PassQueen
a.k.a dumpsqueen.com

Implementing and Operating Cisco Wireless Core Technologies (WLCOR)v1.0

Cisco 350-101

Version Demo

Total Demo Questions: 10

Total Premium Questions: 101

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Following a controller replacement, several APs fail during the secure CAPWAP join process. The AP certificates and controller trustpoint are valid, but controller logs show that certificate validity checks fail because the controller clock is several days behind the current date. Which action resolves the issue while maintaining secure certificate validation?

A. Disable certificate validation for AP join requests.

B. Configure the controller to synchronize its clock with a reliable NTP source.

C. Replace the AP certificates with self-signed certificates.

D. Change the CAPWAP data channel to a different UDP port.

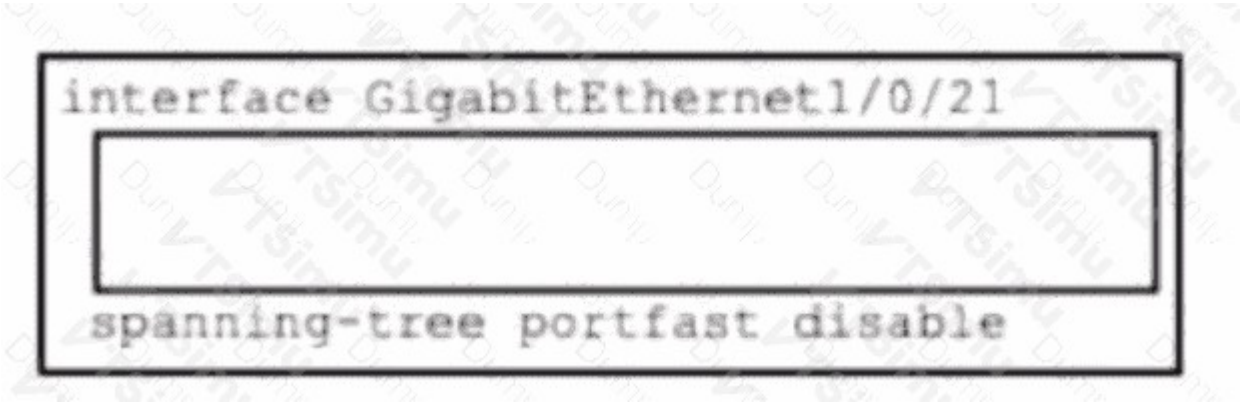
ANSWER: B

Explanation:

Configure the controller to synchronize its clock with a reliable NTP source. Certificate-based CAPWAP security depends on correct time validation because certificates include validity periods. After the controller time is accurate, it can correctly validate the AP certificate and complete the secure join process.

Disabling certificate validation weakens the CAPWAP security model and does not meet the requirement to maintain secure validation. Replacing valid AP certificates is unnecessary when the issue is an inaccurate controller clock. Changing the CAPWAP data port does not affect certificate validity checks.

QUESTION NO: 2



Refer to the exhibit. An engineer is configuring a switch port for a Cisco Spaces deployment at a new branch site. The Spaces connector requires access to the management VLAN 30. The network team plans to add more analytics services in the future, so the configuration must also allow for easy scalability and avoid service interruption for currently connected devices and default switch VLAN settings. Which set of commands must be added to the box in the CLI to complete the configuration?

A. switchport mode accessswitchport access vlan 30

B. switchport mode accessswitchport trunk allowed vlan 30switchport access native vlan

C. switchport mode accessswitchport trunk allowed vlan 30switchport trunk native vlan none

D. switchport mode trunkswitchport trunk allowed vlan 30

E. switchport mode trunk
switchport trunk allowed vlan add 30

ANSWER: E

Explanation:

`switchport mode trunk` followed by `switchport trunk allowed vlan add 30` is correct because it configures the connector-facing interface as an 802.1Q trunk while adding VLAN 30 to the port's existing allowed-VLAN list. A trunk is appropriate when the connected Cisco Spaces connector must carry management traffic on VLAN 30 and the design must accommodate additional service VLANs later through the same physical interface. Crucially, the `add` keyword is required: it preserves every VLAN already permitted on that trunk. This meets the stated requirement to avoid interrupting traffic for devices or services already using the interface and avoids replacing the switch's established VLAN allowance with a new, restrictive list. VLAN 30 can therefore traverse the link immediately, while future analytics VLANs can be appended without redesigning the port or changing native-VLAN behavior. Cisco documents that an 802.1Q trunk carries traffic for multiple VLANs and that the allowed-VLAN command supports adding VLANs to the current list rather than overwriting it. See Cisco's VLAN trunk configuration guide and the Cisco Spaces documentation.

QUESTION NO: 3

```
configure terminal
wlan branch1 10 branch1
security dot1x authentication-list ISE_GROUP
security web-auth
security web-auth authentication-list default
security web-auth parameter-map webauth_param_map
no shutdown
!
wireless profile policy branch1_policy
 no ip mac-binding
!
vlan configuration <vlan-id>
 arp broadcast
!
wireless profile policy branch1_policy
 aaa override enable
 local-switching enable
!
wireless tag policy branch1_policy_tag
 wlan branch1 policy branch1_policy
!
end
```

Refer to the exhibit. A wireless controller is deployed at a branch location to facilitate secure client connectivity. A network engineer configures a WLAN using 802.1X to align with company security policies. Which configuration enables client authentication for this WLAN?

A. no ip mac-binding

B. security dot1x authentication-list ISE_GROUP

C. aaa override enable

D. wlan branch1 policy branch1_policy

ANSWER: B

Explanation:

`security dot1x authentication-list ISE_GROUP` enables 802.1X client authentication on the WLAN by associating the WLAN's 802.1X security configuration with the named AAA authentication method list, `ISE_GROUP`. When a client joins this SSID, the controller uses that configured method list to process the client's Extensible Authentication Protocol exchange and send the authentication request to the RADIUS/Identity Services Engine servers defined for the list. This is the essential WLAN-level configuration step that makes enterprise 802.1X authentication active for clients rather than merely defining related policy behavior elsewhere on the controller. The method list provides the connection between the WLAN's Layer 2 802.1X security setting and the AAA infrastructure responsible for validating user or device credentials. Cisco's Catalyst 9800 wireless-controller configuration guidance identifies the `security dot1x authentication-list` command under WLAN configuration as the command used to apply an authentication method list for 802.1X security. See Cisco's 802.1X Authentication configuration guide and the Catalyst 9800 WLAN security documentation.

QUESTION NO: 4

A hotel wants to provide guests with wireless connectivity via a captive portal using a Cisco 9800 WLC. The solution must meet these requirements:

• Ensure that guests are redirected to a custom web page for login and after authentication must have only internet access.

• The guest SSID must not require a password and must be visible to all clients.

• Network segmentation between staff and guests is required at the VLAN level.

What must the IT team configure on the WLAN?

A. central web authentication with WPA2-PSK security and a DNS ACL assigned to the WLAN profile

B. open authentication with a local web server for the guest WLAN

C. PSK WLAN with VLAN override and enable mDNS for guest users

D. central web authentication and assign a policy with ACLs restricting access to internal networks

ANSWER: D

Explanation:

Central web authentication and assign a policy with ACLs restricting access to internal networks is correct because Central Web Authentication (CWA) is designed for an open guest WLAN that redirects unauthenticated users to a captive portal. The WLAN can advertise normally and does not require a pre-shared key, while the controller intercepts initial web traffic and sends the guest to the configured login page. Following successful authentication, the controller applies the authorized policy to the client session.

On a Catalyst 9800 controller, the WLAN is associated with a policy profile. That profile provides the guest VLAN mapping, ensuring that guest devices are placed in a network segment separate from staff devices. The policy and its access-control lists can permit required internet services, such as DNS, DHCP, and web traffic, while preventing access to internal address ranges. This provides both the required captive-portal onboarding experience and controlled post-authentication connectivity. Cisco documents web authentication configuration and its interaction with WLAN and policy-profile settings in the Catalyst 9800 Web Authentication Configuration Guide. Cisco also describes policy profiles and VLAN assignment in the Catalyst 9800 Policy Profiles documentation.

QUESTION NO: 5

A network administrator at a retail company recently deployed a Cisco Catalyst 9800 WLC. The NOC was unaware of wireless issues until it received reports from users. The network administrator must configure Cisco Catalyst Center to enable effective client issue alerts via email to prevent this happening again. Which action must the network administrator take in Cisco Catalyst Center to meet the requirements?

A. Configure a new event alert by navigating to Use Assurance > Platforms > Notifications.

B. Configure a new notification by navigating to Platform > Developer Toolkit > Event Notifications.

C. Add the NOC email address by navigating to Use Assurance > Issue Settings > Email.

D. Add the NOC email address by navigating to Platform > Event Notifications > Email.

ANSWER: B

Explanation:

Configure a new notification by navigating to Platform > Developer Toolkit > Event Notifications. Cisco Catalyst Center Assurance detects and manages client and wireless issues, but proactively delivering an alert to the NOC requires an event-notification subscription. In the Event Notifications workflow, an administrator selects the relevant Assurance issue events and associates them with a delivery channel. EMAIL is a supported notification channel, allowing the administrator to specify the email-message details and recipients so the NOC receives notifications when the selected issue events occur or their status changes. This subscription-based configuration is what connects Assurance-generated client issue events to operational email alerting; merely viewing issues or defining an email address elsewhere does not itself create the event-to-email notification workflow. Event Notifications is accessed from the Platform menu under Developer Toolkit and is intended for viewing available events and subscribing notification consumers to them. This enables the operations team to receive timely email alerts for wireless client problems detected after the Catalyst 9800 WLC deployment. Cisco documents the Event Notifications feature and subscription workflow in its Cisco Catalyst Center Event Notifications documentation and provides Catalyst Center configuration guidance in the Cisco Catalyst Center documentation portal.

QUESTION NO: 6

Refer to the exhibit. A startup company has recently moved to new offices and performed a full network refresh. The application development team requested a high-speed reliable wireless network to use for testing real-time applications. Although, the wireless network is Wi-Fi 7 enabled, the wireless clients are connecting using lower speeds. Which configuration must be applied on the WLC to increase throughput?

A. security wpa3 akm sae ext-key

B. security wpa wpa2 wpa3 aes512

C. security wpa wpa2 wpa3 tkip512

D. security wpa wpa2 ciphers gcmp256

ANSWER: D

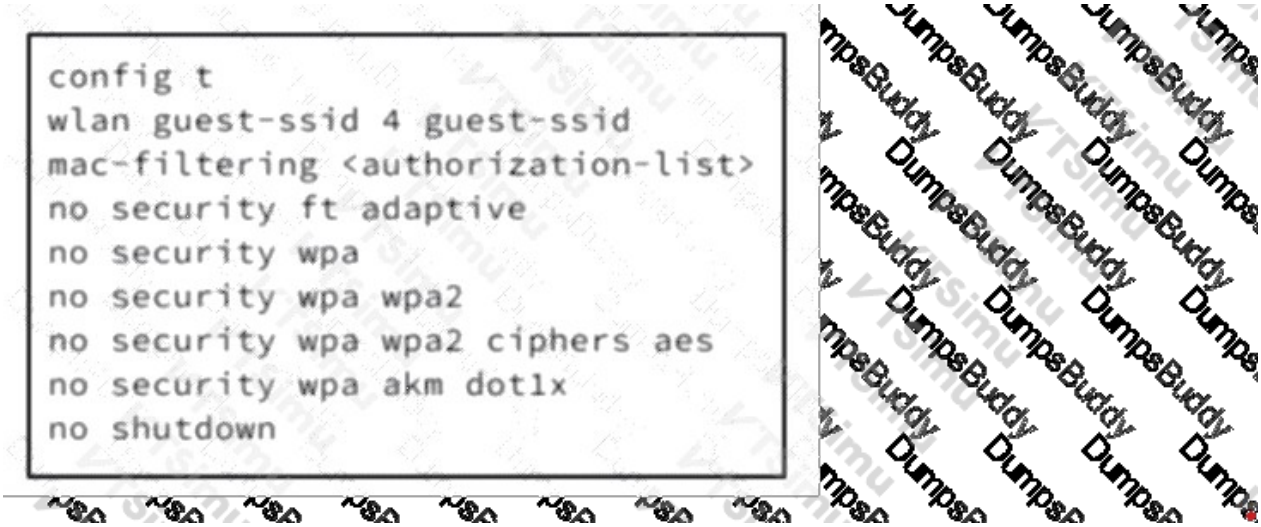
Explanation:

`security wpa wpa2 ciphers gcmp256` is the required WLAN configuration because it enables the GCMP-256 data cipher suite. Wi-Fi 7 client operation has stricter security requirements than earlier Wi-Fi generations. In particular, a WPA3-Personal Wi-Fi 7 WLAN requires SAE with the SAE extended-key capability, together with GCMP-256 encryption. The exhibit already indicates that the WLAN has SAE extended-key authentication configured, so the remaining required security component is the GCMP-256 cipher.

GCMP-256 provides the 256-bit Galois/Counter Mode Protocol cipher required for this Wi-Fi 7 WPA3-Personal security combination. Applying `security wpa wpa2 ciphers gcmp256` under the Catalyst 9800 WLAN policy profile permits eligible clients to associate using the required cipher rather than falling back to a non-Wi-Fi 7 security mode. This allows compatible clients to use Wi-Fi 7 capabilities and their associated higher-throughput operation, assuming the AP radio, channel configuration, client hardware, and RF conditions also support it.

Cisco documents the WPA3 and Wi-Fi 7 security requirements, including GCMP-256 and SAE extended-key support, in its WPA3 Security Enhancements configuration guide. Additional Wi-Fi 7 deployment guidance is available in Cisco's Wi-Fi 7 overview.

QUESTION NO: 7



Refer to the exhibit. An engineer must configure a wireless guest WLAN, which requires clients to use VLAN 10 for a deployment at site A. Based on the configuration commands shown, which additional configuration meets the requirements?

A. wlan guest-ssid 4 guest-ssidaccess vlan 10no shutdown

B. wlan guest-ssid 4 guest-ssidvlan 10no shutdown

C. wlan policy profile guest-policyaccess vlan 10no shutdown

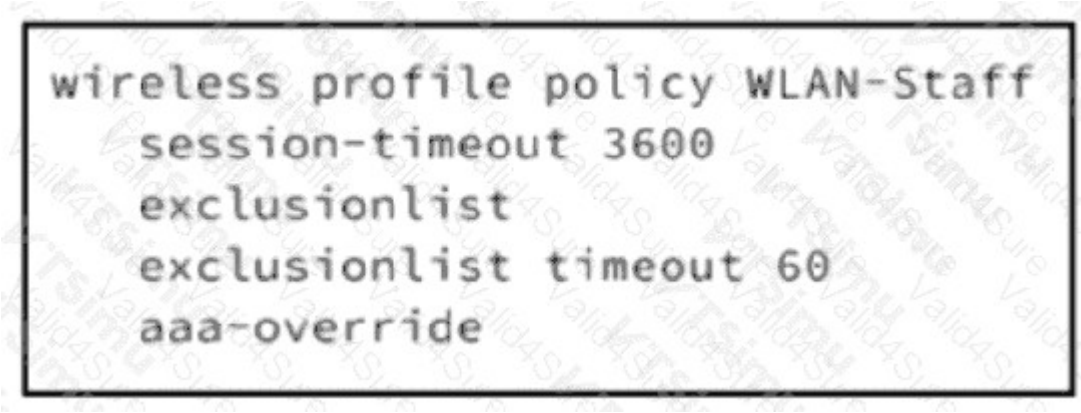
D. wireless profile policy guest-policyvlan 10no shutdown

ANSWER: D

Explanation:

```
wireless profile policy guest-policy
vlan 10
```
`no shutdown` is the required configuration because Catalyst 9800 controllers assign a client data VLAN through the wireless policy profile. The `vlan 10` command in the policy-profile configuration identifies VLAN 10 as the client VLAN used for WLAN traffic when that policy profile is applied through the WLAN's policy-tag mapping. Enabling the policy profile with `no shutdown` ensures it is operational and can be selected for client sessions. This structure separates the WLAN definition, which provides the SSID and WLAN-specific settings, from the policy profile, which supplies forwarding and client-access parameters such as VLAN assignment. Once the guest WLAN is mapped to `guest-policy` in the relevant policy tag for site A, associated guest clients are placed into VLAN 10. The wired infrastructure must also carry VLAN 10 to the controller and provide the corresponding Layer 3 services, such as DHCP and routing, for those guest clients. Cisco's Catalyst 9800 configuration model documents VLAN configuration as a policy-profile setting and uses policy tags to associate WLANs with those profiles. See Cisco's Policy Profiles configuration guide and Policy Tags configuration guide.

QUESTION NO: 8



Refer to the exhibit. A network administrator must configure a client management parameter for a wireless deployment in a multi-site enterprise. The enterprise is using Cisco ISE as the management platform to oversee wireless access policies. To meet the organization's compliance requirements, all wireless endpoints must be evaluated against a posture policy before gaining access. Which configuration change must be applied on the WLAN level of the WLC to meet the requirement?

A. config wlan WLAN-staff enable aaa-override

B. wireless profile policy WLAN-Staff
nac

C. config wlan WLAN-StaffWLAN-staff radius enable

D. wireless profile policy WLAN-Staff config wlan 5 enable radius

ANSWER: B

Explanation:

`wireless profile policy WLAN-Staff`
`nac` is the required configuration because it enables Network Admission Control on the wireless policy profile associated with the WLAN. NAC integrates the wireless access workflow with Cisco ISE posture services, so endpoints can be directed to posture assessment and remediation processes before they receive the level of network access permitted by the organization’s compliance policy. The policy profile is the Catalyst 9800 WLC configuration object that defines client-related WLAN behavior, including access control and NAC handling. When NAC is enabled, Cisco ISE can apply its posture policy to determine whether a client satisfies required conditions, such as endpoint security status, operating-system compliance, or required software configuration. The resulting authorization decision can then provide the appropriate client access outcome after posture evaluation. This directly addresses the requirement that every wireless endpoint be assessed for compliance before gaining normal network access. Cisco documents NAC as a policy-profile feature for wireless client admission and describes Cisco ISE posture as the mechanism used to assess and remediate endpoint compliance. See Cisco’s Catalyst 9800 client configuration guide and the Cisco ISE posture administration guide.

QUESTION NO: 9

A branch uses FlexConnect APs and must continue forwarding traffic for already authenticated local users when the WAN connection to the central Catalyst 9800 WLC fails. New user authentication can wait until WAN service is restored. Which deployment approach meets this requirement?

A. Configure the WLAN for central switching and central authentication.

B. Configure the FlexConnect WLAN for local switching with a local VLAN mapping.

C. Configure the APs in monitor mode and tunnel client traffic to the controller.

D. Configure the AP uplinks as access ports in the guest VLAN only.

ANSWER: B

Explanation:

Configure the FlexConnect WLAN for local switching with an appropriate local VLAN mapping. In FlexConnect local switching, client data is switched at the AP onto the branch wired network rather than being tunneled across the WAN to the central controller. Existing authenticated clients can therefore continue using local data connectivity during a controller WAN outage.

Central switching would require client traffic to traverse the CAPWAP tunnel to the controller and would be affected by the WAN failure. Local switching does not by itself provide offline authentication for new users; that would require an additional local authentication design if it were required.

QUESTION NO: 10

A network engineer has been tasked with migrating the management mode of a Cisco 9176 AP named "Cisco-AP053540555" in a large enterprise wireless deployment. The AP is currently managed by a Cisco Catalyst 9800 Series WLC, but the organization is transitioning to Meraki cloud management for centralized control and monitoring. To complete this migration, the engineer needs to change the AP's management mode to Meraki with force and noprompt to skip validations using the CLI on the wireless controller. What command must the engineer use?

A. management meraki force noprompt mode

B. ap management mode meraki force noprompt

C. ap management meraki force noprompt mode

D. management-mode meraki force noprompt

E. ap name Cisco-AP053540555 management-mode meraki force no-prompt

ANSWER: E

Explanation:

The command `ap name Cisco-AP053540555 management-mode meraki force no-prompt` is the correct Cisco IOS XE syntax because the management-mode change is applied in the context of a specific access point. The `ap name` portion identifies the target AP on the Catalyst 9800 controller, and `management-mode meraki` changes that AP from Cisco Catalyst controller management to Meraki cloud management. This workflow is used for universal Cisco wireless access points that support conversion to Meraki-managed operation. The `force` keyword permits the requested transition when the controller would otherwise require a validation or confirmation condition, while `no-prompt` suppresses the interactive confirmation prompt so the operation can be performed noninteractively, such as during a scripted migration. After the management-mode conversion, the AP leaves the Catalyst controller environment and must establish connectivity to the Meraki cloud so it can be claimed and managed in the intended Meraki organization and network. Cisco documents management-mode migration for supported AP platforms and the relevant Catalyst 9800 AP command structure in its wireless configuration guidance. See the Meraki management-mode migration guide and the Cisco Catalyst 9800 configuration guide.