A. All conditions in the policy must match before a user is presented with the captive portal.
B. Conditions in the policy apply only to wireless users.
C. Portal policies can be used only for BYODs.

Answer: B

Explanation:
Captive portal policies are used to define the conditions and settings for presenting a captive portal to users who need to authenticate before accessing the network. A captive portal policy consists of a set of conditions and a set of actions. The conditions can be based on various attributes, such as source IP address, MAC address, user group, device type, or RADIUS client. The actions can include redirecting the user to a specific portal, applying a specific authentication method, or assigning a specific VLAN or firewall policy. A single policy can have multiple conditions, and all conditions in the policy must match before a user is presented with the captive portal.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/portal-services#captive

NEW QUESTION 36
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 41
Which method is the most secure way of delivering FortiToken data once the token has been seeded?

A. Online activation of the tokens through the FortiGuard network
B. Shipment of the seed files on a CD using a tamper-evident envelope
C. Using the in-house token provisioning tool
D. Automatic token generation using FortiAuthenticator

Answer: A

Explanation:
Online activation of the tokens through the FortiGuard network is the most secure way of delivering FortiToken data once the token has been seeded because it eliminates the risk of seed files being compromised during transit or storage. The other methods involve physical or manual delivery of seed files which can be intercepted, lost, or stolen. References: https://docs.fortinet.com/document/fortiauthenticator/6.4/administration-guide/372403/fortitoken

NEW QUESTION 45
When generating a TOTP for two-factor authentication, what two pieces of information are used by the algorithm to generate the TOTP?

A. UUID and time

B. Time and seed
C. Time and mobile location
D. Time and FortiAuthenticator serial number

Answer: B

Explanation:
TOTP stands for Time-based One-time Password, which is a type of OTP that is generated based on two
pieces of information: time and seed. The time is the current timestamp that is synchronized between the client and the server. The seed is a secret key that is shared between the client and the server. The TOTP algorithm combines the time and the seed to generate a unique and short-lived OTP that can be used for two-factor authentication.
References:
https://docs.fortinet.com/document/fortiauthenticator/6.4.0/administration-guide/906179/two-factor-authenticati

NEW QUESTION 46
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE6_FAC-6.4 Practice Exam Features:

* NSE6_FAC-6.4 Questions and Answers Updated Frequently

* NSE6_FAC-6.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE6_FAC-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE6_FAC-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year