# **TOPIC 1**

1. For which two reasons can an organization become “Out of License”? (Choose two.)
2. licenses that are in the wrong network
3. more hardware devices than device licenses
4. expired device license
5. licenses that do not match the serial numbers in the organization
6. MR licenses that do not match the MR models in the organization

Answer: BC

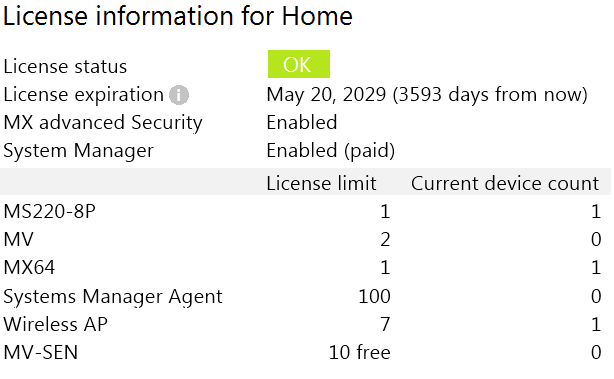
1. Cloud license has expired
2. the number of HW devices exceeds the number of cloud licenses <https://documentation.meraki.com/General_Administration/Licensing/Meraki_Licensing_FAQs#:~:text=If%20an%20organization%20is%20%22out,manageable%20using%20the%20Meraki%20cloud>.
3. In an organization that uses the Co-Termination licensing model, which two operations enable licenses to be applied? (Choose two.)
4. Renew the Dashboard license.
5. License a network.
6. License more devices.
7. Call Meraki support.
8. Wait for the devices to auto-renew.

Answer: AC

There are two operations in which a license can be applied, License more devices or Renew my dashboard license. This article will compare both operations and describe their behaviors.

<https://documentation.meraki.com/General_Administration/Licensing/Meraki_Licensing_-_License_More_Devices_vs_Renewal>

1. Refer to the exhibit. This Dashboard organization uses Co-Termination licensing model. What happens when an additional seven APs are claimed on this network without adding licenses?



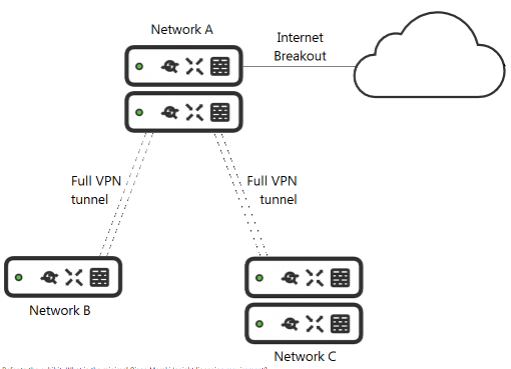
1. All APs immediately stop functioning.
2. Refer to the exhibit. This Dashboard organization uses Co-Termination licensing model.
3. What happens when an additional seven APs are claimed on this network without adding licenses?
4. A. All APs immediately stop functioning.

Answer : B

The number of devices in an organization can not exceed the license limits. If this occurs, the organization will enter a 30-day grace period, during which the organization must be brought back into compliance, otherwise it will be shut down until proper licensing is applied to the organization.

<https://documentation.meraki.com/General_Administration/Licensing/Meraki_Co-Termination_Licensing_Overview>

1. Refer to the exhibit. What is the minimal Cisco Meraki Insight licensing requirement?



1. A single Meraki Insight license must be configured on network A to gain Web App Health visibility on network B.
2. A single Meraki Insight license must be configured on network B to gain Web App Health visibility on network B.
3. A single Meraki Insight license must be configured on network A, and a single license must be configured on network B, to gain Web App Health visibility on network B.
4. Two Meraki Insight licenses must be configured on network A to gain Web App Health visibility on network B.
5. Two Meraki Insight licenses must be configured on network A and a single license must be configured on network B, to gain Web App Health visibility on network B.

Answer: B

Licensing Guidelines

A license is only required for those networks where Meraki Insight functionality is desired. One license is required per network, regardless of whether that network has a single MX or HA pair. Licenses can be moved between networks, but historical data for the old network will be lost.

<https://meraki.cisco.com/lib/pdf/meraki_datasheet_mi.pdf>

1. How does a Meraki device behave if cloud connectivity is temporarily lost?
2. The offline device continues to run with its last known configuration until cloud connectivity is restored.
3. The offline device reboots every 5 minutes until connection is restored.
4. The offline device stops passing traffic.
5. The offline device tries to form a connection with a local backup sever.

Answer: A

Should be A there is no local server

1. What are two organization permission types? (Choose two.)
2. Full
3. Read-only
4. Monitor-only
5. Write
6. Write-only

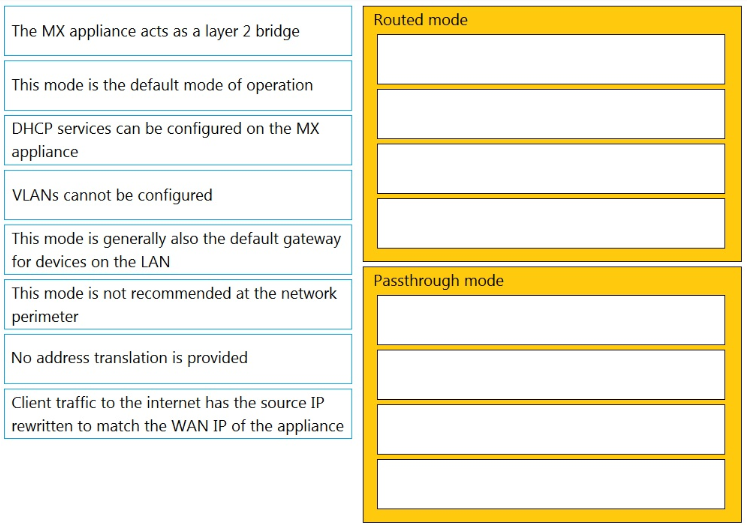
Answer: AB

<https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions>

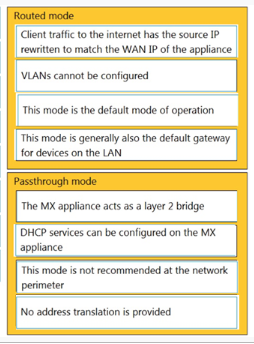
1. What is the role of the Meraki Dashboard as the service provider when using SAML for single sign-on to the Dashboard?
2. The Dashboard generates the SAML request.
3. The Dashboard provides user access credentials.
4. The Dashboard parses the SAML request and authenticates users.
5. The Dashboard generates the SAML response.
6. A customer wants to use Microsoft Azure to host corporate application servers. Which feature does the customer get by using a vMX appliance rather than connecting directly to Azure by VPN?
7. malware protection
8. SD-WAN
9. next-generation firewall
10. intrusion prevention

# **TOPIC 2**

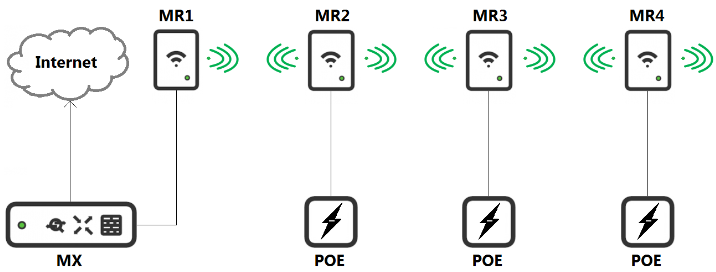
1. Drag and drop the descriptions from the left onto the corresponding MX operation mode on the right.



Answer:



1. What is a feature of distributed Layer 3 roaming?
2. An MX Security Appliance is not required as a concentrator.
3. An MX Security Appliance is required as a concentrator.
4. All wireless client traffic can be split-tunneled.
5. All wireless client traffic is tunneled.
6. Refer to the exhibit. Which design recommendation should be considered?



1. A 25-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 1-hop maximum.
2. A 25-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 2-hop maximum.
3. A 50-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 1-hop maximum.
4. A 50-percent throughput loss occurs for every hop. Cisco Meraki best practice recommends a 2-hop maximum.
5. Which two features and functions are supported when using an MX appliance in Passthrough mode? (Choose two.)
6. intrusion prevention
7. site-to-site VPN
8. secondary uplinks
9. DHCP
10. high availability
11. What are two ways peers interact with ports that Auto VPN uses? (Choose two.)
12. For IPsec tunneling, peers use high UDP ports within the 32768 to 61000 range.
13. Peers contact the VPN registry at UDP port 9350.
14. For IPsec tunneling, peers use high TCP ports within the 32768 to 61000 range.
15. Peers contact the VPN registry at TCP port 9350.
16. For IPsec tunneling, peers use UDP ports 500 and 4500.
17. One thousand concurrent users stream video to their laptops. A 30/70 split between 2.4 GHz and 5 GHz is used. Based on client count, how many APs (rounded to the nearest whole number) are needed?
18. 26
19. 28
20. 30
21. 32
22. What is the best practice Systems Manager enrollment method when deploying corporate-owned iOS devices?
23. manual
24. Apple Configurator
25. Sentry enrollment
26. DEP
27. A customer requires a hub-and-spoke Auto VPN deployment with two NAT-mode hubs with dual uplink connections and 50 remote sites with a single uplink connection.

How many tunnels does each hub need to support?

1. 52
2. 54
3. 100
4. 104
5. How is high-availability supported for Cisco Meraki devices?
6. Only the MX Security Appliances that use VRRP support high availability.
7. An active/active high-availability pair is recommended for MX Security Appliances.
8. The MX Security Appliances and MS Series Switches that use VRRP support an active/passive high-availability pair.
9. The MX Security Appliances and MS Series Switches that use HSRP support an active/passive high-availability pair.
10. Which Cisco Meraki product must be deployed in addition to Systems Manager so that Systems Manager Sentry enrollment can be used?
11. MS Switch
12. Meraki Insight
13. MR Access Point
14. MV Smart Camera
15. Which information do the MXs in a High Availability pair share?
16. spanning-tree state
17. time synchronization state
18. DHCP association database
19. stateful firewall database

41. A new application needs to be pushed to all iOS devices. Some devices report ''NotNow'' in the event log and do not install the application. What does the ''NotNow'' event indicate?

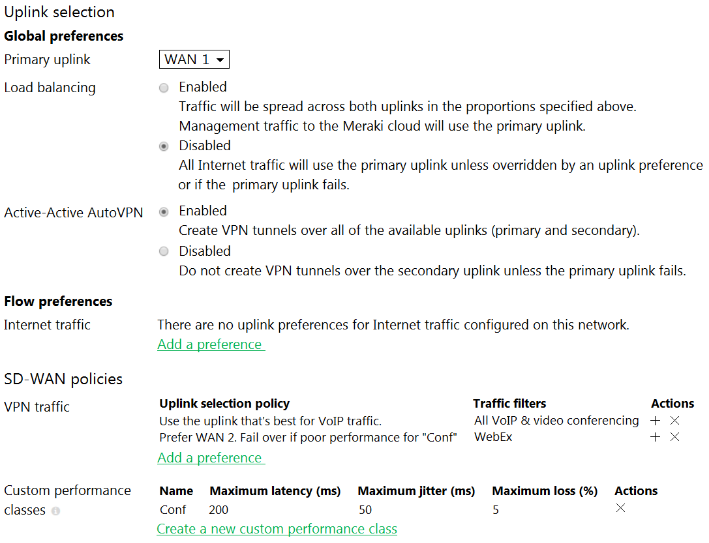
1. The application requires the most recent iOS version.
2. The device is locked with a passcode.
3. The device cannot connect to Apple servers.
4. The device cannot connect to Cisco Meraki servers.

# **TOPIC 3**

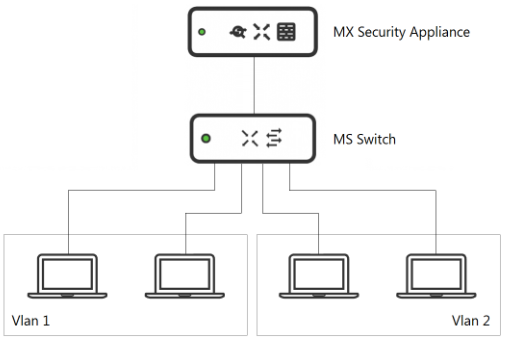
1. When an SSID is configured with Sign-On Splash page enabled, which two settings must be configured for unauthenticated clients to have full network access and not be allow listed? (Choose two.)
2. Controller disconnection behavior
3. Captive Portal strength
4. Simultaneous logins
5. Firewall & traffic shaping
6. RADIUS for splash page settings
7. Air Marshal has contained a malicious SSID.

What are two effects on connectivity? (Choose two.)

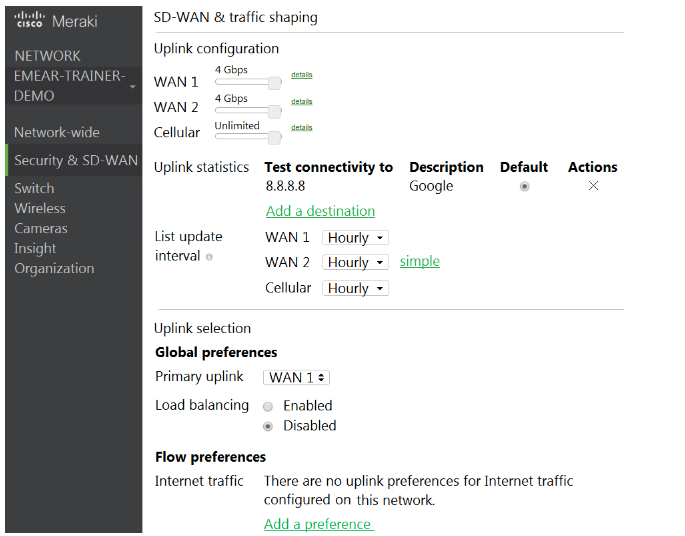
1. Currently associated clients stay connected.
2. New clients can connect.
3. Currently associated clients are affected by restrictive traffic shaping rules.
4. New clients cannot connect.
5. Currently associated clients are disconnected.
6. Refer to the exhibit. Assuming this MX has established a full tunnel with its VPN peer, how will the MX route the WebEx traffic?



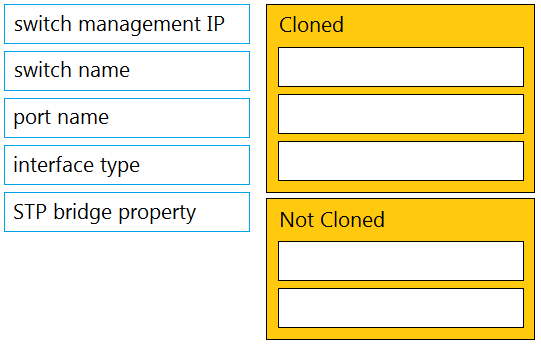
1. WebEx traffic will prefer WAN 2 as long as it meets the thresholds in the “Conf” performance class.
2. WebEx traffic will prefer WAN 1 as it is the primary uplink.
3. WebEx traffic will prefer WAN 2 as long as it is up.
4. WebEx traffic will be load-balanced between both active WAN links.
5. Refer to the exhibit. What is an advantage of implementing inter-VLAN routing on an MX Security Appliance rather than performing inter-VLAN routing on an MS Series Switch?



1. The MX appliance performs IDS/IPS for inter-VLAN traffic.
2. The MX appliance performs AMP for inter-VLAN traffic.
3. The MX appliance performs data encryption for inter-VLAN traffic.
4. The MX appliance performs content filtering for inter-VLAN traffic.
5. Refer to the exhibit. Which two actions are required to optimize load balancing asymmetrically with a 4:1 ratio between links? (Choose two.)



1. Change the primary uplink to "none".
2. Add an internet traffic preference that defines the load-balancing ratio as 4:1.
3. Enable load balancing.
4. Set the speed of the cellular uplink to zero.
5. Change the assigned speeds of WAN 1 and WAN 2 so that the ratio is 4:1.
6. Which requirement is needed to implement Fast Lane on Cisco Meraki APs?
7. wireless profile installed on an Apple iOS device
8. wireless profile installed on a Cisco iOS access point
9. adaptive 802.11r disabled
10. traffic shaping rule tagging traffic with a DSCP value of 46 to Apple.com
11. Which type of authentication protocol is used when using OSPF on an MX appliance?
12. MD5
13. certificate
14. plaintext
15. SHA-1
16. When wireless SSIDs are configured in Dashboard, which setting on the Access Control page affects the ability of a 2.4 GHz only client device from associating to the WLAN for the first time?
17. Content filtering
18. Bridge mode
19. 802.11r
20. Dual band operating with Band Steering
21. Which two actions can extend the video retention of a Cisco Meraki MV Smart Camera? (Choose two.)
22. enabling audio compression
23. installing an SSD memory extension
24. enabling motion-based retention
25. enabling maximum retention limit
26. configuring a recording schedule
27. What occurs when a configuration change is made to an MX network that is bound to a configuration template?
28. The configuration change in the bound network is combined with the template configuration inside the template.
29. The more restrictive configuration is preferred.
30. The configuration change in the bound network overrides the template configuration.
31. The template configuration overrides the configuration change in the bound network.
32. DRAG DROP - Drag and drop the settings from the left into the boxes on the right to indicate if the setting will be cloned or not cloned using the Cisco Meraki MS switch cloning feature.



Answer:

Cloned:

Port name

Interface type

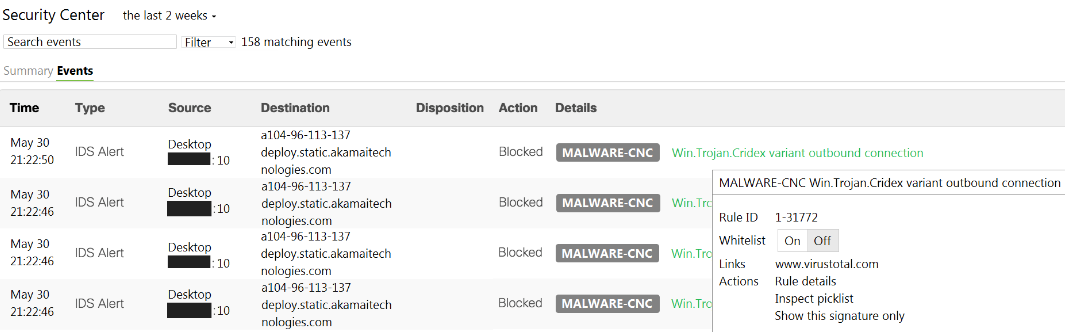
STP bridge priority

Not cloned:

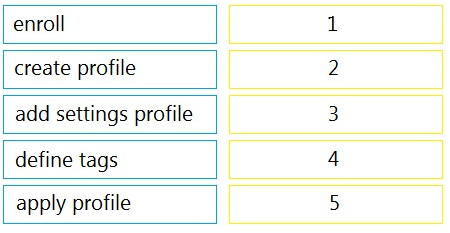
Switch name

Switch management IP

1. Refer to the exhibit. Which IDS/IPS mode is the MX Security Appliance configured for?



1. quarantine
2. prevention
3. detection
4. blocking
5. DRAG DROP - Drag and drop the steps from the left into the sequence on the right to manage device control, according to Cisco Meraki best practice.



Answer:

enroll>create profile> add settings profile > define tags >apply profile

1. Which configuration step is necessary when automatic updating is required of iOS apps provisioned through Systems Manager that are found in the App Store?
2. No configuration step is necessary; automatic updating is the default behavior.
3. Configure automatic updating of iOS devices in the Meraki installed profile.
4. Create a security policy that enables automatic updates.
5. Create a profile with automatic update enabled and apply it to iOS devices

# **TOPIC 4**

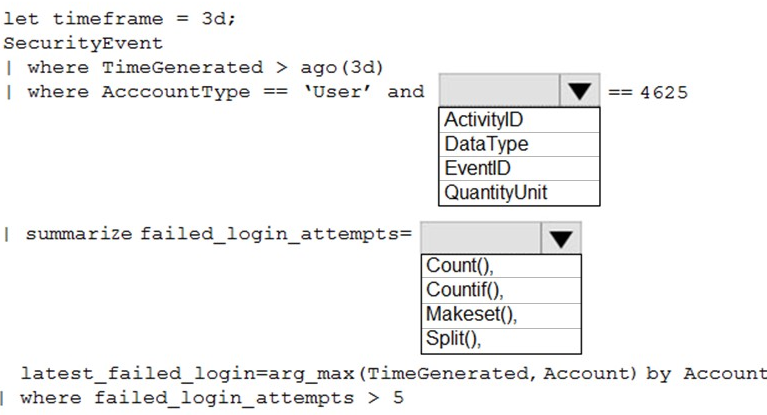
1. Which Cisco Meraki best practice method preserves complete historical network event logs?
2. Configuring the preserved event number to maximize logging.
3. Configuring the preserved event period to unlimited.
4. Configuring a syslog server for the network.
5. Configuring Dashboard logging to preserve only certain event types.
6. Which design requirement is met by implementing syslog versus SNMP?
7. when automation capabilities are needed
8. when proactive alerts for critical events must be generated
9. when organization-wide information must be collected
10. when information such as flows and client connectivity must be gathered
11. You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

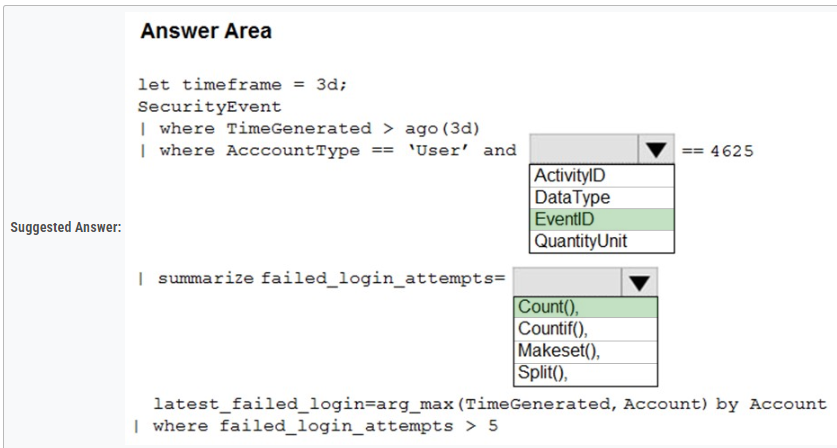
How should you configure the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer:



The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in. let timeframe = 1d;

SecurityEvent -

| where TimeGenerated > ago(1d)

| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in

| summarize failed\_login\_attempts=count(), latest\_failed\_login=arg\_max(TimeGenerated, Account) by Account

| where failed\_login\_attempts > 5

| project-away Account1

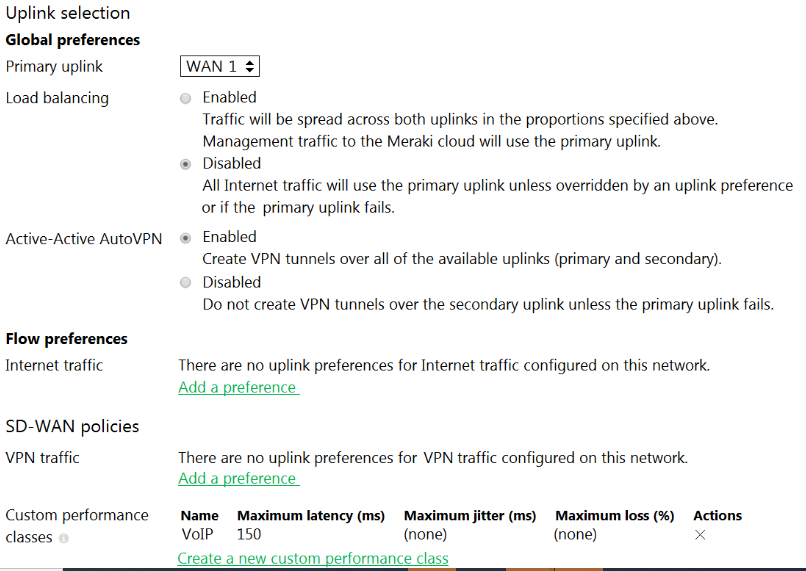
Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples>

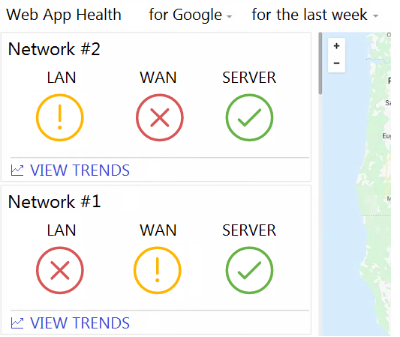
1. Refer to the exhibit. For an AP that displays this alert, which network access control method must be in use?



1. preshared key
2. WPA2-enterprise with my RADIUS server
3. splash page with my RADIUS server
4. MAC-based access control with RADIUS server
5. Refer to the exhibit. What does the MX Security Appliance send to determine whether VPN traffic exceeds the configured latency threshold in the VoIP custom performance class?



1. 1000-byte TCP probes every second, through VPN tunnels that are established over the primary WAN link.
2. 100-byte UDP probes every second, through VPN tunnels that are established over every WAN link.
3. 100-byte UDP probes every second, through VPN tunnels that are established over the primary WAN link.
4. 1000-byte TCP probes every second, through VPN tunnels that are established over every WAN link.
5. Which two primary metrics does Meraki Insight use to calculate the Application Performance Score? (Choose two.)
6. Maximum Jitter
7. Total Bandwidth Usage
8. Maximum Latency
9. Per-flow Goodput
10. Application Response Time
11. Refer to the exhibit. What are two outcomes reflected in the Web App Health application? (Choose two.)



1. Users on both networks may be experiencing issues when attempting to reach Google.
2. Network #1 could not load Google because of a remote server issue.
3. Network #2 had better application performance than Network #1.
4. Network #2 could not load Google because of a local client misconfiguration.
5. Neither network recorded any server-side performance issues.
6. Where should a network admin navigate to investigate wireless mesh information between Meraki APs?
7. Wireless > Monitor > Access Points > AP > RF
8. Wireless > Configure > Radio Settings
9. Wireless > Monitor > Wireless Health
10. Wireless > Monitor > RF Spectrum
11. A Cisco Meraki MV camera is monitoring an office and its field of vision currently captures work desks and employee computer screens. However, recording employee computer screens is prohibited by local regulation.

Which feature in Dashboard can be used to preserve the current position of the camera while also meeting regulation requirements?

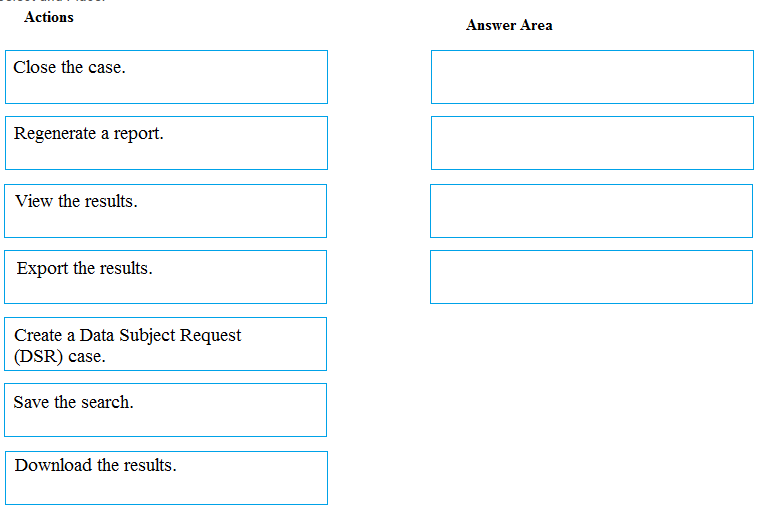
1. zone exclusion
2. privacy window
3. area or interest
4. sensor crop
5. restricted mode
6. You have a Microsoft 365 subscription.

A customer requests that you provide her with all documents that reference her by name.

You need to provide the customer with a copy of the content.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

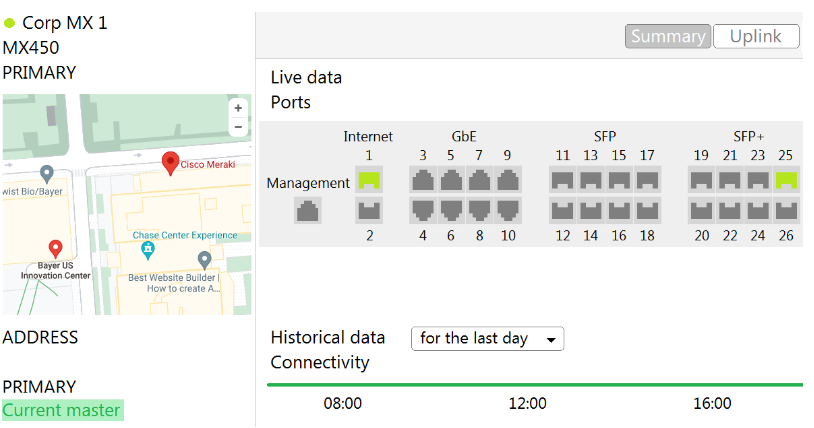
Select and Place:



Answer:

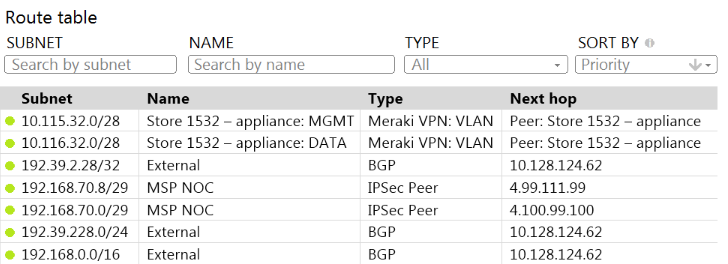
1. Refer to the exhibit. The VPN concentrator is experiencing issues.

Which action should be taken to ensure a stable environment?



1. Add a deny any/any firewall rule to the end of the firewall rules.
2. Remove the connection from Internet 1.
3. Physically disconnect all LAN ports.
4. Configure the MX appliance to Routed mode on the Addressing & VLANS page.
5. Refer to the exhibit. A packet arrives on the VPN concentrator with source IP 10.168.70.3 and destined for IP 10.116.32.4.

What is the next hop for the packet, based on this concentrator routing table?



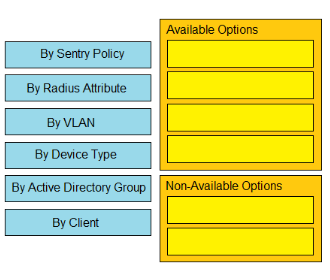
1. The concentrator gateway (10.128.124.62) is the next hop.
2. Not enough detail is available to determine the next hop.
3. The packet is stopped.
4. The Auto VPN peer “Store 1532 – appliance” is the next hop.
5. Company iPads are enrolled in Systems Manager without supervision, and profiles are pushed through Systems Manager.

Which outcome occurs when a user attempts to remove the “Meraki Management” profile on an iPad?

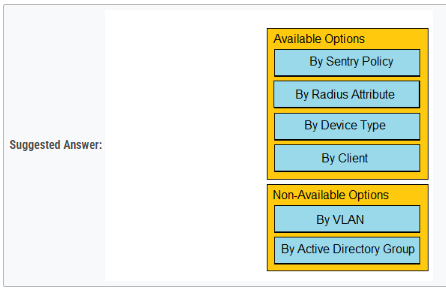
1. The “Meraki Management” profile cannot be removed.
2. The “Meraki Management” profile is removed and then pushed automatically by Systems Manager.
3. The “Meraki Management” profile is removed. All the profiles that Systems Manager pushed are also removed.
4. The “Meraki Management” profile is removed. All the profiles Systems Manager pushed remain.
5. Which two Systems Manager Live tools are available only for Apple Macs and Windows PCs and cannot be used on iOS or Android mobile devices? (Choose two.)
6. OS updates
7. Send notification
8. Selective wipe
9. Screenshot
10. Remote Desktop
11. Which order is accurate for a firmware upgrade on MX appliances in a high-availability configuration?
12. starts on the secondary MX appliance and then occurs on the primary MX appliance
13. starts on both MX appliances at the same time and then reboots both appliances after traffic on the primary MX appliance ceases
14. starts on both MX appliances at the same time and then immediately reboots both appliances
15. starts on the primary MX appliance and then occurs on the secondary MX appliance
16. Which three verbs of request are available in the Cisco Meraki API? (Choose three.)
17. SET
18. PUT
19. PATCH
20. ADD
21. POST
22. GET
23. Which Meraki Dashboard menu section is accessed to enable Sentry enrollment on an SSID?
24. Wireless > Configure > Access Control
25. Wireless > Configure > Splash page
26. Wireless > Configure > Firewall & Traffic Shaping
27. Wireless > Configure > SSIDs
28. What are two roles of the network and device tags in a Dashboard? (Choose two.)
29. Tags enable administrators to configure a combination of network and device specific tags to create summary reports filtered for specific devices across multiple networks.
30. Network tags can be used to assign networks to separate Auto VPN domains in an Organization with many networks.
31. Network tags can be used to simplify the assignment of network-level permissions in an Organization with many networks.
32. Device tags can be used to simplify the assignment of device-level permissions in an Organization with many administrators.
33. Device tags can be assigned to MR APs to influence the gateway selection for repeaters in a mesh wireless network.
34. Refer to the exhibit. Which outcome occurs when logging is set to Enabled?
35. Outbound flows are sent to a configured syslog server if a syslog sender is configured for flows.
36. The hits counter within this section is now enabled.
37. This firewall rule is now enabled.
38. Inbound flows are sent to a configured syslog server if a syslog server configured for flows.
39. Which API endpoint clones a new Organization?
40. POST /organizations/clone/{organizationId}
41. PUT /organizations/{organizationId}/clone
42. POST /organizations/{organizationId}/new
43. POST /organizations/{organizationId}/clone

# **TOPIC 5**

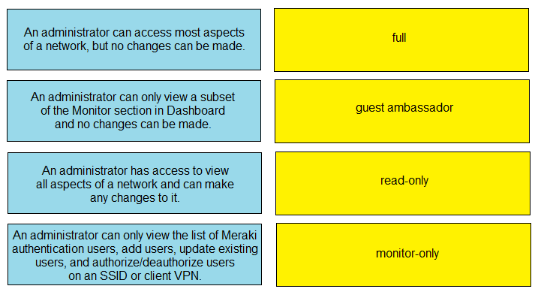
1. Drag and drop the settings from the left onto the available or non-available methods of applying a group policy to a Cisco Meraki MR access point on the right.



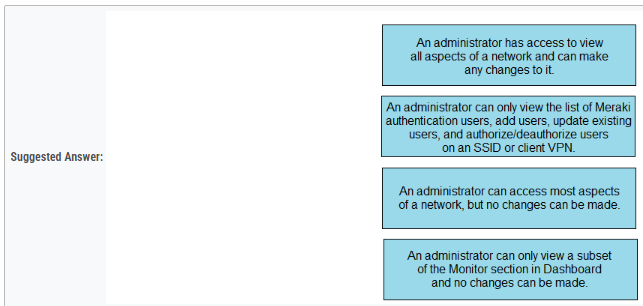
Answer:



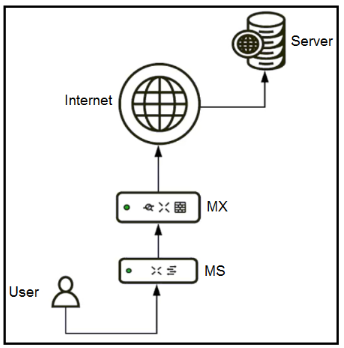
1. Which enrollment method must be used when containerization is required on BYOD Android devices managed by Systems Manager?
2. Systems Manager network ID
3. Android Enterprise utilizing a Work Profile
4. Android Business utilizing a BYOD Profile
5. Systems Manager container ID
6. A Cisco Meraki MX security appliance is trying to route a packet to the destination IP address of 172.18.24.12. Which routes contained in its routing table does it select?
7. Auto VPN route 172.18.0.0/16
8. non-Meraki VPN route 172.18.24.0/24
9. directly connected 172.18.16.0/20
10. static route 172.16.0.0/12
11. Drag and drop the descriptions from the left onto the permission types on the right.



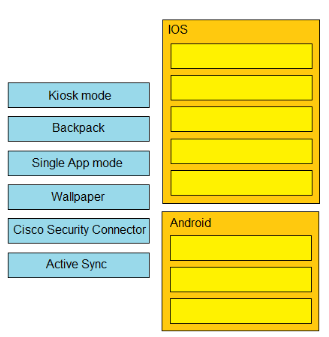
Answer:



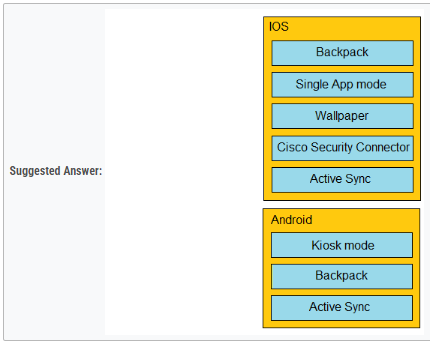
1. What is out of scope when considering the best practices for high-density wireless designs?
2. number of SSIDs
3. maximum beamforming
4. band selection
5. minimum bitrate
6. There will be 100 concurrent users streaming video to their laptops. A 30/70 split between 2.4 Ghz and 5 Ghz will be used. Roughly how many APs (rounded to the nearest whole number) are needed based on client count?
7. 2
8. 3
9. 4
10. 5
    1. The WAN connection of a Cisco Meraki MX security appliance is congested, and the MX appliance is buffering the traffic from LAN ports going to the WAN ports. High, normal, and low priority queue buffers are all full. Which proportion of the normal traffic is forwarded compared to the other queues?
11. 4/10 packets
12. 2/10 packets
13. 2/7 packets
14. 5/15 packets
    1. Refer to the exhibit. Which two configurations are needed to successfully monitor custom applications that a user is accessing using Cisco Meraki Insight? (Choose two.)



1. The custom application uses TLS on any ports.
2. The custom application uses HTTP on port 8080.
3. The custom application uses HTTPS on TCP 443.
4. The custom application uses SMB/CIFS.
5. The custom application uses HTTPS on port 8080.
   1. Drag and drop the settings from the left onto the OS system or systems that support it on the right. Settings can be used more than once.

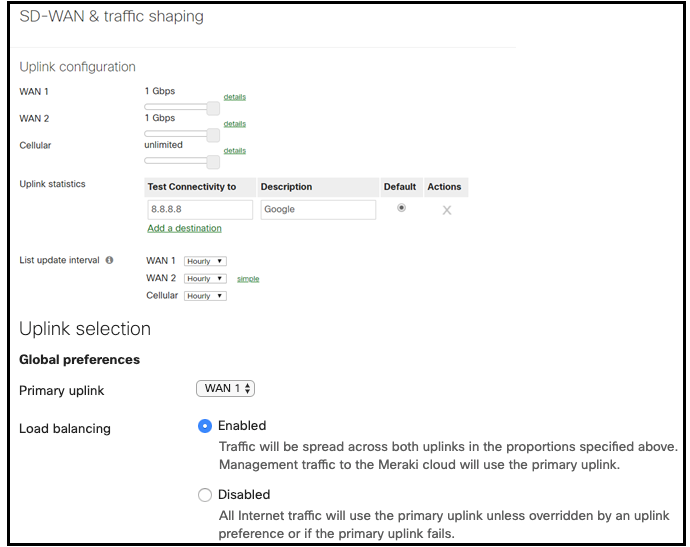


Answer:



* 1. Refer to the exhibit. Why does the end user complain of poor wireless performance

1. Channel 48 utilization is at 84 percent.
2. The client is using 20 MHz channel width to connect.
3. Non-802.11 traffic of 18 percent indicates poor AP placement.
4. The client is connected to the secondary radio of the AP instead of the primary radio.
   1. What is the default frequency of SD-WAN probes sent between VPN peers in a Cisco Meraki MX SD-WAN deployment?
5. 10 milliseconds
6. 100 milliseconds
7. 1 second
8. 10 seconds
   1. An organization requires that BYOD devices be enrolled in Systems Manager before they gain access to the network. Part of the enrollment includes pushing out the corporate SSID preshared key, corporate email settings, and some business-sensitive PDFs. When a user leaves the organization, which Systems Manager feature allows the removal of only the MDM-delivered content from the user’s device?
9. Unenroll Device
10. Clear Pushed Data
11. Selective Wipe
12. Erase Device
    1. Refer to the exhibit. What is the ratio of internet-bound flows that route via WAN 1 compared with WAN 2?



1. All flows egress via WAN 1.
2. All flows alternate in a 1:1 ratio.
3. All flows alternate in a 5:1 ratio.
4. All flows alternate in a 2:1 ratio.