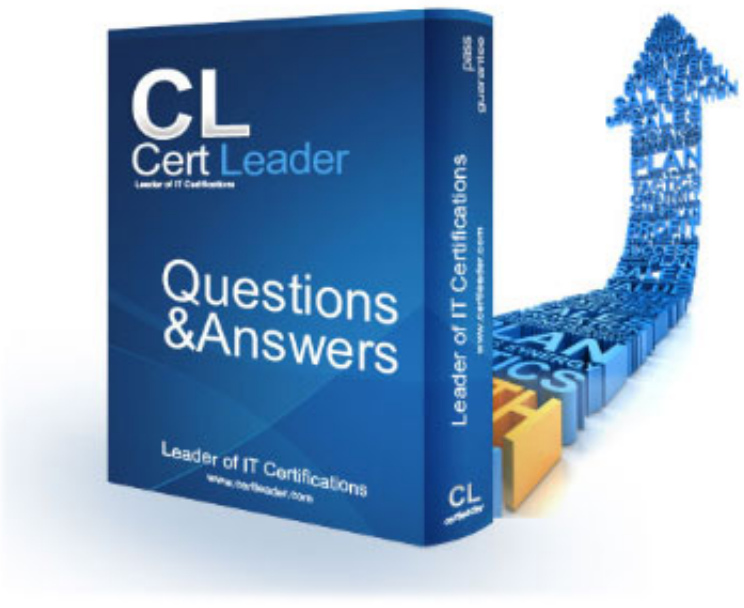
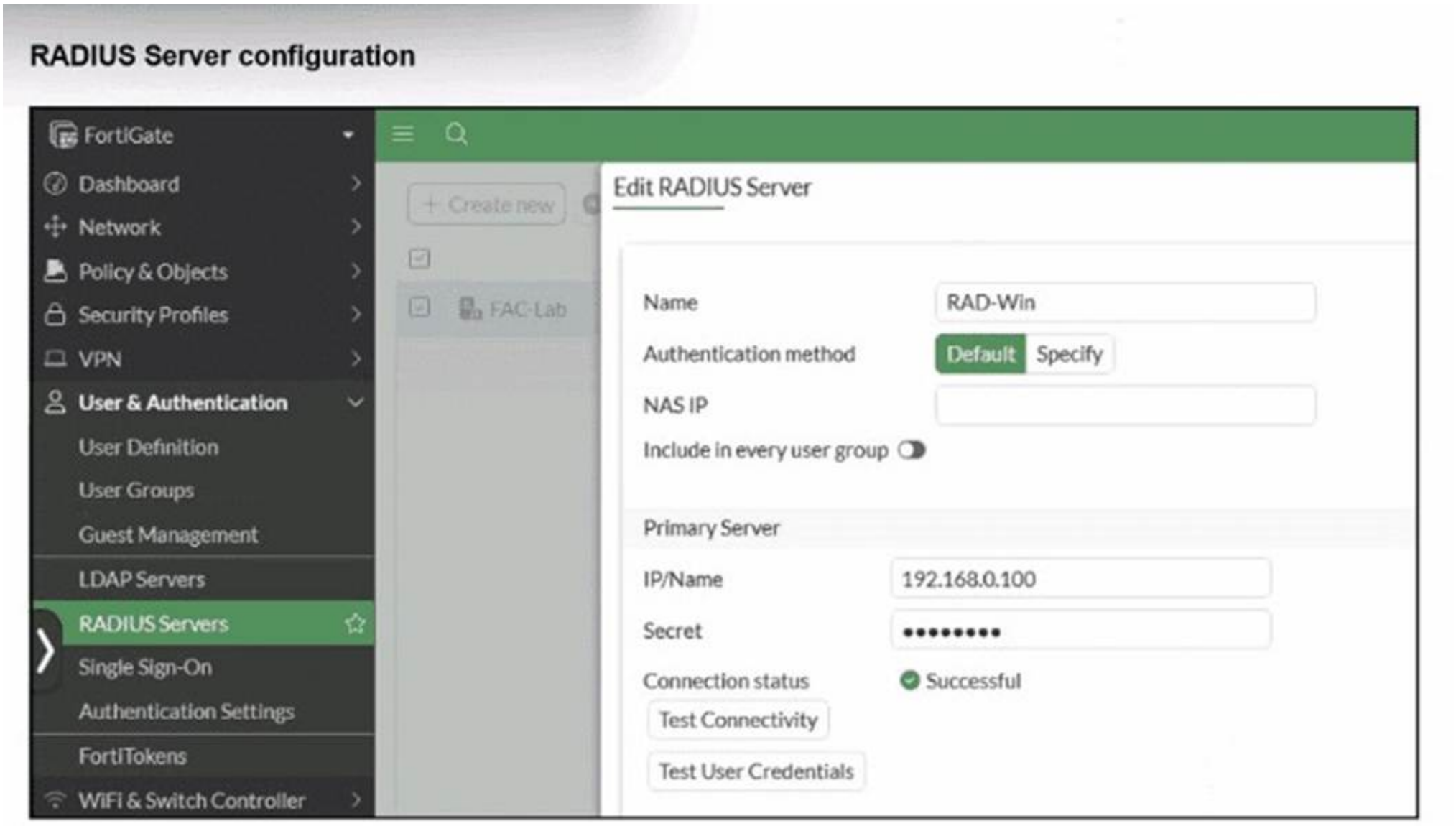
FCSS_LED_AR-7.6 Dumps

FCSS - LAN Edge 7.6 Architect

https://www.certleader.com/FCSS_LED_AR-7.6-dumps.html



NEW QUESTION 1
Refer to the exhibit.



On FortiGate, a RADIUS server is configured to forward authentication requests to FortiAuthenticator, which acts as a RADIUS proxy. FortiAuthenticator then relays these authentication requests to a remote Windows AD server using LDAP.
While testing authentication using the CLI command diagnose test authserver. the administrator observed that authentication succeeded with PAP but failed when using MS- CHAFV2.
Which two solutions can the administrator implement to enable MS-CHAPv2 authentication? (Choose two.)

A. Change the FortiGate authentication method to CHAP instead of MS-CHAPv2.
B. Enable Windows Active Directory domain authentication on FortiAuthenticator.
C. Enable RADIUS attribute filtering on FortiAuthenticator.
D. Configure FortiAuthenticator to use RADIUS instead of LDAP as the back-end authentication server

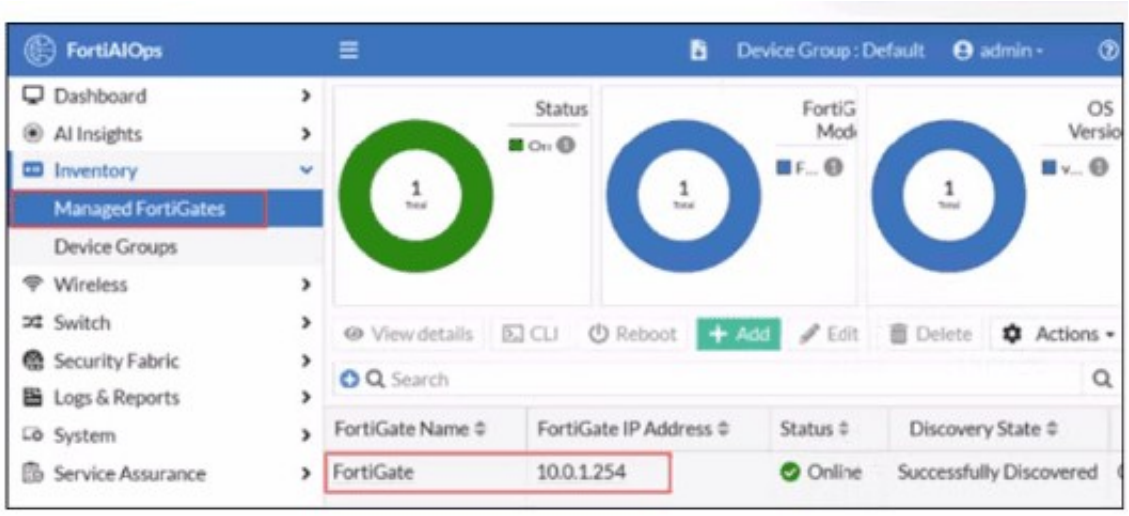
Answer: AD

NEW QUESTION 2
What is the expected behavior when enabling auto TX power control on a FortiAP interface?

A. FortiGate monitors the signal strength of nearby AP interfaces and adjusts its own transmit power every 30 seconds to match the signal strength of the adjacent AP
B. FortiGate measures the signal strength of nearby FortiAP interfaces every 30 seconds and adjusts their transmit power to ensure they remain detectable at -70 dBm.
C. FortiGate periodically measures the signal strength of the weakest associated client and adjusts the AP radio power to align with the detected signal strength of that client.
D. The AP periodically evaluates the signal strength of its own transmission from the client perspective and adjusts its power to ensure the signal is detected at -70 dBm.

Answer: C

NEW QUESTION 3
FortiGate has been added to FortiAIOps for management.

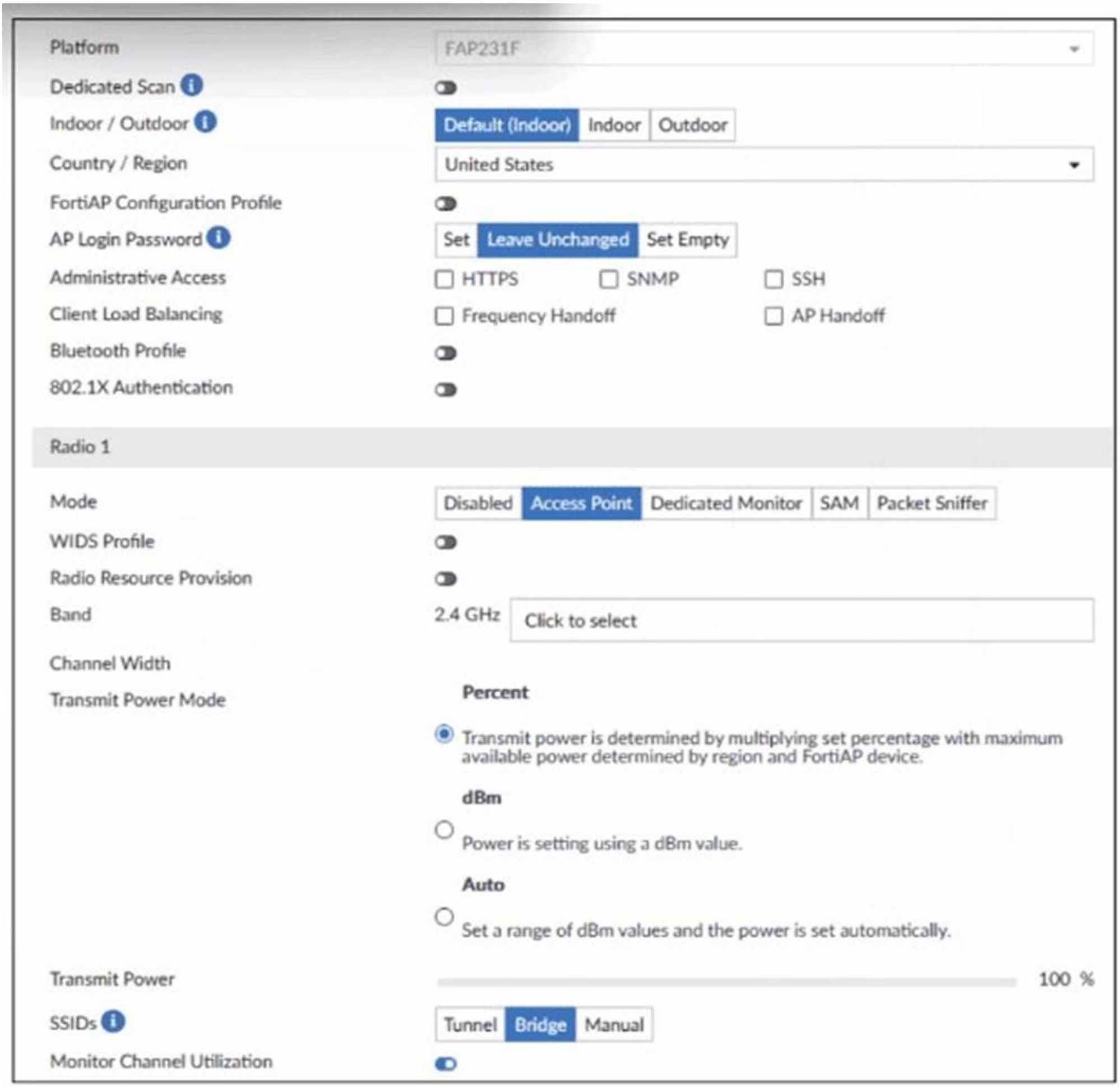


Which step must be performed on FortiAIOps to add a FortiSwitch device connected to the recently added FortiGate?

A. Add the FortiSwitch device by submitting its serial number.
B. FortiAIOps requires that the FortiSwitch IP address is submitted.
C. FortiSwitch is added automatically.
D. Configure the FortiSwitch IP address, user ID, and password

Answer: C

NEW QUESTION 4
Refer to the exhibits.



A set of SSID profiles has been configured on FortiManager, and an AP profile has been assigned to a group of AP managed by FortiGate. However, none of the designated SSIDs are being broadcast by these APs.
Which configuration change is required to make the APs broadcast these SSIDs as intended?

A. Adjust the AP profile to ensure all SSIDs are configured in a supported mode, either bridge or tunnel, but not a mix of both.
B. Change the AP profile to use a platform that supports the configured mix of SSIDs.
C. Choose Manual in the SSIDs setting and select the SSIDs to broadcast.
D. Set the Transmit Power Mode to Auto.

Answer: C

NEW QUESTION 5
Refer to the exhibits.

FortiGate VLAN AP settings

```
config system interface
    edit "APs"
        set vdom "root"
        set ip 10.10.100.254 255.255.255.0
        set allowaccess ping
        set alias "AP Management"
        set device-identification enable
        set role lan
        set snmp-index 118
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 100
    next
end
```

DHCP configuration

```
config system dhcp server
    edit 7
        set dns-service default
        set default-gateway 10.10.100.254
        set netmask 255.255.255.0
        set interface "APs"
        config ip-range
            edit 1
                set start-ip 10.10.100.1
                set end-ip 10.10.100.253
            next
        end
    next
end
```

FortiSwitch port1 VLAN AP assignment

```
config switch-controller managed-switch
    edit "FortiSwitch"
        set sn "S224EPTF19006016"
        set fsw-wan1-peer "fortilink"
        set fsw-wan1-admin enable
        set poe-detection-type 2
        set version 1
        set max-allowed-trunk-members 8
        set pre-provisioned 1
        set dynamic-capability 0x00000000000000001551027757ddfff7
        config ports
            edit "port1"
                set poe-capable 1
                set vlan "APs"
                set allowed-vlans "VLAN102" "VLAN101" "quarantine"
                set untagged-vlans "quarantine"
                set export-to "root"
                set mac-addr 04:d5:90:39:7d:8e
            next
```

A FortiSwitch is successfully managed by a FortiGate. FortiAP is connected to port1 of the managed FortiSwitch. On FortiGate, the VLAN AP is configured to detect and manage FortiAP, along with a DHCP server for the VLAN AP. Additionally, the VLAN AP is assigned to port1 of FortiSwitch. However. FortiGate is unable to detect or manage FortiAP.
Which FortiGate misconfiguration is preventing the detection of FortiAP?

A. Security Fabric is disabled in the administrative access options of the VLAN.
B. The FortiAP firmware is incompatible with the FortiGate firmware version.
C. The VLAN is not tagged correctly on the FortiSwitch uplink port.
D. The CAPWAP ports (UDP 5246 and 5247) are not open on FortiGate.

Answer: A

NEW QUESTION 6
A network engineer is deploying FortiGate devices using zero-touch provisioning (ZTP). The devices must automatically connect to FortiManager and receive their configurations upon first boot. However, after powering on the devices, they fail to register with FortiManager.
What could be a possible cause of this issue?

A. The FortiGate device requires manual intervention to accept the FortiManager connection.
B. In this scenario, the ZTP process works only when devices are connected using a console cable.
C. The FortiGate device must be preloaded with a configuration file before ZTP can function.
D. The FortiManager IP address is not reachable over TCP port 541.

Answer: D

NEW QUESTION 7
Connectivity tests are being performed on a newly configured VLAN. The VLAN is configured on a FortiSwitch device that is managed by FortiGate. During testing, it is observed that devices within the VLAN can successfully ping FortiGate. and FortiGate can also ping these devices.
Inter-VLAN communication is working as expected. However, devices within the same VLAN are unable to communicate with each other.
What could be causing this issue?

A. Access VLAN is enabled on the VLAN.
B. The FortiSwitch MAC address table is missing entries.
C. The FortiGate ARP table is missing entries.
D. The native VLAN configured on the ports is incorrect.

Answer: A

NEW QUESTION 8
Your office wants to set up a Wi-Fi network for visitors. Your company would like to require them to log in for (racking purposes. Which two types of captive portals could be enabled on an interface? (Choose two.)

A. Terms Acknowledgment Without Authentication
B. Email Notification Only
C. Disclaimer + Authentication
D. Guest Pass Access
E. Authentication

Answer: AE

NEW QUESTION 9
A FortiSwitch is not appearing in the FortiGate management interface after being connected via FortiLink. What could be a first troubleshooting step?

A. Ensure that the FortiGate security policies allow traffic from the FortiSwitch.
B. Manually assign a static IP to the FortiSwitch.
C. Verify that FortiGate device DHCP server is assigning an IP to the FortiSwitch.
D. Ensure the FortiSwitch has internet access.

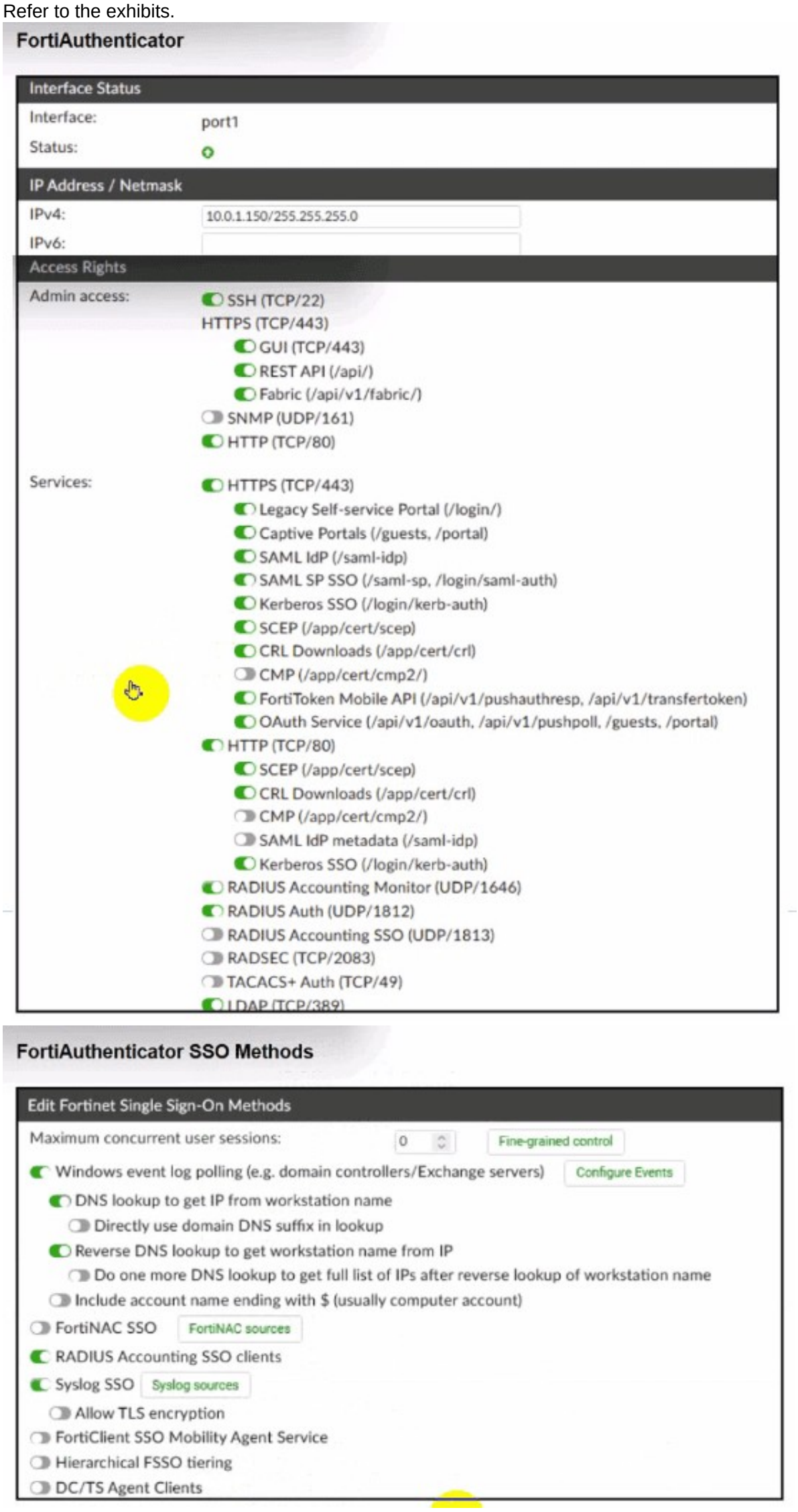
Answer: C

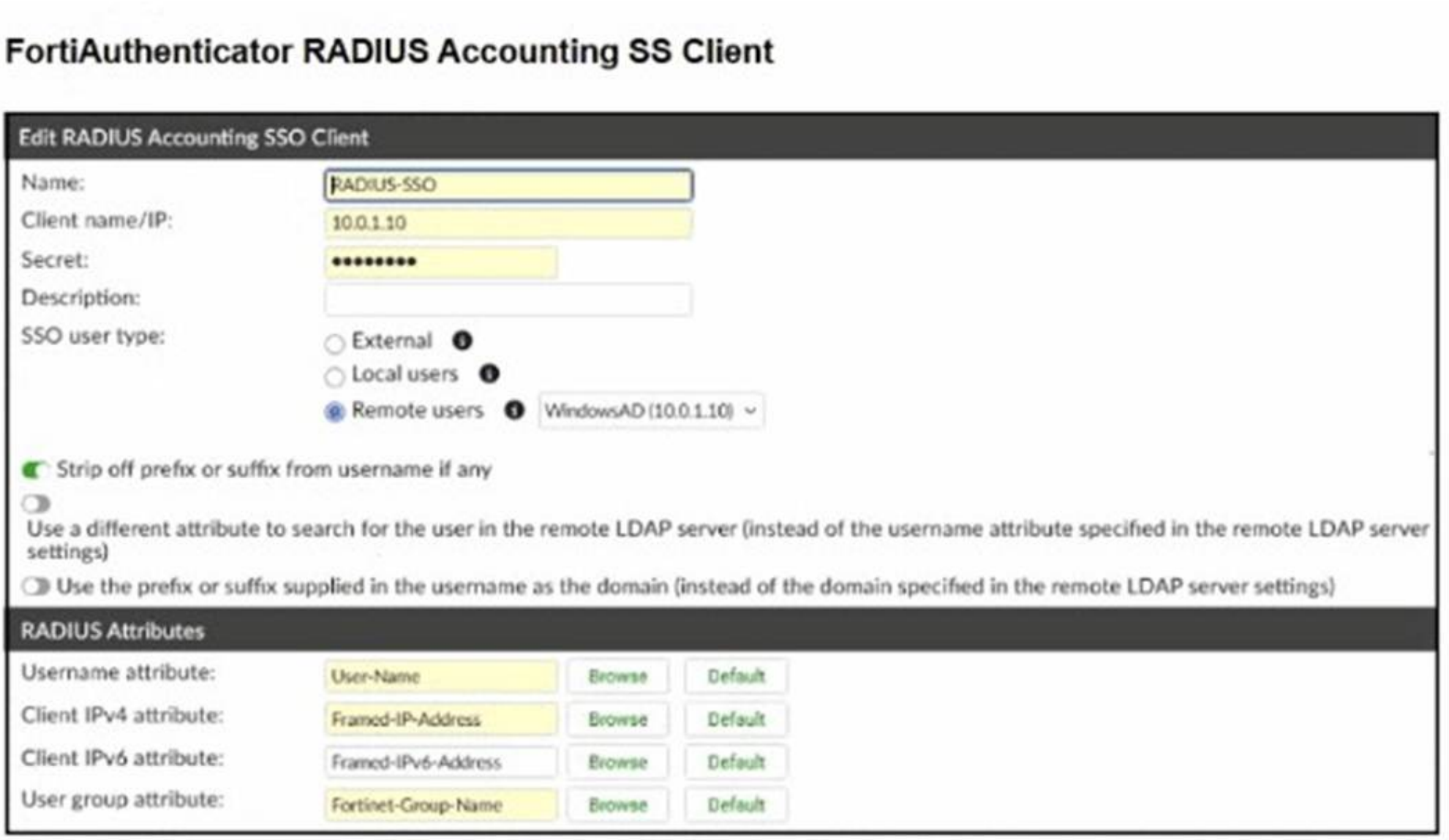
NEW QUESTION 10
APs have been manually configured to connect to FortiGate over an IPsec network, and FortiGate successfully detects and authorizes them. However, the APs remain unmanaged because FortiGate is unable to establish a CAPWAP tunnel with them.
What configuration change can resolve this issue and enable FortiGate to establish the CAPWAP tunnel over the IPsec connection?

A. Configure a static route on FortiGate to reach the APs over the IPsec tunnel.
B. Assign a custom AP profile for the remote APs with the set mpls-connection option enabled.
C. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
D. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.

Answer: B

NEW QUESTION 10
Refer to the exhibits.





A company has multiple FortiGate devices deployed and wants to centralize user authentication and authorization. The administrator decides to use FortiAuthenticator to convert RSSO messages to FSSO, allowing all FortiGate devices to receive user authentication updates.
After configuring FortiAuthenticator to receive RADIUS accounting messages, users can authenticate, but FortiGate does not enforce the correct policies based on user groups. Upon investigation, the administrator discovers that FortiAuthenticator is receiving RADIUS accounting messages from the RADIUS server and successfully queries LDAP for user group information. But, FSSO updates are not being sent to FortiGate devices and FortiGate firewall policies based on FSSO user groups are not being applied.
What is the most likely reason FortiGate is not receiving FSSO updates?

A. The RADIUS Username and Client IPv4 attributes are not defined on FortiAuthenticator.
B. The LDAP server is not configured to retrieve group memberships for RSSO users.
C. FortiAuthenticator is missing the FSSO user group attribute in the configuration.
D. The FortiAuthenticator interface is not enabled to receive RADIUS accounting messages.

Answer: A

NEW QUESTION 11
A network administrator connects a new FortiGate to the network, allowing it to automatically discover andI register with FortiManager.
What occurs after FortiGate retrieves the FortiManager address?

A. FortiGate establishes a secure tunnel to FortiManager over TCP port 541.
B. The device needs to be manually authorized on FortiManager.
C. FortiGate configures its interface settings based on a DHCP response from FortiManager.
D. FortiGate sends a discovery request to all devices on the local network using UDP port 1068.

Answer: A

NEW QUESTION 14
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCSS_LED_AR-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_LED_AR-7.6-dumps.html