DUMPSARENA

Implementing and Configuring Cisco Identity Services Engine (SISE) v4.0 (300-715 SISE)

Cisco 300-715

Version Demo

Total Demo Questions: 46

Total Premium Questions: 465

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Deployment	79
Topic 2, Policy Enforcement	84
Topic 3, Web Authentication and Guest Services	68
Topic 4, Profiling	65
Topic 5, BYOD	39
Topic 6, Endpoint Compliance	39
Topic 7, Network Access Device Administration	90
Topic 8, Mix Questions	1
Total	465

QUESTION NO: 1

What are two requirements of generating a single certificate in Cisco ISE by using a certificate provisioning portal, without generating a certificate signing request? (Choose two.)

A. Enter the IP address of the device.

B. Enter the common name.

C. Choose the hashing method.

D. Locate the CSV file for the device MAC.

E. Select the certificate template.

ANSWER: B E

Explanation:

Generating a single certificate without first submitting a certificate signing request uses the Certificate Provisioning Portal workflow in which Cisco ISE collects the certificate identity and issuance settings directly. **Enter the common name.** is required because the common name supplies the subject identity that is placed in the issued certificate. This identifies the endpoint, server, or device for which the certificate is being generated. The value must correspond to the identity expected by the intended authentication or service use case.

Select the certificate template. is also required because the template defines the certificate profile that the issuing CA applies. In particular, it governs certificate characteristics such as permitted subject information, validity constraints, key usage, enhanced key usage, and other CA policy settings. ISE must have both the subject identity and an applicable template in order to request and issue a certificate through this direct, non-CSR portal flow. Cisco documents the Certificate Provisioning Portal as a mechanism for generating certificates for endpoints and describes selecting a certificate template as part of certificate issuance configuration. See Cisco's Certificate Provisioning Portal guidance and the Cisco ISE certificate administration documentation.

QUESTION NO: 2

A network administrator changed a Cisco ISE deployment from pilot to production and noticed that the JVM memory utilization increased significantly. The administrator suspects this is due to replication between the nodes.

What must be configured to minimize performance degradation?

A. Enable the endpoint attribute filter.

B. Review the profiling policies for any misconfiguration.

C. Ensure that Cisco ISE is updated with the latest profiler feed update.

D. Change the reauthentication interval.

ANSWER: A

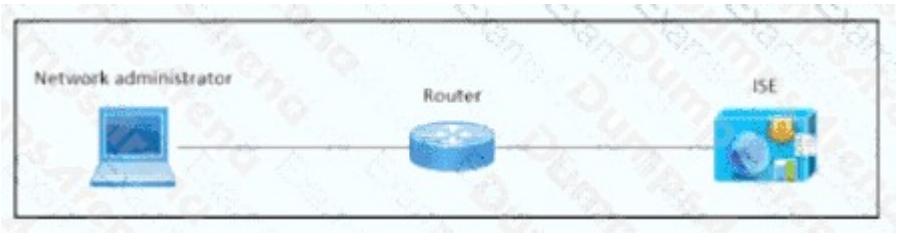
Explanation:

Enable the endpoint attribute filter. In a production Cisco ISE deployment, the endpoint database commonly grows substantially as more devices are profiled and more probe-derived attributes are collected. These endpoint records and their attributes are replicated among ISE nodes, so retaining every learned attribute can increase database size, replication processing, and Java virtual machine memory consumption. The endpoint attribute filter lets the administrator control which endpoint attributes are retained in the endpoint database. By excluding attributes that are not needed for endpoint classification, authorization, reporting, or operations, ISE reduces the amount of endpoint data that must be stored and synchronized between nodes. This directly minimizes replication-related resource use and helps preserve system performance as the deployment scales beyond a pilot environment. The filter should be planned around attributes actually required by profiling policies and other operational workflows, ensuring that unnecessary data is not replicated while required identification data remains available. Cisco documents endpoint attribute filtering as a mechanism for managing endpoint

attribute storage and replication impact in larger deployments. See the Cisco ISE Administrator Guide and Cisco's Identity Services Engine configuration guides.

QUESTION NO: 3 - (DRAG DROP)

Refer to the exhibit.



An engineer must configure Cisco ISE to be used as the TACACS+ server for any administrator that signs into the router. Users must be able to change their Telnet password through the TACACS+ server. Drag and drop the configuration steps from the left into the sequence on the right.

Enable Password Change Control.	step 1
Open Work Centers, open Device Administration, and then open Settings.	step 2
Select Enable Telnet Change Password.	step 3
Open the Session Key Assignment tab, and then click Save.	step 4

ANSWER:

Answer:

Answer:

Enable Password Change Control.	Open Work Centers, open Device Administration, and then open Settings.
Open Work Centers, open Device Administration, and then open Settings.	Enable Password Change Control.
Select Enable Telnet Change Password.	Select Enable Telnet Change Password.
Open the Session Key Assignment tab, and then click Save.	Open the Session Key Assignment tab, and then click Save.

Explanation:

Cisco ISE Device Administration settings are where TACACS+ administrative access behavior is configured. The process begins by navigating through Work Centers to Device Administration and then to Settings, because this is the location that exposes the global Device Admin password-change controls. Once on that page, Password Change Control must be enabled first. This turns on the ISE function that supports password-change transactions for TACACS+ device-administration users, allowing ISE to participate in the password-change workflow rather than only authenticating a normal login.

With the password-change function enabled, the Telnet-specific setting is selected. Enabling Telnet password change is the setting that permits an administrator using a Telnet session to initiate a password update through the TACACS+ server. The final action is to open the Session Key Assignment area and save the configuration. Saving from this configuration area

persists the selected password-change settings and makes them available for the TACACS+ device-administration flow. This sequence follows the normal Cisco ISE pattern of navigating to the feature area, enabling the parent capability, selecting the protocol-specific behavior, and saving the resulting configuration. Cisco documents Device Administration and TACACS+ configuration concepts in the Cisco ISE Administrator Guide and describes TACACS+ device administration in the Device Administration documentation.

QUESTION NO: 4

A network engineer needs to ensure that the access credentials are not exposed during the 802.1x authentication among components. Which two protocols should complete this task?

A. PEAP

B. EAP-MD5

C. LEAP

D. EAP-TLS

E. EAP-TTLS

ANSWER: A D E

Explanation:

PEAP, EAP-TLS, and EAP-TTLS each prevent access credentials from being exposed on the network during 802.1X authentication. PEAP first establishes a TLS tunnel between the endpoint and the authentication server. The client's inner authentication, commonly a username and password method such as MSCHAPv2, then occurs within that encrypted tunnel. EAP-TTLS uses the same essential protection model: TLS protects the outer exchange and carries the inner authentication credentials securely within the tunnel. EAP-TLS provides TLS-based mutual authentication using client and server certificates. Instead of transmitting a reusable password for authentication, the endpoint proves possession of its private key during the TLS handshake, while TLS protects the exchange from interception and tampering. These methods are appropriate for Cisco ISE deployments when the requirement is to avoid clear-text exposure of user credentials or other reusable authentication secrets between the supplicant, authenticator, and RADIUS server. EAP-TLS is generally preferred where certificate lifecycle management is practical, while PEAP and EAP-TTLS are commonly used when password-based inner authentication must be retained but protected. See RFC 5216: EAP-TLS Authentication Protocol and RFC 5281: EAP-TTLS.

QUESTION NO: 5

What should be considered when configuring certificates for BYOD?

A. An endpoint certificate is mandatory for the Cisco ISE BYOD

B. An Android endpoint uses EST whereas other operation systems use SCEP for enrollment

C. The CN field is populated with the endpoint host name.

D. The SAN field is populated with the end user name

ANSWER: A

Explanation:

An endpoint certificate is mandatory for Cisco ISE BYOD because certificate provisioning is the central outcome of the onboarding workflow. During onboarding, ISE redirects the user to the BYOD portal, registers the device, and provisions an identity certificate onto that managed endpoint through the configured certificate authority and enrollment method. The device can then use the installed certificate for strong, passwordless network authentication, typically EAP-TLS, on later wired or wireless connections.

This certificate establishes a durable cryptographic identity for the onboarded device and allows ISE authorization policy to distinguish an enrolled endpoint from an unknown device. It also supports certificate-based authentication without repeatedly relying on user passwords and enables policy decisions based on certificate identity details, certificate issuer, and device-registration context. Consequently, a functional BYOD design requires certificate services to be planned and configured, including the issuing CA, appropriate certificate template or profile settings, trust distribution, certificate lifetime, and renewal behavior. Cisco's BYOD documentation describes the provisioning of client certificates as part of endpoint onboarding and the use of those certificates for secure access. See Cisco ISE Administrator Guide: BYOD and Cisco ISE Administrator Guide: Certificate Management.

QUESTION NO: 6

Which supplicant(s) and server(s) are capable of supporting EAP-CHAINING?

A. Cisco Secure Services Client and Cisco Access Control Server

B. Cisco AnyConnect NAM and Cisco Identity Service Engine

C. Cisco AnyConnect NAM and Cisco Access Control Server

D. Windows Native Supplicant and Cisco Identity Service Engine

ANSWER: B

Explanation:

Cisco AnyConnect NAM and Cisco Identity Service Engine is the supported pairing for EAP-Chaining in this context. EAP-Chaining is a Cisco enhancement used with EAP-FAST that places both machine and user authentication information into one authentication process. This gives the policy server reliable context for both the endpoint and the logged-in user, allowing authorization policy to use conditions such as the machine identity, user identity, AD group membership, endpoint attributes, and posture state together rather than treating the machine and user authentications as unrelated events.

Cisco AnyConnect Network Access Manager acts as the capable endpoint supplicant because it implements the Cisco EAP-FAST chaining functionality and can provide the machine and user portions of the chained exchange. Cisco Identity Services Engine is the capable RADIUS policy server because it processes EAP-FAST authentication, recognizes the chained identities, and applies authorization policy using the resulting combined context. This capability is particularly useful for wired or wireless enterprise access designs that must ensure that both a managed corporate device and an authorized user are present before granting access. Cisco describes the EAP-FAST chaining implementation at Understanding EAP-FAST and Chaining; ISE product and deployment information is available at Cisco Identity Services Engine.

QUESTION NO: 7

An administrator is manually adding a device to a Cisco ISE identity group to ensure that it is able to access the network when needed without authentication Upon testing, the administrator notices

that the device never hits the correct authorization policy line using the condition EndPoints LogicalProfile EQUALS static_list Why is this occurring?

A. The dynamic logical profile is overriding the statically assigned profile

B. The device is changing identity groups after profiling instead ot remaining static

C. The logical profile is being statically assigned instead of the identity group

D. The identity group is being assigned instead of the logical profile

ANSWER: D

Explanation:

The identity group is being assigned instead of the logical profile is correct because Cisco ISE treats endpoint identity groups and endpoint logical profiles as distinct endpoint attributes. Manually placing an endpoint in an identity group changes the

endpoint's group membership; it does not populate the *EndPoints:LogicalProfile* attribute evaluated by the authorization condition. Therefore, a rule that tests whether *EndPoints LogicalProfile EQUALS static_list* requires the endpoint itself to have `static_list` as its logical profile.

Logical profiles are associated with endpoint profiling. ISE can derive them from configured profiling policies based on collected endpoint attributes, or an administrator can assign a static logical profile directly to an endpoint record when that workflow is appropriate. For the intended authorization rule to match, the administrator must configure profiling so the device is classified into `static_list`, or assign `static_list` as the endpoint's static logical profile. Assigning an identity group alone supports policy conditions that explicitly evaluate endpoint identity-group membership, but it does not satisfy a condition evaluating the logical-profile field. Cisco documents endpoint profiling and logical-profile assignment in its ISE administration guidance: Cisco ISE Admin Guide: Profiling and Cisco ISE Admin Guide: Endpoint Device Administration.

QUESTION NO: 8

Which two events trigger a CoA for an endpoint when CoA is enabled globally for ReAuth? (Choose two.)

A. endpoint marked as lost in My Devices Portal

B. addition of endpoint to My Devices Portal

C. endpoint profile transition from Apple-Device to Apple-iPhone

D. endpoint profile transition from Unknown to Windows 10-Workstation

E. updating of endpoint dACL.

ANSWER: C D

Explanation:

When Cisco ISE has Change of Authorization enabled globally for reauthentication, a profiling reclassification can cause ISE to send a CoA Reauth to the network access device. This lets the device immediately reevaluate the endpoint's authorization using its newly determined endpoint profile, rather than waiting for the existing session to expire or for the endpoint to reconnect. Therefore, an endpoint profile transition from Apple-Device to Apple-iPhone triggers the reauthentication workflow because profiling has refined the endpoint classification. Likewise, a transition from Unknown to Windows 10-Workstation triggers CoA because ISE has moved the endpoint from an unclassified state to a recognized profile. In each case, the profile change can alter the authorization result selected by policy, and CoA ensures that the active access session is reevaluated promptly with the updated profiling information. Cisco documents profiling, endpoint classification, and related authorization behavior in its ISE administration guides; see the Cisco ISE Administrator Guide and Cisco's Identity Services Engine configuration guide index.

QUESTION NO: 9

An organization is implementing Cisco ISE posture services and must ensure that a host-based firewall is in place on every Windows and Mac computer that attempts to access the network. They have multiple vendors' firewall applications for their devices, so the engineers creating the policies are unable to use a specific application check in order to validate the posture for this.

What should be done to enable this type of posture check?

A. Enable the default application condition to identify the applications installed and validate the firewall app.

B. Enable the default firewall condition to check for any vendor firewall application.

C. Use a compound condition to look for the Windows or Mac native firewall applications.

D. Use the file registry condition to ensure that the firewall is installed and running appropriately.

ANSWER: B

Explanation:

Enable the default firewall condition to check for any vendor firewall application. Cisco ISE Posture includes a built-in Firewall condition intended to assess the endpoint firewall security control without requiring policy authors to identify a particular vendor's executable, file path, registry value, or application name. This is appropriate for a mixed endpoint estate in which Windows and macOS devices can use different firewall products. The Cisco Secure Client posture module gathers the endpoint posture data and reports the firewall state to ISE, allowing the posture policy to determine whether the firewall requirement is satisfied and to apply the configured remediation or authorization result when it is not. Using the standard firewall condition makes the policy durable across supported firewall vendors and product updates because the policy evaluates the firewall control rather than an implementation-specific artifact. Cisco documents Firewall as a native posture requirement/condition type in the ISE posture policy configuration workflow. See the Cisco ISE Posture Administration Guide and Cisco's Cisco Secure Client product documentation for posture-module capabilities and deployment details.

QUESTION NO: 10

A network engineer must configure BYOD using Cisco ISE. In the deployment, the users must be able to submit CSR through the end devices. Which two features must be enabled to meet the

requirement? (Choose two.)

A. Define a certificate group tag.

B. A new BYOD portal must be created.

C. A certificate provisioning portal must be configured.

D. Cisco ISE Internal CA service must be enabled.

E. Add SuperAdmin account into portal admin group.

ANSWER: C D

Explanation:

A certificate provisioning portal must be configured because this portal provides the endpoint-facing certificate enrollment workflow used during Cisco ISE BYOD onboarding. It redirects or guides an authorized user through device registration and certificate provisioning, enabling the endpoint to generate and submit the certificate signing request needed to obtain an identity certificate. The resulting endpoint certificate can subsequently be used for certificate-based network authentication, such as EAP-TLS.

Cisco ISE Internal CA service must be enabled because ISE needs an issuing certificate authority available to process and sign the certificate request in an ISE-managed BYOD certificate deployment. After the Internal CA service is enabled and its certificate authority hierarchy is configured, ISE can issue endpoint certificates through the certificate provisioning workflow. This combines an enrollment interface for the user device with the CA capability that creates the signed certificate, which is the required end-to-end functionality for CSR-based BYOD provisioning. Cisco documents the BYOD certificate-provisioning workflow and its use of the ISE internal certificate authority in the Cisco ISE BYOD administration guide and documents Internal CA configuration in the Cisco ISE certificate administration guide.

QUESTION NO: 11

Refer to the exhibit.

ISE Nodes	
PAN	192.168.255.15
MnT	192.168.255.16
PSN	192.168.255.17
PSN	192.168.255.18
PSN	192.168.255.19

Which two configurations are needed on a catalyst switch for it to be added as a network access device in a Cisco ISE that is being used for 802 1X authentications? (Choose two)



A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

ANSWER: A C

Explanation:

A Catalyst switch acting as a network access device must have a reachable Layer 3 management IP address configured. Cisco ISE uses this IP address to identify the source network device for incoming RADIUS packets; the same address must be entered as the device IP address when the switch is defined under *Administration > Network Resources > Network Devices* in ISE. The switch and ISE must also be configured with an identical RADIUS shared secret. This secret is used to authenticate and protect the RADIUS communication between the authenticator (the switch) and Cisco ISE. On the switch, the secret is configured as part of the RADIUS server or RADIUS server group configuration; in ISE, it is configured in the

network-device RADIUS Authentication Settings section. These two settings establish the trusted RADIUS relationship required before the switch can submit 802.1X authentication requests to ISE. Cisco documents the need to define the network device IP address and RADIUS shared secret when adding a network device, and to configure corresponding RADIUS server settings on the NAD. See Cisco ISE Network Access Administration Guide and Cisco IOS XE IEEE 802.1X Configuration Guide.

QUESTION NO: 12

Which three default endpoint identity groups does Cisco ISE create? (Choose three.)

A. endpoint

B. unknown

C. block list

D. profiled

E. allow list

ANSWER: B C D

Explanation:

Cisco ISE creates the default endpoint identity groups *unknown*, *block list*, and *profiled* to provide immediate endpoint classification for access-control policy. The *unknown* group is the initial classification for endpoints that ISE has not yet identified through profiling data or an assigned identity group. It provides a practical baseline condition that policy can use while endpoint discovery and classification are incomplete. The *profiled* group is used for endpoints for which ISE profiling has determined endpoint characteristics, allowing more granular policy decisions based on the endpoint type and associated profile. The *block list* group identifies endpoints that are explicitly blocked, enabling administrators to apply deny or containment authorization results consistently when those endpoints attempt network access. These built-in groups are available in the endpoint identity-group configuration and can be referenced in authorization policy conditions; administrators can additionally create custom endpoint identity groups to suit their organization's classifications and policy design. Cisco documents endpoint identity groups and their role in endpoint management in the Cisco ISE Administrator Guide and the Cisco ISE Identity Management Guide.

QUESTION NO: 13

While configuring Cisco TrustSec on Cisco IOS devices the engineer must set the CTS device ID and password in order for the devices to authenticate with each other. However after this is complete the devices are not able to property authenticate What issue would cause this to happen even if the device ID and passwords are correct?

A. The device aliases are not matching

B. The 5GT mappings have not been defined

C. The devices are missing the configuration cts credentials trustsec

D. EAP-FAST is not enabled

ANSWER: C

Explanation:

The devices are missing the `cts credentials trustsec` configuration is correct because configuring a CTS device ID and password only defines the credentials that the Cisco IOS device will use. The device must also be configured to use those credentials for Cisco TrustSec credential enrollment and authentication. The `cts credentials trustsec` command initiates the TrustSec credential process with the configured AAA infrastructure, allowing the device to obtain and use the TrustSec credentials needed for authenticated TrustSec operation. In a typical deployment, the device has reachable AAA servers, appropriate RADIUS configuration, and an Identity Services Engine policy that permits the network device to

authenticate. After credentials are successfully provisioned, Cisco TrustSec can establish authenticated security associations with neighboring TrustSec-capable devices and exchange the authorization information required to apply TrustSec policy. The relevant operational state can be checked with commands such as `show cts credentials` and `show cts environment-data`. Cisco's TrustSec configuration documentation describes configuring device credentials followed by TrustSec credential enrollment: Cisco IOS XE TrustSec Credentials Configuration Guide. Cisco also provides an overview of the device authentication and credential-provisioning model in its Cisco TrustSec documentation.

QUESTION NO: 14

What allows an endpoint to obtain a digital certificate from Cisco ISE during a BYOD flow?

A. Application Visibility and Control

B. Supplicant Provisioning Wizard

C. My Devices Portal

D. Network Access Control

ANSWER: B

Explanation:

Supplicant Provisioning Wizard is correct because it is the Cisco ISE BYOD onboarding component that runs on, or is delivered to, the endpoint to provision secure network access settings. During BYOD onboarding, ISE identifies the endpoint operating system and directs the user through the appropriate provisioning workflow. The Supplicant Provisioning Wizard configures the device's wired or wireless supplicant for the required authentication method and performs certificate enrollment when certificate-based authentication, such as EAP-TLS, is used. It obtains a client certificate through Cisco ISE's certificate provisioning process, using the ISE internal certificate authority or a configured external certificate authority, and installs the resulting certificate and related configuration on the endpoint. This gives the device a credential that can subsequently be presented for certificate-based network authentication, allowing ISE to recognize the enrolled device as part of the BYOD process. Cisco's BYOD documentation describes provisioning as the process that configures the endpoint's supplicant and provisions certificates needed for secure access. See the Cisco ISE BYOD administration guide and Cisco's Identity Services Engine configuration guides.

QUESTION NO: 15

A network administrator is configuring authorization policies on Cisco ISE There is a requirement to use AD group assignments to control access to network resources After a recent power failure and Cisco ISE rebooting itself, the AD group assignments no longer work What is the cause of this issue?

A. The AD join point is no longer connected.

B. The AD DNS response is slow.

C. The certificate checks are not being conducted.

D. The network devices ports are shut down.

ANSWER: A

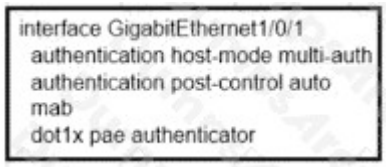
Explanation:

The AD join point is no longer connected. Cisco ISE authorization rules that use Active Directory group membership require a functioning AD join point and communication with the configured domain controllers. ISE uses its AD integration to look up a successfully authenticated user's group memberships and expose those memberships as identity attributes that authorization policy conditions can evaluate. If the ISE node restarts after a power failure and its AD connection does not recover, group lookup cannot be completed. Consequently, authorization conditions based on AD groups no longer receive the required group information and do not match as intended.

The ISE administrator should check the AD join point status and connectivity from the ISE administration interface, verify that domain controllers and DNS are reachable, and confirm that the ISE machine account's secure relationship with the domain remains valid. If the join point remains disconnected, restoring connectivity or leaving and rejoining the ISE node to the domain, as appropriate for the reported status, restores the ability to retrieve AD group membership for authorization. Cisco documents that AD join points must be connected and operational for AD identity and group-based authorization processing. See the Cisco ISE Active Directory integration documentation and Cisco ISE CLI Reference for AD status and troubleshooting information.

QUESTION NO: 16

Refer to the exhibit.



Which switch configuration change will allow only one voice and one data endpoint on each port?

A. Multi-auth to multi-domain

B. Mab to dot1x

C. Auto to manual

D. Multi-auth to single-auth

ANSWER: A

Explanation:

Multi-auth to multi-domain is correct because the Cisco Auth Manager host mode must be changed to `multi-domain` when a switch access port supports an IP phone and a single endpoint connected through that phone. Multi-domain authentication creates separate authorization domains for the voice and data roles on the same physical port. It therefore permits one authenticated device in the voice domain, typically the IP phone using the voice VLAN, and one authenticated device in the data domain, such as a workstation using the access VLAN. This behavior matches the stated requirement of allowing only one voice endpoint and one data endpoint per port while retaining independent authentication and authorization decisions for each domain. On Cisco switches, this is configured with the `authentication host-mode multi-domain` interface command as part of the IEEE 802.1X/MAB access-policy configuration. Cisco documents multi-domain mode as supporting one voice device and one data device on an access interface. See Cisco's IEEE 802.1X policy configuration guide and the Cisco Community discussion of multi-auth and multi-domain host modes.

QUESTION NO: 17

Which two fields are available when creating an endpoint on the context visibility page of Cisco IS? (Choose two)

A. Policy Assignment

B. Endpoint Family

C. Identity Group Assignment

D. Security Group Tag

E. IP Address

ANSWER: A C

Explanation:

When an administrator manually creates an endpoint in Cisco ISE Context Visibility, **Policy Assignment** and **Identity Group Assignment** are available assignment fields. Policy Assignment is used to associate the endpoint with the appropriate endpoint policy context, allowing Cisco ISE to apply endpoint-specific handling and classification-related policy logic. Identity Group Assignment places the endpoint into an endpoint identity group. This grouping is important because endpoint identity groups can be referenced in authorization policy conditions, enabling differentiated network access decisions for categories of endpoints.

Manual endpoint creation is useful for known devices that must be defined before they are observed through profiling or authentication activity. Cisco ISE stores endpoint identity information and uses endpoint groups and policy-related attributes as part of its contextual data for policy evaluation. Administrators can subsequently use this context in authorization rules to assign access based on the endpoint's established identity and associated policy settings. Cisco's ISE administration documentation describes Context Visibility endpoint management and the endpoint attributes available to administrators: Cisco ISE Administrator Guide. Additional Cisco documentation on endpoint identity and contextual policy use is available at Cisco Identity Services Engine.

QUESTION NO: 18

An engineer is configuring TACACS+ within Cisco ISE for use with a non-Cisco network device. They need to send special attributes in the Access-Accept response to ensure that the users are given the appropriate access. What must be configured to accomplish this'?

A. dACLs to enforce the various access policies for the users

B. custom access conditions for defining the different roles

C. shell profiles with custom attributes that define the various roles

D. TACACS+ command sets to provide appropriate access

ANSWER: C

Explanation:

shell profiles with custom attributes that define the various roles is correct because a TACACS+ shell profile is the Cisco ISE authorization-result component used to return session attributes to an administered device after a user has been authorized. Within the shell profile, the administrator can configure custom attributes, including vendor-specific attribute-value pairs required by a non-Cisco device. The device interprets those returned attributes to assign the authenticated administrator the intended role, privilege level, administrative domain, or other device-specific access context.

The shell profile is then selected in the applicable TACACS+ authorization policy rule. When that rule matches, ISE includes the shell-profile attributes in its TACACS+ authorization response. This makes shell profiles the appropriate configuration point whenever the requirement is to deliver special, device-dependent authorization data rather than merely evaluate policy conditions. Cisco documents TACACS+ authorization policies as returning authorization results that can include shell profiles, and documents custom attributes in shell profiles for devices that need attribute formats beyond the standard Cisco privilege-level settings. See the Cisco ISE Administrator Guide: TACACS+ Device Administration and Cisco's Identity Services Engine configuration-guide library.

QUESTION NO: 19

An administrator needs to allow guest devices to connect to a private network without requiring usernames and passwords. Which two features must be configured to allow for this? (Choose two.)

A. hotspot guest portal

B. device registration WebAuth

C. central WebAuth

D. local WebAuth

E. self-registered guest portal

ANSWER: A C

Explanation:

The **hotspot guest portal** is Cisco ISE's passwordless guest-access portal type. It presents guests with a configurable acceptable-use-policy or terms-and-conditions page and authorizes access after the guest accepts it; it does not require the guest to enter credentials or create an account. This provides an appropriate low-friction workflow while retaining a record of the acceptance event and enabling ISE authorization policy to limit the resulting network access.

Central WebAuth supplies the redirection mechanism that sends an unauthenticated endpoint's web request from the network access device to the Cisco ISE guest portal. ISE then hosts and processes the portal interaction centrally, allowing the hotspot acceptance flow to occur before the authorization result is returned to the access device. In practice, the authorization policy redirects guests to the selected hotspot portal and, following successful portal acceptance, applies the intended guest-access authorization profile. Cisco documents hotspot portals as a guest-access option that does not require credential entry and documents Central Web Authentication as the redirection architecture used for ISE-hosted web portals. See Cisco's Identity Services Engine Administrator Guide and the Cisco ISE installation and configuration guides.

QUESTION NO: 20

An engineer is tasked with placing a guest access anchor controller in the DMZ. Which two ports or port sets must be opened up on the firewall to accomplish this task? (Choose two.)

A. UDP ports 1812 and 1813 for RADIUS

B. TCP port 161

C. C. TCP port 514

D. UDP port 79

E. UDP ports 16666 and 16667 for mobility

ANSWER: A E

Explanation:

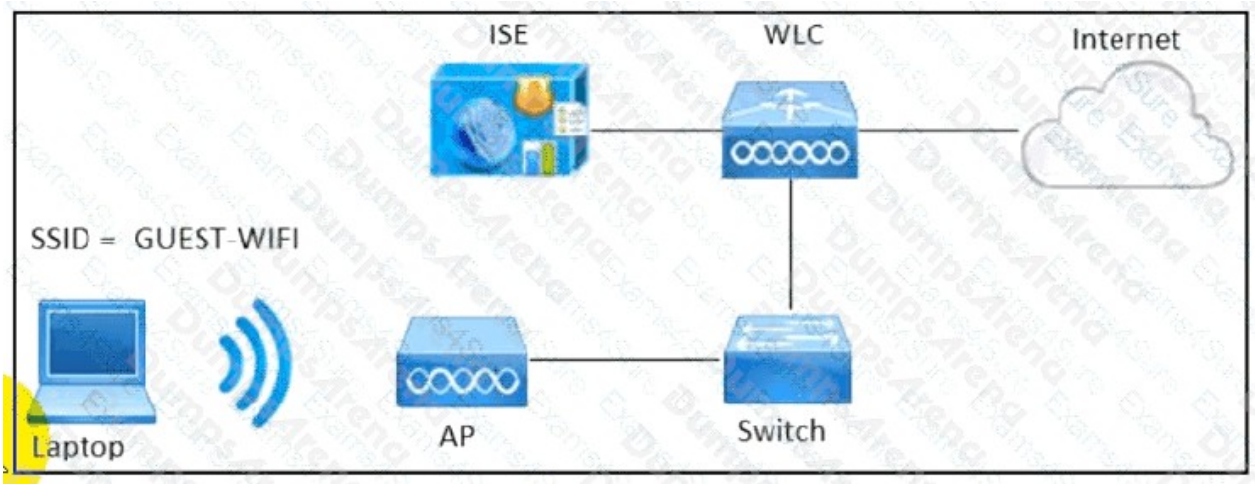
A guest anchor controller in a DMZ needs connectivity for both guest-user authentication and mobility tunneling with the internal foreign controller. **UDP ports 1812 and 1813 for RADIUS** permit the anchor controller to send RADIUS authentication requests and receive related accounting responses when Cisco ISE or another RADIUS server provides guest authentication and accounting services. RADIUS is a UDP-based protocol; 1812 is the standard authentication port and 1813 is the standard accounting port.

UDP ports 16666 and 16667 for mobility are required between the internal foreign controller and the DMZ guest anchor controller. Cisco wireless controllers use these mobility ports to establish the mobility relationship and carry guest client traffic that is anchored to the DMZ controller. This separation allows guest traffic to remain isolated from the internal enterprise network while still allowing clients to associate through internal access points.

Firewall policy should permit these flows only between the specific controller and RADIUS endpoints involved, rather than broadly exposing the services. Cisco documents mobility UDP ports 16666 and 16667 in its controller port and protocol guidance, and documents the RADIUS authentication and accounting port assignments in its ISE guidance. See Cisco Wireless Controller Ports and Protocols and Cisco ISE Administrator Guide.

QUESTION NO: 21

Refer to the exhibit.



An engineer must configure the guest access settings in Cisco IS

E.

• Configured the Wireless LAN Controller and added it as a network device in Cisco IS

E.

• Created an endpoint identity group and a self-registered guest type.

• Configured SMTP and the registration form to send credentials by email.

Which two types of profiles must be configured next in Cisco ISE to meet the requirement? (Choose two.)

A. An authorization profile to allow internet access

B. An authorization profile to redirect users to the guest portal

C. An authorization profile to redirect users to the sponsor portal

D. An authentication profile to allow access to the guest portal

E. An authentication profile to allow internet access

ANSWER: A B

Explanation:

Guest access through Cisco ISE Central Web Authentication requires authorization results at two distinct points in the guest lifecycle. Before a guest has registered or authenticated, the wireless controller needs an authorization result that applies web redirection. The authorization profile to redirect users to the guest portal supplies the Central Web Authentication redirect attributes, enabling the client browser to reach the configured self-registration portal. This lets the guest complete registration and receive the credentials that were configured for delivery by email.

After the guest submits valid credentials and ISE identifies the session as an authorized guest, ISE must return an authorization result that defines the access granted to that guest. The authorization profile to allow internet access is the post-authentication result and can apply the organization's intended guest-access controls, such as an internet-only VLAN assignment, a downloadable ACL, or equivalent access restrictions. In practice, these profiles are selected by separate authorization-policy rules: one matching the unauthenticated redirect state and one matching the successfully authenticated guest identity or guest endpoint state. Cisco documents guest portal redirection and the associated authorization-policy workflow in its Cisco ISE Guest Access Deployment Guide and its Cisco ISE Administrator Guide.

QUESTION NO: 22

What is a method for transporting security group tags throughout the network?

A. by embedding the security group tag in the 802.1Q header

B. by the Security Group Tag Exchange Protocol

C. by enabling 802.1AE on every network device

D. by embedding the security group tag in the IP header

ANSWER: B

Explanation:

by the Security Group Tag Exchange Protocol is correct. Security Group Tag Exchange Protocol (SXP) is a Cisco TrustSec control-plane protocol used to distribute IP-address-to-Security-Group-Tag bindings between network devices. Rather than requiring every device in the path to receive an inline tag, an SXP speaker can advertise the learned binding to an SXP peer. The receiving device then associates the endpoint IP address with the appropriate Security Group Tag and can use that group context when enforcing TrustSec policy.

This mechanism is particularly valuable where inline TrustSec tagging is unavailable or impractical, including certain Layer 3 boundaries and integrations with devices that must receive group context through binding exchange. Cisco ISE can act as part of the centralized TrustSec policy architecture, while switches, routers, firewalls, and other supported enforcement devices use the propagated bindings to apply Security Group Access Control Lists. In this way, the endpoint's logical security classification can remain available across network segments, supporting consistent identity-based segmentation and policy enforcement. Cisco documents SXP as the protocol for propagating IP-to-SGT bindings within TrustSec deployments. See the Cisco TrustSec overview and Cisco's ISE TrustSec administration documentation.

QUESTION NO: 23 - (SIMULATION)

Drag the Cisco ISE node types from the left onto the appropriate purposes on the right.



ANSWER: See the explanation for the answer

Explanation:

Match the Cisco ISE node types as follows:

Administration nodes host the ISE configuration and administration functions. Policy Service Nodes (PSNs) process access requests and enforce policy decisions. Monitoring nodes provide logging, reporting, and troubleshooting visibility. pxGrid nodes publish ISE context to integrated subscriber systems.

QUESTION NO: 24

Which profiling probe collects the user-agent string?

A. DHCP

B. HTTP

C. NMAP

D. AD

ANSWER: B

Explanation:

HTTP is the profiling probe that collects the user-agent string. When HTTP profiling is enabled, Cisco ISE examines HTTP traffic observed from endpoints and extracts attributes from HTTP headers. The `User-Agent` request header identifies characteristics of the software making the request, such as the browser or HTTP client, operating-system indicators, and, in many cases, distinctive application or device-family information. ISE stores the collected value as an endpoint attribute that can be evaluated by profiling policies. This gives the profiling engine useful evidence for classifying endpoints, particularly when the user-agent value is combined with attributes from other enabled probes and contextual sources. HTTP-derived attributes are passive observations: ISE receives the relevant traffic information from network devices configured to forward it, rather than requiring an interactive scan of the endpoint. Cisco documents HTTP as one of the probes used by the Profiler service and identifies HTTP header fields, including User-Agent, as data available for endpoint profiling. See Cisco's ISE Profiler administration documentation and the Cisco ISE configuration guides.

QUESTION NO: 25

An administrator is configuring the Native Supplicant Profile to be used with the Cisco ISE posture agents and needs to test the connection using wired devices to determine which profile settings are

available. Which two configuration settings should be used to accomplish this task? (Choose two.)

A. authentication mode

B. proxy host/IP

C. certificate template

D. security

E. allowed protocol

ANSWER: A D

Explanation:

For a wired Native Supplicant Profile, the applicable configuration areas are **authentication mode** and **security**. Authentication mode controls the identity context that the Windows wired 802.1X supplicant uses when it attempts network access. Depending on the profile and endpoint requirements, this can support user authentication, computer authentication, or user-or-computer authentication. This setting is particularly important for posture because the endpoint may need network access before a user signs in, after sign-in, or during a transition between machine and user authentication.

The security configuration defines the wired 802.1X security behavior, including the EAP authentication configuration and certificate/server-validation details required by the native operating-system supplicant. These settings enable the endpoint to establish the secure wired connection that permits Cisco ISE to apply authentication and posture workflows. Cisco ISE uses Native Supplicant Profiles to deliver the appropriate wired or wireless supplicant settings to supported endpoints through client provisioning. See Cisco's Identity Services Engine configuration guides and the Cisco Secure Client configuration guides for platform-specific Native Supplicant Profile and posture-agent configuration details.

QUESTION NO: 26

An administrator is configuring a Cisco ISE guest portal authorization profile with URL redirection. Which two destinations must be permitted by the preauthentication redirect ACL so that a guest endpoint can resolve and reach the guest portal? (Choose two.)

A. DNS servers

B. The Cisco ISE guest portal address

C. Internal file servers

D. All corporate application servers

E. The Active Directory domain controllers

ANSWER: A B

Explanation:

DNS servers must be permitted so that the guest endpoint can resolve the fully qualified domain name used for the Cisco ISE guest portal. If DNS traffic is redirected or denied before portal authentication, the endpoint may be unable to locate the portal hostname.

The Cisco ISE guest portal address must also be permitted. The redirect ACL identifies traffic that bypasses web redirection and is allowed during the preauthentication state. Allowing the required HTTPS traffic to the ISE portal enables the endpoint to load the portal and complete the guest authentication workflow. Other traffic remains subject to redirection or restriction until Cisco ISE returns the postauthentication authorization result. Cisco describes guest-access redirection and authorization profiles in the Cisco ISE Administrator Guide.

QUESTION NO: 27

Which two events trigger a CoA for an endpoint when CoA is enabled globally for ReAuth? (Choose two.)

A. addition of endpoint to My Devices Portal

B. endpoint marked as lost in My Devices Portal

C. updating of endpoint dACL

D. endpoint profile transition from Apple-device to Apple-iPhone

E. endpoint profile transition from Unknown to Windows10-Workstation

ANSWER: D E

Explanation:

When Cisco ISE is configured to send Change of Authorization (CoA) for global reauthentication events, a meaningful endpoint profiling change causes ISE to request a new authorization decision from the network access device. Therefore, **endpoint profile transition from Apple-device to Apple-iPhone** is a CoA trigger: the profiler has refined the endpoint classification, and authorization policy may need to apply access controls specific to an iPhone rather than a more general Apple-device profile.

Likewise, **endpoint profile transition from Unknown to Windows10-Workstation** triggers CoA because ISE has acquired enough profiling evidence to replace the initial unknown classification with a recognized Windows workstation profile. CoA enables policy based on that new classification to take effect during the active session rather than waiting for a periodic reauthentication interval or a user reconnect. This supports immediate enforcement of the authorization result, such as the appropriate authorization profile, downloadable ACL, VLAN, or Security Group Tag associated with the newly identified endpoint type. Cisco ISE documentation describes profiling as a mechanism for classifying endpoints and applying policy based on that classification; CoA is the RADIUS mechanism used to dynamically alter an active session. See Cisco's Identity Services Engine installation and configuration guides and the RADIUS dynamic authorization specification in RFC 5176.

QUESTION NO: 28

A network engineer needs to ensure that the access credentials are not exposed during the 802.1X authentication among components.

Which two protocols should be configured to accomplish this task? (Choose two.)

A. PEAP

B. EAP-TLS

C. EAP-MD5

D. EAP-TTLS

E. LEAP

ANSWER: A D

Explanation:

PEAP and EAP-TTLS protect password-based access credentials by first establishing a TLS-protected tunnel between the endpoint supplicant and the RADIUS authentication server, such as Cisco ISE. The user authentication exchange is then performed inside that encrypted tunnel rather than being exposed on the access network. This is particularly important when an inner method uses a username and password, because the credentials are protected while traversing the authenticator and RADIUS infrastructure.

PEAP uses the server certificate to authenticate the server and create the TLS tunnel; a common deployment then uses an inner EAP method such as EAP-MSCHAPv2 for user authentication. EAP-TTLS similarly creates a TLS tunnel using server-side certificate authentication, then carries an inner authentication exchange within the protected channel. In both cases, the endpoint must validate the authentication server certificate to prevent a rogue server from impersonating the legitimate network and capturing credentials.

Cisco ISE supports these tunneled EAP methods for wired and wireless 802.1X deployments. Cisco's guidance on EAP protocol selection and configuration is available in the Cisco ISE Administration Guide. The TLS tunneling behavior for EAP-TTLS is also defined in RFC 5281.

QUESTION NO: 29

Wireless network users authenticate to Cisco ISE using 802.1X through a Cisco Catalyst switch. An engineer must create an updated configuration to assign a security group tag to the user ' s traffic using inline tagging to prevent unauthenticated users from accessing a restricted server. The configurations were performed:

• configured Cisco ISE as a Cisco TrustSec AAA server

• configured the switch as a RADIUS device in Cisco ISE

• configured the wireless LAN controller as a TrustSec device in Cisco ISE

• created a security group tog for the wireless users

• created a certificate authentication profile

? created an identity source sequence

• assigned an appropriate security group tag to the wireless users

• defined security group access control lists to specify an egress policy

• enforced the access control lists on the TrustSec policy matrix in Cisco ISE

• configured TrustSec on the switch

• configured TrustSec on the wireless LAN controller

Which two actions must be taken to complete the configuration? (Choose two.)

A. Configure Security Group Tag Exchange Protocol on the wireless LAN controller.

B. Configure Security Group Tag Exchange Protocol to distribute IP to security group tags on Cisco ISE.

C. Configure inline tag propagation on the switch and wireless LAN controller.

D. Create static IP-to-SGT mapping for the restricted web server.

E. Configure Security Group Tag Exchange Protocol on the switch.

ANSWER: B C

Explanation:

Configure Security Group Tag Exchange Protocol to distribute IP to security group tags on Cisco ISE and configure inline tag propagation on the switch and wireless LAN controller. The wireless LAN controller learns the user identity and assigned security group tag as part of the authentication and authorization process. Security Group Tag Exchange Protocol provides the IP-address-to-security-group-tag binding information required for TrustSec-aware devices and Cisco ISE to maintain consistent identity-to-IP association for the wireless endpoint. This binding distribution is particularly important where the endpoint's traffic is represented by its IP address after wireless termination.

Inline tag propagation must also be enabled on both the switch and the wireless LAN controller so that the assigned tag is carried with the user traffic across the TrustSec-capable path. The downstream enforcement point can then evaluate the security group access control list selected by the TrustSec policy matrix and deny access to the restricted server for traffic that does not have the required security group tag. Together, binding exchange and inline propagation ensure that the authorization decision made by Cisco ISE is preserved and enforceable in the data plane. Cisco documents TrustSec policy, security group tags, and binding distribution in the Cisco ISE TrustSec administration guide and the Cisco IOS XE TrustSec configuration guide.

QUESTION NO: 30

Which two actions occur when a Cisco ISE server device administrator logs in to a device? (Choose two)

A. The device queries the internal identity store

B. The Cisco ISE server queries the internal identity store

C. The device queries the external identity store

D. The Cisco ISE server queries the external identity store.

E. The device queries the Cisco ISE authorization server

ANSWER: B D

Explanation:

For Cisco ISE device administration, the network device is configured as a TACACS+ client. When an administrator initiates a login, the device sends the TACACS+ authentication request to Cisco ISE, which acts as the centralized AAA policy decision point. Cisco ISE evaluates the Device Admin authentication policy and uses the identity source or identity source sequence selected by that policy to validate the administrator's credentials. Consequently, Cisco ISE can query its internal identity store for locally defined administrative accounts, and it can query an external identity store, such as Microsoft Active Directory or LDAP, for externally managed accounts. In an identity source sequence, ISE can use the configured stores and their lookup order to locate the user and authenticate the submitted credentials. After authentication succeeds, ISE continues with TACACS+ authorization to apply the appropriate shell profile, privilege level, and command set for that administrator. This centralized process lets organizations use consistent device-access identities and policies without requiring each managed device to perform directory lookups itself. Cisco documents that Device Administration uses TACACS+ and that authentication policy specifies the identity source used for authentication. See the Cisco ISE Device Administration Guide and the Cisco ISE identity-source documentation.

QUESTION NO: 31

An administrator needs to connect ISE to Active Directory as an external authentication source and allow the proper ports through the firewall. Which two ports should be opened to accomplish this task? (Choose two.)

A. TELNET: 23

B. HTTPS: 443

C. HTTP: 80

D. LDAP: 389

E. MSRPC:445

ANSWER: D E

Explanation:

LDAP: 389 and **MSRPC:445** are required for core Cisco ISE communication with Microsoft Active Directory. ISE uses LDAP on port 389 to perform directory lookups against domain controllers, including queries for users, computers, and AD group membership. Those lookups enable ISE to use AD as an external identity source during authentication and authorization processing.

TCP port 445 supports Microsoft RPC-related communications carried over SMB, which ISE requires as part of its AD domain integration and ongoing interaction with domain-controller services. In particular, ISE must be able to access the AD resources and services needed to join and operate as a domain member. Cisco's AD integration guidance identifies LDAP and Microsoft RPC/SMB connectivity among the required communications between ISE and domain controllers.

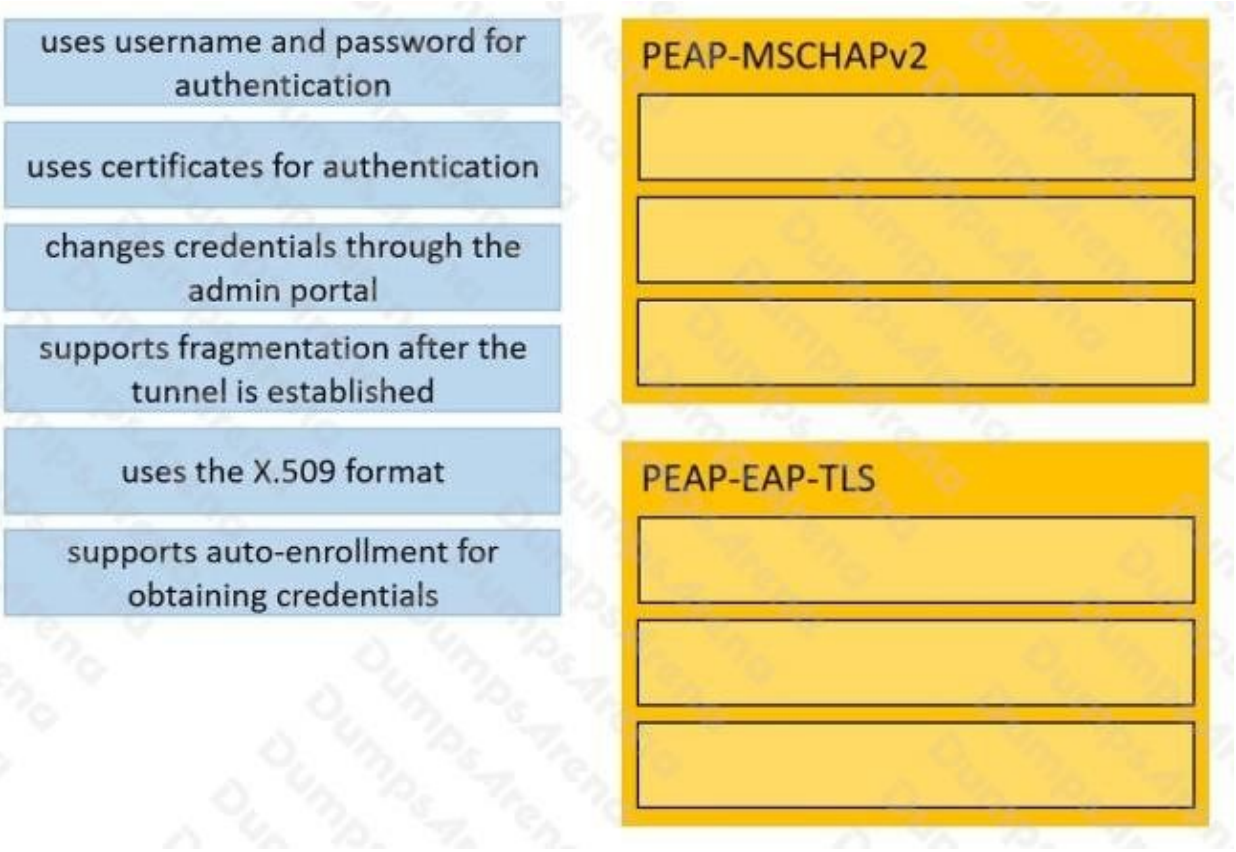
These ports are only part of the full connectivity model: a production AD integration also commonly needs supporting services such as DNS, Kerberos, and applicable RPC services. However, for the two ports represented here that directly support ISE's LDAP directory access and Microsoft RPC/SMB AD communication, LDAP port 389 and MSRPC port 445 are the correct selections. See Cisco's Active Directory integration guidance and Microsoft's service and network port requirements.

QUESTION NO: 32 - (DRAG DROP)

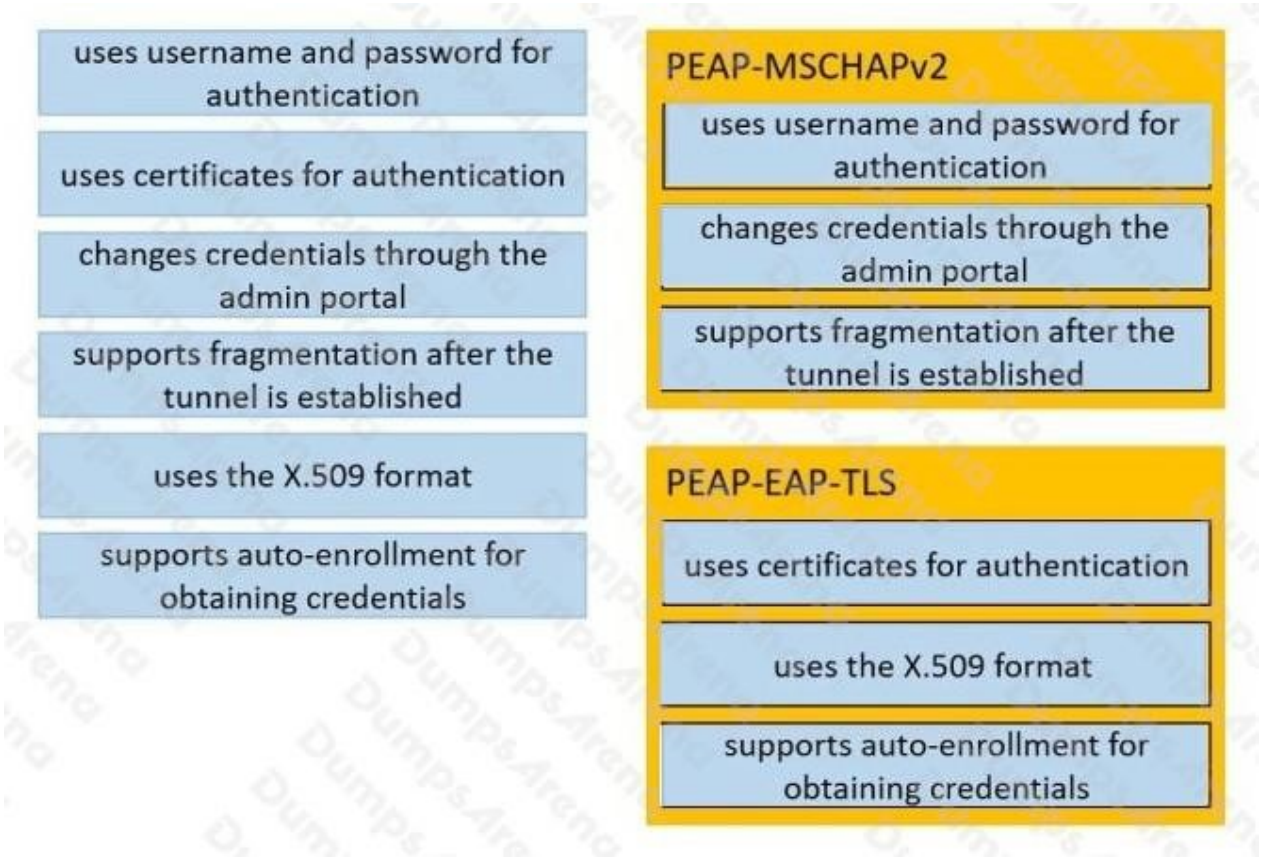
DRAG DROP

An organization wants to implement 802.1X and is debating whether to use PEAP-MSCHAPv2 or PEAP-EAP-TLS for authentication. Drag the characteristics on the left to the corresponding protocol on the right.

Select and Place:



ANSWER:



Explanation:

PEAP-MSCHAPv2 is correctly associated with username-and-password authentication because MSCHAPv2 is a password-based challenge-response method carried inside the protected PEAP tunnel. The tunnel protects the user's credential exchange from exposure on the access network, while the identity itself is normally validated against a directory-backed

identity store. Since the credential in this model is a user password, credential lifecycle tasks naturally include password updates or changes made through an administrative portal. The characteristic concerning fragmentation after the tunnel is established also belongs with the PEAP-MSCHAPv2 flow in this question's protocol comparison, reflecting the PEAP tunneled exchange behavior after the outer TLS channel is in place.

PEAP-EAP-TLS is correctly associated with certificate authentication because the inner EAP-TLS exchange authenticates the endpoint or user by presenting a client certificate rather than by proving knowledge of a password. These client certificates use the X.509 certificate format, which contains the subject identity, public key, issuer information, validity period, and digital signature required for PKI-based trust validation. In an enterprise deployment, issuing and renewing those certificates manually would be difficult to operate at scale. Auto-enrollment is therefore an appropriate characteristic for this method: a managed endpoint can obtain and renew its authentication certificate from an enterprise certificate authority according to policy. This makes certificate-based access practical for large managed-device environments. The certificate and TLS behavior underlying EAP-TLS is specified in RFC 5216, while Microsoft's overview of supported enterprise EAP methods describes the practical use of PEAP with MS-CHAP v2 and certificate-based EAP-TLS in network access deployments: EAP methods documentation.

QUESTION NO: 33

An administrator is configuring RADIUS on a Cisco switch with a key set to Cisc403012128 but is receiving the error "Authentication failed: 22040 Wrong password or invalid shared secret. "what must be done to address this issue?

A. Add the network device as a NAD inside Cisco ISE using the existing key.

B. Configure the key on the Cisco ISE instead of the Cisco switch.

C. Use a key that is between eight and ten characters.

D. Validate that the key is correct on both the Cisco switch as well as Cisco ISE.

ANSWER: D

Explanation:

Validate that the key is correct on both the Cisco switch as well as Cisco ISE. Cisco ISE message 22040 indicates that ISE could not validate the RADIUS request using the shared secret associated with the requesting network access device. The RADIUS shared secret must match exactly between the switch's configured RADIUS server definition and the corresponding Network Device entry in Cisco ISE. Shared secrets are case-sensitive, so differences in capitalization, characters, or inadvertent spaces cause the request validation to fail. The administrator should also verify that the source IP address used by the switch is the IP address configured for that specific Network Device in ISE. If ISE identifies the request as coming from a different device entry, it may apply a different shared secret and produce the same error. After correcting the switch configuration or the ISE Network Device shared secret so they are identical, the administrator should save the configuration and retest RADIUS authentication. Cisco documents error 22040 as a wrong password or invalid shared-secret condition and recommends checking the shared secret on both the network device and ISE. See Cisco's 22040 RADIUS troubleshooting guidance and the Cisco ISE Network Device management documentation.

QUESTION NO: 34

An employee must access the internet through the corporate network from a new mobile device that does not support native supplicant provisioning provided by Cisco ISE. Which portal must the employee use to provision to the device?

A. BYOD

B. Personal Device

C. My Devices

D. Client Provisioning

ANSWER: D

Explanation:

Client Provisioning is correct because it is the Cisco ISE portal and workflow used when an endpoint requires a downloadable provisioning component rather than configuration through the operating system's native supplicant. In this scenario, the mobile device cannot use native supplicant provisioning, so ISE must deliver the appropriate client-side provisioning resource to establish the required enterprise network-access configuration. Depending on the configured deployment and supported endpoint platform, this can include Cisco Secure Client components, profiles, certificates, and settings needed for secure access.

ISE applies client-provisioning policies after identifying the endpoint and evaluating the authorization result. Those policies determine which provisioning resources are offered and direct the user to the Client Provisioning portal to download and install them. This enables the device to be prepared for the corporate access policy even when ISE cannot directly configure the device's built-in network supplicant. Cisco's ISE administration documentation describes Client Provisioning as the feature for defining client-provisioning resources and policies used to distribute endpoint software and configuration. See Cisco's Identity Services Engine Administrator Guide and the Cisco ISE configuration guide library.

QUESTION NO: 35

Which two values are compared by the binary comparison function in authentication that is based on Active Directory?

A. user-presented certificate and a certificate stored in Active Directory

B. MS-CHAPv2 provided machine credentials and credentials stored in Active Directory

C. user-presented password hash and a hash stored in Active Directory

D. subject alternative name and the common name

ANSWER: A

Explanation:

In Cisco ISE certificate-based authentication with Active Directory as the external identity source, binary comparison compares the complete certificate presented by the endpoint with the certificate retrieved for the corresponding Active Directory account. ISE uses this method when it must verify that the authenticating user or machine possesses the same certificate that is associated with that AD identity, rather than merely using a text identity value extracted from a certificate field. The comparison is performed on the certificate data itself, providing an exact certificate match and binding the authentication attempt to the certificate stored in Active Directory. This is useful in deployments that publish user or computer certificates to AD and want ISE to validate the presented certificate against that directory-held certificate as part of the identity lookup and authentication process. Cisco documents certificate-based authentication and Active Directory integration in its ISE administration guidance: Cisco ISE Administrator Guide and Cisco ISE Installation and Configuration Guides.

QUESTION NO: 36

A network administrator must configure endpoints using an 802.1X authentication method with EAP identity certificates that are provided by the Cisco ISE. When the endpoint presents the identity certificate to Cisco ISE to validate the certificate, endpoints must be authorized to connect to the network.

Which EAP type must be configured by the network administrator to complete this task?

A. EAP-TTLS

B. EAP-TLS

C. EAP-FAST

D. EAP-PEAP-MSCHAPv2

ANSWER: B

Explanation:

EAP-TLS is the appropriate EAP method because it provides certificate-based, mutual authentication for 802.1X network access. In an EAP-TLS exchange, Cisco ISE presents a server certificate to the endpoint, and the endpoint presents its own identity certificate to Cisco ISE during the TLS handshake. ISE validates the endpoint certificate by checking its issuing CA and certificate chain, validity dates, intended usage, and—where configured—certificate revocation status. ISE can use a certificate issued through its internal certificate authority capabilities or a certificate from an external PKI, provided that ISE trusts the issuing CA and is configured to process the certificate for authentication.

After successful EAP-TLS authentication, Cisco ISE evaluates the endpoint against its authorization policy and returns the applicable authorization result to the network access device. That result can permit access and apply controls such as an authorization VLAN, downloadable ACL, or security group tag. This certificate-based workflow directly meets the requirement for endpoints to present identity certificates for Cisco ISE validation before network authorization. Cisco documents EAP-TLS as the EAP type for client-certificate authentication with ISE: Configure EAP-TLS Authentication with ISE. See also Cisco's ISE EAP Types documentation.

QUESTION NO: 37

An administrator needs to add a new third party network device to be used with Cisco ISE for Guest and BYOD authorizations. Which two features must be configured under Network Device Profile to achieve this? (Choose two.)

A. dACL

B. TACACS

C. URL Redirect

D. SNMP community

E. CoA Type

ANSWER: C E

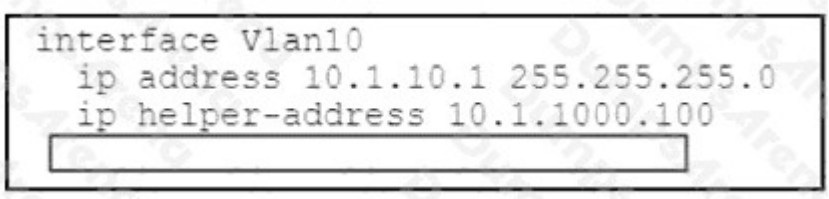
Explanation:

URL Redirect and **CoA Type** are the Network Device Profile capabilities needed for third-party network access devices participating in Cisco ISE Guest and BYOD workflows. URL Redirect tells ISE that the device supports receiving and enforcing a RADIUS redirect attribute. This lets an unauthenticated or limited-access client be directed to the appropriate Cisco ISE guest portal or BYOD onboarding portal, where the user can accept terms, authenticate, register a device, or complete provisioning.

CoA Type enables Cisco ISE to use RADIUS Change of Authorization or session disconnect behavior appropriate to that device. After the guest or BYOD portal workflow completes, ISE must trigger a new authorization evaluation so that the endpoint moves from its initial redirect or restricted-access authorization state to the access policy granted after successful authentication or registration. Configuring the applicable CoA behavior in the device profile allows this transition to occur without relying on the existing session to expire naturally. Cisco ISE documents Network Device Profiles as the location for defining NAD capabilities such as URL redirection and CoA support; the CoA protocol behavior is standardized by RFC 5176. See the Cisco ISE Network Access Administration Guide and RFC 5176.

QUESTION NO: 38

Refer to the exhibit.



An engineer must configure a Cisco switch to send DHCP probes to a Cisco ISE Policy Service Node with IP address 10.1.100.6 on interface VLAN 10. Which code snippet completes the configuration?

A. ip helper-address 10.1.100.6

B. ip dhcp-address 10.1.100.6

C. ip dhcp-relay 10.1.100.6

D. ip helper-address 10.1.10.6

ANSWER: A

Explanation:

`ip helper-address 10.1.100.6` is the correct interface-level command. DHCP clients initially communicate by broadcast because they do not yet have an assigned IP address or sufficient routing information to reach a server on another subnet. When configured on the Layer 3 interface for VLAN 10, the helper-address function relays the relevant DHCP broadcast traffic as unicast UDP traffic to the specified destination. Adding the Cisco ISE Policy Service Node address as a helper address enables the ISE DHCP probe to receive DHCP request and reply information for endpoints on that VLAN.

ISE uses the DHCP attributes it observes for endpoint profiling. These can include values such as the client hardware address, requested address, hostname, vendor class identifier, and parameter request list. The command belongs under the VLAN 10 switched virtual interface because that interface is the routed gateway that receives broadcasts from devices in that VLAN. Cisco IOS supports multiple helper-address entries on an interface, so the ISE node can be configured in addition to the production DHCP server or relay destination as required by the deployment design. Cisco documents DHCP relay configuration with `ip helper-address` at Cisco DHCP Relay Agent Configuration; ISE profiling guidance is available in the Cisco ISE Administrator Guide.

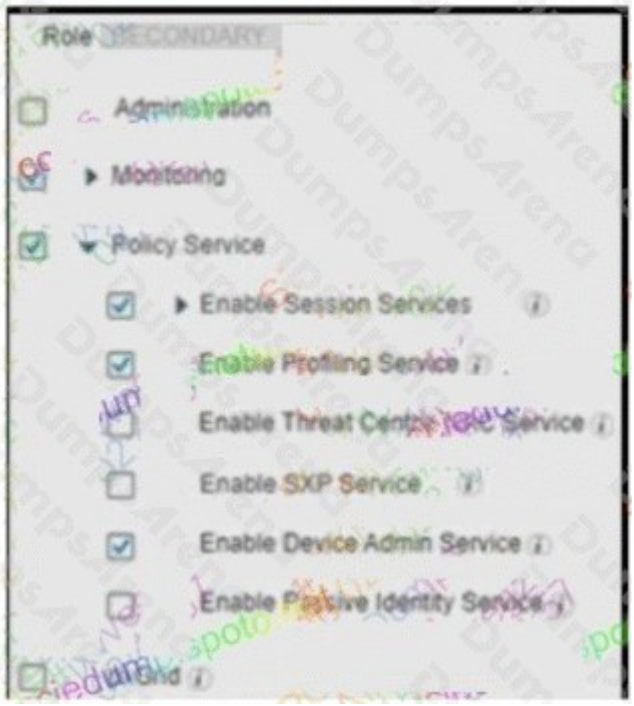
QUESTION NO: 39

An engineer builds a five-node distributed Cisco ISE deployment The first two deployed nodes are responsible for the primary and secondary administration and monitoring personas Which persona configuration is necessary to have the remaining three Cisco ISE nodes serve as dedicated nodes in the Cisco ISE cube that is responsible only for handling the RADIUS and TACACS+ authentication requests, identity lookups, and policy evaluation?

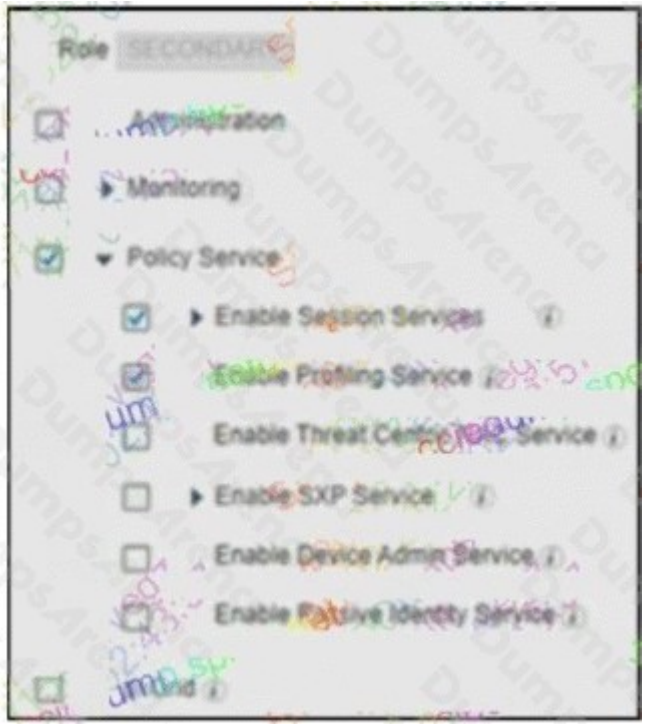
A)



B)


Role SECONDARY
Administration
Monitoring
Policy Service
Enable Session Services
Enable Profiling Service
Enable Threat Centric NAC Service
Enable SXP Service
Enable Device Admin Service
Enable Passive Identity Service
pxGrid

C)


Role SECONDARY
Administration
Monitoring
Policy Service
Enable Session Services
Enable Profiling Service
Enable Threat Centric NAC Service
Enable SXP Service
Enable Device Admin Service
Enable Passive Identity Service
pxGrid

D)



A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: D

Explanation:

Option D is correct because dedicated Cisco Identity Services Engine workhorse nodes must be assigned only the Policy Service persona. A Policy Service Node receives and processes RADIUS and TACACS+ requests from network devices, performs the configured authentication and authorization policy evaluation, and queries internal or external identity stores, such as Active Directory or LDAP, when policy processing requires identity information. This is the ISE persona intended to provide scalable access-control services to endpoints, users, and network-device administrators.

In the described five-node distributed deployment, the Administration and Monitoring responsibilities are already hosted redundantly by the first two nodes. Assigning only Policy Service to each of the remaining three nodes keeps them dedicated to real-time policy processing rather than management, configuration replication, logging, reporting, or troubleshooting functions. This separation allows the deployment to scale authentication and authorization capacity independently while retaining dedicated administration and monitoring infrastructure. Cisco describes the Policy Service persona as the component that provides RADIUS and TACACS+ services and enforces policy decisions in a distributed ISE deployment. See Cisco's Identity Services Engine Administration Guide: Deploy Cisco ISE and the Cisco ISE installation and configuration guides.

QUESTION NO: 40

Which two probes must be enabled for the ARP cache to function in the Cisco ISE profile service so that a user can reliably bind the IP address and MAC addresses of endpoints? (Choose two.)

A. NetFlow

B. SNMP

C. HTTP

D. DHCP

E. RADIUS

ANSWER: D E

Explanation:

The correct probes are **DHCP** and **RADIUS**. Cisco ISE Profiling uses its ARP cache to maintain a reliable association between an endpoint's IP address and MAC address. This mapping requires probe data that includes both identity values. The DHCP probe supplies endpoint addressing details from DHCP exchanges, including the requested IP address and the client MAC address. The RADIUS probe can provide the assigned endpoint address through the RADIUS Framed-IP-Address attribute while associating it with the endpoint MAC address used for the session. By enabling DHCP or RADIUS probing, ISE receives the information needed to create and maintain the IP-to-MAC bindings in its profiling ARP cache. In a deployment where both DHCP and RADIUS data are available, enabling both probes provides complementary visibility and improves the consistency of endpoint context available to profiling policies. Cisco documents that the ARP cache depends on DHCP or RADIUS probe data because these probes carry the IP and MAC address information required for the mapping. See Cisco's Identity Services Engine Administrator Guide and the Cisco ISE Profiling documentation.

QUESTION NO: 41

An engineer must use Cisco ISE to provide network access to endpoints that cannot support 802.1X. The endpoint MAC addresses must be allowlisted by configuring an endpoint identity group. These configurations were performed:

Configured an identity group named allowlist

Configured the endpoints to use the MAC address of incompatible 802.1X devices

Added the endpoints to the allowlist identity group

Configured an authentication policy for MAB users

What must be configured?

A. Authorization profile that has the PermitAccess permission and matches the allowlist identity group

B. Authentication profile that has the PermitAccess permission and matches the allowlist identity group

C. Authorization policy that has the PermitAccess permission and matches the allowlist identity group

D. Logical profile that matches the allowlist identity group based on the configured policy

ANSWER: C

Explanation:

Authorization policy that has the PermitAccess permission and matches the allowlist identity group is required after MAC Authentication Bypass (MAB) successfully authenticates an endpoint. MAB submits the endpoint MAC address as the credential, and Cisco ISE uses its internal endpoint database to identify the endpoint and its assigned Endpoint Identity Group. Authentication establishes that the MAB request is accepted; authorization then determines the network-access outcome for that authenticated endpoint.

The authorization rule should use a condition that matches the endpoint's identity-group membership, such as an Endpoint Identity Group condition equal to *allowlist*. The rule must return an authorization result that permits access. In Cisco ISE, this is commonly the built-in *PermitAccess* authorization profile, or a custom authorization profile that allows access and optionally applies a VLAN, downloadable ACL, security group tag, or other enforcement attributes. This policy-based mapping ensures that only MAC addresses placed in the allowlist group receive the intended authorization decision.

Cisco documents MAB as an authentication method for devices that do not support 802.1X and describes authorization policies as the mechanism that evaluates conditions and returns authorization results. See Cisco: Configure MAC Authentication Bypass and Cisco ISE Policy Administration Guide.

QUESTION NO: 42

Which two features should be used on Cisco ISE to enable the TACACS+ feature? (Choose two)

A. External TACACS Servers

B. Device Admin Service

C. Device Administration License

D. Server Sequence

E. Command Sets

ANSWER: B C

Explanation:

Device Admin Service and **Device Administration License** are the foundational requirements for Cisco ISE device-administration AAA using TACACS+. Device Admin Service must be enabled on the relevant Policy Service Node. Enabling this service activates the ISE device-administration persona and permits the node to listen for, process, and evaluate TACACS+ authentication, authorization, and accounting requests from managed network devices. It also makes the device-administration policy configuration available, including authorization policy rules and result elements used for administrative access control.

A Device Administration License entitlement is also required for Cisco ISE to provide TACACS+ device-administration functionality. Licensing must be installed and assigned appropriately in the deployment before the service can be used for managing administrator access to routers, switches, firewalls, and similar infrastructure. After these two prerequisites are in place, administrators can add network devices, define device-admin identity sources and authorization rules, and optionally configure command authorization with command sets. Cisco documents the Device Administration service and its license as the prerequisites for configuring TACACS+ device administration. See the Cisco ISE Device Administration Guide and Cisco ISE Licensing documentation.

QUESTION NO: 43

A Cisco ISE server sends a CoA to a NAD after a user logs in successfully using CWA Which action does the CoA perform?

A. It terminates the client session

B. It applies the downloadable ACL provided in the CoA

C. It applies new permissions provided in the CoA to the client session.

D. It triggers the NAD to reauthenticate the client

ANSWER: D

Explanation:

It triggers the NAD to reauthenticate the client. In a Central Web Authentication (CWA) workflow, the endpoint initially connects under a restricted, preauthentication authorization result that permits redirection to the guest or login portal. After the user successfully completes portal authentication, Cisco ISE has a new authorization outcome to enforce for that already-established endpoint session. ISE sends a RADIUS Change of Authorization (CoA) request to the network access device (NAD) so that the NAD refreshes authorization for the client rather than waiting for the session to end or for the client to reconnect manually.

For this CWA transition, the relevant CoA behavior is a reauthentication request. The NAD initiates reauthentication of the client, resulting in a new RADIUS authorization exchange with ISE. ISE can then return the postauthentication authorization profile and associated policy attributes, allowing the NAD to move the client out of the redirect/restricted state and into its authorized access state. This immediate policy transition is central to delivering access promptly after successful CWA login. Cisco documents CoA as the mechanism used by ISE to alter authorization for an active session and describes CWA deployment behavior in its guidance: Cisco: Central Web Authentication and Cisco: Configure Web Authentication with ISE.

QUESTION NO: 44

An administrator is adding network devices for a new medical building into Cisco ISE. These devices must be in a network device group that is identifying them as "Medical Switch" so that the policies can be made separately for the endpoints connecting through them. Which configuration item must be changed in the network device within Cisco ISE to accomplish this goal?

A. Change the device type to Medical Switch.

B. Change the device profile to Medical Switch.

C. Change the model name to Medical Switch.

D. Change the device location to Medical Switch.

ANSWER: A

Explanation:

Change the device type to Medical Switch. Cisco ISE uses Network Device Groups (NDGs) to classify network access devices and to make those classifications available as policy conditions. The built-in Device Type NDG hierarchy is intended to identify the functional type or category of a network device, such as switches, routers, wireless controllers, or more specific organizational classifications. Creating or selecting a Device Type value named Medical Switch and assigning it to each relevant network device identifies the devices consistently for policy evaluation.

When an endpoint authenticates through one of those switches, ISE can use the device's NDG assignment as contextual information in authentication or authorization policy. This enables rules that apply specifically to sessions originating through devices classified as Medical Switch, independently of sessions arriving through other switch groups or device categories. The assignment is made in the network device definition, under its Network Device Group settings, which makes this approach scalable as additional medical-building switches are added.

Cisco documents that NDGs, including Device Type, are used to group network devices and can be selected when configuring an individual network device. See the Cisco ISE Administrator Guide and Cisco's Identity Services Engine user-guide index.

QUESTION NO: 45

Users in an organization report issues about having to remember multiple usernames and passwords. The network administrator wants the existing Cisco ISE deployment to utilize an external identity source to alleviate this issue. Which two requirements must be met to implement this change? (Choose two.)

A. Enable IPC access over port 80.

B. Ensure that the NAT address is properly configured

C. Establish access to one Global Catalog server.

D. Provide domain administrator access to Active Directory.

E. Configure a secure LDAP connection.

ANSWER: C D

Explanation:

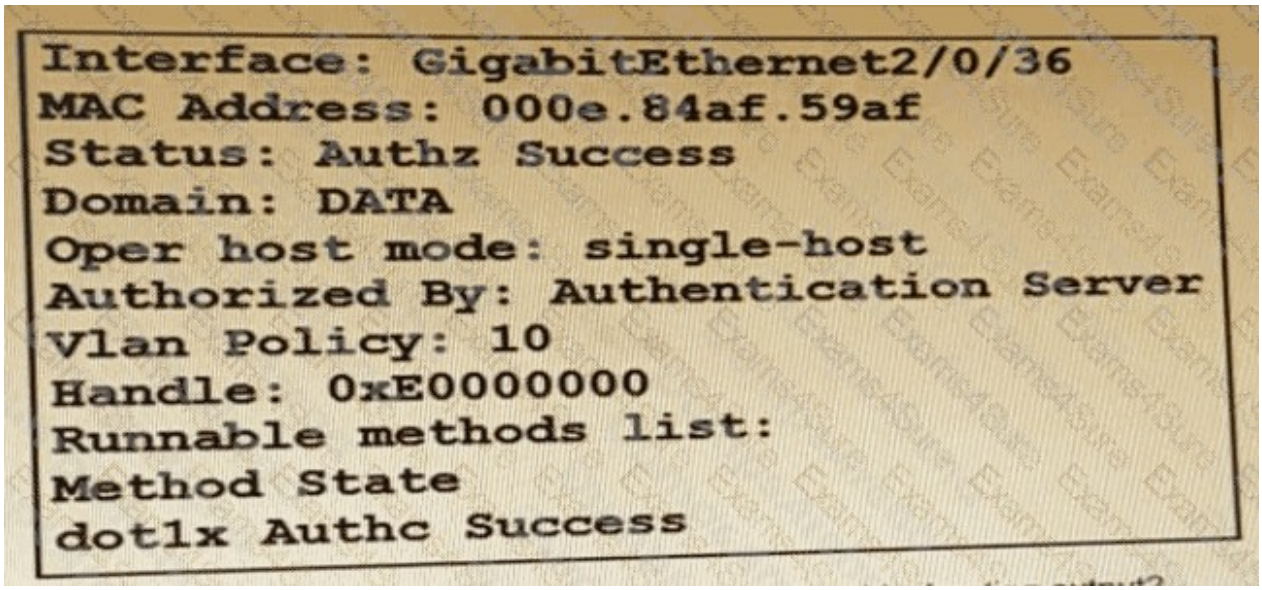
Cisco ISE can integrate with Microsoft Active Directory as an external identity source, allowing network-access authentication and authorization to use established domain identities rather than separate ISE-local credentials. Establishing access to one Global Catalog server is required because ISE uses the Global Catalog to search directory objects across the Active Directory forest and to obtain the user and group information needed for identity lookup and policy evaluation. Reliable DNS resolution and network reachability to the relevant domain controllers and Global Catalog are therefore essential to the integration.

Providing domain administrator access to Active Directory satisfies the permissions needed to join ISE to the AD domain and create or manage the ISE computer account and its machine trust relationship. In a production deployment, an organization may delegate the necessary computer-account and domain-join permissions to a less-privileged service account rather than

use a full Domain Admin account; however, the supplied domain-administrator access meets the requirement stated in the question. Once joined, ISE can query AD users and groups for authentication and authorization decisions. Cisco documents the AD join workflow and directory-service prerequisites in its Cisco ISE Administrator Guide; Microsoft describes the forest-wide directory-search role of the Active Directory Global Catalog.

QUESTION NO: 46

Refer to the exhibit:



Which command is typed within the CU of a switch to view the troubleshooting output?

A. show authentication sessions mac 000e.84af.59af details

B. show authentication registrations

C. show authentication interface gigabitethemet2/0/36

D. show authentication sessions method

ANSWER: A

Explanation:

The command `show authentication sessions mac 000e.84af.59af details` is the appropriate switch CLI command because it queries the access-session table for the endpoint identified by that specific MAC address and requests the detailed session output. This is useful for troubleshooting an individual wired client because the detailed view consolidates the information associated with its active authentication session, such as the interface, current session state, authentication method and result, authorization state, assigned policy information, accounting details, and session identifiers. Specifying the MAC address is especially valuable when a switch has many authenticated endpoints: it limits the output to the client implicated by the troubleshooting evidence rather than requiring an administrator to manually locate the relevant session in broader output. The command uses Cisco IOS authentication-session operational data, which is central to validating 802.1X, MAB, and ISE authorization behavior on an access port. Cisco's identity-based networking configuration documentation describes monitoring authentication sessions and their associated authorization information: Cisco IOS XE Securing Identity-Based Networking Guide. This operational troubleshooting area is also within the scope of Cisco's ISE implementation curriculum: Cisco 300-715 SISE exam overview.