EXAMS 4 SUCCESS

# Fortinet

# FCP_FAC_AD-6.5

## Questions & Answers

### FCP - FortiAuthenticator 6.5 Administrator

(Demo Version - Limited Content)

# Version: 4.0

## Question: 1

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

A. RADIUS accounting

B. FortiClient SSO Mobility Agent

C. SSH sessions

D. FortiGate

E. FortiAuthenticator in SAML SP role

**Answer: A, B, D**

Explanation:

RADIUS accounting can be used by FortiAuthenticator to obtain user identity and session details for SSO.

FortiClient SSO Mobility Agent reports user login events to FortiAuthenticator for SSO.

FortiGate can act as an SSO source by sending user authentication information to FortiAuthenticator.

## Question: 2

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. Enable Adaptive Authentication in the portal policy.

B. Specify the appropriate RADIUS clients in the authentication policy.

C. Create an admin realm in the authentication policy.

D. Enable the Resolve user geolocation from their IP address option in the authentication policy

**Answer: A**

Explanation:

Enabling Adaptive Authentication in the portal policy allows FortiAuthenticator to apply contextual rules, such as bypassing two-factor authentication when users connect from specific secured networks.

## Question: 3

When configuring an active-passive HA deployment, what is the recommended data synchronization path?

A. Dedicated fiber channel

B. Same VLAN

C. Dedicated point-to-point VPN connection

D. Direct cable connection

**Answer: D**

Explanation:

A direct cable connection is the recommended data synchronization path in an active-passive HA deployment because it provides the fastest, most reliable, and secure method for synchronizing data between FortiAuthenticator units without depending on external network infrastructure.

## Question: 4

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

A. RADIUS accounting

B. FortiClient SSO mobility agent

C. DC polling

D. Windows AD polling

**Answer: B**

Explanation:

The FortiClient SSO Mobility Agent runs on the endpoint and communicates login and logoff events directly to FortiAuthenticator, allowing transparent detection of logged-off users without relying on external mechanisms like WMI polling.

## Question: 5

When performing a remote LDAP server integration with FortiAuthenticator, how do server type templates assist with the integration?

A. They autopopulate the simple and regular bind settings.

B. They automatically set the LDAP user auto provisioning settings.

C. They populate the query element fields with defined attribute and class values.

D. They define the connection security and domain authentication settings for each LDAP server you integrate with.

**Answer: C**

Explanation:

Server type templates in FortiAuthenticator assist LDAP integration by prepopulating the query element fields with the correct attribute and class values for the selected LDAP server type, simplifying configuration and ensuring accurate directory queries.

EXAMS 4 SUCCESS

## Thank you for trying

# Our FCP_FAC_AD-6.5 Exam Dumps PDF Demo

## Try FCP_FAC_AD-6.5 practice question

**If you want to try FCP_FAC_AD-6.5 Exam Practice Test Questions So go to below link and try it!**

https://www.exams4success.com/fcp-fac-ad-6-5/practice-questions