DUMPSARENA

Fortinet NSE 6 - FortiAuthenticator 6.1

Fortinet NSE6_FAC-6.1

Version Demo

Total Demo Questions: 5

Total Premium Questions: 51

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, User Management	3
Topic 2, Authentication	12
Topic 3, FSSO	4
Topic 4, Portal Services	8
Topic 5, Certificate Management	10
Topic 6, Token Management	4
Topic 7, RADIUS and TACACS+	6
Topic 8, High Availability and Troubleshooting	3
Topic 9, Mix Questions	1
Total	51

QUESTION NO: 1

Which FortiAuthenticator configuration controls the permissions available to an administrator after login?

A. Administrator access profile

B. Authentication realm

C. RADIUS client

D. Certificate revocation list

ANSWER: A

Explanation:

An **administrator access profile** controls the permissions available to an administrator. Access profiles define the administrative privileges that are assigned to administrator accounts, allowing organizations to provide only the required level of access for tasks such as user management, certificate administration, or system configuration.

Access profiles can support delegated administration when combined with appropriate administrator and realm configuration. A user group controls authentication membership, but it does not by itself grant administrative permissions to the FortiAuthenticator management interface. See the FortiAuthenticator 6.1 Administration Guide.

QUESTION NO: 2

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:

All conditions in the policy must match before a user is presented with the guest portal. In FortiAuthenticator, guest portal policies are evaluated to determine whether a particular authentication request should be redirected to, or handled by, a specified guest portal. A policy can contain multiple matching criteria, such as attributes of the authentication client, network details, or user/session context. These criteria are combined as required conditions: the request must satisfy the complete policy match for that guest portal policy to take effect. This allows an administrator to create targeted portal behavior, ensuring that a portal is shown only for the intended access scenario rather than broadly applying it to unrelated authentication activity. The policy's ordered evaluation and complete condition matching are important when multiple guest portals or access contexts are configured, because they provide predictable control over which portal experience is selected. FortiAuthenticator's guest-management and portal configuration capabilities are documented in the FortiAuthenticator 6.1 Administration Guide. Fortinet also provides the product documentation index at FortiAuthenticator Documentation.

QUESTION NO: 3

Which two protocols are the default management access protocols for administrative access for FortiAuthenticator? (Choose two)

A. Telnet

B. HTTPS

C. SSH

D. SNMP

ANSWER: B C

Explanation:

HTTPS and SSH are the default protocols used to administer a FortiAuthenticator appliance. HTTPS provides the encrypted browser-based connection to the FortiAuthenticator graphical management interface, where administrators configure authentication services, users, realms, certificates, policies, and system settings. SSH provides encrypted command-line administrative access, supporting secure management and troubleshooting from an SSH client. Both protocols protect the confidentiality of administrator credentials and management traffic in transit, which is essential because an authentication platform stores and processes highly sensitive identity and access-control information. FortiAuthenticator documentation describes administration through both its web-based GUI and CLI, and the platform's management-access design uses secure protocols for these interfaces by default. Administrators can use the HTTPS service to reach the GUI and an SSH session to access the CLI after network connectivity and appropriate administrator credentials are available. See the FortiAuthenticator 6.1 Administration Guide for FortiAuthenticator management guidance and the FortiAuthenticator 6.1 CLI Reference for command-line administration details.

QUESTION NO: 4

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

A. LinkedIn

B. Apple ID

C. Instagram

D. Email

ANSWER: A D

Explanation:

LinkedIn and Email are supported authentication methods for FortiAuthenticator captive and guest portals. FortiAuthenticator guest management supports configurable portal authentication that can use email-based registration and verification workflows, allowing a guest to receive access credentials or a verification message through an email address. This is a common guest-access design because it provides a contact method and can be combined with sponsor approval, account expiry, and usage controls.

FortiAuthenticator also supports social-login integration for guest portals, including LinkedIn. With social login, the portal redirects the guest to the selected identity provider for authentication and then uses the successful social-login result to grant controlled network access. Administrators configure the appropriate social-login provider and guest portal settings before publishing the portal to users. These methods are documented as part of FortiAuthenticator guest-management and captive-portal capabilities. See the FortiAuthenticator 6.1 Administration Guide and Fortinet's FortiAuthenticator product documentation for configuration guidance.

QUESTION NO: 5

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

A. Windows AD polling

B. FortiClient SSO Mobility Agent

C. Radius Accounting

D. DC Polling

ANSWER: B

Explanation:

FortiClient SSO Mobility Agent is the correct FSSO discovery method because it runs on the endpoint and communicates user session information directly to FortiAuthenticator. This endpoint-based approach reports session changes, including user logoff, rather than requiring FortiAuthenticator to determine whether a session remains valid through external polling mechanisms. Consequently, FortiAuthenticator can remove or update the user-to-IP association when the agent reports that the authenticated Windows session has ended.

This is especially useful for mobile devices and environments in which clients can move between networks, change addresses, or be unavailable to server-side management queries. The Mobility Agent maintains FSSO awareness from the client side, allowing identity information to follow the endpoint and allowing logged-off status to be communicated promptly. Its behavior therefore directly meets the requirement for transparent logged-off-user detection without dependence on WMI polling. Fortinet documents the available FortiAuthenticator FSSO integrations and configuration concepts in the FortiAuthenticator 6.1 documentation and describes endpoint SSO capabilities in the FortiClient documentation.